International Journal of Quantum Information
Vol. 17, No. 1 (2019) 1975001 (4 pages)
© World Scientific Publishing Company
DOI: 10.1142/S0219749919750017

Double CNOT attack on "Quantum key distribution with limited classical Bob"

Po-Hua Lin[*,‡], Tzonelih Hwang[*,§] and Chia-Wei Tsai[†,¶]

[*] *Department of Computer Science and Information Engineering,*
National Cheng Kung University,
No. 1, University Rd., Tainan City 70101, Taiwan, R.O.C.

[†] *Department of Computer Science and Information Engineering,*
Southern Taiwan University of Science and Technology,
Tainan City, Taiwan
[‡] *ca830531@gmail.com*
[§] *hwangtl@csie.ncku.edu.tw*
[¶] *cwtsai676@stust.edu.tw*

Received 8 May 2018
Revised 24 January 2019
Accepted 27 January 2019
Published 12 March 2019

This paper points out a security loophole in the Quantum key distribution with limited classical Bob [*Int. J. Quantum Inf.* **11**(01) (2013) 1350005]. With the loophole, an eavesdropper can perform the double CNOT attack to reveal about $n/4$-bits out of an n-bit key without being detected by the protocol.

Keywords: Semi-quantum; quantum key distribution; CNOT attack.

1. Introduction

In 2013, Sun *et al.*[1] proposed a quantum key distribution (QKD) protocol with limited classical Bob, who only has to perform simple quantum operations: (1) generate qubits in Z basis $\{|0\rangle, |1\rangle\}$, (2) reflect qubits without disturbance. This kind of protocol is also called the "Semi-quantum key distribution (SQKD)". This protocol allows a quantum Alice, who has a full quantum power, to share a secret key with a classical Bob. However, this paper will point out that Sun *et al.*'s protocol may suffer from a double CNOT attack,[2] allowing an external eavesdropper to obtain about $n/4$-bits out of an n-bit key without being detected.

[§] Corresponding author.

2. Review of Sun *et al.*'s SQKD

Let the integer n be the length of the final key, and let $\delta > 0$ be some fixed parameter. Sun *et al.*'s SQKD is reviewed briefly as follows:

Step 1. Alice randomly generates $N = 8n(1+\delta)$ qubits in either Z basis $\{|0\rangle, |1\rangle\}$ or X basis $\{|+\rangle, |-\rangle\}$, where $|+\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle), |-\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$. Then, Alice sends these qubits to Bob.
Step 2. For each qubit Bob received, he chooses randomly to either reflect the received qubit or discard the qubit and randomly generate a new qubit in Z basis instead to send it back to Alice.
Step 3. Alice measures each qubit in either Z basis or X basis, according to the way she originally generated the qubit in Step 1.
Step 4. Alice announces the basis that she generated in Step 1 and Bob discloses what action he did in Step 2. Note that, there is at least $2n$ expected SIFT bits that Bob sent the new qubits in Step 2 and Alice measured them in Z basis in Step 3. If the number of SIFT bits is less than $2n$, they abort the protocol. Otherwise, Alice checks the error rate on the qubits which Bob reflected in Step 2. If the error rate exceeds a threshold τ, they will terminate the protocol and start a new one again. Otherwise, the protocol will continue.
Step 5. Bob randomly chooses n bits in SIFT bits to check eavesdropper. He publishes these positions he selected, and Alice discloses the value of these bits. If the error rate exceeds a threshold τ', they will terminate the protocol and start a new one again. Otherwise, the protocol will continue.
Step 6. Alice and Bob take the first n-bits of the remaining SIFT bits to derive the final key.

3. Double CNOT Attack

In Step 2 of Sun *et al.*'s protocol, for a qubit Bob discarded, he has to randomly generate a qubit in Z basis. This operation allows an eavesdropper to get the partial information of the shared secret key without being detected by using the double CNOT attack. The detail is shown as follows:

Assume that an eavesdropper, called Eve, intercepts each qubit send from Alice to Bob in Step 1. Eve generates a qubit $|0\rangle_E$ and performs a CNOT operation, where Alice's qubit is the control qubit and Eve's qubit $|0\rangle_E$ is the target qubit. Here, the CNOT operation is $U_{12} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|)_{12}$, where the particle 1 is the control qubit and the particle 2 is the target one. According to Alice's quantum state, the qubit systems become the following:

$$U_{AE}(|0\rangle_A \otimes |0\rangle_E) = |0\rangle_A \otimes |0\rangle_E,$$
$$U_{AE}(|1\rangle_A \otimes |0\rangle_E) = |1\rangle_A \otimes |1\rangle_E,$$
$$U_{AE}(|+\rangle_A \otimes |0\rangle_E) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AE},$$

$$U_{AE}(|-\rangle_A \otimes |0\rangle_E) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AE}. \tag{1}$$

Note that, the subscript A means the qubit sent from Alice and the subscript E denotes the qubit generated from Eve. After the operation, Eve sends Alice's qubit to Bob. According to the protocol, Bob either reflects it or resends a new one. Then, Eve intercepts each qubit send from Bob to Alice in Step 2 and performs the other CNOT operation on Bob's qubit and the corresponding qubit kept by Eve. If Bob chose to reflect the qubit in Step 2, the qubit systems become the following:

$$\begin{aligned} U_{AE}(|0\rangle_A \otimes |0\rangle_E) &= |0\rangle_A \otimes |0\rangle_E,\\ U_{AE}(|1\rangle_A \otimes |1\rangle_E) &= |1\rangle_A \otimes |0\rangle_E,\\ U_{AE}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AE}\right) &= |+\rangle_A \otimes |0\rangle_E,\\ U_{AE}\left(\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AE}\right) &= |-\rangle_A \otimes |0\rangle_E. \end{aligned} \tag{2}$$

If Bob chose to generate the new qubit $|0\rangle_B$ in Step 2, the qubit systems become the following:

$$\begin{aligned} U_{BE}(|0\rangle_B \otimes |0\rangle_E) &= |0\rangle_B \otimes |0\rangle_E,\\ U_{BE}(|0\rangle_B \otimes |1\rangle_E) &= |0\rangle_B \otimes |1\rangle_E,\\ U_{BE}\left(|0\rangle_B \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AE}\right) &= |0\rangle_B \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AE},\\ U_{BE}\left(|0\rangle_B \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AE}\right) &= |0\rangle_B \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AE}. \end{aligned} \tag{3}$$

The subscript B means the new qubit generated by Bob. If Bob chose to resend the new qubit $|1\rangle_B$ in Step 2, the qubit systems become the following:

$$\begin{aligned} U_{BE}(|1\rangle_B \otimes |0\rangle_E) &= |1\rangle_B \otimes |1\rangle_E,\\ U_{BE}(|1\rangle_B \otimes |1\rangle_E) &= |1\rangle_B \otimes |0\rangle_E,\\ U_{BE}\left(|1\rangle_B \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AE}\right) &= |1\rangle_B \otimes \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AE},\\ U_{BE}\left(|1\rangle_B \otimes \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AE}\right) &= |1\rangle_B \otimes \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)_{AE}. \end{aligned} \tag{4}$$

According to Eqs. (1) and (2), if Bob reflects the qubit directly and Eve measures her qubit in Z basis, she will always get the measurement result "0". However, according to Eqs. (3) and (4), if Bob generates a new qubit and Eve measures her qubit in Z basis, then there is a $1/2$ probability that Eve will get the measurement result 1. If the measurement result is 1, it implies that Bob generated a new qubit in Z basis. So, Eve can measure Bob's qubit in Z basis and record the result. Then Eve generates the qubit in Z basis with the same value as the recorded one and resends it to Alice. If the measurement result is 0, Eve cannot distinguish the current qubit is a reflected one or one generated by Bob. So, Eve sends the qubit directly to Alice without any disturbance. Consequently, Eve can reveal about $n/4$ key bits in average and will not be detected by the protocol.

4. Conclusion

A simple way to avoid the attack is to let Bob measure the qubit received from Alice in the Z basis and then generate a new qubit of the same value as he measured in Step 2. By this way, Eve will always get the measurement result 0 from her qubit after performing a double CNOT operation. However, by this way, the quantum capability of the classical Bob will not be so limited anymore as claimed in Sun *et al.*'s protocol.

Acknowledgments

We thank the anonymous referee for telling us that similar results have been obtained independently by Walter Krawec, but as far as the referee could find out, have never been published. This research is partially supported by the Ministry of Science and Technology, Taiwan, R.O.C., under the Contract Nos. MOST 107-2627-E-006-001- and MOST 107-2218-E-218-004-MY2.

References

1. Z.-W. Sun, R.-G. Du and D.-Y. Long, *Int. J. Quantum Inf.* **11**(01) (2013) 1350005.
2. M. Boyer, D. Kenigsberg and T. Mor, *Phys. Rev. Lett.* **99** (2007) 140501.