Quantum secure direct communication with optimal quantum superdense coding by using general four-qubit states

Zhihao Liu · Hanwu Chen · Wenjie Liu · Juan Xu · Dong Wang · Zhiqiang Li

Received: 31 January 2012 / Accepted: 27 March 2012 / Published online: 10 April 2012
© Springer Science+Business Media, LLC 2012

Abstract  From the perspective of quantum circuit, a construction framework and a measurement framework of a general kind of four-qubit states are sketched, respectively. By utilizing the properties of this kind of states, a quantum secure direct communication (QSDC) protocol is put forward, which adopts the idea of optimal quantum superdense coding to achieve a maximal efficiency and high resources capacity. The security of the proposed protocol is discussed in detail and it is proved to be secure theoretically. Moreover, the sufficient and necessary condition of which multipartite states are suitable for optimal quantum superdense coding in quantum secure direct communication is figured out.

Keywords  Quantum cryptography · Quantum secure direct communication · Quantum superdense coding · Four-qubit state
1 Introduction

Quantum mechanics contains a lot of magic laws, such as no-cloning theorem and Heisenberg uncertainty principle. Quantum cryptography communication is one of its remarkable applications in quantum information. Quantum key distribution (QKD), an important branch of quantum cryptography communication, provides a secure way for two legitimate parties to create a secret key over a long distance with negligible leakage of information. Since the famous BB84 protocol [1] was proposed by Bennett and Brassard first, a great many QKD schemes have been put forward, such as the E91 [2], BBM92 [3], B92 [4] and six-state protocol [5].

Recently, the so-called quantum secure direct communication (QSDC), a novel branch of quantum cryptography communication, has been proposed and pursued. With QSDC, two legitimate users can transmit their private key (even plaintext) directly in a deterministic and secure way. In Long et al. [6] proposed the strategy of direct communication in QKD. Meanwhile Beige et al. [7] presented a QSDC scheme with two-qubit single photons. Then Boström and Felbinger [8] put forward a “Ping-pong” protocol with Einstein-Podolsky-Rosen (EPR) pairs. Later, Deng et al. [9] proposed the “two-step” protocol using EPR pair block, where the dense coding idea was generalized into secure communication. Afterwards, a lot of QSDC achievements [10–31] were made. All of these protocols are on the basis of the use of concrete resources without exception, and we note that some QSDC protocols with different resources have the same ability of communication. For example, every four-particle $\chi$-type entangled state [32] carries four bits of classical information in Lin et al.s’ QSDC protocol [33]. So does every four-qubit cluster state [34] in Cao et al.s’ [35] and Tsai et al.s’ [36] QSDC protocols. The idea of optimal quantum superdense coding is generalized to these schemes. Here, the meaning of optimal quantum superdense coding is that the sender Alice can decode two bits of information on two of the four qubits respectively. That is to say, these three protocols have the same ability of communication, but different communication resources are exploited. However, why different concrete resources have the same ability in quantum communication is rarely studied. Inspired by these three QSDC protocols, a thought comes to our minds: Are there any other four-qubit states can be also used for QSDC with optimal quantum superdense coding? Fortunately, the answer is true, and it will be shown that any four-qubit states having the same applications have certain connections.

In this paper, a construction framework of a general kind of four-qubit states will be firstly sketched from the perspective of quantum reversible logic circuits. Of course, for the sake of realizing the measurement of this kind of states, a quantum logic circuit will be also designed. Then it can be found that this kind of states can be applied to QSDC with optimal quantum superdense coding as the same as the four-qubit $\chi$-type entangled states and the four-qubit cluster states. With optimal quantum superdense coding, the proposed protocol has high resource capacity and the maximum efficiency 100%. Through analyzing the security, it shows that the proposed protocol is secure against usual attacks. What’s more important, a theorem about what four-qubit states can be used for optimal quantum superdense coding in quantum secure direct communication will be put forward and proved. That is to say, we deduce the general cases of which four-qubit states can be utilized for QSDC with optimal quantum superdense coding.