Contents lists available at SciVerse ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Maximally efficient protocols for direct secure quantum communication

Anindita Banerjee [a,b], Anirban Pathak [a,c,*]

[a] Department of Physics and Materials Science Engineering, 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, 77146 Olomouc, Czech Republic

ARTICLE INFO

Article history:
Received 18 March 2012
Received in revised form 30 July 2012
Accepted 20 August 2012
Available online 23 August 2012
Communicated by P.R. Holland

Keywords:
Quantum cryptography
Deterministic secure quantum communication
Quantum secure direct communication
Applications of dense coding
Efficiency of quantum communication

ABSTRACT

Two protocols for deterministic secure quantum communication (DSQC) using GHZ-*like* states have been proposed. It is shown that one of these protocols is maximally efficient and that can be modified to an equivalent protocol of quantum secure direct communication (QSDC). Security and efficiency of the proposed protocols are analyzed and compared. It is shown that dense coding is sufficient but not essential for DSQC and QSDC protocols. Maximally efficient QSDC protocols are shown to be more efficient than their DSQC counterparts. This additional efficiency arises at the cost of message transmission rate.

1. Introduction

A protocol for quantum key distribution (QKD) was first introduced in 1984 by Bennett and Brassard [1]. Since then several protocols for different cryptographic tasks have been proposed. Most of the initial works [1–3] on quantum cryptography were limited to QKD. But very soon people realized that quantum states can be used for more complex and more specific cryptographic tasks. For example, in 1999, Hillery et al. [4] proposed a protocol for quantum secret sharing (QSS). Almost simultaneously, Shimizu and Imoto [5] proposed a protocol for direct secure quantum communication using entangled photon pairs. These protocols established that unconditionally secure quantum communication is possible without the generation of keys. Such protocols of direct secure quantum communications are broadly divided into two classes: (a) Protocols for deterministic secure quantum communication (DSQC) [6–10] and (b) protocols for quantum secure direct communication (QSDC) [11,12]. In DSQC protocols receiver (Bob) can read out the secret message only after at least one bit of additional classical information for each qubit is transmitted by the sender (Alice). In contrary to this, no such exchange of classical information is required in QSDC protocols [13]. A conventional QKD protocol generates the unconditionally secure key by quantum means but then uses classical cryptographic resources to encode the message. No such classical means are required in DSQC and QSDC. Further, since all DSQC and QSDC protocols can be used to distribute keys, these protocols of direct communications are more useful than the traditional QKD protocols. In recent past, these facts have encouraged several groups to study DSQC and QSDC protocols in detail [[13] and reference therein].

In the pioneering work of Shimizu and Imoto [5], they had cleverly used entangled photon pairs and Bell measurement to achieve the task of DSQC. In 2002, Beige et al. [14] extended the idea and proposed another protocol for DSQC using single photon two-qubit states. But eventually the authors themselves found out the protocol to be insecure. In the same year, Bostrom and Felbinger proposed the famous ping-pong protocol [11] of QSDC, which uses EPR states for communication. Since then several unconditionally secure protocols of DSQC and QSDC are presented. The unconditional security of those protocols is obtained by using different quantum resources.[1] We are specifically interested in the DSQC protocols based on the rearrangement of order of particles. Such a protocol was first proposed by Zhu et al. [8] in 2006 but almost immediately after its publication, it was reported by Li et al. [6]

* Corresponding author at: Department of Physics and Materials Science Engineering, Jaypee Institute of Information Technology, A-10, Sector-62, Noida, UP-201307, India. Tel.: +420 608 650694.
E-mail address: anirban.pathak@jiit.ac.in (A. Pathak).

[1] In principle the unconditional security arises from quantum non-realism and conjugate coding.

0375-9601/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.physleta.2012.08.032

that the protocol of Zhu et al. is not secure under Trojan horse attack. Li et al. had also proposed a modified version of Zhu et al.'s protocol. Thus Li et al.'s protocol may be considered as the first unconditionally secure protocol of DSQC based on rearrangement of order of the particles. In the last five years, many such protocols of DSQC are proposed. Very recently, Yuan et al. [10] and Tsai, Hsieh and Hwang [15] have proposed two very interesting DSQC protocols based on rearrangement of order of the particles. The Yuan et al. protocol uses four-qubit symmetric W state for communication, while the Tsai, Hsieh and Hwang's protocol utilizes the dense coding of four-qubit cluster states. Present work aims to improve the qubit efficiency of the existing DSQC protocols and to explore the possibility of designing DSQC and QSDC protocols using GHZ-*like* states and other quantum states.

GHZ states have been used for quantum information processing since a long time. Recently, the ideas have been extended to GHZ-*like* states [4,16–19]. GHZ-*like* states belong to GHZ class and can be generated by an EPR state, a single qubit state and a controlled-NOT operation. GHZ-*like* states can be described in general as

$$\frac{(|\psi_i\rangle|0\rangle+|\psi_j\rangle|1\rangle)}{\sqrt{2}}, \tag{1}$$

where $i, j \in \{0,1,2,3\}$, $i \neq j$ and also $|\psi_i\rangle$ and $|\psi_j\rangle$ are Bell states which are usually denoted as

$$\begin{aligned}
|\psi_0\rangle &= |\psi_{00}\rangle = \left|\psi^+\right\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}},\\
|\psi_1\rangle &= |\psi_{01}\rangle = \left|\phi^+\right\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}},\\
|\psi_2\rangle &= |\psi_{10}\rangle = \left|\psi^-\right\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}},\\
|\psi_3\rangle &= \left|\psi_{11}\right\rangle = |\phi^-\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}.
\end{aligned} \tag{2}$$

Earlier we have shown that GHZ-*like* states are useful for controlled quantum teleportation and quantum information splitting [19]. Here we have shown that we can form an orthonormal basis set in 2^3-dimensional Hilbert space with 8 GHZ-*like* states, which can be used for dense coding and DSQC. Thus GHZ-*like* states are established as a useful resource for quantum information processing. Remaining part of the Letter is organized as follows: In the following section a protocol for DSQC using GHZ-*like* states without complete utilization of dense coding is provided. In Section 3 we have provided an efficient protocol of DSQC using GHZ-*like* states with complete utilization of dense coding. In Section 4 it is shown that the second DSQC protocol (i.e. the one with complete utilization of dense coding) may be converted to an equivalent QSDC protocol having better qubit efficiency. In Section 5 we have analyzed the security and efficiency of the proposed DSQC and QSDC protocols and have shown that the proposed protocols are unconditionally secure and maximal efficiency can be achieved here. Finally, we have concluded the work in Section 6 and have shown that any set of orthogonal states where dense coding is possible may be used for DSQC (and QSDC) and consequently for QKD. Some examples of such quantum states, which may be used for designing of efficient DSQC and QSDC protocols, are provided. Further, it is shown that dense coding is sufficient but not essential for DSQC and QSDC protocols of the present kind.

2. DSQC using GHZ-*like* states without complete utilization of dense coding

Let us suppose that Alice and Bob are two distant or spatially separated legitimate/authenticated communicators. Alice wants to transmit a secret classical message to Bob. The proposed protocol of DSQC can be implemented by the following steps:

DSQC1 Alice prepares the state $|\lambda\rangle^{\otimes n}$, where $|\lambda\rangle = \frac{|\phi^+0\rangle+|\psi^+1\rangle}{\sqrt{2}} = \frac{|0\phi^+\rangle+|1\psi^+\rangle}{\sqrt{2}}$ is a GHZ-*like* state. $|\lambda\rangle^{\otimes n}$ is a $3n$-qubit state, whose qubits[2] are indexed as $p_1, p_2, \ldots, p_{3n}$. Thus p_s is the sth qubit of $|\lambda\rangle^{\otimes n}$ and $\{p_{3l-2}, p_{3l-1}, p_{3l}\colon\ l \leqslant n\}$ are the three entangled qubits of lth GHZ-*like* state $|\lambda\rangle$.

DSQC2 Alice applies unitary operation $\{U_{00} = X \otimes I, U_{01} = I \otimes I, U_{10} = I \otimes Z, U_{11} = I \otimes iY\}$ on the first two qubits of each GHZ-*like* state to encodes the secret message $\{00, 01, 10, 11\}$ respectively. Here I is the single qubit identity operator and $X = \sigma_x$, $Y = \sigma_y$ and $Z = \sigma_z$ are usual Pauli operators. These operations U_{ij} $(i, j \in \{0,1\})$ will transform the GHZ-*like* state $|\lambda\rangle$ into another orthogonal GHZ-*like* state $|\lambda_{ij}\rangle$ i.e. $|\lambda_{ij}\rangle = U_{ij}|\lambda\rangle$.

DSQC3 Alice keeps the first photon of each GHZ-*like* state with her and prepares an ordered sequence, $P_A = [p_1, p_4, p_7, \ldots, p_{3n-2}]$. Similarly, she uses all the remaining photons to prepare an ordered sequence $P_B = [p_2, p_3, p_4, p_5, \ldots, p_{3n-1}, p_{3n}]$ for Bob and randomizes it by applying a permutation operator Π_{2n}. Thus Alice creates a random sequence $P'_B = \Pi_{2n} P_B$. The actual order is known to Alice only.

DSQC4 To prevent eavesdropping, Alice prepares $m = 2n$ decoy photons.[3] The decoy photons are randomly prepared in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$ i.e. decoy photons state is $|\phi_{2n}\rangle = \bigotimes_{j=1}^{2n} |P_j\rangle$, $|P_j\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ $(j = 1, 2, \ldots, m)$. Then Alice randomly inserts these decoy photons into the sequence P'_B and that yields a new sequence P''_B, which she transmits to Bob. P_A remains with Alice.[4]

DSQC5 After confirming that Bob has received the entire sequence P''_B, Alice announces the positions of the decoy photons. Bob measures the corresponding particles in the sequence P''_B by using X basis or Z basis at random, here $X = \{|+\rangle, |-\rangle\}$ and $Z = \{|0\rangle, |1\rangle\}$. After measurement, Bob informs his outcomes to Alice who computes error rate. If sufficiently few errors are found they go to the next step otherwise they repeat the protocol.

DSQC6 Alice discloses the remaining ordering information Π_{2n}.

DSQC7 Bob rearranges the particle pairs and perform Bell measurements on them. Alice also measures her qubits in computational (Z) basis and announces the result. Now Bob decodes the encoded information by using Table 1.

Let us explain the protocol with a simple example, assume that Alice has to communicate a six bit secret message 100001. Since

[2] In the entire manuscript we have used photon and qubit as anonymous but all the conclusions will remain valid for other form of qubits too.

[3] In this kind of protocols it is often assumed that number of decoy photon $m \ll n$. For example, such an assumption is used in Yuan et al. protocols [10]. This is not a correct assumption because if $m \ll n$ then Bob may fail to detect Eve as there will be a finite possibility that most of the verification-qubits (decoy states) are not measured by Eve. In contrary, when $2x$ qubits (a random mix of message qubits and decoy qubits) travel through a channel accessible to Eve and x of them are tested for eavesdropping then for any $\delta > 0$, the probability of obtaining less than δn errors on the check qubits (decoy qubits), and more than $(\delta + \epsilon)n$ errors on the remaining x qubits is asymptotically less than $\exp[-O(\epsilon^2 x)]$ for large x [20]. As the unconditional security obtained in quantum cryptographic protocol relies on the fact that any attempt of eavesdropping can be identified. Thus to obtain an unconditional security we always need to check half of the travel qubits.

[4] Alternatively Alice may use part of the original sequence for verification and the remaining part for encoding of information (messaging).