Publications

Available Online

J. Sci. Res. **14** (1), 179-187 (2022)

JOURNAL OF
SCIENTIFIC RESEARCH

www.banglajol.info/index.php/JSR

Bidirectional Quantum Secure Direct Communication Using Dense Coding of Four Qubit Cluster States

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

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

Received 2 July 2021, accepted in final revised form 17 October 2021

Abstract

We are introducing an efficient bidirectional quantum secure direct communication protocol that employs the four qubit cluster states, creating a novel quantum channel based on dense coding between the transmitter and receiver. By dense coding, after a conventional announcement, two legitimate users can simultaneously exchange their messages. Two safety checking measures are taken to ensure safe transmission. Information leaking is not an issue in this protocol, and it is secure against some well-known eavesdropping assaults. It is also accessible with cutting-edge technology.

Keywords: Bidirectional Quantum Secure Direct Communication (BQSDC); Four qubit cluster state; Dense coding; Information leakage.

doi: http://dx.doi.org/10.3329/jsr.v14i1.54479 J. Sci. Res. **14** (1), 179-187 (2022)

1. Introduction

Quantum cryptography provides a unique way to communicate secure communication among legitimate users using the law of quantum mechanics. The foundation of quantum cryptography was led by Bennet and Brassard [1] by introducing the first QKD protocol. Subsequently, many QKD protocols have been proposed [2-6]. Quantum cryptography has a quick expansion and has developed various branches such as QKD [3-6], quantum secret sharing (QSS) [7,8], quantum secure direct communication (QSDC) [9-13], quantum dialogue [14,15], quantum teleportation (QT) [16] and super dense coding [17-21], etc.

Different from QKD, QSDC provides a way by which the secret message can be transmitted securely without generating a private key in advance. In 2002 Long *et al.* proposed the first QSDC protocol by using EPR pair [9]. Further, many QSDC protocols have been introduced based on cluster states [22-27] and other than cluster states. However, they permit one-sided communication, not bidirectional, i.e., users cannot exchange their messages simultaneously. To overcome this drawback, the first

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

BQDC protocol named Quantum Dialogue (QD) was put forward by Nguyen [28] and Zhang *et al*. [29], in which legal users transmit secret messages simultaneously. Many QD protocols have been introduced using various quantum properties [30-34], but information leakage problems still exist [35,36]. Several researchers have proposed new QD procedures [37-42] in response to this problem. In recent years, entanglement has received a lot of attention because of its practical application in quantum information theory. It plays a critical role in preventing information leaking in many QD protocols using multipartite entangled states. In 2013, Chang came up with a BQSDC protocol based on five qubit cluster states [43]. Gao also put forward two protocols of BQSC based on genuine four particles entangled state and one dimensional four-particle cluster states [44,45]. A controller independent bidirectional quantum direct communication was introduced by Mohapatra in 2017 [46]. In 2019, Zhang *et al*. [47] proposed a controller independent quantum dialogue protocol with four-particle states. A secure QD protocol based on four qubit cluster state [48] has been put forward by Li *et al*., further improved by Zhinao *et al*. [49]. A measurement device-independent QD protocol was introduced by Das [50] in which they discard less qubit to prevent information leakage. Subsequently, Huang *et al*. [51] proposed a QD technique based on three-qubit GHZ states, but this approach inadvertently leaks 50 percent of the secret message transmitted data. Further, Zhi *et al.* [52] cryptanalyzed it and improved it by encoding the one-bit secret message using one of the two unitary operations. In addition, a number of QD procedures have been proposed to limit information leaking, particularly by integrating multiparticle entangled states [53-55]. According to the aforementioned research findings, an effective QD protocol using entangled states with no information leakage has theoretical and practical relevance, prompting us to propose this approach using cluster states.

Before commencement, the features of the cluster state should be looked into. It was first reported by Briegel and Raussendoof in 2001 [56-59]. Cluster states, a type of entangled state with unique features, play a significant role in the problem of information leakage. Some of their characteristics are similar to GHZ class and W class entangled state. Due to the considerable persistence of entanglement, the cluster states are more difficult to dismantle through local operations than GHZ states or other states and are robust against de-coherence. Here, we offer a BQSDC protocol that allows two authorized users to share a secret four-bit message via a quantum channel with four qubit cluster states at the same time. This approach uses quantum superdense coding to encode two bits of information on a single quantum bit without disrupting the entanglement. The following characteristics distinguish our scheme: (i) We introduce a QD scheme that uses reusable four-qubit cluster states with dense coding via local unitary operation while keeping the shared channel entanglement.. (ii) With an efficiency of 66.7 %, our scheme is more efficient. (iii) Furthermore, our scheme also poses no risk of data leaking. (iv) In addition, in order to transmit 4N bits of classical data, we employ 2N qubits of four qubit cluster states. As a result, our protocol is the most capable and meets the Holevo constraint. (v) Two security assessments have made our system more secure.

2. Description of BQSDC Protocol

The two non-orthogonal bases of single photon measurement are in B_Z bases $(|0\rangle, |1\rangle)$ and B_X bases $(|+\rangle, |-\rangle)$ where, $|+\rangle = \frac{|+\rangle + |-\rangle}{2}$ and $|-\rangle = \frac{|+\rangle - |-\rangle}{2}$

The unitary operation used for two-bit secret messages ij encoding using dense coding are defined as

$U_0 = I = |0\rangle\langle 0| + |1\rangle\langle 1|$

$U_1 = \sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$

$U_2 = \sigma_y = |0\rangle\langle 1| - |1\rangle\langle 0|$

$U_3 = \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1|$

The two bit classical information can be represented by four Pauli operators as,

$U_0 \leftrightarrow 00, \quad U_1 \leftrightarrow 01, \quad U_2 \leftrightarrow 10, \quad U_3 \leftrightarrow 11$

From the perspective of quantum reversible logic circuits, two authors [52,53] have investigated a precise circuit for the physical attainment of four qubit cluster states. The four qubit cluster states that can be generated by implementing the following general circuit diagram by changing the inputs $|0000>_{abcd}$ to different computational bases, are as follow

$|C\rangle = |0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle$

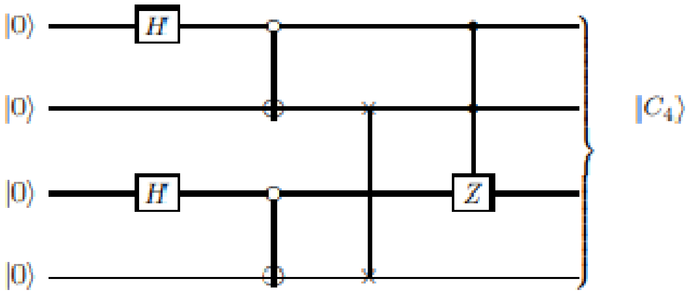

Fig. 1. Circuit diagram for generating four qubit cluster states.

In a group of sixteen orthogonal cluster states, dense coding changes one cluster state to another by implementing a relevant unitary operation (on the first and third qubit), as illustrated in Table 1. All these states are orthogonal to each other and taken as measuring bases of four qubit cluster states through Von Neumann measurement. The reduced density matrices of the qubits (1, 3) and (2, 4) are entirely mixed and indistinguishable states because they are maximally entangled states.

$\rho = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$

If N orthogonal states, present in quantum states aggregation, one can encrypt $\log_2 n$ classical bit in a quantum state by using dense coding.

Table 1. Dense coding for $|\mathbf{C}\rangle_{\mathbf{abcd}}$.

$$\begin{aligned}
&|\mathbf{C_1}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{0000}\rangle + |\mathbf{0011}\rangle + |\mathbf{1100}\rangle - |\mathbf{1111}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_2}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_1^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{0010}\rangle + |\mathbf{0001}\rangle + |\mathbf{1110}\rangle - |\mathbf{1101}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_3}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_2^c}|\mathbf{C}\rangle = \tfrac{1}{2}(-|\mathbf{0010}\rangle + |\mathbf{0001}\rangle - |\mathbf{1110}\rangle - |\mathbf{1101}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_4}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_3^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{0000}\rangle - |\mathbf{0011}\rangle + |\mathbf{1100}\rangle + |\mathbf{1111}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_5}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{1000}\rangle + |\mathbf{1011}\rangle + |\mathbf{0100}\rangle - |\mathbf{0111}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_6}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{1010}\rangle + |\mathbf{1001}\rangle + |\mathbf{0110}\rangle - |\mathbf{0101}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_7}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(-|\mathbf{1010}\rangle + |\mathbf{1001}\rangle - |\mathbf{0110}\rangle - |\mathbf{0101}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_8}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{0000}\rangle - |\mathbf{1011}\rangle + |\mathbf{0100}\rangle + |\mathbf{0111}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_9}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(-|\mathbf{1000}\rangle - |\mathbf{1011}\rangle + |\mathbf{0100}\rangle - |\mathbf{0111}\rangle)'_{\mathbf{abcd}}\\
&|\mathbf{C_{10}}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(-|\mathbf{1010}\rangle - |\mathbf{1001}\rangle + |\mathbf{0110}\rangle - |\mathbf{0101}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_{11}}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{1010}\rangle - |\mathbf{1001}\rangle - |\mathbf{0110}\rangle - |\mathbf{0101}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_{12}}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(-|\mathbf{1000}\rangle + |\mathbf{1011}\rangle + |\mathbf{0100}\rangle + |\mathbf{0111}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_{13}}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{0000}\rangle + |\mathbf{0011}\rangle - |\mathbf{1100}\rangle + |\mathbf{1111}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_{14}}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(|\mathbf{0010}\rangle + |\mathbf{0001}\rangle - |\mathbf{1110}\rangle + |\mathbf{1101}\rangle)_{\mathbf{abcd}}\\
&|\mathbf{C_{15}}\rangle = \mathbf{U_0^a}\otimes\mathbf{U_0^c}|\mathbf{C}\rangle = \tfrac{1}{2}(-|\mathbf{0010}\rangle + |\mathbf{0001}\rangle + |\mathbf{1110}\rangle + |\mathbf{1101}\rangle)_{\mathbf{abcd}}
\end{aligned}$$

2.1. *BQSDC protocol*

In our BQSDC protocol, Alice and Bob are two valid users who can transmit secret messages at the same time. Following is the description of the protocol:

Step 1: Alice prepares two same sequences (1S and 2S sequence) of n cluster states in a state $S = \{S_1^a, S_1^b, S_1^c, S_1^d, S_2^a, S_2^b, S_2^c, S_2^d \ldots\ldots\ldots S_n^a, S_n^b, S_n^c, S_n^d\}$ where a,b,c,d refer to four particles in a cluster state, and the subscript 1,2,3,4…..n represents the order of cluster states in a sequence. Alice prepares two batches of decoy photon (say l and m particles) randomly either in B_Z bases $(|0\rangle, |1\rangle)$ or in $\mathrm{B_X}$ bases $(|+\rangle, |-\rangle)$. By inserting l particles in 1S sequence and a new (n+l) sequence is sent to Bob.

Step 2: After sending the sequence to Bob, Alice announces the actual position and correct measuring basis of each l particle of decoy photon. After that, Bob measures the l particles in the correct basis and compares the results. Then Bob has analyzed the error rate. The process is terminated if it reaches the threshold; else, it will continue.

Step 3: Alice performs a unitary operation $U_i^a \otimes U_i^c$ on each cluster states of 2S sequence in the absence of an eavesdropper, which corresponds to a four-bit classical message. Alice inserts m particles into 2S sequence for the second security check and sends the (n+m) particles sequence to Bob.

Step 4: Bob receives a 2*S* sequence. To ensure the security of transmission, Alice announces the position and the states of m decoy particles. Then, Bob measures the particles correctly and compares them with Alice's announcement to check whether the sequence has eavesdropped. Bob eliminates m particles and encodes his secret message by executing $U_i^a \otimes U_i^c$ operation on the first and third qubits of cluster states in the 2*S* sequence.

Step 5: After performing the unitary operation, Bob gets a new cluster state and then he announces his outcome. As per Bob's outcome, Alice can conclude Bob's secret message. In the meantime, Bob is also able to get the result, according to Table 2.

For instance, If Alice prepared $|C_1\rangle$ as the initial state of four qubit cluster states and 0011 and 0111 is the secret messages of Alice and Bob with their encoding operation $U_0^a \otimes U_4^c$ and $U_1^a \otimes U_3^c$ respectively, they will get the final result $|C_5\rangle$ (according to Table 2), which is as follows:

$|\mathrm{C}_1\rangle_{\mathrm{abcd}} = \mathrm{U}_0^{\mathrm{a}} \otimes \mathrm{U}_3^{\mathrm{c}} |\mathrm{C}_1\rangle = |\mathrm{C}_4\rangle_{\mathrm{abcd}}$

$\mathrm{U}_1^{\mathrm{a}} \otimes \mathrm{U}_3^{\mathrm{c}} |\mathrm{C}_4\rangle = |\mathrm{C}_5\rangle$

The final result $|C_5\rangle$ is measured and announced by Bob. Then, with the help of three known messages ($|C_1\rangle_{\mathrm{abcd}}$, their encoding operation, $|C_5\rangle$). Alice is able to deduce Bob's secret operation is $U_1^a \otimes U_3^c$. Since Bob has got the initial cluster state information by 1*S* sequence, as both 1*S* and 2*S* are identical. Bob also can deduce Alice's secret operation is $U_0^a \otimes U_3^c$. So, Alice and Bob can deliver secret information simultaneously to one another.

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

Classical bit	Encoding operation	$\|C_1\rangle$	$\|C_2\rangle$	$\|C_3\rangle$	$\|C_4\rangle$	$\|C_5\rangle$	$\|C_6\rangle$	$\|C_7\rangle$	$\|C_8\rangle$	$\|C_9\rangle$	$\|C_{10}\rangle$	$\|C_{11}\rangle$	$\|C_{12}\rangle$	$\|C_{13}\rangle$	$\|C_{14}\rangle$	$\|C_{15}\rangle$	$\|C_{16}\rangle$
0000	$U_0^a \otimes U_0^c$	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}
0001	$U_0^a \otimes U_1^c$	C_2	C_1	$-C_4$	$-C_3$	C_6	C_5	$-C_8$	$-C_7$	C_{10}	C_9	$-C_{12}$	$-C_{11}$	C_{14}	C_{13}	$-C_{16}$	$-C_{15}$
0010	$U_0^a \otimes U_2^c$	C_3	C_4	$-C_1$	$-C_2$	C_7	C_8	$-C_5$	$-C_6$	C_{11}	C_{12}	$-C_9$	$-C_{10}$	C_{15}	C_{16}	$-C_{13}$	$-C_{14}$
0011	$U_0^a \otimes U_3^c$	C_4	C_3	C_2	C_1	C_8	C_7	C_6	C_5	C_{12}	C_{11}	C_{10}	C_9	C_{16}	C_{15}	C_{14}	C_{13}
0100	$U_1^a \otimes U_0^c$	C_5	C_6	C_7	C_8	C_1	C_2	C_3	C_4	$-C_{13}$	$-C_{14}$	$-C_{15}$	$-C_{16}$	$-C_9$	$-C_{10}$	$-C_{11}$	$-C_{12}$
0101	$U_1^a \otimes U_1^c$	C_6	C_5	$-C_8$	$-C_7$	C_2	C_1	$-C_4$	$-C_3$	$-C_{14}$	$-C_{13}$	C_{16}	C_{15}	$-C_{10}$	$-C_9$	C_{12}	$-C_{11}$
0110	$U_1^a \otimes U_2^c$	C_7	C_8	$-C_5$	$-C_6$	C_3	C_4	$-C_1$	$-C_2$	$-C_{15}$	$-C_{16}$	C_{13}	C_{14}	$-C_{11}$	$-C_{12}$	C_9	C_{10}
0111	$U_1^a \otimes U_3^c$	C_8	C_7	C_6	C_5	C_4	C_3	C_2	C_1	$-C_{16}$	$-C_{15}$	$-C_{14}$	$-C_{13}$	$-C_{12}$	C_{11}	$-C_{10}$	$-C_9$
1000	$U_2^a \otimes U_0^c$	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}	$-C_1$	$-C_2$	$-C_3$	$-C_4$	$-C_5$	$-C_6$	$-C_7$	$-C_8$
1001	$U_2^a \otimes U_1^c$	C_{10}	C_9	$-C_{12}$	$-C_{11}$	C_{14}	C_{13}	$-C_{16}$	$-C_{15}$	$-C_2$	$-C_1$	C_4	C_3	$-C_6$	$-C_5$	C_8	C_7
1010	$U_2^a \otimes U_3^c$	C_{11}	C_{12}	$-C_9$	$-C_{10}$	C_{15}	C_{16}	$-C_{13}$	$-C_{14}$	$-C_3$	$-C_4$	C_1	C_2	$-C_7$	$-C_8$	C_5	C_6
1011	$U_2^a \otimes U_3^c$	C_{12}	C_{11}	C_{10}	C_9	C_{16}	C_{15}	C_{14}	C_{13}	$-C_4$	$-C_3$	$-C_2$	$-C_1$	$-C_8$	$-C_7$	$-C_6$	$-C_5$
1100	$U_3^a \otimes U_0^c$	C_{13}	C_{14}	C_{15}	C_{16}	C_9	C_{10}	C_{11}	C_{12}	C_5	C_6	C_7	C_8	C_1	C_2	C_3	C_4
1101	$U_3^a \otimes U_1^c$	C_{14}	C_{13}	$-C_{16}$	$-C_{15}$	C_{10}	C_9	$-C_{12}$	$-C_{11}$	C_6	C_5	$-C_8$	$-C_7$	C_2	C_1	$-C_4$	$-C_3$
1110	$U_3^a \otimes U_2^c$	C_{15}	C_{16}	$-C_{13}$	$-C_{14}$	C_{11}	C_{12}	$-C_9$	$-C_{10}$	C_7	C_8	$-C_5$	$-C_6$	C_3	C_4	$-C_1$	$-C_2$
1111	$U_3^a \otimes U_3^c$	C_{16}	C_{15}	C_{14}	C_{13}	C_{12}	C_{11}	C_{10}	C_9	C_8	C_7	C_6	C_5	C_4	C_3	C_2	C_1

3. Security Analysis

3.1. *Information leakage analysis*

In our scheme, Bob publishes only the final outcome, i.e. $|C_5\rangle$ and the initial state is not published and is entirely secret between Alice and Bob. Besides, that there are 16x16 possible combinations of operations which are equally probable then, the channel contains

$$-\sum p_i \, log \, p_i = -\,(16 \times 16\,)\, x \, \frac{1}{16\times16} \log \frac{1}{16\times16}$$

= 8-bit secret message

Since the message exchanged between Alice and Bob is also 8 bits. As a result, all the information is communicated securely without any leakage.

3.2. *Some types of attack*

In this segment, we will examine and discuss the integrity of our approach against some prevalent attacks.

3.2.1. *Intercept and Resend attack*

Eve intercepts 1*S* state, which is travelling from Alice to Bob, and a counterfeit sequence 1S is sent to Bob in which each particle is in one of the four states $|0\rangle, |1\rangle$, $(|+\rangle, |-\rangle)$ to obtain information about cluster state in 1*S* sequence. Since the intercepted particles contain l decoy particles, when Alice announces the state and position of l particles, Eve will get a cluster state after discarding decoy particles. However, Bob will not get the same result as he measures Eve's fake sequence, which introduces a big error rate. Consequently, Eve can be easily detected.

3.2.2. *Entangle and Measure attack*

Assume Eve intends to extract some relevant data by performing an entangle and measure attack on a 1S sequence transmitting between Alice and Bob. She executes a general operation U_e on 1S and the auxiliary particle $|\mathcal{E}\rangle$ that she had previously created. Then Eve gets the following result.

$$\mathrm{U_e}|0\rangle|\mathcal{E}\rangle = \mathrm{a}|0\rangle|\mathcal{E}_{00}\rangle + \mathrm{b}|1\rangle|\mathcal{E}_{01}\rangle$$

$$\mathrm{U_e}|1\rangle|\mathcal{E}\rangle = \mathrm{c}|0\rangle|\mathcal{E}_{10}\rangle + \mathrm{d}|1\rangle|\mathcal{E}_{11}\rangle$$

where $|\mathrm{a}|^2 + |\mathrm{b}|^2 = |\mathrm{c}|^2 + |\mathrm{d}|^2 = 1$ and the four states, i.e., $|\mathcal{E}_{00}\rangle, |\mathcal{E}_{01}\rangle, |\mathcal{E}_{10}\rangle, |\mathcal{E}_{11}\rangle$ can be distinguished by Eve.

To prevent from the detection, the result of $\mathrm{U_e}|0\rangle|\mathcal{E}\rangle$ must be $|\mathrm{a}\rangle$, hence b = c = 0 and

$$\mathrm{a}|\mathcal{E}_{00}\rangle + \mathrm{d}|\mathcal{E}_{11}\rangle = 0$$

$$\mathrm{a}|\mathcal{E}_{00}\rangle = \mathrm{d}|\mathcal{E}_{11}\rangle$$

i.e., Eve has difficulty distinguishing between the states $|\mathcal{E}_{00}\rangle$ and $|\mathcal{E}_{11}\rangle$. Hence, no valuable information can be obtained by Eve. An error occurs because of Eve

$$\mathcal{E} = |b|^2 = |c|^2 = 1 - |a|^2 = 1 - |d|^2$$

So, this type of attack can be easily detected.

3.2.3. *Controlled not attack*

In this attack, Eve prepares a two-qubit ancilla state to copy the transmitted qubit by performing the CNOT gate in which the first and third qubit are control bits, and ancilla qubits are target bits. Nevertheless, in this type of attack, Eve could not get complete information of the cluster state because of checking particles.

3. Efficiency of Protocol

Using Cabello's definition, the efficiency of the BQSDC protocol is,

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

where *m* is the number of secret bits conveyed, *q* and *b* are the number of qubits used, and the number of classical bits, respectively. In this situation, the quantum and classical bits used in eavesdropping detection are ignored. The number of secret bits received in this case is 8, hence *m* = 8, the number of qubits used is 8, and the number of classical bits used in the final announcement is *b* = 4. As a result, the suggested protocol's quantum efficiency is 66.6 percent. Table 3 compares the proposed protocol to the prior method in terms of efficiency. It is self-evident that our protocol's efficacy is high with the maximum qubit transmission.

Table 3. Efficiency comparison of different protocols.

Protocols	Qubit transmitted	Efficiency (%)
Shi *et al.* [37]	4 bits	66.7
Gao *et al.* [44]	4 bits	40
Mohapatra *et al.* [46]	4 bits	33.33
Zhang *et al.* [47]	2 bits	50
Our protocol	8 bits	66.7

5. Conclusion

This paper has come up with an efficient bidirectional secure quantum communication protocol in which two authorized users can exchange 8-bit secret messages simultaneously using four qubit cluster states. Using dense coding and two security check, makes it more secure. Information leakage problems have been removed from it. The use of reversible quantum operation makes it a lesser amount of energy consumption and proves unconditionally secure. Finally, the security analysis ensures us about the security of our protocol against various attacks. The scheme is deterministic and secure.

References

1. C. H. Bennett and G. Brassard – *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (Bangalore, 1984) pp. 175–179.
2. A. Ekert. Phys. Rev. Lett. **67**, 661 (1991). https://doi.org/10.1103/PhysRevLett.67.661
3. C. H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992). https://doi.org/10.1103/PhysRevLett.68.557
4. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992). https://doi.org/10.1103/PhysRevLett.68.3121
5. A. Cabello, Phys. Rev. Lett. **85**, 5635 (2000). https://doi.org/10.1103/PhysRevLett.85.5635
6. T. Yan and F. Yan, Chin. Sci. Bull. **56**, 24 (2011). https://doi.org/10.1007/s11434-010-4208-y
7. Z. J. Zhang, Phys. Lett. A **342**, 60 (2005). https://doi.org/10.1016/j.physleta.2005.05.049
8. C. R. Hsieh, C. W. Tasi, and T. Hwang, Commun. Theor. Phys. **54**, 1019 (2010). https://doi.org/10.1088/0253-6102/54/6/13
9. G. L. Long and X. S. Liu, Phys. Rev. A 65, ID 0323302 (2002). https://doi.org/10.1103/PhysRevA.65.032302
10. F. G. Deng, G. L. Long, and X. S. Liu, Phys. Rev. A **68**, ID 042317 (2003). https://doi.org/10.1103/PhysRevA.68.042317
11. F. G. Deng and G. L. Long, Phys. Rev. A **69**, ID 052319 (2004). https://doi.org/10.1103/PhysRevA.69.052319
12. A. D. Zhu, Y. Xia, Q. B. Fan, and S. Zhang, Phys. Rev. A **73**, ID 022338 (2006). https://doi.org/10.1103/PhysRevA.73.022338
13. W. Tie-Jun, L. Tao, D. Fang-Fang, D. Fu-Guo, Chin. Phys. Lett. **28**, ID 040305 (2011). https://doi.org/10.1088/0256-307X/28/4/040305
14. K. J. Bostrom, T. Felbinger, Phys. Rev. Lett. **89**, ID 187902 (2002). https://doi.org/10.1103/PhysRevLett.89.187902
15. H. Yuan, Q. Zhang, L. Hong, W. J. Yin, D. Xu, and J. Zhou, Int. J. Theor. Phys. **53**, 2558 (2014). https://doi.org/10.1007/s10773-014-2053-5
16. L. Z. Yu, T. Wu, Acta Photonica Sin. 42(5), 623 (2013)
17. L. Dong, H. K. Dong, X. M. Xiu, Y. J. Gao, and F. Chi, Int. J. Quant. Inf. **7**, 645 (2009). https://doi.org/10.1142/S021974990900533X
18. C. W. Tsai, C. R. Hsieh, and T. Hwang, Eur. Phys. J. **D61**, 779 (2011). https://doi.org/10.1140/epjd/e2010-10189-8
19. K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zellinger, Phys. Rev. Lett. **76**, 4656 (1996). https://doi.org/10.1103/PhysRevLett.76.4656
20. A. K. Pati, P. Parashar, and P. Agrawal, Phys. Rev. A **72**, ID 012329 (2005).
21. R. Laurenza, C. S. Lupo, S. Lloyd, S. Pirandola, Phys. Rev. Res. **2**, ID 023023 (2020). https://doi.org/10.1103/PhysRevResearch.2.023023
22. X. Y. Zheng and Y. X. Long, Acta Phys. Sin. **66**, 180303 (2017). https://doi.org/10.7498/aps.66.180303
23. J. Li, H. F. Jin, and B. Jing, Int. J. Theor. Phys. **51**, 2759 (2012). https://doi.org/10.1007/s10773-012-1151-5
24. L. L. Zhang, Y. B. Zhang, and Q. Y. Zhang, Int. J. Theor. Phys. **48**, 2971 (2009). https://doi.org/10.1007/s10773-009-0090-2
25. W. F. Cao, Y. G Yang, Q. Y. Wen, Sci. China Phys. Mech. Astron. **53**, 1271 (2010). https://doi.org/10.1007/s11433-010-3210-3
26. D. Wang and X. W. Zha, Chin. J. Quant. Elect. **28**, 687 (2011).
27. J. Li, D. J. Song, X. J. Guo, and B. Jing, Chin. Phys. C **36**, 31 (2012). https://doi.org/10.1088/1674-1137/36/1/005
28. B. A. Nguyen, Phys. Lett. A, **328**, 6 (2004). https://doi.org/10.1016/j.physleta.2004.06.009
29. Z. J. Zhang and Z. X. Man, Quant. Phys. (2004). https://arxiv.org/abs/quant-ph/0403215
30. X. Ji and S. Zhang, Chin. Phys. **15**, 1418 (2006). https://doi.org/10.1088/1009-1963/15/7/005
31. Z. X. Man and Y. J. Xia, Chin. Phys. Lett. **23**, 1680 (2006). https://doi.org/10.1088/0256-307X/23/7/007

32. Y. Chen, Z. X. Man, and Y. J. Xia, **24**, 19 (2007). https://doi.org/10.1088/0256-307X/24/1/006
33. 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
34. Y. G. Yang and Q. Y. Wen, Sci. China Ser. Phys. Mech. Astron. **50**, 558 (2007). https://doi.org/10.1007/s11433-007-0057-3
35. F. Gao, F. Z. Guo, Q. Y. Wen, and F. C. Zhu, Sci. China Ser. Phys. Mech. Astron. **51**, 559 (2008). https://doi.org/10.1007/s11433-008-0065-y
36. Y. G. Tan and Q. Y. Cai, Int. J. Quant. Inf. **6**, 325 (2008).
37. G. F. Shi, X. Q. Xi, X. L. Tian, and R. H. Yue, Optic Communicat. **282**, 2460 (2009). https://doi.org/10.1016/j.optcom.2009.02.062
38. A. H. Yin, Z. H. Tang, and D. Chen, Mod. Phys. Lett. B **29** (2015). https://doi.org/10.1142/S0217984915500189
39. Z. Liu and H. Chen, Mod. Phys. Lett. A **34**, 1950241 (2019). https://doi.org/10.1142/S0217732319502419
40. Z. H. Liu and H. W. Chen, Int. J. Theor. Phys. **57**, 311 (2018). https://doi.org/10.1007/s10773-017-3563-8
41. M. L. Wang, W. P. Ma, D. S. Shen, and L. L. A. Wang, Int. J. Theor. Phys. **54**, 1388 (2015). https://doi.org/10.1142/S0217732319502419
42. T. Y. Ye, Quant Inf. Process. **14**, 1487 (2015). https://doi.org/10.1007/s11128-015-0919-y
43. Y. Chang, S. B. Zhang, and L. L. Yan, Chin. Phys. Lett. **30**, ID 090301 (2013). https://doi.org/10.1088/0256-307X/30/9/090301
44. G. Gao and L. P. Wang, Commun. Theor. Phys. **54**, 447 (2010). https://doi.org/10.1088/0253-6102/54/3/13
45. G. Gao, Int. J. Theor. Phys. **53**, 2282 (2014). https://doi.org/10.1007/s10773-014-2028-6
46. A. K. Mohapatra and S. Balakrishnan, Quant. Inf. Process. **16**, 1 (2017). https://doi.org/10.1007/s11128-017-1598-7
47. L. Zhang, S. Dong, K. -J. Zhang, H. -W. Sun, Int. J. Theor. Phys. **58**, 1927 (2019). https://doi:10.1007/s10773-019-04087-7
48. W. Li, X. W. Zha, and Y. Yu, Int. J. Theor. Phys. **57**, 371 (2018) https://doi.org/10.1007/s10773-017-3569-2
49. Z. Liu and H. Chen, Int. J. Theor. Phys. **59**, 2120 (2020). https://doi:10.1007/s10773-020-04485-2
50. N. Das and G. Paul, Int. J. Quant. Inf. **18**, ID 2050038 (2020). https://doi.org/10.1142/S0219749920500380
51. Z. M. Huang and H. Z. Situ, Quant. Inf. Process. **18**, 16 (2019). https://doi.org/10.1007/s11128-018-2152-y
52. Z. H. Liu and H. W. Chen, Quant. Inf. Process. **20**, 93 (2021). https://doi.org/10.1007/s11128-018-2152-y
53. A. Banerjee, C. Shukla, K. Thapliyal, A. Pathak, P. K. Panigrahi, Quant. Inf. Process. **16**, 49 (2017). https://doi.org/10.1007/s11128-016-1508-4
54. H. Wang, Y. Zhang, G. Wu, and H. Ma, Chin. J. Electronics **27,** 270 (2018). https://doi.org/10.1049/cje.2018.01.010
55. Y. -G. Yang, S. Gao, Y. -H. Zhou, W. -M. Shi, Int. J. Theor. Phys. **58**, 2810 (2019). https://doi.org/10.1007/s10773-019-04165-w
56. H. Briegel and R. Raussendorg,. Phys. Rev. Lett. **86**, 910 (2001).
57. R. Raussendorg and H. A. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
58. S. Murlidharan, S. Jain, and P.K. Panigrahi, Quant. Phys. (2010). https://arxiv.org/abs/0904.0563
59. S. Muralidharan, S. Jain, S. E. Prasath, P. K. Panigrahi, Quant. Phys. (2009). https://arxiv.org/abs/0906.2147