Publications

Available Online

J. Sci. Res. **14** (3), 959-972 (2022)

JOURNAL OF
SCIENTIFIC RESEARCH

www.banglajol.info/index.php/JSR

Review Article

Quantum Dialogue Protocols: A Review

S. Chauhan[1*], G. Ahmed[1], N. L. Gupta[2]

[1]Department of Physics, Mewar University, Chittorgarh, Rajasthan, India

[2]Department of Physics, Government College Dungarpur, Rajasthan, India

Received 20 February 2021, accepted in final revised form 20 May 2022

Abstract

In recent years, quantum cryptography (QC) has received much attention in academic and commercial fields. It has proved to be a promising technology for ensuring the security of future data transmission. In this paper, we review the development of a remarkable area of quantum cryptography, i.e., Quantum dialogue (QD), which is currently in the theoretical stage but is of great interest to academics. We will discuss the quantum dialogue protocols in two categories, single photon-based protocols, and entanglement-based protocols, depending on the quantum resource employed. Finally, experimental implementation, comparison and analysis, security and practical feasibility, and future work for the above-mentioned branch will also be discussed.

Keywords: Quantum cryptography; Quantum information; Quantum dialogue; Information leakage.

doi: http://dx.doi.org/10.3329/jsr.v14i3.53280 J. Sci. Res. **14** (3), 959-972 (2022)

1. Introduction

Security is one of the utmost serious concerns in the present era, as electronic data transfer performs an essential role in all types of communications. Although classical encryption techniques have been in use for a long time and have been difficult to crack in many situations, the emergence of quantum computing and quantum cryptography [1–3], notably Shor's algorithm [4], has rendered conventional classical encryption algorithms ineffective. The RSA method, for example, has long been thought to be hard to crack. But as Ekert demonstrated in 1996, the perceived intransigence of factoring huge numbers that RSA relies on is under threat due to the emergence of quantum algorithms [5].

Quantum cryptography, on the other hand, offers a new security level that can be accomplished due to quantum mechanics' unique features. Quantum Key Distribution (QKD) is an early quantum communication system that focuses on securely disseminating

[*] *Corresponding author*: humsihachauhan@gmail.com

an arbitrary public key to the two communicating users. It can then utilize the key as a one-time pad to cipher and convey its information classically. The most well-known QKD protocols are BB84 [6] and E91 [7]. Since there are several issues regarding the distribution of keys before communication; as a result, Quantum Secure Direct Communication (QSDC) has been proposed and intensively investigated as an alternative to QKD [8,9]. Despite having a similar purpose to QKD, QSDC does not use a conventional channel to send encrypted data; instead, encrypted messages are sent directly over the quantum channel. Many QSDC protocols have been presented using different techniques.

Further, Quantum Dialogue (QD), a new category of quantum communication protocol based on QSDC, has just been suggested. Many QSDC and QD properties are similar, such as information being transmitted fully over the quantum channel. However, the latter allows participants to interact bidirectionally, which is important in practice. In 2004, Nguyen [10] presented the first Bidirectional Quantum Secure Direct Communication (BQSDC) system, which is also called Quantum Dialogue (QD). It allowed both authorized parties to communicate directly their secret messages utilizing Bell states. This, however, could not withstand an intercept-and-resend attack. However, Gao *et al.* [11] and Tan *et al.* [12] separately showed a type of insecurity known as information leakage or classical correlation in those quantum dialogue schemes. From the context of information theory, they pointed out that the transmitted data can be partially leaked out. To put it another way, an eavesdropper can gather some information regarding secret messages from legal user’s public pronouncements. Following that, several techniques that do not leak information were provided. Man *et al.* [13] were the first to incorporate a controller into the design of a QD. As a result, QD protocols are classified into two types based on whether or not a controller is present: Controlled Quantum Dialogue (CQD) and Controller Independent Quantum Dialogue (CIQD).

In the controlled quantum dialogue (CQD), the users use a controller to monitor the communication. A secure CQD protocol must fulfill at least two conditions: First, users cannot collaborate to communicate without the controller's approval. Second, neither outsider attackers nor the controller has access to confidential information. Subsequently, the issue of information leaking in Man *et al.* CQD's protocol was highlighted, and numerous improvements were offered. Information leaking is a challenge in constructing controlled quantum dialogue (CQD) protocols. Compared to CQD protocols, CIQD protocols outperform, especially in terms of efficiency. The majority of the prior QD schemes were two-qubit CIQD schemes, but later it was generalized to multiqubit systems.

In this paper, the progress of Quantum dialogue, with attention to many unresolved challenges and technical difficulties, will be discussed. We also categorized these schemes into single photon-based and entanglement-based schemes, depending on the quantum resource used. Finally, we will discuss the branch's future issues and research ambitions.

2. Quantum Dialogue (QD)

For the sake of this study, all of these quantum dialogue schemes can be broadly classified into two classes based on the quantum resources employed: Class A refers to single-qubit-based schemes that use a single photon to implement the protocol, while Class B refers to entangled-state-based protocols which utilize one or more entangled states to perform the protocol.

2.1. *Single photon-based protocol*

In this technique, a single photon or a sequence of single photons is encrypted with a bit value of 0 or 1, often by a photon superposition state like polarisation. A conventional laser emits photons as dim light pulses, so the majority of pulses do not emit a photon. This method ensures that only a few pulses comprising more than one photon pass through the fiber-optic line. Finally, only a small percentage of the received pulses contain a photon. The photons that reach the receiver are used. The message is usually encoded in the polarization or relative phase of the photon. The single particle-based protocols are as follows:

Ji and Zhang [14] introduced a quantum dialogue approach by employing N groups of single photons. The sender encodes the same cryptic information on each group of single photons by applying two distinct unitary operations I = $|0\rangle\langle 0|$ + $|1\rangle\langle 1|$, and $i\sigma_y$ = $|0\rangle\langle 1| - |1\rangle\langle 0|$ where I → $0, i\sigma_y \rightarrow 1$, and then sends the N groups of single photons to the recipient. The data is encrypted on the leftover group by the receiver after the eavesdropping check. Because the photons are delivered once in the quantum dialogue approach, it is possible to prevent the intercept-and-resend assault and pair ancillary types of assaults more effectively.

Shi *et al*. [15] devised a quantum dialogue using single photons. To prevent data loss, a participant produces single photons and puts both of the two adjoining photons to an identical state, with the earlier photons (referred to as message photons) containing the hidden message. In contrast, the latter photons indicate the actual states. Both communicants embed their private information on the message photons after ensuring that photon transmission is reliable. The problem of information leakage is resolved since the actual states are hidden from outcasts.

In the same year, Shi and Tian [16] suggested another quantum dialogue involving controlled-not (CNOT) operations. The controlled-not operations are also used by two communicants to exchange the initial states confidentially. Because both protocols' message photons must travel round-trip via quantum channels, many single photons are employed to counteract Trojan horse attacks, malicious user attacks, and denial-of-service attacks. Consequently, this technique is less efficient.

Luo and Lin [17] presented a protocol that relied on the secret sending sequence of particles and a one-way hash function requiring only one quantum communication and five classical communication. The suggested protocol ensures safe bidirectional communication while verifying the message's integrity. The proposed protocol was devoid of information leakage since the starting states of the single photons are transmitted confidentially betwixt the two participants. Because the total photons are sent in a single attempt, Trojan horse assaults are intrinsically eliminated

Min [18] introduced a CQD protocol that prevents data leakage across an ideal channel by using single photons to carry secret data and pre-shared keys to verify the integrity and regulate data decryption. Additionally, a unique unitary encoding method with better quantum operation discriminating properties is used to prevent active attacks from external eavesdroppers. For secret encoding messages, the four local unitary operations I, U, C, and UC are used.

where

$$U = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$C = \sqrt{U} = \frac{1+i}{2}\begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}$$

This protocol also concentrated on three fault-tolerant variants of the proposed CQD technique that can counteract collective-dephasing, collective-rotation, and all types of unitary collective noise, respectively, by replacing logical qubits for single photons and designing unitary encoding procedure with almost the similar feature as logical qubits.

A measurement device-independent QD protocol was put forward by Das [19] in which nearly half of the qubits are discarded to avoid data loss. The authors eliminated nearly half of the abandoned qubits following the error estimating stage to make the approach secure from information leaking. In this paper, they proposed two improved versions of the Measurement Device Independent (MDI) QD protocol. The majority of abandoned qubits is lowered to nearly one-fourth of the leftover qubits after the error estimation phase. They use almost half of all their abandoned qubits alongside their utilized qubits to make the protocol extra efficient in terms of qubit tally.

Lang *et al*. [20] came up with a way to enhance the quantum channel's capacity that relies on a single photon in polarisation and spatial-mode degree of freedom (PSDF). This task utilizes solely two single unitary operations. Their analysis reveals that the suggested QD approach is protected and does not permit information to leak. It does not use ancillary photons and requires single photons in PSDF, which can be readily generated and measured using today's technology.

2.2. *Entanglement based protocol*

Entangled states have attracted considerable attention in recent years due to their potential applicability in quantum information theory. As a result, numerous researchers proposed QD techniques based on entanglement. To strengthen the protocol’s authenticity and security, some introduced a third party (say Charlie) as a controlling authority of the communication, while others did not. Depending upon the controller's role, the entanglement based protocols can be further classified as:

2.2.1. *Controlled quantum dialogue (CQD)*

Man *et al*. [13] utilized the Greenberger–Horne–Zeilinger (GHZ) states and dense coding to achieve quantum dialogue with the controller's assistance. It can encode the GHZ state with a four-bit classical message and two unitary encoding operations on two qubits, a superdense coding signature. Despite having all of the information required for users to communicate, the controller cannot acquire relevant secret messages. On the other hand, the users cannot establish communication without the controller's parameter.

Xia *et al*. [21] suggested a controlled, secure quantum dialogue protocol that incorporates pure entangled GHZ states and purifies the noisy quantum channel to accomplish reliable communication. In the same year, Xia [22] introduced a controlled N-party simultaneous QD approach by utilizing three-particle GHz and then generalized it to a controlled N-party simultaneous QD scheme based on N + 1- particle GHZ states. Rather than using joint-basis measurement, the suggested techniques require merely single-qubit measurement, making them easier to implement experimentally.

Ye *et al*. [23] discovered that the protocol proposed by Man *et al*. [19] has an information leakage problem, which means that the first bit of cryptic information from any communicating partner is often spilled out unintentionally after the controller announces measurement outcomes and proposed two improved solutions to overcome it based on GHZ states and EPR pairs. However, it was demonstrated that these two improved techniques still face the problem of information leakage [24] and the intercept-and-resend attack [25]. Specifically, employing the intercept-and-resend attack, a malicious user, Bob, can receive the other user's cryptic information without the controller's authorization. Using Bell states, an enhancement is offered accordingly to eliminate the information leaking issue and the intercept-and-resend attack.

Kao *et al*. [26] reported that several prior CQD techniques were vulnerable to the colluding attack and provided a modified approach. In this paper, they presented a conspiring assault to allow participants to conspire for obtaining the control factor from the controller for secure communications. By employing the suggested conspiring assault, the communicants will be able to exchange an entangled correlation. Therefore, they can communicate securely without the authorization of the controller. As a result of this finding, this study presents a new constraint for CQD protocols for the first time that the users cannot connive to interact without the controller's consent.

Subsequently, in 2017, they suggested a new CQD protocol [27] based on four-particle cluster entangled states resistant to most of the attacks, have a greater qubit efficiency, and reduce the controller's waiting time, but without taking into account the possibility that the controller is untrustworthy. They also offered a modified version of Man *et al*.'s protocol [19] that met the three requirements of CQD.

Liu *et al*. [28] highlighted that the protocol presented by Kao et al. [27] would unavoidably be vulnerable to dishonest controller assaults, such as different-initial-state (DIS) and denial-of-service (DoS) attacks, and devised a better technique to address these security flaws. To prohibit a dishonest controller from creating alternative initial states, a security check to the controller has been introduced, and message authentication to rectify the DoS attack. Owing to these loopholes, a new requirement is introduced for CQD protocols that the users should be capable of preventing the attacks of a dishonest controller.

During the transmission process, the polarization of photons is affected by the channel noise. Since the quantum channels are prone to noise, it's unavoidable. So, in 2020, to eradicate the disruption from the surrounding factors, Chang [29] designed a CQD protocol against collective noise, which are against collective-dephasing noise and collective-rotation noise, respectively, by employing decoherence-free states, e.g., χ- type entangled state. Especially, it needs to emphasize that not only are two types of logical χ-type states generated by them, in theory, to be against collective noise, but their protocols can effectively withstand both the conspiring assault and the dishonest controller's assaults. It is worth noting that not only do they generate two types of logical-type states to combat collective noise, but their protocols can also efficaciously endure both the conspiring assault and the dishonest controller's assaults

Further, Hong [30] developed two controlled quantum dialogue schemes employing six-qubit entangled states. Under the supervision of an honest supervisor, one entangled state can be utilized to interchange two private bits between two communicants. According to security analysis, it can solve the problem of information leaking and withstand active assaults from an external attacker. The proposed technique mainly requires single-particle and Bell state measurements, which are both attainable with existing technologies.

2.2.2. *Controller independent quantum dialogue (CIQD)*

Nguyen [10] proposed the first quantum dialogue protocol, which uses Bell states to allow two legitimate participants to communicate secret messages simultaneously. He modified the previous ping-pong protocol [30], using superdense coding to quadruple quantum channel capacity subtly. He asserted that against some assaults, this technique is asymptotically secure.

Shi *et al.* [31] pointed out that only two bits of the four-bit information are safely conveyed in the preceding approach. The Holevo quantity, which asserts that in a two-level system, n qubits cannot be utilized to convey more than n bits of classical data, limits the efficiency of data transmission. However, with Nguyen's protocol, this limit has been overrun; thus, Nguyen's protocol is unquestionably insecure. To solve the issue of information leakage, they suggested a bidirectional secure quantum communication scheme in which the shortcoming of "information leakage" is resolved by transferring a private quantum state between the participants. This approach can also improve the existing bidirectional quantum communication protocols.

Additionally, the scheme's 4-bit secret data is transmitted by four qubits, indicating that it has the Holevo limit's greatest potential. Yin [32] presented a two-photon entanglement efficient bidirectional protocol. In this approach, just half of the entangled photon pairs must be generated for the same amount of hidden messages as in Shi's protocol. In Shi's protocol, 2N bits of classical information must be disclosed in classical public communication, while just N bits must be announced in this scheme. Also, it is more efficient and secure because it employs two non-orthogonal measuring bases.

Banerjee *et al.* [33] proposed a framework for Asymmetric Quantum Dialogue (AQD) in a noisy environment in which Alice and Bob's entangled state and encoding technique are determined by the amount of classical data they wish to transmit. It was created with the help of a group-theoretic structure of the operators. The analysis conducted on the suggested method also showed that the suggested AQD exhibits greater leakage than its QD equivalent. However, the leakage can be entirely avoided by incorporating a QSDC approach for transmitting information about Bob's initial condition. Furthermore, as the number of travel qubits in AQD decreases (compared to an equivalent QD scheme), the effect of various noise models tends to decrease. Moreover, by adopting an entangled state with an odd number of particles (such as the GHZ state), it was proven that the suggested AQD's qubit efficiency can be enhanced and that it was robust to various noises while using the optimal amount of quantum resources.

Mohapatra [34] proposed an improvement to the Chang protocol [25] by introducing four states arbitrarily as Charlie's initial state, allowing Alice and Bob to select their hidden message regardless of the original states created by Charlie. However, the hidden messages can be used to choose the initial states. This is only achievable if the communicants construct the most entangled initial states. As a result, the controller's role is rendered insignificant. So, he devised a new protocol in which Alice and Bob can generate Bell states as their original states based on their hidden messages and share their secret messages without relying on Charlie's controller.

Cao [35] designed a four-qubit cluster state channel in the protocol, which can be utilized to realize four-qubit bidirectional direct communication. After verifying the quantum channel's security, the users transmit an ordered sequence of four qubit cluster states generated by Alice. Then, based on the final result, both will perform unitary operations in accordance with their secret message and deduce each other's message.

A safe QD scheme comprised of four qubit cluster states [36] had been introduced by Li *et al*. Two authorized users can communicate their information safely and concurrently utilizing four Bell measurements and unitary operation. Moreover, due to entanglement swapping, data transfer cannot be interrupted or influenced by noise in the communication process once the quantum channel is perfectly established. But it has information leakage, which was further improved by Zhihao *et al.* in 2020 [37] by requiring only a single particle measurement rather than a Bell-basis measurement and no unitary operation. Furthermore, the Li's QD protocol's communication efficiency has been enhanced to 1.33 times.

Zhang [38] devised a novel scheme to accomplish the purpose of CIQD utilizing a type of four-particle entangled states and a special feature of entangled states, for instance, if each qubit is evaluated on a $\{|0\rangle, |1\rangle\}$ basis, the appropriate outcomes of measurement q_i, q_j, q_s, q_t will satisfy the equation $q_i \oplus q_j = q_s \oplus q_t$. Two authorized communication users can communicate their secret messages concurrently using the proposed protocol. According to the security analysis, this scheme can withstand different assaults, like intercept-and-resend, entangle-and-measure, and counterfeit entangled particle assaults. Furthermore, the data cannot be leaked to authorized communicating users.

Huang [39] presented a three GHZ state-based QD technique. It enables two distant lawful users to send encrypted messages simultaneously. For today's technology, the approach may be practically achievable. According to the authors, this technique has a large potency because each GHZ state may share two bits of encrypted messages with each participant. Since the users merely use a single unitary operation to encrypt the two-bit secret data so, 50 percent of the exchanged data is accidentally revealed in this approach. It was cryptanalysis by Zhi *et al*. [40] and upgraded by encrypting the one-bit hidden message with one of the two unitary operations. For instance, if Alice wishes to convey Bob confidential bit 0, she can use U_{00} or U_{01}, whereas she can encode 1 using U_{00} or U_{10} randomly. If Bob wishes to transmit Alice's confidential bit 0, he can use U_{00} or U_{10} and U_{01} or U_{11} to convey secret bit 1 at random**.**

Chauhan [41] developed a secure QD approach characterized by four qubit cluster states employed as initial states to carry secret messages. This approach involves the notion of optimum quantum superdense coding, which indicates that two bits of data can be encoded on a sole quantum bit without interrupting entanglement. Therefore, it satisfies the Holevo constraint. This method is robust to various known assaults having no issues with data leakage. The secure realization of the quantum dialogue is contingent on the quantum channel's security, which is accomplished through two security checks.

3. Comparison and Analysis

According to the above study, the merits and demerits of both types of protocols are as follows:

1. Decoherence: Single photon-based QD methods are the most affected by various disturbances, but entanglement-based schemes are robust against decoherence due to the utilization of multiparticle entangled states, allowing for reliable transmission over noisy channels.

2. Efficiency: The single photon-based schemes have low efficiency, whereas the efficiency of entanglement-based protocols can be enhanced by using dense coding on multiparticle entangled states.

3. Information leakage: Single photon-based QD methods have a high risk of information leakage, but entanglement plays a significant role in overcoming this issue.

4. Practicability: A single photon-based protocol is a realistic candidate for long-distance communication, but it is difficult to produce a single photon experimentally. Since other photons can be generated simultaneously in the given time window, disrupting communication and causing attacks such as PNS attacks and invisible photon attacks. In the case of an entangled state, it is difficult to implement a multipartite entangled state

practically because of the non-availability of nonlinear devices. But still, these multiqubit entangled states can be generated in laboratories with the help of suitable quantum gates.

5. Distribution: It is easy to disseminate a single photon compared to entangled states in the case of N party distribution.

6. Expenditure: The transmission of single-photon is less expensive than entangled states.

The present work's comparative analysis of single-photon-based and entanglement-based schemes of secure quantum communication systems yielded a number of intriguing results. It has been noticed that it is difficult to claim unequivocally that entanglement-based schemes outperform single-photon-based approaches or vice versa. Precisely, single-photon-based schemes are usually considered to be the best alternative for long-distance communication and experimental feasibility. Furthermore, the single-photon-based QD technique generally requires additional communication rounds. As a result, the single-photon-based QD method has been the most susceptible to noise. This issue can be solved by employing multiparticle entangled states decoherent against disturbances. Also, multiparticle entangled state protocols are significantly better in terms of efficiency and information leakage.

In addition, the above protocols can be analyzed in terms of the controller's counterpart also. As quantum entanglement is the controlling element in these protocols, most contemporary CQD protocols are developed on entangled states. Since the controller in CQD is more capable than the outside unauthorized user, the possibility that the controller is being dishonest in order to attack the protocol should be rigorously examined. Even though the system is robust against any outside eavesdropper attack but vulnerable to attacks from a deceitful controller, it is still not secure. However, the possibility of a deceitful controller was not addressed. If we investigate this situation, we can see that the deceitful controller can eavesdrop on the user’s private messages using the so-called different initial state (DIS) attack [19,20]. In addition, the original CQD protocol has another security flaw. Because there is no authentication process for the controller, he (she) can intentionally publish false operations. Consequently, the messages received by Alice and Bob differ from the actual messages. This type of attack is known as a DoS attack [21,22]. The controller of this attack has the malicious idea of destroying communication without being identified. Despite all, these protocols are less efficient.

In short, how to design an efficient, authenticated, and safe CQD protocol that fulfills the four features is a popular area of research. To remove assaults that are created due to controller, many QD schemes without controlling heads have been introduced by using entangled multiparty states, which is of great theoretical and practical significance.

Table 1. The comparison of various quantum dialogue protocols.

Year	Author	Quantum resource used	Quantum state used	Controller's role	Efficiency	References
2004	Nguyen	Entanglement based	Bell state	No	67	[10]
2006	Ji *et al*.	Single photon-based	Single-photon	No	50	[14]
2006	Man *et al*.	Entanglement based	GHZ state	Yes	66.6	[13]
2007	Xia *et al*.	Entanglement based	GHZ state	Yes	26	[21]
2009	Shi *et al.*	Entanglement based	Bell state	No	66.7	[31]
2010	Shi *et al.*	Single photon-based	Single-photon	No	16	[15]
2010	Shi *et al.*	Single photon-based	Single-photon	No	22	[16]
2013	Ye *et al.*	Entanglement based	Bell state & GHZ state	Yes	28	[23]
2013	Yin *et al.*	Entanglement based	Two-photon entanglement	No	80	[32]
2014	Luo *et al.*	Single photon-based	Single-photon	No	50	[17]
2016	Kao *et al.*	Entanglement based	Bell state & GHZ state	Yes	10.5	[26]
2016	Banerjee *et al.*	Entanglement based	n-qubit entangled state	No	60 % for four qubit cluster state and 62.5 % for GHZ state	[33]
2017	Kao *et.al*	Entanglement based	Four particle cluster state	Yes	25	[27]
2017	Mohapatra *et al.*	Entanglement based	Bell state	No	33.33	[34]
2018	Min *et al.*	Single photon-based	Single-photon	Yes	50	[18]
2018	Li *et al.*	Entanglement based	Four qubit cluster state	No	25	[36]
2019	Liu *et al.*	Entanglement based	Four qubit cluster state	Yes	12.5	[28]
2019	Cao *et al.*	Entanglement based	Four qubit cluster state	No	66.7	[35]
2019	Zhang *et al.*	Entanglement based	Four particle entangled state	No	33	[38]
2020	Chang *et al*.	Entanglement based	X-type entangled state	Yes	6.25	[29]
2021	Hong *et al*.	Entanglement based	Six qubit entangled state	Yes	40	[30]
2021	Zhi *et al*.	Entanglement based	Three qubit GHZ states	No	100	[40]
2022	Lang *et al.*	Single photon-based	Single-photon with two degrees of freedom	No	66.67	[20]
2022	Chauahan *et al.*	Entanglement based	Four qubit cluster state	No	66.7	[41]

4. Security and Practical Feasibility

For the above-mentioned branch of study, it's still difficult to develop a secure and efficient protocol since we all know that quantum cryptography protocols or systems can be attacked in various ways. While constructing a protocol, it is impossible to consider all conceivable assaults. As a result, most protocols only look at a few well-known sorts of attacks. Furthermore, many new sorts of attacks against cryptosystems may yet be identified despite the known kinds of attacks. To summarise, developing a secure protocol can be challenging, if not impossible. The following are the most frequent approaches for ensuring security at the moment: (1) Creating extra entangled states and utilizing their entanglement correlation to validate the states' legitimacy and determine whether quantum channels are being eavesdropped. (2) Using decoy photon technology to determine if eavesdropping occurs. (3) Protecting data privacy by employing the entanglement correlation of entangled states.

Xu [42] demonstrated a new way for successfully transferring quantum information using paired optical polarization-maintaining (PM) fibers by increasing the usage of a Mach-Zehnder interferometer, where noises are neutralized by interference. This approach can be an enhanced version of fiber optics present Decoherence-free subspace (DFS) approach and can be applied bi-directionally to achieve robust quantum communication. However, Lin *et al*. [43] suggested a novel quantum communication scheme named Continuous Quantum Secure Dialogue (CQSD) in 2019, which permits two participants to transfer information constantly without pausing and maintaining the discourse's confidentiality. They also offer a CQSD protocol implementation based on Qiskit. In the same year, Messa [44] proved that quantum superposition enables two-way communication between two remote parties who can only interchange one particle at a time, which was accomplished by preparing a single photon in a coherent superposition at two participant's sites. These crucial characteristics could contribute to the development of new quantum communication systems that are confidential, safe, and resource-efficient all at the same time.

In most cases, quantum measurement is required in a technique that retrieves data from quantum states. Aside from measurements, implementing other quantum technologies will inevitably raise the requirement for associated devices and technologies.

It is well understood that cryptographic study is geared toward commercial applications. Therefore, protocol efficiency must be considered while creating the protocols. From the aspect of protocol effectiveness, figuring out how to make protocols more efficient while maintaining security is similarly difficult. However, high qubit efficiency is frequently impossible to attain just by quantum measurement, as qubit efficiency typically governs the number of states a protocol uses. Many existing protocols have embraced dense coding techniques as one of the most significant ways of enhancing qubit efficiency.

Furthermore, entanglement swapping among different quantum states has several intriguing aspects that could lead to novel protocol design concepts and methodologies. Multiparticle entangled states are commonly employed in protocol design as information carriers to make protocols more efficient. However, the more qubits in the entangled state, the more complicated it is to construct, making it harder for the scheme to achieve the high-efficiency requirement. Luckily, with the advancement of relevant technologies, numerous significant breakthroughs in the generation and distribution of multiparticle entangled states have been made. Preparing multiparticle entangled states may not be challenging in the coming years.

5. Conclusion

In this paper, we have reviewed the research and development of a significant and well-studied branch of QSDC in quantum cryptography, known as quantum dialogue. We also classified the QD protocols based on the quantum resource utilized as single photon-based and entanglement-based protocols. In addition, entanglement-based protocols are discussed in CQD and CIQD protocols. Based on the above discussion, it is realized that while prior CQD procedures can resist most assaults, certain protocols overlook the data leaking problem and internal attacks, such as the deceitful controller's assault. Furthermore, if users cannot validate the counterpart's authenticity during security checks, the eavesdropper may execute a particular assault known as a man-in-the-middle attack. All these vulnerabilities can be readily avoided by ending the role of the controller in QD protocols.

Furthermore, most of the available QD schemes are developed in an idealistic situation. Since, in the physical world, quantum systems are intrinsically linked with their surrounding environment, which can result in a loss of quantum correlation or decoherence. An attacker may use noise to conceal his assaults in a quantum noise channel. So, in this direction, cluster states, a sort of entangled states, with unexpected and distinctive attributes have attracted much attention. These states have distinct entanglement features than GHZ states and are invulnerable to decoherence. All these make the cluster states helpful resources for QD.

In addition, the experimental implementation, security, and practical feasibility of the research mentioned above, as well as future problems and research possibilities, have also been reviewed. Even though most quantum communication efforts are still being tested and are largely employed in the lab, we believe quantum communication will eventually replace traditional ways due to its greater rate of security and efficiency.

References

1. I. L. Chuang and Y. Yamamoto, Phys. Rev. A, **52**, 3489(1995). https://doi.org/10.1103/PhysRevA.52.3489
2. D. Kielpinski, C. Monroe, and D. J. Wineland. Nature, **417**, 709 (2002). https://doi.org/10.1038/nature00784

3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Rev. Mod. Phys. **74**, 145 (2002). https://doi.org/10.1103/RevModPhys.74.145
4. P. W. Shor - *Proc. 35th Annual Symp. on Foundations of Computer Science* (1994) pp.124-134. https://doi.org/10.1109/SFCS.1994.365700
5. A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996). https://doi.org/10.1103/RevModPhys.68.733
6. C. Bennett and G. Brassard, Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India, (1984) pp. 175–179. https://doi.org/10.48550/arXiv.2003.06557
7. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991). https://doi.org/10.1103/PhysRevLett.67.661
8. F. G. Deng and G. L. Long, Phys. Rev. A **69**, (2004). https://doi.org/10.1103/PhysRevA.69.052319
9. F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, 1094 (2003). https://doi.org/10.1103/PhysRevA.68.042315
10. B. A. Nguyen, Phys. Lett. A **328**, 6 (2004). https://doi.org/10.1016/j.physleta.2004.06.009
11. F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, Sci. China Ser. G-Phys. Mech. Astron. **51**, 559 (2008). https://doi.org/10.1007/s11433-008-0065-y
12. Y. G. Tan and Q. Y. Cai, Int. J. Quant. Inf. **6**, (2008) pp. 325-329. https://doi.org/10.1142/S021974990800344X
13. Z. X. Man and Y. J. Xia, Chin. Phys. Lett. **23**, 1680 (2006). https://doi.org/10.1088/0256-307X/23/7/007
14. X. Ji and S. Zhang, Chin. Phys. **15**, 1418 (2006). https://doi.org/10.1088/1009-1963/15/7/005
15. G. F. Shi, X. Q. Xi, M. L. Hu, and R. H. Yue, Opt. Commun. **283**, 1984 (2010). https://doi.org/10.1016/j.optcom.2010.01.007
16. G. F. Shi and X. L. Tian, J. Mod. Opt. **57**, 2027 (2010). https://doi.org/10.1080/09500340.2010.514072
17. Y. P. Luo, C. Y. Lin, and T. Hwang, Quant. Inf. Processing **13**, 2451 (2014). https://doi.org/10.1007/s11128-014-0803-1
18. X. Min and L. Guang, Chin. J. Elect. **27**, (2018). https://doi.org/10.1049/cje.2017.08.004
19. N. Das and G. Paul, Int. J. Quantum Inf. **18**, ID 2050038 (2020). https://doi.org/10.1142/S0219749920500380
20. Y. F. Lang, Int. J. Theor. Phys. **61**, 105 (2022). https://doi.org/10.1007/s10773-022-05098-7
21. Y. Xia, J. Song, J. Nie, and H. S. Song, Commun. Theor. Phys. **48**, 841 (2007). https://doi.org/10.1088/0253-6102/48/5/017
22. Y. J. Xia and Z. X. Man, Commun. Theor. Phys. **48**, 79 (2007). https://doi.org/10.1088/0253-6102/48/1/017
23. T. Y. Ye and L. Z. Jiang, Chin. Phys. Lett. **30**, ID 040305 (2013). https://doi.org/10.1088/0256-307X/30/4/040305
24. Z. H. Liu and H. W. Chen, Chin. Phys. Lett. **30**, ID 079901 (2013). https://doi.org/10.1088/0256-307X/30/7/079901
25. C. H. Chang, Y. P. Luo, C. W. Yang, and T. Hwang, Quant. Inf. Proc. **14**, 3515 (2015). https://doi.org/10.1007/s11128-015-1050-9
26. S. H. Kao and T. Hwang, Quant. Inf. Proc. **15**, 4313 (2016). https://doi.org/10.1007/s11128-016-1370-4
27. S. H. Kao and T. Hwang, Quant. Inf. Proc. **16**, 139 (2017).
28. Z. Liu and H. Chen, Quantum Inf. Proc. **18**, 98 (2019). https://doi.org/10.1007/s11128-019-2214-9
29. L. W. Chang, Y. Q. Zhang, X. X. Tian, Y. H. Qian, H. Yu, and S. H. Zheng, Chin. Phys. B **29**, ID 010304, (2020). https://doi.org/10.1088/1674-1056/ab5786
30. H. M. Pan, Int. J. Theor. Phys. **60**, 2943 (2021). https://doi.org/10.1007/s10773-021-04866-1
31. G. F. Shi, X. Q. Xi, X. L. Tian, and R. H. Yue, Optic Commun. **282**, 2460 (2010). https://doi.org/10.1016/j.optcom.2009.02.062

32. X. R. Yin, W. P. Ma, and W. Y. Lin, Quant. Inf. Proc. **12**, 3093 (2013). https://doi.org/10.1007/s11128-013-0584-y
33. A. Banerjee, C. Shukla, and K. Thapliyal, Quant. Inf. Proc. **16**, 49 (2017). https://doi.org/10.1007/s11128-016-1508-4
34. A. K. Mohapatra and S. Balakrishnan, Quant. Inf. Proc. **16**, 1 (2017). https://doi.org/10.1007/s11128-017-1598-7
35. Y. Cao, X. W. Zha, and S. K. Wang, Int. J. Theor. Phys. **57**, 2007 (2018). https://doi.org/10.1007/s10773-018-3726-2
36. W. Li, X. W. Zha, and Y. Yu., Int. J. Theor. Phys. **57**, 371 (2018). https://doi.org/10.1007/s10773-017-3569-2
37. Z. Liu and H. Chen, Int. J. Theor. Phys. **59**, 2120 (2020). https://doi.org/10.1007/s10773-020-04485-2
38. L. Zhang, S. Dong, K. J. Zhang, H. –W. Sun, Int. J. Theor. Phys. **58**, 1927 (2019) https://doi.org/10.1007/s10773-019-04087-7
39. Z. Huang and H. Situ, Quant. Inf. Proc. **18**, 37 (2019). https://doi.org/10.1007/s11128-018-2152-y
40. Z. H. Liu and H. W. Chen, Quant. Inf. Proc. **20**, 93 (2021). https://doi.org/10.1007/s11128-020-02850-y
41. S. Chauhan and N. L. Gupta, J. Sci. Res. **14**, 179 (2022). http://dx.doi.org/10.3329/jsr.v14i1.54479
42. J. S. Xu, M. H.Yung, X. Y. Xu, J. S. Tang, C. F. Li, and G. C. Guo, Quant. Phys. (2013). https://doi.org/10.48550/arXiv.1305.1497
43. S. Lin, Z. Wang, and L. Horesh, Quant. Phys. (2019). https://doi.org/10.48550/arXiv.1910.08135
44. F. Massa, A. Moqanaki, A. Baumeler, F. D. Santo, J. A. Kettlewell, B. Daki, and P. Walther, Quant. Phys. (2019). https://doi.org/10.48550/arXiv.1802.05102