Quantum no-key protocol for secure communication of classical message

Li Yang
State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

Abstract
We propose a class of quantum no-key protocols for private communication of classical message based on quantum computing of random Boolean permutations, and demonstrate that they are information-theoretic secure. These protocols are designed to resist middleman attack for two parties preshared authentication key, and achieve perfect mutual data origin authentication which ensures the permanent reusing of authentication key. Finally, we simplify the protocol to a 4-round one, and show that any protocol with 3 or less rounds cannot achieve perfect security without consuming preshared key.

Keywords: quantum cryptography, information-theoretic security, quantum no-key protocol, data origin authentication

Quantum no-key protocol is one of the earliest interactive quantum secure communication protocols[1–3], which remains three-round structure of Shamir’s original idea, but can be improved to resist man-in-the-middle (MIM) attack[2, 4, 5]. This kind of protocols have been applied to meet various cryptographic demands[7–10]. When the communication is limited to transmitting classical message, and we do not require it to keep exponential-security under the MIM attack, a protocol can be simplified to a two-round one[11]. So far, there are various quantum no-key protocols presented [5], but none with rigorous security proof. Here we propose a new quantum no-key protocol for classical message communication with provable perfect security.

1. Basic protocol
Alice intends to transmit classical message \( x \) to Bob through a quantum channel. She can complement it by the following protocol:
Protocol 1.

(1) Alice prepares quantum state:

$$|x⟩_I \xrightarrow{H^{(s)}} \frac{1}{\sqrt{2^n}} \sum_m (-1)^{x_m} |m⟩_I.$$ (1)

(2) Alice chooses a Boolean permutation $F_A(\cdot)$ randomly, and executes:

$$\frac{1}{\sqrt{2^n}} \sum_m (-1)^{x_m} |m⟩_I |0⟩_{II} \rightarrow \frac{1}{\sqrt{2^n}} \sum_m (-1)^{x_m} |m⟩_I |F_A(m)⟩_{II}.$$ (2)

(3) Alice sends quantum register $I$ to Bob, the state appeared in the channel is:

$$\rho_1 = tr_{II} \left[ \frac{1}{2^n} \sum_{m,n} (-1)^{x_m} (-1)^{x_n} |m⟩_I ⟨n| \otimes |F_A(m)⟩_{II} ⟨F_A(n)| \right]$$

$$= \frac{1}{2^n} \sum_{m,n} (-1)^{x_m} (-1)^{x_n} |m⟩_I ⟨n| \sum_k ⟨k|F_A(m)⟩ ⟨F_A(n)|k⟩.$$ (3)

Since $F_A(\cdot)$ is a Boolean permutation, we have:

$$\rho_1 = \frac{1}{2^n} \sum_m |m⟩⟨m| = \frac{1}{2^n} I_{2^n}.$$ (4)

That is, the state appeared on the channel is only an ultimate mixed state.

(4) After receiving the quantum state $\rho_1$, Bob randomly chooses a Boolean permutation $F_B(\cdot)$ and computes:

$$|m⟩_I |0⟩_{III} \rightarrow |m⟩_I |F_B(m)⟩_{III}.$$ (5)

Then, the state of quantum register $I$ will be:

$$\rho_2 = tr_{III} \left[ \frac{1}{2^n} \sum_m |m⟩_I ⟨m| \otimes |F_B(m)⟩_{III} ⟨F_B(m)| \right]$$

$$= \frac{1}{2^n} \sum_m |m⟩_I ⟨m| \otimes \sum_k ⟨k|F_B(m)⟩_{III} ⟨F_B(m)|k⟩_{III}$$

$$= \frac{1}{2^n} I_{2^n}.$$ (6)
That is, while Bob sending the quantum register $I$ to Alice, the state in the channel is also an ultimate mixed state.

(5) After received register $I$, Alice does computation:

$$|m⟩_I|F_A(m)⟩_{II} → |m⟩_I|F_A(m) ⊕ F_A(m)⟩_{II} = |m⟩_I|0⟩_{II}, \quad (7)$$

and sends register $I$ to Bob again. Then the state transmitted in the channel will be:

$$\rho_3 = tr_{II} \left[ \frac{1}{2^n} \sum_m |m⟩_I⟨m|⟨0⟩_{II}⟨0| \right] = \frac{1}{2^n} I_{2^n}. \quad (8)$$

The transmitted state is an ultimate mixed state again.

(6) After received $\rho_3$, Bob executes computation:

$$|m⟩_I|F_B(m)⟩_{II} → |m⟩_I|F_B(m) ⊕ F_B(m)⟩_{II} = |m⟩_I|0⟩_{II}, \quad (9)$$

and obtains the state: $\frac{1}{\sqrt{2^n}} \sum_m (-1)^x_m |m⟩_I$. Finally, Bob has the message $x$ via performing $H^{(n)}$ transformation and measuring register $I$.

It can be seen more clearly if we exhibit the whole evolution of $(A,B)$ composite system:

$$\frac{1}{\sqrt{2^n}} \sum_m (-1)^x_m |m⟩_I|0⟩_{II}⟨0|_{III} \rightarrow \frac{1}{\sqrt{2^n}} \sum_m (-1)^x_m |m⟩_I|F_A(m)⟩_{II}⟨0|_{III} \rightarrow \frac{1}{\sqrt{2^n}} \sum_m (-1)^x_m |m⟩_I|F_A(m)⟩_{II}|F_B(m)⟩_{III}.$$
\[ \rightarrow \frac{1}{\sqrt{2^n}} \sum_{m} (-1)^{x_m} |m\rangle_I |F_A(m)\rangle_{II} |F_B(m)\rangle_{III} \]

\[ = \frac{1}{\sqrt{2^n}} \sum_{m} (-1)^{x_m} |m\rangle_I |0\rangle_{II} |F_B(m)\rangle_{III} \]

\[ \rightarrow \frac{1}{\sqrt{2^n}} \sum_{m} (-1)^{x_m} |m\rangle_I |0\rangle_{II} |F_B(m)\rangle_{III} \]

\[ = \frac{1}{\sqrt{2^n}} \sum_{m} (-1)^{x_m} |m\rangle_I |0\rangle_{II} |0\rangle_{III}. \]  

That is, Bob obtains the quantum state of the first quantum register:

\[ \frac{1}{\sqrt{2^n}} \sum_{m} (-1)^{x_m} |m\rangle_I. \]

With respect to secrecy, \( F_A(\cdot), F_B(\cdot) \) are both randomly selected Boolean permutation, and the transmitted quantum states \( \rho_1, \rho_2, \rho_3 \) are all ultimate mixed states, so the adversary can not get any information, protocol 1 has information-theoretic security. However, this protocol cannot resist MIM attack. When that the adversary Eve impersonates Bob to communicate with Alice, at the same time, he impersonates Alice to communicate with Bob, he will get \( x \) from Alice and send \( x' \) to Bob successfully.

2. Protocol with data origin authentication

In this section, we improve protocol 1 to be one with mutual authentication. The protocol we shall construct is a 9-round no-key protocol with mutual identification. The whole protocol consists of three stages, each includes three rounds.

Protocol 2.

Alice and Bob share randomly chosen Boolean functions \( s_A(\cdot) \) and \( s_B(\cdot) \) in advance.

(1) Alice randomly chooses Boolean permutation \( F_A(\cdot) \) and random number \( r_A \), then prepares quantum state:

\[ \sum_{m} \alpha_m |m\rangle_I |0\rangle_{II} |0\rangle_{III} \rightarrow \sum_{m} \alpha_m |m\rangle_I |F_A(m)\rangle_{II} |s_A(m)\rangle_{III} \]
where $\alpha_m = \frac{1}{\sqrt{2}}(-1)^x m$, then Alice sends the first and the third registers to Bob. For the adversary, the quantum state transmitted in the channel is:

$$
\sigma_1 = tr_{II} \left[ \sum_{m,n,r_A} \frac{\alpha_m \alpha_n^*}{2^l} |m\rangle \langle m| \otimes |s_A(m) \oplus r_A\rangle \langle s_A(n) \oplus r_A| \right]
$$

$$
= \frac{1}{2^l} \sum_{m,r_A} |\alpha_m|^2 |m\rangle \langle m| \otimes |s_A(m) \oplus r_A\rangle \langle s_A(m) \oplus r_A| 
$$

$$
= \frac{1}{2^l} \sum_{m} |\alpha_m|^2 |m\rangle \otimes I_{2^l}
$$

$$
= \frac{1}{2^{n+l}} I_{2^n} \otimes I_{2^l}
$$

Therefore, $\sigma_1$ is an ultimate mixed state.

(2) Bob randomly chooses Boolean permutation $F_B(\cdot)$ and random number $r_B$, then uses $F_B(\cdot)$, $r_B$ and the preshared Boolean function $s_B(\cdot)$ to accomplish computation:

$$
|m\rangle_I |s_A(m) \oplus r_A\rangle_{III} |0\rangle_{IV} |0\rangle_{V} \rightarrow |m\rangle_I |r_A\rangle_{III} |F_B(m)\rangle_{IV} |s_B(m) \oplus r_B\rangle_{V}.
$$

(13)

Then Bob measures the third quantum register and sends the first and the fifth register to Alice. Similar to the analysis in step (1), we can see that quantum state $\sigma_2$ in the channel is also an ultimate mixed state.

(3) Alice chooses random number $r_A'$ and do the transformation:

$$
|m\rangle_I |F_A(m)\rangle_{II} |s_B(m) \oplus r_B\rangle_{V} |0\rangle_{VI} \rightarrow |m\rangle_I |F_A(m) \oplus F_A(m)\rangle_{II} |s_B(m) \oplus s_B(m) \oplus r_B\rangle_{V} |s_A(m) \oplus r_A'\rangle_{VI}
$$

$$
= |m\rangle_I |0\rangle_{II} |r_B\rangle_{V} |s_A(m) \oplus r_A'\rangle_{VI}.
$$

(14)

Then Alice measures the fifth quantum register, and sends register $I$ and register $VI$ to Bob. It can also be proved that the quantum state appeared in channel is $\sigma_3 = \frac{1}{2^{n+l}} I_{2^n+l}$.

(4) After he receives $\sigma_3$, Bob executes transformation:

$$
|m\rangle_I |F_B(m)\rangle_{IV} |s_A(m) \oplus r_A'\rangle_{VI} \rightarrow |m\rangle_I |F_B(m) \oplus F_B(m)\rangle_{IV} |s_A(m) \oplus s_A(m) \oplus r_A'\rangle_{VI}
$$

$$
= |m\rangle_I |0\rangle_{IV} |r_A'\rangle_{VI}.
$$

(15)
and obtains the quantum state: \( \frac{1}{\sqrt{2^n}} \sum_m (-1)^{x \cdot m} |m\rangle \).

(5) Bob performs Hadamard transformation on the received quantum state, and measures the quantum register \( I \). Finally, he obtains the classical message \( x \).

There exists an obvious weakness in the above protocol. Though Eve cannot obtain \( x \), she can tamper the system without being detected. A direct way to resist this attack is to execute the protocol three times as follows:

**Protocol 3.**

(1) The first stage (1-3 rounds): Alice sends classical message \( x \) to Bob via executing protocol 2. We can see that, for Eve without \( s_A(\cdot) \) and \( s_B(\cdot) \), obtaining the message \( x \) is a too difficult task to accomplish.

(2) The second stage (4-6 rounds): Bob sends the message \( x \) back to Alice via protocol 2. We can see that even if Eve impersonates Bob to communicate with Alice, she cannot send back the right \( x \) to Alice, and then Alice will find that she has not accomplished the communication task.

(3) The third stage (7-9 rounds): Alice sends \( x \) to Bob again via protocol 2. If Eve impersonates Alice to communicate with Bob, Bob will receive two different messages in this and the first stage respectively, because Eve does not have \( s_A \) and \( s_B \). Therefore, via this stage, Bob can discriminate the attacker from the expected message sender Alice.

The interaction of this protocol is up to 9 so as to achieve perfect security. Since all the quantum states transmitted are ultimate mixed states, the adversary cannot get any information.

(1) For different message \( x \) and \( y \), the quantum states in the channel are all the ultimate mixed state, so the trace distance of \( \rho_i(x) \) and \( \rho_j(y) \) \((i = 1, 2, 3)\) is:

\[
D(\rho_i(x), \rho_j(y)) = 0 \tag{16}
\]

Therefore, Eve cannot attack the plaintext directly.
For Alice and Bob’s authentication Boolean function $s_A$, $s_B$, due to $r_A$ and $r_B$ are local random bit strings chosen for each round independently, we have:

$$D(\rho_i(x, s_A(\cdot)), \rho_j(y, s_A'(\cdot))) = D(\rho_i(x, s_B(\cdot)), \rho_j(y, s_B'(\cdot))) = D(\frac{I_{2^n+i}}{2^{n+i}}, \frac{I_{2^n+i}}{2^{n+i}}) = 0$$

That is, the adversary cannot attack $s_A$, $s_B$.

Though this 9-round protocol is constructed so complicated, there still exists a MIM attack. The adversary can perform $Z_x$ operation to quantum register $I$ in each of the 9 passes: $Z_x^x |m\rangle = (-1)^{x \cdot m} |m\rangle$. This attack will change the final message Bob recieved from $x$ to $x \oplus x'$. We can easily understand this attack from the basic relation $HX = ZH$.

To resist this attack, Alice and Bob have to use authentication key to code $x$: $x \rightarrow e_k(x)$. While Eve tampered, Alice and Bob will find that the message received has been changed. That is, when we use this additional authentication, Eve cannot implement her MIM attack without being detected.

3. Simplification of the previous protocols

The protocol 2 can be simplified as follows:

Protocol 4.

(1) The message receiver Bob executes computation as below:

$$|0\rangle_I |0\rangle_{II} |0\rangle_{III} \rightarrow \frac{1}{\sqrt{2^n}} \sum_m |m\rangle_I |0\rangle_{II} |0\rangle_{III}$$

$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_m |m\rangle_I |F_B(m)\rangle_{II} |0\rangle_{III}$$

$$\rightarrow \frac{1}{\sqrt{2^n}} \sum_m |m\rangle_I |F_B(m)\rangle_{II} |s_B(m) \oplus r_B\rangle_{III},$$

where $F_B(\cdot)$ is a randomly chosen Boolean permutation, $s_B$ is a Boolean Function preshared by Alice and Bob for authentication, and $r_B$ is a randomly chosen bit string. Then, Bob sends register $I$ and $III$ together to Alice.
(2) The message sender Alice executes computation:

\[ |m⟩_I |s_B(m) ⊕ r_B⟩_{III} \rightarrow |m⟩_I |s_B(m) ⊕ s_B(m) ⊕ r_B⟩_{III} = |m⟩_I |r_B⟩_{III} \quad (19) \]

and measures the third register, then she performs quantum operation \( Z^x \) to register \( I \): \( Z^x |m⟩_I = (-1)^{x \cdot m} |m⟩_I \), and executes computation: \( |m⟩_I |0⟩_{IV} \rightarrow |m⟩_I |s_A(m) ⊕ r_A⟩_{IV} \). Then she sends the two registers to Bob. Where \( s_A \) is another Boolean function preshared by Alice and Bob for authentication, and \( r_A \) is a bit-string randomly chosen by Alice.

(3) Bob computes:

\[ |m⟩_I |s_A(m) ⊕ r_A⟩_{IV} \rightarrow |m⟩_I |s_A(m) ⊕ s_A(m) ⊕ r_A⟩_{IV} = |m⟩_I |r_A⟩_{IV}, \quad (20) \]

and measures the register \( IV \), then he computes:

\[ |m⟩_I |F_B(m)⟩_{II} \rightarrow |m⟩_I |F_B(m) ⊕ F_B(m)⟩_{II} = |m⟩_I |0⟩_{II}, \quad (21) \]

and obtains the quantum state:

\[ \frac{1}{\sqrt{2^n}} \sum_{m} (-1)^{x \cdot m} |m⟩_I \xrightarrow{H^{(x)}} |x⟩_I \quad (22) \]

Finally, Bob measures the register \( I \) and results in the message \( x \) from Alice.

Because \( F_B(\cdot) \) is a Boolean permutation, we can prove as in protocol 2 that the two quantum states transmitting in channel are both ultimate mixed states. Based on this results, the protocol 3 can be simplified to a 6-round protocol with mutual authentication:

**Protocol 5.**

1. Alice executes protocol 4 to send a message \( x \) to Bob;
2. Bob executes protocol 4 to send \( x \) back to Alice;
3. Alice executes protocol 4 with Bob to send \( x \) to Bob again.
Via this three stage protocol, Alice can confirm that the message $x$ is really received by the expected receiver Bob, and Bob also acknowledges that the message is really from the expected sender Alice. Actually, this protocol can be simplified further to a 4-round one as follows:

**Protocol 6.**

(1) Alice encodes: $x \rightarrow e_k(x)$ with some information-theoretic secure authentication code, and executes the first step of protocol 5 to send $x' = (x, e_k(x))$ to Bob.

(2) Bob executes the second step of protocol 5, and sends $e_k(x)$ back to Alice.

It can be seen that since a classical authentication code $e_k$ is embedded in the protocol, the 6-round protocol can be simplified to a 4-round one which can resist the MIM attack with operation $Z^x$.

4. Security analysis of protocols with 3 or less rounds

**A. Non-interactive protocol**

The sender Alice intends to send $x$ to receiver Bob, she firstly computes $e_k(x)$, the MAC of $x$, and gets $x' = (x, e_k(x))$. Then she computes as below:

$$
|x'\rangle \rightarrow \frac{1}{\sqrt{2^n}} \sum_m (-1)^{x' \cdot m}|m\rangle_I |0\rangle_{II}
$$

$$
\rightarrow \frac{1}{\sqrt{2^n}} \sum_m (-1)^{x' \cdot m}|m\rangle_I |s_A(m) \oplus r_A\rangle_{II},
$$

and sends the two registers to Bob. For the adversary, the mixed state in the channel is:

$$
\rho = \frac{1}{N} \sum_{s_{A},r_A} \sum_{m,n} \frac{(-1)^{m \cdot x' \oplus n \cdot x'}}{2^l} |m\rangle_I |n\rangle \otimes |s_A(m) \oplus r_A\rangle_{II} |s_A(n) \oplus r_A\rangle
$$

$$
= \frac{1}{N2^l} \sum_{m,n} (-1)^{m \cdot x' \oplus n \cdot x'} |m\rangle_I |n\rangle \otimes \sum_{s_{A},r_A} |s_A(m) \oplus r_A\rangle_{II} |s_A(n) \oplus r_A\rangle
$$

Up till now, we cannot prove its security yet, though there is no effective attack found.

**B. Two-round protocol**
Two-round protocol is that includes only the first step of the 4-round protocol. Since $D(\rho_i(x), \rho_j(y)) = 0$, information-theoretic security can be guaranteed. Because $D(\rho_i(x, s_A(\cdot)), \rho_j(y, s_A'(\cdot))) = 0$, $D(\rho_i(x, s_B(\cdot)), \rho_j(y, s_B'(\cdot))) = 0$ authentication key $s_A(\cdot)$ and $s_B(\cdot)$ can be used permanently. However, in this protocols, Alice cannot identify whether the message has been sent to Bob. As soon as Bob adds authentication message in the quantum state, the protocol is no longer of provable information-theoretic security, and lost the permanent reusable property of authentication key. The reason is that because that the protocol cannot keep conditions: $D(\rho_i(x), \rho_j(y)) = 0$, $D(\rho_i(x, s_A(\cdot)), \rho_j(y, s_A'(\cdot))) = 0$ in that case.

C. Three-round protocol

Three-round protocol can overcome the difficulty of the two-round protocol described above, and realize mutual authentication, but it cannot ensure the permanent employment of authentication key. To satisfy the security requirement mentioned above, the protocols introduced here compute random Boolean permutation $\{F_A(\cdot), F_B(\cdot)\}$ controlled by local random numbers to produce entangled states, and use local random numbers $r_A$, $r_B$ to protect authentication keys $s_A(\cdot)$, $s_B(\cdot)$. It can be seen that the three-round protocol cannot satisfy all these requirements.

In a three round protocol, the entangled state without message has to be sent by Bob firstly. Then, Alice adds the message in the entangled state in the way as in two-round protocol. As the security analysis in two-round protocol, Alice cannot verify the legitimacy of Bob without consuming key, any further authentication depends on the additional third round. It is difficult for the third round to do that relies on entangled state which is produced by local random number, so the leakage of authentication key is inevitable. Therefore, three-round protocol cannot ensure the permanent use of authentication key while guarantees perfect encryption and origin data authentication.

5. Conclusion

We propose a new kind of quantum no-key protocol with provable information-theoretic security. We simplify the initial 9-round protocol to a 4-round protocol, and shows that any protocol of this kind cannot ensure both the security and the permanent employment of the authentication key if its number of rounds is less than or equal to 3.
Acknowledgement

This work was supported by the National Natural Science Foundation of China under Grant No.61173157.

References

[1] Yang L, Wu L -A. Transmit classical and quantum information secretly. arXiv: quant-ph/0203089, 2002.

[2] Yang L, Wu L A and Liu S H. A quantum three-pass cryptography protocol. in Quantum Optics in Computing and Communication, SPIE, 2002.

[3] Boström K and Felbinger T. Deterministic secure direct communication using entanglement. Physical Review Letters, 89(18): 187902, 2002.

[4] Yang L. Quantum no-key protocol for direct and secure transmission of quantum and classical messages. arXiv: quant-ph/0309200, 2003.

[5] Yang L, Liang M, Li B, Hu L and Wu L -A. Quantum no-key protocols for secret transmission of quantum and classical message. arXiv: 1112.0981, 2011.

[6] Yang L and Liang M. Cryptography based on operator theory (I): quantum no-key protocols. arXiv:1210.8251, 2012.

[7] Lang J. A no-key-exchange secure image sharing scheme based on Shamirs three-pass cryptography protocol and the multiple-parameter fractional Fourier transform. Optics Express, 20(3): 2386-2398, 2012.

[8] Kanamori Y, Yoo S -M and Al-Shurman M. A quantum no-key protocol for secure data communication, in 43rd ACM SE Conference, 2005.

[9] Kak S. A three stage quantum cryptography protocol. Foundations of Physics Letters, 19(3): 293, 2006.

[10] Kye W -H et al. Quantum key distribution with blind polarization bases. Physical Review Letters, 95(4): 040501, 2005.

[11] Deng F -G , Long G L and Liu X -S. Two-step quantum direct communication protocol using the Einstein-podolsky-Rosen pair block. Phys. Rev. A, 68(4): 042317, 2003.