QUANTUM DIALOGUE PROTOCOL USING SIX QUBIT CLUSTER STATES WITH OPTIMAL SUPERDENSE CODING

S. Chauhan, N. L. Gupta*

[1] Science & Humanities Dept., Government Polytechnic College Ajmer, Rajasthan,
[2] Department of Physics, Government College Dungarpur, Rajasthan
India

* Corresponding Author, e-mail: humsihachauhan@gmail.com

Abstract: By utilizing the attributes of a cluster state, a quantum dialogue protocol using a six qubit cluster state is put forward, which employs the idea of superdense coding to achieve maximal efficiency and high resource capacity. In our protocol, two users can simultaneously exchange five qubits of secret messages by using only three qubits for encoding. This protocol's superdense coding capacity is Holevo constrained and can be achieved with the current approaches. It guarantees a high level of security because it considers specific eavesdropping attacks while avoiding data leaking. The new scheme outperforms the existing one in terms of efficiency.

Key words: Quantum dialogue, Six qubit cluster state, information leakage, superdense coding.

1. INTRODUCTION

With the expanding computational power of traditional computers and the ongoing research into quantum computers, the confidentiality of classical cryptography will confront a growing risk. Quantum cryptography integrating classical cryptography with quantum information systems has the potential to provide unconditional security, as ensured by the Heisenberg uncertainty principle and the quantum non-cloning theorem, allowing quantum cryptography to perform better and have more applications. Quantum dialogue (QD) is one of the most characteristic applications of quantum cryptography. QD refers to two-way quantum communication, also known as bidirectional communication, in which two lawful communication partners can send secret information through a quantum channel simultaneously. Since Nguyen [6] proposed the first QD procedure, it has received great attention. The use of QD will significantly increase the efficiency, secrecy, and security of communication. Entanglement plays an essential role in removing

information leakage problems in many QD protocols using multipartite entangled states.

In recent years, cluster states, a subset of entangled states, have attracted much attention because of their potential applicability in quantum information theory. Using proper reversible quantum gates in diverse systems, these states have also been experimentally achieved. For N>4 under Local Operation and Classical Communication (LOCC), it has distinct entanglement features than GHZ states. They also exhibit a significant violation of local reality and are resistant to decoherence. All these make cluster states helpful resources for QD.

Here, we present a QD protocol in which two authorized users can simultaneously share a secret five-bit message via a quantum channel comprising six qubit cluster states. This scheme incorporates the concept of optimal quantum superdense coding, which means one can encode two bits of information on a single quantum bit without disturbing the entanglement. Our scheme is distinguished by the following features: (i) We recommend a QD protocol scheme that employs reusable six-qubit cluster states with dense coding via local unitary operation while preserving the shared channel's entanglement. (ii) Our approach is more efficient, with an efficiency of 83.33%. (iii) In addition, our scheme does not have the problem of information leaking. (iv) Further, in order to convey 5N bits of classical information, we utilize 3N qubits of six qubit cluster states. Thus, our protocol complies with the Holevo constraint and has the highest capacity. (v) As a result of two security checks and authentication methods, our system is more secure.

The rest of the paper is organized as follows: section 2 presents the prior work related to this paper, section 3 describes the Quantum dialogue protocol, and then the protocol's security against various attacks and information leakage analysis in section 4. The efficiency has been discussed in section 5. Finally, the paper is concluded in section 6.

2. RELATED WORK AND BACKGROUND

Quantum communication offers a revolutionary method of communication that is guaranteed to be secure. Quantum communication methods involve quantum key distribution (QKD) [1], quantum secure direct communication (QSDC) [2-3], quantum teleportation, quantum dense coding [4-5], and so on. QKD allows a key to be securely transferred across a long distance between two parties. However, without establishing a key in advance, quantum secure direct communication (QSDC) can send secret messages to one another in a predictable and secure manner. The significant disadvantage of QSDC protocols is that one can send messages only in one direction. Keeping this in mind, Nguyen [6] offered the first entanglement based Quantum dialogue (QD) protocol, which makes use of Bell states. Quantum dialogue is a two way quantum secure communication, also called bidirectional quantum secure direct communication (BQSDC), in which users can simultaneously communicate with each other. More significant QD procedures have been introduced

since then [7-8]. Though, in 2008, Gao et al. and Tan et al. [9, 10] separately identified a security flaw in several QD protocols known as information leaking or classical correlation. Consequently, an eavesdropper may obtain certain information regarding secret communications from the classical communication between the legal users without any active attack. To address this flaw, Shi et al. suggested a shared private quantum entanglement channel to enhance bidirectional quantum secure communication. More QD techniques [11-13] have now been proposed to overcome this problem. Subsequently, in 2019, Huang et.al. [14] put forward a QD protocol based on three-qubit GHZ states, but 50 percent of the secret message exchanged is accidentally leaked out in this approach. It was cryptanalysed by Zhi et al. [15] and improved by encoding the one-bit secret message with one of the two unitary operations. Furthermore, information leakage can be prevented by incorporating multiparticle entangled states (especially cluster states) in many QD protocols [16-20]. Cluster states [21-23], a type of entangled state with surprising and special features, play a significant role in the problem of information leakage and is given by,

$$|C\rangle = \frac{1}{2^{\frac{N}{2}}} \otimes_{a=1}^{N} \left(|0\rangle_a \sigma_z^{a+1} + |1\rangle_a \right)$$

In the actual world, quantum systems are unavoidably coupled with their surroundings, which can lead to a loss in quantum correlation, resulting in so-called decoherence. These states are invulnerable to decoherence. Most of the protocols outlined above have assumed that the two communicators are authentic. But unfortunately, a counterfeit may take the secret message or send a false message to legitimate users. As a result, verifying users' identities is also indispensable. From above discussion, it is analyzed that the study on efficient QD protocols avoiding information leakage has essential theoretical and practical implications, which prompted us to propose this scheme.

3. DESCRIPTION OF OUR PROTOCOL

To achieve the purpose of QD protocol, first, we define a six qubit cluster state as following

$$|C\rangle = |000000\rangle + |000111\rangle + |111000\rangle - |111111\rangle$$

The two legal users can utilize unitary operations on the first, fourth, and sixth qubits to encode their message as $U_1 \otimes I \otimes I \otimes U_2 \otimes I \otimes U_3 \rightarrow |C\rangle$, where, $U_1, U_2 \epsilon \left(I, \sigma_x, \sigma_y, \sigma_z \right) \epsilon [00, 01, 10, 11]$ and $U_3 \epsilon \left(I, \sigma_x \right) \epsilon [0,1]$ respectively. The four Pauli operators that are used to encode secret messages are defined as

$$\begin{aligned} I &= |0\rangle\langle 0| + |1\rangle\langle 1| \\ \sigma_x &= |0\rangle\langle 1| + |1\rangle\langle 0| \\ \sigma_y &= |0\rangle\langle 1| - |1\rangle\langle 0| \\ \sigma_z &= |0\rangle\langle 0| - |1\rangle\langle 1| \end{aligned}$$

The other states (as shown in Table 1) can be obtained by utilizing the above-mentioned local operations. Using Von Neuman measurement, all of the states obtained are used as measuring bases.

Table 1 Dense coding of $|\boldsymbol{C}\rangle_{\boldsymbol{abcdef}}$

$$|\boldsymbol{C_1}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{000000}\rangle + |\boldsymbol{000111}\rangle + |\boldsymbol{111000}\rangle - |\boldsymbol{111111}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_2}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{000001}\rangle + |\boldsymbol{000110}\rangle + |\boldsymbol{111001}\rangle - |\boldsymbol{111110}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_3}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{000100}\rangle + |\boldsymbol{000011}\rangle + |\boldsymbol{111100}\rangle - |\boldsymbol{111011}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_4}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{000101}\rangle + |\boldsymbol{000010}\rangle + |\boldsymbol{111101}\rangle - |\boldsymbol{111010}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_5}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(-|\boldsymbol{000100}\rangle + |\boldsymbol{000011}\rangle - |\boldsymbol{111100}\rangle - |\boldsymbol{111011}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_6}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(-|\boldsymbol{000101}\rangle + |\boldsymbol{000010}\rangle - |\boldsymbol{111101}\rangle - |\boldsymbol{111010}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_7}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{000000}\rangle - |\boldsymbol{000111}\rangle + |\boldsymbol{111000}\rangle + |\boldsymbol{111111}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_8}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{000001}\rangle - |\boldsymbol{000110}\rangle + |\boldsymbol{111001}\rangle + |\boldsymbol{111110}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_9}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{100000}\rangle + |\boldsymbol{100111}\rangle + |\boldsymbol{011000}\rangle - |\boldsymbol{011111}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{10}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{100001}\rangle + |\boldsymbol{100110}\rangle + |\boldsymbol{011001}\rangle - |\boldsymbol{011110}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{11}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{100100}\rangle + |\boldsymbol{100011}\rangle + |\boldsymbol{011100}\rangle - |\boldsymbol{011011}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{12}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{100101}\rangle + |\boldsymbol{100010}\rangle + |\boldsymbol{011101}\rangle - |\boldsymbol{011010}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{13}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(-|\boldsymbol{100100}\rangle + |\boldsymbol{100011}\rangle - |\boldsymbol{011100}\rangle - |\boldsymbol{011011}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{14}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(-|\boldsymbol{100101}\rangle + |\boldsymbol{100010}\rangle - |\boldsymbol{011101}\rangle - |\boldsymbol{011010}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{15}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{100000}\rangle - |\boldsymbol{100111}\rangle + |\boldsymbol{011000}\rangle + |\boldsymbol{011111}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{16}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{100001}\rangle - |\boldsymbol{100110}\rangle + |\boldsymbol{011001}\rangle + |\boldsymbol{011110}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{17}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(-|\boldsymbol{100000}\rangle - |\boldsymbol{100111}\rangle + |\boldsymbol{011000}\rangle - |\boldsymbol{011111}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{18}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(-|\boldsymbol{100001}\rangle - |\boldsymbol{100110}\rangle + |\boldsymbol{011001}\rangle - |\boldsymbol{011110}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{19}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(-|\boldsymbol{100100}\rangle - |\boldsymbol{100011}\rangle + |\boldsymbol{011100}\rangle - |\boldsymbol{011011}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{20}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(-|\boldsymbol{100101}\rangle - |\boldsymbol{100010}\rangle + |\boldsymbol{011101}\rangle - |\boldsymbol{011010}\rangle)_{\boldsymbol{abcdef}}$$

$$|\boldsymbol{C_{21}}\rangle = \frac{\boldsymbol{1}}{\boldsymbol{2}}(|\boldsymbol{100100}\rangle - |\boldsymbol{100011}\rangle - |\boldsymbol{011100}\rangle - |\boldsymbol{011011}\rangle)_{\boldsymbol{abcdef}}$$

$$|C_{22}\rangle = \frac{1}{2}(|100101\rangle - |100010\rangle - |011101\rangle - |011010\rangle)_{abcdef}$$
$$|C_{23}\rangle = \frac{1}{2}(-|100000\rangle + |100111\rangle + |011000\rangle + |011111\rangle)_{abcdef}$$
$$|C_{24}\rangle = \frac{1}{2}(-|100001\rangle + |100110\rangle + |011001\rangle + |011110\rangle)_{abcdef}$$
$$|C_{25}\rangle = \frac{1}{2}(|000000\rangle + |000111\rangle - |111000\rangle + |111111\rangle)_{abcdef}$$
$$|C_{26}\rangle = \frac{1}{2}(|000001\rangle + |000110\rangle - |111001\rangle + |111110\rangle)_{abcdef}$$
$$|C_{27}\rangle = \frac{1}{2}(|000100\rangle + |000011\rangle - |111100\rangle + |111011\rangle)_{abcdef}$$
$$|C_{28}\rangle = \frac{1}{2}(|000101\rangle + |000010\rangle - |111101\rangle + |111010\rangle)_{abcdef}$$
$$|C_{29}\rangle = \frac{1}{2}(-|000100\rangle + |000011\rangle + |111100\rangle + |111011\rangle)_{abcdef}$$
$$|C_{30}\rangle = \frac{1}{2}(-|000101\rangle + |000010\rangle + |111101\rangle + |111010\rangle)_{abcdef}$$
$$|C_{31}\rangle = \frac{1}{2}(|000000\rangle - |000111\rangle - |111000\rangle - |111111\rangle)_{abcdef}$$
$$|C_{32}\rangle = \frac{1}{2}(|000001\rangle - |000110\rangle - |111001\rangle - |111110\rangle)_{abcdef}$$

QD Protocol

In this protocol, Alice and Bob, two authorized users, can simultaneously communicate five qubit secret messages via six qubit cluster states. The following is the protocol:

Step 1. Alice first prepares two identical sequence 1S and 2S sequence of n cluster states in the state, which is arranged as

$$S = \{S_1^a, S_1^b, S_1^c, S_1^d, S_1^e, S_1^f, S_2^a, S_2^b, S_2^c, S_2^d, S_2^e, S_2^f, \ldots\ldots\ldots S_n^a, S_n^b, S_n^c, S_n^d, S_n^e, S_n^f\}$$

Here, a,b,c,d,e,f represent six particles in a six qubit cluster state, and the subscript 1,2...n indicates the order of cluster state in a sequence. Also, she puts together two batches of decoy photons (say l and m particles) randomly, either in X basis $(|+\rangle, |-\rangle)$ or in Z basis $(|0\rangle, |1\rangle)$ which are used to check the channel's security. By inserting l particles into the 1S sequence, she sends the (n+l) sequence to Bob.

Step 2. On receiving the sequence to Bob, they initially examine the channel's security. Alice reveals the position and correct measuring basis for each l decoy photon. Then Bob measures the particle in the announced basis. By reviewing the outcomes, Bob can figure out what the error rate is. The process is terminated if it exceeds the threshold; else, it continues. Bob discards l particles and measures each

of the four particles in the 1S sequence in order using a cluster basis. Consequently, he retrieves the original state of that cluster state in the 1S sequence.

Step 3. To verify Bob's identification, Alice chooses a sufficient number of particles from the 2S sequence, performs Z basis measurement, and tells the position. Bob chooses the particle in the same place in the 1S sequence, measures the Z basis, and correlates his results to Alice's. If it is the same, then the authentication of the users is verified.

Step 4. Alice performs the unitary operation $U_1 \otimes U_2 \otimes U_3$ on the first, fourth, and sixth particle of each cluster state into a 2S sequence, corresponding to a five-bit classical message. Alice inserts m particles into the 2S sequence for a second security check and sends (n+m) particles to Bob.

Step 5. Bob obtains the 2S sequence. Alice communicates the position as well as their basis of m particles in a 2S sequence. To ensure the security of channel transmission, Bob measures them in the correct basis, correlates it with Alice's announcement, and ensures whether the sequence has eavesdropped. After eliminating m particles. Bob encodes his secret message by executing $U_1 \otimes U_2 \otimes U_3$ operation on the first, fourth, and sixth qubits (on the encoded qubits) in a 2S sequence. After performing the encoding process, Bob executes a cluster state measurement on each of the six particles in the 2S sequence and sends it back to Alice.

Step 6. Bob's result is measured by Alice. According to Table 2, Alice can infer the secret messages based on Alice's operations and Bob's outcome. Bob can also acquire the message (according to Table 2) on the basis of measurement results received from Alice and the known initial cluster states.

For instance, suppose Alice prepared $|C_1\rangle_{abcdef}$ as the initial state of the cluster state, and Alice and Bob wish to transmit a secret message 00101 and 10111 to each other. In that case, their encoding operation will be $\mathrm{I} \otimes \sigma_y \otimes \sigma_x$ and $\sigma_y \otimes \sigma_z \otimes \sigma_x$ respectively and will get the final result $|C_{19}\rangle$ (as per Table 2), which can be shown as.

$$Msg_A(00101) = |C_1\rangle, \sigma_y \otimes \sigma_z \otimes \sigma_x, |C_{19}\rangle \Longrightarrow \text{Bob}$$
$$Msg_B(10111) = |C_1\rangle, \ \mathrm{I} \otimes \sigma_y \otimes \sigma_x, |C_{19}\rangle \Longrightarrow \text{Alice}$$

Then according to above mentioned three known messages, she is able to figure out Bob's secret operation is $\sigma_y \otimes \sigma_z \otimes \sigma_x$. As 1S and 2S sequences are equal, so Bob already knows the initial cluster state. Bob can deduce Alice's secret operation is $\mathrm{I} \otimes \sigma_y \otimes \sigma_x$. Consequently, both the users can transmit the secret message simultaneously.

Table 2. The possible outcomes of measurement results and corresponding dense coding operation

Classical bit	*Encoding operation*	$\|C_1\rangle$	$\|C_2\rangle$	$\|C_3\rangle$	$\|C_4\rangle$	$\|C_5\rangle$	$\|C_6\rangle$	$\|C_7\rangle$	$\|C_8\rangle$	$\|C_9\rangle$	$\|C_{10}\rangle$	$\|C_{11}\rangle$
00000	$I\otimes I\otimes I$	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
00001	$I\otimes I\otimes\sigma_x$	C_2	C_1	C_4	C_3	C_6	C_5	C_8	C_7	C_{10}	C_9	C_{12}
00010	$I\otimes\sigma_x\otimes I$	C_3	C_4	C_1	C_2	$-C_7$	$-C_8$	$-C_5$	$-C_6$	C_{11}	C_{12}	C_9
00011	$I\otimes\sigma_x\otimes\sigma_x$	C_4	C_3	C_2	C_1	$-C_8$	$-C_7$	$-C_6$	$-C_5$	C_{12}	C_{11}	C_{10}
00100	$I\otimes\sigma_y\otimes I$	C_5	C_6	C_7	C_8	$-C_1$	$-C_2$	$-C_3$	$-C_4$	C_{13}	C_{14}	C_{15}
00101	$I\otimes\sigma_y\otimes\sigma_x$	C_6	C_5	C_8	C_7	$-C_2$	$-C_1$	C_4	$-C_3$	C_{14}	C_{13}	C_{16}
00110	$I\otimes\sigma_z\otimes I$	C_7	C_8	C_5	C_6	C_3	C_4	C_1	C_2	C_{15}	C_{16}	C_{13}
00111	$I\otimes\sigma_z\otimes\sigma_x$	C_8	C_7	C_6	C_5	C_4	C_3	C_2	C_1	C_{16}	C_{15}	C_{14}
01000	$\sigma_x\otimes I\otimes I$	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_1	C_2	C_3
01001	$\sigma_x\otimes I\otimes\sigma_x$	C_{10}	C_9	C_{12}	C_{11}	C_{14}	C_{13}	C_{16}	C_{15}	C_2	C_1	C_4
01010	$\sigma_x\otimes\sigma_x\otimes I$	C_{11}	C_{12}	C_9	C_{10}	$-C_{15}$	$-C_{16}$	$-C_{1}$	$-C_{14}$	C_3	C_4	C_1
01011	$\sigma_x\otimes\sigma_x\otimes\sigma_x$	C_{12}	C_{11}	C_{10}	C_9	$-C_{16}$	$-C_{15}$	$-C_{1}$	$-C_{13}$	C_4	C_3	C_2
01100	$\sigma_x\otimes\sigma_y\otimes I$	C_{13}	C_{14}	C_{15}	C_{16}	$-C_9$	$-C_{10}$	$-C_{1}$	$-C_{12}$	C_5	C_6	C_7
01101	$\sigma_x\otimes\sigma_y\otimes\sigma_x$	C_{14}	C_{13}	C_{16}	C_{15}	$-C_{10}$	$-C_9$	$-C_{1}$	$-C_{11}$	C_6	C_5	C_8
01110	$\sigma_x\otimes\sigma_z\otimes I$	C_{15}	C_{16}	C_{13}	C_{14}	C_{11}	C_{12}	C_9	C_{10}	C_7	C_8	C_5
01111	$\sigma_x\otimes\sigma_z\otimes\sigma_x$	C_{16}	C_{15}	C_{14}	C_{13}	C_{12}	C_{11}	C_{10}	C_9	C_8	C_7	C_6
10000	$\sigma_y\otimes I\otimes I$	C_{17}	C_{18}	C_{19}	C_{20}	C_{21}	C_{22}	C_{23}	C_{24}	C_{25}	C_{26}	C_{27}
10001	$\sigma_y\otimes I\otimes\sigma_x$	C_{18}	C_{17}	C_{20}	C_{19}	C_{22}	C_{21}	C_{24}	C_{23}	C_{26}	C_{25}	C_{28}
10010	$\sigma_y\otimes\sigma_x\otimes I$	C_{19}	C_{20}	C_{17}	C_{18}	$-C_{23}$	$-C_{24}$	$-C_{2}$	$-C_{22}$	C_{27}	C_{28}	C_{25}
10011	$\sigma_y\otimes\sigma_x\otimes\sigma_x$	C_{20}	C_{19}	C_{18}	C_{17}	$-C_{24}$	$-C_{23}$	$-C_{2}$	$-C_{21}$	C_{28}	C_{27}	C_{26}
10100	$\sigma_y\otimes\sigma_y\otimes I$	C_{21}	C_{22}	C_{23}	C_{24}	$-C_{17}$	$-C_{18}$	$-C_{1}$	$-C_{20}$	C_{29}	C_{30}	C_{31}
10101	$\sigma_y\otimes\sigma_y\otimes\sigma_x$	C_{22}	C_{21}	C_{24}	C_{23}	$-C_{18}$	$-C_{17}$	$-C_{2}$	$-C_{19}$	C_{30}	C_{29}	C_{32}
10110	$\sigma_y\otimes\sigma_z\otimes I$	C_{23}	C_{24}	C_{21}	C_{22}	C_{19}	C_{20}	C_{17}	C_{18}	C_{31}	C_{32}	C_{29}
10111	$\sigma_y\otimes\sigma_z\otimes\sigma_x$	C_{24}	C_{23}	C_{22}	C_{21}	C_{20}	C_{19}	C_{18}	C_{17}	C_{32}	C_{31}	C_{30}
11000	$\sigma_z\otimes I\otimes I$	C_{25}	C_{26}	C_{27}	C_{28}	C_{29}	C_{30}	C_{31}	C_{32}	C_{17}	C_{18}	C_{19}
11001	$\sigma_z\otimes I\otimes\sigma_x$	C_{26}	C_{25}	C_{28}	C_{27}	C_{30}	C_{29}	C_{32}	C_{31}	C_{18}	C_{17}	C_{20}
11010	$\sigma_z\otimes\sigma_x\otimes I$	C_{27}	C_{28}	C_{25}	C_{26}	$-C_{31}$	$-C_{32}$	$-C_{2}$	$-C_{30}$	C_{19}	C_{20}	C_{17}
11011	$\sigma_z\otimes\sigma_x\otimes\sigma_x$	C_{28}	C_{27}	C_{26}	C_{25}	$-C_{32}$	$-C_{31}$	$-C_{3}$	$-C_{29}$	C_{20}	C_{19}	C_{18}
11100	$\sigma_z\otimes\sigma_y\otimes I$	C_{29}	C_{30}	C_{31}	C_{32}	$-C_{25}$	$-C_{26}$	$-C_{2}$	$-C_{28}$	C_{21}	C_{22}	C_{23}
11101	$\sigma_z\otimes\sigma_y\otimes\sigma_x$	C_{30}	C_{29}	C_{32}	C_{31}	$-C_{26}$	$-C_{25}$	$-C_{2}$	$-C_{27}$	C_{22}	C_{21}	C_{24}
11110	$\sigma_z\otimes\sigma_z\otimes I$	C_{31}	C_{32}	C_{29}	C_{30}	C_{27}	C_{28}	C_{25}	C_{26}	C_{23}	C_{24}	C_{21}
11111	$\sigma_z\otimes\sigma_z\otimes\sigma_x$	C_{32}	C_{31}	C_{30}	C_{29}	C_{28}	C_{27}	C_{26}	C_{25}	C_{24}	C_{23}	C_{22}

Table 2. Continued.

Classical bit	*Encoding operation*	$\|C_{12}\rangle$	$\|C_{13}\rangle$	$\|C_{14}\rangle$	$\|C_{15}\rangle$	$\|C_{16}\rangle$	$\|C_{17}\rangle$	$\|C_{18}\rangle$	$\|C_{19}\rangle$	$\|C_{20}\rangle$	$\|C_{21}\rangle$	$\|C_{22}\rangle$
00000	$I\otimes I\otimes I$	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	C_{17}	C_{18}	C_{19}	C_{20}	C_{21}	C_{22}
00001	$I\otimes I\otimes\sigma_x$	C_{11}	C_{14}	C_{13}	C_{16}	C_{15}	C_{18}	C_{17}	C_{20}	C_{19}	C_{22}	C_{21}
00010	$I\otimes\sigma_x\otimes I$	C_{10}	$-C_{15}$	$-C_{16}$	$-C_{13}$	$-C_{14}$	C_{19}	C_{20}	C_{17}	C_{18}	$-C_{23}$	$-C_{2}$
00011	$I\otimes\sigma_x\otimes\sigma_x$	C_9	$-C_{16}$	$-C_{15}$	$-C_{14}$	$-C_{13}$	C_{20}	C_{19}	C_{18}	C_{17}	$-C_{24}$	$-C_{2}$
00100	$I\otimes\sigma_y\otimes I$	C_{16}	$-C_9$	$-C_{10}$	$-C_{11}$	$-C_{12}$	C_{21}	C_{22}	C_{23}	C_{24}	$-C_{17}$	$-C_{1}$
00101	$I\otimes\sigma_y\otimes\sigma_x$	C_{15}	$-C_{10}$	$-C_9$	$-C_{12}$	$-C_{11}$	C_{22}	C_{21}	C_{24}	C_{23}	$-C_{18}$	$-C_{1}$
00110	$I\otimes\sigma_z\otimes I$	C_{14}	C_{11}	C_{12}	C_9	C_{10}	C_{23}	C_{24}	C_{21}	C_{22}	C_{19}	C_{20}
00111	$I\otimes\sigma_z\otimes\sigma_x$	C_{13}	C_{12}	C_{11}	C_{10}	C_9	C_{24}	C_{23}	C_{22}	C_{21}	C_{20}	C_{19}
01000	$\sigma_x\otimes I\otimes I$	C_4	C_5	C_6	C_7	C_8	$-C_{25}$	$-C_{26}$	$-C_{27}$	$-C_{28}$	$-C_{29}$	$-C_{3}$
01001	$\sigma_x\otimes I\otimes\sigma_x$	C_3	C_6	C_5	C_8	C_7	$-C_{26}$	$-C_{25}$	$-C_{28}$	$-C_{27}$	$-C_{30}$	$-C_{2}$
01010	$\sigma_x\otimes\sigma_x\otimes I$	C_2	$-C_7$	$-C_8$	$-C_5$	$-C_6$	$-C_{27}$	$-C_{28}$	$-C_{25}$	$-C_{26}$	C_{31}	C_{32}
01011	$\sigma_x\otimes\sigma_x\otimes\sigma_x$	C_1	$-C_8$	$-C_7$	$-C_6$	$-C_5$	$-C_{28}$	$-C_{27}$	$-C_{26}$	$-C_{25}$	C_{32}	C_{31}
01100	$\sigma_x\otimes\sigma_y\otimes I$	C_8	$-C_1$	$-C_2$	$-C_3$	$-C_4$	$-C_{29}$	$-C_{30}$	$-C_{31}$	$-C_{32}$	C_{25}	C_{26}
01101	$\sigma_x\otimes\sigma_y\otimes\sigma_x$	C_7	$-C_2$	$-C_1$	$-C_4$	$-C_3$	$-C_{30}$	$-C_{29}$	$-C_{32}$	$-C_{31}$	C_{26}	C_{25}
01110	$\sigma_x\otimes\sigma_z\otimes I$	C_6	C_3	C_4	C_1	C_2	$-C_{31}$	$-C_{32}$	$-C_{29}$	$-C_{30}$	$-C_{27}$	$-C_{2}$
01111	$\sigma_x\otimes\sigma_z\otimes\sigma_x$	C_5	C_4	C_3	C_2	C_1	$-C_{32}$	$-C_{31}$	$-C_{30}$	$-C_{29}$	$-C_{28}$	$-C_{2}$
10000	$\sigma_y\otimes I\otimes I$	C_{28}	C_{29}	C_{30}	C_{31}	C_{32}	$-C_1$	$-C_2$	$-C_3$	$-C_4$	$-C_5$	$-C_6$
10001	$\sigma_y\otimes I\otimes\sigma_x$	C_{27}	C_{30}	C_{29}	C_{32}	C_{31}	$-C_2$	$-C_1$	$-C_4$	$-C_3$	$-C_6$	$-C_5$
10010	$\sigma_y\otimes\sigma_x\otimes I$	C_{26}	C_{31}	C_{32}	$-C_{29}$	$-C_{30}$	$-C_3$	$-C_4$	$-C_1$	$-C_2$	C_7	C_8
10011	$\sigma_y\otimes\sigma_x\otimes\sigma_x$	C_{25}	C_{32}	C_{31}	$-C_{30}$	$-C_{29}$	$-C_4$	$-C_3$	$-C_2$	$-C_1$	C_8	C_7
10100	$\sigma_y\otimes\sigma_y\otimes I$	C_{32}	$-C_{25}$	$-C_{26}$	$-C_{27}$	$-C_{28}$	$-C_5$	$-C_6$	$-C_7$	$-C_8$	C_1	C_2
10101	$\sigma_y\otimes\sigma_y\otimes\sigma_x$	C_{31}	$-C_{26}$	$-C_{25}$	$-C_{28}$	$-C_{27}$	$-C_6$	$-C_5$	$-C_8$	$-C_7$	C_2	C_1
10110	$\sigma_y\otimes\sigma_z\otimes I$	C_{30}	C_{27}	C_{28}	C_{25}	C_{26}	$-C_7$	$-C_8$	$-C_5$	$-C_6$	$-C_3$	$-C_4$
10111	$\sigma_y\otimes\sigma_z\otimes\sigma_x$	C_{29}	C_{28}	C_{27}	C_{26}	C_{25}	$-C_8$	$-C_7$	$-C_6$	$-C_5$	$-C_4$	$-C_3$
11000	$\sigma_z\otimes I\otimes I$	C_{20}	C_{21}	C_{22}	C_{23}	C_{24}	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}
11001	$\sigma_z\otimes I\otimes\sigma_x$	C_{19}	C_{22}	C_{21}	C_{24}	C_{23}	C_{10}	C_9	C_{12}	C_{11}	C_{14}	C_{13}
11010	$\sigma_z\otimes\sigma_x\otimes I$	C_{18}	$-C_{23}$	$-C_{24}$	$-C_{21}$	$-C_{22}$	C_{11}	C_{12}	C_9	C_{10}	$-C_{15}$	$-C_{16}$
11011	$\sigma_z\otimes\sigma_x\otimes\sigma_x$	C_{17}	$-C_{24}$	$-C_{23}$	$-C_{22}$	$-C_{21}$	C_{12}	C_{11}	C_{10}	C_9	$-C_{16}$	$-C_{15}$
11100	$\sigma_z\otimes\sigma_y\otimes I$	C_{24}	$-C_{17}$	$-C_{18}$	C_{19}	C_{20}	C_{13}	C_{14}	C_{15}	C_{16}	$-C_9$	$-C_{10}$
11101	$\sigma_z\otimes\sigma_y\otimes\sigma_x$	C_{23}	$-C_{18}$	$-C_{17}$	C_{20}	C_{19}	C_{14}	C_{13}	C_{16}	C_{15}	$-C_{10}$	$-C_9$
11110	$\sigma_z\otimes\sigma_z\otimes I$	C_{22}	C_{19}	C_{20}	C_{17}	C_{18}	C_{15}	C_{16}	C_{13}	C_{14}	C_{11}	C_{12}
11111	$\sigma_z\otimes\sigma_z\otimes\sigma_x$	C_{21}	C_{20}	C_{19}	C_{18}	C_{17}	C_{16}	C_{15}	C_{14}	C_{13}	C_{12}	C_{11}

Table 2. Continued.

Classical bit	*Encoding operation*	$\|C_{23}\rangle$	$\|C_{24}\rangle$	$\|C_{25}\rangle$	$\|C_{26}\rangle$	$\|C_{27}\rangle$	$\|C_{28}\rangle$	$\|C_{29}\rangle$	$\|C_{30}\rangle$	$\|C_{31}\rangle$	$\|C_{32}\rangle$
00000	$I\otimes I\otimes I$	C_{23}	C_{24}	C_{25}	C_{26}	C_{27}	C_{28}	C_{29}	C_{30}	C_{31}	C_{32}
00001	$I\otimes I\otimes\sigma_x$	C_{24}	C_{23}	C_{26}	C_{25}	C_{28}	C_{27}	C_{30}	C_{29}	C_{32}	C_{31}
00010	$I\otimes\sigma_x\otimes I$	$-C_{21}$	$-C_{22}$	C_{27}	C_{28}	C_{25}	C_{26}	$-C_{31}$	$-C_{32}$	$-C_{29}$	$-C_{30}$
00011	$I\otimes\sigma_x\otimes\sigma_x$	$-C_{22}$	$-C_{21}$	C_{28}	C_{27}	C_{26}	C_{25}	$-C_{32}$	$-C_{31}$	$-C_{30}$	$-C_{29}$
00100	$I\otimes\sigma_y\otimes I$	$-C_{19}$	$-C_{20}$	C_{29}	C_{30}	C_{31}	C_{32}	$-C_{25}$	$-C_{26}$	$-C_{27}$	$-C_{28}$
00101	$I\otimes\sigma_y\otimes\sigma_x$	$-C_{20}$	$-C_{19}$	C_{30}	C_{29}	C_{32}	C_{31}	$-C_{26}$	$-C_{25}$	$-C_{28}$	$-C_{27}$
00110	$I\otimes\sigma_z\otimes I$	C_{17}	C_{18}	C_{31}	C_{32}	C_{29}	C_{30}	C_{27}	C_{28}	C_{25}	C_{26}
00111	$I\otimes\sigma_z\otimes\sigma_x$	C_{18}	C_{17}	C_{32}	C_{31}	C_{30}	C_{29}	C_{28}	C_{27}	C_{26}	C_{25}
01000	$\sigma_x\otimes I\otimes I$	$-C_{31}$	$-C_{32}$	$-C_{17}$	$-C_{18}$	$-C_{19}$	$-C_{20}$	$-C_{21}$	$-C_{22}$	$-C_{23}$	$-C_{24}$
01001	$\sigma_x\otimes I\otimes\sigma_x$	$-C_{32}$	$-C_{31}$	$-C_{18}$	$-C_{17}$	$-C_{20}$	$-C_{19}$	$-C_{22}$	$-C_{21}$	$-C_{24}$	$-C_{23}$
01010	$\sigma_x\otimes\sigma_x\otimes I$	C_{29}	C_{30}	$-C_{19}$	$-C_{20}$	$-C_{17}$	$-C_{18}$	C_{23}	C_{24}	C_{21}	C_{22}
01011	$\sigma_x\otimes\sigma_x\otimes\sigma_x$	C_{30}	C_{29}	$-C_{20}$	$-C_{19}$	$-C_{18}$	$-C_{17}$	C_{24}	C_{23}	C_{22}	C_{21}
01100	$\sigma_x\otimes\sigma_y\otimes I$	C_{27}	C_{28}	$-C_{21}$	$-C_{22}$	$-C_{23}$	$-C_{24}$	C_{17}	C_{18}	C_{19}	C_{20}
01101	$\sigma_x\otimes\sigma_y\otimes\sigma_x$	C_{28}	C_{27}	$-C_{22}$	$-C_{21}$	$-C_{24}$	$-C_{23}$	C_{18}	C_{17}	C_{20}	C_{19}
01110	$\sigma_x\otimes\sigma_z\otimes I$	$-C_{25}$	$-C_{26}$	$-C_{23}$	$-C_{24}$	$-C_{21}$	$-C_{22}$	$-C_{19}$	$-C_{20}$	$-C_{17}$	$-C_{18}$
01111	$\sigma_x\otimes\sigma_z\otimes\sigma_x$	$-C_{26}$	$-C_{25}$	$-C_{24}$	$-C_{23}$	$-C_{22}$	$-C_{21}$	$-C_{20}$	$-C_{19}$	$-C_{18}$	$-C_{17}$
10000	$\sigma_y\otimes I\otimes I$	$-C_7$	$-C_8$	$-C_9$	$-C_{10}$	$-C_{11}$	$-C_{12}$	$-C_{13}$	$-C_{14}$	$-C_{15}$	$-C_{16}$
10001	$\sigma_y\otimes I\otimes\sigma_x$	$-C_8$	$-C_7$	$-C_{10}$	$-C_9$	$-C_{12}$	$-C_{11}$	$-C_{14}$	$-C_{13}$	$-C_{16}$	$-C_{15}$
10010	$\sigma_y\otimes\sigma_x\otimes I$	C_5	C_6	$-C_{11}$	$-C_{12}$	$-C_9$	$-C_{10}$	C_{15}	C_{16}	C_{13}	C_{14}
10011	$\sigma_y\otimes\sigma_x\otimes\sigma_x$	C_6	C_5	$-C_{12}$	$-C_{11}$	$-C_{10}$	$-C_9$	C_{16}	C_{15}	C_{14}	C_{13}
10100	$\sigma_y\otimes\sigma_y\otimes I$	C_3	C_4	$-C_{13}$	$-C_{14}$	$-C_{15}$	$-C_{16}$	C_9	C_{10}	C_{11}	C_{12}
10101	$\sigma_y\otimes\sigma_y\otimes\sigma_x$	C_4	C_3	$-C_{14}$	$-C_{13}$	$-C_{16}$	$-C_{15}$	C_{10}	C_9	C_{12}	C_{11}
10110	$\sigma_y\otimes\sigma_z\otimes I$	$-C_1$	$-C_2$	$-C_{15}$	$-C_{16}$	$-C_{13}$	$-C_{14}$	$-C_{11}$	$-C_{12}$	$-C_9$	$-C_{10}$
10111	$\sigma_y\otimes\sigma_z\otimes\sigma_x$	$-C_2$	$-C_1$	$-C_{16}$	$-C_{15}$	$-C_{14}$	$-C_{13}$	$-C_{12}$	$-C_{11}$	$-C_{10}$	$-C_9$
11000	$\sigma_z\otimes I\otimes I$	C_{15}	C_{16}	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8
11001	$\sigma_z\otimes I\otimes\sigma_x$	C_{16}	C_{15}	C_2	C_1	C_4	C_3	C_6	C_5	C_8	C_7
11010	$\sigma_z\otimes\sigma_x\otimes I$	$-C_{13}$	$-C_{14}$	C_3	C_4	C_1	C_2	$-C_7$	$-C_8$	$-C_5$	$-C_6$
11011	$\sigma_z\otimes\sigma_x\otimes\sigma_x$	$-C_{14}$	$-C_{13}$	C_4	C_3	C_2	C_1	$-C_8$	$-C_7$	$-C_6$	$-C_5$
11100	$\sigma_z\otimes\sigma_y\otimes I$	$-C_{11}$	$-C_{12}$	C_5	C_6	C_7	C_8	$-C_1$	$-C_2$	$-C_3$	$-C_4$
11101	$\sigma_z\otimes\sigma_y\otimes\sigma_x$	$-C_{12}$	$-C_{11}$	C_6	C_5	C_8	C_7	$-C_2$	$-C_1$	$-C_4$	$-C_3$
11110	$\sigma_z\otimes\sigma_z\otimes I$	C_9	C_{10}	C_7	C_8	C_5	C_6	C_3	C_4	C_1	C_2
11111	$\sigma_z\otimes\sigma_z\otimes\sigma_x$	C_{10}	C_9	C_8	C_7	C_6	C_5	C_4	C_3	C_2	C_1

4. SECURITY ANALYSIS

In this segment, the security of the current protocol has been examined from two perspectives: leaking of information and susceptibility to existing attacks.

4.1. Information Leakage

In this part, we asserted that our protocol had no information leaking. The initial state is already known to both users and is entirely confidential between the users. Because Alice and Bob's encoding operation combinations are completely arbitrary, the channel comprises 32 × 32 equally likely combinations of operations, then the channel contains

$$-\sum p_i \, log \, p_i \;\; = -(32 \times 32) \times \frac{1}{32 \times 32} \log \frac{1}{32 \times 32}$$
$$= 10 \text{ bits}$$

However, the payload of Alice and Bob's exchange message is also 10 bits. As a result, the QD protocol has no data leakage.

4.2. Various Attacks

The security of the secret message's transmission under the given protocol is dependent on the security of the quantum channel employed. Assume Alice and Bob have the same quantum state, ρ^{AB}. Both users then perform the unitary operation U_i on the first, fourth, and sixth qubits of the state ρ^{AB} to encode the classical information i with probability p_i.

The amount of classical bits that can be encoded for a given quantum state is thus given by [24]

$$\chi(\rho^{AB}) = \log_2 d_A + S\,(\rho^{A \, or \, B}) - S\,(\rho^{AB})$$

where d is the dimension of Alice's system of the Hilbert space of ρ^{AB} then we obtain the capacity of dense coding of $|C\rangle$ quantum system is

$$\chi(\rho^{AB}) = 3 + 2 - 0 \; = 5$$

Thus, by sending only three qubits to each other, both can convey five classical bits. Because $|C\rangle$ is a pure state, it can be considered the state in which two subsystems are most entangled that means $S(\rho^{AB}) = 0$ and $S(\rho^{A}) = S(\rho^{B}) = 2$ where $S(\rho)$ is Von Neumann entropy that defines

$$S(\rho) = -\,tr\,(\rho \log \rho) = -\sum_i \lambda_i \log \lambda_i$$

As a result, entanglement in a state ρ^{AB} is beneficial to dense coding if

$$S\,(\rho^{B}) \; - \; S(\rho) > \; 0$$

Intercept and Resend Attack: Eve intercepts the 1S sequence on its way from Alice to Bob, retains it, and then transmits another newly prepared false sequence to eavesdrop on the information about the cluster state that was first created. Because the captured particle comprises l decoy particles, Alice discloses the decoy particle's position and measurement basis. By deleting decoy photons, Eve can return to the original cluster state. However, when Bob deals with Eve's false sequence, he will

get different outcomes, introducing a significant error rate. As a result, Eve is easily detectable during the security verification process. If l decoy photons are present, Assuming the existence of l decoy photons, then this attack can be identified with $(1-\frac{1}{4^l})$ probability (only when Eve makes exactly the identical decoy photons as Alice, no error occurs, the probability of this condition is $\frac{1}{4^l}$. Thus, the overall error rate is $(1-\frac{1}{4^l})$).

Impersonation or Man in the Middle Attack: Eve might pretend to be Bob to Alice. This attack can be avoided in the present protocol by authenticating the sender and receiver's identities prior to quantum communication. The receiver should also notify the sender that the transmitted qubits were received over an authenticated classical channel. Regardless, Eve's presence would be discovered with a 50% probability.

Trojan Horse Attack: Another method of attack, known as the Trojan horse attack [25], involves Eve changing the photon number and inserting an extra eavesdropping photon between the original and steal the information. To eavesdrop on the information, she can utilize the delay photon attack or the invisible photon attack. To spy on the discourse between the users, either a delayed photon with the same frequency as Alice's original photon or a simultaneous photon with a frequency different from Alice are utilized in these two sorts of attacks. Using a photon number splitter (PNS 50/50) to detect and filter invisible photons, these attacks can be effectively prevented.

Controlled Not Attack: Eve prepares an auxiliary state which is as follow

$$|\phi\rangle = (|000000\rangle + |111111\rangle)_{789101112}$$

She executes the CNOT operation on the first, fourth, and sixth qubits, which serve as control bits and her particles 7, 8, 9 serve as target bits. Eve sends 10, 11, 12 particles to Bob after her operation.

$$\begin{aligned}|\psi\rangle &= |C\rangle \otimes |\phi\rangle \\ &= \frac{1}{2}[|000000\rangle + |000111\rangle + |111000\rangle - |111111\rangle]_{123456} \\ &\quad \otimes \frac{1}{2}[|000000\rangle + |111111\rangle]_{789101112} \\ &= \frac{1}{4}[|000000000000\rangle + |0001110000000\rangle + |111000000000\rangle \\ &\quad - |111111000000\rangle + |000000111111\rangle + |000111111111\rangle \\ &\quad + |111000111111\rangle - |111111111111\rangle]\end{aligned}$$

$$|\psi'\rangle = I_{235} \otimes CNOT_{17} \otimes CNOT_{48} \otimes CNOT_{69} \otimes I_{101112} \otimes |\psi\rangle$$

$$\begin{aligned}&= \frac{1}{4}[|000\rangle|000000\rangle\,|000\rangle + |001\rangle|011011\rangle\,|000\rangle \\ &\quad + |110\rangle\,|100100\rangle\,|000\rangle - |111\rangle\,|111111\rangle\,|000\rangle \\ &\quad + |000\rangle\,|000111\rangle\,|111\rangle + |001\rangle\,|011100\rangle\,|111\rangle \\ &\quad + |110\rangle|100011\rangle\,|111\rangle - |111\rangle\,|111000\rangle\,|111\rangle]\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{4}[|000\rangle_{235}(|000000\rangle\,|000\rangle + |000111\rangle\,|111\rangle)_{146789101112} \\
&\quad + |001\rangle_{235}(|011011\rangle\,|000\rangle + |011100\rangle\,|111\rangle)_{146789101112} \\
&\quad + |110\rangle_{235}(|100100\rangle\,|000\rangle + |100011\rangle\,|111\rangle)_{146789101112} \\
&\quad - |111\rangle_{235}(|111111\rangle\,|000\rangle\ +\ |111000\rangle\,|111\rangle)_{146789101112}]
\end{aligned}
$$

As can be seen, Bob will only ever get two sorts of measurement results after introducing the auxiliary state. As a result, Bob will readily notice the communication's eavesdropping, stop the protocol, and Eve will receive no benefit from the aforesaid attack.

Another Type of Attack: Eve tries to intercept the particle when Alice sends the initial state to Bob. Eve again attacks the particles when they are encoded by Alice while sending to Bob and then attacking the particle in the final result when Bob sends and encodes bit to Alice. Following Eve's attack, the density matrix of the entire system is now ρ. So, according to the Holevo bounds [22], the quantity of accessible information of Eve is

$$
\begin{aligned}
I_{Eve} &\leq \chi(\rho) \\
\chi(\rho) &= S(\rho) - \sum p_i S(\rho_i)
\end{aligned} \tag{1}
$$

Here p_i is the appearing probability of six qubit cluster state ρ_i and $\rho = \sum p_i \rho_i$ is the average density matrix of all six qubit clusters state. We know $S(\rho)$ is the upper bound of $\chi(\rho)$ and high fidelity implies low entropy.

Assume the fidelity [26] of the message transmission process is

$$
F(|C\rangle, \rho)^2 = (\langle C|\rho|C\rangle)^2 = 1 - \gamma \tag{2}
$$

where $\gamma(0 \leq \gamma \leq 1)$and the detection probability is d $\geq \frac{\gamma}{2}$. So,$S(\rho)$is no more than $S(\rho_{max})$ where ρ_{max} is a 32×32 diagonal matrix with diagonal entries $1-\gamma, \frac{\gamma}{31}, \frac{\gamma}{31} \ldots . \frac{\gamma}{31}$. The entropy of is

$$
\begin{aligned}
S(\rho_{max}) &= -tr\,(\rho_{max} \log_2 \rho_{max}) \\
&= -(1-\gamma)\log_2(1-\gamma) - \gamma \log_2 \frac{\gamma}{31}
\end{aligned} \tag{3}
$$

Then the accessible information of Eve is satisfied according to equations (1) and (3).

$$
I_{Eve} \leq \chi(\rho) \leq S(\rho) \leq S(\rho_{max}) = -(1-\gamma)\log_2(1-\gamma) - \gamma \log_2 \frac{\gamma}{31}
$$

Evidently, when $\gamma = 0, I_{Eve} \leq 0$ means, If Eve does not wish to be discovered, she will receive nothing. On the flip side, when $\gamma = \frac{31}{32}$, $I_{Eve} \leq 5$, Eve may be able to eavesdrop on all information with the detection probability$\gamma = \frac{31}{32}$.

5. EFFICIENCY

A quantitative assessment of the efficiency of a secure quantum communication scheme [27] is defined as

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

where, m is the number of secret bits exchanged, and q and b denote the number of qubits and classical bits used, respectively. In this situation, the quantum and classical bits needed for eavesdropping detection are ignored. The number of secret bits received is 10, indicating that m=10, the number of qubits used is 12, and there is no classical announcement, i.e., b = 0. Thus, the suggested protocol's quantum efficiency is 83.33 %. The comparative analysis (summarised in Table 3) shows that the suggested protocol is substantially more efficient than existing approaches.

Table 3. Efficiency comparison of different protocols

Protocols	***Qubit transmitted***	***Efficiency (in %)***
Shi et. al. [11]	*4 bits*	*66.7*
Gao [17]	*8 bits*	*66.7*
Zhang et.al. [19]	*2 bits*	*33.33*
Liu et.al. [20]	*2 bits*	*50*
Our protocol	*10 bits*	*83.33*

6. CONCLUSION

The most significant difference between our QD protocol and the protocols listed in Table 3 is that we use six qubit cluster states as the quantum channel. The following are some of the scheme's key highlights: (i) We utilize the concept of dense coding to encode our information using local unitary operation without breaking the entanglement of cluster states. (ii) This approach has greater efficiency than the protocols stated in Table 3. (iii) Our protocol has no information leaking issues. (iv) The channel capacity of our protocol is high because we require only three qubits to deliver five bits of classical data. (v) Our scheme is resistant to the various known attacks. (vi) The quantum dialogue's secure realization is dependent on the quantum channel's security, which is achieved through two security checks. Furthermore, two users can confirm each other's identity. Finally, no classical key is ever generated in our QD protocol; however, Table 2 serves as an interpreter.

In summary, the current scheme achieves quantum dialogue by employing six qubit cluster states as an entangled resource, allowing two legitimate users to interchange five-bit secret messages concurrently while encoding with only three qubits. This approach makes use of the concept of superdense coding with capacity inside the Holevo limit. It has strong security since it uses a two steps security check, authentication process, and accounts for various eavesdropping attacks without leaking any information. In comparison to prior work, this protocol improves efficiency. Since an entanglement between six-qubit cluster states has been attained

experimentally, we anticipate that our scheme might be helpful for constructing multiparties QD protocols, which would be an intriguing future research topic.

REFERENCES

[1] Bennett, C. H., Brassard, G. Quantum cryptography: public-key distribution and coin tossing. In: *Proceedings IEEE International Conference on Computers, Systems and Signal Processing, Bangalore*, IEEE, New York, 1984. pp. 175–179.

[2] Long, G. L., Liu X. S. Theoretically efficient high-capacity quantum key distribution scheme. *Physical Review A*, Vol. 65, No. 3, art. 0323302, 2002.

[3] Liu, Z. H., Chen, H. W., Liu, W. J., Xu, J., Wang, D., Li, Z. Q. Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states. *Quantum Information Processing,* Vol. 12, No. 1, 2013, pp. 587–599.

[4] Dong, L., Dong, H. K., Xiu, X. M., Gao, Y J., Chi, F. Quantum secure direct communication using a six-qubit maximally entangled state with dense coding. *International Journal of Quantum Information,* Vol. 07, No. 3, 2009, pp. 645–651. doi.org/10.1142/S021974990900533X

[5] Laurenza, R., Lupo, C., Lloyd, S., et al. Dense coding capacity of a quantum channel. *arXiv preprintarXiv*:1903.09168,2019.

[6] Nguyen B. A. Quantum dialogue. *Physics Letters A*, Vol. 328, No. 1, 2004, pp.6 -10.

[7] Ji, X., Zhang, S. Secure quantum dialogue based on single-photon. *Chinese Physics*, Vol. 15, No. 7, 2006, pp. 1418–1420.

[8] Xia, Y., Song, J., Nie, J., Song, H.S. Controlled secure quantum dialogue using a pure entangled GHZ states. *Communication in Theoretical Physics,* Vol. 48, No. 5, 2007, pp. 841–846.

[9] Gao, F., Guo, F.Z., Wen, Q.Y., Zhu, F.C. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Science in China Series G: Physics, Mechanics and Astronomy*, Vol. 51, No. 5, 2008, pp. 559–566. doi.org/10.1007/s11433-008-0065-y

[10] Tan, Y.G., Cai, Q.Y. Classical correlation in quantum dialogue. *International Journal of Quantum Information,* Vol. 6, No. 3, 2008, pp. 325–329.

[11] Shi, G.F., Xi, X.Q., Tian, X.L., Yue, R.H. Bidirectional quantum secure communication based on a shared private Bell state. *Optic Communications* 282, 2009, pp. 2460-2463. doi.org/10.1016/j.optcom.2009.02.062

[12] Liu, Z., 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 Letter A,* Vol. 34, No. 29, art. 1950241, 2019. doi.org/10.1142/S0217732319502419

[13] Liu, Z. H., Chen, H. W. Analysis and improvement of large payload bidirectional quantum secure direct communication without information leakage. *International Journal of Theoretical Physics,* Vol. 57, No. 2, 2018, pp. 311–321. doi.org/10.1007/s10773-017-3563-8

[14] Huang, Z. M., Situ, H. Z. Protection of quantum dialogue affected by quantum field. *Quantum Information Process,* Vol. 18. 2019. doi.org/10.1007/s11128-018-2152-y

[15] Liu, Z. H., Chen, H. W. Comment on "Protection of quantum dialogue affected by quantum field". *Quantum Information Processing,* Vol. 20, 2021. doi.org/10.1007/s11128-018-2152-y

[16] Gao, G., Wang, L. P. A Protocol for bidirectional quantum secure communication based on genuine four-particle entangled states. *Communication Theoretical Phys*ics, Vol. 54, No. 3, 2010, pp. 447-451. doi.org/10.1088/0253-6102/54/3/13

[17] Gao, G. Bidirectional quantum secure communication based on one dimensional four-particle cluster states. *Journal of Theoretical Physics,* Vol. 53, No. 7, 2014, pp. 2282-2287. doi.org/10.1007/s10773-014-2028-6

[18] Li, W., Zha, X.W., Yu, Y. Secure quantum dialogue protocol based on four qubit cluster state. *International Journal of Theoretical Physics,* Vol. 57, No. 2, 2018, pp. 371–380.

[19] Zhang, L., Dong, S., Zhang, K.J., et al. A controller-independent quantum dialogue protocol with four particle states. *International Journal of Theoretical Physics,* Vol. 58, No. 6, 2019, pp. 927-1936. doi:10.1007/s10773-019-04087-7

[20] Liu, Z., Chen, H. Analyzing and improving the secure quantum dialogue protocol based on four-qubit cluster state. *International Journal of Theoretical Physics,* Vol. 59, No. 3, 2020, pp. 2120-2126. doi:10.1007/s10773-020-04485-2

[21] Briegel, H., Raussendorg, R. Presisent entanglement in arrays of interacting particles. *Physics Review Letters,* Vol. 86, No. 5, art. 910, 2001.

[22] Muralidharan, S., Jain, S., Panigrahi, P. K. Non-destructive discrimination of multiparticle cluster states for quantum computation*, arXiv*:0906.2147, 2009.

[23] Paul, N., Menon, J. V., Karumanchi, S., Muralidharan, S., Panigrahi, P. K. Quantum tasks using six qubit cluster states. *Quantum Information Processing* Vol. 10, 2011, pp. 619–632. doi.org/10.1007/s11128-010-0217-7

[24] Bruss, D., D'Ariano, G. M., Lewenstein, M., Macchiavello, C., Sen(De), A., Sen, U. Distributed quantum dense coding. *Physics Review Letters*. Vol. 93, art. 210501, 2004. doi.org/10.1103/PhysRevLett.93.210501

[25] Cai, Q. Y. Eavesdropping on two way communication protocols with invisible photons. *Physics Letter A*, Vol. 351, 2005, pp. 23-25.

[26] Neilsen, M. A., Chuang, I. L. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[27] Cabello, A. Quantum key distribution in Holevo limit. *Physics Review Letters*. Vol. 85, art. 5635, 2000, pp. 5635-5638. doi.org/10.1103/PhysRevLett.85.5635

Information about the authors:

Sanju Chauhan –Ph.D. Scholar at Mewar University, Chittorgarh, Rajasthan, in Department of Physics, Currently working as Lecturer in Government Polytechnic college, Ajmer, Rajasthan, India, areas of scientific research are quantum information and quantum computation.

Dr. Narayan Lal Gupta – Associate Professor at Government College, Dungarpur, Rajasthan, India, in the Department of Physics, areas of scientific research are quantum information and computation, quantum optics, etc.

Manuscript received on 15 July 2021