International Journal of Applied Research 2020; 6(3): 508-514

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 5.2
IJAR 2020; 6(3): 508-514
www.allresearchjournal.com
Received: 22-01-2020
Accepted: 25-02-2020

Dr. Vandana Vanegal
Department of Physics,
CCS University, Meerut,
Uttar Pradesh, India

Correspondence Author:
Dr. Vandana Vanegal
Department of Physics,
CCS University, Meerut,
Uttar Pradesh, India

On the group-theoretic structure of a class of quantum dialogue protocols

Dr. Vandana Vanegal

Abstract
In this paper we have provided a generalized protocol of the QD and analyzed its efficiency and security. To implement the protocol, we require a set of unitary operators that form a group under multiplication and a set of mutually orthogonal states on which the information is to been coded by this group of unitary operators. A systematic procedure for the construction of such groups and specific examples of states that can be used to implement the generalized protocol of QD are provided. It is shown that GHZ state, GHZ-like state, W state, cluster state, $|\Omega\rangle$ state, Q_4 state and Q_5 state can be used for implementation of the QD protocol.

Keywords: QD, unitary operators, W state and cluster state

Introduction
Until now, we have discussed only the protocols of unidirectional secure quantum communication. Interestingly, in all these protocols, the meaningful information (secret messages) travel only from Alice to Bob (i.e., in one direction only) [1]. In other words, in these protocols, Alice and Bob cannot simultaneously transmit their secret messages to each other (dialogue). Such a scheme of bidirectional quantum communication is referred to as quantum dialogue (QD) protocol. The essential idea of QD protocols is already provided in Subsection. Here, we note that the possibility of extending the DSQC and QSDC protocols, and the absolute need of bidirectional quantum communication motivated the quantum communication community to investigate the possibility of designing of QD protocols. First protocol of QD was proposed by BaAn [19] using Bell states in 2004. Subsequently, it was found that the protocol is not secure under intercept-resend attack [50]. However, the modification made in [49] did not solve the problem since it loses the feature of the dialogue (i.e., both way direct communication). In this connection, satisfactory improvements to the QD protocol of Ba An [19] was obtained in [50]. Later on Xia *et al*. proposed a protocol of QD using GHZ states [41] and Dong *et al*. proposed another protocol of QD using tripartite W states [42]. But in essence, all these protocols are same. Here, we will refer to all these protocols as Ba-An-type of protocol. In recent past, several other protocols of QD have also been proposed using (i) dense coding [29, 31, 33], (ii) entanglement swapping [24], (iii) single photon [25], (iv) auxiliary particles [46], etc. These protocols are referred to as bidirectional quantum communication protocols [16], quantum telephone [13, 14], QD [19, 25], quantum conversation [26], etc. These are actually different names used for the equivalent protocols. Here, we refer all of them as QD and provide a generalized structure to the Ba-An-type of QD protocols, and will use the generalized structure to obtain several examples of quantum systems where QD is possible. Before we describe those specific quantum systems, it is important to understand that in QD the communication between Alice and Bob is simultaneous. The simultaneity implies that quantum channel (i.e., the quantum states on which the classical information of Alice and Bobareen coded) must simultaneously contain the information encoded by both the parties. This particular point distinguishes QD protocol from the QSDC and DSQC protocols. Otherwise, Alice and Bob can always communicate with each other by using DSQC/QSDC into steps or by using two different quantum channels (i.e., by using a DSQC/QSDC scheme for Alice to Bob communication and another for Bob to Alice communication). In such a case, the secret information of Alice and Bobare not simultaneously encoded in the same quantum channel, this is not the QD.

This important and distinguishing feature of QD is often overlooked by authors. For example, Jain, Muralidharan and Panigrahi's [26] protocol is essentially two QSDC. Clearly, their protocol is not a protocol of QD as Bob knows the encoded information of Alice even before he encodes his own information. In this paper we have provided a generalized protocol of the QD and analyzed its efficiency and security. To implement the protocol, we require a set of unitary operators that form a group under multiplication and a set of mutually orthogonal states on which the information is to been coded by this group of unitary operators. A systematic procedure for the construction of such groups and specific examples of states that can be used to implement the generalized protocol of QD are provided. It is shown that GHZ state, GHZ-like state, W state, cluster state, $|\Omega)$ state, Q_4 state and Q_5 state can be used for implementation of the QD protocol.

The Ba An protocol and its intrinsic symmetry

Let us first describe BaAn's originals scheme of QD. This simple scheme works in the following steps:

Step1: Bob prepares a large number of copies of a Bell state |φ+i= |01i+|10i √2. He keeps the first qubit of each Bell states with himself as home qubit and encodes his secret message 00,01,10 and 11 by applying unitary operations U0,U1,U2 and U3 respectively on the second qubit. Without loss of generality, wemayassumethatU0 =I,U1 =σx =X,U2 = iσy = iY andU3 =σz = Z whereσi are Pauli matrices.

Step2: Bob then sends the second qubit (travel qubit) to Alice and confirms that Alice has received a qubit.

Step3: Alice encodes her secret message by using the same set of encoding operations as was used by Bob and sends back the travel qubit to Bob. After receiving the encoded travel qubit Bob measures it in Bell basis.

Step 4: Alice announces whether it was run in message mode (MM) or in control mode (CM). In MM, Bob decodes Alice's bits and announces his Bellbas is measurement result. Alice uses that result to decode Bob's bits. In CM, Alice reveals her encoding value to Bob to check the security of their dialogue. It is easy to recognize that it is a modification of the PP protocol [16] and the operations used for encoding are the operators usually used for dense coding and the protocol starts with an initial state |ψiinitial =|φ+i. Now, after Step 1, |φ+i is mapped to one of the four Bell states |ψiintermediate = UB|ψiinitial = UB|φ+i, depending upon the secret message of Bob which is encoded by unitary operation UB (to be precise, we may say that the state at this time is one of the Bell states I|φ+i=|φ+i, X|φ+i=|ψ+i, iY|φ+i=|ψ−i, Z|φ+i=|φ−i). Thus, in the second step, second qubit of one of the Bell states (one of the mutually orthogonal states) is communicated to Alice via the quantum channel. At this stage, neither Alice nor Eve can know what information is sent by Bob as they have access to only one qubit of the entangled pair. Now, in Step 3, Alice encodes her secret message using the same set of unitary operations and Alice's encoding will map the state into another Bell state (|ψi final =UA|ψi intermediate = UAUB|ψi initial =UAUB|φ+i. Now, here information splitting is done in an excellent way. Alice, Bob and Eve, all know |ψi initial and |ψi final states, but in addition, Alice and Bob know the unitary operators used by them for encoding. Availability of this additional information allows them to decode each other's information and lack of this information makes it impossible for Eve to decode the information encoded by Alice and Bob. To make it clearer, assume that |ψi final =|φ+i, thus UAUB = I. This is possible in 4 different ways: UA =UB = I, UA =UB = X, UA =UB = iY, UA =UB = Z. Thus, from the initial state and final state Alice and Bob can come to know the encoding of each other, but for Eve all encodings are possible. She just obtains a correlation between the encoding of Alice and that of Bob. In this particular example, Eve knows that Alice and Bob have encoded the same message (i.e., the same classical bits in this particular example), but that does not reveal the encoding of Alice and Bob. Since in this QD protocol secure classical information (4 bits of classical information in this case as 2 bits are sent from Alice to Bob and 2 bits are sent from Bob to Alice) that is communicated using the quantum channel is more than the dense coding capacity of the quantum channel, so it is obvious that some correlation between Alice's encoding and Bob's encoding will be obtained by Eve. This has recently been pointed out by [18]. But the information splitting is done in such a way that the correlation does not directly leak the encoding. To be precise, in the above example, even after knowing the correlation (i.e., both Alice and Bob have encoded the same classical message) Eve will not be able to develop any procedure to obtain the encoding of Alice or Bob. For Eve all the encodings of Alice are equally probable. So, she has to guess randomly. If her guess is correct (the probability of which is 1/4) only then she will correctly obtain Bob's encoded information. Now, the probability of Eve's success can be reduced by three means: 1) Using multi-partite entangled states. For example, if we use 25 unitary operations and 5-qubit Brown state [48] to implement QD protocol, then the success probability of Eve would be 1 32 only. This is so because after obtaining the correlation Eve has to guess among 32 equally probable alternatives. This point would be clearer when we will describe the generalized protocol 2) by encoding lesser amount of information in the quantum channel (compared to the dense coding capacity of the quantum channel). In that case it is obvious that Eve's mean information gain on Alice's and Bob's bits would reduce [18] and 3) by using both 1) and 2) above. Here, it is important to note that the existence of a classical correlation between the encoding of Alice and Bob is an intrinsic problem with the QD protocols, but the rear strategies (as mentioned above) to circumvent that problem and essentially the security of all Ba-An-type of QD protocols arises from the above described process of information splitting. The protocol of Ba An appears quite satisfactory up to this point. However, there is a problem. Eavesdropping checking is done at the last stage and the protocol is not safe under intercept-resend attack. This was first pointed out by [49]. The idea behind the attack is simple: Eve intercepts the travel photon, keeps it with herself and prepares a fake entangled pair in |φ+i. She keeps the home (first) photon of this fake entangled state and sends the second one to Alice. As Alice cannot distinguish it from the qubit sent by Bob, she will encode her message. On the return path, Eve will intercept her fake travel photon and does a Bell measurement on the fake entangled pair to obtain the message encoded by Alice. Once Eve knows the unitary operation used by Alice, she would apply the same

unitary operation on the actual travel photon and send it back to Bob. After Bob announces publicly his Bell basis measurement result, Eve can deduce Bob's bits. Thus, the protocol of Ba An is not secure under this intercept-resend attack. In order to make it secure, we have to change the strategy for eaves dropping checking. There exist simple and equivalent strategies which can be used to make the Ba An protocol secure: (1) From Bob to Alice communication, Bob keeps some qubits as verification qubits and after confirming that Alice has received the qubits, he announces the position of verification qubits. Now, verification qubits are measured by Alice randomly in {|0i,|1i} or {|+i,|−i} basis. After the measurement, Alice announces the measurement outcome and the basis used, then Bob measures the corresponding qubits using the same basis. Looking at the correlation of the outcomes, Alice and Bob would be able to determine the presence of Eve. [2] When Bob sends a sequence of travel photons then he can insert an equal number of decoy photons randomly in these quence of the travel photons. These decoy photons are prepared randomly in {|0i,|1i,|+i,|−i}states. After confirming that Alice has received all the qubits, Bob announces the position of the decoy photons. After Bob's announcement, Alice randomly measures decoy qubits in {|0i,|1i}or{|+i,|−i} basis. After the measurement, Alice announces the measurement outcomes and the basis used. If she has chosen the correct basis (the same basis in which decoy state is prepared) the measurement outcomes will be in perfect correlation with the decoy states prepared by Bob. In any of the above two strategies, if Eve is detected, then Alice does not perform her encoding operation and the protocol is truncated. On the other hand, the absence of Eve in the communication channel from Bob to Alice would essentially mean that no fake photon sequence has been sent to Alice and that will make the protocol secure against intercept-resend attack. The first strategy was used by [19]. We will use the second (decoy photon) strategy, which is equivalent to the first strategy. So far, we have seen that a clever choice of information splitting plays the key role in the construction of QD protocols. To construct a generalized protocol of QD, we need a deeper understanding of this information splitting process. To be precise, a deeper understanding of the information splitting process would help us to obtain a more general and sufficient condition for the construction of a QD protocol. Then, just by using the standard tricks of eavesdropping checking and the sufficient conditions we will construct a generalized protocol of QD.

Sufficient condition for construction of quantum dialogue protocol

Before we generalize the protocol, we need to visualize certain intrinsic symmetries and the requirements of the Ba-An-type of protocols. In the following discussion, |ψi initial is an n-qubit state in general, |ψi intermediate is the n-qubit state after encoding operation of Bob and |ψi final is an n-qubit state after encoding of Alice. Thus, they are not limited to Bell states. Now, we can note that after encoding operations of Bob, the initial state |ψi initial must be mapped to a mutually orthogonal set of intermediate states (|ψi intermediate). Because only in that case, Alice would be able to deterministically discriminate the intermediate states prepared by Bob and thus will be able to decode the encoded message. To be precise, if we have k unitary operations U0, U1, U2,⋯,Uk−1 and Bob encodes i^{th} message by applying the unitary operator UBi, then after the encoding operation the initial states are mapped to UBi|ψi initial = |ψii intermediate : intermediate hψi|ψji intermediate = δi,j. Following the same logic, Alice's encoding operation UAi should also map the intermediate states to a mutually orthogonal set of final states, i.e., UAi|ψi intermediate = |ψii final: final hψi|ψji final = δi,j. Now, the Hilbert space of n-qubit states is C2n. Therefore, we can have at most 2 n mutually orthogonal states in that space. Let us denote these states as{|φ0i,|φ1i,⋯,|φii,⋯,|φ2n−1i}. It is easy to recognize that these states are nothing but the elements of a mutually orthogonal basis set inC2n. To make the remaining discussion convenient, without loss of generality, we may assume that at the beginning of the generalized protocol, Bob prepares a large number of copies of the state|φ0i. Now, to encode an arbitrary n-bit classical message we would require 2n unitary operators. In principle, one can choose to work with the less number of encoding operations, but that would not have any effect other than reducing the communication efficiency. So, for an efficient protocol we need 2n number of m-qubit unitary operations {U0,U1,U2,⋯,U2n−1} where m≤n. As the operators are required to map the initial state|φ0iinto one of the state vector of the mutually orthogonal set {|φ0i,|φ1i,⋯,|φii,⋯,|φ2n−1i}. Without loss of generality, we can assume that Ui|φ0i= |φii. If m < n, then we have dense coding, and if m = n 2, then we have a maximally efficient dense coding. Thus, all those physical systems where dense coding is possible can be used for encoding of information by one party and thus all such systems can be used for DSQC. It is a sufficient criterion for DSQC but not essential (as in cases where m = n, there dense coding will not happen, but encoding will happen). But even dense coding is not sufficient for QD protocol of Ba-An-type. Here, the demand is more because the encoding is done by both Alice and Bob using the same set of operators. So, after the encoding operation of Alice (say Uj) and that of Bob (say Ui) the final states must also be a member of the mutually orthogonal states to ensure the deterministic discrimination of the state and thus to decode the encoded message. To be precise, |ψi final =UjUi|φ0i=Uj|φii∈{|φ0i,|φ1i,⋯,|φii,⋯,|φ2n−1i∀i, j∈ {0,1,⋯,2n−1}⇒UBUA ∈{U0,U1,U2,⋯,U2n−1}. Thus, the product of any two arbitrary unitary operators should be a member of the set of unitary operators. This is a property of a group. So, we may conclude that if we have a set of mutually orthogonal n-qubit states {|φ0i,|φ1i,⋯,|φii,⋯,|φ2n−1i} and a set of m-qubit unitary operators {U0,U1,U2,⋯,U2n−1} such that the Ui|φ0i=|φii and{U0,U1,U2,⋯,U2n−1} forms a group under multiplication, then it would be sufficient to construct a QD protocol of Ba-An-type. This is true in general as information splitting in the sense of Ba An protocol is possible and Eve knows only |ψi initial and |ψi final. Consequently, Eve knows the product of the operators of Alice Uj and that of Bob Ui. Say UjUi =Uk and |ψifinal =Uk|ψi initial. Now, from the rearrangement theorem of the groups, we know that each row and each column in the group multiplication table lists each of the group elements once and only once. From this, it follows that Uk can be decomposed in 2n different ways. Thus, all possible 2n encoding of Bob may lead to the same Uk. Now, if Eve wants to obtain the secret information encoded by Alice and Bob then she has to guess either Ui or Uj, i.e., she has to

guess among 2n equiprobable events. Clearly, the probability of her success is 2−n and consequently the QD protocol of the present type is more secure when a multi-partite state is used. To be precise, if the QD is implemented using Bell state, 5-qubit Brownstateand6-qubit cluster states respectively, then the probability of Eve's success is 25%, 3.1% and 1.6% respectively. Now, since the multi-partite entangled states can be experimentally prepared (for example 6-qubit cluster state is experimentally prepared by [14]) so efficient QD protocols with negligible information leakage can be designed. Thus, we have obtained a sufficient condition for the construction of a QD protocol of Ba-An-type.

Generalized protocol of quantum dialogue

Our generalized protocol works using the above mentioned n-qubit mutually orthogonal states {|φ0i,|φ1i,⋯,|φii,⋯,|φ2n−1i} and m-qubit (m≤n) unitary operators {U0,U1,⋯,U2n−1} as follows:

Step1: Bob prepares a large number of copies (say N copies) of state |φ0i, and encodes his classical secret message by applying m-qubit unitary operators {U0, U1,⋯,U2n−1}. For example, to encode 0102⋯0n, 0102⋯1n, 0102⋯1n−10n,⋯,1112⋯1n he applies U0, U1, U2, ⋯,U2n−1, respectively. The information encoded states should be mutually orthogonal to each other as discussed above.

Step2: There are two possibilities: i) m < n i.e., dense coding is possible and ii) m = n i.e., dense coding is not possible for set of quantum states and set of unitary operators used for encoding. If m<n, then Bob uses them photons on which encoding is done as travel photons and remaining n−m photons as home photons and keeps them with himself in an ordered sequence PB = [p1(h1,h2,⋯,hn−m),p2(h1,h2,⋯,hn−m),⋯,pN(h1,h2,⋯,hn −m)] where the subscripts 1,2,⋯,N denote the order of an n-partite state pi ={h1,h2,⋯,hn−m, t1,t2,⋯,tm}, which is in one of the n-partite states |φji (value of j depends on the encoding). Symbol h and t are used to indicate home photon (h) and travel photon (t), respectively. If dense coding is not possible, then he has to use all qubits as travel qubits. In general, he uses all the travel photons to prepare an ordered sequence PA = [p1(t1,t2,⋯,tm),p2(t1,t2,⋯,tm),⋯, pN(t1,t2,⋯,tm)]. Now, before transmitting the travel qubits to Alice, Bob first prepares N m decoy photons in a random sequence of {|0i,|1i,|+i, |−i}, i.e., the decoy photon state is ⊗m j=1|Pji,|Pji∈{|0i,|1i,|+i,|−i},(j =1,2,⋯,m). Then, Bob randomly rearranges the sequence PA of the travel qubits (the actual ordering is known to Bob only) and inserts N m decoy photons, randomly in them and makes a new sequence P0 A which contains 2Nm photons (Nm travel photons and Nm decoy photons)[4] and sends the rearranged sequence P0 A to Alice.

Step3: After confirming that Alice has received all the 2Nm photons, Bob announces the position of the decoy photons. Alice measures the corresponding particles in the sequence P0 A by using X basis or Z basis at random, here X ={|+i,|−i}and Z ={|0i,|1i}. After measurement, Alice publicly announces the result of her measurement and the basis used for the measurement. Now, the initial state of the decoy photon as noted by Bob during preparation and the measurement outcome of Alice should coincide in all such cases where Alice has used the same basis as was used to prepare the decoy photon. Bob can compute the error rate, and check whether it exceeds the predeclared threshold or not. If it exceeds the threshold, then Alice and Bobabort this communication and repeat the procedure from the beginning. Otherwise, they go on to the next step. So, all intercept-resend attacks will be detected in this step and even if eavesdropping has happened Eve has no information about the encoding operation executed by Bob as the sequence is randomly rearranged.

Step 4: Bob announces the actual order.

Step 5: After knowing the actual order, Alice transforms the sequence into actual order and encodes her information using the same encoding scheme as was used by Bob. That creates a new sequence P00 A. Alice prepares Nm decoy photons in a random sequence of {|0i,|1i,|+i,|−i}, rearranges P00 A and randomly inserts decoy photon in that to convert that into a new sequence P000 A. She then sends the sequence P000 A to Bob.

Step 6: After confirming that Bob has received all the 2Nm photons, Alice announces the position of the decoy photons. Bob measures the corresponding particles in the sequence P000 A by using X basis or Z basis at random, here X = {|+i,|−i}and Z ={|0i,|1i}. After measurement, Bob publicly announces the result of his measurement and the basis used for the measurement. Now, the initial state of the decoy photon as noted by Alice during preparation and the measurement outcome of Bob should coincide in all such cases where Bob has used the same basis as was used to prepare the decoy photon. Alice can compute the error rate and check whether it exceeds the predeclared threshold or not. If it exceeds the threshold, then Alice and Bob abort this communication and repeat the procedure from the beginning. Otherwise, they go on to the next step. This makes the protocol safe from all kinds of eavesdropping strategy in the return path.

Step 7: Alice announces the actual order.

Step 8: Bob reorders the sequence to obtain P00 A. Recombines it with PB and measures each n-partite state in {|φ0i,|φ1i,⋯,|φii,⋯,|φ2n−1i} basis. As he already knows the unitary operators applied by him or the state |φii sent by him, he can now easily decode the message encoded by Alice. After the measurement, Bob publicly announces the final states that he has obtained in sequence.

Step 9: Now, as Alice knows her encoding into a particular state she will be able to decode the secret message of Bob.

Now, we would like to note that in case m = n, then in Step 5 after knowing the actual order, Alice could have decoded the message of Bob and in that case the public announcement of Bob in Step 8 and the entire Step 9 would be redundant. In such a case, the protocol essentially gets decomposed into two protocols of DSQC: One from Alice to Bob and the other from Bob to Alice. That is not really in accordance with the true spirit of the QD protocols and consequently we have excluded such cases from the remaining discussion. It is straight to note that neither

DSQC nor QD protocol requires dense coding as an essential resource, but it is always useful. In case of DSQC, it is sufficient [44] and in case of QD, in addition, the unitary operators must form a group. Now, to further clarify that dense coding is not essential for a QD protocol, we may give a different example, where only the subset of the basis set is used. To be precise, we may use U0 = I⊗I, U1 = I⊗iσy,U2 = σx⊗I,U3 = σx⊗iσy as our unitary operators (these operators form a group) and following set of 4-qubit W states provides example of required orthogonal states [14]:

$$|\varphi_0\rangle = U_0|\varphi_0\rangle = \frac{1}{2}(|0001\rangle + |0010\rangle + |0100\rangle + |1000\rangle),$$
$$|\varphi_1\rangle = U_1|\varphi_0\rangle = \frac{1}{2}(|0000\rangle - |0011\rangle - |0101\rangle - |1001\rangle),$$
$$|\varphi_2\rangle = U_2|\varphi_0\rangle = \frac{1}{2}(|0011\rangle + |0000\rangle + |0110\rangle + |1010\rangle),$$
$$|\varphi_3\rangle = U_3|\varphi_0\rangle = \frac{1}{2}(|0010\rangle - |0001\rangle - |0111\rangle - |1011\rangle).$$

This resource would be good enough for an efficient protocol of QD, but here we can send only 2 bits of classical information using 2 ebits so this is not dense coding. Before we proceed further, it would be apt to analyze the security and efficiency of the protocol described above. The same is done in the following subsection.

Table 1: Dense coding operation for 4-qubit Omega states |Ωi and cluster states |Ci. The unitary operators operate on the qubits 1 and 3 in both the cases. As all the elements of G2 group are used as unitary operators for encoding, these two states may be used for QD using the generalized protocol presented here

Unitary Operations	$\|\Omega\rangle =$ $\frac{1}{2}(\|0000\rangle + \|0110\rangle + \|1001\rangle - \|1111\rangle)$	$\|C\rangle =$ $\frac{1}{2}(\|0000\rangle + \|0011\rangle + \|1100\rangle - \|1111\rangle)$
$U_0 = I \otimes I$	$\frac{1}{2}(\|0000\rangle + \|0110\rangle + \|1001\rangle - \|1111\rangle)$	$\frac{1}{2}(\|0000\rangle + \|0011\rangle + \|1100\rangle - \|1111\rangle)$
$U_1 = I \otimes Z$	$\frac{1}{2}(\|0000\rangle - \|0110\rangle + \|1001\rangle + \|1111\rangle)$	$\frac{1}{2}(\|0000\rangle - \|0011\rangle + \|1100\rangle + \|1111\rangle)$
$U_2 = Z \otimes I$	$\frac{1}{2}(\|0000\rangle + \|0110\rangle - \|1001\rangle + \|1111\rangle)$	$\frac{1}{2}(\|0000\rangle + \|0011\rangle - \|1100\rangle + \|1111\rangle)$
$U_3 = Z \otimes Z$	$\frac{1}{2}(\|0000\rangle - \|0110\rangle - \|1001\rangle - \|1111\rangle)$	$\frac{1}{2}(\|0000\rangle - \|0011\rangle - \|1100\rangle - \|1111\rangle)$
$U_4 = I \otimes X$	$\frac{1}{2}(\|0010\rangle + \|0100\rangle + \|1011\rangle - \|1101\rangle)$	$\frac{1}{2}(\|0001\rangle + \|0010\rangle - \|1101\rangle + \|1110\rangle)$
$U_5 = I \otimes iY$	$\frac{1}{2}(-\|0010\rangle + \|0100\rangle - \|1011\rangle - \|1101\rangle)$	$\frac{1}{2}(-\|0001\rangle + \|0010\rangle + \|1101\rangle + \|1110\rangle)$
$U_6 = Z \otimes X$	$\frac{1}{2}(\|0010\rangle + \|0100\rangle - \|1011\rangle + \|1101\rangle)$	$\frac{1}{2}(\|0001\rangle + \|0010\rangle + \|1101\rangle - \|1110\rangle)$
$U_7 = Z \otimes iY$	$\frac{1}{2}(-\|0010\rangle + \|0100\rangle + \|1011\rangle + \|1101\rangle)$	$\frac{1}{2}(-\|0001\rangle + \|0010\rangle - \|1101\rangle - \|1110\rangle)$
$U_8 = X \otimes I$	$\frac{1}{2}(\|1000\rangle + \|1110\rangle + \|0001\rangle - \|0111\rangle)$	$\frac{1}{2}(\|0100\rangle - \|0111\rangle + \|1000\rangle + \|1011\rangle)$
$U_9 = X \otimes Z$	$\frac{1}{2}(\|1000\rangle - \|1110\rangle + \|0001\rangle + \|0111\rangle)$	$\frac{1}{2}(\|0100\rangle + \|0111\rangle + \|1000\rangle - \|1011\rangle)$
$U_{10} = iY \otimes I$	$\frac{1}{2}(-\|1000\rangle - \|1110\rangle + \|0001\rangle - \|0111\rangle)$	$\frac{1}{2}(\|0100\rangle - \|0111\rangle - \|1000\rangle - \|1011\rangle)$
$U_{11} = iY \otimes Z$	$\frac{1}{2}(-\|1000\rangle + \|1110\rangle + \|0001\rangle + \|0111\rangle)$	$\frac{1}{2}(\|0100\rangle + \|0111\rangle - \|1000\rangle + \|1011\rangle)$
$U_{12} = X \otimes X$	$\frac{1}{2}(\|1010\rangle + \|1100\rangle + \|0011\rangle - \|0101\rangle)$	$\frac{1}{2}(-\|0101\rangle + \|0110\rangle + \|1001\rangle + \|1010\rangle)$
$U_{13} = X \otimes iY$	$\frac{1}{2}(-\|1010\rangle + \|1100\rangle - \|0011\rangle - \|0101\rangle)$	$\frac{1}{2}(\|0101\rangle + \|0110\rangle - \|1001\rangle + \|1010\rangle)$
$U_{14} = iY \otimes X$	$\frac{1}{2}-\|1010\rangle - \|1100\rangle + \|0011\rangle - \|0101\rangle)$	$\frac{1}{2}(-\|0101\rangle + \|0110\rangle - \|1001\rangle - \|1010\rangle)$
$U_{15} = iY \otimes iY$	$\frac{1}{2}(\|1010\rangle - \|1100\rangle - \|0011\rangle - \|0101\rangle)$	$\frac{1}{2}(\|0101\rangle + \|0110\rangle + \|1001\rangle - \|1010\rangle)$

Table 2: Dense coding of GHZ state using the elements of G1 2(8) and G2 2(8)

Unitary operations on qubits 1 and 2 (elements of $G_2^1(8)$)	GHZ states	Unitary operations on qubits 1 and 2 (elements of $G_2^2(8)$)	GHZ states
$U_0 = I \otimes I$	$\frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$	$U_0 = I \otimes I$	$\frac{1}{\sqrt{2}}(\|000\rangle + \|111\rangle)$
$U_1 = Z \otimes I$	$\frac{1}{\sqrt{2}}(\|000\rangle - \|111\rangle)$	$U_1 = Z \otimes I$	$\frac{1}{\sqrt{2}}(\|000\rangle - \|111\rangle)$
$U_2 = X \otimes I$	$\frac{1}{\sqrt{2}}(\|100\rangle + \|011\rangle)$	$U_2 = X \otimes I$	$\frac{1}{\sqrt{2}}(\|100\rangle + \|011\rangle)$
$U_3 = iY \otimes I$	$\frac{1}{\sqrt{2}}(-\|100\rangle + \|011\rangle)$	$U_3 = iY \otimes I$	$\frac{1}{\sqrt{2}}(-\|100\rangle + \|011\rangle)$
$U_4 = I \otimes X$	$\frac{1}{\sqrt{2}}(\|010\rangle + \|101\rangle)$	$U_4 = I \otimes iY$	$\frac{1}{\sqrt{2}}(-\|010\rangle + \|101\rangle)$
$U_5 = Z \otimes X$	$\frac{1}{\sqrt{2}}(\|010\rangle - \|101\rangle)$	$U_5 = Z \otimes iY$	$\frac{1}{\sqrt{2}}(-\|010\rangle - \|101\rangle)$
$U_6 = X \otimes X$	$\frac{1}{\sqrt{2}}(\|110\rangle + \|001\rangle)$	$U_6 = X \otimes iY$	$\frac{1}{\sqrt{2}}(-\|110\rangle + \|001\rangle)$
$U_7 = iY \otimes X$	$\frac{1}{\sqrt{2}}(-\|110\rangle + \|001\rangle)$	$U_7 = iY \otimes iY$	$\frac{1}{\sqrt{2}}(\|110\rangle + \|001\rangle)$

Thus, these two examples show that the formation of a group of unitary operators alone is not sufficient for QD, we also need appropriate quantum states on which that particular group of unitary operators can be applied to implement QD. With the similar intention, we may note that there exists a set of 8 operators (as shown in above tables) which may be used for dense coding in GHZ-like states [44], but these operators do not form a group under multiplication, since $U_7U_6 = iY \otimes Z, U_6U_5 = X \otimes iY$, etc., are not in the set $\{U_0, U_1, \cdots, U_7\}$ used here for dense coding. Consequently, if Bob applies U_6 and Alice applies U_7 then the QD protocol will fail.

Thus, this example shows that dense coding alone is not also sufficient for QD. This does not may satisfy the sufficient condition introduced here. We have verified that $G^9(8)$ may be used really mean that we cannot obtain a QD protocol with GHZ-like state; another set of operators for dense coding in GHZ-like state and the same sub-group can also be used for dense coding in 4-qubit W state. Thus, both 3-qubit GHZ-like state and 4-qubit W state can be used for QD. These particular examples just show that for QD, we need to simultaneously satisfy both the conditions discussed above. Alternatively, we can also use the elements of G^8 (8) to implement QD using 4-qubit W states. Thus, there are at least two different ways to implement QD using W states. Similarly, there are atleast six different ways to implement QD using GHZ-like states by using $G^2(8)$, $G^3(8)$, $G^5(8)$, $G^6(8)$, $G^8(8)$ and $G^9(8)$. The dense coding of GHZ-like states is found to be possible using the elements of $G^2(8), G^3(8), G^5(8), G^6(8), G^8(8)$ and $G^9(8)$. 4- qubit Q_4 state and 4-qubit Q_5 state introduced in [55] are also very interesting as there are at least 2 different ways to implement QD using Q_4 state and atleast 3 different ways to implement QD using Q_5 state. To be precise, QD can be implemented using Q_4 state by using the elements $G^6(8)$ and $G^7(8)$, respectively. Similarly, we can perform dense coding on Q_5 state by elements of $G^3(8)$, $G^4(8)$ and $G^5(8)$. Again by using our systematic approach we have observed that dense coding can be done on 5-qubit Brown state in at least 6 different ways by using the elements of $G^1(32)$, $G^2(32)$, $G^4(32), G^5(32), G^7(32), G^8(32)$ and similarly on 5-qubit cluster state in at least 4 different ways by using the elements of $G^4(32), G^5(32), G^7(32), G^8(32)$. Thus, QD can be implemented in several ways by using 5-qubit states. In brief, our generalized protocol can be used to implement QD using Bell state, 4- and 5-qubit cluster states, $|\Omega\rangle$state, Q_4 state, Q_5 state, W state, GHZ state, GHZ-like state, 5-qubit Brown state, etc. Our systematic approach has produced a large number of useful dense coding schemes. A few of these dense coding schemes can also be found in the existing literature. For example, useful dense coding operations for 4-qubit cluster state is discussed in [24] in a different context (in context of DSQC). Similarly, in a different context useful dense coding schemes (only one scheme for each case) for the $|\Omega\rangle$ state, Q_4 state, Q_5 state, W state are reported in [45], also in [17] a dense coding scheme for 5-qubit Brown states is reported [8]. Our systematic approach has yielded additional schemes of useful dense coding using GHZ, W, Q_4, Q_5 and Brown states and new examples of useful dense coding schemes using GHZ-like states and 5-qubit cluster states. This chapter is focused on QD, but the newly found useful dense coding schemes can find their applications on other aspects of quantum communication (e.g., DSQC) and quantum games. It is not our purpose to discuss those possibilities here. Rather, we would like to note that our group-theoretic approach provides a wide choice of possible quantum states that can be used for QD.

Conclusion

Our results can be easily extended to secure multi-party computation (SMC) tasks. We have explored the underlying symmetry of the existing QD protocols and have shown that the information splitting plays a crucial role in their implementation. Then, we have obtained a sufficient condition for implementation of QD. We have used this sufficiency condition to provide a generalized algorithm for implementation of QD. All the existing Ba-An-type of QD protocol, thus automatically become special cases of our protocol. We have also provided a systematic way of generating groups of unitary operators that are useful for implementation of QD and have shown that those groups may be used to implement our generalized QD protocol using Bell state, 4- qubit and 5-qubit cluster states, $|\Omega\rangle$ state, Q_4 state, Q_5 state, W state, GHZ state, GHZ-like state, Brown state, etc. From the perspective of experimental implementation, it is a very attractive situation as there are so many options to implement the same task (QD and solution of the socialist millionaire problem) and thus the current work is expected to motivate experimentalist. It is indeed attractive, but the situation is actually more favorable because we have just given a handful of examples. A simple computer program can generate all the relevant subgroups of G_n and the set of states that are unitarily connected by the elements of a particular subgroup or group.

References

1. Bennett CH, Brassard G, Cr´epeau C, Jozsa R, Peres A, Wootters WK. Teleporting an Unknown Quantum Statevia Dual Classical and Einstein- Podolsky- Rosen Channels, Phys. Rev. Lett 1993;70:1895-1899.
2. Bennett CH, Wiesner SJ. Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States, Phys. Rev. Lett 1992;69:2881-2884.
3. Bennett CH, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing, Proc. of the IEEE Int. Conference on Computers, Systems, and Signal Processing, Bangalore, India 1984, 175-179.
4. Bennett CH. Quantum Cryptography using any two Nonorthogonal States, Phys. Rev. Lett 1992;68:3121-3124.
5. Goldenberg L, Vaidman L. Quantum Cryptography Based on Orthogonal States, Phys. Rev. Lett 1995;75:1239-1243.
6. Hillery M, Bu˘zek V, Berthiaume A. Quantum Secret Sharing, Phys. Rev. A 1999;59:1829-1834.
7. Liu J, Liu YM, Cao HJ, Shi SH, Zhang ZJ. Revisiting Quantum Secure Direct Communication with W State, Chin. Phys. Lett 2006;23:2652-2655.
8. Li XH, Deng FG, Li CY, Liang YJ, Zhou P, Zhou HY. Deterministic Secure Quantum Communication without Maximally Entangled States, J Korean Phys. Soc 2006;49:1354-1359.
9. Yan FL, Zhang XQ. A Scheme for Secure Direct Communication using EPR Pairs and Teleportation, Euro. Phys. J B 2004;41:75-78.
10. Man ZX, Zhang ZJ, Li Y. Deterministic Secure Direct Communication by using Swapping Quantum Entanglement and Local Unitary Operations, Chin. Phys. Lett 2005;22:18-21.

11. Hwang T, Hwang CC, Tsai CW. Quantum Key Distribution Protocol using Dense Coding of Three-Qubit W State, Eur. Phys. J D 2011;61:785-790, 139.
12. Zhu AD, Xia Y, Fan QB, Zhang S. Secure Direct Communication Basedon Secret Transmitting Order of Particles, Phys. Rev. A 2006;73:022338.
13. Cao HJ, Song HS. Quantum Secure Direct Communication with W State, Chin. Phys. Lett 2006;23:290-292.
14. Yuan H, Song J, Zhou J, Zhang G, Wei XF. High-Capacity Deterministic Secure Four-Qubit W State Protocol for Quantum Communication Based on Order Rearrangement of Particle Pairs, Int. J Theor. Phys 2011;50:2403-2409.
15. Long GL, Liu XS. Theoretically Efficient High-Capacity Quantum-Key-Distribution Scheme, Phys. Rev. A 2002;65:032302.
16. Bostr¨om K, Felbinger T. Deterministic Secure Direct Communicationusing Entanglement, Phys. Rev. Lett 2002;89:187902.
17. Degiovanni IP, Berchera IR, Castelletto S, Rastello ML, Bovino FA, Colla AM *et al*., Quantum Dense Key Distribution, Phys. Rev. A 2004;69:032310.
18. Lucamarini M, Mancini S. Secure Deterministic Communication without Entanglement, Phys. Rev. Lett 2005;94:140501.
19. An NB. Quantum Dialogue, Phys. Lett. A 2004;328:6-10.
20. Shukla C, Kothari V, Banerjee A, Pathak A. On the Group-Theoretic Structure of a Class of Quantum Dialogue Protocols, Phys. Lett. A 2013;377:518-527.
21. Shukla C, Alam N, Pathak A. Protocols of Quantum Key Agreement Solelyusing Bell States and Bell Measurement Quantum Inf. Process 2014;13:2391-2405.
22. Traina P, Gramegna M, Avella A, Cavanna A, Carpentras D, Degiovanni IP *et al*., Review on Recent Groundbreaking Experiments on Quantum Communication with Orthogonal States, Quantum Matter 2013;2:153-166.
23. Cai QY, Li BW. Improving the Capacity of the Bostr Om-Felbinger Protocol, Phys. Rev. A 2004;69:054301.
24. Tsai CW, Hsieh CR, Hwang T. Dense Coding using Cluster States and its Application on Deterministic Secure Quantum Communication, Eur. Phys. J D 2011;61:779-783.
25. Noh TG. Counterfactual Quantum Cryptography, Phys. Rev. Lett 2009;103:230501, 140.
26. Guo GC, Shi BS. Quantum Cryptography Based on Interaction-Free Measurement, Phys. Lett. A 1999;256:109-112.
27. Koashi M, Imoto N. Quantum Cryptography Based on Split Transmission of One-Bit Information in two Steps, Phys. Rev. Lett 1997;79:2383-2386.
28. Avella A, Brida G, Degiovanni IP, Genovese M, Gramegna M, Traina P. Experimental Quantum-Cryptography Scheme Basedon Orthogonal States, Phys. Rev. A 2010;82:062309.
29. Ren M, Wu G, Wu E, Zeng H. Experimental Demonstration of Counterfactual Quantum Key Distribution, Laser Phys 2011;21:755-760.
30. Brida G, Cavanna A, Degiovanni IP, Genovese M, Traina P. Experimental Realization of Counterfactual Quantum Cryptography, Laser Phys. Lett 2012;9:247-252.
31. Liu Y, Ju L, Liang XL, Tang SB, Tu GLS, Zhou L *et al*., Experimental Demonstration of Counterfactual Quantum Communication, Phys. Rev. Lett 2012;109:030501.
32. Shukla C, Pathak A, Srikanth R. Beyond the Goldenberg-Vaidman Protocol: Secure and Efficient Quantum Communication using Arbitrary, Orthogonal, Multi-Particle Quantum States, Int. J Quantum Inf 2012;10:1241009.
33. Yadav P, Srikanth R, Pathak A. Two-Step Orthogonal-State-Based Protocol of Quantum Secure Direct Communication with the help of Order-Rearrangement Technique, Quantum Inf. Process 2014;13:2731-2743. Generalization of the Goldenberg Vaidman QKD Protocol, arxiv: 1209.4304v1 (quant-ph) 2012.
34. Shukla C, Pathak A. Orthogonal-State-Based Deterministic Secure Quantum Communication without Actual Transmission of the Message Qubits Quantum Inf. Process 2014;13:2099-2113.
35. Salih H, Li ZH, Al-Amri M, Zubairy MS. Protocol for Direct Counterfactual Quantum Communication, Phys. Rev. Lett 2013;110:170502.
36. Sun Y, Wen QY. Counterfactual Quantum Key Distribution with High Efficiency, Phys. Rev. A 2010;82:52318.
37. Shenoy HA, Srikanth R, Srinivas T. Counterfactual Quantum Certificate Authorization, Phys. Rev. A 2014;89:052307.
38. Salih H. Protocol for Counterfactually Transporting an Unknown Qubit, arxiv: 1404. 2200 (quant-ph) 2014.
39. Salih H. Tripartite Counterfactual Quantum Cryptography, Phys. Rev. A 2014;90:012333.
40. Vaidman L. Comment on Protocol for Direct Counterfactual Quantum Communication, Phys. Rev. Lett 2014;112:208901.
41. Salih H, Li ZH, Al-Amri M, Zubairy MS. Salihetal. Reply, Phys. Rev. Lett 2014;112:208902.
42. Shenoy HA, Srikanth R, Srinivas T. Semi-Counterfactual Cryptography, Europhys. Lett 2013;103:60008.
43. Deng FG, Long GL. Controlled Order Rearrangement Encryption for Quantum Key Distribution, Phys. Rev. A 2003;68:042315.
44. Banerjee A, Pathak A. Maximally Efficient Protocols for Direct Secure Quantum Communication, Phys. Lett. A 2012;376:2944-2950.
45. Shukla C, Banerjee A, Pathak A. Improved Protocols of Secure Quantum Communication using W States, Int. J Theor. Phys 2013;52:1914-1924.
46. Peres A. Quantum Cryptography with Orthogonal States?, Phys. Rev. Lett 1996;77:3264.
47. Goldenberg L, Vaidman L. Goldenberg, Vaidman Reply, Phys. Rev. Lett 1996;77:3265.
48. Mor T. No Cloning of Orthogonal States in Composite Systems, Phys. Rev. Lett 1998;80:3137-3140.
49. Elitzur AC, Vaidman L. Quantum Mechanical Interaction-Free Measurements, Found. Phys 1993;23:987-997.
50. Aravinda S, Yadav P, Srikanth R, Pathak A. From Local Nonclassicality to Nonclassical Correlations, Communicated.