International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org, editorijettcs@gmail.com
Volume 9, Issue 5, September - October 2020 ISSN 2278-6856

# An Overview of Major Developments, Applications and Challenges in Quantum Cryptography

**Amod Aggarwal[1] and K Shahana[2]**

[1]Delhi Earth Station, Space Applications Centre, ISRO,
New Delhi, India

[2]Delhi Earth Station, Space Applications Centre, ISRO,
New Delhi, India

**Abstract:** ***Modern Cryptography is based on computationally-secure algorithms. With the emergence of quantum computers, it is possible to crack the heritage computationally-secure algorithms. Quantum Cryptography/ Quantum Key Distribution is a new and evolving field for secure communication. It is able to detect eavesdropping in a failsafe manner as it is impossible to copy the data encoded in a quantum state without changing its state. This paper discusses the types of modern cryptography, limitations of their use in practical applications, quantum safe-encryption schemes that overcome the challenges associated with the modern cryptography, and various aspects of one of the safe encryption schemes i.e. quantum cryptography. This paper focuses on discussing the work done in the field of quantum cryptography such as line-based and space-based experiments and the challenges associated with its practical implementation. Impact of satellite orbit is also addressed, recommending a preferred scheme for a global network based on the quantum approach. This paper also provides a detailed discussion of various quantum cryptography protocols.***

**Keywords:** Quantum Superposition, Quantum Entanglement, BB84, BB92, SARG04, Decoy State protocol

## 1. INTRODUCTION

In this era of Internet, a lot of information is getting exchanged over the Network. Some of this information is sensitive, highly confidential and any breach in its security can lead to alarming consequences that could approach devastating proportions worldwide. Modern cryptographic techniques do not guarantee secure sharing of the secret key between sender and receiver, particularly in this era of cyber-attacks and malicious hacking. The development of quantum computers introduces another dimension to this problem, leaving systems open to what is termed as quantum attacks. Although quantum computers are still in the early development phase and their global commercial uptake will take some time, yet an eavesdropper may save encrypted information and then decrypt it later on using quantum computing. It is important to consider the future technological challenges in the field of secure data transmission and communication in order to protect critical data and prevent any potentially devastating effects. In order to cope with these limitations, a new class of cryptography i.e. Quantum Cryptography has evolved. This is an emerging field and provides a foolproof, super-secure means to communicate or exchange data. Since data transfer and communication at a global scale has become possible due to satellite-based communication, it is of utmost importance to secure the data exchange over the satellite-satellite links and satellite-ground links along with fibre-based links.

This paper is organized as follows. Section I gives the basic introduction to modern cryptography, its types and their pros and cons. Section II provides the brief description of Quantum-Safe Encryption schemes. The basic terminology related to Quantum Cryptography is introduced in Section III. Section IV discusses the work done in the field of Quantum Cryptography. It includes the discussion of the line-based and satellite-based QKD experiments and the challenges associated with them. Section V describes some of the standard Quantum Cryptography protocols in details. The conclusions are drawn in Section VI.

## 2. MODERN CRYPTOGRAPHY

Traditional Cryptography and Modern Cryptography both use the concepts of mathematics for encryption and decryption of data. Modern Cryptography is an advanced form of Traditional Cryptography and it uses more complex mathematics in terms of computation to secure the network communication. Modern cryptography can be divided into two types: Symmetric Cryptography and Asymmetric Cryptography.

### 2.1 Symmetric Cryptography

This category of cryptography is based on the concept of sharing the same secret key between the sender and the receiver. The same cryptographic algorithm is used to encrypt and decrypt the data at both ends. The problem with this method is the secured sharing of the secret key. It is of utmost importance that the key should be shared in a way that it is known only to the sender and the receiver. Moreover, the key must be unique for every session of data sharing. Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are examples of symmetric cryptography algorithms.

### 2.2 Symmetric Cryptography

This technique uses a public-private key pair. The sender encrypts the data using the public key of the receiver which is known to everyone. But the private key used for decryption is known only to the intended receiver. This cryptography is based on the use of mathematical functions that are easy to perform in one direction but hard to invert. These are also termed as one-way functions. For example: multiplication and factorization. It is easy to multiply two numbers but it is hard to find the prime factors of a given number. Some asymmetric cryptography algorithms are Rivest-Shamir-Adleman (RSA), Diffie-Hellman and Elliptic Curve Digital Signature Algorithm.

Asymmetric algorithms seem superior to symmetric algorithms as they do not require sharing of the secret key between the sender and the receiver. Instead, they use public-private key pair. But this does not imply that they have replaced symmetric algorithms because they are computationally very expensive to use. Asymmetric algorithms are used along with the symmetric key algorithms for secure data exchange. They are used mainly for secure key exchange between the sender and the receiver because actual data is very large in size. The encryption of the huge amount of data using asymmetric algorithms needs considerable computational power.

These cryptography techniques are computationally secure as they assume a limited computational power of the eavesdropper. RSA relies on the difficulty of finding the prime factors of some large number; Diffie Hellman uses the difficulty of computing discrete logarithms while Elliptic Curve DSA relies on the computational difficulty of solving the elliptic-curve logarithmic problem. Yet, with advancements in technology, quantum algorithms that can crack these modern key algorithms have also been developed. These[1] modern key algorithms are also weak against quantum computers. There is a need of algorithms which are robust with respect to quantum computations. Quantum-safe encryption schemes are the new methods to securely distribute the secret keys between the involved parties.

## 3. Quantum-Safe Encryption Schemes

There are two approaches to quantum-safe encryption schemes.

### 3.1 Post-quantum cryptography

This focuses on developing more advanced native public key encryption schemes such as hash-based or code-based encryption schemes. The known quantum attacks such as Shor's Algorithm and Grover's Algorithm are not capable of cracking these schemes. These techniques have the advantage of being compatible with existing crypto-infrastructure because they use the classical channels for key and data exchange. They have high key rates and are available over long distances. Yet, these algorithms have proved to be secure against only the known quantum attacks. If a stronger algorithm for quantum attack is developed in future, there is a risk of breaching the security of the data.

### 3.2 Quantum Cryptography

This provides the information-theoretic security based on the fundamental laws of quantum physics. An information-theoretic secure system is a system that remains secure even if an attacker has unlimited resources available to perform the cryptographic analysis.

## 4 Basic Terminology Related to Quantum Cryptography

Quantum cryptography is based on the laws of quantum physics and uses the concept of qubits for transferring the data over the network. In modern cryptography, a bunch of photons represents each bit of data whereas in quantum cryptography, the individual photon carries one bit of data across the channel. This makes it more secure due to the inherent encryption of the data. This section introduced some basic terms related to quantum cryptography. Though these are addressed in literature in greater detail [2][3][4], a brief introduction is provided for sake of completeness.

### 4.1 Basic Terms of Quantum Cryptography

The basic terms of quantum cryptography are described below:

1. *Photon/Quantum:* It is a discrete packet of electromagnetic energy as per physics definition. In quantum cryptography, this photon is used to represent one qubit.
2. *Qubits:* A classical computer uses a binary bit to store the data whereas a quantum computer uses qubits. A binary bit can take either of two values (0 or 1) at a time. A qubit uses superposition of all available states to store the information that allows a quantum computer to operate on all possible values at once. Qubit collapses into a single state on measuring it.
3. *Polarization bases:* It is the process of passing a photon through a polarization filter which causes it to spin in a particular state. A photon can spin in four states: diagonal (±45°), horizontal or vertical. If a photon polarized in one state is passed through the filter polarized in the other state, then its actual state is absorbed and it is polarized in some random state.
4. *Non-orthogonal polarization/phase basis sets:* In this set, state of one basis measured using state of other basis of a set yields some random result. Rectilinear basis and diagonal basis together form a non-orthogonal basis set. Rectilinear basis consists of vertical and horizontal linearly polarized state whereas diagonal basis consists of linearly polarized light at 45°and -45°.
5. *Quantum Key Distribution (QKD):* QKD is a way of distributing a key between the sender and the receiver using photons. Real world QKD system consists of three major components: source, channel and detector.

*a) Source:* It emits the photons on the sender's side. There are various practical photon sources for QKD such as weak coherent-state source, thermal source, and entangled photon source [5]. The weak coherent-state source is the most widely employed in QKD as it can be easily realized using attenuated laser pulses.

*b) Channel:* Two type of channels are used for the key distribution. Quantum channels that allows light to pass through them are used for the transfer of key bits using photons. Classical channels are used for the post processing such as error correction and privacy amplification.

*c) Detector:* It detects the photons on the receiver's side.

### 4.2 Quantum Properties

There are two important quantum properties i.e. Quantum Superposition and Quantum Entanglement, which have no meaning without Heisenberg's Uncertainty Principle.

#### 4.2.1 Quantum Superposition

It means that the quantum can have many possible states but it exists in all of them simultaneously until it is measured. Quantum is described by the Schrodinger wave equation. The wave function consists of many states along with their probabilities. When the quantum is measured, then the wave function collapses and one of the state is selected that has the maximum value of probability.

#### 4.2.2 Quantum Entanglement

The properties of the two paired photons are linked i.e. they have orthogonal/perpendicular polarizations. Measurement of one photon will automatically cause the other photon to acquire the opposite state immediately irrespective of the distance between them i.e. if the electric field of one of the photons is vibrating vertically, the other will be vibrating horizontally.

#### 4.2.3 Quantum Channels

The optical fibre and the open-space based ground-satellite links are the two types of quantum channels that can be used for quantum communication. Both of these channels have their own pros and cons which are discussed in the succeeding section.

## 5 WORK DONE IN THE FIELD OF QUANTUM CRYPTOGRAPHY

Earlier experiments have been performed considering the ideal source of photons i.e. single photon source. Later on, it was realized that an ideal photon source is impractical as some of the light pulses emitted from devices may contain more than one photon. Then, some more secure QKD experiments were performed with practical devices that are non-ideal. In this section, we discuss various experiments sequentially from Subsection A to F.

### 5.1 Line-based QKD experiments using ideal photon sources

The first proposal of QKD i.e. BB84 protocol took place in 1984 [6]. In 1989, BB84 was demonstrated by Bennet et al. [7]. Quantum signals were transmitted between the sender and the receiver separated by only 30 cm. Later on, more implementations of QKD followed with a larger distance between the sender and the receiver. In 1991, Ekert proposed the first entanglement based QKD protocol, commonly called E91 [8]. The basic idea was to test the security of QKD by using the violation of Bell's inequality standard [9]. The approach was to put the entanglement source right in middle of the sender and the receiver. In 1992, BB92 protocol was proposed by Bennet et al [10] which used only two non-orthogonal states.

### 5.2 Line-based QKD experiments using real imperfect photon sources

In 2000, the first proposal of a hacking attack called the Photon Number Splitting (PNS) attack appeared that took advantage of loopholes in the QKD implementations [11]. This type of attack is possible due to the fact that perfect single photon sources are impractical. Real-life QKD systems use attenuated laser pulses (i.e. a weak coherent states) that generate the pulses having more than one photon.

In PNS Attack, the attacker blocks all the single photon signals and splits all multi-photon signals. It sends one copy to the receiver and retains other copy with itself until the sender and the receiver exchange information regarding the correct basis. It can then use the basis information to measure the photons it has kept with itself.

In 2003, Hwang [12] proposed the decoy state method in order to tackle the sophisticated PNS attack. In 2004, Lo et al. [13] showed that only a few decoy states are sufficient as the states with large photon numbers contribute almost negligible in comparison to the states with small photon numbers. They proposed a Vacuum+ Weak decoy state protocol. Wang [14] analysed the security of Vacuum+ Weak decoy state protocol. The significance of vacuum state is that it helps in estimating the background noise. In 2005, it was shown that the decoy state QKD can be secure over 140km of telecom fibres which implied that decoy state method can substantially increase both the distance and the key generation rate of QKD [15]. They derived the general theorem for a decoy state protocol which states that there should be any two weak decoy states.

Both of the decoy states can be non-vacuum or one can be vacuum. They performed an optimization of the key generation rate as a function of the intensities of the two decoy states and a signal state and showed that the key generation rate is optimized, when both the decoy states are weak. Another protocol proposed to defeat the PNS attack was SARG04 [16] which is discussed in detail in Section V.

### 5.3 Challenges in Line-based Quantum Communication

In order to use quantum cryptography for practical applications, it is important to increase the key generation rate and the distance between the sender and the receiver. As the optical signal gets attenuated with distance, amplification of signal by optical relay stations/repeaters is required. But classical relay stations require measurement of the signal to get the key bits which are to be relayed. This makes the nodes susceptible to hacking although the number of vulnerable points is reduced.

The solution is to establish the ground-satellite quantum link or building up the quantum repeaters. Both solutions are challenging and the practical deployment of the quantum repeaters is beyond the current technology. But, a lot of work has been reported in the field of the ground-satellite quantum links.

### 5.4 Significance of Satellite-based QKD

In present scenario, the communication and transmission of data such as video, images, voice and text is possible at a global scale. Two parties who are separated by huge distances such as inter-continental ranges can communicate and transmit data at a very high speed. This is possible due to satellite-based communication. Satellite-based network has also established the communication link at places where line-based links are very difficult to install such as mountains and water bodies. Therefore, it is very important to have secure satellite based communication. Satellite based communication uses modern cryptographic techniques for maintaining the integrity of satellite uplink and downlink transmissions. As mentioned earlier, these techniques can be compromised by quantum algorithms and quantum computers; hence, it is important to use quantum cryptography for satellite based transmissions.

Quantum-enabled satellites can also be used to exchange the secret key between the two ground stations which enables secure data exchange between them. Satellite-based QKD can make it possible to transmit photons over large distances such as pan-global. Quantum satellites can act as trusted relay nodes for the photons and can enable secure transmission of data between the ground stations separated by a large distance.

As opposed to fibre-based links, that have high channel loss and decoherence; the attenuation of photons in vacuum is nearly zero while being very less in the atmosphere. Therefore, satellite-based QKD provides a promising solution for long distance secure communication.

### 5.5 Satellite-based QKD experiments

There are two different types of protocols for satellite-based QKD. These are the Prepare-and-measure protocols and the entanglement-based protocols.

In Prepare-and-measure protocols, satellite acts as a trusted central node for the two ground stations that have to communicate with each other. It establishes one QKD secret key between itself and the sender and another QKD secret key between itself and the receiver. It combines the two QKD secret keys using the mathematical operations such as XOR operation and then sends the combined key to both the sender and the receiver. The sender and the receiver are able to decode the counterpart key and are able to establish the secure communication link with each other. The satellite should be trustworthy as it knows the keys of both the sender and the receiver. In Figure 1, $QK_A$ is QKD key shared between Sender i.e. Ground Station '$GS_A$' and Relay Node. $QK_B$ is key shared between Receiver i.e. Ground Station '$GS_B$' and Relay Node. Relay Node calculates $QK_{AB}= QK_A+QK_B$ and shares it with both '$GS_A$' and '$GS_B$'. '$GS_A$' calculates $QK_B$ using $QK_{AB}$□$QK_A$. Similarly, '$GS_B$' calculates $QK_A$ using $QK_{AB}$□$QK_B$.

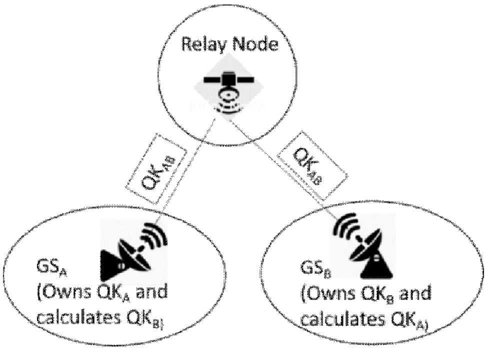
Relay Node
$QK_{AB}$
$QK_{AB}$
$GS_A$ (Owns $QK_A$ and calculates $QK_B$)
$GS_B$ (Owns $QK_B$ and calculates $QK_A$)

**Figure 1** Exchange of secret key between two ground stations using satellite as a relay node

In case of entanglement-based protocols, the satellite sends two beams of entangled photons at the same time: one beam for each ground station. The sender and the receiver measure the quantum correlations between two beams of entangled photons sent by the satellite at the same time. Its disadvantage is that it demands the line-of-sight connection of the satellite with both the ground stations at the same time. Along with that, the required correlations suffer from channel loss resulting in the decreased key rate.

In 2005, Peng et al reported the first distribution of entangled photon pairs over 13 km, beyond the effective thickness of the atmosphere [17]. This experiment showed that the entangled photons are not destroyed after propagating through the atmosphere. In 2007, two experiments i.e. entanglement-based [18] and decoy-state [19] quantum key distribution were realized on a 144 km free-space path by a European collaboration. The sender was at Canary Island of La Palma and the receiver was the optical ground station of European Space Agency at Tenerife. These experiments were significant as they increase the magnitude of distance between the sender and the receiver significantly.

In August, 2016, China launched the first quantum-communication satellite, Micius having a weight of 635 Kg. The satellite was placed in LEO at an altitude of ~500km. In 2017, a quantum-entanglement experiment was performed in which three ground stations were coordinating with the satellite. One quantum communication link was established between Delingha and Nanshen which are 1120km apart. The second quantum communication link was established between Delingha and Yunnan which are 1203km apart [16,17]. In 2017, decoy state QKD with over kHz key rate was implemented between Micius and Xinglong Observatory ground station over a distance up to 1200 km [20] [21]. It was up to 20 orders of magnitude more efficient than that expected using an optical fiber (with 0.2 dB/km loss) of the same length. The downlink protocol was adopted over uplink so that the beam divergence due to atmospheric turbulence occurs only in the last few kilometres of the distance.

Heasin Ko et al [22] demonstrated successful free-space QKD in day light using the self-developed polarization encoding chip. The experiment was performed by deploying the transmitter and receiver on two distant buildings that were 275m apart in Electronics and

Telecommunication Research Institute (ETRI), South Korea. A lot of experiments have already been performed for successful demonstration of QKD systems in day light. But, this research is of great significance as it does the detailed examination of the issues related to implementation of noise filtering techniques in practical systems. They also configured QKD systems with the self-developed polarization encoding chip that reduces the size of QKD systems significantly.

In 2019, The National Institute of Information and Communications Technology (NICT), Japan developed the world's smallest and lightest quantum-communication transmitter (SOTA: 6kg) on-board the microsatellite SOCRATES (50kg). They demonstrated that satellite based QKD can be implemented using the microsatellites. This is a significant achievement as it opens the gates for establishing the global quantum based secure network due to very small size of the satellites [23].

### 5.6 Challenges in Satellite-based QKD experiments

Although satellite based QKD seems to be a promising solution for creating a global network for secure data transmission and communication, it also has some technical challenges associated with its practical implementation. In order to use the space-based QKD, it is necessary to provide the satellite coverage to the targeted ground station all the time. Along with that, the quality of the signals should also be maintained. The signal quality is described by two parameters: Signal-to-Noise Ratio (SNR) and the key exchange rate [24]. There are two different types of satellite constellations that can be considered: LEO and GEO.

Channel losses due to diffraction are higher in GEO-based QKD because GEO satellites are at a higher altitude as compared to LEO. This results in low SNR and low key generation rate. The SNR cannot be increased by increasing the signal power as the single photon pulses have to be weak coherent pulses [25]. Only the channel attenuation and the background noise can be reduced. LEO-based QKD has comparatively less channel losses due to the proximity of LEO satellites. Drawback of LEO satellites is that they provide coverage of the location for a limited period of time whereas GEO satellites provide full-time coverage of the station. This demands the optimization of the constellation so that the ground stations can be provided full-time coverage with high SNR and key generation rate. This can be achieved by having a hybrid constellation of satellites such that LEO satellites can communicate with each other using GEO satellites and an optimized constellation of LEO satellites should be created to provide the global coverage. In addition, these LEO satellites will then communicate with major ground stations for secure data exchange and these major ground stations will be connected to sub-stations using fibre. The links between GEO satellites, LEO satellites and ground stations are shown in Figure 2 where SGEO1 is GEO satellite, SLEO1 and SLEO2 are LEO satellites, and GS1, GS2, GS3 and GS4 are ground stations.

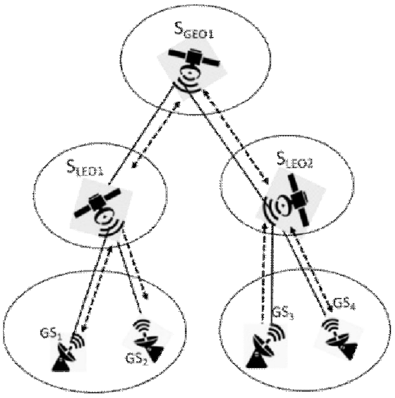

**Figure 2:** Inter-linkage between GEO satellites, LEO satellites and ground stations

## 6 Quantum Cryptography Protocols

There are two types of Quantum Cryptography protocols. These are Prepare-And-Measure protocols and Entanglement-based protocols. In Prepare-And-Measure protocols, sender prepares a single photon in a quantum state and sends it to receiver that then measures the photon. In this section, we will discuss various Prepare-and-Measure protocols.

Some of basic terminology used in context of these protocols have been described. Two polarization bases used are Rectilinear (R) and Diagonal (D). Rectilinear basis has 2 states: |h> and |v>. Diagonal basis has two states: |lcp> and |rcp>. A photon can be polarized using any of the mentioned four states. Sender, Receiver and Eavesdropper/Intruder are denoted by ‘A’, ‘B’ and ‘E’ respectively. All the protocols discussed are based on Heisenberg’s Uncertainty Principle. Since bits are represented by polarized photons in quantum cryptography, bit ‘0’ is represented by photons polarized in state |h> or |lcp>. Bit ‘1’ is represented by photons polarized in state |v> or |rcp>.

We have made an effort to explain BB84, BB92, SARG04 and Decoy State Protocol briefly and in a simplified way. We have also made the comparative analysis for better understanding.

### 6.1 BB84 protocol

It is the first QKD protocol proposed ever. It includes various steps as mentioned below:

#### 6.1.1 Exchange of the secret key (Communication over quantum channel)

Sender (A) prepares a photon randomly with either ‘R’ or ‘D’ polarization. Receiver (B) receives the photon and measures it using ‘R’ or ‘D’ on a random basis. ‘B’ records the basis used by it and the polarization measured by it for each photon.

#### 6.1.2 Final Key Extraction (Communication over public channel)

Receiver (B) communicates to Sender (A) which basis it has used for the measurement. In response, ‘A’ communicates to ‘B’ which of the bases used are correct. They delete all the bits measured with incorrect basis and the key left is called sifted key. Since B selects the basis used for measuring on random basis, the probability of ‘B’ measuring the bit using the correct basis is 50%. The errors which may occur due to corruption of bases information over the channel are rectified during ‘Error Correction’ stage.

### 6.1.3 Error Estimation and Error Correction (Communication over the public channel)

‘A’ and ‘B’ compare some randomly chosen bits in sifted key to estimate error rate ‘error_rate’ due to presence of eavesdropper or some other error sources such as noise, echo etc. If error rate ‘error_rate’ is greater than threshold ‘T’ i.e. approx. 20% of randomly chosen bits [27], then they discard key and start all over again. Otherwise, they perform error correction procedure on remaining part of key to prepare final key. After that, a privacy amplification procedure is followed over public channel in order to get a more secure and shorter key about which eavesdropper has partial information.

Table 1 provides the formal description of BB84 protocol. Here, BA represents the basis used by ‘A’ for encoding the bit and $V_A$ represents the value of the bit sent by A. $B_E$ and $B_B$ represent the basis used by ‘E’ and ‘B’ for decoding the bit respectively. $O_E$ and $O_B$ represent the bit decoded by ‘E’ and ‘B’ respectively. $Flag_{AB}$ represents whether the bases of ‘A’ and ‘B’ are same or not. $K_S$ represents the bits of the sifted key. ‘N’ corresponds to ‘No’ and ‘Y’ corresponds to ‘Yes’.

S.No.1-4 are performed in absence of ‘E’ and S.No.5-10 are performed in presence of ‘E’. In S.No.2, even though bit outcome of ‘B’ is same as that sent by ‘A’, still it is discarded during 'Final Key Extraction' Stage. This is because the bases of ‘A’ and ‘B’ do not match. Since the basis of ‘A’ and ‘B’ matches in S.No.3 and S.No.4, the bit measured by ‘B’ is retained. In S.No.8 even though bases of ‘A’ and ‘B’ are same, ‘B’ has decrypted the bit wrongly due to presence of ‘E’. ‘B’ has decrypted the bit as '1' using ‘R’ basis because ‘E’ has changed polarization basis of the photon to 'D'. This error cannot be identified during 'Key Extraction' Stage as bases of both A and B are same. But, it can be detected and rectified during 'Error Correction' Stage.

**Table 1:** Formal description of BB84 protocol in both absence and presence of the eavesdropper

| **S. No.** | **A** | | **E present?** | **E** | | **B** | | **Flag$_{AB}$** | **$K_S$** |
|---|---|---|---|---|---|---|---|---|---|
| | $B_A$ | $P_A$ | | $B_E$ | $O_E$ | $B_B$ | $O_B$ | | |
| 1 | R | 1 | N | - | - | D | 0 | N | - |
| 2 | D | 0 | N | - | - | R | 0 | N | - |
| 3 | R | 1 | N | - | - | R | 1 | Y | 1 |
| 4 | D | 1 | N | - | - | D | 1 | Y | 1 |
| 5 | R | 0 | Y | R | 0 | R | 0 | Y | 0 |
| 6 | D | 1 | Y | R | 1 | R | 1 | N | - |
| 7 | R | 1 | Y | R | 1 | R | 1 | N | - |
| 8 | R | 0 | Y | D | 0 | R | 1 | Y | Error |
| 9 | R | 1 | Y | R | 1 | R | 1 | Y | 1 |
| 10 | R | 0 | Y | R | 0 | D | 0 | N | - |

### 6.2 BB92 protocol

It is similar to BB84 but it uses a single non-orthogonal basis rather than using two orthogonal bases. Non-orthogonal basis of Sender (A) consists of two polarization states i.e. |h> and |rcp> whereas non-orthogonal basis of Receiver (B) consists of two polarization states i.e. |v> and |lcp> (as shown in Figure 3).

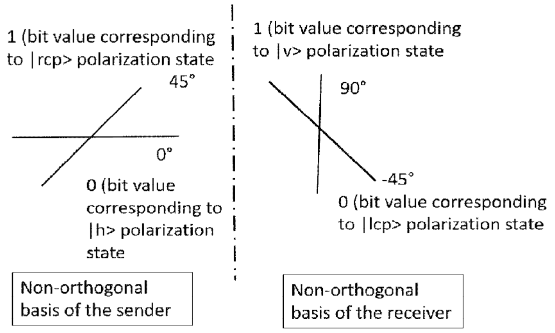
1 (bit value corresponding to |rcp> polarization state
45°
0°
0 (bit value corresponding to |h> polarization state
Non-orthogonal basis of the sender
1 (bit value corresponding to |v> polarization state
90°
-45°
0 (bit value corresponding to |lcp> polarization state
Non-orthogonal basis of the receiver

**Figure 3**: Non-orthogonal basis of Sender and Receiver in BB92 protocol

Following steps are performed for key exchange.

### 6.2.1 Exchange of secret key (Communication over quantum channel)

Sender (A) transmits a photon in one of two polarization states |h> or |rcp>. Receiver (B) receives the photon and measures it using any one of two polarization states |v> or |lcp>. If ‘B’ chooses orthogonal polarization state to polarization state used by ‘A’, it cannot detect the photon. For example: photon polarized using |h> by ‘A’ and measured using orthogonal state |v> by ‘B’ cannot be detected. Another scenario is that ‘B’ chooses other polarization state which is non-orthogonal to the state used by ‘A’, then it can detect the photon with 50% probability. It means that the probability of correctly identifying bit at side of ‘B’ is 25%.

### 6.2.2 Final Key Extraction (Communication over public channel)

‘B’ sends information to ‘A’ about the number of bits it has been able to detect. Both parties then delete all those bits which are not detected by ‘B’.

### 6.2.3 Error Correction stage

This stage is same as for BB84 protocol.

We have explained BB92 protocol using Table 2. Here, $P_A$ represents the polarization state used by ‘A’ for encoding the bit. $V_A$ represents the value of bit sent by ‘A’. $P_{Ed}$ and $P_B$ represent the basis used by ‘E’ and ‘B’ respectively for decoding the received bit. $P_{Ee}$ represents the polarization in which bit is sent by ‘E’ to ‘B’. $Flag_E$ and $Flag_B$ represent whether photons are detected by ‘E’ and ‘B’ respectively. $K_s$ represents the bits of the sifted key. If eavesdropper ‘E’ is present, then it tries to measure photons leading to destruction of some of the photons. It may then send some randomly polarized photons on its own so as to keep the photon number same for ‘A’ and ‘B’. In Table 2, S.No.1-4 shows bit transmissions that take place in absence of ‘E’. S.No.1 shows that ‘B’ is able to detect the correct bit. S.No.5-7 shows the transmissions that take place in presence of ‘E’. ‘. S.No.7 shows that ‘B’ has detected the bit wrongly due to presence of ‘E’ as it has sent randomly polarized photon (|h> in this case) to ‘B’. In absence of ‘E’, ‘B’ would not have detected the photon. ‘N’ corresponds to ‘No’ and ‘Y’ corresponds to ‘Yes’.

**Table 2:** Formal description of BB92 protocol in both the absence and the presence of eavesdropper

| **S. No.** | **A** | | **E present?** | **E** | | | **B** | | **$K_s$** |
|---|---|---|---|---|---|---|---|---|---|
| | **$P_A$** | **$V_A$** | | **$P_{Ed}$** | **$Flag_E$** | **$P_{Ee}$** | **$P_B$** | **$Flag_B$** | |
| 1 | h | 0 | N | - | - | - | lcp | Y | 0 |
| 2 | rcp | 1 | N | - | - | - | v | N | - |
| 3 | h | 0 | N | - | - | - | v | N | - |
| 4 | rcp | 1 | N | - | - | - | lcp | N | - |
| 5 | rcp | 1 | Y | lcp | No | rcp | lcp | N | - |
| 6 | h | 0 | Y | lcp | Yes (0) | lcp | lcp | Y | 0 |
| 7 | rcp | 1 | Y | v | No | h | lcp | Y | 0 (Error) |

### 6.3 SARG04 protocol [16]

This protocol is also similar to BB84 but it is more robust to PNS attack. It differs from BB84 in classical post-processing procedure. In this protocol, Sender ‘A’ does not communicate to Receiver ‘B’ about the basis it has used for measurement. Instead, ‘A’ sends to ‘B’ a pair of non-orthogonal states out of which one state has been used for polarization/encoding of the photon/bit. Eavesdropper ‘E’ also have to select randomly from one of these two non-orthogonal states for measuring the copy of photons which means that ‘E’ does not know the bit value with certainty.

Suppose that Sender ‘A’ has sent a photon polarized in state ‘|h>’ and it sends (|h>,|lcp>) pair to ‘B’. If ‘B’ has measured the polarization of photon as |rcp>, then it comes to know that ‘A’ has polarized the photon using |h>. This is because, ‘B’ cannot get the measured polarized state as |rcp> if |lcp> is used by ‘A’ as both are orthogonal to each other. But, if it has measured the polarization as |h> or |lcp>, then it discards the bit as it cannot distinguish between the two possibilities. This reduces the probability of identifying the polarization correctly to 25% on sender’s side as compared to 50% in case of BB84 protocol. As ‘E’ also does not have polarization information of bits with certainty, it will only be able to guess the partial key which makes it robust to PNS attack.

### 6.4 Decoy-State protocol [12]

This protocol is an extension of BB84 protocol. But, it is again robust to PNS attacks (refer Section 5.2) whereas BB84 protocol is more vulnerable. It uses decoy states to detect PNS attacks. This is cost effective as it extends BB84 protocol with little addition of hardware. The key idea is that Sender ‘A’ prepares a set of additional signal states called decoy states in addition to standard BB84 signal states. Those decoy states are used only for the purpose of detecting eavesdropping attacks, whereas standard BB84 states are used for only key generation. Decoy states are used to estimate error-rate using a set of mathematical equations. If calculated value of error rate is above the upper bound, it confirms the presence of an eavesdropper.

Table 3 provides the comparison of the above discussed protocols

**Table 3:** Comparison of above discussed protocols

| **Parameter** | **BB84** | **BB92** | **SARG04** | **BB84 with Decoy States** |
|---|---|---|---|---|
| **No. of states** | 4 | 2 | 4 | 4+ |

| | | | | |
|---|---|---|---|---|
| **Polarization** | Orthogonal | Non-Orthogonal | Orthogonal | Orthogonal |
| **PNS attack** | Vulnerable | Vulnerable | Less Vulnerable due to sharing 2 states between 'A' and 'B' | Least vulnerable due to use of decoy states |
| **Setup Complexity** | Low | Lowest | Low | Average |
| **Secure Key Generation Rate** | Average | Small | Small | High as detection of 'E' is done using decoy states |

SARG04 and BB92 have low key generation rate among the four discussed protocols as they have 25% probability of detecting the bit correctly at the sender's side. But, SARG04 is better than BB84 and BB92 as it provides protection against PNS attack. In terms of setup complexity, BB92 is the simplest as it does not require the alignment of the polarizations. Decoy State Protocol seems the best among the discussed protocols as it provides high key generation rate and protection from PNS attacks with little enhancement in Hardware.

## 7 CONCLUSION

In this study paper, we have introduced modern cryptography and showed that quantum-safe encryptions schemes can overcome the challenges of modern cryptographic techniques. Quantum Cryptography, which is one of the quantum-safe encryption schemes has been elaborated and its various aspects have been covered. Various Quantum Key Distribution (QKD) experiments performed using fibre links and space-based links along with the challenges associated with their practical implementations have been discussed in detail. It has been concluded that it is important to make the satellite-ground links secure using quantum cryptography in order to secure the global network and prevent compromising the satellite command and control data. Quantum satellites can be used as trusted relay nodes for exchanging the secret keys between two ground stations or between two satellites. We have also discussed the orbit types of quantum satellites along with their shortcomings. Day-time, night-time, uplink and downlink operations of space-based QKD have also been discussed. This paper has also attempted to explain some of the famous quantum cryptographic protocols. BB84 protocol is the first ever and widely implemented quantum cryptography protocol and is the base protocol for many new protocols. BB84 and BB92 are vulnerable to PNS attacks whereas SARG04 and Decoy State Protocols are more robust to PNS attacks and are capable of detecting eavesdropper in case of multi-photon sources. A lot of work is being done to develop the protocols, which are cost effective, have high secure key generation rate over long distances and are robust to attacks against QKD systems.

## 8 ACKNOWLEDGMENTS

The authors express their sincere gratitude to Sh. D. K. Das, Director SAC, Sh. N. M. Desai, Associate Director SAC, Dr. Khagindra Kumar Sood, Deputy Director SSAA/SAC and Sh. S. N. Satashia, ex-Group Director CTAG/SSAA/SAC for their support and encouragement.

### References

[1] V. Mavroeidis, K. Vishi, M. D. Zych, and A. Jøsang, "The impact of quantum computing on present cryptography", Int. J. Adv. Comput. Sci. Appl. 9, 405 (2018).

[2] Nielsen, M. and Chuang, I., "Quantum computation and Quantum information. Cambridge", Cambridge Univ. Press, 2000.

[3] Scarani, Valerio, et al., "The security of practical quantum key distribution", Reviews of modern physics 81.3 (2009): 1301.

[4] Gisin, Nicolas, et al., "Quantum cryptography", Reviews of modern physics 74.1 (2002): 145.

[5] Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W, "Quantum cryptography with realistic devices", arXiv:1903.09051 (2019).

[6] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing pp. 175-179 (1984).

[7] Charles H Bennett and Gilles Brassard, "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working", ACM Sigact News, 20(4): 78–80, (1989).

[8] A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. 67, 661 (1991).

[9] J. F. Clauser, A. Shimony, "Bell's theorem: experimental tests and implications", Reports on Progress in Physics 41, 1881 (1978).

[10] Bennett, C. H., "Quantum cryptography using any two non-orthogonal states", Physical Review Letters 68, 3121–3124 (1992).

[11] G. Brassard, N. Lutkenhaus, T. Mor, and B. Sanders, "Limitations on Practical Quantum Cryptography", Phys. Rev. Lett. 85, 1330 (2000).

[12] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett. 91, 057901 (2003).

[13] H.-K. Lo, X. Ma and K. Chen, "Decoy State Quantum Key Distribution", Proceedings of IEEE ISIT 2004, Page 137, IEEE Press (July 2004).

[14] Xiang-Bin Wang, "Beating the PNS attack in practical quantum cryptography", http://arXiv:quant-ph/0410075, v5 24 (Jan 2005) [Accessed: September 24, 2019].

[15] Ma, X., Qi, B., Zhao, Y. & Lo, H.-K, "Practical Decoy State for Quantum Key Distribution". Phys. Rev. A 72,012326 (2005).

[16] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. 92, 057901 (2004).

[17] Peng C-Z et al., "Experimental free-space distribution of entangled photon pairs over 13 km: towards satellite-based global quantum communication", Phys. Rev. Lett. 94 150501 (2005).

[18] Ursin R et al., "Entanglement based quantum communication over 144 km", Nat. Phys. 3 481–6 (2007).

[19] Schmitt-Manderbach T et al., "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km", Phys. Rev. Lett. 98 010504 (2004).

[20] Liao et al., "Satellite-to-ground quantum key distribution", Nature 549, 43 (2017a).

[21] Liao et al., "Satellite-Relayed Intercontinental Quantum Network", Phys. Rev. Lett. 120, 030501 (2018).

[22] Heasin Ko, Kap-Joong Kim, Joong-Seon Choe, Byung-Seok Choi, Jong-Hoi Kim, Yongsoon Baek, Chun Ju Youn, "Experimental filtering effect on the daylight operation of a free-space quantum key distribution", Scientific Reports (2018).

[23] https://www.sciencedaily.com/releases/2017/07/170710113725.htm [Accessed: August 20, 2019]

[24] Biswasa, Sanat K., Abhijit Mitrab, and Anand Srivastavac, "Challenges in Designing Satellite Constellation for Providing Uninterrupted Network Security through Quantum Key Distribution at a Larger Geographic Region", IAC-18, B2, 1, 10, x44754 (2018).

[25] Bedington, Robert, Juan Miguel Arrazola, and Alexander Ling, "Progress in satellite quantum key distribution", npj Quantum Information 3, no. 1: 1-13 (2017).

[26] C Bonato et al, "Feasibility of satellite quantum key distribution", New J. Phys. 11 045017

[27] Gottesman, D., & Lo, H. K, "Proof of security of quantum key distribution with two-way classical communications", IEEE Transactions on Information Theory 49.2 (2003): 457-475.

[28] Hwang, W. Y., "Quantum Key Distribution with High Loss: Toward Global Secure Communication", Phys. Rev. Lett. 91, 057901 (2003).

## AUTHORS

Amod Aggarwal received M.tech degree in Computer Science & Engineering from IIT Roorkee and B.Tech degree in Computer Science & Engineering From NIT Jalandhar. She worked as Software Engineer in Samsung Research Institute, Noida for a year. She is currently working as Scientist/Engineer in Space Applications Centre, ISRO. Her interests include Quantum Cryptography, Data Mining, Big Data Technologies and Software Development.

Shahana K is Division Head of Delhi Earth Stati, Space Applications Centre, ISRO. She has an experience of 25 years in the organization. She has completed her post-graduation from IETE, New Delhi. She has worked in various SATCOM projects during her tenure.