Absolutely secure distributed superdense coding: entanglement requirement for optimality

Sagnik Dutta1 ©, Asmita Banerjee2 and Prasanta K Panigrahi1 ©

1 Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata; Mohanpur, West Bengal 741246, India
2 Narula Institute of Technology, Agarpara, Kolkata, West Bengal 700109, India

E-mail: sagnikdutta17@gmail.com, asmibanerjee42@gmail.com and pprasanta@gmail.com

Keywords: superdense coding, GHZ state, quantum communication

Abstract

Superdense coding uses entanglement as a resource to communicate classical information efficiently through quantum channels. A superdense coding method is optimal when its capacity reaches Holevo bound. We show that for optimality, maximal entanglement is a necessity across the bipartition of Alice and Bob, but neither absolute nor genuine multipartite entanglement is required. Unlike the previous schemes, which can transmit either even or odd bits of information, we demonstrate a generalized dense coding protocol using the genuine multipartite entangled GHZ state to send arbitrary information bits. Expressed in the eigenbasis of different Pauli operators, GHZ state is characterized by a unique parity pattern which enables us to formulate a security checking technique to ensure absolute security of the protocol. We show this method is better applicable in a scenario, where the initial information is distributed among spatially separated parties. Finally, optimizing the number of qubit(s) sent to Bob, we construct a distributed dense coding method, which completely depicts absolutely secure quantum communication between many to one party.

1. Introduction

Quantum communication [1] is known to provide unparalleled level of security and speedup as opposed to its classical counterpart. It uses the unique features of quantum mechanics such as entanglement [2, 3], steering [4], quantum discord [5] and no cloning theorem [6] to its advantage, which is not achievable through classical communication. Superdense coding [7–10] and quantum teleportation [11–14] are the two most widely studied processes in this respect. These two share a close relationship in terms of using quantum resource like entanglement. While quantum teleportation transfers information between two parties using a distributed entangled state and a classical channel, superdense coding transfers classical information encoded in quantum mechanical bits using a distributed entangled state and a quantum channel.

In the last two decades, Quantum Secure Direct Communication (QSDC) [15–22] has emerged as one of the important branches of quantum cryptography [23–25]. QSDC protocols using superdense coding provides security against eavesdropping with high channel capacity. Where QSDC protocols ensure the security superdense coding maximizes the channel capacity. After Bennett and Wiesner [7] demonstrated the superdense coding protocol to send two bits of information using EPR pair, various multipartite entangled states like Greenberger-Horne-Zeilinger (GHZ) state [26, 27], W states [28], cluster state [29], Brown state [8] was shown to successfully accomplish it. Generalized superdense coding has been done to send even number of bits 2N of information using N EPR pairs [30]. Saha and Panigrahi [31] proposed a generalized protocol for odd number of bits (2N + 1) of information using a GHZ states and (N − 1) EPR pairs.

Here, entanglement is used as a resource [32] which provides the quantum advantage in terms of qubits sent for sending the classical information as well as the security of this communication protocol. It is then required to inquire about the precise requirement of entanglement in the process. Since entanglement is the main resource behind all these communication protocols, detailed and extensive study of the same is an active research field [33, 34]. Till now, entanglement classes upto four qubits [35–39] are completely documented. As the number of
qubits increases, degrees of freedom for local quantum subsystems increase as well [40–43] and that makes our understanding of multipartite entanglement limited. Absolute maximally entangled (AME) [44–46] states are those multipartite states that have maximal entanglement across all bipartitions. When a multipartite state is not necessarily maximally entangled but non-separable across all bipartitions, one considers them as genuine multipartite entangled (GME) states. The requirement of these AME or GME states are yet to be analized in the context of superdense coding, which may also be achievable using mixed entangled states. However, that will never be optimal [47] because a N partite mixed state can be considered as a reduced state of a (N + 1) partite pure entangled state. The other scenario of superdense coding, where the information is distributed among different senders and they want to send it to one particular receiver is known as the distributed superdense coding. It is known that the information is possible to send to the receiver only by applying local operations, without reducing the channel capacity [48–50]. However, there does not exist any efficient method yet to do so.

In section 2, we prove that optimized superdense coding using two qubits can take place only on AME states. For more than three qubit systems, neither AME nor GME states are required for optimal dense coding, but maximal entanglement across the bipartition of Alice and Bob is a necessity. Section 3 briefly describes the superdense coding protocol for even bits of information using a N-separable state. In section 4, we demonstrate a complete generalized version of superdense coding using the genuine multipartite entangled (GME) [51, 52] N qubit GHZ state. Using the particular pattern present in GHZ state while written in different eigen basis of Pauli operators we provide a security checking protocol at ideal conditions in section 5. Using this present generalized scheme we formulate the new distributed dense coding technique D(N, k) in section 6 optimizing over the number of qubits to send to Bob and the number of parties initial information is distributed. We also show that the capacity of all these protocols reache Holevo bound, making them optimal. In section 7, we state the benefits of D(N, k) in comparison to other similar protocols using superdense coding.

2. Entanglement requirement for generalized superdense coding

A pure state consisting n qudits of dimension d, |ψ⟩ ∈ C_d^n can be considered as a AME state iff every bipartition of the system such as A and B with m = |B| ≤ |A| = n − m, is strictly maximally entangled i.e., S(ρ_B) = m log_2 d.

As a consequence, for each bipartition the reduced density matrix of subsystem B must be of the form:

\[ ρ_B = Tr_A |ψ⟩⟨ψ| = \frac{I_d}{d^m}, \quad 0 < m \leq \frac{n}{2}. \]  

(1)

Total number of AME states are quite limited. There does not exist any AME state for four, seven or more qudits. Similar to AME, a pure GME state is a pure state, for which each bipartition of the system such as A and B with m = |B| ≤ |A| = n − m, is strictly maximally entangled i.e., S(ρ_B) > 0 ∀ 0 < m ≤ \( \frac{n}{2} \).

While sending N bit information through superdense coding, Alice operates a combination of four possible operations \{I, σ_X, σ_Y, iτ_Y\} on her qubits to encode the message. That generates 2^N mutually orthogonal states which Bob measures and identifies the message. Suppose, Alice possess |A| number of qubits, then maximum number of different states she can prepare is 4^|A|. For the protocol to be ‘optimal’ i.e., to reach its maximal capacity it must satisfy:

\[ 4^{|A|} ≥ 2^N \Rightarrow |A| \geq \frac{N}{2}. \]

Hence, to show entanglement requirement, we only need to focus on Bob’s reduced subsystem.

The capacity (X) of any particular superdense coding protocol [53, 54] using given shared state (ρ_{AB}) is given as:

\[ X(ρ_{AB}) = \log_2 d_A + S(ρ_B) - S(ρ_{AB}), \]

(3)

where d_A is the dimension of Alice’s subsystem and ρ_B is the reduced state of Bob. A superdense coding protocol is considered ‘optimal’ when its capacity is maximum i.e., it reaches the Holevo bound. Therefore, to optimize the protocol we must use such a state that maximizes X hence S(ρ_B). From equation (3), it is evident that no mixed state can be used to get an optimized scheme because S(ρ_{AB}) is minimum only for pure states. Suppose Bob possesses |B| qubits then from equation (2), |B| ≤ \( \frac{N}{2} \leq |A| \). To maximize S(ρ_B), the reduced density matrix of Bob (dimension d_B) must yield maximal entropy. That can only happen when,

\[ ρ_B = \frac{I_{d_B}}{d_B}, \quad 2 \leq d_B = 2^{|B|} \leq 2^N. \]

(4)

For any bipartite two qubit system Bob can only have one qubit with the marginal state \( \frac{I_{d_B}}{d_B} \). Using Schmidt decomposition, any two qubit pure state χ can be written as χ = \( \sum_{i=0}^{l} \lambda_i |a_i⟩⟨b_i| \), where \{ |a_i⟩ \} and \{ |b_i⟩ \} are sets of orthogonal basis vectors for the subsystem of Alice and Bob respectively. This Schmidt decomposed form of χ also yields the reduced state of Alice and Bob as ρ_A = \( \sum_{i=0}^{l} \lambda_i |a_i⟩⟨a_i| \) and ρ_B = \( \sum_{i=0}^{l} \lambda_i |b_i⟩⟨b_i| \). For
maximally mixed $\rho_B$, we get $\lambda_0 = \lambda_1 = \frac{1}{2}$ for any chosen basis $\{|b_i\rangle\}$. Hence, the reduced state of Alice becomes $\rho_A = \frac{1}{2} (|a_0\rangle \langle a_0| + |a_1\rangle \langle a_1|)$, which is exactly $I/2$ for the chosen basis $\{|a_i\rangle\}$ for Alice. So, the state $\chi$ must be a maximally entangled state. It implies that AME condition is a necessity to apply superdense coding using two qubits.

As we increase the number of qubits used in the dense coding protocol, entanglement requirement changes. From condition 4, we can conclude that across the bipartition of Alice and Bob, maximal entanglement is necessary for optimized superdense coding to happen. We note that equation (4) does not impose any condition across other bipartitions. It is not required for a state to be AME or even GME state to perform this protocol successfully. Any biseparable, triseparable or even $N$-separable state can be used, ensuring that across Alice and Bob’s bipartition, the state is maximally entangled.

If one try to make the dense coding scheme secure, one should have an entanglement criteria for Alice’s subsystem. For getting a absolutely secure protocol using dense coding, the marginal state of Alice must be a GME state. If it is not the case then we can write $\rho_A$ as:

$$\rho_A = \sum_i \rho_i \left( \begin{array}{ccc} a_{i1} & \cdots & a_{im} \\ a_{m1} & \ddots & \vdots \\ \vdots & \ddots & a_{mn} \end{array} \right) \otimes \left( \begin{array}{ccc} b_{i1} & \cdots & b_{im} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{array} \right)_{m \times n},$$

with $m + n = |A|$. This implies that the state is separable across those $m$ qubits versus rest bipartition. While sending those $m$ qubits to Bob, Eve can manage to have access to all of those. Whatever the decoding scheme of Bob be for those $m$ qubits, Eve can always apply the same and get the classical information encoded within those $m$ qubits. Hence, the protocol will not remain completely secure.

3. Generalized dense coding using $N$-separable states

In this section, we briefly outline a generalized superdense coding protocol to transfer even $(2N)$ bits of information. For this scheme, first proposed by Rigolin et al [30], following $N$-separable $2N$ qubit state is used:

$$|\psi_{2N}\rangle = |\phi^+\rangle_{AB}^{\otimes N}; \quad |\phi^+\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle).$$

The first qubit of each $|\phi^+\rangle$ of this product state of $N$ Bell states belongs to Alice and the other one to Bob. Alice encodes exactly two bits of classical information on each of her qubits by applying $\{|I, \sigma_X, \sigma_Y, i\sigma_Y\}$ for the bit strings $\{00, 01, 10, 11\}$ respectively and sends her qubits to Bob. Finally, Bob makes a Bell measurement on each of the $N$ pairs. Thus, by sending only $N$ qubits to Bob, she manages to transfer $2N$ bits of information.

Here, $|\phi^+\rangle$ being a maximally entangled state, both particles have a reduced state $I/2$. That makes the marginal state of the subsystems of both Alice and Bob $\rho_A = \rho_B = |\phi^+\rangle_{AB}^{\otimes N} = \frac{I_{2N}}{2}$, which ensures the presence of maximal entanglement between Alice and Bob despite $|\psi_{2N}\rangle$ being a $N$-separable state. It also makes sure that the protocol remains safe from eavesdropping. Each qubit sent by Alice, being maximally mixed Eve cannot extract any information from them, even if she has access to all of them.

4. Generalized dense coding using genuinely entangled GHZ states

Previously, we illustrated an example of a superdense coding protocol to communicate even bit of information through an $N$-separable quantum channel. In this section, we provide a completely generalized new scheme of dense coding, showing that GME states like generalized GHZ states can be safely used as a dense coding channel with an absolute security checking method. First, we show the protocol using three qubit GHZ state and then based on that scheme we generalize it.

4.1. Three qubit GHZ state protocol

Since entanglement is necessary for efficient communication of any information, we consider the maximally entangled tripartite GHZ state $|\psi_3\rangle = 1/\sqrt{2} (|000\rangle + |111\rangle)_{AAB}$ distributed among the two parties Alice and Bob. Here, the first two qubits belongs to Alice (denoted by subscript $A_1$ and $A_2$) and one to Bob (denoted by subscript $B$). Alice now applies suitable unitary transformations on her qubits, according to the classical information she wants to send. She chooses her unitary operations from the set $\{I, \sigma_X, \sigma_Y, i\sigma_Y\}$ and generates 16 states out of which 8 states will be mutually orthogonal. After Alice sends her qubits to Bob, he then performs a tripartite measurement in that GHZ basis to distinguish them uniquely and get the encoded information. The list of all unitary transformations Alice does to encode the information message and the respective states obtained are demonstrated in the following table (table 1). Here, all the eight states generated through Alice’s operation are orthogonal to each other and hence forms the measurement basis for Bob. From the above table
When To avoid the repetition of obtaining same state from different operations, we let Alice to have 4 choices for three qubit protocol, here Alice chooses the unitary operation for her first qubit, whereas for the rest of her qubits, she is left to choose any one from \{I, \sigma_Z, \sigma_Y\} unbiasedly and without any restriction. Then to obtain all unique states and to avoid the repetition of obtaining same state from different operations, she is left with only two choices for her second qubit. Those must be any one from \{I, \sigma_Z\} and any one from \{\sigma_X, \sigma_Y\}. Here, we choose them to be I and \sigma_X.

### 4.2. Generalized protocol

Using the previous technique applied for three qubit superdense coding, we generalize the concept for N qubits. For that we consider generalized N qubit GHZ state given as:

$$|\psi_N\rangle = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})_{\sigma_{N-1}\cdots \sigma_2\sigma_1 \forall N \in \mathbb{N} - \{1\}}. \tag{7}$$

where first \(N - 1\) qubits belong to Alice and the last one qubit to Bob. Similarly, the unitary operation choice for three qubit protocol, here Alice chooses the unitary operation for her first qubit from the set \{I, \sigma_X, \sigma_Z, \sigma_Y\} unbiasedly and for the rest of her qubits, she is left to choose any one from \{I, \sigma_Z\} and also any one from \{\sigma_X, \sigma_Y\}. Hence, we can write Alice’s operation choice as:

$$\mathcal{P} \otimes Q^{N-2} | \mathcal{P} \in \{I, \sigma_X, \sigma_Z, \sigma_Y\}, Q \in \{I/\sigma_Z, \sigma_X/\sigma_Y\}. \tag{8}$$

To avoid the repetition of obtaining same state from different operations, we let Alice to have 4 choices for first qubit, whereas for the rest of the N - 2 qubits, Alice has only 2 choices each. So, total available unitary operations for Alice is \(4 \times 2^{N-2} = 2^N\) and by applying them on first \(N - 1\) qubits of \(|\psi_N\rangle\), Alice will get \(2^N\) different states. Now, superdense coding is possible only if these \(2^N\) states become mutually orthonormal to each other. To prove orthonormality condition, we consider two general unitary operators \(\mathcal{M} = \mathcal{P}' \otimes Q_k^{N-1}\) and \(\mathcal{N} = \mathcal{P}'' \otimes Q_k^{N-1}\) acting on \(|\psi_N\rangle\). Taking inner product of these two states we get:

$$\langle \mathcal{M}|\psi_N\rangle' \langle \mathcal{N}|\psi_N\rangle = \left[\mathcal{P}' \otimes Q_k^{N-1} \frac{1}{\sqrt{2}} (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})\right] \left[\mathcal{P}'' \otimes Q_k^{N-1} \frac{1}{\sqrt{2}} (|0\rangle^{\otimes N} + |1\rangle^{\otimes N})\right]$$

$$= \frac{1}{2} \langle 0|\mathcal{P}'|0\rangle \otimes \langle 0|Q_k^{N-2}|0\rangle + \langle 1|\mathcal{P}'|1\rangle \otimes \langle 1|Q_k^{N-2}|1\rangle + \langle 0|\mathcal{P}''|0\rangle \otimes \langle 0|Q_k^{N-2}|0\rangle + \langle 1|\mathcal{P}''|1\rangle \otimes \langle 1|Q_k^{N-2}|1\rangle.$$

The following relations hold for Pauli operators:

$$\langle 0|0\rangle = \langle 1|1\rangle = \langle 0|\sigma_Z|0\rangle = 1, \quad \langle 1|\sigma_Z|1\rangle = -1,$$

$$\langle 0|\sigma_X|0\rangle = \langle 1|\sigma_X|1\rangle = \langle 0|\sigma_Y|0\rangle = \langle 1|\sigma_Y|1\rangle = 0. \tag{10}$$

When \(\mathcal{M} = \mathcal{N}, \mathcal{P}' = \mathcal{P}''\) and \(Q_k^{N} = Q_k^{N} \forall k.\) This immediately leads to get \(\mathcal{P}'\mathcal{P}'' = Q_k^{N}Q_k^{N} = I \forall k.\)

Therefore, using the relations of equation (10), equation (9) becomes:

\[\text{Table 1. State obtained by Alice after applying suitable unitary operation (The coefficient } \frac{1}{\sqrt{2}} \text{ along with any global phase is removed for convenience.)}\]

| Message | Unitary Operation | Alternate Operation | State       |
|---------|------------------|---------------------|-------------|
| 000     | I ⊗ I            | σ_Z ⊗ σ_Z          | 000 + 111   |
| 001     | I ⊗ σ_X          | σ_Z ⊗ iσ_Y         | 010 + 101   |
| 010     | σ_X ⊗ I          | iσ_Y ⊗ σ_Z         | 010 - 011   |
| 011     | σ_X ⊗ σ_X        | iσ_Y ⊗ iσ_Y        | 110 + 001   |
| 100     | σ_Z ⊗ I          | I ⊗ σ_Z            | 000 - 111   |
| 101     | σ_Z ⊗ σ_X        | I ⊗ iσ_Y           | 010 - 011   |
| 110     | iσ_Y ⊗ σ_X       | σ_Y ⊗ σ_Z          | 100 - 011   |
| 111     | iσ_Y ⊗ iσ_Y      | σ_X ⊗ iσ_Y         | 110 - 001   |
\[ [\mathcal{M}|\psi_N]\} \} \} \} \} \} \} [\mathcal{N}|\psi_N]\] \\
= \frac{1}{2} [(0|0) \otimes (0|0) \otimes \cdots \otimes (0|0) + \langle 1|1\rangle \otimes \langle 1|1\rangle \otimes \cdots \otimes \langle 1|1\rangle ] \\
= \frac{1}{2} [1 + 1] = 1. \quad (11)

For the other condition \( \mathcal{M} = \mathcal{N} \) we consider the following two cases as:

**Case 1:** Suppose \( \mathcal{P}' = \mathcal{P}'' \) then for \( \forall i \in [1, 2, \cdots, N-2] \) s.t. \( Q'_{i} \neq Q''_{i} \). Hence, it follows that \( Q'_{i} \otimes Q''_{i} = \pm \sigma_{X} / i\sigma_{Y} \). Hence, equation (9) becomes:

\[
[\mathcal{M}|\psi_N]\} \} \} \} \} \} [\mathcal{N}|\psi_N]\] \\
= \frac{1}{2} [(0|0) \otimes \cdots \otimes (0|0) \otimes \cdots \otimes (0|0) Q'_{N-2} Q''_{N-2} |0\rangle + \langle 1|1\rangle \otimes \cdots \otimes \langle 1|1\rangle \otimes \cdots \otimes \langle 1|1\rangle ] \\
= \frac{1}{2} [10 + 01] = 0. \quad (12)

**Case 2:** When \( \mathcal{P}' \neq \mathcal{P}'' \) if \( \forall i \in [1, 2, \cdots, N-2] \) such that \( Q'_{i} \neq Q''_{i} \) then equation (9) identically vanishes just like equation (12). If \( Q'_{k} = Q''_{k} \forall k \), then for \( \mathcal{P}' \neq \mathcal{P}'' = \pm \sigma_{X} / i\sigma_{Y} \) equation (9) again vanishes too. Now, when \( \mathcal{P}' \neq \mathcal{P}'' = \pm \sigma_{X} \) then equation (9) becomes:

\[
[\mathcal{M}|\psi_N]\} \} \} \} \} [\mathcal{N}|\psi_N]\] \\
= \frac{1}{2} [(0|0) \otimes \cdots \otimes (0|0) \otimes \cdots \otimes (0|0) + \langle 1|1\rangle \otimes \cdots \otimes \langle 1|1\rangle \otimes \cdots \otimes \langle 1|1\rangle ] \\
= \frac{1}{2} [1 - 1] = 0. \quad (13)

Hence, from equations (11), (12), (13), one finds that all the \( 2^{N} \) generated states are orthonormal to each other and they can be used for superdense coding of any \( N \) bit classical information.

Although the encoding of this classical information through Alice’s operation need not have any unique technique, we provide an efficient scheme of encoding. First qubit operation \( \mathcal{P} = I, \sigma_{X}, \sigma_{Z}, i\sigma_{Y} \) corresponds those information consisting 00, 01, 10, 11, respectively at leftmost 2 bits. For the remaining operations \( Q = I / \sigma_{Z}, \sigma_{X} / i\sigma_{Y} \) on ith qubit will correspond 0, 1 bit respectively at \( (i+1) \)-th place of the total information string. For example, a five qubit information ‘10110’ will be encoded by the unitary operator \( \sigma_{Z} \otimes \sigma_{X} \otimes \sigma_{X} \otimes I \) or \( \sigma_{Z} \otimes \sigma_{X} \otimes \sigma_{X} \otimes \sigma_{Z} \) or \( \sigma_{Y} \otimes \sigma_{Y} \otimes i\sigma_{Y} \otimes I \) or \( \sigma_{X} \otimes i\sigma_{Y} \otimes i\sigma_{Y} \otimes \sigma_{Z} \) as per the choice of Alice.

In the following, we show that this generalized protocol is optimal. For a \( N \) qubit system its dimension is \( d = 2^{N} \). Holevo bound for any such channel is \( H = \log_{2} d = N \). Here, Alice possesses \( N-1 \) qubits while 1 qubit belongs to Bob. Therefore, the dimension of Alice’s subsystem is \( d_A = 2^{N-1} \). Generalized GHZ state is a GME state having a marginal state \( I/2 \) for each of its qubits. This fact ensures that Alice’s and Bob’s subsystems are maximally entangled making the entropy of Bob’s marginal maximum. Also, \( |\psi_N\rangle \) being a pure state possesses zero entropy. Hence, from equation (3) we get the capacity of the channel as \( X = \log_{2} 2^{N-1} + S(\rho_B = \frac{1}{2}) - S(|\psi_N\rangle \langle \psi_N|) = (N - 1) + 1 - 0 = N \), which is exactly same as the Holevo bound.

## 5. Security analysis

### 5.1. Different measurement basis for Alice and Bob

Interestingly, the two qubit Bell state (|\psi^\rangle\rangle) and three qubit GHZ state can be written in \( \{|+\rangle, |\rangle \rangle \} \) basis as:

\[
|\psi_2\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|++\rangle + |--\rangle). \quad (14)
\]

\[
|\psi_3\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle) = \frac{1}{\sqrt{2}} (|++++\rangle + |-----\rangle + |++--\rangle + |--++\rangle). \quad (15)
\]

One notices that all GHZ states written in \( \{|+\rangle, |\rangle \rangle \} \) basis are superposition of all possible terms that contain even number of \( |\rangle \rangle \) states. In general \( N \) qubit GHZ state can be written as:

\[
|\psi_N\rangle = \frac{1}{\sqrt{2}} (|0\rangle\rangle^{\otimes N} + |1\rangle\rangle^{\otimes N})_{A_1 \cdots A_N, B} \quad (16)
\]

\[
|\psi_N\rangle = \frac{1}{\sqrt{2^{N+1}}} \sum_{a_1, \cdots, a_N = 0}^{1} \left( \begin{array}{c} a_1 \cdots a_N \\ a_1 \cdots a_N \end{array} \right)_{A_1 \cdots A_N, B} \quad (17)
\]
where, \(|a_i = 0\rangle = \langle +\rangle\) and \(|a_i = 1\rangle = \langle -\rangle\). Alice and Bob can utilize this different basis measurement technique for security analysis. First, Bob can measure in computational basis i.e. in \(|0\rangle, |1\rangle\) basis and we denote this choice as BMB\(_1\) (Bob’s measurement choice 1). Correspondingly, Alice’s computational basis choice will be denoted by AMB\(_1\). On the other hand, if the state is measured as equation (17) then both AMB\(_2\) and BMB\(_2\) are \(|\langle +\rangle, |-\rangle\rangle\). Using these two choices, Alice and Bob can construct a strategy to check for eavesdropping in the quantum channel.

### 5.2. Eavesdropping check

From a sufficiently large set of same states \(|\psi_N\rangle\) distributed among Alice and Bob, Bob randomly chooses some of the states as a sample set to check whether Eve has anyhow altered the original state. He then measures his qubit either in BMB\(_1\) or in BMB\(_2\) and accordingly tells Alice about his measurement choice along with the corresponding outcome. For computational basis measurements (BMB\(_1\) and AMB\(_1\)) Alice’s outcome must collapse into \(|0\rangle^{\otimes N-1} \text{ or } |1\rangle^{\otimes N-1}\rangle\) according to his outcome \(|0\rangle\text{ or } |1\rangle\). When Bob measures in BMB\(_2\) and gets \(|\langle +\rangle\rangle\text{ then the outcome of AMB}\(_2\) must be a state which contains even number(s) of \(|-\rangle\text{ and for } |\langle -\rangle\rangle\text{ outcome of BMB}\(_2\) Alice must get odd number(s) of \(|-\rangle\text{ as outcome of AMB}\(_2\). Finally, they check their corresponding outcomes and if for majority of the chosen states those remain consistent then they can securely use the remaining states for communication. Otherwise, the channel is corrupted and they need to abort further communication using them.

### 5.3. Complete security check

Suppose, Eve still has some strategy to get the secret message sent by Alice. In this section, we show that Eve can not apply any other successful method to get the secret message without getting caught.

In this protocol, Eve does not have access of all \(N\) qubits at the same time. After encoding the secret message, Alice physically sends her \(N-1\) qubits to Bob. If Eve attacks those qubits, it will not be possible for her to extract the \(N\) bit secret message completely by doing any kind of operations or measurement on those \(N-1\) qubits. So, her strategy will be to prepare some ancilla qubit \(|\xi\rangle\) to intercept the \(N\)-th qubit which belongs to Bob. Then, when the \(N-1\) qubits will be sent to Bob, she might capture those and make a joint measurement on those qubits along with her ancilla to get the secret information. Before Alice and Bob are engaged in the protocol let Eve operate some unitary operation \(U\) on Bob’s qubit and her ancilla qubit \(|\xi\rangle\). In most general form, we can write the operations as:

\[
U: |0\rangle_i |\xi\rangle_E \rightarrow |0\rangle_i |\xi_0\rangle + |1\rangle_i |\xi_1\rangle_E \\
|1\rangle_i |\xi\rangle_E \rightarrow |0\rangle_i |\xi_0\rangle + |1\rangle_i |\xi_1\rangle_E
\]  

(18)

where, \(|\xi_i\rangle\) for \(i, j \in [0, 1]\) are ancilla states of Eve, completely determined by the unitary operation \(U\).

We now show that Eve fails to get any information for any \(N\) qubit GHZ state. After Eve’s interaction with Bob’s qubit, the generalized state takes the form:

\[
|\psi_N^i\rangle = \frac{1}{\sqrt{2}} (|0\rangle^{\otimes N-1} |0\rangle |\xi_0\rangle + |1\rangle^{\otimes N-1} |0\rangle |\xi_1\rangle + |1\rangle^{\otimes N-1} |1\rangle |\xi_1\rangle)_{A_1, \ldots, A_m, \cdot E}\]

\[
= \frac{1}{\sqrt{2}} (|\eta_1\rangle |0\rangle + |\eta_2\rangle |1\rangle)_{A_1, \ldots, A_m, \cdot E}
\]

(19)

where,

\[
|\eta_1\rangle_{A_1, \ldots, A_m, \cdot E} = (|0\rangle^{\otimes N-1} |\xi_0\rangle + |1\rangle^{\otimes N-1} |\xi_1\rangle)
\]

\[
|\eta_2\rangle_{A_1, \ldots, A_m, \cdot E} = (|0\rangle^{\otimes N-1} |\xi_0\rangle + |1\rangle^{\otimes N-1} |\xi_1\rangle)
\]

(20)

As Bob measures in BMB\(_1\), Alice’s outcome for AMB\(_1\) must be \(|0\rangle^{\otimes N}\text{ or } |1\rangle^{\otimes N}\rangle\) according to Bob’s outcome. The conditions for Eve to remain undiscovered while eavesdropping check by Alice and Bob must be,

\[
|\langle 1\rangle^{\otimes N-1} |\eta_1\rangle\rangle = (0^{\otimes N-1} |\eta_2\rangle) = 0
\]

(21)

Solving equations (20) and (21) we arrive at the following results,

\[
|\xi_0\rangle = |\xi_0\rangle = 0
\]

(22)

The generalized state after Eve’s action can be expressed in AMB\(_2\) and BMB\(_2\) as:

\[
|\psi_N^i\rangle = \frac{1}{\sqrt{2} N+1} (|\langle +\rangle + |\langle -\rangle\rangle^{\otimes N} |\xi_0\rangle + |\langle +\rangle - |\langle -\rangle\rangle^{\otimes N} |\xi_1\rangle)_{A_1, \ldots, A_m, \cdot E}
\]

\[
= \frac{1}{\sqrt{2} N+1} (|\phi_1\rangle |\langle +\rangle + |\phi_2\rangle |\langle -\rangle\rangle_{A_1, \ldots, A_m, \cdot E}
\]

(23)
where,
\[
\begin{align*}
|\phi_1\rangle &= |\psi_{N-1}\rangle (|\xi_{00}\rangle + |\xi_{11}\rangle) + |\tilde{\psi}_{N-1}\rangle (|\xi_{00}\rangle - |\xi_{11}\rangle)_{A_1\cdots A_{N-1}\text{-E}} \\
|\phi_2\rangle &= |\psi_{N-1}\rangle (|\xi_{00}\rangle - |\xi_{11}\rangle) + |\tilde{\psi}_{N-1}\rangle (|\xi_{00}\rangle + |\xi_{11}\rangle)_{A_1\cdots A_{N-1}\text{-E}}
\end{align*}
\]

Here, \( |\psi_{N}\rangle \) is defined in equation \((17)\) and \( |\tilde{\psi}_{N}\rangle = \frac{1}{\sqrt{2^{N-1}}} \sum_{a_0,\ldots,a_{N-1}=0}^{1} a_0\cdots a_{N-1} (|a_0\cdots a_{N-1}\rangle + (-1)^{a_0+\cdots+a_{N-1}} |a_0\cdots a_{N-1}\rangle)_{A_1\cdots A_{N-1}\text{-E}} \) with \( |a_i=0\rangle = |+\rangle \) and \( |a_i=1\rangle = |-\rangle \), Alice must obtain even (odd) number(s) of \( |-\rangle \), when she measures \( |\phi_{N}\rangle (|\tilde{\psi}_{N}\rangle) \) in AMB2. Hence, it must satisfy,
\[
\langle p_1p_2\cdots p_{N-1} \rangle |\phi_1\rangle = \langle q_1q_2\cdots q_{N-1} \rangle |\phi_2\rangle = 0 \text{ s.t. } \sum_{i=1}^{N-1} p_i = \text{even}, \sum_{i=1}^{N-1} q_i = \text{odd}
\]

With the condition \( |p_i, q_i=0\rangle = |+_\rangle \)\&\( |p_i, q_i=1\rangle = |-_\rangle \forall i\). From the construction it is evident that \( |\psi_{N}\rangle (|\tilde{\psi}_{N}\rangle) \) contains even (odd) number(s) of \( |-\rangle \). Solving equations \((24)\) and \((25)\) we arrive at the conclusion that,
\[
|\xi_{00}\rangle = |\xi_{11}\rangle.
\]

Applying the results of equations \((22)\) and \((26)\) in equation \((18)\), one obtains:
\[
U: |0\rangle_E |\xi_{i}\rangle_E \rightarrow |0\rangle_E |\xi_{i}\rangle_E \\
|1\rangle_E |\xi_{i}\rangle_E \rightarrow |1\rangle_E |\xi_{i}\rangle_E
\]

This clearly shows that the joint state of Bob and Eve will be a product state, as \(U\) is effectively a local unitary operation for Eve. As a result, we deduce that this protocol makes the process absolutely secure and effective under the assumption that the channel is not noisy and no information is getting lost within it.

### 6. Distributed superdense coding technique

As we compare the two dense coding protocols described in section 3 (Protocol 1) and 4.2 (Protocol 2), we notice that absolutely secure generalized superdense coding is possible using two complete different types of states, one \( N \)-separable and another GME state. The only common feature they both possess is that both of these states show maximal entanglement across the bipartition of Alice and Bob. Noticeably, protocol 1 is only applicable to transfer even bits of information whereas protocol 2 is applicable for any \( N \). In terms of the number of qubits needed to physically transfer from Alice to Bob, protocol 1 using \( N \)-separable states requires only \( N/2 \) \( (N \text{ even}) \) qubits which is much less (for \( N > 2 \)) compared to \( N-1 \) qubits for the other one. However, Protocol 2 using GHZ states is more beneficial in different type of scenarios. Suppose, the original \( N \) bit classical information is distributed among \( N-1 \) spatially separated parties and all of them wants to send it to Bob.

In this scenario (see figure 1), the proposed protocol 2 using generalized GHZ state will be the most efficient one. Since, all the unitaries operated to perform this protocol act only on individual qubits and no global multiqubit operations are required, therefore, all those \( N-1 \) qubits which are supposed to be with Alice, can...
now be distributed among those spatially separated $N - 1$ sender parties. Now, each of them would apply the operation according to the protocol and send their individual qubit to Bob. Only one party who has $2$ bits of information (as $N$ bit information is distributed among $N - 1$ parties) is able to operate all of those $4$ operation choices mentioned in section 4.2.

Immediate next question that arises is whether protocol 1 is applicable in this type of scenario. Noticing the structure of the state $|\psi_{2N}\rangle$ used in section 3, increasing just one more qubit to Alice’s part would result in Alice containing one complete EPR pair $|\phi^+\rangle$. That would make the marginal state of Alice of the form equation (5) and the protocol will not remain absolutely secure anymore. Therefore, protocol 1 must be carried out only by keeping $\frac{N}{2}$ to both the parties.

The number of parties among whom the initial information can be distributed may vary from 1 to $N - 1$. We provide a distributed superdense coding method optimizing the number of qubits transferred and number of senders by combining protocol 1 and 2. We define this distributed generalized dense coding scheme $D(N, k)$ where $N$ is the size of information bit and $1 \leq k \leq N - 1$ is the number of parties between whom the information is distributed. The quantum state required for this scheme is given by,

$$|\psi_{D(N, k)}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^\otimes k + |1\rangle^\otimes k)_{A_1...A_k, B} \otimes |\phi^+\rangle_{AB}^{\otimes \frac{N-k}{2}}; = \max (2, 2(k + 1) - N) \quad \forall N = \text{even}$$

$$|\psi_{D(N, k)}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^\otimes k + |1\rangle^\otimes k)_{A_1...A_k, B} \otimes |\phi^+\rangle_{AB}^{\otimes \frac{N-k}{2}}; = \max (3, 2(k + 1) - N) \quad \forall N = \text{odd}$$

When $k \leq \frac{N}{2}$, for even $N$ $|\psi_{D(N, k)}\rangle$ becomes exactly similar as $|\psi_{2N}\rangle$ of protocol 1 with $\tilde{N} = \frac{N}{2}$ EPR pairs. For odd $N$ it is a product state of one 3 qubit GHZ state and $\frac{N-3}{2}$ pairs of $|\phi^+\rangle$. When $k > \frac{N}{2}$, $|\psi_{D(N, k)}\rangle$ becomes a $(N - k)$-separable state containing $N - (k + 1)$ pairs of $|\phi^+\rangle$ and a GHZ state of $2(k + 1) - N$ qubits. All encoding technique for GHZ states will be like protocol 2 where, that for EPR pairs will follow protocol 1. For $k \leq \frac{N}{2}$ number of qubits belonging to Alice is always $\frac{N}{2}$, hence those qubits can be distributed among $k$ parties according to their information content. For $k > \frac{N}{2}$ total number of qubits Bob possess is $N - k$ (1 from GHZ part and $N - k - 1$ from EPR part). Therefore, the remaining qubits will be equally distributed among $k$ parties. If we notice Bob’s marginal state for $|\psi_{D(N, k)}\rangle$ it will be $\rho_B = I_2 \otimes I_2^{\otimes \frac{N-k}{2}}$, making their $D\left(\frac{N}{2}, k\right)$ optimal.

7. Benefits in comparison to other protocols

In order to send the $N$ bit information distributed among $k(1 \leq k \leq N - 1)$ different parties to Bob, other than using $D(N, k)$ they might create separate quantum channels between Bob and each one of them. Among those $k$ parties, those possessing $m(1 < m \leq N)$ bits of information will have to share $m$ qubits among that party and Bob. For those parties having only one bit of information must share a channel consisting 2 qubits. Then they might apply superdense coding according to protocol 1 to pass the total number of qubits Bob possesses. But in that case total required qubits will be $N + p$ qubits where $p$ is the number of parties possessing one bit information. For $k > \frac{N}{2}, p$ must be at least 1. Hence, that will require $p$ more qubits to complete the process which is optimal. As $k$ increases our method becomes more resource efficient compared to protocol 1.

Recently, Wu et al. [55] provided a private dense coding model of QSDC where they generalized the superdense coding using arbitrary dimension qudits. As they focused more to the reliability of the information received to Bob, chances of aborting the process becomes much higher there. Although our protocol also has moderate chance of aborting the process, but it is optimal when the process does not get aborted. Since, they use a bipartite model it is impossible to apply their method in distributed information scenario where our scheme works best. The main advantage of using generalized GHZ state is to avail the ability of having multiple senders keeping the security of the process intact. From experimental perspective, creating higher dimensional qudit systems and maintaining entanglement among them is much more difficult compared to that for qubit systems. Hence, our method gives an edge over their protocol in terms of application.

8. Conclusion

In conclusion, we have shown that for any superdense coding protocol using two qubit systems, maximal entanglement is necessary i.e., the state must be an AME state. For a general $N$ qubit system ($N > 2$) we established that Bob’s subsystem with dimension $d$ must have the maximally mixed marginal $I_d/d$, making their bipartition maximally entangled. This is the only condition required for optimal dense coding to happen. To
show that neither AME nor GME conditions are required we have briefly described a protocol to send even bit of information using an N-separable state. We then presented a new generalized dense coding technique to send a N bit classical information using genuinely entangled GHZ states. Later we provided a scheme to make this protocol completely secure from eavesdropper’s attack.

Furthermore, considering a different type of scenario where the initial information is split among different spatially separated parties, our method using GHZ state is the only applicable dense coding method known for these scenarios. We further generalized this method to provide the distributed superdense coding protocol $D(N, k)$ to optimize number of qubits sent to Bob and the number of parties the information is distributed among. Hence, this work provides a complete idea of absolutely secure quantum communication between two or more spatially separated parties through Distributed superdense coding in noise free quantum channels.

Acknowledgments

The authors acknowledge Mr. Abhinash Kumar Roy and Mr. Soumik Mahanty of IISER Kolkata for many encouraging and insightful discussions. They would also like to express their gratitude for the financial support from DST, India through Grant No. DST/ICPS/QuST/Theme1/2019-2020/21 to and to the hospitality of IISER Kolkata.

Data availability statement

No new data were created or analysed in this study.

ORCID iDs

Sagnik Dutta @ https://orcid.org/0000-0003-2083-9922
Prasanta K Panigrahi @ https://orcid.org/0000-0001-5812-0353

References

[1] Nielsen M A and Chuang I L 2010 Quantum Computation and Quantum Information: 10th Anniversary Edition (Cambridge University Press)
[2] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Rev. Mod. Phys. 81 865
[3] Briegel H J and Raussendorf R 2001 Phys. Rev. Lett. 86 910
[4] Uola R, Costa A C S, Nguyen H C and Gühne O 2020 Rev. Mod. Phys. 92 015001
[5] Modi K, Brodutch A, Cable H, Paterek T and Vedral V 2012 Rev. Mod. Phys. 84 1655
[6] Wootters W K and Zurek W H 1982 Nature 239 820
[7] Bennett C H and Wiesner S J 1992 Phys. Rev. Lett. 69 2881
[8] Muralidharan S and Panigrahi P K 2008 Phys. Rev. A 77 032321
[9] Aabyesinghe A, Hayden P, Smith G and Winter A 2006 IEEE Trans. Inf. Theory 52 3635–41
[10] Barenco A and Ekert A K 1995 J. Mod. Opt. 42 1253
[11] Bouwmeester D, Pan J-W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 Nature 390 575
[12] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1992 Phys. Rev. Lett. 70 1895
[13] Riebe M et al 2004 Nature 429 734–7
[14] Jain S, Muralidharan S and Panigrahi P K 2009 EPL 87 60008
[15] Hillery M, Bužek V and Berthiaume A 1999 Phys. Rev. A 59 1829
[16] Gottesman D 2000 Phys. Rev. A 61 042311
[17] Boström K and Felbinger T 2002 Phys. Rev. Lett. 89 187902
[18] Beige A, Englert B-G, Kurtsiefer C and Weinfurter H 2002 Acta. Phys. Polon. A 101 357
[19] Deng F-G, Long G L and Liu X-S 2003 Phys. Rev. A 68 042317
[20] Deng F-G and Long G L 2004 Phys. Rev. A 69 052319
[21] Wang G, Deng F-G, Li Y-S, Liu X-S and Long G L 2005 Phys. Rev. A 71 044305
[22] Lee H, Lim J and Yang H 2006 Phys. Rev. A 73 042303
[23] Bennett C H and Brassard G 2014 Theor. Comput. Sci. 560 7–11
[24] Ekert A K 1991 Phys. Rev. Lett. 67 661
[25] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 J. Cryptol. 5 3–28
[26] Karlsson A and Bourennane M 1998 Phys. Rev. A 58 4394
[27] Hildebrand A 2012 Electronic Proceedings in Theoretical Computer Science 95 103–21
[28] Agrawal P and Pati A 2006 Phys. Rev. A 74 062320
[29] Raussendorf R and Briegel H J 2001 Phys. Rev. Lett. 86 5188
[30] Rigolin G 2004 arXiv:10.48550
[31] Saha D and Panigrahi P K 2011 Quantum Inf. Process. 11 615–28
[32] Wootters W K and Leng W S 1998 Philosophical Transactions: Mathematical, Physical and Engineering Sciences 356 1717
[33] Heaney L and Vedral V 2009 Phys. Rev. Lett. 103 200502 10.1103/physrevlett.103.200502
[34] Xie S and Eberly J H 2021 Phys. Rev. Lett. 127 040403
[35] Dür W, Vidal G and Cirac J I 2000 Phys. Rev. A 62 062314
[36] Verstraete F, Dehaene J, De Moor B and Verschelde H 2002 Phys. Rev. A 65 052312
[37] Higuchi A and Sudbery A 2000 Phys. Lett. A 273 213
[38] Luque J G and Thibon J-Y 2003 Phys. Rev. A 67 042303
[39] Acín A, Andrianov A, Costa L, Jané E, Latorre J I and Tarrach R 2000 Phys. Rev. Lett. 85 1560
[40] Miyake A and Wadati M 2002 Quantum Info. Comput. 2 540–55
[41] Gelfand T, Kapranov M and Zelevinsky A 1994 Discriminants, Resultants, and Multidimensional Determinants (Basel: Birkhäuser)
[42] Facchi P, Florio G, Parisi G and Pascazio S 2008 Phys. Rev. A 77 060304
[43] OSTERLOH A and SIEWERT J 2006 International Journal of Quantum Information 04 531
[44] Gour G and Wallach N R 2010 J. Math. Phys. 51 112201
[45] Borras A, Plastino A R, Batle J, Zander C, Casas M and Plastino A 2007 J. Phys. A: Math. Theor. 40 13407
[46] Helwig W, Cui W, Latorre J I, Riera A and Lo H-K 2012 Phys. Rev. A 86 052335
[47] Bose S, Plenio M B and Vedral V 2000 J. Mod. Opt. 47 291
[48] Bruß D, D'Ariono G M, Lewenstein M, Macchiavello C, Sen (De) A and Sen U 2004 Phys. Rev. Lett. 93 210501
[49] Brub D, Lewenstein M, Sen (De) A, Sen U, D’Arino G M and Macchiavello C 2006 International Journal of Quantum Information 04 415–28
[50] Shadman Z, Kampermann H, Bruß D and Macchiavello C 2012 Phys. Rev. A 85 052306
[51] Yeo Y and Chua W K 2006 Phys. Rev. Lett. 96 060502
[52] Navascués M, Wolfe E, Rosset D and Pozas-Kerstjens A 2020 Phys. Rev. Lett. 125 240505
[53] Hausladen P, Jozsa R, Schumacher B, Westmoreland M and Wootters W K 1996 Phys. Rev. A 54 1869
[54] Bowen G 2001 Phys. Rev. A 63 022302
[55] Wu J, Long G-L and Hayashi M 2022 Phys. Rev. Applied 17 064011