Secure Quantum Dialogue Based on Non-Orthogonal Entangled States and Local Unitary Operation

SANJU CHAUHAN[1]
GULZAR AHMED[2]
NARAYAN LAL GUPTA[3]

Mewar University
[1,2]Department of Physics, Chittorgarh, Rajasthan, India
[3]Department of Physics, Government College Kishangarh, Rajasthan, India
[1]humsihachauhan@gmail.com
[2]gulzarahmed61@gmail.com
[2]nlgupt@gmail.com

Abstract. We introduce a secure quantum dialogue scheme characterized by non-orthogonal entangled states that use the concept of superdense coding to obtain optimum efficiency and high resource capacity. In this scheme, two non-orthogonal four-qubit cluster states are deployed as a quantum channel to communicate four-qubit secret information by encrypting only two qubits. By virtue of the non-orthogonality of the quantum channel, the current approach can effectively prevent various sorts of viable unauthorized access while establishing a robust quantum channel. Furthermore, two security checks and authentication processes make it more secure, and it also overcomes the disadvantage of information loss and is technically attainable with present technology.

Keywords: Quantum Dialogue, Non-Orthogonal States, Information Leakage, Clusters States.

(Received December 12th, 2023 / Accepted June 28th, 2024)

1 Introduction

In recent years, quantum cryptography (QC) has received great interest in both academic and commercial fields and proves a promising technology for ensuring the security of future data transmission. A significant branch of quantum cryptography, i.e. Quantum dialogue (QD), which is currently in the theoretical research stage but is of great interest to academics.

Quantum Dialogue (QD), a new category of quantum communication protocol [?] based on Quantum secure direct communication (QSDC), has just been suggested. Many of QSDC and QD properties are similar, such as transmitting information entirely through the quantum channel, but the latter allows users to interact bidirectionally, which is important in practice.

Entanglement has sparked global attention in the last decade due to its practical usage in quantum information theory. It is crucial in preventing information leakage in various QD protocols. Furthermore, information leakage can be mitigated by incorporating multiparticle entangled states (particularly cluster states) into many QD protocols [6, 7, 9, 11, 12, 14, 19, 26]. Cluster states [3], a sort of entangled state with unexpected and distinctive attributes, are crucial in the issue of data leaking. 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, and these states are invulnerable to decoherence.

It is also noteworthy that authentication is a hot concern in quantum communication, as it is utilized to verify a user's authenticity. This strategy can successfully increase the protocol's invulnerability. Many notable protocols [24] that use authentication mechanisms have been offered thus far. However, a counterfeiter may intercept the hidden message or send a fake message to genuine users. Hence, user's identities must be verified.

In this study, we propose a secure QD approach characterized by the non-orthogonality of entangled states. For ensuring the security of QD, two four qubit cluster states are employed as initial states to carry secret messages that are not orthogonal. Here, the nocloning theorem inhibits unauthorized users from replicating them exactly, and the uncertainty principle forbids any unauthorized user from differentiating them without any effect. Because of the considerable endurance of entanglement, cluster states are tougher to destroy using local operations. Unlike previous protocols, 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, our protocol satisfies the Holevo constraint [21] and is the most capable. In addition, with an efficiency of 61.53 percent, our method is more effective.Furthermore, information leakage is not an issue with our scheme. The protocol is safer as a result of two security checks and authentication procedures.

2 Literature and Related Work

In the world of information security, quantum cryptography is a comparatively new entrant. The objective of cryptography is to guarantee that encrypted information is sent between two users somehow in a way that an unauthorized person cannot intercept it. The vulnerability of most cryptosystems in classical cryptography is predicated on the conception of computational intricacy. On the contrary, all contemporary classical cryptographic techniques struggle to develop an arbitrary key that would be reliable for all communicants. Favourably, quantum key distribution (QKD) [1, 2], a significant extension of quantum cryptography [10], can successfully complete this job. Quantum cryptography incorporates quantum mechanics ideas into the cryptographic process, as these are the underlying principles that thus ensure absolute security. Another field of quantum cryptography that has recently emerged and gained much interest is quantum secure direct communication (QSDC) [18, 15, 25]. It enables the sender to convey information straight to the recipient predictably and securely without generating a prior key. In addition, a well-developed QSDC protocol can provide guaranteed protection . Initially, QSDC protocols only allowed communication in a single direction (from Alice to Bob or vice versa). Consequently, as one type of quantum secure direct communication (QSDC), quantum dialogue (QD), that was explicitly introduced by Nguyen [20] and Zhang et al. [27], has a unique feature; namely, it can achieve the mutual interchange of a hidden message from two participants concurrently through the dissemination of the quantum signal. Afterward its discovery, QD has captivated the curiosity of academics, prompting the creation of several other QD schemes [8, 17, 20, 23, 27].

Though we all know that people's growing computing capabilities are seriously jeopardizing the robustness of most conventional cryptographic techniques. The major goal of quantum cryptography would be to alter it and come up with new techniques to achieve greater security. Thus, quantum cryptography's high security is not only a privilege but also a necessity. Nevertheless, not all the existing approaches can meet this criterion. Some protocols, for example, have been effectively assaulted by subtle methods that were not considered whenever they were devised [17]. Quantum cryptography, as we are already aware, requires public classical communication. We must assure that the secret message's information is not disclosed to others through traditional communication. Otherwise, the desired level of security would be compromised. However, Gao et al. [8] reported that the communicated secret information was partially leaked out in several QD protocols in 2008. Tan and Cai [23] revealed the phenomenon known as classical correlation in the same year. In reality, the issue of information leaking is caused by the attributes of classical correlation. To address this flaw, Shi et al. [22] suggested a shared private quantum entanglement channel to achieve bidirectional quantum secure communication. Since then, researchers have focused on developing QD techniques that are immune to information loss [13, 16]. The study on reliable and efficient QD protocols that avoid information leaking, as discussed above, has important theoretical and practical aspects, motivating us to present this scheme.

3 Description of our Protocol

First, we define a four-qubit cluster state as follows to meet the purpose of the QD protocol.

$$|\phi\rangle = \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle\right) \quad (1)$$

Let the four Pauli operators that are employed to encrypt secret data are defined as

$$\sigma_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$$
$$\sigma_1 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$\sigma_2 = \sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$$
$$\sigma_3 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$$

The two-bit classical data can be expressed by four Pauli operators,

$$\sigma_0 \leftrightarrow 00,\ \ \sigma_1 \leftrightarrow 01,\ \ \sigma_2 \leftrightarrow 10,\ \ \sigma_3 \leftrightarrow 11$$

Then, on applying local unitary operation on the first and third particle, the cluster states given in eq. (1) can be converted into the following

$|\phi_1\rangle = \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle\right)_{abcd}$
$|\phi_2\rangle = \frac{1}{2}\left(|0010\rangle + |0001\rangle + |1110\rangle - |1101\rangle\right)_{abcd}$
$|\phi_3\rangle = \frac{1}{2}\left(-|0010\rangle + |0001\rangle - |1110\rangle - |1101\rangle\right)_{abcd}$
$|\phi_4\rangle = \frac{1}{2}\left(|0000\rangle - |0011\rangle + |1100\rangle + |1111\rangle\right)_{abcd}$
$|\phi_5\rangle = \frac{1}{2}\left(|1000\rangle + |1011\rangle + |0100\rangle - |0111\rangle\right)_{abcd}$
$|\phi_6\rangle = \frac{1}{2}\left(|1010\rangle + |1001\rangle + |0110\rangle - |0101\rangle\right)_{abcd}$
$|\phi_7\rangle = \frac{1}{2}\left(-|1010\rangle + |1001\rangle - |0110\rangle - |0101\rangle\right)_{abcd}$
$|\phi_8\rangle = \frac{1}{2}\left(|0000\rangle - |1011\rangle + |0100\rangle + |0111\rangle\right)_{abcd}$
$|\phi_9\rangle = \frac{1}{2}\left(-|1000\rangle - |1011\rangle + |0100\rangle - |0111\rangle\right)_{abcd}$
$|\phi_{10}\rangle = \frac{1}{2}\left(-|1010\rangle - |1001\rangle + |0110\rangle - |0101\rangle\right)_{abcd}$
$|\phi_{11}\rangle = \frac{1}{2}\left(|1010\rangle - |1001\rangle - |0110\rangle - |0101\rangle\right)_{abcd}$
$|\phi_{12}\rangle = \frac{1}{2}\left(-|1000\rangle + |1011\rangle + |0100\rangle + |0111\rangle\right)_{abcd}$
$|\phi_{13}\rangle = \frac{1}{2}\left(|0000\rangle + |0011\rangle - |1100\rangle + |1111\rangle\right)_{abcd}$
$|\phi_{14}\rangle = \frac{1}{2}\left(|0010\rangle + |0001\rangle - |1110\rangle + |1101\rangle\right)_{abcd}$
$|\phi_{15}\rangle = \frac{1}{2}\left(-|0010\rangle + |0001\rangle + |1110\rangle + |1101\rangle\right)_{abcd}$
$|\phi_{16}\rangle = \frac{1}{2}\left(|0000\rangle - |0011\rangle - |1100\rangle - |1111\rangle\right)_{abcd}$

Dense coding switches one cluster state to another in an ensemble of sixteen orthogonal cluster states by operating an appropriate unitary operator (on the first and third qubits), as shown above. Alongwith the orthogonality of these states,they can be implemented as measuring bases for four qubit cluster states via Von Neumann measurement.

Let measuring basis $MB_1 = |\phi_1\rangle, |\phi_2\rangle, .|\phi_{16}\rangle$ is a basis set for a four-qubit cluster state. Another basis set $MB_2 = |\psi_1\rangle, |\psi_2\rangle, .|\psi_{16}\rangle$ can be acquired by applying Hadamard operation

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

on second and fourth particles as

$$|\psi\rangle = \frac{1}{2}\left(|0+0+\rangle + |0+1-\rangle + |1-0+\rangle - |1-1-\rangle \right. \quad (2)$$

where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$

On applying local unitary operation on the second and fourth particle, the above cluster states are given in eq. (2) can be changed into the following

$$|\psi_1\rangle = \frac{1}{2}\left(|0+0+\rangle + |0+1-\rangle + |1-0+\rangle - |1-1-\rangle\right)_{abcd}$$

$$|\psi_2\rangle = \frac{1}{2}\left(|0+0+\rangle - |0+1-\rangle + |1-0+\rangle + |1-1-\rangle\right)_{abcd}$$

$$|\psi_3\rangle = \frac{1}{2}\left(|0+0-\rangle - |0+1+\rangle + |1-0-\rangle + |1-1+\rangle\right)_{abcd}$$

$$|\psi_4\rangle = \frac{1}{2}\left(|0+0-\rangle + |0+1+\rangle + |1-0-\rangle + |1-1+\rangle\right)_{abcd}$$

$$|\psi_5\rangle = \frac{1}{2}\left(|0+0+\rangle + |0+1-\rangle - |1-0+\rangle + |1-1-\rangle\right)_{abcd}$$

$$|\psi_6\rangle = \frac{1}{2}\left(|0+0+\rangle - |0+1-\rangle - |1-0+\rangle - |1-1-\rangle\right)_{abcd}$$

$$|\psi_7\rangle = \frac{1}{2}\left(|0+0-\rangle - |0+1+\rangle - |1-0-\rangle - |1-1+\rangle\right)_{abcd}$$

$$|\psi_8\rangle = \frac{1}{2}\left(|0+0-\rangle + |0+1+\rangle - |1-0-\rangle + |1-1+\rangle\right)_{abcd}$$

$$|\psi_9\rangle = \frac{1}{2}\left(|0-0+\rangle + |0-1-\rangle - |1+0+\rangle + |1+1-\rangle\right)_{abcd}$$

$$|\psi_{10}\rangle = \frac{1}{2}\left(|0-0+\rangle - |0-1-\rangle - |1+0+\rangle - |1+1-\rangle\right)_{abcd}$$

$$|\psi_{11}\rangle = \frac{1}{2}\left(|0-0-\rangle - |0-1+\rangle - |1+0-\rangle - |1+1+\rangle\right)_{abcd}$$

$$|\psi_{12}\rangle = \frac{1}{2}\left(|0-0-\rangle + |0-1+\rangle - |1+0-\rangle + \right. \\ \left. |1+1+\rangle_{abcd}\right.$$

$$|\psi_{13}\rangle = \frac{1}{2}\left(|0-0+\rangle + |0-1-\rangle + |1+0+\rangle - \right. \\ \left. |1+1-\rangle_{abcd}\right.$$

$$|\psi_{14}\rangle = \frac{1}{2}\left(|0-0+\rangle - |0-1-\rangle + |1+0+\rangle + \right. \\ \left. |1+1-\rangle_{abcd}\right.$$

$$|\psi_{15}\rangle = \frac{1}{2}\left(|0-0-\rangle - |0-1+\rangle + |1+0-\rangle + \right. \\ \left. |1+1+\rangle_{abcd}\right.$$

$$|\psi_{16}\rangle = \frac{1}{2}\left(|0-0-\rangle + |0-1+\rangle + |1+0-\rangle - \right. \\ \left. |1+1+\rangle_{abcd}\right.$$

The two basis sets MB_1 and MB_2 are non-orthogonal to one another. The following are four-bit secret data and their accompanying encoding rules:

$0000(\sigma_0^{A_1(A_2)} \otimes \sigma_0^{A_3(A_4)})$, $0001(\sigma_0^{A_1(A_2)} \otimes \sigma_1^{A_3(A_4)})$,
$0010(\sigma_0^{A_1(A_2)} \otimes \sigma_2^{A_3(A_4)})$, $0011(\sigma_0^{A_1(A_2)} \otimes \sigma_3^{A_3(A_4)})$,
$0100(\sigma_1^{A_1(A_2)} \otimes \sigma_0^{A_3(A_4)})$, $0101(\sigma_1^{A_1(A_2)} \otimes \sigma_1^{A_3(A_4)})$,
$0110(\sigma_1^{A_1(A_2)} \otimes \sigma_2^{A_3(A_4)})$, $0111(\sigma_1^{A_1(A_2)} \otimes \sigma_3^{A_3(A_4)})$,
$1000(\sigma_2^{A_1(A_2)} \otimes \sigma_0^{A_3(A_4)})$, $1001(\sigma_2^{A_1(A_2)} \otimes \sigma_1^{A_3(A_4)})$,
$1010(\sigma_2^{A_1(A_2)} \otimes \sigma_2^{A_3(A_4)})$, $1011(\sigma_2^{A_1(A_2)} \otimes \sigma_3^{A_3(A_4)})$,
$1100(\sigma_3^{A_1(A_2)} \otimes \sigma_0^{A_3(A_4)})$, $1101(\sigma_3^{A_1(A_2)} \otimes \sigma_1^{A_3(A_4)})$,
$1110(\sigma_3^{A_1(A_2)} \otimes \sigma_2^{A_3(A_4)})$, $1111(\sigma_3^{A_1(A_2)} \otimes \sigma_3^{A_3(A_4)})$

4 QD PROTOCOL

Alice and Bob, two legal communicants, can concurrently communicate four qubit secret messages via four qubit cluster states in this approach. Our approach can be executed in the following manner:

Step1. Alice first creates two identical 1S and 2S string of n cluster states,each of which is arbitrarily assigned to one of the two non-orthogonal states and are arranged as
S={$S_1^a, S_1^b, S_1^c, S_1^d, S_2^a, S_2^b, S_2^c, S_2^d, ...S_n^a, S_n^b, S_n^c, S_n^d$}

Here, a,b,c,d represent four particles in a four-qubit cluster state, and the notation 1,2...n indicates the order of cluster state in a string. Also, she puts together two groups of decoy photons (for example, *l* and *m* particles) at random, whether it is in X basis $(|+\rangle, |-\rangle)$ or on Z basis $(|0\rangle, |1\rangle)$, to check the channel's security. By incorporating *l* particles into the 1S string, she sends the *(n + l)* string to Bob. In the meantime, Alice develops a classical bit string $R = r_1, r_2, .r_n$ where $r_i 0, 1, i = 1, 2, .N$. If Alice chooses a basis set MB_1 as initial state, then $r_i = 0$ and for $r_i = 1$, Alice choose the MB_2 basis set as the initial state.

Step2. After delivering the string to Bob, they first investigate the channel's security. Alice discloses the position and their respective measuring basis for each *l* decoy photon. The particle is then measured in the announced basis by Bob. He can approximate the error rate by comparing the outcomes. If the procedure reaches the threshold, it is terminated; otherwise, it continues. He abandons *l* particles and measures each of the four particles in the 1S string in order using a cluster basis. Consequently, he recovers the original state of that cluster state in the 1S string.

Step3. To certify Bob's identity, Alice picks a sufficient number of particles from the 2S string, performs Z basis measurement, and reports the position. Bob selects the particle in the same position in the 1S sequence as Alice, examines the Z basis, and compares the findings. If the results are the same, the users' authentication has been confirmed.

After confirming the channel's security, Alice performs the unitary operation $\sigma_2 \otimes \sigma_1$ on the first and third particle of each cluster state into a 2S string if she chooses MB_1 as the initial state. Otherwise, encoding is done on the second and fourth particle of the cluster state, corresponding to a four-bit classical message. For a further security screening, Alice now introduces m particles to the 2S string and transmits *(n + m)* particles to Bob.

Step4. Bob receives the 2S string. Alice broadcasts the position and basis of m particles in a 2S string. To assure the security of channel transmission, Bob measures them in the correct basis, correlates it with Alice's pronouncement, and analyzes whether the string has been eavesdropped and finally, eliminate them. Further, Alice announces the value of R; accordingly, Bob encrypts his secret data by carrying out $\sigma_3 \otimes \sigma_1$ operation on the first and third qubits (if the initial state is a basis set MB_1 otherwise, it is done on the second and fourth particle in a 2S string. After performing the encoding process, Bob executes a cluster state measurement on each of the four particles in the 2S string and publishes his final measurement outcome.

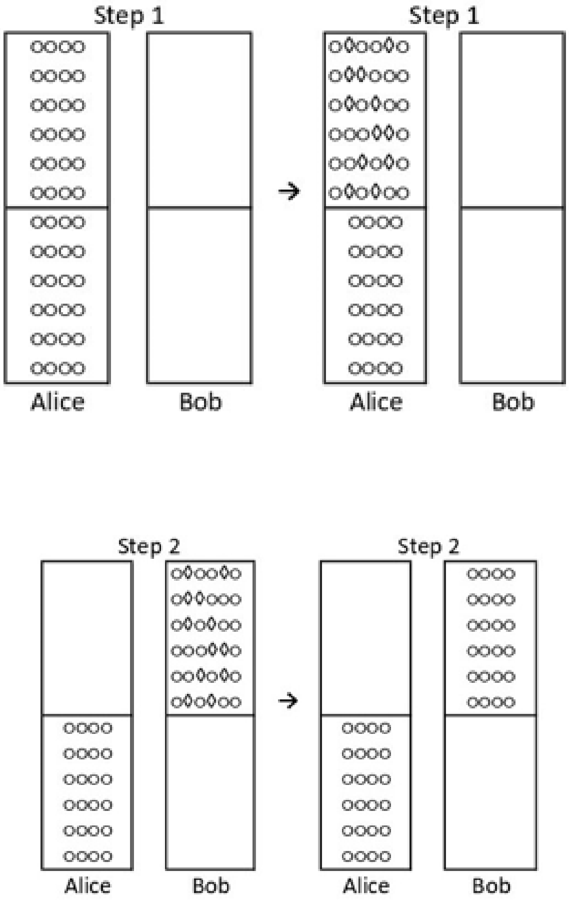
Step5. Alice can infer Bob's secret message based on Bob's findings. Meanwhile, Bob is ready to retrieve

Alice's message.

For example, let Alice declares $r_i = 1,$ and she chooses one of the states $(say|\psi_1\rangle)$ from the basis set MB_2 as initial state, and the communicants Alice and Bob intend to exchange 1001 and 1101 messages, then their encrypting operations are $\sigma_2 \otimes \sigma_1$ and $\sigma_3 \otimes \sigma_1$ respectively, and they obtain the end result $|\psi_8\rangle$ which can be expressed as

$$|\psi_1\rangle = \sigma_2 \otimes \sigma_1|\psi_1\rangle \quad \Rightarrow \text{Alice}$$
$$(\sigma_3 \otimes \sigma_1) \otimes ((\sigma_2 \otimes \sigma_1)|\psi_1\rangle) = |\psi_8\rangle \quad \Rightarrow \text{Bob}$$

The final outcome $|\psi_8\rangle$ is evaluated and broadcasted by Bob. Then as per above mentioned three known messages, she may then figure out Bob's secret operation is $\sigma_3 \otimes \sigma_1$. As 1S and 2S strings are equal, Bob already knows the initial cluster state. Bob can deduce Alice's secret operation is $\sigma_2 \otimes \sigma_1$. Consequently, both the users can transmit the secret message simultaneously.



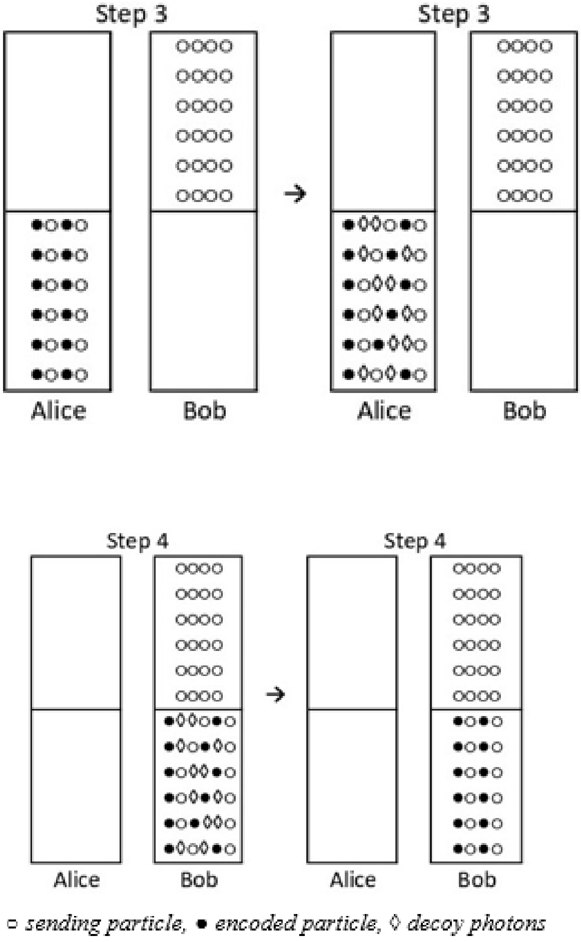


Figure 1: Schematic Illusion of QD

5 Security Analysis

5.1 Information Leakage Analysis

In this scheme, Bob only broadcasts one result, namely $|\psi_8\rangle$ and the actual state is kept between the participants in complete secrecy. Apart from the fact that the channel comprises 16x16 possible sets of operations, which are all equally probable that means
$-\Sigma p_i log p_i = -(16 \times 16) \times \frac{1}{16\times16} log \frac{1}{16\times16}$
= 8 -bit secret message
As the information transferred between Alice and Bob is also 8 bits. Therefore, no information is leaked, and all data is delivered securely.

5.2 Some Attacks

Intercept and Resend attack :Eve captures the 1S state on its way from Alice to Bob and sends a fake 1S string to Bob, with each particle in any one of the four states $|0\rangle,\ |1\rangle,\ (|+\rangle,\ |-\rangle)$ in order to acquire data about the cluster state in the 1S string. However, in our scheme, this issue is avoided because of the usage of two non-orthogonal basis sets. It can make it impossible for anybody to distinguish them flawlessly. Hence, it is safe against this form of attack. As the captured particles comprise decoy photons, Eve will acquire a cluster state after eliminating the decoy photons after Alice reveals the state and location of the particles. On the other end, since Bob is evaluating Eve's counterfeit string, which has a high error rate, he will never get the same output. Consequently, Eve is immediately detectable.

Entangle and Measure attack: A unitary operator on a greater Hilbert Space can actualize Eve's malicious assault, as per Stinespring's dilation theorem. Suppose Eve attempts to retrieve some valuable data from a 1S string going between the communicants by undertaking an entangle and measure attack. To entangle her particle with the communicative sequence, she performs a generic operation U_E on 1S and the adjunct particle $|\varepsilon\rangle$ that she created earlier. When the system's initial state is one of the MB_1 basis sets then Eve's impact on it, is stated as:

$$U_E|0\rangle|\varepsilon\rangle = \alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle \tag{3}$$

$$U_E|1\rangle|\varepsilon\rangle = \gamma|0\rangle|\varepsilon_{10}\rangle + \delta|1\rangle|\varepsilon_{11}\rangle \tag{4}$$

where $|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1$ At such stage, Eve's assault will result in an error rate of $\varepsilon = |\beta|^2 = |\gamma|^2 = 1 - |\alpha|^2 = 1 - |\delta|^2$

When the status of the traveling string is from one of the MB_2 basis sets, then Eve's impact on it is characterized as

$$U_E|+\rangle|\varepsilon\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle + \gamma|0\rangle|\varepsilon_{10}\rangle + \delta|1\rangle|\varepsilon_{11}\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\Bigg[|+\rangle\{\frac{1}{\sqrt{2}}\left(\alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle + \gamma|0\rangle|\varepsilon_{10}\rangle + \delta|1\rangle|\varepsilon_{11}\rangle\right\} + |-\rangle\{\frac{1}{\sqrt{2}}\left(\alpha|0\rangle|\varepsilon_{00}\rangle - \beta|1\rangle|\varepsilon_{01}\rangle + \gamma|0\rangle|\varepsilon_{10}\rangle - \delta|1\rangle|\varepsilon_{11}\rangle\right\}\Bigg]$$

$$= \frac{1}{\sqrt{2}}\left(|+\rangle|\varepsilon_{++} + |-\rangle|\varepsilon_{+-}\right) \tag{5}$$

$$U_E|-\rangle|\varepsilon\rangle = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle - \gamma|0\rangle|\varepsilon_{10}\rangle - \delta|1\rangle|\varepsilon_{11}\rangle\right)$$

$$= \frac{1}{\sqrt{2}}\Bigg[|+\rangle\{\frac{1}{\sqrt{2}}\left(\alpha|0\rangle|\varepsilon_{00}\rangle + \beta|1\rangle|\varepsilon_{01}\rangle - \gamma|0\rangle|\varepsilon_{10}\rangle - \delta|1\rangle|\varepsilon_{11}\rangle\right\} + |-\rangle\{\frac{1}{\sqrt{2}}\left(\alpha|0\rangle|\varepsilon_{00}\rangle - \beta|1\rangle|\varepsilon_{01}\rangle + \gamma|0\rangle|\varepsilon_{10}\rangle + \delta|1\rangle|\varepsilon_{11}\rangle\right\}\Bigg]$$

$$= \frac{1}{\sqrt{2}}\left(|+\rangle|\varepsilon_{-+} + |-\rangle|\varepsilon_{--}\right) \tag{6}$$

Eve's action must lead to an error rate $\hat{\mathrm{A}}\frac{1}{2}$ as far as she attacks the traveling sequence. Furthermore, even though Alice and Bob didn't identify eavesdropping during the testing procedure, Eve can't acquire any valuable data from her auxiliary photon owing to non-orthogonality between the states $\{|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle, |\varepsilon_{++}\rangle, |\varepsilon_{+}\rangle, |\varepsilon_{+}\rangle, |\varepsilon_{++}\rangle\}$. As a result, this form of attack is clearly detectable.

Controlled not attack : During this attack, Eve needs to prepare a two-qubit auxiliary state $|00\rangle_5 6$ to replicate the communicated qubit by utilizing the CNOT gate where the first and third qubits are control bits (if MB_1 basis sets are chosen) and the auxiliary qubits are target bits. Then the cluster state becomes

$$|\phi_0\rangle = |\phi\rangle \otimes |C\rangle$$

$$= \frac{1}{2}\left(|0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle\right) \otimes |00\rangle$$

$$= \frac{1}{2}\left(|0000\rangle|00\rangle + |0011|01\rangle + |1100\rangle|10\rangle - |1111\rangle|11\rangle_{123456}\right) \tag{7}$$

As per the equation (7) mentioned above, Eve and Bob are now in the same position. Due to the usage of two non-orthogonal measuring basis sets and 16x16 different combinations of unitary operations, Eve may still be unable to retrieve the encoded message. While using different basis sets, it is tough to decide for Eve on which particle CNOT operation has to be applied. She is unable to correlate the outcome, even after the final classical proclamation. Despite this, due to the checking particles, Eve was unable to obtain entire knowledge about the cluster state in this sort of assault. *Trojan Horse attack :*Assume an adversary has inserted a Trojan horse [5] in Alice or Bob's apparatus beforehand, the entangled states affected by the Trojan horse are stated as

$$|\phi\rangle = \frac{1}{2}\Bigg(|0^{||}0^{||}0^{||}0^{||}\rangle + |0^{||}0^{||}1^{\perp}1^{\perp}\rangle + |1^{\perp}1^{\perp}0^{||}0^{||}\rangle - |1^{\perp}1^{\perp}1^{\perp}1^{\perp}\rangle \tag{8}$$

$$|\Psi\rangle = \frac{1}{2}\Big(|0^{||}+?0^{||}+?\rangle + |0^{||}+?1^{\perp}-?\rangle + \\ |1^{\perp}-?0^{||}+?\rangle - |1^{\perp}-?1^{\perp}-?\rangle \quad (9)$$

The equations (8) and (9) show that if the qubits are in quantum states $|0\rangle or|1\rangle$, then the Trojan horse feedbacks data $||$ or $\perp$, respectively. However, there is no specified feedback information, if the qubits are in quantum states $|+\rangle or|-\rangle$, which is indicated by the symbol '?'. To put it another way, a Trojan horse is unable to discriminate between non-orthogonal states, as quantum mechanics suggests. Therefore, in practice, this offensive technique is ineffective.

6 Efficiency

A quantitative evaluation of a secure quantum communication scheme's efficiency [4] is defined as

$$\eta = \frac{m}{q+b}$$

where *m* stands for the number of secret bits communicated, and q and b stand for the number of qubits and classical bits used, respectively. The quantum and classical bits required for eavesdropping monitoring are not used in this circumstance. The number of secret bits received is 8, implying that m=8, the number of qubits consumed is 8, and the number of classical bits used is 5, i.e., b = 4+1=5. The quantum efficacy of the suggested protocol is thus 61.53 percent. The comparative assessment (shown in Table 1) reveals that the proposed methodology is significantly more efficient than existing methods.

Table 1: Efficiency comparison of different protocols

$Protocols$	$Qubits$ $transmitted$	$Efficiency$ $(in\%)$
Mohapatra et.al.[19]	4 bits	33.33
Li et.al.[12]	4 bits	25
Zhang et.al.[26]	2 bits	33.33
Liu et.al.[14]	2 bits	50
Shi et.al.[22]	4 bits	66.7
Our protocol	8 bits	61.53

7 Conclusion

From the above study, it is analyzed that our current protocol is reliable in perfect lossless channels. However, in an actual world, the channels are chaotic and lossy, posing a threat to quantum communication security. An eavesdropper attack activity on a poor noisy channel will raise either the error rate or the loss of signal; hence a more significant error rate or the degradation of signal could imply an eavesdropping occurrence. Eve's any viable assault can be identified even in a high-noisy channel because the entangled state is arbitrarily in one of the two non-orthogonal basis sets.

The applicability of the suggested protocol is comparable to that of other similar protocols [8, 17, 15, 16, 13, 20, 22, 23, 27]. Furthermore, since it involves two non-orthogonal entangled states to respond as quantum channels, it can more efficaciously deflect all types of legitimate intercept resent and entangle-measure assaults, that is one of its advantages. Additionally, Alice just requires to conduct a local measurement on the two photons in our technique, rather than a Bell measurement. As a result, our proposed approach is more straight forward to put into action.

Some of the scheme's primary highlights are as follows: (i) We use the concept of dense coding to encapsulate our data using local unitary operations while retaining cluster state entanglement. (ii) This method is more effective (iii) There are no issues with data leakage in our scheme. (iv) Our approach has a large channel capacity as we only need two qubits to send four bits of classical data. (v) Our method is robust to various known assaults. (vi) The secure realization of the quantum dialogue is contingent on the quantum channel's security, which is accomplished through two security checks. In addition, two individuals can authenticate each other's identities.

In summary, the current approach enables quantum dialogue by utilizing two non-orthogonal four qubit cluster states as an entangled resource, allowing two authorized users to share four-bit secret messages while encoding with only two qubits at the same time. This method employs the concept of superdense coding with capacity inside the Holevo limit. It has high security as it employs a two-step security audit, an authentication process, and accounts for numerous eavesdropping attacks without revealing any data. This technique is more efficient than previous efforts. We predict that our approach would be suitable for developing multiparticle QD protocols, which would be a captivating future research issue since entanglement between four-qubit cluster states has been realized experimentally.

References

[1] Bennett, C. H. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.

[2] Bennett, C. H. and Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, 560:7–11, 2014.

[3] Briegel, H. J. and Raussendorf, R. Persistent entanglement in arrays of interacting particles. *Physical Review Letters*, 86(5):910, 2001.

[4] Cabello Quintero, A. Quantum key distribution in the holevo limit. *Physical Review Letters, 85 (26), 5635-5638.*, 2000.

[5] Cai, Q.-Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Physics Letters A*, 351(1-2):23–25, 2006.

[6] Chauhan, S. and Gupta, N. Quantum dialogue protocol using six qubit cluster states with optimal superdense coding. *International Journal on Information Technologies & Security*, 13(4), 2021.

[7] Chauhan, S. and Gupta, N. Bidirectional quantum secure direct communication using dense coding of four qubit cluster states. *Journal of Scientific Research*, 14(1), 2022.

[8] Gao, F., Guo, F., Wen, Q., and Zhu, F. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Science in China Series G: Physics, Mechanics and Astronomy*, 51(5):559–566, 2008.

[9] Gao, G. Bidirectional quantum secure communication based on one-dimensional four-particle cluster states. *International Journal of Theoretical Physics*, 53:2282–2287, 2014.

[10] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[11] Huang, Z. and Situ, H. Protection of quantum dialogue affected by quantum field. *Quantum Information Processing*, 18:1–16, 2019.

[12] Li, W., Zha, X.-W., and Yu, Y. Secure quantum dialogue protocol based on four-qubit cluster state. *International Journal of Theoretical Physics*, 57:371–380, 2018.

[13] Liu, Z. and Chen, H. Cryptanalysis and improvement of the robust quantum dialogue protocols based on the entanglement swapping between any two logical bell states and the shared auxiliary logical bell state. *Modern Physics Letters A*, 34(29):1950241, 2019.

[14] Liu, Z. and Chen, H. Analyzing and improving the secure quantum dialogue protocol based on four-qubit cluster state. *International Journal of Theoretical Physics*, 59:2120–2126, 2020.

[15] Liu, Z., Chen, H., Liu, W., Xu, J., Wang, D., and Li, Z. Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states. *Quantum information processing*, 12:587–599, 2013.

[16] Liu, Z.-H. and Chen, H.-W. Analysis and improvement of large payload bidirectional quantum secure direct communication without information leakage. *International Journal of Theoretical Physics*, 57:311–321, 2018.

[17] Lo, H.-K. and Ko, T.-M. Some attacks on quantum-based cryptographic protocols. *arXiv preprint quant-ph/0309127*, 2003.

[18] Long, G.-L. and Liu, X.-S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Physical Review A*, 65(3):032302, 2002.

[19] Mohapatra, A. K. and Balakrishnan, S. Controller-independent bidirectional quantum direct communication. *Quantum Information Processing*, 16:1–11, 2017.

[20] Nguyen, B. A. Quantum dialogue. *Physics Letters A*, 328(1):6–10, 2004.

[21] Nielsen, M. A. and Chuang, I. L. *Quantum computation and quantum information.* Cambridge university press, 2010.

[22] Okey, O. D., Maidin, S. S., Lopes Rosa, R., Toor, W. T., Carrillo Melgarejo, D., Wuttisittikulkij, L., Saadi, M., and Zegarra RodrÃguez, D. Quantum key distribution protocol selector based on machine learning for next-generation networks. *Sustainability*, 14(23), 2022.

[23] Shi, G.-F., Xi, X.-Q., Tian, X.-L., and Yue, R.-H. Bidirectional quantum secure communication based on a shared private bell state. *Optics communications*, 282(12):2460–2463, 2009.

[24] Tan, Y.-g. and Cai, Q.-Y. Classical correlation in quantum dialogue. *International Journal of Quantum Information*, 6(02):325–329, 2008.

[25] Wang, H., Zhang, Y., Wu, G., and Ma, H. Authenticated quantum dialogue without information leakage. *Chinese Journal of Electronics*, 27(2):270–275, 2018.

[26] Yi, X.-j., Nie, Y.-Y., Zhou, N.-r., Huang, Y.-b., and Hong, Z.-h. Secure direct communication based on non-orthogonal entangled pairs and local measurement. *International Journal of Theoretical Physics*, 47:3401–3407, 2008.

[27] Zhang, L., Dong, S., Zhang, K.-J., and Sun, H.-W. A controller-independent quantum dialogue protocol with four-particle states. *International Journal of Theoretical Physics*, 58:1927–1936, 2019.

[28] Zhang, Z.-J. and Man, Z.-X. Secure direct bidirectional communication protocol using the einstein-podolsky-rosen pair block. *arXiv preprint quant-ph/0403215*, 2004.