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 (QKD)" is currently popular among professionals in the field. For all of the present network security techniques, the situation is grave. The fundamental aspects of quantum physics that interact with network security are as follows. 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 main objective in authoring this article was to provide a succinct analysis and review of latest advancements in the most well-known and technically sophisticated area of quantum computing: QKD. However, we also want to provide a broad overview of several quantum computing domains. The numerous applications of quantum computing, as well as quantum public key cryptography, QKD, and quantum authentication, are discussed in this paper.**

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

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

# I. INTRODUCTION

A

vast field known as quantum computing really falls under the umbrella of quantum physics, a branch of applied physics. The use of tiny particles called "quanta" for communication is referred to as "quantum," or quantum mechanics. In traditional communication, 1 and 0 are represented by bits. Quantum refers to a source of energy that may be negatively or positively charged.

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

* Quantum computing
* QKD
* Blind quantum computing
* Distributed quantum metrology

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]. However, 0.2 dB/km the fiber losses in telecom fibers, not including trusted or quantum booster stations imposes a basic constraint on the range of safe QKD. In fact, it would take 100 years to accurately transmit a single photon even at a GHz repetition rate, across 1000 kilometres of a optical fibre. Furthermore, recent research has established basic restrictions for the secure point-to-point QKD's key rate vs. distance. Among both Alice and Bob, where is the transmittance of the connection? They claim that the key rate scales in a linear manner in the absence of booster sites.

QKD, a unique security technique, to disseminate the secret key leverages the laws of quantum mechanics and provide total security. The quantum physics principles have provided QKD with a new capacity 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. In 1984 the first QKD protocol by Bennett and Brassard was introduced, 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, as well as the Tokyo QKD Network, the DARPA Quantum Network, and the SECOQC QKD Network in Vienna.

A qubit or quantum bit is the polar opposite of a normal bit in quantum computing. Quantum binary 0 and 1 are used in quantum computation exactly like binary 0,1 is used in classical computing to represent 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 or 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 remainder of this essay is organised as follows. We define the fundamental concepts of QKD in Section II. We talk about quantum cryptography in Section III. We discuss several QKD techniques in Section IV, and in Section V, we discuss certain unresolved problems and real-world research implications. We summarise this essay in Section V1 at the conclusion.

II. Basic QKD Principle

**Quantum Cryptography.** The most complex kind of encryption is quantum cryptography, which has advanced beyond conventional cryptography. It merges the two fields of network security and quantum physics. 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. By measuring another particle, we may use this relationship to determine the state of one particle, regardless of how close or how far apart they are. Albert Einstein described this phenomena "spooky activity at a distance."

**Quantum Superposition.** A quantum physics property 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 currently superposed in all of its possible states.

**Non-cloning and the quantum principle of uncertainty.** The production of copies of an unknowable quantum state is prohibited by the non-cloning theorem and the quantum principle of uncertainty. This theorem states that it is simple to identify any undesirable individuals inside a network. This make sure the privacy of any data and the key sent to it.

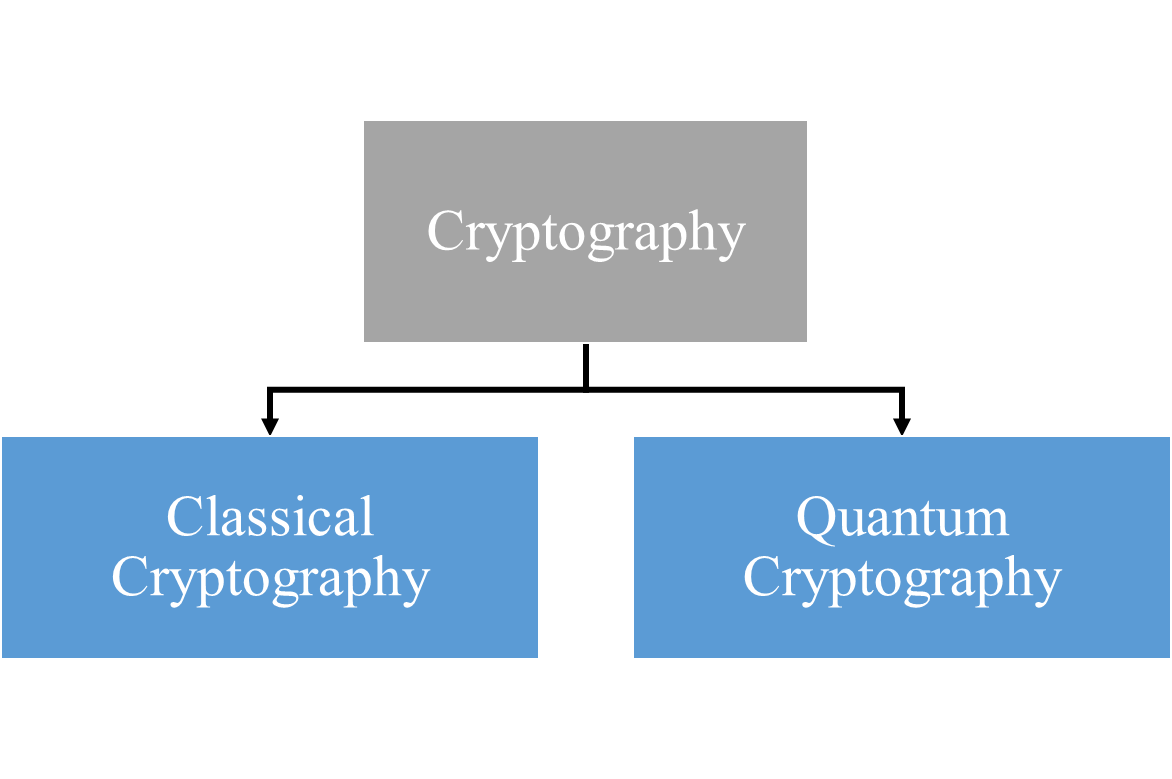
**Quantum measurement.** Quantum measurement is the method of encoding and decoding data using qubits. It is a crucial and extremely significant step in the quantum communication process since it affects the information's integrity. Quantum measurement includes the subprocesses of modification and evolution.

# 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 more information known as a "Key."

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

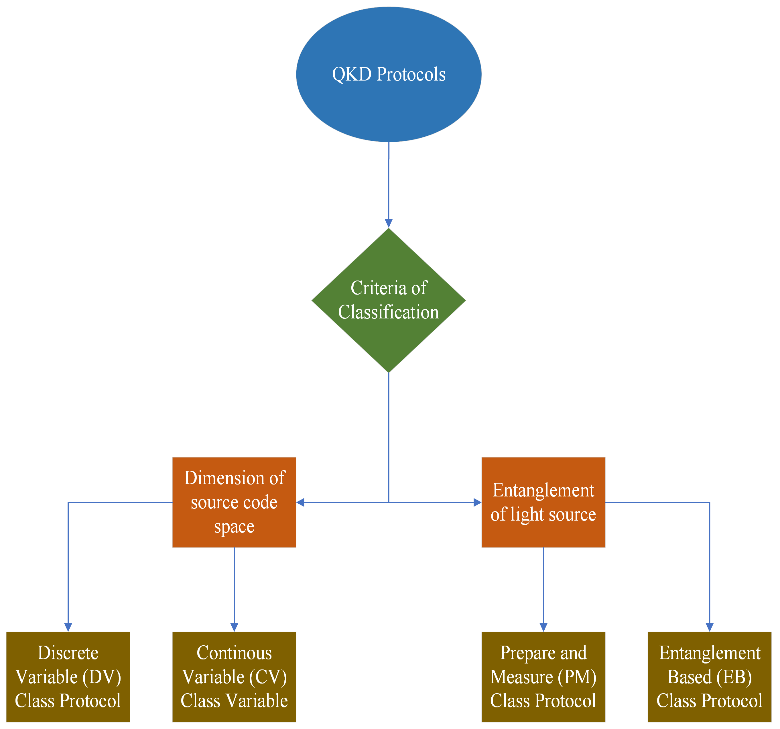
**Fig 1:** Sorting Cryptographic Techniques into Groups



Due to the difference in the number of keys needed in symmetry and asymmetry 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 QKD, quantum dense coding, and quantum teleportation.



**Fig 2:** Classification of QKD Protocols

Key Distribution is the underlying idea behind QKD. 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, in the encryption procedure, the key dissemination is the most crucial and initial step.

1. *QKD*

QKD is built on the use of a non orthogonal, non cloning singular quantum phase to accomplish the key distribution.

Based on its physical characteristics, the QKD procedure may be split among a few separate groups. Built on the size of the source code area, they may be categorised into two groups/class protocols:

* Continuous variable (CV)
* Discrete variable (DV)

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. *Various applications of quantum cryptography*

Other than QKD, 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.
  + Additionally, the user cannot be imitated.; 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:
  + Quantum group
  + Quantum blind
  + Arbitrated quantum

**QPKC (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 to bridge the gap, a new cryptographic system is required. To address this gap, QPKC is a technique that might be used. 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. By developing novel quantum algorithms and processors, Google's Quantum AI initiative aims to enhance quantum computing. It will help researchers and developers identify problems quickly.

# IV. QKD Protocols

In the field of quantum cryptography, QKD is a new technology. Technically, it has been shown that the QKD can guarantee unrestricted security by combining three elements: one-time pad implementation, quantum mechanics law exploit, and hashing technique. The QKD exploits the rules of quantum physics as its security level foundation, in contrast to traditional encryption techniques, which rely on mathematical complication as their security level foundation.

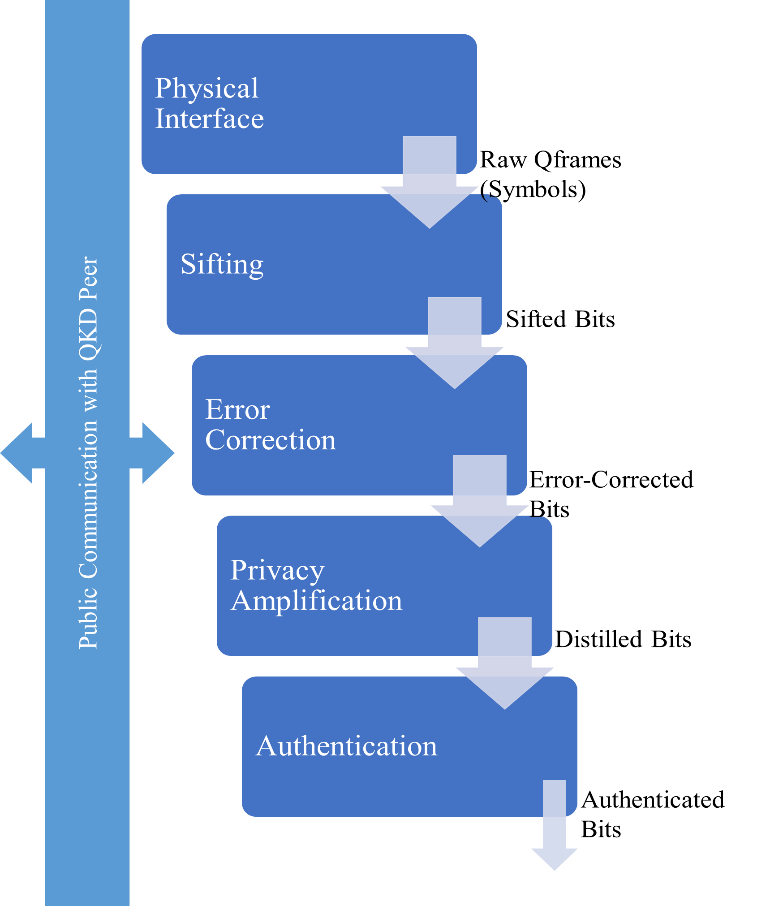
The quantum channel and the public channel are the two channels in the QKD system. The secret key's information is shared and sent through a quantum channel using polarized photons, or quantum bits (qubit). In the meanwhile, agreements on the shared secret key are made while discussing the qubit transfer 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 Eve as the eavesdropper, Bob as the recipient and Alice as the sender.

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

The PM based QKD protocol and the EB QKD protocol are two different kinds of QKD protocol techniques. In this kind of protocol, Alice must "prepare" the data as polarised photons, and Bob, the receiver, then must "measure" the data as received photons. The approach is hence known as "prepare and measure."

The PM based QKD method relies on Heisenberg's uncertainty principle, which holds that it is difficult to quantify a device's quantum status without also modifying its original quantum status. According to the no-cloning theorem, a quantum bit (qubit) cannot be replicated or magnified without being damaged [3]. This method enables the QKD system to identify an eavesdropper by taking use of the error variable readings that appear throughout the photon propagation procedure from Alice to Bob. The secret key is distributed by Alice, Bob, and the entanglement photons principle in the EB QKD algorithm.

**Fig 3:** Complete QKD Protocol Stack



Following five methods make up the whole stack diagram of the QKD protocol, which is shown in Fig 3:

* Raw q-frame
* Bits sifting
* Bits error correction
* Bits distillation
* Bits authentication

QKD protocols: EB and PM based QKD techniques, are covered in this section. By the year of publication, these procedures are discussed in chronological order.

1. *BB84 Protocol*

The Heisenberg uncertainty principle of quantum physics may be used to trade a secret key between two people, according to researchers Bennett and Brassard. in 1984 [4]. 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, also known as the BB84 protocol, is categorised as a PM based QKD protocol.

Using a single photon, the BB84 protocol distributes and transmits random bits of the secret key. The diagonal basis for diagonal and its anti-diagonal polarisation is shown in Fig 4, together with the rectilinear basis for vertical and horizontal polarisation. The single photon is chosen from two conjugate bases and polarised in one of four polarisation states.

The four key phases of the BB84 protocol implementation are:

* Quantum Exchange
* Key Sifting
* Information Reconciliation
* 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*

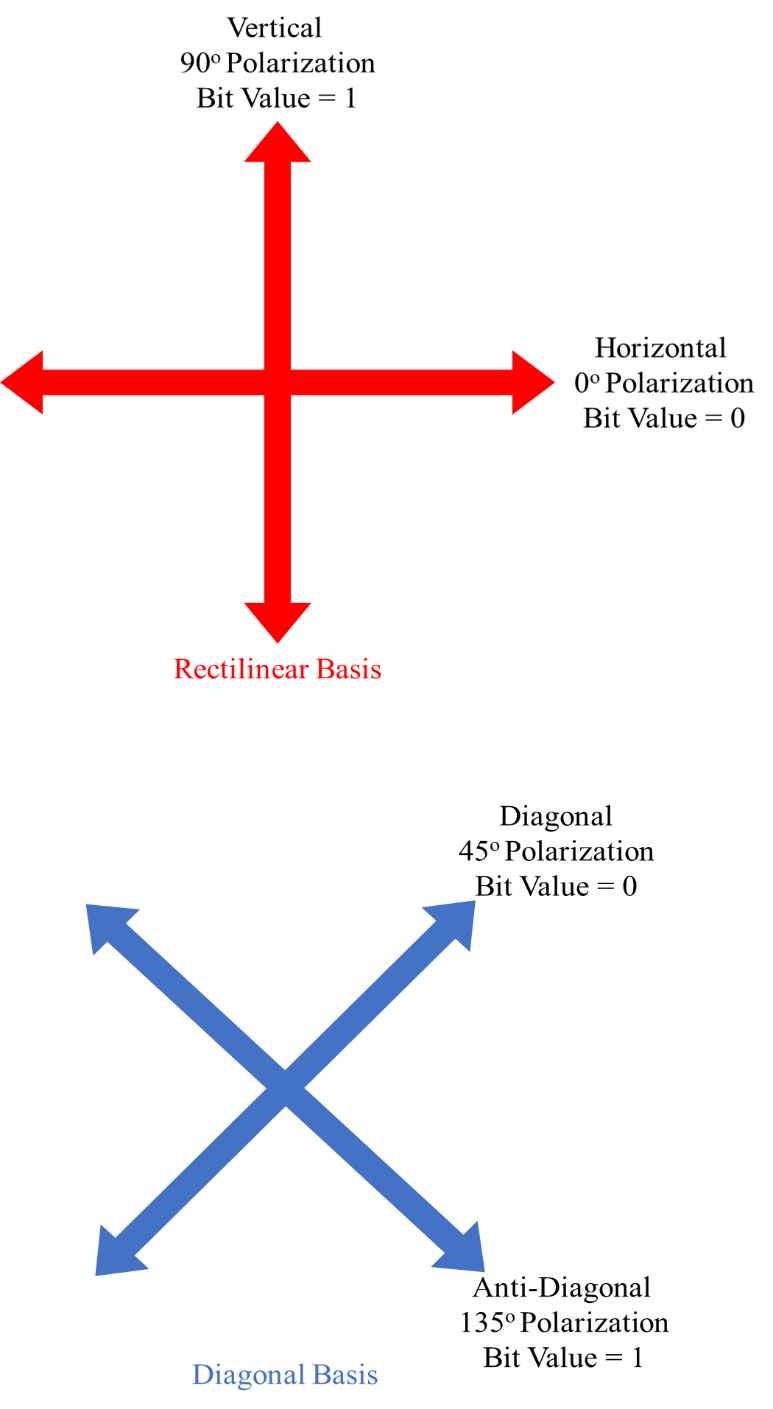
By utilizing entangled photon pairs, a QKD technique was created by Ekert [10] in 1991. Alice or Bob might create the photons as the source utilizing the photon entanglement concept.

From each pair that is released by the entangled photon source, Alice or Bob will each get one entangled photon. In the E91 protocol, Alice and Bob choose a random basis for measuring and converse about it in the classical channel, similar to the BB84 procedure. 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 EB QKD technique.

1. *BBM92 Protocol*

The raw key exchange technique, key sifting, and privacy amplification are common elements of both the BBM92 and BB84 protocols. The EB BBM92 protocol is a variation of the BB84 protocol. Bennett, Brassard, and Mermin suggested this protocol, shortly after Ekert put up his E91 protocol in 1992 [11]. BBM92 is a EB QKD technique.

**Fig 4:** Polarization Base of BB84 Protocol



1. *B92 Protocol*

Bennett's 1992 BB84 protocol has been simplified into the B92 protocol [12]. The B92 protocol simply uses one of the four photon polarisation states, in contrast to the BB84 protocol. It has come to stand out as the key difference among the BB84 and B92 regimens. In the B92 protocol, one bit is encoded as 45 degrees in the diagonal basis and zero bits as 0 degrees in the rectilinear basis. Bennett discovered that the QKD technique may be encoded and decoded using a single non-orthogonal basis without compromising the capacity to detect eavesdroppers. Additional difference between the BB84 and B92 protocols is that using the B92 protocol, Bob would not be capable to gather any data if he selects the wrong foundation. In quantum physics, this occurrence is described to as an erasure. [13]. QKD protocol B92 based on PM is categorized as such.

1. *QKD Protocol Hybrid CV-DV*

A hybrid DV-CV QKD protocol has been devised to overcome the drawbacks of both the DV and CV QKD approaches. In the suggested hybrid QKD protocol, Alice performs both DM-based and time-phase encoding for the DV-QKD and CV-QKD subsystems, respectively. In comparison, Bob switches among a DV-QKD and a CV-QKD receiver via a 1:2 optical space switch, then utilises the same postprocessing on both components to create a single private key from both components. The suggested hybrid QKD protocol may significantly beat CV- and DV-QKD approaches in respect of both potential broadcast range and SKR, as per the SKR findings. 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, such a mixed QKD system will be more complicated.

1. *TF-Type QKD Protocol*

A special TF-type QKD protocol is offered that can go above the fundamental restrictions on the private setting of point-to-point QKD over a lossy fiber link in [16], [17], along with a straightforward confirmation of its security. Its secret key rate scales with the quantum channel's transmittance. 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 impervious to any measurement device side channels. Additionally, it has recently been empirically tested in [18], [19] demonstrating its applicability.

V. Opportunities And Challenges

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.

* Measurement Device Independent (MDI) QKD
* EB QKD
* CV QKD
* DV QKD
* PM QKD

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 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: EB QKD protocols and protocols based on preparation and measurement. The secret key is distributed via the PM based QKD protocol and the EB 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)