Quantum public-key encryption schemes based on conjugate coding

Li Yang[1], Biyao Yang, Chong Xiang

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

Abstract

We present several quantum public-key encryption (QPKE) protocols designed with conjugate coding single-photon string, thus may be realized in laboratory with nowadays techniques. Two of these schemes are orienting one-bit message, and are extended to two kinds of QPKE schemes orienting multi-bits. The novel structure of these protocols ensures they are information-theoretically secure with, probably, a bound greater than any given polynomial of n. Finally, we describe a way to conceal the classical part of the public key with quantum state, this idea is expected to enhance a scheme to be information-theoretically secure.

Keywords: quantum cryptography, quantum public-key encryption, information-theoretic security

1. Introduction

Public-key encryption was first proposed in 1976 [1, 2], which makes the two parties can do secret communication without presharing a secret key. Up till now, the security of a public-key cryptography scheme is based on a mathematically difficult problem, though whose difficulty has not been proved. In a quantum computation environment, most of these problems will be no more difficult [3], then the related public-key protocols will not be secure.

Then we need to find new public-key schemes to resist the attacks of quantum adversaries. One solution is private-key protocols with the aid of

[1] Corresponding author. E-mail: yangli@iie.ac.cn

quantum key distribution (QKD). Many schemes of QKD have been proposed [4, 5, 6, 7, 8]. Another solution is to construct quantum public-key encryption (QPKE). Okamoto et al. [9] introduce a public-key encryption scheme with a quantum algorithm in key generation phase. Gottesman [10] is the first to put forward a protocol named "quantum public key cryptography with information-theoretic security". Yang et al. [11, 12] present some public-key encryption protocols based on induced trap-door one-way transformation. Kawachi et al. present a QPKE scheme of based on "computational indistinguishability" of two quantum states [13, 14] related with automorphism group of graphs problem. Nikolopoulos presents a QPKE scheme [15, 16] based on single-qubit rotations.

This paper is organized as follows. In Section 2, we describe some basic definitions of information-theoretic security, one-way function and hash functions. In Section 3, we present two public-key encryptions orienting one-bit message based on conjugate coding. In section 4, we extend the schemes to those orienting multi-bits. In section 5, we describe a way to conceal the classical part of the public key with quantum state, this idea is expected to enhance a scheme to be information-theoretically secure. In section 6, we discuss a public-key encryption scheme based on a special entanglement state we presented in [19].

2. Preliminary

2.1. Information-theoretic security

The ciphertext-indistinguishability under chosen plaintext attack (IND-CPA) [17] can be understand as that while the adversary chooses two plaintexts and is then given one of the corresponding ciphertexts, the adversary cannot yet determine which plaintext corresponds to the previously unseen ciphertext he received.

Strictly speaking, the concept information-theoretic IND-CPA is defined as [18]: for every circuit family $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n, and every $x, y \in \{0,1\}^*$, the probability $\Pr(\cdot)$ satisfies:

$$|\Pr[C_n(G(1^n), E_{G(1^n)}(x)) = 1] - \Pr[C_n(G(1^n), E_{G(1^n)}(y)) = 1]| < \frac{1}{p(n)}. \qquad (1)$$

In the case of QPKE, the information-theoretic quantum IND-CPA is defined as [19]:

Definition 1. *A quantum public-key encryption scheme is information -theoretically ciphertext-indistinguishable under quantum CPA if for every* *quantum circuit family $\{C_n\}$, every positive polynomial $p(\cdot)$, all sufficiently large n, and every bit-string $x, y \in \{0,1\}^*$, the probability $\Pr(\cdot)$ satisfies:*

$$|\Pr[C_n(G(1^n), E_{G(1^n)}(x)) = 1] - \Pr[C_n(G(1^n), E_{G(1^n)}(y)) = 1]| < \frac{1}{p(n)}, \qquad (2)$$

where the algorithm E is a quantum encryption algorithm, and the ciphertext $E(x)$, $E(y)$ are quantum states.

It is proved [20] that if the trace distance between any two ciphertexts is $O(\frac{1}{2^n})$, Eq. (2) will hold, and the quantum public-key encryption scheme will be information-theoretically secure.

The term "bounded information-theoretically secure" means that the bit number of plaintext encrypted with information-theoretic security has an upper bound. In [14], this bound of the protocol is proven to be the bit number of private key [21], thus it is much less than that of a practical protocol.

2.2. One-way function

A trapdoor one-way function is necessary in a public-key encryption protocol. A one-way function(OWF)based on classical computational complexity hypothesis [17] is a function f such that for each x in the domain of f, it is easy to compute $f(x)$; but for essentially all y in the range of f, it is infeasible to find any x such that $y = f(x)$ in expected polynomial time, i.e.

$$\Pr[A(f(U_n), 1^n) \in f^{-1}(f(U_n))] < \frac{1}{p(n)}. \qquad (3)$$

A trapdoor one-way function [17] is a one-way function f with the additional property that if some extra information (called the trapdoor information) is given, it will becomes feasible to find an x in the domain of f, for any given y in the range of f, such that $f(x) = y$.

The one-way property of classical OWF is usually in the sense of computational security, i.e., it is based on a hypothesis of the adversary's power of computation. The quantum one-way transformation(OWT) we suggest here is in the sense of information-theoretic security, since it is based on the property of quantum states: people with the correct basis can get the exact bits contained in the states, but one without the information of basis cannot get them with an in-negligible probability.

2.3. Hash functions and randomness

In our schemes below, a multi-output Boolean function $F : \{0,1\}^m \to \{0,1\}^n (m > n)$ is used as the private key. Since $m > n$, F can also be taken as a Hash function. Suppose X is the set of all messages (input), and Y is the set of all message digests (output) with $|Y| = M$. The theorem in [22] ensures the randomness of the function's output:

Theorem 1. *Suppose Hash function h is randomly selected, let $X_0 \subseteq X$. Suppose that if and only if $x \in X_0$, $h(x)$ is determined (through querying the oracle). Then for all $x \in X/X_0$ and $y \in Y$, there is always the relation $\Pr[h(x) = y] = 1/M$.*

3. Quantum public-key encryption schemes for one-bit message

Let $k = (k_1, \cdots, k_n)$ be a n-bit string, where $k_1, \cdots, k_n \in \{0,1\}$. For the Hadamard transform $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, we define $H_k = H^{k_1} \otimes \cdots \otimes H^{k_n}$, where H^0 is the unit operator I, and H^1 is H. Similarly for the Pauli operator $Y = \begin{bmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{bmatrix}$, we define $Y_k = Y^{k_1} \otimes \cdots \otimes Y^{k_n}$. Let $\Omega_b = \{i \in \{0,1\}^n | i_1 \oplus \cdots \oplus i_n = b\}$, here $b = 0, 1$.

3.1. First scheme

In this scheme, the OWT is a transformation mapping the classical message b to an unknown state

$$\rho_b = \sum_{P(j)=b} Y_j \left[\sum_F H_{F(s)} \left(\sum_{P(i)=0} p_{iF} |i\rangle\langle i| \right) H_{F(s)} \right] Y_j.$$

The trapdoor information is the basis string $k = F(s)$ on which the quantum states are encoded. The private key is a Boolean function F. Using s, the classical part of the public-key, the private-key owner can get the trapdoor information k by $k = F(s)$. The scheme is shown as follows:

[**Key Generation**] During this phase, Bob can do as follows:

(G1) Select randomly a multi-output Boolean function $F : \{0,1\}^m \to \{0,1\}^n$ as his private key;

(G2) Select randomly $s \in \{0,1\}^m$, and computes $k = F(s)$;

(G3) Generate $|i\rangle$ with $i \in \Omega_0$;

(G4) Apply H_k to $|i\rangle$, and take the classical-quantum pair $(s, H_k|i\rangle)$ as one of his public-keys.

[Encryption] If Alice wants to send one bit message b to Bob, she should get one of Bob's public keys, and then:

(E1) Select j randomly from Ω_b;

(E2) Alice applies Y_j to $H_k|i\rangle$, and then sends $(s, Y_j H_k|i\rangle)$ to Bob.

[Decryption] After receiving the ciphertext, Bob should:

(D1) Calculate $k = F(s)$;

(D2) Apply H_k to $Y_j H_k|i\rangle$, and measure it in the basis $\{|0\rangle, |1\rangle\}^n$.

Here F can be generated efficiently. Each output of the Boolean function F can be written as

$$F^i(s) = \bigoplus_{d_1,\cdots,d_m} \alpha^i_{d_1,\cdots,d_m} s_1^{d_1} \cdots s_m^{d_m}, \tag{4}$$

where $i = 1, \cdots, n$. There are 2^m terms to add up in each $F^i(s)$, but after m times of coin tossing, we can determined a $s_1^{d_1} \cdots s_m^{d_m}$ by one instance of $d_1, \cdots, d_m$. We let the corresponding $\alpha^i_{d_1,\cdots,d_m} = 1$, then one component is determined. If we toss the coin for $m \cdot O(m)$ times, $O(m)$ components are determined. We then let other component coefficients to be zero. Thus F can be efficiently generated by $n \cdot m \cdot O(m)$. This algorithm produces many strings of m random bits, and the number of the strings is polynomial in m.

Bob generates a large amount of public-keys with a private key F. In each of these public-keys, s is different. The classical string s is bounded to the quantum state $H_k|i\rangle$ as a label.

The public key state for the adversary is $\sum_F \sigma_{F,s}$, here

$$\sigma_{F,s} = H_{F(s)} \left(\sum_{P(i)=0} p_{iF} |i\rangle\langle i| \right) H_{F(s)}. \tag{5}$$

The ciphertext state for the adversary is

$$\left(s, \sum_j Y_j \left[\sum_F H_{F(s)} \left(\sum_{P(i)=0} p_{ijF} |i\rangle\langle i| \right) H_{F(s)} \right] Y_j \right), \tag{6}$$

and the quantum part of the ciphertext for a selected j is

$$\rho_j = Y_j \left[\sum_F H_{F(s)} \left(\sum_{P(i)=0} p_{iF} |i\rangle\langle i| \right) H_{F(s)} \right] Y_j. \tag{7}$$

While Bob gets the one-bit message from the parity of bit string he received. The state after applying H_k to $Y_j H_k |i\rangle$ is

$$H_k Y_j H_k |i\rangle = (-1)^{k\cdot j} Y_j |i\rangle = (-1)^{j\cdot(i\oplus k)+\frac{1}{2}W_H(j)} |i \oplus j\rangle. \tag{8}$$

Thus, after measuring it, Bob gets $|i \oplus j\rangle$, here $\oplus$ is bit-wise addition modulo 2. The parity of $W_H(j)$ is equal to the parity of $W_H(i \oplus j)$, because $W_H(i)$ is even. Then the message (plaintext) is obtained.

3.2. Security analysis

The adversary has two ways to attack the QPKE scheme. One is to attack plaintext via distinguishing the two ciphertexts; another is to attack the private key F via getting information of k.

For the first way of attack, we now prove that the trace distance between the two different ciphertexts is $O(\frac{1}{2^n})$.

The quantum part of public key $H_k|i\rangle$ is a state consisting of n qubits from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and the total number of $|1\rangle$ and $|-\rangle$ is even. After encrypted by Alice, the state is also n qubits from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.

If the message is 0, the number of 1 in j is even, then the number of qubits operated by Y is even. If the number of Y on $|1\rangle$ and $|-\rangle$ is odd, then the number of Y on $|0\rangle$ and $|+\rangle$ (which producing $|1\rangle$ and $|-\rangle$) is odd. Remember that the $|1\rangle$ and $|-\rangle$ which are unchanged is odd, then after encrypted by Alice, the total number of $|1\rangle$ and $|-\rangle$ will be even. Given s which is randomly selected, because of the way F is generated, the randomness of k can be ensured. The analysis when the message is 1 is similar. Then we can write the states of ciphertext when the message is b to be:

$$\rho_b = \frac{1}{2^{2n-1}} \sum_{P(i)=b,j} |\psi_{i_1 j_1}\rangle\langle\psi_{i_1 j_1}| \cdots |\psi_{i_n j_n}\rangle\langle\psi_{i_n j_n}|, \tag{9}$$

where $|\psi_{ij}\rangle \equiv H^j X^i |0\rangle$.

Now we calculate the trace distance between ρ_0 and ρ_1 using the method in [23]. Define two trace-preserving quantum operations $\mathcal{E}_1$ and $\mathcal{E}_2$, for any n-bit quantum state ρ

$$\mathcal{E}_1(\rho) = U_{\frac{\pi}{4}}^{\otimes n} \rho U_{\frac{\pi}{4}}^{\otimes n \dagger}, \tag{10}$$

and

$$\mathcal{E}_2(\rho) = \frac{1}{2^n} \sum_{k \in \{0,1\}^n} H_k \rho H_k^{\dagger}. \tag{11}$$

Here $U_{\frac{\pi}{4}} = \mathrm{e}^{-\mathrm{i}\frac{\pi}{4}\mathrm{Y}} = \frac{\sqrt{2}}{2}\left[\begin{array}{cc} 1 & -1 \\ 1 & 1 \end{array}\right]$, which rotates each qubit of ρ around y axis by an angle of $\pi/2$:

$$\begin{array}{rcl} U_{\frac{\pi}{4}}|0\rangle & \rightarrow & |+\rangle, \\ U_{\frac{\pi}{4}}|1\rangle & \rightarrow & -|-\rangle, \\ U_{\frac{\pi}{4}}|+\rangle & \rightarrow & |1\rangle, \\ U_{\frac{\pi}{4}}|-\rangle & \rightarrow & |0\rangle. \end{array} \tag{12}$$

Define

$$\sigma_0 = \frac{1}{2^{n-1}} \sum_{P(j)=0} |\phi_{j_1}\rangle\langle\phi_{j_1}| \cdots |\phi_{j_n}\rangle\langle\phi_{j_n}|, \tag{13}$$

where $|\phi_j\rangle = H^j|0\rangle$.

We can see

$$\begin{array}{rl} & \mathcal{E}_2 \circ \mathcal{E}_1(\sigma_0) \\ = & \mathcal{E}_2(U_{\frac{\pi}{4}}^{\otimes n} \sigma_0 U_{\frac{\pi}{4}}^{\otimes n \dagger}) \\ = & \frac{1}{2^n} \sum_k H_k (U_{\frac{\pi}{4}}^{\otimes n} \sigma_0 U_{\frac{\pi}{4}}^{\otimes n \dagger}) H_k^{\dagger}. \end{array} \tag{14}$$

Because

$$H^i U_{\frac{\pi}{4}}|0\rangle = \left\{ \begin{array}{ll} |+\rangle & (i=0) \\ |0\rangle & (i=1) \end{array} \right.$$

$$H^i U_{\frac{\pi}{4}}|+\rangle = \left\{ \begin{array}{ll} |1\rangle & (i=0) \\ |-\rangle & (i=1) \end{array} \right.$$

then

$$\begin{aligned} & \mathcal{E}_2 \circ \mathcal{E}_1(\sigma_0) \\ = \quad & \frac{1}{2^{2n-1}} \sum_{P(i)=0,j} |\psi_{i_1 j_1}\rangle\langle\psi_{i_1 j_1}| \cdots |\psi_{i_n j_n}\rangle\langle\psi_{i_n j_n}|. \end{aligned} \tag{15}$$

That means

$$\mathcal{E}_2 \circ \mathcal{E}_1(\sigma_0) = \rho_0. \tag{16}$$

And similarly we define

$$\sigma_1 = \frac{1}{2^{n-1}} \sum_{P(j)=1} |\phi_{j_1}\rangle\langle\phi_{j_1}| \cdots |\phi_{j_n}\rangle\langle\phi_{j_n}|. \tag{17}$$

We can get

$$\mathcal{E}_2 \circ \mathcal{E}_1(\sigma_1) = \rho_1. \tag{18}$$

As trace-preserving quantum operations are contractive [24], we get

$$D(\rho_0, \rho_1) \leq D(\sigma_0, \sigma_1). \tag{19}$$

$D(\sigma_0, \sigma_1)$ is easy to compute. By Mathematical induction, we have

$$\begin{aligned} \sigma_0 - \sigma_1 &= \frac{1}{2^{n-1}} (|0\rangle\langle 0| - |+\rangle\langle +|)^{\otimes n} \\ &= \frac{1}{2^{n-1}} \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{bmatrix}^{\otimes n}. \end{aligned} \tag{20}$$

Then

$$\begin{aligned} D(\sigma_0, \sigma_1) &= \frac{1}{2} \cdot \mathrm{tr}\, |\sigma_0 - \sigma_1| \\ &= \frac{1}{2^n} \mathrm{tr} \left| \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{bmatrix}^{\otimes \mathrm{n}} \right|, \end{aligned}$$

here $|A|$ is the singular value matrix of matrix A, $|A| = \sqrt{A^\dagger A}$. By spectral decomposition, we have the following conclusion for normal matrices A_1 and A_2:

$$\mathrm{tr}|\mathrm{A}_1 \otimes \mathrm{A}_2| = \mathrm{tr}|\mathrm{A}_1| \cdot \mathrm{tr}|\mathrm{A}_2|, \tag{21}$$

we then have

$$
\begin{aligned}
D(\sigma_0, \sigma_1) &= \frac{1}{2^n}\left(\mathrm{tr}\left|\left[\begin{array}{cc} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & -\frac{1}{2} \end{array}\right]\right|\right)^n \\
&= (\frac{\sqrt{2}}{2})^n. \qquad (22)
\end{aligned}
$$

Finally

$$D(\rho_0, \rho_1) \leq D(\sigma_0, \sigma_1) = (\frac{\sqrt{2}}{2})^n. \qquad (23)$$

In order to against the second kind of attack, the scheme can be amended as follow.

3.3. Second scheme

In the first scheme, half of i is impossible to appear, here we show a enhance scheme that ensures i's randomness.

[**Key generation**] During key generation phase, Bob generates his private and public keys, he can do as follows:

(G1) Generate randomly a multi-output Boolean function $F = (F_1, F_2)$ as his private key, here $F_1 : \{0,1\}^m \to \{0,1\}^n$ and $F_2 : \{0,1\}^m \to \{0,1\}$ is a balanced Boolean function;

(G2) Select randomly $|i\rangle \in \{0,1\}^n$. Then select $s \in \{0,1\}^m$ randomly, and compute $k = F_1(s), p = F_2(s)$. If $p \neq P(i)$, Bob selects s again until $p = P(i)$;

(G3) Apply H_k to $|i\rangle$, and take $(s, H_k|i\rangle)$ as one of his public-key.

[**Encryption**] If Alice wants to send one bit message b to Bob, she should get one of Bob's public keys, and then:

(E1) Select j randomly from Ω_b;

(E2) Alice applies Y_j to $H_k|i\rangle$, and then sends $(s, Y_j H_k|i\rangle)$ to Bob.

[**Decryption**] After Bob receives $(s, Y_j H_k|i\rangle)$ sent by Alice, he should:

(D1) Calculate $(k, P(i)) = F(s)$;

(D2) Apply H_k to $Y_j H_k|i\rangle$, and measures it in the basis $\{|0\rangle, |1\rangle\}^n$.

F can be generated efficiently by the similar local coin tossing algorithm in 3.1. In addition, to ensure the randomness of i, the set $\mathcal{F}$ made of F_2 should satisfy that: for any $f \in \mathcal{F}$, $f + 1 \in \mathcal{F}$. To achieve this property, we only need to add one extra coin tossing for determining whether add an extra "1" to F_2. Furthermore, for a fixed s, the probability of i distributes evenly to the adversary.

Let $\mathrm{P}(i) = P(i)$ is the parity bit of i. The state after applying H_k to $Y_j H_k|i\rangle$ is $(-1)^{j\cdot(i\oplus k)+W_H(j)/2}|i \oplus j\rangle$. Thus, after measuring $H_k Y_j H_k|i\rangle$, Bob gets $|i\oplus j\rangle$. If $\mathrm{P}(i) = 0$, the parity of $W_H(j)$ is equal to the parity of $W_H(i\oplus j)$; if $\mathrm{P}(i) = 1$, the parity of $W_H(j)$ is opposite to the parity of $W_H(i \oplus j)$. Then the message (0 or 1) is obtained from the parity of $W_H(j)$.

3.4. Security analysis

For the attack to plaintext, the adversary cannot get any information of it from the ciphertext. Let the ciphertexts for a fixed s and b is $\rho_b(s)$, first we divide $\mathcal{F}$ into two part: $\mathcal{F}_s^0$ and $\mathcal{F}_s^1$, they satisfy that

$$\mathcal{F}_s^0 = \{f \in \mathcal{F} | f(s) = 0\},$$

and

$$\mathcal{F}_s^1 = \{f \in \mathcal{F} | f(s) = 1\}. \tag{24}$$

Then we get $|\mathcal{F}_s^0| = |\mathcal{F}_s^1| = \frac{|\mathcal{F}|}{2}$, and

$$\rho_b = \sum_{P(j)=b} p_j Y_j \left[\sum_{F_1,F_2} \sum_i p_{F_1} p_i p_{F_2|i} H_{F_1(s)} |i\rangle\langle i| H_{F_1(s)} \right] Y_j. \tag{25}$$

Here $p_j = \frac{1}{2^{n-1}}$, $p_{F_1} = \frac{1}{|\{F_1\}|}$, $p_i = \frac{1}{2^n}$ and $p_{F_2|i}$ is conditional probability of F_2 while i and s is fixed,

$$p_{F_2|i} = \begin{cases} 0 & (F_2 \in \mathcal{F}_s^b) \\ \frac{2}{|\mathcal{F}|} & (F_2 \in \mathcal{F}_s^{\bar{b}}). \end{cases} \tag{26}$$

Thus we have: $\sum_{F_2} p_{F_2|i} = 1$ and

$$\rho_b = \sum_{P(j)=b} p_j Y_j \sum_{F_1} \sum_i \left[p_{F_1} p_i H_{F_1(s)} |i\rangle\langle i| H_{F_1(s)} \sum_{F_2} p_{F_2|i} \right] Y_j = \frac{I}{2^n}, \tag{27}$$

so

$$D(\rho_0, \rho_1) = 0. \tag{28}$$

Denote

$$\rho_{F,s,b} = \sum_{P(j)=b} \sum_i p_j p_{i|F_2} Y_j \left[H_{F_1(s)} \left(|i\rangle\langle i| \right) H_{F_1(s)} \right] Y_j,$$

$$p_{i|F_2} = \begin{cases} 0 & (P(i) \neq F_2(s)) \\ \frac{1}{2^{n-1}} & (P(i) = F_2(s)). \end{cases} \tag{29}$$

when this scheme is used to encrypt t bits, the ciphertext for the bit-string can be written as

$$\sum_F \left(\rho_{F,s_1,b_1} \otimes \cdots \otimes \rho_{F,s_t,b_t} \right). \tag{30}$$

Thus the security is depend on this trace distance:

$$D\left(\sum_F \left(\rho_{F,s_1,b_1} \otimes \cdots \otimes \rho_{F,s_t,b_t} \right), \sum_F \left(\rho_{F,s_1,b'_1} \otimes \cdots \otimes \rho_{F,s_t,b'_t} \right) \right). \tag{31}$$

Even the Eq. 28 hold, this does not mean the scheme is information-theoretic secure for one-bit oriented encryption. In practical attack, the adversary may own some public keys as extra information, the density operator of public key is: $\sum_F \tau_{F,s}$, here

$$\tau_{F,s} = H_{F_1(s)} \sum_i (p_{i|F_2} |i\rangle\langle i|) H_{F_1(s)}. \tag{32}$$

so the trace distance for different one-bit ciphertexts is:

$$D\left(\sum_F (\rho_{F,s_0,0} \otimes \tau_{F,s_1} \otimes \cdots \otimes \tau_{F,s_t}), \sum_F (\rho_{F,s_0,1} \otimes \tau_{F,s_1} \otimes \cdots \otimes \tau_{F,s_t}) \right). \tag{33}$$

The trace distance for different m-bits string ciphertexts should be

$$D\left(\sum_F (\rho_{F,\vec{s},\vec{b}} \otimes \tau_{F,\vec{s'}}), \sum_F (\rho_{F,\vec{s},\vec{b'}} \otimes \tau_{F,\vec{s'}}) \right), \tag{34}$$

where

$$\rho_{F,\vec{s},\vec{b}} = \rho_{F,s_1,b_1} \otimes \cdots \otimes \rho_{F,s_t,b_t}, \tag{35}$$

$$\tau_{F,\vec{s'}} = \tau_{F,s'_1} \otimes \cdots \otimes \tau_{F,s'_t}. \tag{36}$$

Thus if we want to prove the scheme is information-theoretic secure, it follows that Eqs. (33)(34) are exponential small according to [20].

3.5. Discussion on quantum OWT

To do the OWT from message b to state $\mathcal{E}_b(\rho_0^{(n)}(F(s),i))$, one usually does unitary operation depending on b on the public key $\rho_0^{(n)}(F(s),i)$, then discard the extra outputs and get $\mathcal{E}_m(\rho_0^{(n)}(F(s),i))$. One cannot obtain the original state without the extra outputs. If one has done many operations on $\rho_0^{(n)}(F(s),i)$, he cannot get the original state even with the extra outputs, because he does not know the corresponding state of extra outputs for the certain operation.

Consider the unitary transformation $U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$. $|x\rangle$ is the input qubit, and $|y\rangle$ is auxiliary qubit. For the initial state $\sum_{x_i} \alpha_{x_i}|x_i\rangle|0\rangle$, the output is

$$U_f(\sum_{x_i} \alpha_{x_i}|x_i\rangle|0\rangle) = \sum_{x_i} \alpha_{x_i}|x_i\rangle|f(x_i)\rangle. \tag{37}$$

People with trapdoor information $|x_i\rangle$ can do the following operation

$$U_{f^{-1}}|x_i\rangle|f(x_i)\rangle = |0\rangle|f(x_i)\rangle. \tag{38}$$

For people without trapdoor information $|x_i\rangle$, he can only do as

$$U_f(|x_i\rangle|f(x_j)\rangle) = |x_i\rangle|f(x_j) \oplus f(x_i)\rangle. \tag{39}$$

If $d_H(f(x_i), f(x_j)) = 0$, $|f(x_j) \oplus f(x_i)\rangle = |0\rangle$, then the input for $f(x_j)$ is obtained, here d_H is the Hamming distance. Consider the probability when $d_H(f(x_i), f(x_j)) = 0$ is valid. For a given $f(x_j)$, the probability is $(\frac{1}{2})^n$. Then according to Eq. (3), it is a one-way transformation.

4. Extend to multi-bit-oriented schemes

The scheme in Sec. 3 is one-bit-oriented. We now extend it to multi-bit-oriented schemes. In the following scheme of multi-bit message, the OWT is to map the classical message j to an unknown state

$$\rho_j = Y_j \left[\sum_F H_{F(s)} \left(\sum_i p_{iF} |i\rangle\langle i| \right) H_{F(s)} \right] Y_j.$$

The trapdoor information is the basis $k = F(s)$ on which the quantum states are encoded. The private key is a Boolean function F. Using a part of the public-key s, the owner of private-key can get the trapdoor information k by $k = F(s)$.

4.1. First scheme

[**Key generation**] During this phase, Bob can do as follows:

(G1) Select randomly a multi-output Boolean function $F : \{0,1\}^m \to \{0,1\}^n$ as his private key;
(G2) Select randomly $s_1, s_2 \in \{0,1\}^m$, and compute $k = F(s_1)$, $i = F(s_2)$;
(G3) Apply H_k to $|i\rangle$, and take $(s_1, s_2, H_k|i\rangle)$ as his public key.

[**Encryption**] If Alice wants to send n-bit message j to Bob, she should get one of Bob's public keys, and then:

(E1) Apply Y_j to $H_k|i\rangle$, and then sends $(s_1, s_2, Y_j H_k|i\rangle)$ to Bob.

[**Decryption**] After Bob receives $|\psi_{s_1}\rangle \otimes |\psi_{s_2}\rangle \otimes Y_j H_k|i\rangle$ sent by Alice, he should:

(D1) Calculate $k = F(s_1)$, $i = F(s_2)$;
(D2) Apply H_k to $Y_j H_k|i\rangle$, and measure on the basis $\{|0\rangle, |1\rangle\}^n$.

4.2. Second scheme

[**Key generation**]

(G1) Select randomly two multi-output Boolean function $F_1 : \{0,1\}^n \to \{0,1\}^n$, $F_2 : \{0,1\}^n \to \{0,1\}^n$ as his private key;
(G2) Select randomly $s \in \{0,1\}^m$, and compute $k = F_1(s)$, $i = F_2(s)$;
(G3) Apply H_k to $|i\rangle$, and and take $(s, H_k|i\rangle)$ as his one public-key.

[Encryption] If Alice wants to send n-bit message j to Bob, she should get one of Bob's public keys, and then:

(E1) Apply Y_j to $H_k|i\rangle$, and then sends $(s, Y_jH_k|i\rangle)$ to Bob.

[Decryption] After Bob receives $(s, Y_jH_k|i\rangle)$ sent by Alice, he should:

(D1) Calculate $k = F_1(s)$, $i = F_2(s)$;

(D2) Apply H_k to $Y_jH_k|i\rangle$, and measure on the basis $\{|0\rangle, |1\rangle\}^n$.

4.3. Security analysis for both schemes

In the two multi-bit-oriented schemes described above, Bob can get the message via measuring the result. The state after applying H_k to $Y_jH_k|i\rangle$ is $(-1)^{j\cdot(i\oplus k)+W_H(j)/2}|i \oplus j\rangle$, thus, after measuring $H_kY_jH_k|i\rangle$, Bob gets $|i \oplus j\rangle$. Because Bob can get the exact value of i, he can get the message j finally.

The adversary has also two ways to attack these two schemes. One is to attack the private key via getting information of k; another is to attack plaintext via distinguishing the two ciphertexts. For the first method, similar to the analysis in Sec. 3.4, $H_k|i\rangle$ for k and k' ($k \neq k'$) are $\rho_k = \frac{1}{2^n}\sum_{i\in\{0,1\}^n} H_k|i\rangle\langle i|H_k^\dagger$ and $\rho_{k'} = \frac{1}{2^n}\sum_{i\in\{0,1\}^n} H_{k'}|i\rangle\langle i|H_{k'}^\dagger$, respectively. We can get $\rho_k = \rho_{k'} = I/2^n$, then $D(\mathcal{E}(\rho_k), \mathcal{E}(\rho_{k'})) \leq D(\rho_k, \rho_{k'}) = 0$. Thus no quantum algorithm can distinguish the two quantum states ρ_k and $\rho_{k'}$, the two states are indistinguishable.

For the second way, we can prove that the adversary cannot get any information of the plaintext from the ciphertext. Let the message be j, the ciphertext is

$$\rho_j = Y_j \left[\sum_F H_{F(s)} \left(\sum_i p_{iF}|i\rangle\langle i|\right) H_{F(s)}\right] Y_j = I/2^n. \tag{40}$$

Then for any j and $j'(j \neq j')$, $D(\rho_j, \rho_{j'}) = 0$. Thus $D(\mathcal{E}(\rho_j), \mathcal{E}(\rho_{j'})) \leq D(\rho_j, \rho_{j'}) = 0$. No quantum algorithm can distinguish the two ciphertext. According to [20], this scheme is information-theoretic secure.

5. Enhanced scheme

In the schemes given above, though $H_k|i\rangle$ is unknown to the adversary, he can point out whether each private key is different since s is obvious, so it generally requires that the same public-key should not be reused. Here we show a method to solve this problem, enhance the scheme in Sec. 3.3 for example:

[**Key generation**] During key generation phase, Bob generates his private and public keys, he can do as follows:

(G1) Generate a multi-output Boolean function $F : \{0,1\}^m \to \{0,1\}^{n+1}$ randomly, then select randomly $l \in \{0,1\}^m$. Take (F,l) as his private key;

(G2) Select randomly $|i\rangle \in \{0,1\}^n$. Then select $s \in \{0,1\}^m$ randomly, and compute $(k,p) = F(s)$. If $p \neq P(i)$, Bob selects s again until $p = P(i)$;

(G3) Calculate $|\psi_s\rangle = |s_1\rangle_{l_1} \otimes |s_2\rangle_{l_2} \otimes \cdots \otimes |s_m\rangle_{l_m}$;

(G4) Apply H_k to $|i\rangle$, and take $|\psi_s\rangle \otimes H_k|i\rangle$ as his one public-key.

[**Encryption**] If Alice wants to send one bit message b to Bob, she should get one of Bob's public keys, and then:

(E1) Select j randomly from Ω_b;

(E2) Alice applies $I \otimes Y_j$ to $|\psi_s\rangle \otimes H_k|i\rangle$, and then sends $|\psi_s\rangle \otimes Y_j H_k|i\rangle$ to Bob.

[**Decryption**] After Bob receives $|\psi_s\rangle \otimes Y_j H_k|i\rangle$ sent by Alice, he should:

(D1) Calculate from $|\psi_s\rangle$ and l to get s;

(D2) Calculate $(k, P(i)) = F(s)$;

(D3) Apply H_k to $Y_j H_k|i\rangle$, and measures it in the basis $\{|0\rangle, |1\rangle\}^n$.

This method is also useful for our other schemes. It can be seen that, if we use $(s, H_k|i\rangle)$ as public key, for the same s, k is also the same for one-bit-oriented schemes, and i is also the same for multi-bit-oriented schemes. Then there may exist many copies of the same $(s, H_k|i\rangle)$, the adversary may obtain information of F with these copies. While we use $|\psi_s\rangle \otimes H_k|i\rangle$ as the public key, the adversary cannot get s directly, then he cannot get information of F even as s are reused.

6. Public-key encryption scheme based on a special entanglement state[19]

In [19] we present a public-key encryption scheme based on a special entanglement state, we prove that the scheme is secure under the attack to plaintext, since the ciphertexts encrypted from different plaintexts are indistinguishable. Here we first complete the proof for Theorem 6 in [19], which is related to the attack to plaintext with ciphertext. Then we will give a way to attack the private key by the public key.

Let $\Omega_n = \{k \in Z_{2^n} | W_H(k) \ is \ odd\}$ and $\Pi_n = \{k \in Z_{2^n} | W_H(k) \ is \ even\}$, where $W_H(k)$ is k's Hamming weight. Let a Boolean Function $F : \Omega_n \to \Omega_n$ be the private key. For a randomly chosen s, $(s, \rho^0_{k,i})$ is the public key satisfies that $k = F(s)$ and

$$\rho^0_{k,i} = \frac{1}{2}(|i\rangle + |i \oplus k\rangle)(\langle i| + \langle i \oplus k|), \tag{41}$$

as the same as that of [19].

Then the density operator of ciphertext for $b = 0$ is $\frac{1}{2^{n-1}} \sum_k \rho^0_k$ for the adversary:

$$\rho^0_k = \frac{1}{2 \cdot 2^n} \sum_i 2(|i\rangle\langle i| + |i\rangle\langle i \oplus k|) = \frac{1}{2^n} \sum_i \sum_x |i\rangle\langle i \oplus xk|, \tag{42}$$

where $x \in \{0, 1\}$.

In order to analysis the attack to the plaintext, we should calculate the trace distance between ciphertexts encrypted from different plaintexts:

$$\| \frac{1}{2^{n-1}} \sum_k ((\rho^0_k - \rho^1_k) \otimes (\rho^0_k)^{\otimes t-1}) \|_{\mathrm{tr}},$$

here the first part of the summation $(\rho^0_k - \rho^1_k)$ represent the difference between ciphertexts, and the latter part $(\rho^0_k)^{\otimes t}$ represent the extra $t - 1$ public keys that the adversary would own.

First we give the the trace distance between $\frac{1}{2^{n-1}} \sum_k (\rho^0_k)^{\otimes t}$ and $(\frac{I}{2^n})^{\otimes} t$:

$$\begin{aligned} & \| \frac{1}{2^{n-1}} \sum_k (\rho^0_k)^{\otimes t} - (\frac{I}{2^n})^{\otimes} t \|_{\mathrm{tr}} \\ = & \frac{1}{2^{n-1} 2^{nt}} \| \sum_k \sum_i (\sum_x |i\rangle\langle i \oplus xk| - |i\rangle\langle i|) \|_{\mathrm{tr}} \\ = & \frac{1}{2^{n-1} 2^{nt}} \| \sum_k \sum_i \sum_{x \neq (0 \cdots 0)} |i\rangle\langle i \oplus xk| \|_{\mathrm{tr}} . \end{aligned} \tag{43}$$

Let $A = \sum_k \sum_i \sum_{x \neq (0 \cdots 0)} |i\rangle\langle i \oplus xk|$, it has a polar decomposition $A =$

$|A|V$, then $|\mathrm{tr}(AV^\dagger)| = |\mathrm{tr}|A|| = \mathrm{tr}|A|$, so the eq. (43) is equal to:

$$\begin{aligned}
& \frac{1}{2^n 2^{nt}} |tr(\sum_k \sum_i \sum_{x\neq(0\cdots 0)} |i\rangle\langle i\oplus xk|V^\dagger)| \\
= & \frac{1}{2^n 2^{nt}} |\sum_i (\sum_k \sum_{x\neq(0\cdots 0)} (\langle i\oplus xk|)V^\dagger|i\rangle)| \\
\leq & \frac{1}{2^n 2^{nt}} \sum_i (\| V^\dagger|i\rangle \| \cdot \| \sum_k \sum_{x\neq(0\cdots 0)} \langle i\oplus xk| \|) \\
\leq & \frac{1}{2^n 2^{nt}} \cdot 2^{nt} \cdot \sqrt{2^{n-1}(2^t-1)} < \sqrt{\frac{1}{2^{n-t+1}}}. \qquad (44)
\end{aligned}$$

Similarly, we can get

$$\| \frac{1}{2^{n-1}} \sum_k (\rho_k^1 \otimes (\rho_k^0)^{\otimes t-1} - (\frac{I}{2^n})^{\otimes t}) \|_{\mathrm{tr}} < \sqrt{\frac{1}{2^{n-t+1}}}. \qquad (45)$$

Then we have

$$\begin{aligned}
& \| \frac{1}{2^{n-1}} \sum_k ((\rho_k^0 - \rho_k^1) \otimes (\rho_k^0)^{\otimes t-1}) \|_{\mathrm{tr}} \\
\leq & \| \frac{1}{2^{n-1}} \sum_k (\rho_k^1 \otimes (\rho_k^0)^{\otimes t-1} - (\frac{I}{2^n})^{\otimes t}) \|_{\mathrm{tr}} + \| \frac{1}{2^{n-1}} \sum_k (\rho_k^0)^{\otimes t} - (\frac{I}{2^n})^{\otimes} t \|_{\mathrm{tr}} \\
= & \sqrt{\frac{1}{2^{n-t-1}}}. \qquad (46)
\end{aligned}$$

Thus the proof complete.

We will show a way to attack the private key by the public key. While the attacker gets a public key $(s, \rho_{k,i}^0)$, he can attack by taking a unitary operation as follow:

$$\begin{aligned}
H^n \frac{1}{\sqrt{2}}(|i\rangle + |i\oplus k\rangle) &= \frac{1}{\sqrt{2^{n+1}}} \sum_y \big((-1)^{y\cdot i}|y\rangle + (-1)^{y\cdot(i\oplus k)}|y\rangle\big) \\
&= \frac{1}{\sqrt{2^{n+1}}} \sum_y (-1)^{y\cdot i}(1+(-1)^{y\cdot k})|y\rangle. \qquad (47)
\end{aligned}$$

Then he measures the last state, if he gets a result called y_0, it must satisfy $y_0 \cdot k = 0$, thus he get a equation of F that:

$$F(S) \cdot y_0 = 0, \tag{48}$$

which contains on bit information of F.

F is also built by $n^2 \cdot p(n)$ variables:

$$F(s_1, \cdots, s_n) = (F^1(s), \cdots, F^n(s)),$$

where

$$F^j(s) = (s_1^{a_{j11}} \cdots s_n^{a_{j1n}}) \oplus (s_1^{a_{j21}} \cdots s_n^{a_{j2n}}) \oplus \cdots \oplus (s_1^{a_{jp(n)1}} \cdots s_n^{a_{jp(n)n}}),$$

each $a_{jkl} = G(1)$ is a result of a toss. Since $x^a = xa \oplus a \oplus 1$, There is a linear expression of F:

$$F^j(s) = \bigoplus_{\alpha=1}^{p(n)} \left(\prod_{\beta=1}^{n} (s_\beta a_{j\alpha\beta} + a_{j\alpha\beta} + 1) \right). \tag{49}$$

The scheme should be only called bounded information secure similar to the scheme in [9, 21].

According to the schemes based on conjugate coding, it is secure under the attack to the private key, since that the attack to the private key is equivalent to the attack to the basis of an unknown state, we have already proved that if this attack can be achieved it will lead to a Superluminal communication[20].

7. Discussions

Every classical public-key scheme, such as RSA [1], is insecure under man-in-the-middle (MIM) attack. If the adversary can intercept Bob's public key distribution channel, she can replace Bob's public-key (n, e) with her own public key (n', e'), and send it to Alice. While Alice encrypts her message with (n', e') and sends the ciphertext back to Bob, the adversary may decrypt the ciphertext to get the message. Finally the adversary encrypts the message with (n, e), and sends this ciphertext to Bob. We can see that nobody will be aware of the exist of the adversary. It is clear that for the design of a public-key encryption scheme, it is necessary to provide that Alice can obtain the public-key of Bob securely. Actually, this precondition is necessary for all classical and quautum public-key encryption protocols. To resist the MIM attack is the task of, such as public-key infrastructure (PKI).

A common feature of the scheme in [13] and our bit-oriented scheme is: an n-qubit public key is needed to encrypt a one-bit message. The difference is, in the scheme of [13], for different messages, the public keys are the same; however, in our schemes, the public keys are different for every time of encryption, as a result of choosing different s and $|i\rangle$ at each time of key generation. The security of our schemes is highly improved, while we can see that the resources needed to store the quantum public keys are kept the same.

In symmetric cryptography, one-time pad is information-theoretically secure. In asymmetric cryptography, the schemes presented here can reach bounded information-theoretic security, and the different keys used at different time are public keys rather than private keys. However, in classical asymmetric cryptography, even if we use different public keys for every time of encryption, information-theoretic security still cannot be reached. For example, in the RSA scheme, if a different public key is used every new time of encryption, the private key changes accordingly. Then only two ciphertexts are needed to get the plaintext, and it is not secure.

8. Conclusion

We propose several QPKE schemes of classical messages based on conjugate coding, and prove that some of them are bounded information-theoretic secure. We also discuss a scheme we presented in [19] based on the state $|i\rangle + |i \oplus k\rangle$ and give a way to attack it. These schemes include scheme present in [9] are all bounded information-theoretic secure, but the schemes based on conjugate coding seem to be more secure than those in [9, 19] as their public key's reuse times is limit to the number of bits of the private key. From a practical point of view, our schemes based on single-photon string may be realized in near future.

Acknowledgement

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

References

[1] R. L. Rivest, A. Shamir, and L. A. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Commun. ACM* **21**, pp. 120–126, 1978.

[2] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", *IEEE Trans. Inf. Theory* **31**, pp. 469–471, 1985.

[3] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, S. Goldwasser, ed., pp. 124–134, 1994.

[4] C. H. Bennett and G. Brassard," Quantum cryptography: Public-key distribution and coin tossing", in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York),1984.

[5] G. L. Long and X. S. Liu, " Theoretically efficient high-capacity quantum-key-distribution scheme", *Phys. Rev. A*, **65**, p. 032302, 2002.

[6] W. Chen, Z. F. Han, X. F. Mo, F. X. Xu, G. Wei and G. C. Guo,"Active phase compensation of quantum key distribution system", *Chinese Science Bulletin*,**53**, pp. 1310-1314, 2008.

[7] H. Lu and Q. Y. Cai,"Quantum key distribution with classical Alice",*International Journal of Quantum Information*,**6**, pp. 1195-1202, 2008.

[8] G. Q. He, H. B. Guo, Y. D. Li, S. W. Zhu and G. H. Zeng,"Quantum key distribution using binary-modulated coherent states", *Acta Physica Sinica*,**57**, p.2217, 2008.

[9] T. Okamoto, K. Tanaka, and S. Uchiyama, "Quantum Public-key Cryptosystemns", in *Advances in Cryptology: Crypto 2000 Proceedings*, LNCS, M. Bellare, ed., **1880**, pp. 147–165, 2000.

[10] D. Gottesman, "Quantum Public Key Cryptography with Information-Theoretic Security", See: http://www.perimeterinstitute.ca/personal/dgottesman/Public-key.ppt, 2005.

[11] L. Yang, "Quantum public-key cryptosystem based on classical NP-Complete problem", e-print arXiv: quant-ph/0310076, 2003.

[12] L. Yang, M. Liang, B. Li, L. Hu, and D. G. Feng, "Quantum public-key cryptosystems based on induced trapdoor one-way transformations", e-print arXiv: quant-ph/1012.5249, 2010.

[13] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami, "Computational Indistinguishability between Quantum States and Its Cryptographic Application", in *Advances in Cryptology: Eurocrypt 2005 Proceedings*, LNCS, R. Cramer, ed., **3494**, pp. 268–284, 2005.

[14] A. Kawachi, T. Koshiba, H. Nishimura, and T. Yamakami, "Computational Indistinguishability between Quantum States and Its Cryptographic Application", e-print arXiv: quant-ph/0403069, 2004.

[15] G. M. Nikolopoulos, "Applications of Single-qubit Rotations in Quantum Public-key Cryptography", *Phys. Rev. A.* **77**, p. 032348, 2008.

[16] G. M. Nikolopoulos, "Deterministic quantum-public-key encryption: Forward search attack and randomization", *Phys. Rev. A.* **79**, p. 042327, 2009.

[17] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*,CRC Press, Boca Raton, 1997.

[18] O.Goldreich, *Foundations of Cryptography: Basic Applications*, Publishing House of Electronics Industry, Beijing, 2004.

[19] J. Y. Pan, and L. Yang, "Quantum Public-key Encryption with Information Theoretic Security", e-print arXiv: quant-ph/1006.0354, 2010.

[20] L. Yang, C. Xiang, and B. Li, "Quantum probabilistic encryption protocol based on cojugate coding" *China communications* **10**(2), pp. 19–26, 2013.

[21] M. Hayashi, A. Kawachi, and H. Cobayashi, "Quantum Measurements for Hidden Subgroup Problems with Optimal Sample Complexity", *Quantum Inf. Comput.* **8**, pp. 0345–0358, 2008.

[22] D. R. Stinson, *Cryptography Theory and Practice*,CRC Press, Boca Raton, .

[23] L. Yang, C. Xiang, and B. Li, “Qubit-string-based bit commitment protocols with physical security”, e-print arXiv: quant-ph/1011.5099, 2010.

[24] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information (Cambridge University Press,Cambridge, England), 2000.