Quantum Key Distribution (QKD) Protocols

First A. Author, *Fellow, IEEE*, Second B. Author, and Third C. Author Jr., *Member, IEEE*

[[1]](#footnote-1)

***Abstract*—The term "quantum key distribution" is currently popular among professionals in the field. The situation is serious for all the current network security methods. These are the fundamental characteristics of quantum mechanics that combine with network security. There are several businesses operating now that are advancing in these industries daily. A key technology today that contributes to the security of future network communication is quantum cryptography. Both industry and academics are paying attention to this field. Our primary goal in writing this work is to give a concise assessment and analysis of current developments in the field of quantum key distribution, the most well-known and advanced area of quantum computing. However, we also want to provide a broad overview of several quantum computing domains. This study reviews quantum computing and its various applications, such as quantum public key cryptography, quantum key distribution, and quantum authentication.**

**We first go over the fundamentals of quantum cryptography before moving on to the concept of quantum key distribution and the various protocols used in this area. The opportunities in this field are then discussed.**

***Index Terms*—QKD, Quantum Computing, Neatwork Security, Cryptography, Quantum authentication, Quantum public key cryptography**

# I. INTRODUCTION

A

vast field known as quantum computing really falls under the umbrella of quantum physics, a branch of applied physics. The term "quantum" refers to the utilization of small particles called "quanta" for communication. As we use bits to represent 1 and 0 in conventional communication, quantum signifies the source of energy that may be charged both positively and negatively.

There is a great deal of scientific interest in creating a worldwide quantum internet [1], since this might enable various beneficial uses of quantum technologies, such as, for example, distributed quantum metrology, quantum computing, blind quantum computing, and quantum key distribution (QKD). Among these uses, QKD is unquestionably the most developed technology now. Through satellite to ground connections, long-distance QKD has previously been carried out experimentally across 1000 km of open space and 400 km of telecom fibers [2]. Nevertheless, a fundamental restriction on the range of secure QKD without trusted or quantum repeater nodes is posed by the optical loss in telecom fibers, which is 0.2 dB/km. In fact, it would take 100 years to properly convey a single photon through 1000 km of a telecom fiber, even at a GHz repetition rate. Furthermore, recent research has established basic restrictions for the secure point-to-point QKD's key rate vs. distance. They say that the key rate scales linearly with in the absence of repeater nodes, where is the transmittance of the channel between Alice and Bob.

A novel security solution called quantum key distribution (QKD) uses the principles of quantum mechanics to distribute the secret key and guarantee complete security. By utilizing the laws of quantum physics, QKD has gained a new capability not found in traditional encryption, specifically the capacity to identify eavesdroppers. Every eavesdropper activity can be identified as a mistake. Even with infinite processing power, the security offered by the QKD system has been demonstrated to be resistant to adversary assault. Bennett and Brassard presented the initial QKD protocol in 1984, and the first QKD deployment that was successful took place in 1989. In addition, there are a number of outstanding initiatives that have implemented QKD networks effectively, including the DARPA Quantum Network, the SECOQC QKD Network in Vienna, and the Tokyo QKD Network.

A qubit is a quantum bit, which in quantum computing is the opposite representation of a conventional bit. In quantum computing, we utilize quantum binary 0 and 1, just as in conventional computing, we use binary 0,1 for information. The charged photon produced from some source is truly this quantum binary number 0 and 1, as such. To express a Qubit, we employ a distinct idea notation called Bra-Ket notation.

The benefit of employing quantum bits, also known as qubits, which are vulnerable to classical assaults and employed in classical communication and encryption is that quantum physics gives them unique qualities that make them resistant to those attacks.

The rest of this paper is composed as pursues. In Section II, we characterize basics principles of quantum key distribution. In Section III, we discuss quantum cryptography. In Section IV, we talk about various QKD protocols and some open issues and practical research bearings in section V. At the end, we outline this paper in Section V1.

II. Basics Principle Of Quantum Key Distribution

**Quantum Cryptography.** Due to its advancement over traditional cryptography, quantum cryptography is the most sophisticated type of encryption. It combines the two disciplines of quantum physics and network security. We might put it this way: "Quantum cryptography is a quantum physics application that serves the aim of cryptography." Here, we can benefit from applying quantum physics ideas.

**Quantum Entanglement.** A fundamental characteristic of quantum physics is quantum entanglement. This concept states that two minuscule particles from the same source exhibit a link to one another. This connection allows us to determine the state of one particle by measuring another particle, regardless of how close or how far apart they are. This phenomenon was dubbed "spooky action at a distance" by Albert Einstein.

**Quantum Superposition.** A property of quantum physics called quantum superposition says that a qubit may retain many states concurrently. In layman's terms, we may say that without measuring a qubit's state, we cannot identify what state it is holding since measuring a qubit's state is known as measuring a qubit. As a result, before a measurement is performed on a qubit, its states cannot be known; as a result, it is now in a superposition of all its potential states.

**Quantum principle of uncertainty and non-cloning.** The non-cloning theorem and quantum principle of uncertainty forbid the creation of duplicates of an unknown quantum state. This theorem states that it is simple to identify any undesirable individuals inside a network. This guarantees the confidentiality of the key, or any data transmitted to it.

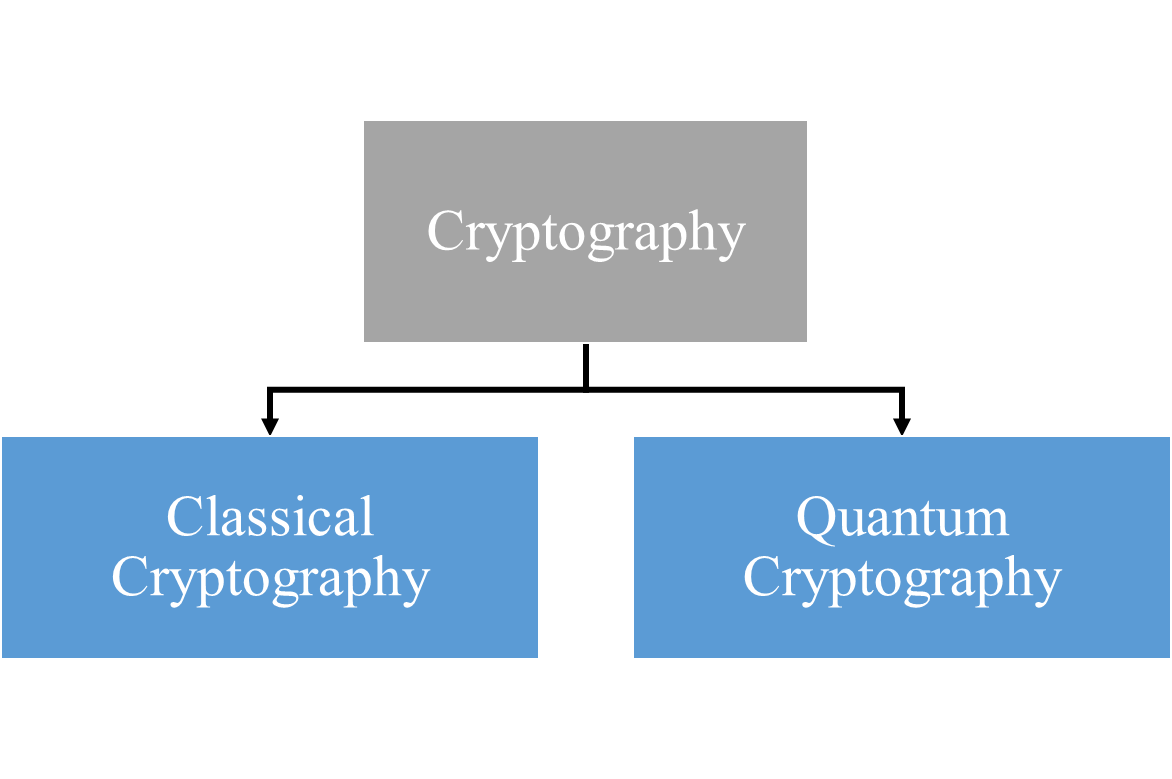
**Quantum-measurement.** The technique of encoding and decoding information using qubits is known as quantum measurement. It is a crucial and extremely significant step in the quantum communication process since it affects the information's integrity. Quantum measurement includes the subprocesses of modification and evolution.

# III. Quantum Cryptography

In the world of information security, the term "cryptography" is not new. A very traditional concept in cryptography is the conversion of information using the assistance of another piece of information known as a "Key."

The present cryptography methods may be divided into two groups according to the Fig 1.

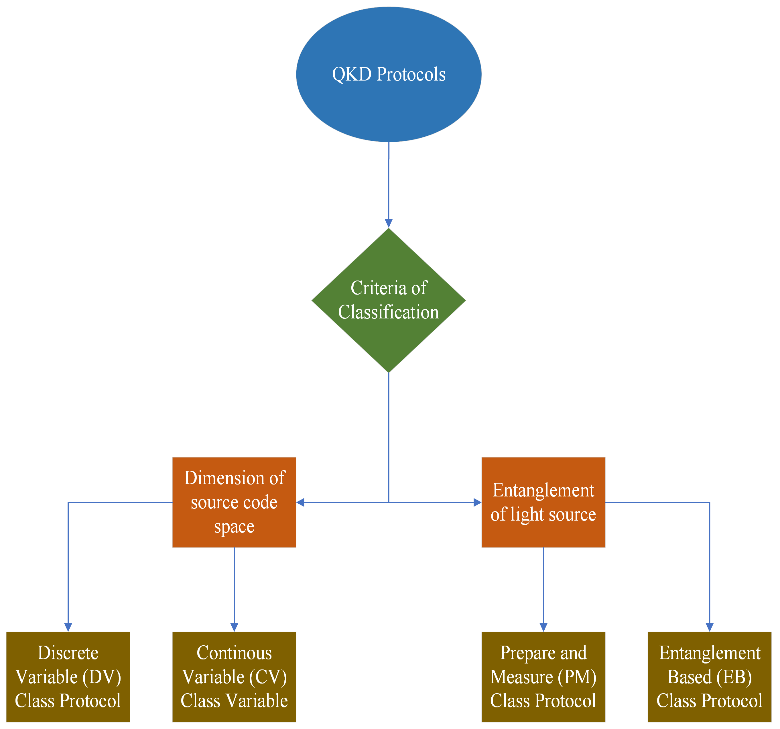
**Fig 1:** Categorization of Cryptographic Techniques



Due to the difference in symmetry and asymmetry in the number of keys needed for encryption, we can further subdivide classical approaches. However, at their heart, they both rely on difficult mathematical factorization issues. However, with today's advanced computing technologies, particularly quantum computers, solving these kinds of complicated issues that often take years to complete takes only a few minutes.

Thus, a novel method known as quantum cryptography—a branch of quantum physics—entered the scene. We can utilize it for cryptographic functions and maintain data security because of its physical characteristics.

The many types of quantum computing include quantum dense coding, quantum teleportation, and quantum key distribution.



**Fig 2:** Classification of QKD Protocols

Key Distribution is the underlying idea behind quantum key distribution. A common key is shared between sender and receiver through a procedure known as key distribution, with the assurance that the key will not be compromised in any manner. In other words, the key distribution is the most crucial and initial step in the encryption process.

1. *Quantum key distribution*

Utilizing a non-cloning, non-orthogonal single quantum state to complete the key distribution is the foundation of quantum key distribution.

Based on its physical characteristics, the QKD procedure may be divided into a few different groups. They may be divided into two categories, Discrete variable (DV) class protocol and Continuous variable (CV) class protocol, based on the size of the source code area. Prepare-and-measure (PM) and Entanglement-based (EB) protocols can be further separated based on whether we believe an entanglement light source to exist.

1. *Other fields of Quantum cryptography*

Other than quantum key distribution, there aren't many other areas where information security is used.

**Quantum Authentication.** The process of authentication involves confirming the sender's identity and the message's integrity. and further assure the communication's security.

* **Quantum Authentication.** Authentication using quantum technology must accomplish the following goals.
  + First, the user must successfully establish her own identity; for example, Alice must convince Bob that "she" is Alice.
  + Second, the user cannot be mimicked; that is, Bob cannot pretend to be Alice to others by utilizing Alice's information once she has finished the verification.
* **Quantum signature.** Digital signatures are primarily used to validate the sender and assure the accuracy of the material in communications. This is the fusion of digital abstract technology with asymmetric key encryption technology. Representative quantum signature techniques come in three varieties:
  + Arbitrated quantum signature
  + Quantum blind signature
  + Quantum group signature.

**Quantum Public Key Cryptography.** The traditional cryptographic approaches based on challenging mathematical problems, such as determining the factors of a number, are no longer safe due to recent advancements in a variety of computer domains, thus a new cryptography system is urgently needed to fill the void. Quantum public key cryptography (QPKC) is a method that may be applied to close this gap. The security of this cryptographic method is guaranteed by using the physical characteristics of photons.

**Post Quantum Cryptography.** The present encryption system is now under scrutiny because to developments in quantum computing. So, a novel strategy called as post quantum cryptography is being developed to address this problem. Theoretically, it guarantees information security from Quantum assaults.

**Quantum A.I.** The use of quantum computing to artificial intelligence is known as quantum AI. It is a Google Corporation research project. The goal of Google's Quantum AI project is to advance quantum computing by creating new quantum algorithms and quantum processors. It will assist academics and developers in finding quick solutions to issues.

# IV. QKD Protocols

In the field of quantum cryptography, QKD is a new technology. Theoretically, it has been demonstrated that the QKD can provide unconditional security by combining three factors, namely exploit the law of quantum mechanics, implemented by using one-time-pad, and hashing scheme. In contrast to conventional cryptography algorithms, which depend on mathematical complexity as their security strength basis, the QKD uses quantum mechanics laws as its security strength basis.

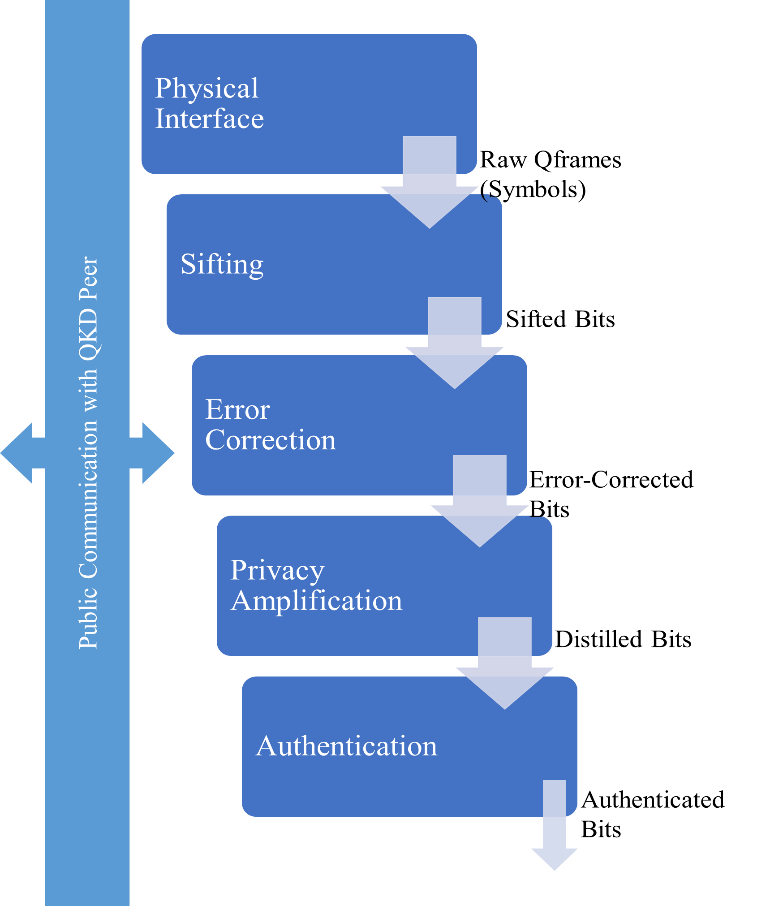
The quantum channel and the public channel are the two channels in the QKD system. The secret key's information is shared and sent through a quantum channel using polarized photons, or quantum bits (qubit). In the meanwhile, agreements on the shared secret key are made while discussing the qubit transfer procedure on the public channel. In general, optical fiber and free space are the two medium kinds of quantum channels that are employed on QKD systems. In the QKD system, some common identification words are Alice as the sender, Bob as the recipient, and Eve as the eavesdropper.

Additionally, the four basic steps in the execution of QKD are raw key exchange, key sifting, key distillation, and usable key size.

There are two different types of QKD protocol schemes: prepare-and-measure-based QKD protocol and entanglement-based QKD protocol. In this sort of protocol, the sender (Alice) must "prepare" the information in the form of polarized photons, and the receiver (Bob) must then "measure" those photons transmitted. Therefore, the protocol is known as prepare-and-measure.

Heisenberg's uncertainty principle is used in the prepare-and-measure-based QKD technique since it states that it is impossible to measure a system's quantum state without changing its initial quantum state. The quantum bit (qubit) cannot be duplicated or amplified without damaging it, as stated in the no-cloning theorem [3]. By exploiting the error parameter measurements that emerge during the photon transmission process from Alice to Bob, this approach allows the QKD system to detect the existence of an eavesdropper. The secret key is distributed by Alice, Bob, and the entanglement photons principle in the entanglement based QKD algorithm.

**Fig 3:** Full Stack of QKD Protocol



Five methods, including the raw q-frame, bits sifting, bits error correction, bits distillation, and bits authentication, make up the whole stack diagram of the QKD protocol, which is shown in Fig 3. Nine protocols—five prepare-and-measure-based QKD techniques and four entanglement-based QKD protocols—are covered in this section. By the year of publication, these procedures are discussed in chronological order.

1. *BB84 Protocol*

In 1984 [4], Researchers Bennett and Brassard suggested a mechanism to exchange a secret key between two parties using the Heisenberg uncertainty principle of quantum physics. The method for using photon polarization state to send secret key information across a quantum communication channel was initially described in the first quantum cryptography protocol. This protocol is characterized as a prepare-and-measure-based QKD protocol and is commonly referred to as the BB84 protocol.

The BB84 protocol transmits and disperses random bits of the secret key using a single photon. Fig 4 shows the rectilinear basis for vertical and horizontal polarization and the diagonal basis for diagonal and its anti-diagonal polarization. The single photon is polarized in one of four polarization states and selected using one of two conjugate bases.

The four key phases of the BB84 protocol implementation are Quantum Exchange, Key Sifting, Information Reconciliation, and Privacy Amplification.

The BB84 protocol has theoretically been shown to give complete security by [5], [6], and discussed in detail in some research publications [7], [8], [9].

1. *E91 Protocol*

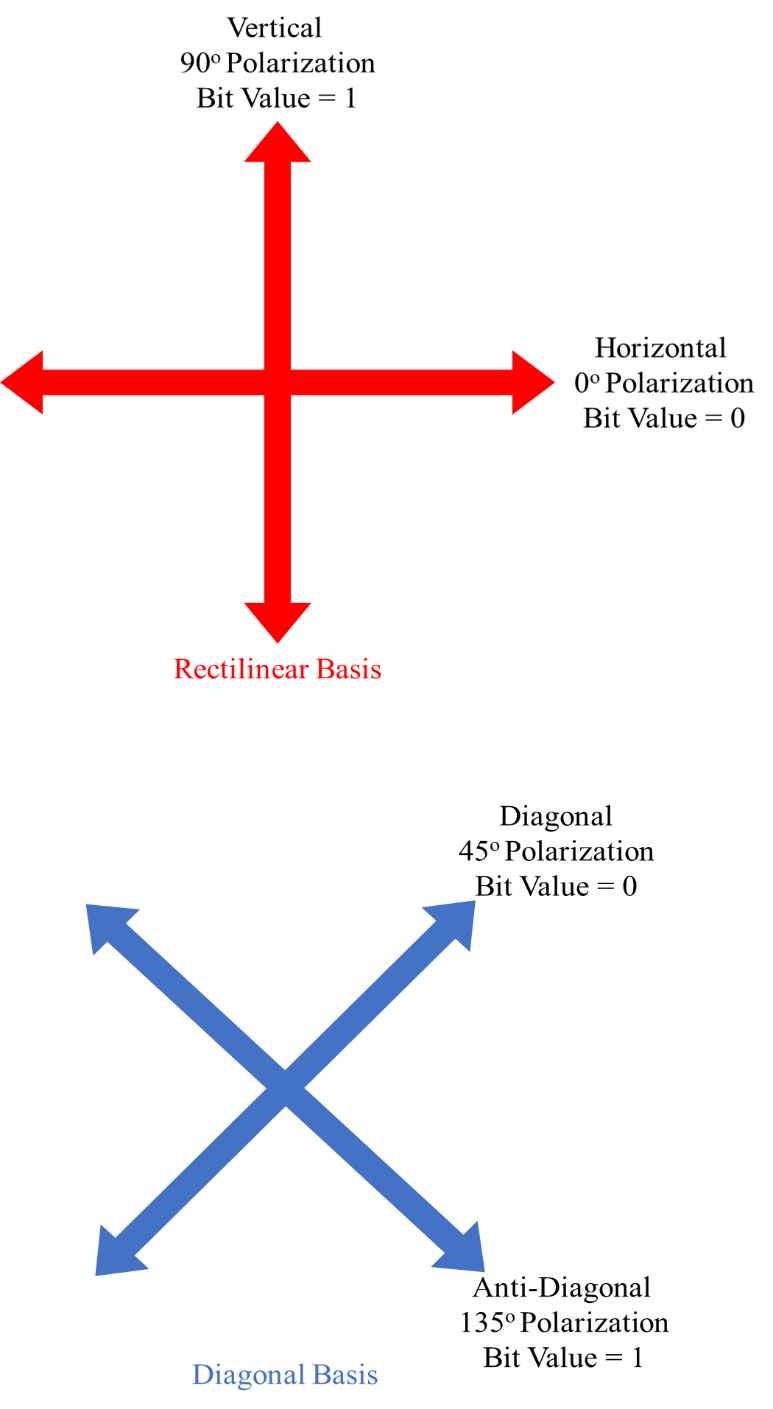
A QKD technique was created by Ekert [10] in 1991 utilizing entangled photon pairs. The source of the photons can be produced by either Alice or Bob utilizing the photon entanglement concept.

Alice or Bob will each receive one entangled photon from each pair that is released by the entangled photon source. Like the BB84 process, Alice and Bob in the E91 protocol pick a random basis for measurement and talk about them in the classical channel. The quantum principle states that if Alice and Bob employ the same foundation, their outcomes should be opposite. Bell's Inequality test is used by the E91 protocol to identify listeners. E91 protocol is a QKD technique based on entanglement.

1. *BBM92 Protocol*

The fundamental ideas of the BBM92 and BB84 protocols are identical, including the raw key exchange method, key sifting, and privacy amplification. The entanglement based BBM92 protocol is a variation of the BB84 protocol. Shortly after Ekert put up his E91 protocol in 1992 [11], Bennett, Brassard, and Mermin suggested this protocol. BBM92 is a QKD technique based on entanglement.

Fig 4: Polarization Base of BB84 Protocol



1. *B92 Protocol*

The B92 protocol is a condensed version of Bennett's 1992 BB84 protocol [12]. In contrast to BB84, the B92 protocol only employs one of four photon polarization states. It has emerged as the primary distinction between the BB84 and B92 protocols. One bit is encoded as 45 degrees in the diagonal basis while zero bits are encoded as 0 degrees in the rectilinear basis in the B92 protocol. Bennett discovered that the QKD technique may be encoded and decoded using a single non-orthogonal basis without compromising the capacity to detect eavesdroppers. Another distinction between the BB84 and B92 protocols is that under the B92 protocol, if the receiver (Bob) chooses the incorrect basis, he will not be able to collect any data. This phenomenon is referred to as an erasure in quantum mechanics. [13]. Prepare and measure based QKD protocol B92 is categorized as such.

1. *Hybrid DV-CV QKD Protocol*

To get around both the DV and CV QKD methods' shortcomings, a hybrid DV-CV QKD protocol has been developed. The proposed hybrid QKD protocol has Alice execute time-phase encoding for the DV-QKD subsystem while also performing DM-based encoding for the CV-QKD subsystem. In contrast, Bob uses a 1:2 optical space switch to choose between a DV-QKD receiver and a CV-QKD receiver, then applies the same postprocessing to both subsystems to produce a joint secure key from both subsystems. According to the SKR results, the proposed hybrid QKD protocol can greatly outperform CV- and DV-QKD techniques in terms of both possible transmission distance and SKR. Slepian states-based encoding [14] or OAM encoding [15] can be employed in place of time-phase encoding to improve its poor spectral efficiency; however, the complexity of such a hybrid QKD system will be larger.

1. *TF-Type QKD Protocol*

A unique TF-type QKD protocol that can surpass the basic limits on the private capacity of point-to-point QKD over a lossy optical channel is provided in [16], [17], along with a straightforward confirmation of its security. Its secret key rate scales as the transmittance of the quantum channel rather than as. This procedure may alternatively be thought of as a single-photon interference phase-encoding MDI QKD method. It does, in fact, carry over the main benefit of conventional MDI QKD, namely, that it is resistant to any side channel in the measuring unit. Moreover, it has now been experimentally demonstrated in [18], [19] thus showing its practicality.

V. Challenges And Opportunities

1. *Challenges of QC*

The difficulties have grown as quantum cryptography has advanced. The most crucial element of QC, QKD, is also one of the key elements of secure quantum communication. The worry that a quantum computer might invalidate the current public key cryptography using the Shor safe method has passed.

**Theoretical challenges.** A significant concern with quantum computing is its practical applicability, in addition to its theoretical difficulties. A handful of those that merit consideration are given below. True random number, light source, detection, post-processing, authentication, repeater, etc. are some of these problems.

**Experimental challenges.** With time, QKD experimental systems have also significantly improved. We may implement and observe a variety of QKD methods based on physical features in current cryptography applications. There aren't many categories of our QKD methods mentioned here.

* Discrete variable Quantum Key Distribution (DVQKD)
* Continuous Variable Quantum Key Distribution (CVQKD)
* Prepare and Measure Quantum Key Distribution (PMQKD)
* Entanglement Based Quantum Key Distribution (EBQKD)
* Measurement Device Independent Quantum Key Distribution (MDIQKD)

Each category has a sizable number of methods that may be tested and observed to produce fresh outcomes. So far, the general result of this field has been excellent, but there is yet much farther to go.

VI. Conclusion

The potential of quantum cryptography has exceeded observers' expectations. Since quantum cryptography was thought to be the best cryptography, it has proven itself via progress and difficulties.

In addition to demonstrating that it is more secure, quantum cryptography has also claimed to demonstrate the intention of traditional cryptography. The sender and receiver can detect eavesdropping and take necessary action thanks to the qualities it has obtained from quantum physics. The second goal is that nobody can crack the quantum key.

Therefore, we can potentially ensure that QC will be able to meet its goals. With the current advancements that are occurring in this sector, it is anticipated that it will reach many more goals along its journey, having already accomplished numerous milestones in such a short amount of time. Therefore, we may be confident that this study area has a promising future for advancement, and the period to come will be referred to as the quantum computing era.

A novel security method called quantum key distribution (QKD) uses the principles of quantum mechanics to distribute the secret key. QKD offers unwavering security and the capacity to identify eavesdroppers. Researchers are paying close attention to this cryptographic technique as a potential solution to the key distribution issue. There have been many of QKD protocols suggested, but there are only two primary types: entanglement based QKD protocols and protocols based on preparation and measurement. The secret key is distributed via the prepare-and-measure based QKD protocol and the entanglement based QKD protocol, both of which are based on the Heisenberg uncertainty principle.

# References

|  |  |
| --- | --- |
| [1] | L. Rigovacca, G. Kato, S. Bäuml, M. S. Kim, W. J. Munro and K. Azuma, "Versatile relative entropy bounds for quantum networks," *New Journal of Physics,* vol. 20, 2018. |
| [2] | A. Boaron, G. Boso, D. Rusca, C. Vulliez and C. Autebert, "Secure quantum key distribution over 421 km of optical fiber," *Physical review letters,* vol. 121, 2018. |
| [3] | W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature,* 1982. |
| [4] | C. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557,* 2020. |
| [5] | S. Singh, "The Code Book: The Secret History of Codes and Codebreaking," *Fourth Estate,* 2000 . |
| [6] | S. Vittorio, "Quantum Cryptography: Privacy though Uncertainty," *CSA Discovery Guides,* 2002. |
| [7] | E. Biham, M. Boyer, P. Boykin, T.Mor and V. Roychowdhury, "A Proof of the Security of Quantum Key Distribution," *Journal of Cryptology,* vol. 19, pp. 381-439, 2006. |
| [8] | D. Mayers, "Unconditional security in quantum cryptography," *J. ACM,* vol. 48, pp. 351-406, 2001. |
| [9] | P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Phys. Rev. Lett.,* vol. 85, pp. 441-444, 2000. |
| [10] | A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical review letters,* vol. 67, pp. 661-663, 1991. |
| [11] | C. H. Bennett, G. Brassard and N. Mermin, "Quantum cryptography without Bell’s theorem," *Physical review letters,* vol. 68, pp. 557-559, 1992. |
| [12] | C. H. Bennett, "Quantum Cryptography using any two Nonorthogonal Sates," *Physical review letters,* vol. 68, pp. 3121-3124, 1992. |
| [13] | D. Bruss, G. Erdelyti, T. Meyer, T. Riege and J. Rothe, "Quantum Cryptography: A Survey," *ACM Computing Surveys,* vol. 39, 2007. |
| [14] | I. B. Djordjevic, "FBG-based weak coherent state and entanglement assisted multidimensional QKD," *IEEE Photon. J.,* vol. 10, 2018. |
| [15] | I. B. Djordjevic, "Multidimensional QKD based on combined orbital and spin angular momenta of photon," *IEEE Photon J.,* vol. 5, 2013. |
| [16] | S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nat. Commun,* vol. 8, 2017. |
| [17] | M. Takeoka, S. Guha and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nat. Commun,* vol. 5, 2014. |
| [18] | M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan and A. J. Shields, "Experimental quantum key distribution beyond the repeaterless secret key capacity," *Nat. Photon,* vol. 13, p. 334–338, 2019. |
| [19] | S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo and Z.-F. Han, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," *Phys. Rev,* vol. 9, 2019. |

1. [↑](#footnote-ref-1)