Improvement of Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement

Zhihao Liu, Hanwu Chen

RECENTLY, a multi-user controlled bidirectional quantum secure direct communication (CBQSDC) network algorithm based on cluster states was proposed [1]. However, there are security problems in this protocol [2]. To be specific, the information leakage problem exists in this protocol. It is also fragile against the intercept-measure-resend attack and the Controlled-Not (CNOT) operation attack by an outside adversary. In addition, the controller can take an effective attack, the so-called different initial state attack, to gain all the messages the users transmitted.

In this abstract, an improved CBQSDC network protocol will be put forward, which is unconditionally secure.

Step 1: Alice and Bob build a connection, with Charlie the controller. Charlie creates $2N + \delta$ numbers of ordered four-qubit cluster states, in which the i-th state is $|\Omega\rangle_{a_i b_i c_i d_i}$.

$$|\Omega\rangle_{a_i b_i c_i d_i} = \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle - |1111\rangle)_{a_i b_i c_i d_i}$$

Then Charlie randomly performs the unitary operations I or X on the first and the second particles of every cluster state.

Step 2: Charlie sorts all the particles a, b, c and d to form the A-sequence, the$B$-sequence, the C-sequence and the D-sequence, respectively. Then Charlie sends A-sequence and B-sequence to Alice and the other two sequences to Bob.

Step 3: Alice (not Charlie) randomly choose δ numbers of cluster states as sample for eavesdropping check and the remaining $2N$ states as information carriers, and the she announces the positions of these photons in each divided sequence. Then she randomly selects the B_Z basis and the B_X basis (or the B_X basis and the B_Z basis) to measure the sample photons in the A-sequence and the B-sequence respectively , and tells Bob to measure the sample photons in the C-sequence and the D-sequence with the B_Z basis and the B_X basis (or the B_X basis and the B_Z basis) respectively. Meanwhile, she requires Charlie publish the random unitary operations that he has performed on the sample cluster states. Next, Alice and Bob compare their results to analyze the error rate. If the error rate is more than the threshold, the communication will stop. Otherwise, it continues.

Step 4: Alice and Bob measure their remaining qubits in B_Z basis and save the results. Then they use classical XOR operations to encode their secret messages. Having taken one bit of the saved measuring results of the A-sequence as the first input and one bit of the secret message she wants to send as the second input, Alice applies XOR operation. Having taken one bit of the saved measuring result of the D-sequence as the first input and one bit of the secret message he wants to send as the second inputs, Bob applies XOR operation. After that, they publish their XOR results through the classical channels, but keep the measuring results of the B-sequence and the C-sequence secret.

Step 5: Charlie announces the unitary operations that he has performed on the first and the seconds photons of the information-carrier cluster states. For example, if he performs II, IX, XI, XX, he will publish “00", “01" , “10" , “11" respectively.

Step 6: Each user obtains the counterparty’s secret message. Since each user has three kinds of bits: The published bits of Charlie, the published bits of her/his counterparty and the bits which have been obtained in Step 4 as the measuring results. For decoding the messages, each user applies the classical XOR operations on all these bits, bit by bit. For example, if Charlie publishes “1" bit about the random unitary on the first photon of an information carrier, Alice publishes “1" bit and Bob obtains “0" bit by measuring the corresponding photon, the final results will be “1" ($1 \oplus 1 \oplus 0 = 0$). Thus Bob knows that “1" is Alice’s secret bit that she sends.

This work was supported by National Natural Science Foundation of China (Grant Nos. 61502101 and 61170321), Natural Science Foundation of Jiangsu Province, China (Grant Nos. BK20140651 and BK20140823), and Funded by PAPD and CICAEET.

Z. Liu is with the School of Computer Science and Engineering, Southeast University, Nanjing 211189, China, and also with the Key Laboratory of Computer Network and Information Integration, Southeast University, Ministry of Education, Nanjing 211189, China (e-mail: liuzhtopic@163.com).

H. Chen is with the School of Computer Science and Engineering, Southeast University, Nanjing 211189, China, and also with the Key Laboratory of Computer Network and Information Integration, Southeast University, Ministry of Education, Nanjing 211189, China.

References

[1] F. Zarmehi and M. Houshmand, "Controlled Bidirectional Quantum Secure Direct Communication Network Using Classical XOR Operation and Quantum Entanglement," *IEEE Communications Letters*, vol. 20, no. 10, pp. 2071-2074, Oct 2016.

[2] Z. Liu, and H. Chen, "Cryptanalysis of controlled bidirectional quantum secure direct communication network using classical XOR operation and quantum entanglement," *IEEE Communications Letters*, to be published, doi: 10.1109/LCOMM.2017.2721952.