Physics Letters A 377 (2013) 518–527

Contents lists available at SciVerse ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

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

Chitra Shukla [a], Vivek Kothari [a], Anindita Banerjee [b], Anirban Pathak [a,c,*]

[a] *Jaypee Institute of Information Technology, A-10, Sector 62, Noida, UP-201307, India*
[b] *Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Block EN, Sector V, Kolkata 700091, India*
[c] *RCPTM, Joint Laboratory of Optics of Palacky University and Institute of Physics of Academy of Science of the Czech Republic, Faculty of Science, Palacky University, 17. listopadu 12, 771 46 Olomouc, Czech Republic*

ARTICLE INFO

Article history:
Received 20 August 2012
Received in revised form 20 November 2012
Accepted 13 December 2012
Available online 28 December 2012
Communicated by P.R. Holland

Keywords:
Quantum dialogue
Dense coding
Socialist millionaire problem
Secure quantum communication
Pauli groups

ABSTRACT

A sufficient condition for implementation of the quantum dialogue protocol is obtained and it is shown that the set of unitary operators used for the purpose must form a group under multiplication. A generalized protocol of quantum dialogue is obtained using the sufficient condition. Further, several examples of possible groups of unitary operators and quantum states that may be used for implementation of quantum dialogue are systematically generated. As examples, it is shown that *GHZ* state, *GHZ-like* state, *W* state, 4 and 5-qubit Cluster states, Ω state, Brown state, Q_4 state and Q_5 state can be used to implement quantum dialogue protocol. It is also shown that if a quantum system is found to be suitable for quantum dialogue then that can provide solution of the socialist millionaire problem too.

1. Introduction

First protocol of unconditionally secure quantum key distribution (QKD) was proposed by Bennett and Brassard in 1984 [1]. In a QKD protocol two remote legitimate users (Alice and Bob) can establish an unconditionally secure key by using quantum resources, i.e. by the transmission of qubits. The protocol of Bennett and Brassard which is popularly known as BB84 protocol, had drawn considerable attention of the cryptographic community since the unconditional security of key obtained in this protocol is not achievable in classical cryptography. Naturally, since 1984 several new protocols for different cryptographic tasks have been proposed. While most of the initial works on quantum cryptography [1–4] were concentrated around QKD, eventually quantum states were applied to other 'post-coldwar' cryptographic tasks. For example, in 1999, a protocol for quantum secret sharing (QSS) was proposed by Hillery, Buzek and Bertaiume [5]. In the same year, Shimizu and Imoto [6] proposed a protocol for deterministic secure quantum communication (DSQC) using entangled photon pairs. In the Shimizu–Imoto protocol Alice can communicate a message to Bob directly (without prior generation of key) with unconditional security. In a DSQC protocol, the receiver can read out the secret message only after the transmission of at least one bit of additional classical information for each qubit. However, the exchange of classical information for decryption of encrypted text is not essential for secure direct quantum communication. A protocol of secure direct quantum communication that does not require such exchange of classical information is called quantum secure direct communication (QSDC) protocol. Important protocols for QSDC were proposed [7,8] after the seminal work of Shimizu and Imoto [6].

Since the pioneering work of Shimizu and Imoto [6] several protocols of DSQC and QSDC are proposed ([9] and references therein). But in all these QSDC and DSQC protocols, the meaningful information (secret message) travels only from Alice to Bob.[1] In other words in these protocols, Alice and Bob cannot simultaneously transmit their different secret messages to each other (dialogue) and consequently advent of these protocols naturally leads to a question: Is it possible to extend these protocols for bidirectional quantum communication in which both Alice and Bob will be able to communicate (with unconditional security) using the same quantum channel. Such bidirectional protocols are quantum dialogue protocols, where information can flow along two directions (i.e. from Alice to Bob and from Bob to Alice). Such protocols are actually an essential requirement of our everyday

[*] Corresponding author at: Jaypee Institute of Information Technology, A-10, Sector 62, Noida, UP-201307, India.
E-mail address: anirban.pathak@jiit.ac.in (A. Pathak).

[1] The protocol may be a two way protocol like Ping-Pong protocol [7] or LM-05 [8] protocol but the meaningful information (message) is transmitted from Alice to Bob only. Thus the flow of information is unidirectional (one way) only.

0375-9601/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.physleta.2012.12.024

communication problems. This can be visualized more clearly if we consider the analogy of a telephone. 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 quantum dialogue protocols. First protocol of quantum dialogue was proposed by Ba An [10] using Bell states in 2004. Subsequently it was found that the protocol is not secure under intercept–resend attack [11]. However, the modification made in [11] does not solve the problem since it loses the feature of dialogue (i.e., direct communication). In this connection, satisfactory improvements to the quantum dialogue protocol of Ba An [10] was obtained in [12]. Later on Xia et al. proposed a protocol of quantum dialogue using *GHZ* states [13] and Dong et al. proposed a protocol of quantum dialogue using tripartite *W* states [14]. 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 quantum dialogue have also been proposed using (i) dense coding [11,13,15], (ii) entanglement swapping [16], (iii) single photon [17], (iv) auxiliary particles [18], etc. These protocols are referred to as bidirectional quantum communication protocols [18], quantum telephone [15,19], quantum dialogue [10,17], quantum conversation [20], etc. These are actually different names used for equivalent protocols. Here we will refer all of them as quantum dialogue and provide a generalized structure to the Ba An type of quantum dialogue protocols and will use the generalized structure to obtain several examples of quantum systems where quantum dialogue is possible. Before we describe those specific quantum systems it is important to understand that in quantum dialogue 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 Bob is encoded) must simultaneously contain the information encoded by both parties. This particular point distinguishes quantum dialogue protocol from the QSDC and DSQC protocols. Otherwise, Alice and Bob can always communicate with each other by using DSQC/QSDC in two steps or by using two different quantum channels (i.e. by using a DSQC/QSDC scheme from Alice to Bob and another from Bob to Alice) but as the secret information of Alice and Bob is not simultaneously encoded in the same quantum channel, this is not quantum dialogue. This important and distinguishing feature of quantum dialogue is often overlooked by authors. For example, Jain, Muralidharan and Panigrahi's [20] protocol is essentially two QSDC. Clearly, their protocol is not a protocol of quantum dialogue as Bob knows the encoded information of Alice even before he encodes his own information.

The remaining part of the Letter is organized as follows: In Section 2, we have briefly described the Ba An protocol and have explored its intrinsic symmetry. We have observed that information splitting is in the core of these protocols.[2] In Section 3 we have provided a sufficient condition for construction of quantum dialogue protocol and have shown that the operators used for encoding of information in a quantum dialogue protocol should form a group. In Section 4 we have provided a generalized protocol of the quantum dialogue 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 be encoded by this group of unitary operators. A systematic procedure for construction of such groups and specific examples of states that can be used to implement the generalized protocol of quantum dialogue are provided in Section 5. It is shown that *GHZ* state, *GHZ-like* state, *W* state, Cluster state, Ω state, Q_4 state and Q_5 state can be used for implementation of quantum dialogue protocol. In Section 6, we have shown that if a quantum system is found to be suitable for quantum dialogue then that can be used to provide a solution of the socialist millionaire problem too. Finally, Section 7 is dedicated for conclusion.

2. The Ba An protocol and its intrinsic symmetry

Let us first describe Ba An's original scheme of quantum dialogue. This simple scheme works in the following steps:

Step 1 Bob prepares large number of copies of a Bell state $|\phi^+\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$. He keeps the first qubit of each Bell state with himself as home qubit and encodes his secret message 00, 01, 10 and 11 by applying unitary operations U_0, U_1, U_2 and U_3 respectively on the second qubit. Without loss of generality we may assume that $U_0 = I$, $U_1 = \sigma_x = X$, $U_2 = i\sigma_y = iY$ and $U_3 = \sigma_z = Z$ where σ_i are Pauli matrices.

Step 2 Bob then sends the second qubit (travel qubit) to Alice and confirms that Alice has received a qubit.

Step 3 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 Bell basis 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 this is a modification of Ping-Pong protocol [7] and the operations used for encoding are the operators usually used for dense coding and the protocol starts with an initial state $|\psi\rangle_{initial} = |\phi^+\rangle$. Now after Step 1, $|\phi^+\rangle$ is mapped to one of the Bell states $|\psi\rangle_{intermediate} = U_B|\psi\rangle_{initial} = U_B|\phi^+\rangle$ depending upon the secret message of Bob which is encoded by unitary operation U_B (to be precise, we may say that the state at this time is one of the Bell states $I|\phi^+\rangle = |\phi^+\rangle$, $X|\phi^+\rangle = |\psi^+\rangle$, $iY|\phi^+\rangle = |\psi^-\rangle$, $Z|\phi^+\rangle = |\phi^-\rangle$). 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 message using the same set of unitary operations and Alice's encoding will map the state into another Bell state $|\psi\rangle_{final} = U_A|\psi\rangle_{intermediate} = U_AU_B|\psi\rangle_{initial} = U_AU_B|\phi^+\rangle$. Now here information splitting is done in an excellent way. Alice, Bob and Eve, all know $|\psi\rangle_{initial}$ and $|\psi\rangle_{final}$ 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 $|\psi\rangle_{final} = |\phi^+\rangle$ thus $U_AU_B = I$, this is possible in 4 different ways: $U_A = U_B = I$, $U_A = U_B = X$, $U_A = U_B = iY$, $U_A = U_B = Z$. 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 (same classical bits in this particular example), but that do not reveal the encoding of Alice and Bob. Since in this quantum dialogue protocol secure classical information (4 bits of classical information in this case as 2 bits are sent from Alice to

[2] Information splitting plays the central role in every secure quantum communication protocol.