*Journal of Quantum Computing*
DOI:10.32604/jqc.2021.019864
***Article***

Tech Science Press

# Quantum Cryptography–A Theoretical Overview

**Pratik Roy*, Saptarshi Sahoo, Amit Kumar Mandal and Indranil Basu**

Institute of Engineering and Management, Salt Lake Electronic Complex, West Bengal, Kolkata, 700091, India
*Corresponding Author: Pratik Roy. Email: ipratikroy582@gmail.com
Received: 15 June 2021; Accepted: 07 September 2021

**Abstract:** Quantum Key Distribution seems very promising as it offers unconditional security, that's why it is being implemented by the tech giants of the networking industry and government. Having quantum phenomenon as a backbone, QKD protocols become indecipherable. Here we have focused on the complexities of quantum key distribution and how this technology has contributed to secure key communication. This article gives an updated overview of this technology and can serve as a guide to get familiar with the current trends of quantum cryptography.

**Keywords:** Quantum information; quantum cryptography; quantum entanglement

## 1 Introduction

Quantum Cryptography was first proposed and theoretically shown by Stephen Wiesner in the early 1970s. He introduced the concept of quantum conjugate coding [1]. In this theory he has shown how to store or transmit two messages by encoding them in two conjugate observables such as linear and circular polarization of light so that either but not both of the messages may be received and decoded. Later, Bennett and Brassard developed the first key distribution protocol based on this theory [2]. In 1994, Peter Shor has developed the famous factoring algorithm that has increased the vulnerability of the widely used RSA scheme [3]. Cryptography is a method used to make the communication more secure between two parties those are sender and receiver in present of a third party, i.e., an adversary. Basically in cryptography we scramble sender's message into some cipher text via some encryption algorithm so that recovering the message without its key becomes difficult and only the authenticated receiver can decipher or decrypt the message via some decryption procedure. Cryptography is broadly classified into three sections. i) Symmetric key cryptography; ii) Asymmetric key cryptography; iii) Hash functions. Quantum key distribution protocols generate identical keys for the two parties. It uses quantum mechanical phenomenon to secure communication between the two parties. Quantum cryptographic algorithm (BB84 QKD PROTOCOL) [3] was first introduced by Charles H. Bennett and Gilles Brassard in 1984. Although it has not been yet completely commercialized, QKD protocols have been proven to be the most secure technique for communication [4–6].

## 2 Quantum States and Density Matrix Formulation

Quantum states can be of two types:

- **Pure state:** Here only one wave function is present in the statistical mixture with hundred percent probability.
- **Mixed state:** Here more than one wave functions present with different probability within the statistical mixture, i.e., it is a probabilistic mixture of pure states. We generally formulate these mixed states using "Density Matrix" ρ.

$$\rho = \sum_x p_x |\psi_x\rangle\langle\psi_x| \quad (1)$$

Here, Eq. (1) represents a mixed state that has the pure state $|\psi_x\rangle$ with probability $p_x$.

If, $\rho = \rho^2$, i.e., ρ is an idempotent matrix then it is a pure state and else a mixed state. Tr(ρ) = 1 holds true for all density matrices.

Basically, we use density matrix to characterize a mixed state. Following is the example of pure state and mixed state. $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ - these are examples of pure state. Now if we make statistical mixture of any pure states then it will be a mixed state like

$$|\rho_x\rangle = \frac{1}{2}(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) + \frac{1}{2}(\gamma|0\rangle + \delta|1\rangle)(\gamma^*\langle 0| + \delta^*\langle 1|)$$

$$= \frac{1}{2}(|\alpha|^2 + |\gamma|^2)|0\rangle\langle 0| + \frac{1}{2}(\alpha\beta^* + \gamma\delta^*)|0\rangle\langle 1| + \frac{1}{2}(\beta\alpha^* + \delta\gamma^*)|1\rangle\langle 0| + \frac{1}{2}(|\beta|^2 + |\delta|^2)|1\rangle\langle 1| \quad (2)$$

So, here by density matrix $\rho_x$ we generally represent a mixed state [7].

## 3 Properties of Quantum State

### *3.1 Superposition*

According, to the law of superposition a quantum particle can be at its all possible state before being measured. On measuring its wave function collapses to any one of the possible states and gives us the result. Here we can show an example of superposed state$|\phi\rangle$,

$$|\phi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle \quad (3)$$

Generally, a single qubit quantum state $|\psi\rangle$ is represented in the two dimensional hilbert space as $\alpha|0\rangle + \beta|1\rangle$ where $\alpha$ and $\beta$ are the complex terms and $|\alpha|^2 + |\beta|^2 = 1$. After measuring the state the probability of finding state $|0\rangle$ is $|\alpha|^2$ and probability of finding the state $|1\rangle$ is $|\beta|^2$ [8]. "$\langle x|\ and\ |x\rangle$"– these two notations are known as Dirac's Bra-Ket notation. Ket is a vector in the d dimensional Hilbert space and Bra is the called the equivalent complex conjugate vector in the dual space of that Hilbert space.

### *3.2 Entanglement Theory in Brief*

Entanglement arises when a group of particle generates or interact in a way such that we cannot describe each of their quantum state independently. Although, Einstein has called it as 'spooky action at a distance' as it seems to violate the concept of locality. But later this conflict has been ended by John Bell through his inequality. Moreover, we can say that entanglement is a non-local correlation.

There are some mathematical intuition to show whether a state is entangled or not. Pure state $|\psi_{AB}\rangle$ is said to be separable if we can represent it as a tensor product state like

$$|\psi_{AB}\rangle = |\psi_A\rangle \otimes |\psi_B\rangle \quad (4)$$

Or else, it will be an entangled state. Similarly, in case of mixed states, mixed state described by a density matrix ρ acting on a composite system $\mathcal{H}_1 \otimes \mathcal{H}_2$ is said to be separable iff it can be represented as the following:

$$\rho = \sum_k p_k \rho_k^1 \otimes \rho_k^2 \quad (5)$$

$p_k$ is the weight factor and $\{\rho_k^1\}$ and $\{\rho_k^2\}$ are the density states for the respective subsystems [9–13].

## 4 Some Facts Related to Quantum Cryptography

### *4.1 Monogamy of Entanglement*

Let us have our three friends Alice, Bob and Charlie. Now according to monogamy of entanglement if Alice and Bob are entangled to each other, and then that entanglement cannot be shared with a third party, i.e., Charlie. For an example let's make a statement that Alice and Bob are entangled to a bipartite state

$|\psi_{AB}\rangle$ and let's make a statement that Alice, Bob and Charlie are entangled into a tripartite state $|\psi_{ABC}\rangle$. Now, if we find the reduced density state from the state $|\psi_{ABC}\rangle$ then the reduced density state $\rho_{AB}$ that we achieve is a separable state not an entangled state. So, here a contradiction occurs. From this example we can draw a conclusion, i.e., monogamy of entanglement exists. Let's do the following analysis:

$$|\psi_{AB}\rangle = \lambda_0|00\rangle + \lambda_1|11\rangle \quad (6)$$

Now copying Bob's bit to Charlie we have

$$|\psi_{ABC}\rangle = \lambda_0|000\rangle + \lambda_1|111\rangle \quad (7)$$

$$\rho_{ABC} = |\psi_{ABC}\rangle\langle\psi_{ABC}| \quad (8)$$

We can observe that Bob's bit has been copied to Charlie's bit.

$$\rho_{AB} = Tr_C[\rho_{ABC}] = |\lambda_0|^2|0\rangle\langle 0| \otimes |0\rangle\langle 0| + |\lambda_1|^2|1\rangle\langle 1| \otimes |1\rangle\langle 1| \quad (9)$$

According to Eq. (9) we can observe that $\rho_{AB}$ is a separable state whereas according to Eq. (6) it is an entangled state. Here a contradiction arises giving rise to the Monogamy [14–16].

### *4.2 Ignorance*

We say sometime that the Eve is ignorant about the key or Alice is ignorant about Bob's input or vice versa. Let's assume that we have a 'n' bit key K that can be either 0 or 1. Whereas E is the information that Eve contains about the key. Every position in the key is equiprobable. So, probability of each position is $\frac{1}{2}$ and probability of getting a particular string is $\frac{1}{2^n}$ or in terms of density state it is $\rho_k = \frac{\mathbb{I}}{|K|}$, where, K = $2^n$.

Now, E may be quantum or classical anything. So, we can think of a classical-quantum state (cq state) $\rho_{KE}$. So, we call Eve as an ignorant if we can represent $\rho_{KE}$ as following:

$$\rho_{KE} = \frac{\mathbb{I}}{|K|} \otimes \rho_E \quad (10)$$

### *4.3 Trace Distance*

In real world we do not get everything ideal, so we have to think of the almost ideal. Now, let's do an experiment that is–let's say we have two systems System A and System B. System A is ideal and System B is real. Alice and Eve does some operations on system A and B and produces two cq(classical-quantum) states $\rho_{KE}^{ideal}$ and $\rho_{KE}^{real}$. Now, we always want Eve to be ignorant because then only we can achieve maximum amount of information from Eve about the key. If, Eve is ignorant about the key then (10) gives the status of $\rho_{KE}^{ideal}$. Now, for $\rho_{KE}^{real}$ to be almost equals to $\rho_{KE}^{ideal}$ we must have the distance between them lesser than or equals to $\epsilon$ or the two states must be $\epsilon$ close. The last paragraph says about Distance between two states. This distance is known as Trace Distance. It is given as

$$D(\rho_1, \rho_2) = \max_M Tr[M(\rho_1 - \rho_2)] \quad (11)$$

M is the POVM matrix. POVM means positive operator valued measurement. These are set of $(d \times d)$ positive semidefinite matrices $\{M_1, M_2, \cdots, M_K\}$. We have k matrices means that we must have k outcomes. So, probability of coming any i[th] outcome is given by [17]

$$\Pr(i) = \mathrm{Tr}[\rho M_i] \quad (12)$$

If $\rho_1$ *and* $\rho_2$ commute with each other such that

$$\rho_1 = \sum_x p_x |x\rangle\langle x| \quad (13)$$

$$\rho_2 = \sum_x q_x |x\rangle\langle x| \quad (14)$$

Then Trace distance is given by

$$D(\rho_1, \rho_2) = \frac{1}{2}Tr|\rho_1 - \rho_2|$$
$$= \frac{1}{2}Tr|\sum_x p_x |x\rangle\langle x| - \sum_x q_x |x\rangle\langle x||$$

$$= \frac{1}{2}\sum_x |(p_x - q_x) Tr(|x\rangle\langle x|)|$$

$$\therefore D(\rho_1, \rho_2) = \frac{1}{2}\sum_x |p_x - q_x| \quad (15)$$

$D(\rho_1, \rho_2)$ has to > 0 in order to be distinguishable [18].

### *4.4 Randomness*

Let's assume that we have a randomness generator that generates a string X of n bit randomly such that X = $\{X_1, X_2, \cdots, X_n\}$. P(X = x) = $\frac{1}{2^n}$. The density state of the above string X is $\rho_x = \frac{\mathbb{I}}{2}^{\otimes n}$ and now, if we write the state $\rho_x$ $as$ $\rho'_x = \frac{\mathbb{I}}{2}^{\otimes n-1} \otimes |0\rangle\langle 0|$, i.e., the last bit is always zero, then if we find the trace distance between $\rho_x$ $and$ $\rho'_x$, i.e., D($\rho_x, \rho'_x$ ), it comes to be large enough such that we can distinguish between the states. So, the eavesdropper can easily detect the string X that is being sent. So, trace distance is not a fruitful measure to quantify randomness. If we define our probability distribution like the following:

$$P(X = x) = \begin{cases} \frac{1}{2}, & X = 111\cdots 1 \\ \frac{1}{2(2^n - 1)}, & Otherwise \end{cases} \quad (16)$$

In that case, if we find out the Shannon's entropy [19] then it becomes $\frac{n}{2}$. So, the problem with Shanon's entropy is the eavesdropper can always guess the string correctly with probability $\frac{1}{2}$ and otherwise it is always dependent of the string's length. So, Shannon's entropy cannot give us the maximum information. So, it becomes very necessary for us to define an entropic relation that can retrieve the maximum information. So, in case of Quantum cryptography we use "Min Entropy". The min entropic relation is given by

$$H_{min}(X) = -\max_x [\log_2 P(X = x)] \quad (17)$$

For the above given probability distribution if we find $H_{min}(X)$ it comes as 1, i.e., hundred percent information we can retrieve [20].

## 5 Classical One Time Pad

Here, we will recall our two protagonists Alice and Bob. The idea we use here is the concept of symmetric Key cryptography, i.e., the key used in encryption is same as the key used in decryption. The key length must be same as the message length. So, initially we will encrypt our message $|m\rangle$ using the Pauli's X matrix, i.e.,

$$|e\rangle = X^k|m\rangle \text{ [Encryption]} \quad (18)$$

where, $|e\rangle$ is the encrypted message or the cipher text that is being sent by Alice to Bob. Whereas, Bob decrypt the cipher text into plain text by applying one more Pauli's X matrix, i.e.,

$$|m\rangle = X^k X^k|e\rangle \text{ [Decryption]} \quad (19)$$

K is the key here.

### *5.1 Mathematical Analysis*

Density matrix of $|e\rangle$ is $\rho_e$. The key k will be 0 or 1 with probability $\frac{1}{2}$ each.

$$\rho_e = |e\rangle\langle e| = X^k|m\rangle\langle m|X^k$$

$$= \frac{1}{2}|m\rangle\langle m| + \frac{1}{2}X|m\rangle\langle m|X$$

$$= \frac{1}{2}[|0\rangle\langle 0| + |1\rangle\langle 1|]$$

$$= \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\therefore \rho_e = \frac{\mathbb{I}}{2} \tag{20}$$

We get $\rho_e$ as the maximally mixed state that is independent of the message m. So, the eavesdropper cannot be able to detect what is the main encrypted text and each time as the message reaches to Bob the key 'k' will be discarded and 'k' is random every time depending on the message 'm'.

But, classical one time pad has a disadvantage, i.e., if the message $|m\rangle = |+\rangle$ state or $|m\rangle = |-\rangle$ state in that case X $|+\rangle$ = $|+\rangle$ and X $|-\rangle$ = -$|-\rangle$, i.e., no inversion of state has happened. So, if this occurs, in that case the eavesdropper will be able to detect the message very easily. So, here comes the idea of Quantum one time pad to draw over this disadvantage, shown as Fig. 1.

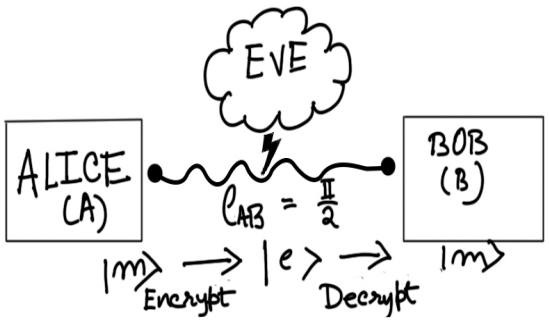


**Figure 1:** One time pad

## 6 Quantum One Time Pad

Quantum one time pad is also a symmetric key cryptography but here in this case the number of keys are increased. We will use here two keys $k_1$ and $k_2$ and to veil over the previous disadvantage. Here Pauli's Z matrix is used along with the X matrix because Z $|+\rangle = |-\rangle$ and Z $|-\rangle = |+\rangle$. So the problem disappears. Now the algorithm for this one is like the following:

$$|e\rangle = X^{k_1} Z^{k_2} |m\rangle \text{ [Encryption]} \tag{21}$$

$$|m\rangle = Z^{k_2} X^{k_1} |e\rangle \text{ [Decryption]} \tag{22}$$

### *6.1 Mathematical Analysis*

Density matrix of cipher text $|e\rangle$ *is* $\rho_e$. Table 1 shows the key combinations and respective probabilities.

**Table 1:** Probability distribution

| $k_1$ | $k_2$ | Probability of getting this combination |
|---|---|---|
| 0 | 0 | $\frac{1}{4}$ |
| 0 | 1 | $\frac{1}{4}$ |
| 1 | 0 | $\frac{1}{4}$ |
| 1 | 1 | $\frac{1}{4}$ |

$$\begin{aligned}\rho_e &= |e\rangle\langle e| \\ &= X^{k_1} Z^{k_2} |m\rangle\langle m| Z^{k_2} X^{k_1} \\ &= \frac{1}{4}[\, |m\rangle\langle m| + Z|m\rangle\langle m|Z + X|m\rangle\langle m|X + XZ|m\rangle\langle m|ZX\,] \\ &= \frac{\mathbb{I}}{2}\end{aligned} \tag{23}$$

It is a maximally mixed state. So, the eavesdropper will see a state that is completely independent of the message $|m\rangle$. In this case we are using qubits and it is a glimpse of Quantum Cryptography [21,22].

## 7 Quantum Key Distribution

### *7.1 Introduction*

In this section, we will briefly introduce to the quantum key distribution. The first quantum key distribution protocol is BB84 protocol which was developed by Charles H. Bennett and Gilles Brassard in the year of 1984. Some famous QKD protocols are BB84 protocol, B92 protocol, E91 protocol, etc.

### *7.2 Theory*

As shown in Fig. 2, QKD protocols are used to generate identical keys for Alice and Bob without transferring any information to the adversary. The two basic building blocks of a quantum cryptographic protocol are:

- Heisenberg's uncertainty principle
- Photon polarization

According to uncertainty principle it is not possible to measure a quantum state without disturbing its state which makes the quantum cryptographic protocols almost unbreakable because if the eavesdropper try to measure the quantum state coming from Alice it will change the state of the message and Bob will receive wrong information which clearly shows that someone has tried to eavesdrop the channel. Secondly, to encode the message bits practically Alice uses rectilinear and diagonal polarizer to restrict the orientation of the unpolarized light in a particular direction, i.e., to encode them in vertical ($90^o$ or ↑) or horizontal ($0^o$ or →) or diagonal ($\pm 45^o$ or ↗ or ↖ ) basis. After the encoding process is done Alice sent those via the quantum communication channel and at the receiving end Bob measures those in random basis and get respective results. Now, Bob and Alice discuss the basis they have used via classical public channel and accordingly discard the unused one and get a key. After that in almost all quantum cryptographic protocols there is a function called extractor function which is used to extract randomness. This function takes one 'n' bit input string X and one d bit seed Y which is uncorrelated from X and eavesdropper information E as inputs and generate a 'm' bit string Z that is totally uncorrelated from the eavesdropper. This step is known as privacy amplification which is used in all quantum cryptographic protocol as a final step to generate the final key. In order to be a quantum key distribution protocol it has to be $\epsilon$ correct and $\epsilon$ secure [23–25].

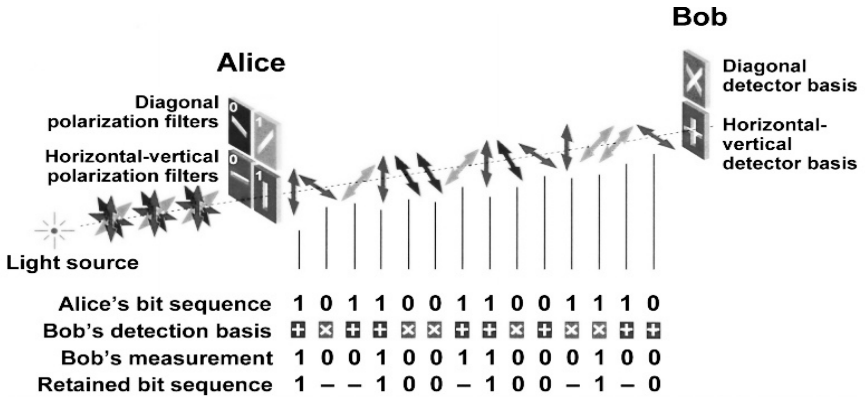


**Figure 2:** QKD scheme

### *7.3 Extractor*

Extractor is a function that is used to extract randomness. Extractors can be of three kinds:

- Deterministic extractors
- Seeded extractors
- Multiple source extractors

In this context we will only talk about the strong seeded extractors. Extractors are defined as Ext: $\{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$, where X is the n bit weak secret that is to be amplified. Y is called the seed of the extractor which is d bit long and it is uncorrelated from X and eavesdropper side information E. The output of the extractor function is a 'm' bit string Z which is completely random from the eavesdropper side and also uncorrelated from the input string X and eavesdropper side information E.

$\therefore$ Z = Ext(X , Y). Z is the amplified secret. It is called a (k, $\epsilon$) strong seeded extractor if the min entropy conditioned on eavesdropper side information E is at least k, i.e., $H_{min}(X|E) \geq k$ and $\left\| \rho_{ZYE} - \frac{\mathbb{I}}{2^m} \otimes \rho_{YE} \right\|_{Tr} \leq \epsilon$ [26].

### *7.4 Key Distribution Scheme*

At the beginning, we have to consider that Alice and Bob both has access over an insecure public classical channel, a secure classical channel and a quantum channel. Eve has also access to the public classical channel and the quantum channel. The scheme is described as below:

1. Let us think that Alice wants to send a message 11001011 to Bob. Now to send it to Bob she chooses random basis like XZZXZZXX and then encode the message string accordingly into $|+\rangle|0\rangle|1\rangle|-\rangle|0\rangle|0\rangle|-\rangle|+\rangle$.
2. Alice sends this encoded message to Bob via quantum communication channel.
3. Now what Bob does is he chooses his random basis like XXZXZXXZ and measure the incoming encoded message in the basis he has chosen and gets the result like 10001111. Now point to be remembered that when measuring $|+\rangle$ in Z basis it will give 0 or 1 with probability $\frac{1}{2}$.
4. Alice and Bob now discuss the basis they have used through the public channel and discard the cases where they do not agree and both of them at last comes up with a string $X_A$ = 100111 and $X_B$ = 100111.
5. After this the final step comes privacy amplification. In this step Alice will generate a random seed 'r' and send to bob via the public channel. Now Alice and Bob generate the keys using the extractor function as $K_A$ = Ext$(X_A, r)$ and $K_B$ = Ext$(X_B, r)$. $K_A$ and $K_B$ are completely uncorrelated from Eve and from $X_A$, $X_B$ and $r$.
6. After generation of the keys, they discuss the keys via the secret channel they have. This whole scenario is implemented using the photon polarization phenomenon.

### *7.5 Challenges in Implementation*

The following factors are playing a major role in order to develop high performance and low cost QKD systems [27].

- **Key rate** is a major factor in implementing QKD. Encryption keys generated using QKD can be used in symmetrical cipher scheme like one time pad to enhance the security. Nowadays there exists strong disparity between classical and QKD key rates. Today, Mbit/sec rate is enough for video transmission using QKD. But in order to encrypt high volumes of classical network traffic using one time pad major developments on key rate of QKD is required. This key rate crucially depends on the detectors used. As shown in Fig. 3, for QKD systems having single photon detectors, high efficiency and short dead time of the detectors are mandatory to reach a higher key rate.

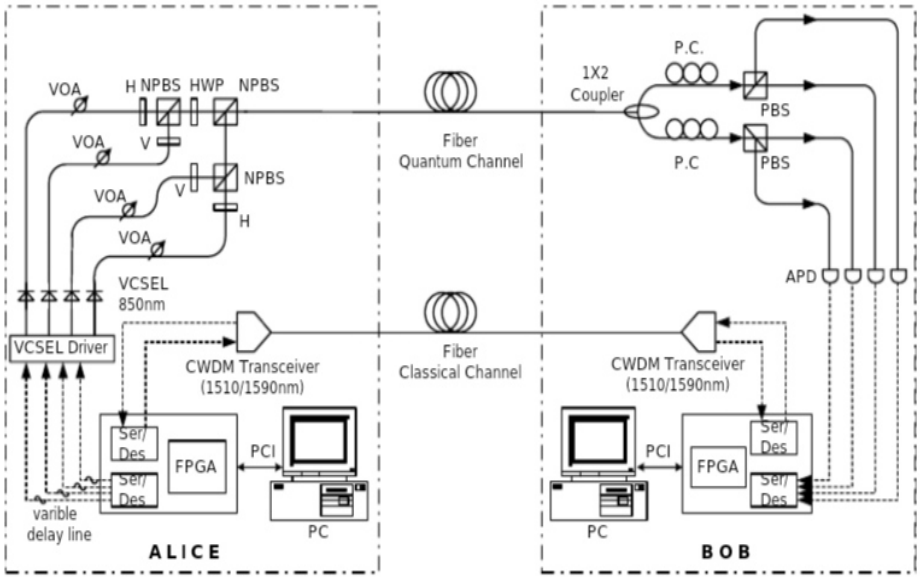


**Figure 3:** Implementation of BB84 QKD Scheme

- **Distance** or technically the communication range is the major factor for future implementations of QKD in different networking applications. Here the low noise single photon detectors are the key enabling factors. The maximum attainable range through QKD depends on the type of operation and temperature of the detectors used. In GaAs avalanche photodiodes can tolerate losses of 30 and 52 dB when cooled to –30º and –120ºC respectively whereas SNSPD's cooled to cryogenic temperature can withstand with a loss of 72 dB. This loss is analogous to 360 km of general single mode fiber or about 450 km of ultra-low loss fiber. Now further increasing the point to point communication range although technologically possible, but the channel noise will reduce the key rate which is unwanted.
- For, QKD systems to be used in real time applications **lower cost & robustness** are the inevitable features. As QKD techniques have been implemented along a single point-to-point link till date, it might happen that the link is being disrupted (maybe through active eavesdropping). Then in that case all the flow of communication will be interrupted and the data will be ceased. So, robustness of a QKD network is indispensable.

## 8 Recent Advancements in Industry

At present the Quantum Cryptography market is dominated by a few globally established organizations such as ID Quantique(Switzerland), ISARA(Canada), Quintessence Labs(Australia), MagiQ Technologies(US), QuantumCTek(China). The global quantum cryptography market size is estimated to be USD 89 million in 2020 and projected to reach USD 214 million by 2025. Recent developments include [28]:

- In March 2021, ISRO has successfully demonstrated free-space Quantum Communication over a distance of 300 m. The demonstration has included live videoconferencing using quantum-key-encrypted signals. This is a major milestone achievement for unconditionally secured satellite data communication using quantum technologies [29].
- In May 2020, Crypta Labs collaborated with Space Research and Innovation Network for Technology (SPRINT) to develop its QRNGs for space applications [30].
- In January 2020, Qubitekk acquired QinetiQ's Quantum Key Distribution (QKD) patent portfolio. The portfolio covers novel technological approaches in quantum science, including 57 patent filings, across 17 patent families [31].

- In December 2019, ID Quantique announced that its product Cerberis3 Quantum Key Distribution (QKD) system could be deployed in any network configurations, including point-to-point communication [32].

## 9 Conclusion

At last we can conclude that quantum computing has changed the way of working of classical systems those, which use the classical bits. In quantum computing we use the qubits those use quantum parallelism. Due to this all conventional classical cryptographic algorithms turns out to be abortive in terms of speed and accuracy. There have been substantial advancements in the field of quantum computing for last several years. QKD protocols have become the most useful in the field of cryptography in terms of secrecy maintaining and randomness but there are still challenges ahead in this field. In this era of digitalization the increasing number of connected device has given rise in frequent cyber-attacks. Although quantum cryptography is an effective solution which enhances the security, these technologies are highly expensive and time consuming to implement. The cost goes up with increase in distance which includes developing complicated hardware for long range communication. Proper customer awareness is also needed to enhance the market growth. Nevertheless, as a new science this is still under development and researchers around the globe have already made a breakthrough contribution in this field which seems that in near future quantum cryptography will be uncrackable. The laws of quantum mechanics have made this technology as one of the hot research topics of this decade [33].

**Acknowledgement:** We are thankful to the peoples who have always encouraged and supported us.

**Funding Statement:** The authors received no specific funding for this study.

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

[1] S. Wiesner, "Conjugate coding," *ACM Sigact News*, vol. 15, no. 1, pp. 78–88, 1983.

[2] H. K. Lo and Z. Yi, "Quantum cryptography," arXiv:0803.2507, 2008.

[3] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proc. 35th Annual Sym. on Foundations of Computer Science*, pp. 124–134, 1994.

[4] R. P. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, no. 6, pp. 1–15, 1982.

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no. 1, pp. 3–28, 1992.

[6] D. McMahon, *Quantum Computing Explained*. John Wiley & Sons, 2007.

[7] P. Horodecki, "Separability criterion and inseparable mixed states with positive partial transposition," *Physics Letters A*, vol. 232, no. 5, pp. 333–339, 1997.

[8] T. Hey, "Quantum computing: An introduction," *Computing & Control Engineering Journal*, vol. 10, no. 3, pp. 105–112, 1999.

[9] A. Acín, A. Andrianov, L. Costa, E. Jané, J. Latorre *et al.,* "Generalized schmidt decomposition and classification of three-quantum-bit states," *Physical Review Letters*, vol. 85, no. 7, pp. 1560–1569, 2000.

[10] D. J. Saunders, S. J. Jones, H. M. Wiseman and G. J. Pryde, "Experimental EPR-steering using bell-local states," *Nature Physics*, vol. 6, no. 11, pp. 845–849, 2010.

[11] G. Blaylock, "The EPR paradox, bell's inequality, and the question of locality," *American Journal of Physics*, vol. 78, no. 1, pp. 111–120, 2010.

[12] S. J. Jones, H. M. Wiseman and A. C. Doherty, "Entanglement, einstein-podolsky-rosen correlations, bell nonlocality, and steering," *Physical Review A*, vol. 76, no. 5, pp. 052116–052126, 2007

[13] A. Einstein, B. Podolsky and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" *Physical review*, vol. 47, no. 10, pp. 777–787, 1935.

[14] D. Yang, "A simple proof of monogamy of entanglement," *Physics Letters A*, vol. 360, no. 2, pp. 249–250, 2006.

[15] Y. Bai, M. Ye and Z. Wang, "Entanglement monogamy and entanglement evolution in multipartite systems," *Physical Review A*, vol. 80, no. 4, pp. 044301–044311, 2009.

[16] M. P. Seevinck, "Monogamy of correlations versus monogamy of entanglement," *Quantum Information Processing*, vol. 9, no. 2, pp. 273–294, 2010.

[17] J. P. Gazeau and B. Heller, "Positive-operator valued measure (POVM) quantization," *Axioms*, vol. 4, no. 1, pp. 1–29, 2015.

[18] S. Rana, P. Parashar and M. Lewenstein, "Trace-distance measure of coherence," *Physical Review A*, vol. 93, no. 1, pp. 012110–012120, 2016.

[19] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[20] G. Smith, "Quantifying information flow using min-entropy," in *Eighth Int. Conf. on Quantitative Evaluation of Systems*, IEEE, pp. 159–167, 2011.

[21] F. G. Deng and G. L. Long, "Secure direct communication with a quantum one time pad," *Physical Review A*, vol. 69, no. 5, pp. 052319–052329, 2004.

[22] S. Kute and C. Desai, "Quantum cryptography: A review," *Indian Journal of Science and Technology*, vol. 10, no. 3, pp. 1–11, 2017.

[23] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of the Int. Conf. on Computer*s*, Systems and Signal Processing*, 1984.

[24] C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915– 1923, 1995.

[25] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, no. 6, pp. 661, 1991.

[26] R. Shaltiel, "An introduction to randomness extractors," in *Int. Colloquium on Automata, Languages, and Programming*, Springer, pp. 21–41, 2011.

[27] E. Diamanti, H. K. Lo, B. Qi and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Information*, vol. 2, no. 1, pp. 1–12, 2016.

[28] Markets, "Quantum cryptography market by component (solutions and services), services (consulting and advisory, deployment and integration, and support and maintenance), security type (network and application security), vertical region-global forecast to 2025," 2020. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/quantum-cryptography-market-45857130.html.

[29] A. Jain, A. Khanna, J. Bhatt, P. V. Sakhiya and R. Bahl, "Experimental demonstration of free space quantum key distribution system based on the bb84 protocol," in *11th Int. Conf. on Computing*, *Communication and Networking Technologies*, IEEE, pp. 1–5, 2020.

[30] C. Kollmitzer, S. Petscharnig, M. Suda and M. Mehic, "Quantum random number generation," in *Quantum Random Number Generation*, Springer, pp. 11–34, 2020.

[31] C. Elliott, A. Colvin, D. Pearson, O. Pikalo and J. Schlafer, "Current status of the DARPA quantum network," in *Quantum Information and Computation III*, vol. 5815, no. 1, pp. 138–149, 2005.

[32] L. Widmer, "Cerberis: High-speed encryption with quantum cryptography," in *Internet–Technical Development and Applications*, Springer, pp. 217–221, 2009.

[33] C. G. Almudever, L. Lao, X. Fu, N. Khammassi and I. Ashraf *et al.,* "The engineering challenges in quantum computing," in *Design, Automation & Test in Europe Conf. & Exhibition*, IEEE, pp. 836–845, 2017.