A Quantum Cryptosystem With Perfect Secrecy and Message Authentication

Chia-Mu Yu[*]　　Yuh-Dauh Lyuu[†]

Abstract

In this paper, we investigate a quantum cryptosystem with perfect secrecy and message authentication. In an insecure quantum channel that Bob communicates with Alice, we provide a cryptosystem allowing Alice to encrypt and authenticate an n-qubit message by $2n$ qubits with probability at least $1 - \frac{1}{2^{O(n)}}$ that Alice and Bob can detect eavesdropper(Eve), and we prove our quantum cryptosystem has perfect secrecy, that is, we can guarantee that nobody can steal any useful information from encrypted message.

Key Words. Quantum, Cryptosystem, Authentication

[*] Corresponding author. Department of Computer Science & Information Engineering, National Taiwan University, No 1, Sec 4, Roosevelt Rd, Taipei, Taiwan 106. E-mail: r91045@csie.ntu.edu.tw.

[†] Department of Finance and Department of Computer Science & Information Engineering, National Taiwan University, No 1, Sec 4, Roosevelt Rd, Taipei, Taiwan 106. E-mail: lyuu@csie.ntu.edu.tw.

1 Introduction

In classical cryptography, the technique like Diffie-Hellmann key-exchange protocol [?] or public key encryption scheme are used for key distribution. In 1984 there is a big breakthrough for quantum cryptography when Bennett and Brassard described the first quantum key distribution protocol. But, nobody can develop the algorithm solving a real-world problem until 1994. Since Bennett and Brassard invented a reliable quantum key distribution protocol (BB84), anyone can securely agree on a classical random string by use of this protocol.

2 Protocol

Because we will use a secure quantum key distribution (QKD) protocol in our protocol, we have to discuss the first practical key distributon protocol presented by Bennett and Brassard in 1984, or BB84 for short. BB84 is a quantum key distribution protocol which allows Alice and Bob to securely agree on some classical string over a quantum channel.

Besides, since we will use the random unitary operator (random unitary matrix) in our protocols, we must discuss the properties of random unitary operator and how the BB84 protocol to produce a random unitary operator. Before we talk about it, we have to define some terminology.

Definition *If we only care about the positive value of the square root in the the process of finding the square roots of a in the equation $a^2 = b$, that is, $a = +\sqrt{b}$ although we have $a = \pm\sqrt{b}$ in general, we say such process is a positive process.*

Theorem *Given that a general form of unitary matrix is prepared, and we restrict that the elements in matrix be real, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. When a is a fixed number, we can derive the unique values of b, c and d in a positive process, that is, we can determine the unique unitary matrix.*

Proof. Because of the basic property of unitary matrix, we have

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Due to the relation above, we have three equations,

$$\begin{cases} a^2 + b^2 = 1 \\ c^2 + d^2 = 1 \\ ac + bd = 0 \end{cases}$$

Since we already know the value of a, we can derive the value b as $b = \pm\sqrt{1-a^2}$. Using the property of positive process we obtain $b = \sqrt{1-a^2}$. The remaining problem is how to solve the linear equation in two unknowns below:

$$\begin{cases} c^2 + d^2 = 1 \\ ac + \sqrt{1-a^2}d = 0 \end{cases}$$

Again we use the property of positive process, to obtain the unique value of c and d. So the unique unitary matrix is determined. QED

Corollary *Given that a general form of unitary matrix is prepared, and we restrict that the elements in matrix be real,* $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. *Once we fix the value of one of elements in matrix U, we can derive the unique values of the other elements in positive process, that is , we can determine the unique unitary matrix.*

If Alice and Bob want to share a 2 × 2 random unitary operator $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the BB84 protocol can be used to determine the value of the element a in the unitary operator U. But there is a trick here for selecting the value of a to avoid letting the value of b to be a complex number. In practice, assuming that Alice and Bob share an n-bit string, we don't directly use the corresponding decimal number to be the value of a. Instead, if the corresponding decimal value of that string is Φ, we let the value of a be $\frac{\Phi}{2^n}$.

we can use the property above to give a simple protocol like below,

Protocol III

1. *Alice and Bob use the BB84 protocol to share a bit string s and we can see s as a unitary operator U.*

2. *For each bit t Alice wants to send, Alice sends $|t_s\rangle{\equiv}U|t\rangle$ to Bob.*

3. *Bob uses $U^\dagger$ to get the original message.*

Many researcher call this kind of protocol *quantum one-time pad*, and we will use this kind of protocols to build one with authentication.

We first analysis quantum one-time pad using in view of information theory. To do this, we have to define a concept about secrecy. The notion of perfect secrecy is introduced by Shannon. It is usually used to describe that the encrypted messages are safe under the condition that the private key is secretly shared by Alice and Bob, that is, Eve cannot learn anything from the encrypted message. We give the formal definition below.

Definition 10 *The cryptosystem has perfect secrecy if the events that a particular ciphertext occurs and that a particular plaintext has been encrypted are independent, i.e., $Pr[p|c] = Pr[p]$ for all plaintexts p and all ciphertexts c.*

After we define the perfect secrecy, we give a theorem which prove the *quantum one-time pad* has perfect secrecy.
Theorem 13 *The protocol **III** has perfect secrecy when the unitary matrices are real and symmetric.*
Proof We can use the BB84 protocol to determine a random symmetric unitary operator with real elements, in other words, the probability distribution is a uniform distribution.

Assuming that we have two symmetric matrices $U_1 = \begin{pmatrix} a & b \\ b & d \end{pmatrix}$, $U_2 = \begin{pmatrix} x & y \\ y & z \end{pmatrix}$, and a arbitrary quantum state $|\phi\rangle = \begin{pmatrix} A \\ B \end{pmatrix}$. We want to prove $U_1 = U_2$ if $U_1|\phi\rangle = U_2|\phi\rangle$. Given that

$$\begin{pmatrix} a & b \\ b & d \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} x & y \\ y & z \end{pmatrix}\begin{pmatrix} A \\ B \end{pmatrix}$$

After some simple matrix operation we can get

$$\begin{pmatrix} aA + bB \\ bA + dB \end{pmatrix} = \begin{pmatrix} xA + yB \\ yA + zB \end{pmatrix}$$

According to the equation above, we can obtain the relation below,

$$\begin{cases} (a - x)A = (y - b)B \\ (b - y)A = (z - d)B \end{cases}$$

Since we only use our cryptosystem to send classical bit string, we only care about it. Because of the property of classical bit, we have two situations: the first, $A = 1$ and $B = 0$. The second, $A = 0$ and $B = 1$. No matter what situation we have, we can say $b = y$. By Corollary 8, we conclude $U_1 = U_2$.QED

Then, we modify the quantum one-time pad to obtain a new protocol which has authentication.

Protocol with Authentication

1. *Alice and Bob first share a unitary operator U and a number $m, 0 \leq m \leq n$.*
2. *Alice prepares n EPR-pairs,* $\{\frac{1}{\sqrt{2}}(|00\rangle_{a_1b_1} + |11\rangle_{a_1b_1}), \frac{1}{\sqrt{2}}(|00\rangle_{a_2b_2} + |11\rangle_{a_2b_2}), ..., \frac{1}{\sqrt{2}}(|00\rangle_{a_nb_n} + |11\rangle_{a_nb_n})\}$.
3. *Alice initially sets* $\texttt{count} = 0$.
4. *Alice lets* $B_{\texttt{count+0} \mod \texttt{2n}} = U|t_1\rangle, B_{\texttt{count+1} \mod \texttt{2n}} = U|t_2\rangle, ..., B_{\texttt{count+n-1} \mod \texttt{2n}} = U|t_n\rangle$.
5. *Alice lets* $B_{\texttt{count+n} \mod \texttt{2n}} = |a_1\rangle, B_{\texttt{count+n+1} \mod \texttt{2n}} = |a_2\rangle, ..., B_{\texttt{count+2n-1} \mod \texttt{2n}} = |a_n\rangle$ *and sets* $\texttt{count} = \texttt{count} + \texttt{m} \mod \texttt{2n}$.
6. *Alice sends block B to Bob through the public quantum channel.*
7. *Bob receives block B and measures the qubits the appropriate locations of the block according to the shared information m, and announces the result through the public classical broadcast channel.*
8. *Through the public classical broadcast channel, if the result between Alice and Bob is distinct anywhere, we can detect the existence of Eve.*

When Eve wants to eavesdrop on the original messages from Alice, she must do something on her received encrypted message. The basic notion of inserting some qubits to block from the EPR-pairs is to prevent such action, that is, this method ensures that Eve cannot successfully guess the correct location of encrypted qubits.

3 Conclusions

First, in view of information theory, we have proven that the *quantum one-time pad* has perfect secrecy. Second, we presented a new cryptographic protocol which have authentication. Up to now, we have solved a large number of problem in cryptosystem, including key size and message source. Another related interesting problem is how to extends this notion to quantum public-key cryptosystem? In other words, does small size key can always be used to build a quantum public-key cryptosystem with Authentication.

References