SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

February 2018, Vol. 61 022502:1–022502:8
https://doi.org/10.1007/s11432-017-9180-2

Mutual authenticated quantum no-key encryption scheme over private quantum channel

Li YANG[1,2,3*], Chenmiao WU[1,2,3] & Huiqin XIE[1,2,3]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing* 100093*, China;*
[3]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049*, China*

Received 13 June 2017/Revised 19 June 2017/Accepted 16 July 2017/Published online 27 December 2017

Abstract In this paper, we realize Shamir's no-key protocol via quantum computation of Boolean functions and a private quantum channel. The proposed quantum no-key protocol has three rounds and provides mutual data origin authentication. Random Boolean functions are used to create entanglement and guarantee that any adversary without keys cannot pass the authentication. Thus, our protocol can resist the man-in-the-middle attack. A security analysis has shown that pieces of ciphertexts of the three rounds are completely mixed state. This property ensures no adversary can get any information about the sent message or authentication keys. Therefore, our protocol is unconditionally secure and its authentication keys can be reused.

Keywords quantum cryptography, no-key protocol, quantum entanglement, information-theoretical security, private quantum channel

Citation Yang L, Wu C M, Xie H Q. Mutual authenticated quantum no-key encryption scheme over private quantum channel. Sci China Inf Sci, 2018, 61(2): 022502, https://doi.org/10.1007/s11432-017-9180-2

1 Introduction

First proposed by Shamir [1], the no-key protocol can be used to transmit classical messages secretly over a public channel without a public or secret key. Shamir's protocol is based on a discrete logarithm problem that is vulnerable to man-in-the-middle (MIM) attacks. However, a quantum version of the no-key protocol based on single-photon rotations has been previously developed [2, 3]. The security of quantum no-key (QNK) protocol is based on the laws of quantum mechanics rather than on computational hypotheses. Note that similar protocols have also been proposed previously [4–6].

QNK protocols can achieve unconditional security; however, QNK protocols without identity authentication cannot resist MIM attack. A protocol with inherent identification based on quantum computation of Boolean functions that can prevent MIM attack has been proposed previously [7]. In addition, another study [8] proposed a practical QNK protocol with mutual identification and presented the unbalance-of-information-source attack. A nine-round QNK protocol with data origin authentication that achieves perfect security has also been constructed [9], wherein an encryption key is not required and the authentication key can be reused. In this study, we proposed a QNK protocol with mutual authentication via quantum computation of Boolean functions and a private quantum channel (PQC). This protocol

[*] Corresponding author (email: yangli@iie.ac.cn)

requires only three transmissions and is unconditionally secure. In addition, we prove that the proposed protocol's authentication key can be reused. PQCs are quantum message-oriented protocols based on Shannon's one-time-pad encryption scheme in classical cryptography [10, 11]. Development of quantum one-time pad schemes has been addressed in the literature [12]. Note that the proposed QNK protocol is based on a previously proposed algorithm [10, 11].

Qubit-wise teleportation has been applied to construct a quantum public-key encryption protocol that is unconditionally secure [13]. Although a quantum public-key encryption protocol can achieve unconditional security, it requires an additional system to distribute and authenticate public keys, such as public key infrastructure (PKI). This is not required in no-key protocols. A previously proposed protocol allows a one-time pad to be reused safely with the help of quantum coding [14], and its security does not depend on complexity-theoretic assumptions. The proposed protocol also realizes the permanent use of the key and its security does not depend on computational assumptions.

2 QNK scheme without identification

2.1 PQC

Ambainis et al. [11] defined the notion of PQC, which has an ancillary quantum state. It is a quantum analog of the classical one-time-pad encryption scheme. Here we only consider the case without the ancillary state. Assume N possible keys $1,\dots,N$ and each key $k\in\{1,2,\dots,N\}$ corresponds to a $2^n\times 2^n$ unitary matrix U_k, and p_k represents the probability of choosing k as the secret key. If for every n-qubit quantum message ρ, the output state is a completely mixed state expressed as

$$\sum_k p_k U_k \rho U_k^\dagger = \frac{I}{2^n}, \tag{1}$$

then $\{p_k, U_k\}$ forms a PQC.

Let the plaintext state be n-qubit quantum message ρ. In the encryption stage, U_k is applied to the quantum state. Therefore, the ciphertext is expressed as follows:

$$\rho_{\rm c} = U_k \rho U_k^\dagger. \tag{2}$$

To decrypt the ciphertext, $U_k^\dagger$ is applied to $\rho_{\rm c}$ as follows:

$$\rho = U_k^\dagger \rho_{\rm c} U_k. \tag{3}$$

An eavesdropper without the secret key can only obtain a completely mixed state, which is independent of the plaintext state ρ. Ambainis et al. [11] constructed a PQC by selecting $p_k=\frac{1}{2^{2n}}$, $U_k=X^\alpha Z^\beta, \alpha,\beta\in\{0,1\}^n$, where $X^\alpha=\otimes_{i=1}^n \sigma_x^{\alpha(i)}$, and similarly for Z^β.

We use PQC $\{p_k=\frac{1}{2^{2n}}, U_k=Y^\alpha H^\beta, k=(\alpha,\beta), \alpha,\beta\in\{0,1\}^n\}$ to construct a QNK protocol. First, we prove the following proposition.

Proposition 1. $\{p_k=\frac{1}{2^{2n}}, U_k=U_1^\alpha U_2^\beta, k=(\alpha,\beta), \alpha,\beta\in\{0,1\}^n\}$ is a PQC, if U_1,U_2 is Hermitian, $U_1U_2=-U_2U_1$, and $\{U_1^aU_2^b : a,b\in\{0,1\}\}$ form the basis of the 2×2 matrix space.

Proof. Since $\{U_1^aU_2^b : a,b\in\{0,1\}\}$ forms the basis of the 2×2 matrix space, $\{U_1^\alpha U_2^\beta, \alpha,\beta\in\{0,1\}^n\}$ is a complete orthonormal basis of a $2^n\times 2^n$ matrix space. Therefore, any n-qubit state ρ can be represented as a linear combination of these 2^{2n} unitary matrixes:

$$\rho = \sum_{\alpha,\beta} a_{\alpha,\beta} U_1^\alpha U_2^\beta,$$

where $a_{\alpha,\beta} = {\rm tr}(\rho U_2^\beta U_1^\alpha)/2^n$.

Thus,

$$\begin{aligned}\sum_k p_k U_k \rho U_k^\dagger &= \frac{1}{2^{2n}}\sum_{\gamma,\delta} U_1^\gamma U_2^\delta \rho U_2^\delta U_1^\gamma \\ &= \frac{1}{2^{2n}}\sum_{\alpha,\beta} a_{\alpha,\beta}\sum_{\gamma,\delta} U_1^\gamma U_2^\delta U_1^\alpha U_2^\beta U_2^\delta U_1^\gamma.\end{aligned}$$

From $U_1U_2 = -U_2U_1$, we have $U_2^\delta U_1^\alpha = (-1)^{\alpha\cdot\delta}U_1^\alpha U_2^\delta$. Thus, the above mentioned formula can be expressed as

$$\begin{aligned}&\frac{1}{2^{2n}}\sum_{\alpha,\beta} a_{\alpha,\beta}\sum_{\gamma,\delta}(-1)^{\alpha\cdot\delta}U_1^\alpha U_1^\gamma U_2^\delta(-1)^{\beta\cdot\gamma}U_2^\delta U_1^\gamma U_2^\beta \\ &= \frac{1}{2^{2n}}\sum_{\alpha,\beta} a_{\alpha,\beta}\sum_{\gamma,\delta}(-1)^{\alpha\cdot\delta}(-1)^{\beta\cdot\gamma}U_1^\alpha U_2^\beta.\end{aligned}$$

Because $\frac{1}{2^n}\sum_{\gamma\in\{0,1\}^n}(-1)^{\beta\cdot\gamma} = \delta_{\beta,0}$, the above formula is equal to

$$\sum_{\alpha,\beta} a_{\alpha,\beta}\delta_{\alpha,0}\delta_{\beta,0}U_1^\alpha U_2^\beta = a_{00}I = \frac{\mathrm{tr}(\rho)}{2^n}I = \frac{I}{2^n}.$$

Therefore, it is a PQC.

Corollary 1. $\{p_k = \frac{1}{2^{2n}}, U_k = Y^\alpha H^\beta, k = (\alpha,\beta), \alpha,\beta\in\{0,1\}^n\}$ forms a PQC.

2.2 QNK protocol based on PQC

Assume Alice intends to transmit message ρ to Bob. We construct the QNK protocol without identification based on PQC as follows:

(1) Alice encrypts ρ with $Y^{\alpha_{\rm A}}H^{\beta_{\rm A}}$ and sends Bob $\rho_1 = Y^{\alpha_{\rm A}}H^{\beta_{\rm A}}\rho H^{\beta_{\rm A}}Y^{\alpha_{\rm A}}$;

(2) Bob encrypts ρ_1 with $Y^{\alpha_{\rm B}}H^{\beta_{\rm B}}$ and sends Alice $\rho_2 = Y^{\alpha_{\rm B}}H^{\beta_{\rm B}}\rho_1 H^{\beta_{\rm B}}Y^{\alpha_{\rm B}}$;

(3) Alice decrypts ρ_2 with $H^{\beta_{\rm A}}Y^{\alpha_{\rm A}}$ and sends Bob $\rho_3 = H^{\beta_{\rm A}}Y^{\alpha_{\rm A}}\rho_2 Y^{\alpha_{\rm A}}H^{\beta_{\rm A}}$;

(4) Bob decrypts ρ_3 with $H^{\beta_{\rm B}}Y^{\alpha_{\rm B}}$ to recover ρ.

The plaintext state ρ can be a classical or quantum message. The soundness of this protocol can be checked easily. The plaintext is encrypted using a PQC; thus, the ciphertext state is a completely mixed state that has nothing to do with the plaintext.

However, this protocol cannot resist MIM attacks. If an attacker Eve intercepts message ρ_1 from Alice, Eve randomly select bit strings α_E and β_E to encrypt ρ_1 and send Alice $\rho_2' = Y^{\alpha_{\rm E}}H^{\beta_{\rm E}}\rho_1 H^{\beta_{\rm E}}Y^{\alpha_{\rm E}}$. Alice decrypts ρ_2' with $H^{\beta_{\rm A}}Y^{\alpha_{\rm A}}$ and sends Eve $\rho_3' = H^{\beta_{\rm A}}Y^{\alpha_{\rm A}}\rho_2' Y^{\alpha_{\rm A}}H^{\beta_{\rm A}}$. Eve receives ρ_3' and decrypts it with $H^{\beta_{\rm E}}Y^{\alpha_{\rm E}}$. Finally, Eve can obtain message ρ successfully. Note that we add identification to the protocol to resist MIM attacks (Section 3).

Remark 1. There are many choices for U_1 and U_2 to construct a PQC, such as X and Z, X and Y, and Y and H, X and H. Thus, the following examples are all quantum perfect encryptions.

(1) PQC1: $\{p_k = \frac{1}{2^{2n}}, U_k = X^\alpha Z^\beta, k = (\alpha,\beta), \alpha,\beta\in\{0,1\}^n\}$;

(2) PQC2: $\{p_k = \frac{1}{2^{2n}}, U_k = X^\alpha Y^\beta, k = (\alpha,\beta), \alpha,\beta\in\{0,1\}^n\}$;

(3) PQC3: $\{p_k = \frac{1}{2^{2n}}, U_k = X^\alpha H^\beta, k = (\alpha,\beta), \alpha,\beta\in\{0,1\}^n\}$;

(4) PQC4: $\{p_k = \frac{1}{2^{2n}}, U_k = Y^\alpha H^\beta, k = (\alpha,\beta), \alpha,\beta\in\{0,1\}^n\}$.

(1) When we select PQC1: $\{p_k = \frac{1}{2^{2n}}, U_k = X^\alpha Z^\beta, \alpha,\beta\in\{0,1\}^n\}$ the QNK protocol cannot transmit classical information securely because the X operation reverses the bit and the Z operation shifts the phase. Thus the attacker can measure the ciphertext state in the basis $\{|0\rangle,|1\rangle\}$ without breaking it. In addition, because the three ciphertexts transmitted between Alice and Bob are $X^{\alpha_{\rm A}}Z^{\beta_{\rm A}}|m\rangle$, $X^{\alpha_{\rm B}}Z^{\beta_{\rm B}}X^{\alpha_{\rm A}}Z^{\beta_{\rm A}}|m\rangle$, and $X^{\alpha_{\rm B}}Z^{\beta_{\rm B}}|m\rangle$, the attacker can acquire three strings $\alpha_{\rm A}\oplus m, \alpha_{\rm B}\oplus\alpha_{\rm A}\oplus m$, and $\alpha_{\rm B}\oplus m$ by measuring the three ciphertexts. The attacker can compute $\alpha_{\rm B}$ using the 1st and the 2nd string. Then, they can compute message m using the value of $\alpha_{\rm B}$ and the 3rd string.

(2) When selecting the PQC2: $\{p_k = \frac{1}{2^{2n}},\ U_k = X^{\alpha}Y^{\beta}, \alpha, \beta \in \{0,1\}^n\}$ for the QNK protocol, it is also unsafe to transmit classical information for the same reason. In this case, the three ciphers transmitted between Alice and Bob are $X^{\alpha_{\rm A}}Y^{\beta_{\rm A}}|m\rangle$, $X^{\alpha_{\rm B}}Y^{\beta_{\rm B}}X^{\alpha_{\rm A}}Y^{\beta_{\rm A}}|m\rangle$, and $X^{\alpha_{\rm B}}Y^{\beta_{\rm B}}|m\rangle$, and measuring the three ciphers can obtain the three strings $\alpha_{\rm A} \oplus \beta_{\rm A} \oplus m$, $\alpha_{\rm B} \oplus \beta_{\rm B} \oplus \alpha_{\rm A} \oplus \beta_{\rm A} \oplus m$, and $\alpha_{\rm B} \oplus \beta_{\rm B} \oplus m$. The attacker can computes $\alpha_{\rm B} \oplus \beta_{\rm B}$ using the first and second string. Then, they can compute message m using the value of $\alpha_{\rm B} \oplus \beta_{\rm B}$ and the third string.

(3) In PQC3: $\{p_k = \frac{1}{2^{2n}}, U_k = X^{\alpha}H^{\beta}, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$, X and H do not satisfy the condition that X and Y should form an orthonormal basis.

(4) By using $Y^{\alpha}H^{\beta}$ in the protocol, the message is encoded into conjugate coding, and the flaw stated above is eliminated. If POC1 and POC2 are used, after the classical bits are encoded into the computational basis state, the message states will stay in computational basis state during the exchange in the protocol. Here, it is better to choose PQC4: $\{p_k = \frac{1}{2^{2n}}, U_k = Y^{\alpha}H^{\beta}, k = (\alpha, \beta), \alpha, \beta \in \{0,1\}^n\}$ for the QNK protocol.

3 QNK scheme with interactive identification

3.1 Boolean function

We use a Boolean function to construct QNK protocol with interactive identification. We can choose a multi-output Boolean function $F: \{0,1\}^n \to \{0,1\}^n$ randomly via a coin toss. In particular, for security parameter n, let $p(n)$ be a polynomial of n, let $F(x) = (F^{(1)}(x), F^{(2)}(x), \ldots, F^{(n)}(x))$, $x = (x_1, \ldots, x_n)$, and for $z_i, c_i \in F_2$, let $z_i^1 = z_i$, $z_i^0 = \bar{z}_i = 1 + z_i$, then we have

$$z_i^{c_i} = \begin{cases} 1, & z_i = c_i, \\ 0, & z_i \neq c_i. \end{cases}$$

Therefore,

$$z_1^{c_1} z_2^{c_2} \cdots z_n^{c_n} = \begin{cases} 1, & (z_1, z_2, \ldots, z_n) = (c_1, c_2, \ldots, c_n), \\ 0, & (z_1, z_2, \ldots, z_n) \neq (c_1, c_2, \ldots, c_n). \end{cases}$$

To determine the value of $F^{(i)}(x)$, where $i = 1, \ldots, n$, we toss a coin $np(n)$ times to generate $p(n)$ random n-tuples $(c_{j1}^{(i)}, c_{j2}^{(i)}, \ldots, c_{jn}^{(i)})$, $j = 1, 2, \ldots, p(n)$. Here, $F^{(i)}(x)$ is expressed as follows:

$$F^{(i)}(x) = \sum_{j=1}^{p(n)} x_1^{c_{j1}^{(i)}} x_2^{c_{j2}^{(i)}} \cdots x_n^{c_{jn}^{(i)}}.$$

Therefore, we can determine the value of $F(x)$ by tossing a coin for $n^2p(n)$ times.

It is possible that for fixed i, $p(n)$ coin tosses generate the same two n-tuples $(c_{j1}^{(i)}, c_{j2}^{(i)}, \ldots, c_{jn}^{(i)})$. In this situation, we can simply discard the duplicate terms because the probability of this happening is negligible.

3.2 Scheme description

In the protocol description, we only take a classical message as an example. The QNK protocol with identification can also be used to transmit a quantum message. Here assume Alice and Bob preshare bit strings s and r, $s \in \{0,1\}^{n^2p(n)}$, and $r \in \{0,1\}^{\frac{n}{2}}$, and Alice intends to transmit classical message $x \in \{0,1\}^n$ to Bob through a quantum channel.

(1) Alice randomly selects $\alpha_{\rm A}, \beta_{\rm A} \in \{0,1\}^n$ to encrypt $|x\rangle_{\rm I}\langle x|$ with $Y^{\alpha_{\rm A}}H^{\beta_{\rm A}}$:

$$Y^{\alpha_{\rm A}}H^{\beta_{\rm A}}|x\rangle_{\rm I}\langle x|H^{\beta_{\rm A}}Y^{\alpha_{\rm A}} = \sum_m \alpha_m |m\rangle_{\rm I}\langle m|. \tag{4}$$

Then, by considering s as the result of $n^2p(n)$ coin tosses, Alice performs a unitary transform U_s on the quantum state:

$$\begin{aligned} & U_s\bigg(\sum_m \alpha_m |m\rangle_{\rm I}\langle m| \otimes |0\rangle_{\rm II}\langle 0|\bigg)U_s^\dagger \\ & = \sum_m \alpha_m |m\rangle_{\rm I}\langle m| \otimes |F_s(m)\rangle_{\rm II}\langle F_s(m)|, \end{aligned} \tag{5}$$

where F_s is the Boolean function described in Subsection 3.1. Here U_s is defined as $U_s|x\rangle_{\rm I}|y\rangle_{\rm II} = |x\rangle_{\rm I}|y \oplus F_s(x)\rangle_{\rm II}$. Then Alice uses r and a randomly selected bit string $r_{\rm A} \in \{0,1\}^{\frac{n}{2}}$ to perform an exclusive-or operation to obtain

$$\sum_m \alpha_m |m\rangle_{\rm I}\langle m| \otimes |F_s(m) \oplus r\|r_{\rm A}\rangle_{\rm II}\langle F_s(m) \oplus r\|r_{\rm A}|. \tag{6}$$

The first register represents the plaintext encryption, and the second register consists of the identity information about Alice.

Finally Alice sends Bob registers I, II.

(2) Bob then uses preshared s to perform the following computation:

$$\begin{aligned} & U_s\bigg(\sum_m \alpha_m |m\rangle_{\rm I}\langle m| \otimes |F_s(m) \oplus r\|r_{\rm A}\rangle_{\rm II}\langle F_s(m) \oplus r\|r_{\rm A}|\bigg)(U_s)^\dagger \\ & = \sum_m \alpha_m |m\rangle_{\rm I}\langle m| \otimes |F_s(m) \oplus F_s(m) \oplus r\|r_{\rm A}\rangle_{\rm II}\langle F_s(m) \oplus F_s(m) \oplus r\|r_{\rm A}| \\ & = \sum_m \alpha_m |m\rangle_{\rm I}\langle m| \otimes |r\|r_{\rm A}\rangle_{\rm II}\langle r\|r_{\rm A}|, \end{aligned} \tag{7}$$

then Bob measures the second register to obtain the string $r\|r_{\rm A}$. If the first $\frac{n}{2}$ bits are identical to r, Bob accepts that the message has come from Alice; otherwise, he aborts the scheme.

Through verification, Bob randomly selects $\alpha_{\rm B}, \beta_{\rm B} \in \{0,1\}^n$, and uses $Y^{\alpha_{\rm B}}H^{\beta_{\rm B}}$ to encrypt register I:

$$Y^{\alpha_{\rm B}}H^{\beta_{\rm B}}\bigg(\sum_m \alpha_m |m\rangle_{\rm I}\langle m|\bigg)H^{\beta_{\rm B}}Y^{\alpha_{\rm B}} = \sum_m \alpha'_m |m\rangle_{\rm I}\langle m|. \tag{8}$$

The first register contains the transmitted plaintext, and Bob will uses the third register to add his identity information.

Bob performs transform U_s as follows:

$$U_s\bigg(\sum_m \alpha'_m |m\rangle_{\rm I}\langle m| \otimes |0\rangle_{\rm III}\langle 0|\bigg)U_s^\dagger = \sum_m \alpha'_m |m\rangle_{\rm I}\langle m| \otimes |F_s(m)\rangle_{\rm III}\langle F_s(m)|, \tag{9}$$

and uses $r_{\rm A}$ and a randomly selected $r_{\rm B}$ to perform an exclusive-or operation. Then, the quantum state becomes

$$\sum_m \alpha'_m |m\rangle_{\rm I}\langle m| \otimes |F_s(m) \oplus r_{\rm A}\|r_{\rm B}\rangle_{\rm III}\langle F_s(m) \oplus r_{\rm A}\|r_{\rm B}|. \tag{10}$$

Bob then sends Alice registers I, III.

(3) Alice uses s to disentangle the registers as follows:

$$\begin{aligned} & U_s\bigg(\sum_m \alpha'_m |m\rangle_{\rm I}\langle m| \otimes |F_s(m) \oplus r_{\rm A}\|r_{\rm B}\rangle_{\rm III}\langle F_s(m) \oplus r_{\rm A}\|r_{\rm B}|\bigg)(U_s)^\dagger \\ & = \sum_m \alpha'_m |m\rangle_{\rm I}\langle m| \otimes |r_{\rm A}\|r_{\rm B}\rangle_{\rm III}\langle r_{\rm A}\|r_{\rm B}|. \end{aligned} \tag{11}$$

Alice then measures the third register. If the first part of the measurement result equals to $r_{\rm A}$, she accepts the legality of Bob; otherwise, the scheme is aborted.

Through verification, Alice decrypts the state with $H^{\beta_{\rm A}}Y^{\alpha_{\rm A}}$:

$$H^{\beta_{\rm A}}Y^{\alpha_{\rm A}}\bigg(\sum_m \alpha'_m|m\rangle_{\rm I}\langle m|\bigg)Y^{\alpha_{\rm A}}H^{\beta_{\rm A}}=\sum_m \alpha''_m|m\rangle_{\rm I}\langle m|, \tag{12}$$

Alice randomly chooses bit string $r_C\in\{0,1\}^{\frac{n}{2}}$. She uses s to perform transform U_s and r_C, $r_{\rm B}$ to perform an exclusive-or operation:

$$\begin{aligned}&\sum_m \alpha''_m|m\rangle_{\rm I}\langle m|\otimes|0\rangle_{\rm IV}\langle 0|\\ &\quad\to\sum_m \alpha''_m|m\rangle_{\rm I}\langle m|\otimes|F_s(m)\oplus r_{\rm B}\|r_C\rangle_{\rm IV}\langle F_s(m)\oplus r_{\rm B}\|r_C|,\end{aligned} \tag{13}$$

then sends Bob registers I, IV.

(4) Bob uses s to perform U_s transform to disentangle the registers:

$$\begin{aligned}&U_s\bigg(\sum_m \alpha''_m|m\rangle_{\rm I}\langle m|\otimes|F_s(m)\oplus r_{\rm B}\|r_C\rangle_{\rm IV}\langle F_s(m)\oplus r_{\rm B}\|r_C|\bigg)(U_s)^\dagger\\ &=\sum_m \alpha''_m|m\rangle_{\rm I}\langle m|\otimes|r_{\rm B}\|r_C\rangle_{\rm IV}\langle r_{\rm B}\|r_C|.\end{aligned} \tag{14}$$

By measuring register IV, Bob can verify the legitimacy of Alice. He retains r_C to replace r. Thus, the preshared bit strings between Alice and Bob for the next session are s and r_C.

If Bob verifies the message sender is Alice, he decrypts the message with $H^{\beta_{\rm B}}Y^{\alpha_{\rm B}}$:

$$H^{\beta_{\rm B}}Y^{\alpha_{\rm B}}\bigg(\sum_m \alpha''_m|m\rangle_{\rm I}\langle m|\bigg)Y^{\alpha_{\rm B}}H^{\beta_{\rm B}}=|x\rangle_{\rm I}\langle x|, \tag{15}$$

and obtains the transmitted message x.

The soundness of the protocol can be evaluated easily. We use a Boolean function to produce entanglement between the ciphertext state and the identity information. In addition, local random numbers $r, r_{\rm A}, r_B$, and r_C can also protect the authentication key s.

3.3 Security analysis

In the first round of communication, if the adversary intercepts the transmitted message in the quantum channel, the message state for the adversary is as follows:

$$\sigma_1=\sum_{m,s,r,r_{\rm A}}\alpha_m|m\rangle_{\rm I}\langle m|\otimes|F_s(m)\oplus r\|r_{\rm A}\rangle_{\rm II}\langle F_s(m)\oplus r\|r_{\rm A}|. \tag{16}$$

Since the adversary does not know the value of r and $r_{\rm A}$, the quantum state $\sum_{s,r,r_{\rm A}}|F_s(m)\oplus r\|r_{\rm A}\rangle_{\rm II}\langle F_s(m)\oplus r\|r_{\rm A}|$ is a completely mixed state that has nothing to do with the value of m. Part of the ciphertext state: $\sum_m\alpha_m|m\rangle_{\rm I}\langle m|$ is obtained by performing H and Y on the plaintext state. We have proved that $\{p_k=\frac{1}{2^{2n}}, U_k=Y^\alpha H^\beta, k=(\alpha,\beta), \alpha,\beta\in\{0,1\}^n\}$ forms a PQC. Therefore, $\sum_m\alpha_m|m\rangle_{\rm I}\langle m|$ is a completely mixed state.

Thus, the message state σ_1 for the adversary is as follows:

$$\sigma_1=\sum_m\alpha_m|m\rangle_{\rm I}\langle m|\otimes\sum_{s,r,r_{\rm A}}|F_s(m)\oplus r\|r_{\rm A}\rangle_{\rm II}\langle F_s(m)\oplus r\|r_{\rm A}|=\frac{I}{2^n}\otimes\frac{I}{2^n}=\frac{I}{2^{2n}}. \tag{17}$$

Since σ_1 is a completely mixed state, the adversary cannot acquire anything by measuring it.

In the second round of communication, the transmitted message state becomes

$$\sigma_2=\sum_{m,s,r_{\rm A},r_{\rm B}}\alpha'_m|m\rangle_{\rm I}\langle m|\otimes|F_s(m)\oplus r_{\rm A}\|r_{\rm B}\rangle_{\rm III}\langle F_s(m)\oplus r_{\rm A}\|r_{\rm B}|. \tag{18}$$

Suppose the adversary is able to intercept the transmitted quantum state. Then, the quantum state for the adversary is also a completely mixed state:

$$\sigma_2 = \frac{I}{2^{2n}}. \tag{19}$$

Similarly, in the third round, the transmitted message state is also an completely mixed state:

$$\sigma_3 = \sum_m \alpha''_m |m\rangle_{\mathrm{I}}\langle m| \otimes |F_s(m) \oplus r_{\mathrm{B}} \| r_C\rangle_{\mathrm{IV}}\langle F_s(m) \oplus r_{\mathrm{B}} \| r_C| = \frac{I}{2^{2n}}. \tag{20}$$

The above mentioned analysis demonstrates that the transmitted message states during each round are completely mixed states from the adversary's perspective; thus, the preshared s, r and secret information x will not be disclosed to the attacker. Therefore, an MIM attack is not effective with this protocol. However, a problem remains, i.e., we cannot prove that the direct product of σ_1, σ_2 and σ_3 is a completely mixed state. If the adversary obtains all the three states σ_1, σ_2 and σ_3, she may obtain partial information about x, s or r.

As mentioned previously, the adversary may intercept all transmitted ciphertexts during one session between Alice and Bob. The transmitted ciphertext during the three rounds of communication are as follows:

$$\begin{aligned}
\sigma_1 &= \sum_{m,s,r,r_{\mathrm{A}}} \alpha_m |m\rangle_{\mathrm{I}}\langle m| \otimes |F_s(m) \oplus r \| r_{\mathrm{A}}\rangle_{\mathrm{II}}\langle F_s(m) \oplus r \| r_{\mathrm{A}}|,\\
\sigma_2 &= \sum_{m,s,r_{\mathrm{A}},r_{\mathrm{B}}} \alpha'_m |m\rangle_{\mathrm{I}}\langle m| \otimes |F_s(m) \oplus r_{\mathrm{A}} \| r_{\mathrm{B}}\rangle_{\mathrm{III}}\langle F_s(m) \oplus r_{\mathrm{A}} \| r_{\mathrm{B}}|,\\
\sigma_3 &= \sum_m \alpha''_m |m\rangle_{\mathrm{I}}\langle m| \otimes |F_s(m) \oplus r_{\mathrm{B}} \| r_C\rangle_{\mathrm{IV}}\langle F_s(m) \oplus r_{\mathrm{B}} \| r_C|.
\end{aligned}$$

The entire quantum state from the adversary's perspective is as follows:

$$\begin{aligned}
&\sum_{m_1,m_2,m_3} \sum_{s,r,r_{\mathrm{A}},r_{\mathrm{B}},,r_C} \alpha_{m_1}\alpha'_{m_2}\alpha''_{m_3} |m_1,m_2,m_3\rangle_{\mathrm{I}}\langle m_1,m_2,m_3|\\
&\otimes |F_s(m_1) \oplus r \| r_{\mathrm{A}} F_s(m_2) \oplus r_{\mathrm{A}} \| r_{\mathrm{B}}, F_s(m_3) \oplus r_{\mathrm{B}} \| r_C\rangle_{\mathrm{II}}\\
&\times_{\mathrm{II}}\langle F_s(m_1) \oplus r \| r_{\mathrm{A}}, F_s(m_2) \oplus r_{\mathrm{A}} \| r_{\mathrm{B}}, F_s(m_3) \oplus r_{\mathrm{B}} \| r_C|.
\end{aligned} \tag{21}$$

If we consider the direct product of any two ciphertexts among the three transmitted ciphertexts in the proposed QNK protocol (Section 2). we cannot determine that the state is still a completely mixed state. Therefore, we cannot prove that the trace distance between the states for different plaintext and authentication keys s and r is zero, which indicates that information about authentication keys s and r may leak. As a result, we cannot prove the permanent use of authentication keys s and r.

Fortunately, guaranteed by the no-cloning theorem, the adversary cannot copy the unknown quantum state transmitted in the channel. The participants involved in the communication process send message with identification. A message without identity information is not sent into the channel. All three ciphertexts cannot be possessed by the adversary simultaneously. The coefficients $\alpha_{m_1}, \alpha'_{m_2}$ and α''_{m_3} are essentially functions of time and space, and they are distributed in different space-time points. The product of probability amplitudes α_{m_1}, α'_{m_2}, and α''_{m_3} is zero for any given space-time point. Thus, there is no need to prove that the direct product of any two ciphertexts among the three transmitted ciphertexts is a completely mixed state. There is also no need to prove that the quantum state (21) is a completely mixed state.

The proposed protocol is based on an idea that is similar to that of Shamir's no-key protocol. The protocol achieves mutual authentications; it can resist the MIM attack. The encryption of the message does not require keys, i.e., only authentication requires keys. Fortunately, the authentication key can be used permanently. Thus, we consider the proposed protocol as a QNK protocol although it requires an authentication key.

4 Discussion

One of the most important advantages of the public-key cryptosystem is that multiple users can send message to a user using the same encryption key. In addition, a quantum public-key encryption protocol can achieve unconditional security [13]. However, a public-key cryptosystem requires an additional trusted system to distribute and authenticate public keys, such as PKI. Shamir proposed an identity-based cryptosystem to address this problem. However, an identity-based cryptosystem still requires a private key generator. In addition, the symmetric-key cryptosystem can only provide point-to-point encryption. The no-key encryption scheme can compensate these deficiencies. The proposed QNK protocol can achieve unconditional security and trusted third parties are not required. In addition, when MIM attacks are not considered, the proposed QNK protocol does not require keys.

It is necessary to share the key for identity authentication over a channel. In a classical situation, the authentication keys cannot be used permanently because information leakage always occurs with repeated use of the given key. However, the proposed QNK protocol ensures the permanent use of authentication keys.

5 Conclusion

QNK encryption protocols are based on quantum perfect encryption. The proposed QNK protocol employs random bit strings, Boolean permutation and property of entanglement to ensure security. Using identification information, the proposed protocol can resist MIM attacks. A security analysis has shown that pieces of ciphertexts of the three rounds are completely mixed state, and the authentication keys can be reused permanently.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61672517), National Cryptography Development Fund (Grant No. MMJJ20170108), National Key Research and Development Program of China (Grant No. 2017YFB0802502), and Fundamental Theory and Cutting Edge Technology Research Program of Institute of Information Engineering, CAS (Grant No. Y7Z0301103).

References

1 Menezes G J, van Oorschot P C, Vanstone S A. Handbook of Applied Cryptography. Boca Raton: Crc Press, 1997

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

3 Yang L, Wu L A, Liu S H. Quantum three-pass cryptography protocol. In: Proceedings of SPIE 2002 Quantum Optics in Computing and Communications, SPIE, 2009. 4917: 107–112

4 Kanamori Y, Yoo S M, Mohammad A S. A quantum no-key protocol for secure data communication. In: Proceedings of Proc 43rd Annual Southeast Regional Conference. New York: ACM Press, 2005. 2: 92–93

5 Kak S. A three stage quantum cryptography protocol. Found Phys Lett, 2006, 19: 293–296

6 Kye W H, Kim C M, Kim M S, et al. Quantum key distribution with blind polarization bases. Phys Rev Lett, 2005, 95: 040501

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

8 Wu Y, Yang L. Practical quantum no-key protocol with identification. In: Proceedings of the 5th International Conference on Information Assurance and Security, Xi'an, 2009. 540–543

9 Yang L. Quantum no-key protocol for secure communication of classical message. 2013, arXiv: 1306.3388

10 Boykin P, Roychowdhury V. Optimal encryption of quantum bits. Phys Rev A, 2003, 67: 042317

11 Ambainis A, Mosca M, Tapp A, et al. Private quantum channels. In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science. Redondo Beach: IEEE Computer Society Press, 2000. 547–553

12 Nayak A, Sen P. Invertible quantum operations and perfect encryption of quantum states. Quantum Inf Comput, 2007, 7: 103–110

13 Wu C, Yang L. Qubit-wise teleportation and its application in public-key secret communication. Sci China Inf Sci, 2017, 60: 032501

14 Bennett C H, Brassard G, Breidbart S. Quantum cryptography II: how to re-use a one-time pad safely even if P= NP. Natural Comput, 2014, 13: 453–458