Quantum secure direct communication based on supervised teleportation

Yue Li
School of Computer Science and Technology and Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China

Yu Liu
Department of Electronics and Information Engineering and Institute of National Defense Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China

(Dated: November 18, 2007)

We present a quantum secure direct communication (QSDC) scheme as an extension for a proposed supervised secure entanglement sharing protocol. Starting with a quick review on the supervised entanglement sharing protocol — the “Wuhan” protocol [Y. Li and Y. Liu, arXiv:0709.1449v2], we primarily focus on its further extend using for a QSDC task, in which the communication attendant Alice encodes the secret message directly onto a sequence of 2-level particles which then can be faithfully teleported to Bob using the shared maximal entanglement states obtained by the previous “Wuhan” protocol. We also evaluate the security of the QSDC scheme, where an individual self-attack performed by Alice and Bob — the out of control attack (OCA) is introduced and the robustness of our scheme on the OCA is documented.

PACS numbers: 03.67.Hk, 03.65.Ud

I. INTRODUCTION

As an important branch of the quantum information science, quantum cryptography has become a more and more attractive study area. It ensures that the secret message is intelligible only to the legitimated parties without being altered or stolen in the quantum communications[1]. Since Bennett and Brassard’s BB84[2] protocol for quantum key distribution (QKD) which is the only proved unconditional secure quantum cryptography protocol where the two remote legitimated users establish the shared secret keys through the quantum channel, and the secret keys can then be used to do the secure communication using a one time classical cryptography scheme. Recently, many new QKD schemes have been proposed and the experimental feasibilities are also concerned, however, because of the QKD steps should be followed before the confidential communication, the communication efficiency is certainly reduced. This, in fact, becomes the motivation to find the more efficient quantum cryptography protocols.

To improve the efficiency issue above, a new concept called quantum secure direct communication (QSDC) was first introduced by Beige et al.[3], which paves a new way to the quantum secure communication. Different from the previous QKD, the QSDC does not need to do any encryption for the secret messages before their transmission. Through this idea, Boström and Felbinger presented a novel deterministic QSDC protocol based on EPR pairs — the “Ping-pong” protocol [4] which allows instantaneous secure communication by keeping the home qubit and sending the travel qubit back and forth for encoding use. Recently, many QSDC protocols have been suggested, and most of these protocols perform a similar framework as the “Ping-pong” protocol especially on the necessity to transmit the qubits with secret message in the public channel, this, however, reserves certain opportunities to a third party Eve to attack the qubit during its traveling. In fact, many eavesdropping schemes which are potential threats to the “Ping-pong” and relevant protocols has been commented using such multiways of the qubit traveling[5], therefore, with the previous efficiency issue, finding a new framework to implement the QSDC which leaves less possibilities for a potential eavesdropping becomes hot.

The quantum teleportation[6], which exemplifies a new goal of the quantum information theory, brings a good implication on the very novel framework development for the QSDC. It achieves the destination of quantum state transfer in a different way by utilizing the prior shared entangled states as the quantum channel and local operation and classical communication (LOCC) protocol[7]. Through this, an arbitrary 2-level state collapses in the sender side and “reborns” in the receiver side without the distance qubit traveling. In Ref. 8, Li and Liu presented a protocol...
for secure entanglement sharing, the “Wuhan” protocol, to achieve faithful teleportation via the tripartite W state, where the reliable quantum teleportation can be expected after the secure entanglement distribution assisted by a third believed supervisor. Based on this protocol, in this paper, we suggest one extended using to achieve the QSDC task in the non-qubit-traveling quantum teleportation framework.

We structure the paper as following, first, we quickly revisit the “Wuhan” protocol; then we go further to our QSDC scheme; before the conclusion, we introduce a new concept for the eavesdropping attack — the out of control attack, around which, we provide a security analysis.

II. REVISIT THE “WUHAN” PROTOCOL

As the fundamental of our QSDC scheme, we would like to give a quick review for the “Wuhan” protocol. The protocol is proposed in order to achieve the secure entanglement sharing for further faithful teleportation. By guaranteeing the secure entanglement distribution under a believed supervisor Charlie, the needed Bell states can be distilled from the initial tripartite W states. The later teleportation using the distilled Bell states becomes faithful because of Charlie’s agreement on cooperation and taking the initial states as both the quantum channel and eavesdropping “sensor”. The brief description of the protocol is given by step in the following:

(S. 0) Protocol initialized in the transmission mode. Charlie prepares a sequence of tripartite W states:

\[ |W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)_{abc}. \]  

(S. 1) Charlie keeps the particles c in Eq. (1) as the home qubits, sending the particles a and b as the travel qubits to Alice and Bob respectively.

(S. 2) After they receive the travel qubits, Charlie announces the switching to the detecting mode, performing a nondeterministic local measurements on his home sequence using the basis \( B_z = \{ |0\rangle, |1\rangle \} \). He publishes the location of the measured qubits, according to which Alice and Bob do their own local measurements on their received travel sequence, then publish their outcomes.

(S. 3) Charlie does a comparison by following the proposed checking algorithm to examine whether the qubits have been altered or stolen. If Eve is detected, Charlie then claims to discard this communication and restarts a new round protocol to (S. 0), else protocol continues.

(S. 4) Charlie uses the unmeasured qubits left in (S. 2) to organize a new home sequence, performing local measurements on all the particles sequentially, then he extracts the particles whose outcomes are \( |0\rangle \) and publishes their locations in the original home sequence.

(S. 5) On receiving the location information, Alice and Bob pick out the relevant particles in their own travel sequences and the maximal entanglement states which are all in the same state

\[ |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{ab}. \]  

have been already successfully distilled from the tripartite W states between the two parties, therefore, the entanglement source for further teleportations is faithfully prepared.

In general, by following the two key procedures — the initial states distribution and assisted distillation, the “Wuhan” protocol enables faithful teleportation between Alice and Bob, what’s more, the protocol can be continued only when the supervisor Charlie agrees the security of the quantum channel and assists them to distill the needed Bell states.

In the next section, we suggest a simple QSDC scheme based on the promised faithful teleportation, where classical information can be reliably transmitted between the two parties without using any prior encryption.

III. THE FURTHER QUANTUM SECURE DIRECT COMMUNICATION

In this section, we propose a QSDC scheme as an extension for the “Wuhan” protocol. By means of the faithful teleportation guaranteed by the protocol, Alice simply prepares sequence of 2-level particle states according to the secret message using some encoding rule and teleports them to the Bob who can then read out by measuring. We emphasize that the QSDC between the two parties depends on the agreement of the third supervisor Charlie during the entanglement distillation procedure of the “Wuhan” protocol, and because the scheme is framed by the teleportation, there’s no qubit traveling in the quantum channel.
To be more specific, assuming the direction of the QSDC is from Alice to Bob, Alice then prepares her message qubits following some specified encoding rule to represent the classical information and do the teleportation, after their LOCC, Bob measures his qubits, then the classical information from Alice can be faithfully recovered and read out. We give a communication example for the scheme below:

**Example (E. 0)** Suppose Alice uses the basis \( B_x = \{ |+\rangle, |-\rangle \} \) encoding to represent classical information. At the beginning of the scheme, Alice follows the specified encoding rule to prepare the message qubits according to the classical message sequence, for instance, she wants to send the message 010110 to Bob, then the states of the message sequence should be \( |\rangle = | - \rangle | + \rangle | + \rangle | + \rangle | - \rangle \), where the states \( |\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \) and \( |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \) correspond to the classical bits “0” and “1”, respectively.

**Example (E. 1)** By performing the LOCC protocol with Bob, Alice teleports these message qubits, then after Bob recovers the message qubit states on his own travel qubits, he does the local measurements using the basis \( B_x \) and directly reads out Alice’s message.

Note that this QSDC scheme, which is proposed based on a faithful teleportation, is a simple extension for the “Wuhan” protocol. Because of Charlie’s control on the prior entanglement sharing, the QSDC scheme is still in the charge of the supervisor who gifts the two parties much convenience such as no need to consider much about the secure quantum channel building or even the location of each other, etc.. Different from the well known “Ping-pong” protocol, the skeleton of teleportation guarantees that no qubit carrying message travels in the quantum channel between Alice and Bob, which means the scheme transmits classical information without revealing any information to a potential eavesdropper hidden in the quantum channel. In the next section, we give a more specific discussion on the security of this QSDC scheme.

### IV. THE SECURITY ANALYSIS

In this section, we move on to the security of this QSDC scheme. As the scheme is played on the “Wuhan” protocol, the security of this scheme should be examined in two phases — the “Wuhan” protocol and later encoded teleportation. In Ref. 8, a discussion on the security of the “Wuhan” protocol has already been documented which demonstrates its robustness in case of typical individual eavesdropping attacks such as the intercept-resend attack, entangle-measure attack, etc., therefore the first phase of the security analysis has been fulfilled and what we need to consider in this paper leads to the security on the later phase for the encoded teleportation.

As mentioned, because no qubit is traveling between the two parties during the encoded teleportation, touching the message qubits in the quantum channel for a fourth party Eve becomes impossible, therefore, the security issue may only be brought by Alice and Bob themselves which means the two parties may try to hack the scheme in order to do the under-table communication out of Charlie’s supervision. Through this idea, in the following, we first introduce an example of this potential threat for such supervised teleportation based QSDC scheme — the out of control attack (OCA) [11] by using the same communication protocol framework but different initial states, then we briefly illustrate the robustness of our scheme in case of the OCA.

#### A. The out of control attack

The OCA is a fresh concept for the attacking approaches which is proposed by Alice and Bob themselves and we suggest this be considered in the future quantum secure communication protocol design. Based on the framework of the “Wuhan” protocol with some small modifications, we substitute the original tripartite W state with some other initial state which can also work well with the “Wuhan” protocol, to show that the OCA can successfully attack the modified QSDC scheme after the still secure entanglement sharing, thus the potential security issue brought by the OCA to such kinds of supervised quantum communication protocol is touched.

Assume the initial state be substituted to the state

\[ |\xi\rangle = \frac{1}{2}(|000\rangle + |110\rangle + |011\rangle + |101\rangle)_{abc}, \tag{3} \]

which can still be faithfully shared by the two parties supervised by Charlie after some simple modifications on the steps of the “Wuhan” protocol. It’s quite obvious that the encoded teleportation is still in Charlie’s hand by his local measurements on the home qubits \( c \) and the two parties should contact him for agreement if they naively follow the previous QSDC scheme to do the communication, however, Alice and Bob may perform another under-table QSDC scheme by means of the OCA without Charlie’s acknowledgement. In the following, we show the demonstration of this OCA.
For convenience, we ignore the unitary coefficients in the calculation. As before, Alice follows the previous basis $B_x$ rule to do the encoding on the message qubits which are

\[ |M\rangle = a|0\rangle + b|1\rangle, \]

satisfying $|a|^2 + |b|^2 = 1$, note that $a = 1, b = 1$ gives the state $|+\rangle$ (corresponds to the classical bit “1”) and $a = 1, b = -1$ gives the state $|-\rangle$ (classical bit “0”). With the tripartite new initial state shared by the three communication parties as a whole, they get the joint quardripartite system

\[
|S\rangle_{mabc} = |M\rangle \otimes |\xi\rangle
\]

\[
= (a|0\rangle + b|1\rangle)_m \otimes ((|000\rangle + |110\rangle + |011\rangle + |101\rangle)_{abc}
\]

\[
= (a|0\rangle + b|1\rangle)_m \otimes ((|00\rangle + |11\rangle)_{ab} \otimes |0\rangle_c + (a|0\rangle + b|1\rangle)_m \otimes (|01\rangle + |10\rangle)_{ab} \otimes |1\rangle_c
\]

\[
= |\phi^+\rangle_{ma}(a|0\rangle + b|1\rangle)_b|0\rangle_c + |\psi^+\rangle_{ma}(a|1\rangle + b|0\rangle)_b|0\rangle_c + |\phi^-\rangle_{ma}(a|0\rangle - b|1\rangle)_b|0\rangle_c + |\psi^-\rangle_{ma}(a|1\rangle - b|0\rangle)_b|0\rangle_c
\]

\[
+ |\phi^+\rangle_{ma}(a|1\rangle + b|0\rangle)_b|1\rangle_c + |\psi^+\rangle_{ma}(a|0\rangle + b|1\rangle)_b|1\rangle_c + |\phi^-\rangle_{ma}(a|1\rangle - b|0\rangle)_b|1\rangle_c + |\psi^-\rangle_{ma}(a|0\rangle - b|1\rangle)_b|1\rangle_c,
\]

where $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$.

In the following, we do the individual case analysis cooperating with the specific communication parties as a whole, they get the joint quardripartite system.
In the original protocol which uses the tripartite W state in Eq. (1) the whole system included Alice’s message qubit becomes
\[ |S\rangle_{mabc} = |M\rangle \otimes |W\rangle \\
= (a(0) + b(1))_m \otimes (|100\rangle + |010\rangle + |001\rangle)_abc \\
= (a(0) + b(1))_m \otimes (|10\rangle + |01\rangle)_ab \otimes |0\rangle_c + (a(0) + b(1)) \otimes |00\rangle_{ab} \otimes |1\rangle_c \\
= |\phi^+\rangle_{ma}(a|1\rangle + b|0\rangle)_b|0\rangle_c + |\psi^+\rangle_{ma}(a|0\rangle + b|1\rangle)_b|0\rangle_c + |\phi^-\rangle_{ma}(a|1\rangle - b|0\rangle)_b|0\rangle_c + |\psi^-\rangle_{ma}(a|0\rangle - b|1\rangle)_b|0\rangle_c \\
+ (a(00) + b(10))_ma \otimes |0\rangle_b \otimes |1\rangle_c. \\
(8)\]

Note that in Eq. (8) the item \((a(00) + b(10))_{ma}\) can protect the scheme against the deterministic OCA, because the state \(|X\rangle = (a(00) + b(10))_ma\) can not be deterministically recognized by Alice’s Bell joint measurement, also the state \(|0\rangle\) can not be fully discerned by Bob’s \(B_x\) basis local measurement. In this case, without the exact measurement results, the two parties can not always perform the correct OCA and the efficiency of their QSDC under the OCA greatly decreases. Therefore, based on the correct initial state selection, our QSDC scheme is self-robust on the OCA.

V. CONCLUSIONS

We propose an extension to a QSDC scheme for the “Wuhan” protocol. In this scheme, the encoded message qubits can be reliably transmitted from Alice to Bob by the faithful teleportation. From the security analysis of both the “Wuhan” protocol and this QSDC scheme, we conclude that our QSDC scheme is robust on a series of typical attacks from a fourth eavesdropper and also the introduced OCA from the communication parties themselves. We hope this work will shed some light for the security issue brought by all kinds of self-attacks such as the OCA which should be considered in the future quantum secure communication protocol design.

ACKNOWLEDGMENTS

This research is financially supported by the Innovation Foundation of Aerospace Science and Technology of the China Aerospace Science and Technology Corporation under Grant No. 20060110 and the research foundation for undergraduate novel research from the Ministry of Education of the People’s Republic of China.

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, “Quantum cryptography,” Rev. Mod. Phys. 74: 1, 2002.
[2] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing, Bangalore, India, (IEEE, New York), pp. 175, 1984.
[3] A. Beige, B. G. Englert, C. Kurtsiefer, H. Weinfurter, “Secure communication with a publicly known key,” Acta Phys. Pol. A 101: 357, 2002.
[4] K. Boström and T. Felbinger, “Deterministic secure direct communication using entanglement,” Phys. Rev. Lett. 89: 187902, 2002.
[5] K. Boström and T. Felbinger, “On the security of the Ping-pong protocol,” arXiv:quant-ph/0708. 2986, 2007.
[6] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” Phys. Rev. Lett. 70: 1895, 1993.
[7] M. A. Nielsen, I. L. Chuang, Quantum Information and Computation, Cambridge University Press, UK, 2000.
[8] Y. Li, Y. Liu, “Supervised secure entanglement sharing for faithful teleportation,” arXiv:quant-ph/0709. 1449v2, 2007.
[9] W. Dür, G. Vidal, J. I. Cirac, “Three qubits can be entangled in two inequivalent ways,” Phys. Rev. A 62: 062314, 2000.
[10] Each particle \(c\) in the home sequence owns a probability, say \(d\), to be measured and the whole W state collapses(also, \(1 - d\) to be passed by without any operation).
[11] The concept of the OCA is from private communication and this is the first time for publishing.