Cryptanalysis and improvement of controlled secure direct communication*

Kao Shih-Hung and Hwang Tzonelih†

National Cheng Kung University, Institute of Computer Science and Information Engineering, Tainan City 701, *Taiwan, China*

(Received 13 November 2012; revised manuscript received 10 January 2013)

This paper points out that, due to a flaw in the sender's encoding, the receiver in Gao *et al.*'s controlled quantum secret direct communication (CQSDC) protocol [*Chin. Phys.* **14** (2005), No. 5, p. 893] can reveal the whole secret message without permission from the controller. An improvement is proposed to avoid this flaw.

Keywords: quantum cryptography, quantum communication

PACS: 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/22/6/060308

1. Introduction

Controlled quantum secure direct communication (CQSDC),[1–10] a type of the quantum secure direct communications firstly proposed in 2002,[11] which enables a sender to communicate with a receiver without any pre-shared key, under the supervision of a controller, is an important research topic in quantum cryptography.

In 2005, Gao *et al.*[1] proposed a CQSDC protocol based on controlled teleportation technology. The sender generates single photons in the X basis $\{|+\rangle, |-\rangle\}$ according to his/her secret bits, where $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. With the help of the controller, these photons are teleported to the receiver, and then the receiver can measure them to reveal the secret message under the permission of that controller. Because of the use of quantum teleportation, the quantum channel between the sender and the receiver is not required, which further reduces the use of optics devices. However, due to a flaw in the sender's encoding function, the receiver can obtain the secret message directly by measuring his/her qubits, without the controller's permission (i.e., the controller's measurement result). This study points out this loophole in Gao *et al.*'s protocol, and proposes an improvement to avoid the loophole. The rest of the article is organized as follows: Section 2 reviews Gao *et al.*'s CQSDC protocol. The security loophole is described in Section 3, and Section 4 gives an improved protocol. Finally, a conclusion is given in Section 5.

2. Review of Gao *et al.*'s CQSDC protocol

This section reviews Gao *et al.*'s CQSDC protocol based on the controlled quantum teleportation strategy. The protocol which includes the sender, Alice, the receiver, Bob, and the controller, named Charlie, can be described as follows:

Step 1 The controller, Charlie, prepares a sequence of three-particle GHZ-like states:

$$|\xi\rangle = (|000\rangle + |110\rangle + |011\rangle + |101\rangle)/2.$$

Let Q'_A (Q'_B, Q'_C) be an ordered set includes all the first (second, third) particles in the sequence. The controller distributes the Q'_A sequence to Alice, and the Q'_B sequence to Bob using the block transmission strategy.[11]

Step 2 Alice, Bob, and Charlie choose a subset of particles randomly, and then discuss publicly to make sure that the entanglement relationship is still exists. After the discussion process, the remaining particles in the set Q'_A (Q'_B, Q'_C) are denoted as Q_A (Q_B, Q_C).

Step 3 Alice generates a particle sequence Q_M according to her secret message, M. If the secret bit is 0 (1), she will generate $|+\rangle_M = (|0\rangle + |1\rangle)/\sqrt{2}$ $(|-\rangle_M = (|0\rangle - |1\rangle)/\sqrt{2})$.

Step 4 If Charlie allows the communication between Alice and Bob, he will measure each particle in his sequence Q_C in the Z basis $\{|0\rangle, |1\rangle\}$ (the first permission). Then Alice takes the Bell measurement on the particles from the sequence Q_A and Q_M, and Alice will send her measurement results to Bob. Then, if Charlie permits Bob to read Alice's secret, he will publicly announce his Z-basis measurement result (the second permission).

Step 5 To recover the quantum state of Alice's secret message, Bob performs the unitary operations according to Charlie and Alice's measurement results. All the eight possible measurement results of Charlie and Alice and the corresponding unitary operations are listed in Table 1, where the Bell states are defined as $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, $|\Phi^-\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$, $|\Psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$, and $|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$; the unitary operation are defined as $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $X = |0\rangle\langle 1| + |1\rangle\langle 0|$, $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, and

*This research is partially supported by the National Science Council, Taiwan, (Grant No. NSC 100-2221-E-006-152-MY3).

†Corresponding author. E-mail: hwangtl@ismail.csie.ncku.edu.tw

© 2013 Chinese Physical Society and IOP Publishing Ltd

$ZX = -|0\rangle\langle 1| + |1\rangle\langle 0|$. After performing the unitary operation on each particle of the sequence Q_B, Bob measures them in the X basis to reveal Alice's secret message.

Table 1. The unitary operation table to Bob with $|\xi\rangle$. The second and third columns are the state of q_B after Step 4. To recover the state of q_B to the teleported state in q_M, the corresponding unitary operation in the fourth column has to be performed on q_B.

Charlie and Alice's measurement result	State of q_B ($q_M = \|+\rangle$)	State of q_B ($q_M = \|-\rangle$)	Unitary operation
$\|0\rangle_C\|\Phi^+\rangle_{MA}$	$\|+\rangle$	$\|-\rangle$	I
$\|0\rangle_C\|\Phi^-\rangle_{MA}$	$\|-\rangle$	$\|+\rangle$	Z
$\|0\rangle_C\|\Psi^+\rangle_{MA}$	$\|+\rangle$	$-\|-\rangle$	X
$\|0\rangle_C\|\Psi^-\rangle_{MA}$	$\|-\rangle$	$-\|+\rangle$	ZX
$\|1\rangle_C\|\Phi^+\rangle_{MA}$	$\|+\rangle$	$-\|-\rangle$	X
$\|1\rangle_C\|\Phi^-\rangle_{MA}$	$\|-\rangle$	$-\|+\rangle$	ZX
$\|1\rangle_C\|\Psi^+\rangle_{MA}$	$\|+\rangle$	$\|-\rangle$	I
$\|1\rangle_C\|\Psi^-\rangle_{MA}$	$\|-\rangle$	$\|+\rangle$	Z

It should be noted that there are two permissions in this protocol. The first one is the "measurement action" by the controller, Charlie, given in Step 4. If Charlie did not measure his q_C (in Q_C) in the Z basis, Alice's secret state (i.e., q_M) would not be able to teleport to Bob's q_B, where q_B denotes any qubit in the quantum sequence Q_B. Hence, the first permission controls if Alice is allowed to transmit her secret message. And the second permission is Charlie's measurement result on each qubit in sequence Q_C, in Step 4, which controls if Bob can reveal Alice's secret or not. That is, without knowing Charlie's measurement result, Bob cannot perform the corresponding unitary operation on q_B to recover the state q_M from q_B.

3. A security loophole in Gao *et al.*'s CQSDC protocol

According to the quantum property, the phase of a qubit does not affect its value (i.e., its measurement result). For example, the X-basis measurement result of both qubits $|+\rangle$ or $-|+\rangle$ is $|+\rangle$. Equation (1) shows the result of each unitary operation performed on an X-basis qubit. It can be seen that the unitary operations I and X do not change the value of an X-basis qubit, but the unitary operations Z and ZX do.

$$\begin{aligned} &I|+\rangle = |+\rangle, \\ &I|-\rangle = |-\rangle, \\ &X|+\rangle = |+\rangle, \\ &X|-\rangle = -|-\rangle, \\ &Z|+\rangle = |-\rangle, \\ &Z|-\rangle = |+\rangle, \\ &ZX|+\rangle = |-\rangle, \\ &ZX|-\rangle = -|+\rangle, \end{aligned} \tag{1}$$

In Gao *et al.*'s CQSDC protocol,[1] because the qubit of Alice's secret message, q_M is produced in the X basis, the state of the teleported qubit is thus in the X basis before Bob performs the recovering unitary operation (see the second and the third columns of Table 1). Therefore, in Step 5 of Gao *et al.*'s protocol, Bob can directly measure his particle q_B in the X basis without performing any unitary operations on his qubits, and then determines whether to flip the value or not according to the unitary operation table. That is, if the corresponding unitary operation is Z or ZX, he will flip the value to obtain the secret message. For example, if Bob's measurement result is $|-\rangle$, which corresponds to the classical bit "1", and thus he knows the required unitary operation is Z. Then, he knows that Alice's secret message is "0" because $Z|-\rangle = |+\rangle$.

In Table 1, the unitary operation is either Z or ZX (I or X) when Alice's measurement result is $|\Phi^-\rangle_{MA}$ or $|\Psi^-\rangle_{MA}$ ($|\Phi^+\rangle_{MA}$ or $|\Psi^+\rangle_{MA}$). This property is independent of Charlie's measurement result. Hence, in Step 4, if Charlie and Alice have already measured their particles, and with Alice's published measurement results, Bob is able to determine the secret message directly without the second permission from Charlie. For example, if Alice's published Bell measurement result is $|\Psi^-\rangle_{MA}$, and Bob's measurement result is $|+\rangle_B$ on his particle q_B, then the secret message from Alice is $\bar{0} = 1$, where $\bar{i}$ represents an NOT operation, for $i = 0, 1$.

4. The improvement

This section presents an improved protocol to avoid the security loophole in Gao *et al.*'s CQSDC protocol. The improved protocol is described as follows.

Step 1–2 The controller produces and distributes GHZ-like states to Alice and Bob as described in Section 2.

Step 3′ According to her secret message M, Alice produces the quantum sequence Q_M in Z basis, i.e., Alice produces $|0\rangle$ ($|1\rangle$) if her secret bit is 0 (1).

Step 4–5 The rest the of steps are the same as the original protocol described in Section 2. With the help from the controller, the qubits in Q_M will be teleported from Alice to Bob.

For those Z-basis qubits, the unitary operations I and Z do not affect the value of them, but the unitary operations X and ZX will flip the value of the Z-basis qubits (see Eq. (2)). Hence, the receiver, Bob can measure q_B in the Z basis after Alice's Bell measurement. Then he can recover the measurement result to Alice's secret according to the demanded unitary operation one of $\{I, Z\}$ or $\{X, ZX\}$.

$$\begin{aligned} &I|0\rangle = |0\rangle, \\ &I|1\rangle = |1\rangle, \\ &X|0\rangle = |1\rangle, \end{aligned}$$

$$
\begin{aligned}
&X|1\rangle = |0\rangle,\\
&Z|0\rangle = |0\rangle,\\
&Z|1\rangle = -|1\rangle,\\
&ZX|0\rangle = -|1\rangle,\\
&ZX|1\rangle = |0\rangle,
\end{aligned} \tag{2}
$$

However, if Bob tries to reveal the secret without Charlie's measurement result, Table 2 shows that each Bell measurement result has two possible unitary operations, in which one will change the qubit's value and the other will not. For example, if Alice's measurement result is $|\Psi^+\rangle_{MA}$, the corresponding operations are I and X, where X changes the value of a Z-basis qubit, but I does not. Hence, after Bob measures his qubit, q_B in Z basis, without knowing Charlie's measurement result on q_C, he cannot decide whether he should flip the value of his measurement result or not. In other words, Bob can reveal Alice's secret message only if he receives the second permission from Charlie.

Table 2. The unitary operation table to Bob with $|\xi\rangle$ and q_M in the Z basis.

Charlie and Alice's measurement result	State of q_B ($q_M = \|+\rangle$)	State of q_B ($q_M = \|-\rangle$)	Unitary operation
$\|0\rangle_C\|\Phi^+\rangle_{MA}$	$\|0\rangle$	$\|1\rangle$	I
$\|0\rangle_C\|\Phi^-\rangle_{MA}$	$\|0\rangle$	$-\|1\rangle$	Z
$\|0\rangle_C\|\Psi^+\rangle_{MA}$	$\|1\rangle$	$\|0\rangle$	X
$\|0\rangle_C\|\Psi^-\rangle_{MA}$	$\|1\rangle$	$-\|0\rangle$	ZX
$\|1\rangle_C\|\Phi^+\rangle_{MA}$	$\|1\rangle$	$\|0\rangle$	X
$\|1\rangle_C\|\Phi^-\rangle_{MA}$	$\|1\rangle$	$-\|0\rangle$	ZX
$\|1\rangle_C\|\Psi^+\rangle_{MA}$	$\|0\rangle$	$\|1\rangle$	I
$\|1\rangle_C\|\Psi^-\rangle_{MA}$	$\|0\rangle$	$-\|1\rangle$	Z

5. Conclusion

This study points out a security loophole in Gao *et al.*'s CQSDC protocol. Because of the loophole, Bob can directly measure his particle q_B in the X basis to reveal the secret message of Alice directly without Charlie's second permission (i.e., the measurement result). To overcome this loophole, an improved protocol is presented. By changing the state of Alice's message qubits from the X basis to the Z basis, the weakness in the original protocol can be solved. The security of the improved protocol (the same as the original protocol) is based on quantum teleportation.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments, which greatly enhanced the clarity of this paper.

References

[1] Gao T, Yan F L and Wang Z X 2005 *Chin. Phys.* **14** 893
[2] Gao T, Yan F and Wang Z 2005 *Int. J. Quantum Inf.* **3** 1293
[3] Wang J, Zhang Q and Tang C J 2006 *Phys. Lett. A* **358** 256
[4] Chen X B, Wen Q Y, Guo F Z, Sun Y, Xu G and Zhu F C 2008 *Int. J. Quantum Inf.* **6** 899
[5] Xia Y, Song J and Song H S 2008 *Commun. Theor. Phys.* **49** 919
[6] Zhang L L, Zhan Y B and Zhang Q Y 2009 *Int. J. Theor. Phys.* **48** 2971
[7] Dong L, Xiu X M, Gao Y J, Ren Y P and Liu H W 2011 *Opt. Commun.* **284** 905
[8] Wang T Y, Wen Q Y and Zhu F C 2011 *Int. J. Quantum Inf.* **9** 801
[9] Xiu X M, Dong L and Gao Y J 2011 *Opt. Commun.* **284** 2065
[10] Yang Y G, Chai H P, Teng Y W and Wen Q Y 2011 *Int. J. Theor. Phys.* **50** 395
[11] Long G L and Liu X S 2002 *Phys. Rev. A* **65** 032302