Improved protocols of secure quantum communication using W states

Dr. Vandana Vanegal

Abstract

Two effective and stable quantum communication protocols using 3-qubit and 4-qubit symmetric W states have recently been suggested. These two protocols based on dense coding are extended and their efficiencies are greatly increased. Simple bounds are obtained on the qubit efficiency of deterministic secure quantum communication (DSQC) and quantum secure direct communication (QSDC) protocols, and it is shown that dense coding is not sufficient for the design of DSQC and QSDC protocols that are maximally effective. This fact is used to develop DSQC and QSDC protocols that are maximally effective using 3-qubit and 4-qubit W states.

Keywords: Determinist safe quantum communication, 3-qubit and 4-qubit W states

Introduction

Several DSQC and QSDC protocols have been proposed [1]. We would like to remember, however, that all the QKD, DSQC and QSDC protocols basically require the separation of knowledge into two or more bits. The non-revealing of the encoded bit should have each piece by itself. This data slicing can be achieved in many ways. Here, it can clearly be shown that the knowledge is split into two quantum pieces in the GV [2], PP [3], CL [4] and DLL [5] protocols, but it is split into a quantum piece and a classical piece in BB84 and the PoP-based protocols. To be accurate, we first verify in DLL, PP, CL and other QSDC protocols that the first quantum piece of data is sent to the receiver without any eavesdropping. The encoding operation is performed only when this is assured. As a consequence, Eve will never have access to the two pieces of data and a particular piece by itself is non-revealing. We need simultaneous access to both of the pieces for efficient decoding. Bob has this requisite simultaneous entry, but Eve doesn't have it because she can't withhold the quantum piece and wait for the classical piece to be revealed. In the protocols based on PoP, this is the secret of confidentiality. This interesting and nice trick is correctly used in most of the recent protocols of DSQC [1]. In most of DSQC1’s recent protocols, this fascinating and good trick is correctly used. Examples of recent proposals, however, occur where the splitting of data is not handled properly. For e.g. The necessary rearrangement of particle ordering is not achieved in Zhao et al. [6] and some other proposals. Interestingly, most of the DSQC protocols recently proposed still use dense coding operations to encrypt the content. The coupling between dense coding and effective DSQC and QSDC protocols became so intense that people began to believe that the most efficient DSQC/QSDC protocol using W states cannot be designed because maximum dense coding in W states is not feasible [7]. Keeping this in mind, many authors used W states to construct inefficient (non-maximally efficient) DSQC and QSDC protocols and found their protocols to be successful. Contrary to this assumption, we demonstrate in this chapter that for the implementation of maximally efficient DSQC and QSDC protocols, dense coding is not required. We also demonstrate that maximally efficient DSQC and QSDC protocols can be constructed using W states and without the use of dense coding. However as the dense coding is not maximal, the performance of such protocols would not be maximal. We also presented the DSQC generalised protocol that is usually valid for n-qubit symmetric W states, but only n = 3 and n = 4 are provided for the explicit tables of encoding operations. It has been shown that for the implementation of the protocol, dense coding is not necessary. The proposed protocol is further expanded and its connection to QKD is defined as a QSDC protocol.
Existing DSQC and QSDC protocols using symmetric W states

W states have been rigorously researched for a decade as an important resource for quantum communication activities [7]. The goal is not to address all the quantum information processing proposals using W states, but our attention is only on protocols for DSQC and QSDC. In 2006, Cao and Song [8] first suggested a DSQC protocol using the 4-qubit W condition. Using a 4-qubit W state, the Cao and Song protocol will transmit 1 bit of classical data. The Cao and Song protocol, therefore, is not really successful. Similarly, in the following years, some DSQC protocols were also introduced using 3-qubit W states. Using 3-qubit W condition, these protocols can only relay 1 bit of classical qubit W state and 4-qubit W state status [7, 8]. Tsai et al. [9] proposed protocol will transmit 4 bits of classical data using the 4-qubit cluster state. Since dense coding operations are used by these protocols and maximum dense coding is permitted in a cluster state, but not in a W state, it seems reasonable that the protocol based on the cluster state is more efficient.

Generalized protocol of DSQC using symmetric W states

We define a protocol here which is generally true for n-qubit symmetric W states, but only n = 3 and n = 4 are given for the explicit tables of encoding operations. The protocol performs as follows:

Alice prepares a large number of copies (say N copies) of the initial state |W0 which is a symmetric n-qubit W state. Then, she encodes her n-bit classical secret message by applying n-qubit unitary operators \{U_0, U_1, \ldots, U_2^n \} as described in the Table 1 for n = 3 and in Table 2 for n = 4. For example, to encode

\[ 000 \ldots 0_n, 010 \ldots 0_n, 100 \ldots 1_n \]

She applies \( U_0, U_1, \ldots, U_2^n \) n times, respectively. The unitary operators are chosen in such a way that the information encoded states are mutually orthogonal. As Bob knows the initial state and which unitary operation corresponds to what encoded states are mutually orthogonal. As Bob knows the initial state and which unitary operation corresponds to what information about the encoded state and consequently this operation executed by Alice as the encoded information is not obtain any meaningful information about the encoding 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 will not obtain any meaningful information about the encoding operation executed by Alice as the encoded information is randomized by the rearrangement of the order of the particles.

Alice announces the exact sequence.

Bob appropriately orders his sequence and measures his qubits in W basis. This deterministically decodes the information sent by Alice.

How to convert this protocol into a QSDC protocol

The above protocol is a protocol of DSQC as Alice needs to announce the actual order of the sequence. Rearrangement of particle ordering may be avoided by sending the encoded states in n-steps and by checking eavesdropping after each step. Assume that Alice first sends a sequence of all the first qubits with N decoy photons, if no eavesdropping is traced then only she sends the sequence of second photons and so on. Then, the DSQC protocol will be reduced to a QSDC protocol as no classical information will be required for decoding. The previous protocol can be easily generalized to a QSDC protocol. After confirming that Bob has received the entire sequence, she announces the position of the decoy photons and checks eavesdropping. If eavesdropping is found she truncates the protocol otherwise she sends the second sequence PB2+N to Bob and checks for eavesdropping and if no eavesdropping is found then she sends the third sequence and check for eavesdropping and the process continues. Now, Bob can measure the final states in appropriate basis and obtain the message sent by Alice. Since Eve cannot obtain more than 1 qubit of an n-partite state (as we are sending the qubits, one by one and checking for eavesdropping after each step) she has no information about the encoded state and consequently this direct quantum communication protocol is secure. Thus, the rearrangement of particle order is not required if we do the communication in multiple steps. Further, since no quantum measurement is done at Alice’s end and rearrangement of particle order is not required, this protocol does not require any classical communication for the decoding operation. Thus, it is a QSDC protocol. Its efficiency will be naturally higher than the previous protocol. This is so because here Alice does not need to disclose the actual sequence and consequently the amount of classical communication required for decoding of the message is reduced.

Efficiency analysis

In the existing literature, two analogous but different parameters are used for analysis of efficiency of DSQC and QSDC protocols. The first one is simply defined as

\[ \eta = \frac{c}{q} \]

Where \( c \) denotes the total number of transmitted classical bits (message bits) and \( q \) denotes the total number of qubits used.
Table 1: Encoding operations for implementation of maximally efficient DSQC and QSDC protocol using symmetric 3-qubit W state.

| Unitary operators | 3-qubit W state |
|-------------------|-----------------|
| $U_0 = I \otimes I \otimes I$ | $\frac{1}{\sqrt{3}} (|001\rangle + |010\rangle + |100\rangle)$ |
| $U_1 = X \otimes I \otimes I$ | $\frac{1}{\sqrt{3}} (|101\rangle + |110\rangle + |000\rangle)$ |
| $U_2 = i Y \otimes X \otimes I$ | $\frac{1}{\sqrt{3}} (-|111\rangle - |100\rangle + |010\rangle)$ |
| $U_3 = i Y \otimes Y \otimes X$ | $\frac{1}{\sqrt{3}} (|110\rangle - |101\rangle - |011\rangle)$ |
| $U_4 = Z \otimes X \otimes iY$ | $\frac{1}{\sqrt{3}} (|101\rangle + |010\rangle - |110\rangle)$ |
| $U_5 = I \otimes Y \otimes Y$ | $\frac{1}{\sqrt{3}} (|011\rangle + |000\rangle - |110\rangle)$ |
| $U_6 = X \otimes iY \otimes Y$ | $\frac{1}{\sqrt{3}} (|110\rangle + |010\rangle + |101\rangle)$ |
| $U_7 = I \otimes Z \otimes iY$ | $\frac{1}{\sqrt{3}} (|100\rangle + |011\rangle + |110\rangle)$ |

Table 2: Encoding operations for implementation of maximally efficient DSQC and QSDC protocol using symmetric 4-qubit W state.

| Unitary operators | 4-qubit W state |
|-------------------|-----------------|
| $I \otimes I \otimes I \otimes I$ | $(|0000\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$ |
| $X \otimes I \otimes I \otimes I$ | $(|0000\rangle + |0010\rangle + |0100\rangle + |1000\rangle)$ |
| $iY \otimes Z \otimes I \otimes I$ | $(|0000\rangle + |0010\rangle - |1010\rangle - |1000\rangle)$ |
| $I \otimes iY \otimes I \otimes I$ | $(|0000\rangle - |0101\rangle - |1001\rangle - |1100\rangle)$ |
| $Z \otimes X \otimes I \otimes I$ | $(|0000\rangle + |0101\rangle + |1010\rangle + |1110\rangle)$ |
| $Z \otimes Z \otimes X \otimes iY$ | $(|0000\rangle + |0010\rangle + |0111\rangle + |1111\rangle)$ |
| $I \otimes I \otimes X \otimes iY$ | $(|0010\rangle + |0110\rangle + |1110\rangle + |1010\rangle)$ |
| $Z \otimes Z \otimes X \otimes iY$ | $(|0000\rangle + |0010\rangle + |0111\rangle + |1111\rangle)$ |
| $X \otimes X \otimes iY \otimes iY$ | $(|0010\rangle + |0110\rangle + |1110\rangle + |1010\rangle)$ |

Conclusions

From the LM05 protocol and its derivatives, it was well known that dense coding for QSDC is not necessary. Due to the performance of the CL protocol in increasing the reliability of the PP protocol by using dense coding and the use of dense coding in all subsequent effective DSQC and QSDC protocols, it has become standard practise to use dense coding to develop modern stable direct quantum communication protocols. First we have seen here that the performance of current protocols using 4-qubit W states can be enhanced by the appropriate use of dense coding. They're procedures. We also provided two new alternative schemes for dense coding of 4-qubit W states for that reason. Then we have seen that the use of dense coding is not necessary when we use a DSQC protocol based on PoP technique. It is necessary for a simple encoding that maps the input state into a series of mutually orthogonal states.

References

1. Long GL, Deng FG, Wang C, Li XH, Wen K, Wang WY. “Quantum Secure Direct Communication and Deterministic Secure Quantum Communication”, Front. Phys. China 2007;2:251-272.
2. Goldenberg L, Vaidman L. Quantum Cryptography Based on Orthogonal States, Phys. Rev. Lett 1995;75:1239-1243.