English
Research Express@NCKU Volume 14 Issue 9 - July 16, 2010
[http://research.ncku.edu.tw/re/articles/e/20100716/3.html]

New Efficient Three-party Quantum Key Distribution Protocols

Han-Cheng Shih, Kuo-Chang Lee and Tzonelih Hwang*

Department of Computer Science and Information Engineering, College of Electrical Engineering and Computer Science, National Cheng Kung University

islab@ismail.csie.ncku.edu.tw

IEEE Journal of Selected Topics in Quantum Electronics, Vol. 15, No. 6, pp. 1602-1606

Most of the existing quantum key distribution protocols (QKDP) assume that every communicating party is equipped with quantum devices (QD), e.g., the qubit generating machine, or the quantum memory, or the qubit measuring machine. However, in the practical situation, these QDs are expensive and a center may be the only party that affords to own these devices. Though Phoenix et al. first realize the idea, their scheme only has 13% of qubit efficiency. This work proposes two three-party QKDPs. The first QKDP with an honest center allows communicants to share a session key by only performing unitary operations. Moreover, considering the trustworthiness of the center, this work further proposes the second QKDP without the assumption of a trusted center. Besides, the proposed three-party QKDPs provide better qubit efficiency than the other QKDPs due to the use of the quantum memory and the use of one-way hash function for the eavesdropping check.

The Quantum Key Distribution Protocol with Honest Center (KHC)

This subsection proposes the first three-party QKDP, in which the sender Alice would like to distribute her session key to the receiver Bob. The following describes the QKDP with honest center (KHC) in details (see also Figure 1).

Step 1. The center produces n qubits Q_1 in the same polarization state $|0\rangle$, and sends the qubits to Alice through the quantum channel.
Step 2. After receiving Q_1, Alice generates a random string K and computes the checksum $h=H(K)$, where K is the session key and H is the one-way hash function. After getting the n-bit string $K||h$, Alice performs the unitary operation U_i on a qubit based on the bit $(K||h)_i$. Moreover, Alice generates the n-bit random string B_1 and performs the unitary operation U_j on a qubit based on the bit $(B_1)_j$ as follows:

- When the bit $(K||h)_i$, is 0(1), the unitary operation U_i is U_0 (U_1).
- When the bit $(B_1)_j$ is 0(1), the unitary operation U_j is U_0 (U_2).

Alice transforms the polarization states of Q_1 to Q_2 with the unitary operations U_i and U_j. Furthermore, Alice sends the qubits Q_2 to Bob through the quantum channel.

Step 3. After receiving the qubits Q_2, Bob generates two n-bit random strings R_2 and B_2. Moreover, Bob performs the unitary operations U_i on a qubit based on the bit $(R_2)_i$ and U_j based on the bit $(B_2)_j$ as follows:

- When the bit $(R_2)_i$ is 0(1), the unitary operation U_i is U_0 (U_1).
- When the bit $(B_2)_j$ is 0(1), the unitary operation U_j is U_0 (U_2).

Bob transforms the polarization states of Q_2 to Q_3 with the unitary operations and sends Q_3 to the center through the quantum channel.

Step 4. After receiving the qubits Q_3, the center gives Alice and Bob the notification.
Step 5. Alice and Bob send the strings B_1 and B_2 to the center, respectively.
Step 6. With the information of B_1 and B_2, the center recovers the original polarization bases of qubits by performing the unitary operation U_j on qubits as the Step 2 and the Step 3. Then, the center measures the qubits with basis R, gains the measuring result $C'=R_2 \oplus (K||h)$ and sends C' to Bob.
Step 7. After receiving C', Bob recovers $K||h=R_2 \oplus C'$ and verifies whether $h=H(K)$. If the equation $h=H(K)$ holds, Bob gets the correct session key K and tells Alice "OK".

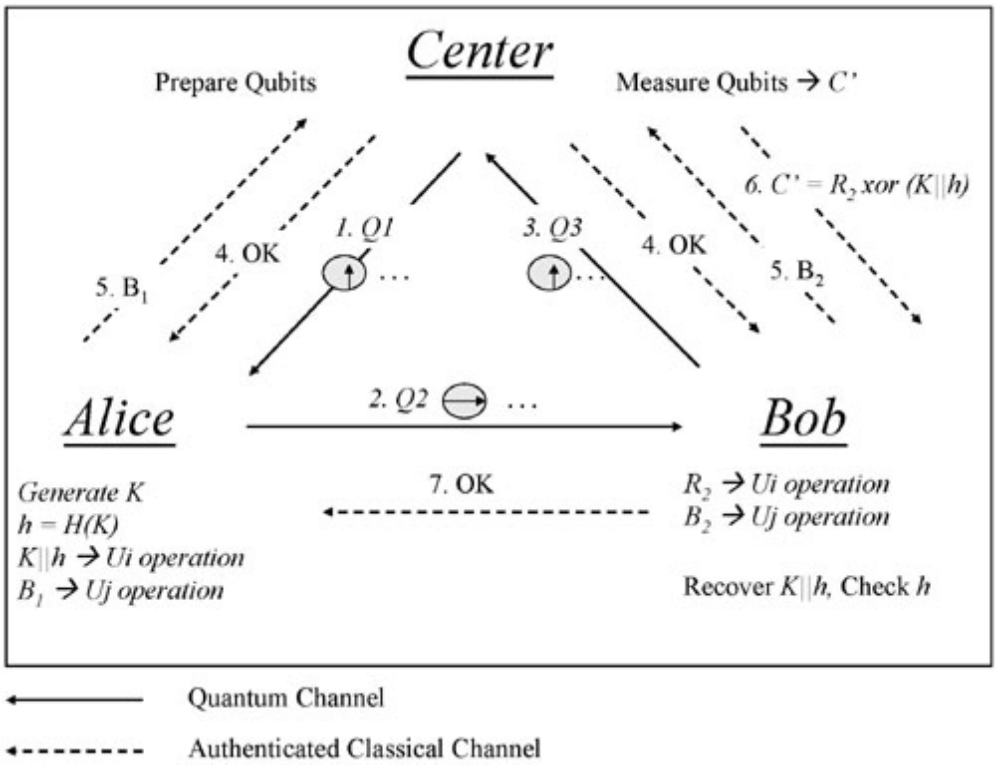

Figure 1: The QKDP with Honest Center.

The Quantum Key Distribution Protocol with Untrusted Center (KUC)

Step 1. Similar to Step 1 of the KHC, the center produces n qubits Q_1 and sends the qubits to Alice through the quantum channel.
Step 2. Similar to Step 2 of the KHC, Alice creates a n-bit random string B_1, generates a random string K and computes the checksum $h=H(K)$, where the length of $K||h$ is n. Moreover, Alice performs the unitary operation U_i and U_j based on the bit $(K||h)_i$ and $(B_1)_j$, respectively. Then, Alice sends the processed qubits Q_2 to Bob through the quantum channel.
Step 3. After receiving qubits, Bob preserves the qubits and tells Alice "OK".
Step 4. After receiving Bob's notification, Alice replies the string B_1 to Bob.
Step 5. Bob performs the unitary operation U_j based on the bit $(B_1)_j$. When the bit $(B_1)_j$ is 0(1), the unitary operation U_j is U_0 (U_2). Moreover, Bob shuffles the sequence of qubits and sends the processed qubits Q_3 to the center through the quantum channel.
Step 6. After receiving the qubits Q_3, the center measures the qubits with the polarization basis R, gains the measuring result $C'=Shuffled\_(K||h)$ and sends C' to Bob.

Step 7. Bob rearranges the sequence of C', recovers the string $K||h$ and checks whether $h=H(K)$. If the equation $h=H(K)$ holds, Bob tells Alice “OK”.

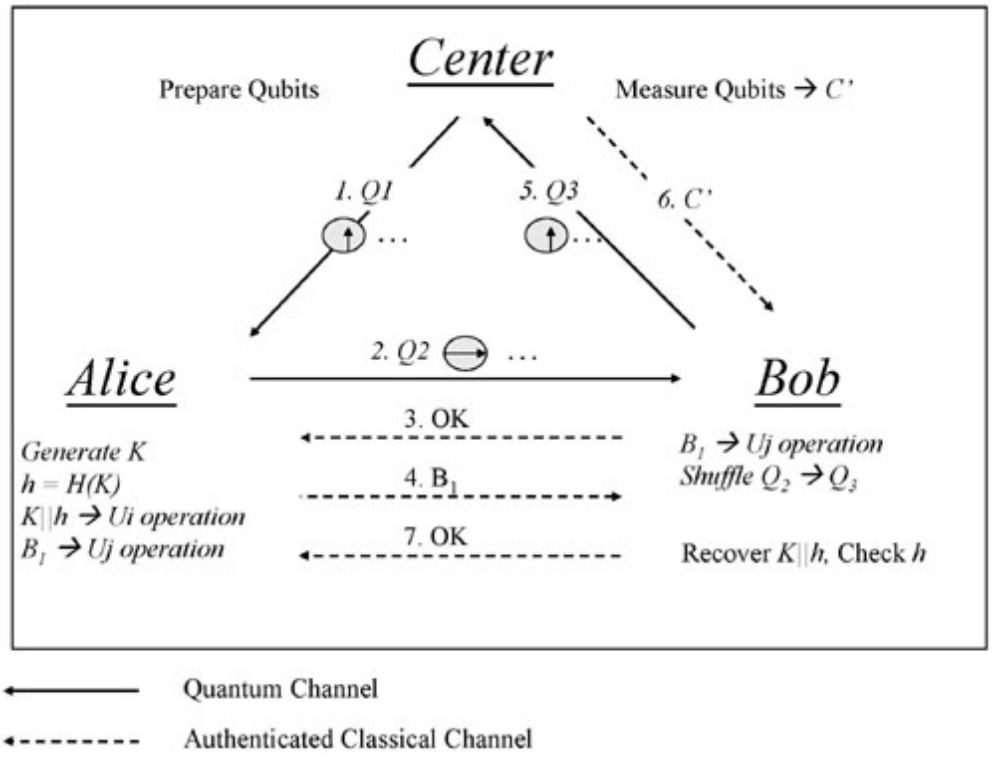

Figure 2: The QKDP with Untrusted Ceter.

Comparison of Three-party QKDPs

	Phoenix et al.	KHC	KUC
Q. Memory of Center	No	Require	No
Q. Memory of User	No	No	Bob
Q. Measure of Center	Require	Require	Require
Quantum Channel	3	3	3
Public Discussion	Random Sampling	Checksum	Checksum
Qubit Efficiency	n/8	n-|h|	n-|h|
Trusted center	No	Require	No
Formal Proof	No	Yes	Yes

This work proposes two efficient three-party QKDPs, in which the center is responsible for equipping most of expensive QDs, whereas users only possess a few of them. In the first three-party QKDP, users simply perform quantum unitary operations to hide their secrets into qubits. The second three-party QKDP can prevent the attack from the untrusted center by replacing Bob’s quantum unitary operation with the sequence shuffling technique. However, Bob should have the quantum memory to perform the shuffling technique. How to design a three-party QKDP with the untrusted center that does not require the user to equip with the expensive quantum memory is an interesting topic for the future research.