Check for updates

IJIST
P ISSN : 2618-1630
E ISSN : 2909-6130

Quantum Key Distribution for Secure Communications

Original Article

Mahira Najeeb[1*], Dr. Ammar Masood[1], Dr. Adnan Fazil[1]
[1]Department of Avionics Engineering, Air University
*Correspondence: Mahira Najeeb 201933@students.au.edu.pk

Citation |Najeeb. M, Masood. A Fazil. A "Quantum Key Distribution for Secure Communications," Int. J. Innov. Sci. Technol., Special Issue, pp. 137-147, 2022.

DOI | https://doi.org/10.33411/IJIST/2022040406

Received | June 30, 2022; **Revised** | Oct 20, 2022; **Accepted** | Oct 25, 2022; **Published** | Oct 30, 2022.

Data protection and information security have been the essence of communication in today's digital era. Authentication and secrecy of secure communication are achieved using key-based cryptographic primitives; the security of which significantly relies upon the underlying computationally complex mathematics. Moreover, these existing cryptographic primitives are considered to be non-deterministic on the basis of the existing computational capabilities. However, the considerable advancements in the development of quantum computers have significantly enhanced parallel computations; thereby, posing a great threat to these existing encryption primitives. Thus, in the future, the physical manifestation of a large successful quantum computer is likely to break all the existing public-key encryption algorithms in no time. This has led to a remarkable surge of interest in propelling quantum mechanics into existence; subsequently, leading cryptographers to research various viable domains to offer quantum-resistant secure communications. Resultantly, quantum cryptography/quantum key distribution has emerged as a futuristic replacement for classical cryptography as it offers unconditionally secure communication along with the inherent detection of any unintended user. Thus, keeping in view the significance of this relatively newer domain of cryptography this research focuses on presenting a consolidated review of the various Quantum Key Distribution (QKD) protocols. A comparative analysis of the working mechanism of the prominent QKD protocols is presented along with an overview of the various emerging trends that have been proposed to optimize the implementational efficiency of the BB84 protocol.

Keywords: Eavesdropping, Classical Cryptography (CC), Quantum Cryptography (QC), Quantum Key Distribution (QKD), continuous and discrete variable protocols.

Acknowledgment.
Firstly, the authors are thankful to Air University, Pakistan for its platform. A special appreciation goes to my co-authors for their guidance and constant support that helped me .complete this research work

Conflict Of Interest: There is no conflict of interest in submitting the manuscript to IJIST by any of the co-authors.

Project details. Nil

Author's Contribution.
Mahira Najeeb: reviewed developed QKD schemes and documented the manuscript. Dr. Ammar Masood: supervised the overall research. Dr. Adnan Fazil: Improvement and finalization of the manuscript.

Introduction

With the embracement of digital communications in our lives, the need for secure communications has become widely crucial to safeguard our sensitive and personal information from any malevolent user. These secure communications, ensuring confidentiality and integrity of information are performed via cryptographic protocols; the necessity of which cannot be over-emphasized. Presently, the major distinction of these cryptographic primitives is in terms of private and public-key cryptographic systems.

In private-key cryptosystem systems, both the communicating parties; the sender (Alice) and the receiver (Bob) must have the same key for performing secure transformations. Subsequently, in a private-key system, the problem of securely distributing the key is as complex as communicating in private itself, as any unintended third party (Eve) may eavesdrop on the key distribution itself hence, resulting in the data breach. On the contrary, in public-key cryptosystems, public and private key pairs are generated and the strength of these systems relies on underlying mathematical complexities. The complexities of these cryptosystems mainly come from [1]:

a. Integer factorization
b. Discrete logarithmic problem
c. NP-hard problems – Elliptic curves

These real-world cryptosystems are considered to be non-deterministic/secure on the basis of existing computational capabilities. However, in 1994, Peter Shor [1]proposed a polynomial-time quantum computer algorithm for efficiently factorizing large odd composite numbers (product of primes) thereby, undermining the security of RSA – integer factorization-based cryptographic algorithm. Similarly, Grover's quantum algorithm [1] proposed in 1996 suggested that successful accelerated attacks can be performed against symmetric ciphers such as AES. This implied that given a sufficiently hefty quantum computer, the presently operational public-key cryptographic systems can be easily compromised in no time; meaning a dead end to existing cryptography and secure communications. As aforementioned in view, it is evident that existing cryptographic schemes (private and public both) suffer from certain limitations which are summarized as follows:

a. Secure key distribution without being intercepted by an untrusted party.
b. Infeasibility of detecting the presence of a malevolent user.
c. Mathematical complexities of public-key algorithms such as RSA, DSA, and ECDSA can be easily computed and compromised provided sufficient physical computing models of quantum computers are made available.

These limitations force us to the conclusion that the advent of a successful quantum computer will fail the existing cryptographic primitives. This eventually led to a surge of interest in the use of quantum mechanics for real-world applications, including the exploration of the feasibility of quantum-resistant cryptographic primitives by cryptographers.

This investigation ultimately yielded a newer domain of quantum cryptography – synonymous with Quantum Key Distribution (QKD) [2] where the security of cryptographic protocols relies on the physical phenomenon of quantum mechanics rather than human-derived complex mathematics. These phenomena offer provably unconditionally secure key distribution along with the intrinsic ability to detect the presence of any unintended user. Thus, quantum cryptography (QC/QKD) deems to be a promising solution to provide unconditionally secure communication to legitimate involved parties in the presence of an eavesdropper having unlimited computational powers at their disposal.

Lastly, it is pertinent to mention that although quantum computing is powerful enough to attack existing cryptosystems, does not exist commercially till now; yet, considering the pace of development as well as the experimental success of QKD, many cryptographers are exploring new quantum-resistant algorithms to safeguard sensitive information – just in case quantum computing becomes a practical unavoidable threat in near future. Apropos, it becomes imperative to rigorously explore quantum computing and accelerate the ongoing research of QKD to overcome its practical challenges; to help rapidly pace us towards the real-world sustainable QKD which not only offers resilience against computational capabilities of quantum computers but also

Motivation/Related Work.

A comprehensive review of the prior work on the subject domain was carried out [1]–[8]However, it was observed that in most of these publications firstly, the authors did not present all the developed QKD protocols. Secondly, the comparative analysis between the working mechanisms of the proposed QKD protocols was very limited. Lastly, it was observed that the previous research either gave or not details the emerging optimization trends in this field. Table 1 below summarizes the prior work related to the review of the developed QKD protocols.

Table1. Comparative study of related work

Ref	Year	Comparative analysis	Emerging research trends	Limitations
[3]	2007	✗	✗	The working mechanism of BB84, B92, and E-91 protocols were discussed.
[4]	2009	BB84 and B92	✗	The working mechanism of BB84, B92, Six-state, SARG04, Decoy-state, and E-91 is discussed only.
[8]	2010	✗	✗	The working mechanism of BB84, B92, E-91, SARG04, DPS, and COW protocols is presented.
[1]	2013	✗	✗	BB84, E-91, GMCS, and Decoy-state protocols are considered only.
[6]	2016	✗	✗	The working mechanism of only BB84, B92, Six-state, and SARG04 is discussed.
[5]	2017	✓	✗	Only the underlying principles of limited QKD protocols are presented
[2]	2018	✗	✗	Only a few QKD protocols have been listed against their working mechanism
[7]	2019	✗	✗	The authors did not present the working mechanisms of the considered QKD protocols

However, it is pertinent to mention that to strengthen the notion of QKD applicability in secure communications, having a background of all developed QKD protocols, understanding the existing implementational limitations of BB84 protocol which is considered to be the most explored QKD protocol to date [9] along with the knowledge of the emerging optimization proposals ensuing enhanced secret key rates and transmitted distances of BB84 is deemed crucial.

Novelty/Contribution.

Compared to the previous research, in this article, we present a comprehensive review of all prominent QKD protocols under their categorization scheme. Additionally, various emerging trends [9]–[20]regarding the implementational optimization of BB84 were also reviewed and the same has been penned down to acquaint the reader with various emerging research trends recently suggested by the researchers for efficient and sustainable implementation of the protocol.

Paper Structure.

The rest of the paper is structured in the following manner: Section II presents the fundamentals of quantum cryptography along with the various developed fields of QC. Section III elaborates on the developed QKD protocols as per their classification schemes, and Sections IV, V, and VI discuss the Prepare and Measure (PM), Entanglement-based, and Continuous variable protocols respectively. Later, the implementational challenges and corresponding emerging trends for optimizing the efficiency of the BB84 protocol are mentioned in Section VII along with the gateway to the future research areas of this domain which is followed by the conclusion of the paper lastly. Apropos, the flow chart given below in Figure1 provides a pictorial illustration of the research methodology followed in this paper.

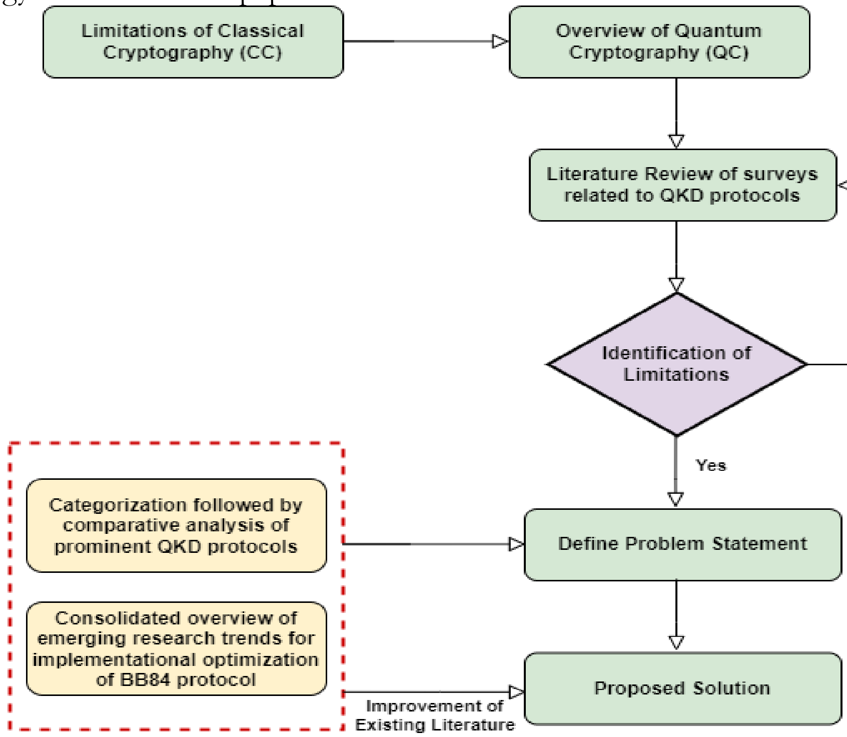
Limitations of Classical Cryptography (CC)
Overview of Quantum Cryptography (QC)
Literature Review of surveys related to QKD protocols
No
Identification of Limitations
Yes
Categorization followed by comparative analysis of prominent QKD protocols
Consolidated overview of emerging research trends for implementational optimization of BB84 protocol
Define Problem Statement
Proposed Solution
Improvement of Existing Literature

Figure1: Pictorial illustration of the research flow adapted for a comprehensive review of all developed QKD protocols

Fundamentals of Quantum-Crypto

Stephen Wiesner [4]proposed the concept of quantum cryptographic procedures by using "conjugate coding" which opened the research gates for achieving secure communications by exploiting the laws of quantum physics. Quantum cryptography relies on the subtle properties of quantum no-cloning, Heisenberg's uncertainty principle, superposition, and entanglement (also known as spooky action at a distance) to accomplish tasks that are otherwise considered intractable using classical cryptography (such as unconditionally secure key distribution, resilience to quantum attacks against classical cryptography and detection of the presence of eavesdropping as a measure of disturbance to the quantum channel).

Various explored domains of quantum cryptography include quantum coin flipping, Quantum Secret Sharing (QSS), Quantum Random Number Generators (PRNGs), Quantum Key Distribution (QKD)[5], Quantum Authentication, Quantum AI, Quantum Digital Signatures (QDS) [6]and Deterministic Secure Quantum Communication (DSQC)[15]. Among all, Quantum Key Distribution (QKD) is the far the most explored and developed application.

Developed QKD Protocols

QKD System Model.

A generic QKD setup comprises two legitimate users (Alice and Bob) communicating in a manner that any activity/observance by an unintended eavesdropper (Eve) is inherently detected by the legitimate parties as a measure of the disturbances observed in the quantum states/channel. This is also elaborated in Figure 2 ahead.

Classification Scheme of QKD Protocols.

BB84 protocol; named after its developers C. H. Bennett of the IBM Research Institute in the United States and G. Brassard of the University of Montreal in Canada in 1984 [1]was the first-ever known protocol of QKD. This protocol was based on the no-clonability principle of quantum states. Ever since many QKD protocols have been developed exploiting different properties of quantum mechanics such as quantum entanglement/teleportation. The major distinction between QKD protocols is, however, between the continuous variable (CV) and discrete variable (DV) QKD [17] based on the dimension of the source.

The DV category of QKD protocols is further categorized as Prepare and Measure (PM) and Entanglement-based (EB) protocols depending upon the underlying property of the quantum mechanics exploited by these classes of protocols.

These categorizations have been summed up in Table 2 presented below for ready reference of readers:

Table 2. Classification scheme of QKD protocols

Category	Salient Features	Pros & Cons
Discrete Variable protocols	**Quantum Signal:** Single photons/ Entangled photons with information encoded as polarization, time-bin / linear momentum states[10] **Detectors:** Single Photon Detectors (SPDs) Prepare and Measure (PM) Entanglement Based (EB)	**Pros:** Compared to CV; DV schemes are optimal in case of harsh channel conditions/ attenuations **Cons:** Detector-induced dark counts; multi-photon pulse probability makes the signal more susceptible to photon number splitting PNS attacks.
Continuous Variable protocols	**Quantum Signal:** Amplitude and phase quadrature of electromagnetic fields are exploited for encoding information in coherent states of light **Detectors:** coherent homodyne or heterodyne detection.	**Pros:** Comparative to DV these protocols are easier to implement with standard telecom components offering higher key rates in metropolitan distances. **Cons:** Requires stability against channel imperfections.

Prepare and Measure (PM) Protocols

These protocols are based on the quantum no-cloning theorem where information is encoded using polarization states of quantum bits- (qubits). The general PM-based setup essentially comprises single-photon sources at the transmitter end, a quantum channel for transmission of information-carrying polarized states of qubits, and a single photon detector at the receiving node. The generic PM model is depicted below in Figure 2.

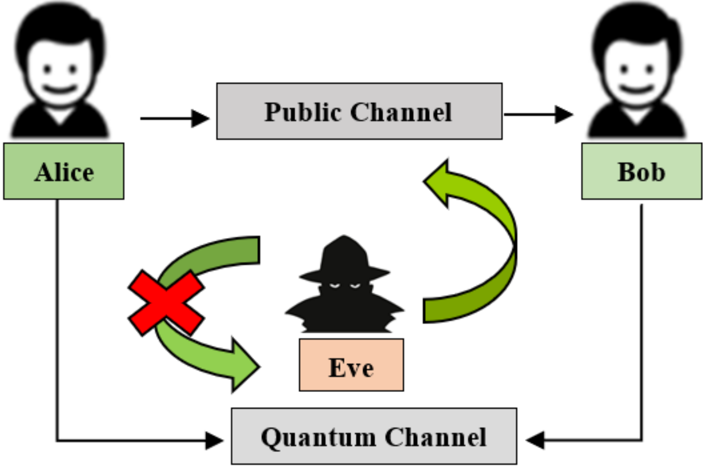

Figure 2: Generic model of PM-based QKD protocol

The encoding of binary information to the optical coherence includes both the quantum and the classical channel. A **quantum channel;** fiber optics or free space is used as a one-way channel for the secure transmission of encoded data from Alice to Bob followed by the communication over a **classical channel;** a two-way path used for authentication and announcement of selected polarization basis. Later on, **post-processing;** including key-sifting, reconciliation, and, error detection and correction is performed for privacy amplification. The protocols developed under this category are as follows:

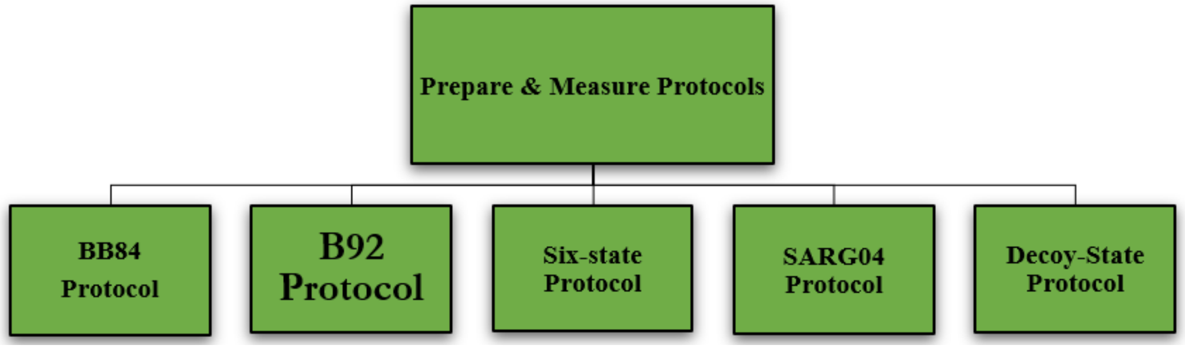

Figure 3 Prepare and measure QKD protocols

BB84 Protocol.

Based on the no-clonability principle, BB84 is the most realized QKD protocol. It encodes classical binary bits as different polarization states of a photon (qubit). Polarization is performed using two different orthogonal bases (rectilinear and diagonal bases) of a two-dimensional Hilbert space. Transmitter randomly selects either of the polarization states and transmits encoded photons to the receiver over a quantum channel. The receiver node unaware of the transmitter's selection again randomly selects the basis and measures the photon. Afterward, the transmitter announces the selected basis over the classical channel corresponding to which the receiver discards all the unmatched bits thereby resulting in the sifted key.

B92 Protocol.

Proposed by Bennet in 1992, this protocol uses one of the two polarization bases used in BB84 (either rectilinear or diagonal); therefore, the receiver measures no output in case of unmatched polarization basis. Resultantly, it offers intrusion detection at lower key rates with efficiency reduced to one-half as compared to BB84[4].

Six-State Protocol.

This protocol was proposed by Brub as an extension of the BB84 protocol with six feasible polarization states. Due to increased polarization states the eavesdropper subsequently, possesses less mutual information resulting in stronger security however, a reduced key distribution rate was observed in the six-state protocol compared to that in BB84[2].

SARG04 Protocol.

Proposed by V. Scarani in 2004, this protocol differed from BB84 in terms of photon sources as it utilized attenuated laser pulses instead of SPS. At the quantum processing level, SARG04 was viewed as equivalent to BB84 by Chi-Hang Fred Fung[7]. Theoretically, SARG04 appeared to be a more feasible practical implementation of PM-QKD but the experimental results in [8]established that the key generation rate of SARG04 is lesser than half of BB84.

Decoy-State Protocol.

This protocol was proposed by Hwang to provide a solution to the inherited PNS vulnerability [1]of BB84 due to SPS. In this protocol, the transmitter emits both the BB84 as well as decoy states. From the produced pulses BB84 states are conventionally used to produce the key whereas the decoy states are used for detecting the possibility of eavesdropping and defining the acceptable thresholds for quantum bit error rate (QBER). The first decoy-state method experiment had a key generation of 165 bits/sec at a distance of 15 km. However, the farthest demonstration showed the impact of QKD at 100 km[2]. This decoy-state BB84 modification/protocol is being aggressively explored as it offers QKD with a larger distance and key generation rate and is compatible with current hardware.

Entanglement-based (EB) Protocols

Lutkenhaus [4]discovered that the single-photon sources (SPS) of PM-based protocols are vulnerable to PNS attacks thus, to overcome the stated limitation this class of QKD protocols named; entanglement-based protocols was proposed. Particles are prepared in a manner that their correlations are preserved irrespective of the spatial distances between them. Mentioned below in Figure 4 are the significant EPR protocols:

Ekert91 - E91 Protocol.

Proposed by Ekert in 1999, this was the first protocol under this category. Contrary to prepare and measure protocols, an entangled pair of polarized photons are generated, one for both the communicating parties. Each user measures the received photon states by randomly selecting the measurement basis and continues with the classical and post-processing phases similar to the BB84 protocol.

Coherent One Way - (COW) Protocol.

Proposed by Nicolas Gisin et al. in 2004[2], this protocol encoded information in time. The sender emits a sequence of coherent pulses and decoy sequences whereas the receiver detects these pulses on both the detector and monitor line and classically shares the same information with the sender. The sender then verifies the presence of Eavesdropper through reduced interference visibility.

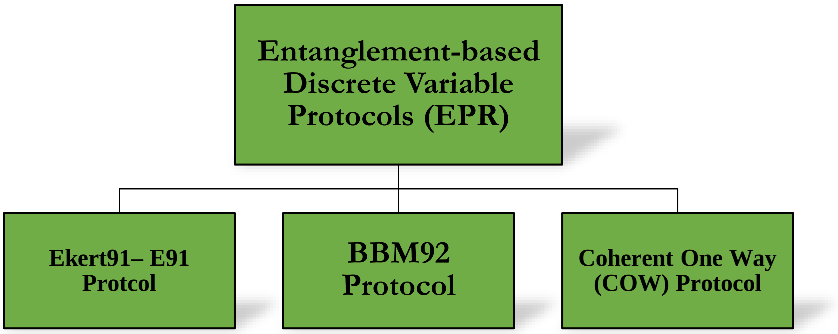
Entanglement-based Discrete Variable Protocols (EPR)
Ekert91– E91 Protocol
BBM92 Protocol
Coherent One Way (COW) Protocol

Figure 4 Entanglement-based (EB) QKD protocols

In generic, EPR-based protocols are not only resistant to PNS attacks but also offer longer transmission paths, easier detection of Eavesdropping, and elimination of insecure storage [1]compared to PM-based protocols.

Continuous Variable (CV) Protocols

Various QKD protocols developed under the category of continuous variables are GG02 (coherent state balanced homodyne detection protocol), Coherent state heterodyne detection protocol, Round-robin differential phase shift (RRDPS), and LMo5[7], however, Gaussian modulated coherent state (GMCS) has attained special consideration from the research community and same is discussed below:-

Gaussian Modulated Coherent State (GMCS).

In GMCS, the transmitter sends the coherent states along with a reference pulse. Before transmission, both the amplitude and phase quadrature of the coherent state is modulated using Gaussian distributed random variables. The receiver randomly selects either of the quadratures and announces the same on the classical channel followed by error detection and correction. Contrary to the BB84 protocol, GMCS uses homodyne detectors which measure electric fields. GMCS protocol offers higher key rates but is suitable only for shorter distances as their performances are limited by channel losses.

The salient features extracted during the review of the above-mentioned QKD protocols are tabulated below in Table 3.

Emerging Trends for Implementation of BB84 Protocol

Secret key generation rate versus the transmission distance plot of the protocols along with the estimation of acceptable intruder-induced transmission known as quantum bit error rate (QBER) and compatibility with the current hardware is very crucial for evaluating the real-world implementation of QKD protocols. Currently, QKD implementations have shown limited key generation rates and transmission distances are also not very encouraging for real-life implementations. Irrespective of these mentioned shortcomings, however, aggressive attempts are being made to integrate QKD with classical optical networks. Inauguration of the 2000km Beijing-Shanghai Quantum Line in 2017[21], the implementation of BB84 for transmitting secret keys in 802.11 wireless architecture and satellite communications are the major milestones that have paved the way for the beginning of a practical era of quantum cryptography.

Having discussed the QKD protocols and their current footings; this section now aims to bring forth the new arenas of research by addressing the challenges faced during practical implementations of BB84. A tabular insight revealing major limitations of BB84 implementation along with the latest solutions adopted by researchers to optimize the above-stated parameters have been elucidated in Table 4 to aid in a better understanding of the emerging trends for efficient implementation of fiber optics-based BB84 - QKD protocol, whereas significant advancements for optimizing free-space implementation of BB84 have also been discussed in[22]–[27].

Table 3. Comparative analysis of salient features of developed QKD protocols

Category	QKD Protocols	Underlying Principle
Prepare and Measure (PM) Protocols	BB84	Based on the no-clonability principle this protocol encodes classical binary information as two different orthogonal polarization bases.
	B92	This protocol is principally similar to BB84 except that it uses either of the two polarization bases resulting in reliable intrusion detection
	Six-State	Extended version of BB84 protocol that encodes information using six polarization states to extend the stronger notion of security
	SARG04	Key rates generated using this protocol are estimated to be lesser than BB84 yet it offers practical feasibility as it employs Attenuated Laser Pulses compared to SPS
	Decoy-State	In addition to the conventional BB84 states, additional decoy states are also transmitted to extend security against the inherent Photon Number Splitting attacks of BB84
Entanglement-based (EB) Protocols	Ekert-91	Correlations between the entangled pair of photons are measured by communicating parties
	BBM92	A working mechanism similar to BB84 with the exception that this protocol uses correlated pairs of photons
	COW	This protocol encodes information as the time when the receiver detects the pulses both on the detector and monitor line for detecting Eve.
Continuous Variable Protocols	GMCS	Compared to other QKD protocols, GMCS uses homodyne detectors for measuring the transmitted electric field of the transmitted signal

Future Research Work.

During the study, it was observed that existing studies and experiments have provided significant contributions to the practical realizations of QKD protocols. However, most of these analyses were carried out in a noise-free channel whereas in real-world applications signal deterioration is observed due to eavesdropping, depolarizing channels, collective dephasing, Amplitude damping (AD), and Phase damping (PD). Apropos in view, performance analysis of QKD protocols under the effect of collective noises is recommended as a future research problem. The study of this analysis will not only enhance the existing knowledge but will also contribute directly toward the practical realization of QKD protocols [28][26].

Table 4. Real-world implementational challenges and proposed optimization schemes for the BB84 protocol

Challenges	Proposed Optimization Strategy	Ref
Low Secure key generation rate (SKR)	Encoding based on Pulse Position Modulation (PPM) Quantum dense coding (QDC) implemented via CNOT quantum gates; is advantageous compared to the Single Photon Sources (SPS) Signature-based authentication combined with an error correction method (based on odd/even parity) followed by a pre-negotiated basis between sender and receiver.	[18]–[20]
Eavesdropping / Susceptibility to PNS attacks	Chromatic dispersion supported pulse modulation PM-PM configuration of frequency-coded QKD	[14]
Transmission losses due to fluctuating polarizations	Subcarrier wave generation (SCW) with a strong reference method; signal photons are generated on subcarrier frequencies, or sidebands, as a result of phase or amplitude modulation of a carrier wave	[13]
Attenuation due to lossy channels	The Legendre symbol is used to calculate the basis of polarization. Both sender and the receiver negotiate on the function of the Legendre symbol resulting in a lesser quantum error rate	[11]
	Hamming code (Parity bits), Cyclic redundancy check (CRC) approach used for error detection and correction results in reduced frequency of mismatched bits	[12][27]

Conclusion.

The objective of this paper was to highlight the necessity of the emerging field of quantum cryptography and subsequently bring forth a comprehensive overview of the current footings of this promising cryptographic field. Apropos, this article reviewed the prominent QKD protocols according to their categorization schemes and highlighted that most of the proposed protocols are modified extensions of basic BB84 protocols. Moreover, it is observed that although the proposed QKD schemes are theoretically non-deterministic yet their implementation inherits hardware limitations which results in limited practicality. However, various optimization schemes are being tested to overcome these limitations. In this regard, the emerging research trends being proposed for improving the implementational efficiency of the BB84 protocol, have been penned down in particular. Hence, this paper primarily focused to acquaint the reader/researcher with the current standings of the quantum field along with evolving research trends for optimizing BB84 real-world implementation to widen the horizons of secure communications in the imminent quantum era.

References

[1] X. Tan, “Introduction to Quantum Cryptography,” Theory Pract. Cryptogr. Netw. Secur. Protoc. Technol., Jul. 2013, doi: 10.5772/56092.

[2] A. I. Nurhadi and N. R. Syambas, “Quantum Key Distribution (QKD) Protocols: A Survey,” Proceeding 2018 4th Int. Conf. Wirel. Telemat. ICWT 2018, Nov. 2018, doi: 10.1109/ICWT.2018.8527822.

[3] A. L, “Survey of Most Prominent Quantum Key Distribution Protocols,” Int. Res. J. Eng. Technol., pp. 2395–56, 2016.

[4] M. Javed and K. Aziz, “A survey of quantum key distribution protocols,” Proc. 6th Int. Conf. Front. Inf. Technol. FIT ’09, 2009, doi: 10.1145/1838002.1838046.

[5] M. Moizuddin, J. Winston, and M. Qayyum, “A comprehensive survey: Quantum cryptography,” 2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017, pp. 98–102, Apr. 2017, doi: 10.1109/ANTI-CYBERCRIME.2017.7905271.

[6] V. Padamvathi, B. V. Vardhan, and A. V. N. Krishna, “Quantum Cryptography and Quantum Key Distribution Protocols: A Survey,” Proc. - 6th Int. Adv. Comput. Conf. IACC 2016, pp. 556–562, Aug. 2016, doi: 10.1109/IACC.2016.109.

[7] A. Sharma and A. Kumar, “A Survey on Quantum Key Distribution,” IEEE Int. Conf. Issues Challenges Intell. Comput. Tech. ICICT 2019, Sep. 2019, doi: 10.1109/ICICT46931.2019.8977649.

[8] M. Javed and K. Aziz, “A survey of quantum key distribution protocols,” Proc. 6th Int. Conf. Front. Inf. Technol. FIT ’09, no. May 2014, 2009, doi: 10.1145/1838002.1838046.

[9] Z. Liliana, “Two, three and four dimensional BB84: A comparative analysis based on C# simulation,” 2019 8th Int. Conf. Emerg. Secur. Technol. EST 2019, Jul. 2019, doi: 10.1109/EST.2019.8806204.

[10] I. H. L. Grande et al., “Adaptable transmitter for discrete and continuous variable quantum key distribution,” Opt. Express, Vol. 29, Issue 10, pp. 14815-14827, vol. 29, no. 10, pp. 14815–14827, May 2021, doi: 10.1364/OE.425382.

[11] R. Amiri, P. Wallden, A. Kent, and E. Andersson, “Secure quantum signatures using insecure quantum channels,” Phys. Rev. A, vol. 93, no. 3, pp. 2619–2633, Mar. 2016, doi: 10.1103/PhysRevA.93.032325.

[12] A. A. Abdullah, R. Z. Khalaf, and H. B. Habib, “Modified BB84 Quantum Key Distribution Protocol Using Legendre Symbol,” SCCS 2019 - 2019 2nd Sci. Conf. Comput. Sci., pp. 154–157, Mar. 2019, doi: 10.1109/SCCS.2019.8852619.

[13] S. Sreelatha and G. Murali, “Error correction and detection techniques in quantum cryptography protocol,” 2017 Int. Conf. Energy, Commun. Data Anal. Soft Comput. ICECDS 2017, pp. 3584–3588, Jun. 2018, doi: 10.1109/ICECDS.2017.8390130.

[14] J. Mora, A. Ruiz, W. Amaya, and J. Capmany, “Dispersion supported BB84 quantum key distribution using phase modulated light,” Jan. 2010, doi: 10.48550/arxiv.1001.0547.

[15] Y. C. Jeong, S. W. Ji, C. Hong, H. S. Park, and J. Jang, “Deterministic Secure Quantum Communication on the BB84 System,” Entropy 2020, Vol. 22, Page 1268, vol. 22, no. 11, p. 1268, Nov. 2020, doi: 10.3390/E22111268.

[16] X. Yang, J. Jiao, Y. Shi, and Y. Liu, “Modeling and Security Analysis Method of Quantum Key Distribution Protocol Based on Colored Petri Nets,” Int. Conf. Commun. Technol. Proceedings, ICCT, pp. 283–289, Oct. 2019, doi: 10.1109/ICCT46805.2019.8947177.

[17] V. Usenko, M. Lasota, and R. Filip, “Continuous and discrete-variable quantum key distribution with nonclassical light over noisy channels,” 2016 39th Int. Conf. Telecommun. Signal Process. TSP 2016, pp. 753–756, Nov. 2016, doi: 10.1109/TSP.2016.7760985.

[18] A. Gueddana, M. Attia, and R. Chatta, “Optimized QKD BB84 protocol using quantum dense coding and CNOT gates: feasibility based on probabilistic optical devices,” Nonlinear Opt. Its Appl. VIII; Quantum Opt. III, vol. 9136, no. May 2020, p. 913627, 2014, doi:

10.1117/12.2048809.

[19] Y. Zhang and I. B. Djordjevic, "Generalized PPM-based BB84 QKD protocol," Int. Conf. Transparent Opt. Networks, 2014, doi: 10.1109/ICTON.2014.6876373.

[20] H. F. Li, L. X. Zhu, K. Wang, and K. Bin Wang, "The improvement of QKD scheme based on BB84 protocol," Proc. - 2016 Int. Conf. Inf. Syst. Artif. Intell. ISAI 2016, pp. 314–317, Jan. 2017, doi: 10.1109/ISAI.2016.0073.

[21] R. Rostom, B. Bakhache, H. Salami, and A. Awad, "Quantum cryptography and chaos for the transmission of security keys in 802.11 networks," Proc. Mediterr. Electrotech. Conf. - MELECON, no. April, pp. 350–356, 2014, doi: 10.1109/MELCON.2014.6820559.

[22] J. S. Choe, H. Ko, B. S. Choi, K. J. Kim, and C. J. Youn, "Silica Planar Lightwave Circuit Based Integrated 1 × 4 Polarization Beam Splitter Module for Free-Space BB84 Quantum Key Distribution," IEEE Photonics J., vol. 10, no. 1, 2018, doi: 10.1109/JPHOT.2017.2788638.

[23] X. Sun, I. B. Djordjevic, and M. A. Neifeld, "Secret Key Rates and Optimization of BB84 and Decoy State Protocols over Time-Varying Free-Space Optical Channels," IEEE Photonics J., vol. 8, no. 3, 2016, doi: 10.1109/JPHOT.2016.2570000.

[24] Z. Yan et al., "Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links," J. Light. Technol., vol. 31, no. 9, pp. 1399–1408, 2013, doi: 10.1109/JLT.2013.2249040.

[25] M. Jofre et al., "100 MHz amplitude and polarization modulated optical source for free-space quantum key distribution at 850 nm," J. Light. Technol., vol. 28, no. 17, pp. 2572–2578, 2010, doi: 10.1109/JLT.2010.2056673.

[26] Y. C. Jeong, Y. S. Kim, and Y. H. Kim, "An experimental comparison of BB84 and SARG04 quantum key distribution protocols," Laser Phys. Lett., vol. 11, no. 9, pp. 1–5, 2014, doi: 10.1088/1612-2011/11/9/095201.

[27] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on practical quantum cryptography," Phys. Rev. Lett., vol. 85, no. 6, pp. 1330–1333, 2000, doi: 10.1103/PhysRevLett.85.1330.

[28] M. Jofre et al., "100 MHz amplitude and polarization modulated optical source for free-space quantum communications at 850 nm," Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng., vol. 43 LNICST, no. 17, pp. 297–304, 2010, doi: 10.1007/978-3-642-13618-4_22.