Three-step semiquantum secure direct communication protocol

ZOU XiangFu1,2,3 & QIU DaoWen1,4*

1. Department of Computer Science, Sun Yat-sen University, Guangzhou 510006, China;
2. School of Mathematics and Computational Science, Wuyi University, Jiangmen 529020, China;
3. Department of Computer Science and Engineering, the Chinese University of Hong Kong, Hong Kong, China;
4. SQIG–Instituto de Telecomunicações, Departamento de Matemática, Instituto Superior Técnico,
Universidade de Lisboa, Av. Rovisco Pais 1049-001, Lisbon, Portugal

Received November 20, 2013; accepted February 12, 2014; published online June 23, 2014

Quantum secure direct communication is the direct communication of secret messages without need for establishing a shared secret key first. In the existing schemes, quantum secure direct communication is possible only when both parties are quantum. In this paper, we construct a three-step semiquantum secure direct communication (SQSDC) protocol based on single photon sources in which the sender Alice is classical. In a semiquantum protocol, a person is termed classical if he (she) can measure, prepare and send quantum states only with the fixed orthogonal quantum basis \{\ket{0}, \ket{1}\}. The security of the proposed SQSDC protocol is guaranteed by the complete robustness of semiquantum key distribution protocols and the unconditional security of classical one-time pad encryption. Therefore, the proposed SQSDC protocol is also completely robust. Complete robustness indicates that nonzero information acquired by an eavesdropper Eve on the secret message implies the nonzero probability that the legitimate participants can find errors on the bits tested by this protocol. In the proposed protocol, we suggest a method to check Eves disturbing in the doves returning phase such that Alice does not need to announce publicly any position or their coded bits value after the photons transmission is completed. Moreover, the proposed SQSDC protocol can be implemented with the existing techniques. Compared with many quantum secure direct communication protocols, the proposed SQSDC protocol has two merits: firstly the sender only needs classical capabilities; secondly to check Eves disturbing after the transmission of quantum states, no additional classical information is needed.

quantum secure direct communication, semiquantum, complete robustness, security

PACS number(s): 03.67.Dd, 03.65.Sq, 03.67.Hk

The most spectacular discovery in quantum computing to date is that quantum computer can efficiently perform some tasks which are likely not feasible on a classical computer. For example, Shor [1] quantum algorithm can solve efficiently two enormously important problems: the problem of finding the prime factors of an integer and the discrete logarithm problem. This indicates most of classical public key cryptographies are not secure if quantum computers could be developed in the future. Fortunately, quantum cryptography depends on fundamental laws of quantum physics to provide unconditional security [2–14].

The question of what a quantum protocol should be, in order to achieve a significant advantage over all classical protocols, is of great interest [15]. To answer this question in the
field of quantum key distribution (QKD), Boyer et al. [15] recently suggested the idea of semiquantum key distribution (SQKD) in which Bob was classical and they proposed an SQKD protocol based on measure-resend. In a semiquantum protocol, a person is called classical if he (she) can measure, prepare and send quantum states only with the fixed orthogonal quantum basis \{(0), (1)\}. For convenience, we will term the Boyer SQKD protocol as BKM2007. In addition, BKM2007 has been proved to be completely robust [15]. This indicates that nonzero information acquired by an eavesdropper Eve on the secret message implies the nonzero probability that the legitimate participants can find errors on the bits tested by this protocol. Because the SQKD is conceptually novel and interesting, this work has been discussed by many researchers [16–26].

Note that, some applications of SQKD have been researched [27, 28]. Li et al. [27] proposed two semiquantum secret sharing protocols using maximally entangled Greenberger-Horne-Zeilinger states. Wang et al. [28] presented a semiquantum secret sharing protocol by using two-particle entangled states in which quantum Alice shares a secret key with two classical parties, Bob and Charlie.

Quantum secure direct communication (QSDC) is a new research direction in the quantum cryptography [29–52]. Different from quantum key distribution [2–14] whose object is to establish a random key between the two parties of communication, QSDC is the direct communication of secret messages without first producing a shared secret key. Note that the secure direct communication is a task that the classical cryptography cannot achieve. Long and Liu [29] proposed theoretically efficient high capacity QKD scheme and generalized their QKD scheme to the case of multiple legitimate users. In fact, to generalize their QKD scheme to multisusers, they [29] constructed the first QSDC scheme. Boström and Felbinger [30] presented a semi-secure deterministic quantum communication protocol based on an entangled pair of qubits. However, Wójcik [31] revealed that the QSDC protocol presented by Boström and Felbinger [30] is not secure as far as quantum channel losses are taken into account. Zhang et al. [32] improved the eavesdropping scheme of Wójcik [31] by constituting a new set of attack operations. Deng and Long et al. [33] proposed a two-step QSDC protocol using blocks of EPR pairs. This scheme is secure because an eavesdropper cannot get both sequences simultaneously. Gao et al. [34] presented a QSDC scheme by EPR pairs and entanglement swapping. Deng and Long [35] proposed a QSDC protocol using quantum one-time pad and single photons. This QSDC protocol does not need entanglement states as the information carrier. Therefore, quantum entanglement and non-locality are not the necessary requirements for QSDC. Other researchers [36] proposed a QSDC protocol by using swapping quantum entanglement and local unitary operations. Gao et al. [37] proposed two quantum secure conditional direct communication schemes where the communications between two communication parties depend on the agreement and help of a trustworthy and cooperative party Charlie. Three high source capacity QSDC protocols using blocks of GHZ state, superdense coding and quantum search algorithm, respectively, was constructed [38–40]. Jin et al. [41] presented a three-party simultaneous QSDC scheme by using GHZ states. Then Deng et al. [42] presented two efficient QSDC network schemes with an ordered EPR pairs. Any one of the authorized users can communicate with another one on the network securely and directly. Others [43] presented a QSDC scheme based on quantum encryption. Wang et al. [44] presented a quantum hyperdense coding protocol and a QSDC protocol based on the quantum hyperdense coding protocol. A two-step QSDC protocol and a bidirectional QSDC network protocol with the hyperentanglement were proposed by Gu et al. [45, 46]. Additionally, Gu et al. [47] gave two robust QSDC schemes with a quantum one-time pad. Shi et al. [48] proposed two QSDC schemes using a set of ordered three-dimensional hyperentangled states. Finally, Guo et al. [49] realized QSDC by swapping entanglements of 3 × 3-dimensional Bell states. Other researchers have suggested a high capacity QSDC protocol with single photons in both the polarization and the spatial-mode degrees of freedom [50]. Sun et al. [51] suggested a QSDC protocol using two-photon four-qubit cluster states. Lastly, Ren et al. [52] presented a robust two-step quantum secure direct communication protocol based on the spatial-mode Bell states and the photonic spatial Bell-state analysis.

In the existing schemes, QSDC is possible when both parties are quantum. It is easy to know that secure direct communication is impossible when both parties are classical. The question needed to be addressed is what is possible when only one party (the receiver Bob) is quantum, yet the other (the sender Alice) has only classical capabilities.

In this paper, we first present a QSDC protocol with this constraint and prove its security. For convenience, we call such a protocol the semiquantum secure direct communication (SQSDC) protocol. Then, it is showed that the proposed protocol can resist the Trojan horse attacks. The security of the proposed SQSDC protocol is guaranteed by the complete robustness of SQKD protocols and the classical one-time pad encryption. Deng et al. [33] noted that a secure direct communication must satisfy two requirements. First, the secret messages should be read out directly by the legitimate user Bob when he receives the quantum states and no additional classical information is needed after the transmission of qubits. Second, the secret messages which have been encoded already with the quantum states should not leak even though an eavesdropper may get hold of the channel. Also, we will show the proposed SQSDC protocol satisfies the two requirements. Moreover, we discuss the method for checking Eves interfering in the doves returning phase such that Alice does not need to announce publicly any position or their coded bits value after the photons transmission is completed. Finally, we point out that the proposed protocol can be implemented with the existing techniques.