Quantum public-key encryption schemes based on conjugate coding

Li Yang1,2 · Biyao Yang1,2,3,4 · Chong Xiang5

Received: 24 April 2020 / Accepted: 22 October 2020 / Published online: 13 November 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
We present several quantum public-key encryption (QPKE) protocols designed using conjugate coding single-photon strings; thus, they may be realized in the laboratory using current techniques. The first two schemes can encrypt one-bit messages; these are then extended to two kinds of QPKE schemes oriented toward multi-bit messages. In these schemes, Boolean functions are used as private keys and classical-quantum pairs as public keys, where one private key corresponds to an exponential number of public keys. Later, we discuss some issues related to authentication and a possible way to improve the security of the proposed schemes in this paper. The novel structure of the protocols presented here ensures that most of them are information-theoretic secure under attacks on the private key and on the encryption, while they can be realized more easily compared to other protocols.

Keywords Quantum cryptography · Quantum public-key encryption · Information-theoretic security · Conjugate coding

Part of this work was presented in a conference proceeding [20].

Biyao Yang
yangbiyao@iie.ac.cn

1 State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2 School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3 Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
4 Beijing Institute of Information Application Technology, Beijing 100044, China
5 China Information Technology Security Evaluation Center, Beijing 100085, China
1 Introduction

Public-key encryption [1,2] is an important branch of modern cryptography. Until now, the security of classical public-key encryption schemes has been based on certain mathematically difficult problems whose difficulty has not been proved. In a quantum computing environment, most of these problems will cease to be difficult [3]; in that case, the related public-key protocols will not be secure.

Therefore, new schemes must be developed to resist the attacks of quantum adversaries. Private key protocols utilizing quantum key distribution (QKD) can be utilized to address such issues [4–8]. Another solution involves the development of quantum public-key encryption (QPKE). Okamoto et al. [9] introduced a public-key encryption scheme with a quantum algorithm in the key generation phase. Gottesman [10] proposed a QPKE protocol based on teleportation with information-theoretic security. Kawachi et al. [11,12] investigated the cryptographic property of the “computational indistinguishability” of two quantum states generated via fully flipped permutations and proposed QPKE schemes based on it. Nikolopoulos constructed a QPKE [13] from the perspective of a single-qubit rotation and trapdoor one-way function and improved the scheme using the parity of an s-bit codeword to encrypt one-bit plaintext to resist forward research attacks [14]. Fujita [15] constructed a McEliece-based QPKE, while Yang et al. [16] proposed another QPKE based on McEliece. Yang and Liang introduced the concept of induced trapdoor one-way quantum function [17] and discussed public-key encryption and authentication of quantum information in [18]. Gao et al. discussed quantum asymmetric cryptography with symmetric keys in [19]. An earlier version [20] of this paper presented some QPKE protocols with information-theoretic security. Wu and Yang proposed a bit-oriented QPKE scheme [21] based on quantum perfect encryption and a QPKE protocol [22] for an unknown multi-qubit state based on qubit-wise teleportation. In [23], a quantum public-key cryptosystem based on Bell states was presented. Wang et al. proposed a practical QPKE model in [24].

The idea of a conjugate code was first introduced by Wiesner [25]. It refers to “any communication scheme in which the physical systems used as signals are placed in states corresponding to elements of several conjugate basis of the Hilbert space describing the individual systems.” Two bases are called “conjugate” [4,25] if each vector of one basis has equal-length projections onto all vectors of the other basis. In this case, a system prepared in a specific state of one basis will behave entirely randomly and lose all its stored information when subjected to measurement corresponding to the other basis. The first quantum public-key protocol BB84 [4] was just based on conjugate coding. In the 1980s, conjugate coding was developed to the world of public-key cryptography as oblivious transfer, first by Rabin [26] and then by Even [27]. Deng and Long proposed a quantum secure direct communication scheme [28] based on conjugate coding. A quantum probabilistic encryption scheme [29] based on conjugate coding was put forward in 2013. These schemes based on conjugate coding can be more easily realized experimentally (such as the implementation of BB84 [30]) compared with others.

In this paper, we propose several QPKE protocols based on conjugate coding which can all be realized with current technology using polarized photons. The first scheme is bit-oriented and can resist attacks on the encryption, while it cannot resist attacks on
the private key. We then improve the scheme to ensure security of both the encryption and the private key. Two secure QPKE schemes oriented toward multi-bit messages are then presented. In these schemes, Boolean functions are used as private keys, and classical-quantum pairs are the public keys.

Most of the QPKE schemes proposed here have two advantages: On the one hand, they can be more easily realized using unentangled photons compared to schemes using entangled photons [21,22]; on the other hand, they can reach information-theoretic security under attacks on the encryption and on the private key compared to computational-secure schemes.

This paper is organized as follows. In Sect. 2, we present two QPKE schemes treating one-bit messages based on conjugate coding. In Sect. 3, we extend the schemes to those oriented toward multi-bit messages. In Sect. 4, we discuss some issues related to authentication and a possible way to improve the security of the proposed schemes in this paper. Some conclusions are reached in Sect. 5.

2 Quantum public-key encryption schemes for one-bit messages

Let \( k = (k_1, \ldots, k_n) \) be an \( n \)-bit string, where \( k_1, \ldots, k_n \in \{0, 1\} \). 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 \( Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \), we define \( Y_k = Y^{k_1} \otimes \cdots \otimes Y^{k_n} \).

### 2.1 First scheme

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

1. Select randomly a multi-output Boolean function \( F : \{0, 1\}^m \rightarrow \{0, 1\}^n \) as his private key;
2. Select randomly \( s \in \{0, 1\}^m \), and compute \( k = F(s) \);
3. Generate \( |i\rangle \) with \( i \in \Omega_0 \);
4. Apply \( H_k \) to \( |i\rangle \), and take the classical-quantum pair \((s, H_k|i\rangle)\) as one of his public keys.

Bob can generate a large amount \((2^n)\) 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.

**[Encryption]** If Alice wants to send a one-bit message \( b \) to Bob, she should get one of Bob’s public keys \((s, H_k|i\rangle)\) and then:

1. Select \( j \) randomly from \( \Omega_b \);
2. Apply \( Y_j \) to \( H_k|i\rangle \), and then send \((s, Y_j H_k|i\rangle)\) to Bob.

**[Decryption]** After receiving the ciphertext, Bob should:

1. Calculate \( k = F(s) \);
2. Apply \( H_k \) to \( Y_j H_k|i\rangle \) and measure it in the basis \( \{|0\rangle, |1\rangle\}^n \).

\( \odot \) Springer
Bob obtains the one-bit message from the parity of the bit string he received. The state after applying $H_k$ to $Y_j H_k |i⟩$ is

$$H_k Y_j H_k |i⟩ = (-1)^{j · Y_j |i⟩} = (-1)^{j · (i ⊕ k) + \frac{1}{2} W_H(j)|i ⊕ j⟩}. \quad (1)$$

Thus, after measuring it, Bob obtains $|i ⊕ j⟩$; here, $⊕$ denotes bit-wise addition modulo 2. The parity of $W_H(j)$ is equal to the parity of $W_H(i ⊕ j)$ because $W_H(i)$ is even. Then, the message (plaintext) is obtained.

### 2.2 Security analysis

The security of the QPKE is now analyzed from two perspectives: (1) Security of the encryption and (2) security of the private key.

#### 2.2.1 Security of the encryption

We first consider the case where the attacker, Eve, acquires two different ciphertexts encrypted by different public keys corresponding to the same private key $F$. The ciphertexts for him can be denoted as

$$\rho_0 = \sum_{P(j) = 0} Y_j \left[ \sum_F H_{F(s)} \left( \sum_{P(i) = 0} p_{ij} F |i⟩⟨i| \right) H_{F(s)} \right] Y_j$$

$$= \frac{1}{2^{5n-2}} \sum_k H_k \left( \sum_{P(i) = 0} \sum_{P(j) = 0} Y_j |i⟩⟨i| Y_j \right) H_k,$$

$$\rho_1 = \sum_{P(j) = 1} Y_j \left[ \sum_F H_{F(s)} \left( \sum_{P(i) = 0} p_{ij} F |i⟩⟨i| \right) H_{F(s)} \right] Y_j$$

$$= \frac{1}{2^{5n-2}} \sum_k H_k \left( \sum_{P(i) = 0} \sum_{P(j) = 1} Y_j |i⟩⟨i| Y_j \right) H_k. \quad (2)$$

Here, the results are obtained under the condition including that the output of $F$ is uniformly distributed. Similar to that in [29], the definition of information-theoretic quantum ciphertext indistinguishability under chosen plaintext attack (IND-CPA) for QPKE protocols is stated as [31]: A QPKE scheme is information-theoretically quantum ciphertext-indistinguishable if for every quantum circuit family $\{C_n\}$, every positive polynomial $p(·)$, all sufficiently large $n$, and every bit-string $x, y \in \{0, 1\}^*$, the probability $Pr(·)$ satisfies:

$$|Pr[C_n(G(1^n), E_{G(1^n)}(x)) = 1] - Pr[C_n(G(1^n), E_{G(1^n)}(y)) = 1]| < \frac{1}{p(n)}, \quad (3)$$
where $G$ is the key generation algorithm, $E$ is the quantum encryption algorithm, and the ciphertext $E(x), E(y)$ are quantum states. It is also proved [29] that a QPKE scheme is information-theoretically secure if the trace distance between any two ciphertexts is $O\left(\frac{1}{n^2}\right)$. Now, we calculate the trace distance between any two ciphertexts in this one-bit scheme. Since $\sum_k H_k \left( \sum_{P(i)=0} \sum_{P(j)=0} |i \oplus j\rangle \langle i \oplus j| \right) H_k + \sum_k H_k \left( \sum_{P(i)=1} \sum_{P(j)=1} |i \oplus j\rangle \langle i \oplus j| \right) H_k = 2^{n-1} I$, we have

$$D(\rho^0, \rho^1) = \frac{1}{2^{3n-2}} \times$$

$$\times D \left( \sum_k H_k \left( \sum_{P(i)=0} \sum_{P(j)=0} |i \oplus j\rangle \langle i \oplus j| \right) H_k, \sum_k H_k \left( \sum_{P(i)=0} \sum_{P(j)=1} |i \oplus j\rangle \langle i \oplus j| \right) H_k \right)$$

$$= \frac{1}{2^{3n-2}} \cdot 2 \cdot \frac{1}{2} \left| \sum_k H_k 2^{n-1} \left( \sum_{P(i)=0} |i\rangle \langle i| - \frac{1}{2} I \right) H_k \right|$$

$$= \frac{1}{2^{3n-2}} \cdot 2^{n-1} \cdot \frac{1}{2} \cdot 2^{n} \left| \sum_{k_{0,1}} H^{k_1} Z H^{k_1} \otimes \ldots \otimes \sum_{k_{n,1}} H^{k_n} Z H^{k_n} \right|. \quad (4)$$

From spectral decomposition, we obtain $\text{tr}|A_1 \otimes A_2| = \text{tr}|A_1| \cdot \text{tr}|A_2|$ for normal matrices $A_1$ and $A_2$. Then, we have

$$D(\rho^0, \rho^1) = \frac{1}{2^{2n}} \left( \text{tr} \sum_{k=0,1} H^k Z H^k \right)^n = \frac{1}{2^{2n}} (2\sqrt{2})^n = \left( \frac{1}{\sqrt{2}} \right)^n. \quad (5)$$

According to the definition of information-theoretic quantum ciphertext-indistinguishability described above, the attacker cannot distinguish any two ciphertexts encrypted by different public keys corresponding to the same private key because of Eq. (5).

Next, we consider the case where the attacker, Eve, intercepts two ciphertexts corresponding to different private keys. 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 being 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 and 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 produces $|1\rangle$ and $|-\rangle$) is odd. Remember that the $|1\rangle$ and $|-\rangle$ which are unchanged are odd; then, after being encrypted by Alice, the total number of $|1\rangle$ and $|-\rangle$ will be even. The analysis when the message is 1 is similar. Then, we can write the states of ciphertexts when the message is $b$ under the private key $F$ and $F'$ as:
\[ \rho_F^b = \rho_F^{b'} = \frac{1}{2^{n-1}} \sum_{P(i)=b,j} |\psi_{i,j_1}\rangle \langle \psi_{i,j_1}| \cdots |\psi_{i,n}\rangle \langle \psi_{i,n}|, \]  

(6)

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

It can be seen that \( D(\rho_F^b, \rho_F^{b'}) = 0 \). Now, consider \( D(\rho_F^b, \rho_F^{b'})(b \neq b') \), e.g.,

the trace distance between \( \rho_F^0 \) and \( \rho_F^1 \). Define two trace-preserving quantum operations \( \mathcal{E}_1 \) and \( \mathcal{E}_2 \) for any \( n \)-bit quantum state \( \rho \) as \( \mathcal{E}_1(\rho) = U_{\pi/4} \rho U_{\pi/4}^\dagger \), and

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

Here, \( U_{\pi/4} = e^{-i \frac{\pi}{4} Y} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \), which rotates each qubit of \( \rho \) around the y axis by an angle of \( \pi/2 \). Then, define \( \sigma_0 = \frac{1}{2^n} \sum_{P(j)=0} |\phi_{j_1}\rangle \langle \phi_{j_1}| \cdots |\phi_{j_n}\rangle \langle \phi_{j_n}| \), where \( |\phi_j\rangle = H^j |0\rangle \). We can see that \( \mathcal{E}_2 \circ \mathcal{E}_1(\sigma_0) = \mathcal{E}_2( U_{\pi/4}^{\otimes n} \sigma_0 U_{\pi/4}^{\otimes n\dagger} ) = \frac{1}{2^n} \sum_{k} H_k \left( U_{\pi/4}^{\otimes n} \sigma_0 U_{\pi/4}^{\otimes n\dagger} \right) H_k^\dagger \).

Because

\[ H^i U_{\pi/4} |0\rangle = \begin{cases} |+\rangle (i = 0) \\ |0\rangle (i = 1) \end{cases}, \]

\[ H^i U_{\pi/4} |+\rangle = \begin{cases} |1\rangle (i = 0) \\ |-\rangle (i = 1) \end{cases}, \]

\[ \mathcal{E}_2 \circ \mathcal{E}_1(\sigma_0) = \frac{1}{2^n-1} \sum_{P(j)=0,j} |\psi_{i,j_1}\rangle \langle \psi_{i,j_1}| \cdots |\psi_{i,n}\rangle \langle \psi_{i,n}| = \rho_0^0. \]

Similarly, we define \( \sigma_1 = \frac{1}{2^n-1} \sum_{P(j)=1} |\phi_{j_1}\rangle \langle \phi_{j_1}| \cdots |\phi_{j_n}\rangle \langle \phi_{j_n}| \), so we can obtain

\[ \mathcal{E}_2 \circ \mathcal{E}_1(\sigma_1) = \rho_0^1. \]

As trace-preserving quantum operations are contractive \([32]\), we obtain \( D(\rho_F^0, \rho_F^1) \leq D(\sigma_0, \sigma_1) \). By mathematical induction, we have

\[ \sigma^0 - \sigma^1 = \frac{1}{2^{n-1}} (|0\rangle \langle 0| - |+\rangle \langle +|) \otimes n = \frac{1}{2^{n-1}} \left[ \begin{array}{cc} 1 & -1 \\ 1 & 1 \end{array} \right] \otimes n. \]  

(7)

then

\[ D(\sigma^0, \sigma^1) = \frac{1}{2} \cdot \text{tr} |\sigma_0 - \sigma_1| = \frac{1}{2^n} \text{tr} \left[ \left[ \begin{array}{cc} 1 & -1 \\ 1 & 1 \end{array} \right] \right] \otimes n = \left( \frac{\sqrt{2}}{2} \right)^n; \]  

(8)

thus \( D(\rho_F^0, \rho_F^1) \leq D(\sigma^0, \sigma^1) = \left( \frac{\sqrt{2}}{2} \right)^n \). Thus, if the attacker intercepts two different ciphertext states encrypted by public keys corresponding to different private keys, he is unable to distinguish them.

### 2.2.2 Security of the private key

Suppose the attacker, Eve, acquires a user’s public key and then measures it. The public-key state for him is

\[ \rho' = \sum_F \sum_{P(i)=0} p_{i,F} H_{F(s)} |i\rangle \langle i| H_{F(s)}. \]  

(9)
Since half of \( i \) is impossible to see, \( \rho' \) is not a totally mixed state and the scheme cannot resist an attack on the private key. In order to resist this kind of attack, the scheme can be amended as follows, ensuring \( i \)'s randomness.

### 2.3 Improved scheme

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

1. Generate randomly a multi-output Boolean function \( F = (F_1, F_2) \) as his private key. Here, \( F_1 : \{0, 1\}^m \rightarrow \{0, 1\}^n \) and \( F_2 : \{0, 1\}^m \rightarrow \{0, 1\} \) is a balanced Boolean function;
2. Randomly select \(|i⟩ \in \{0, 1\}^n\). Then, select \(|s⟩ \in \{0, 1\}^m\) randomly and compute \( k = F_1(s) \), \( p = F_2(s) \). If \( p \neq F(i) \), Bob selects \( s \) again until \( p = F(i) \);
3. Apply \( H_k \) to \(|i⟩ \) and take \((s, H_k|i⟩)\) as one of his public keys.

**[Encryption]** If Alice wants to send a one-bit message \( b \) to Bob, she should obtain one of Bob’s public keys \((s, H_k|i⟩)\) and then:

1. Select \( j \) randomly from \( Ω_b \);
2. Apply \( Y_j \) to \( H_k|i⟩ \) and then send \((s, Y_j H_k|i⟩)\) to Bob.

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

1. Calculate \((k, P(i)) = F(s)\);
2. Apply \( H_k \) to \( Y_j H_k|i⟩ \) and measure it in the basis \( \{|0⟩, |1⟩\}^n \).

Let \( P(i) \) be the parity bit of \( i \). The state after applying \( H_k \) to \( Y_j H_k|i⟩ \) is \((-1)^{j(i \oplus k) + W_H(j)/2}|i \oplus j⟩\). Thus, after measuring \( H_k Y_j H_k|i⟩ \), Bob obtains \(|i \oplus j⟩\).

If \( P(i) = 0 \), then the parity of \( W_H(j) \) is equal to the parity of \( W_H(i \oplus j) \); if \( P(i) = 1 \), the parity of \( W_H(j) \) is opposite to the parity of \( W_H(i \oplus j) \). Then, the message \((0 \text{ or } 1)\) is obtained from the parity of \( W_H(j) \).

### 2.4 Security analysis

The security of the QPKE is also analyzed from two perspectives: (1) Security of the encryption and (2) security of the private key.

#### 2.4.1 Security of the encryption

We first consider the case where the attacker, Eve, acquires two different ciphertexts encrypted by different public keys corresponding to the same private key \( F \). Let the ciphertexts for plaintext \( b \) be \( ρ^b(s) \). First, we divide \( ℋ \) (the set of \( F_2 \)) into two parts: \( ℋ^0 \) and \( ℋ^1 \), which satisfy \( ℋ^0 = \{f ∈ ℋ|f(s) = 0\} \) and \( ℋ^1 = \{f ∈ ℋ|f(s) = 1\} \).

Then, we obtain \(| ℋ^0_s | = | ℋ^1_s | = | ℋ | / 2 \) and

\[
ρ^b = \sum_{P(j)=b} p_j Y_j \left[ \sum_{F_1 ∼ F_2} \sum_i p_{F_1} p_{F_2} |i⟩⟨i| H_{F_1(s)} H_{F_2(s)} \right] Y_j.
\] (10)
Here, \( p_j = \frac{1}{2^{n-1}} \), \( p_{F_1} = \frac{1}{\left|\{F_1\}\right|} \), \( p_i = \frac{1}{2^n} \) and \( p_{F_2|i} \) is the conditional probability of \( F_2 \), while \( i \) and \( s \) are fixed:

\[
p_{F_2|i} = \begin{cases} 
0 & (F_2 \in \mathcal{F}_b^b) \\
\frac{1}{2^n} & (F_2 \in \mathcal{F}_s^b)
\end{cases}.
\]

(11)

Thus, we have \( \sum_{F_2} p_{F_2|i} = 1 \) and

\[
\rho^b = \sum_{p(j) = b} p_j Y_j \sum_i p_{F_1} p_i |i\rangle \langle i| H_{F_1(s)} \sum_{F_2} p_{F_2|i} \Bigg] Y_j = \frac{I}{2^n},
\]

(12)

so

\[
D(\rho^0, \rho^1) = 0.
\]

(13)

According to the definition of information-theoretic quantum ciphertext indistinguishability in 2.2.1, the attacker cannot distinguish any two ciphertexts encrypted by different public keys corresponding to the same private key because of Eq. (13).

Next, we consider the case where the attacker, Eve, intercepts two ciphertexts corresponding to different private keys. From Eq. (12), we obtain the trace distance between ciphertexts of different private keys \( F \) and \( F' \) as:

\[
D(\rho^b_F, \rho^b_{F'}) = 0.
\]

(14)

Then, if the attacker intercepts two different ciphertext states encrypted by public keys corresponding to different private keys, he is unable to distinguish them.

We now analyze the number of bits encrypted by the same public key in a way similar to [21,33]. In order to do this, we need to calculate the trace distance

\[
\| \sum_F p_F \rho_{F(s)}^0 \otimes (\rho_{F(s)}^{\text{pubk}})^{\otimes t-1} - \sum_F p_F \rho_{F(s)}^1 \otimes (\rho_{F(s)}^{\text{pubk}})^{\otimes t-1} \|_{\text{tr}},
\]

here

\[
\rho_{F(s)}^0 = \sum_{p(j) = 0} p_j Y_j [H_{F_1(s)} \left( \sum_i p_i |i\rangle \langle i| \right) H_{F_1(s)}] Y_j
\]

\[
= \frac{1}{2^{2n-1}} \sum_{p(j) = 0} \sum_i H_{F_1(s)} |i \oplus j\rangle \langle i \oplus j| H_{F_1(s)}
\]

is the ciphertext state for message “0,” and

\[
\rho_{F(s)}^1 = \sum_{p(j) = 1} p_j Y_j [H_{F_1(s)} \left( \sum_i p_i |i\rangle \langle i| \right) H_{F_1(s)}] Y_j
\]
is the ciphertext state for message “1,” while

$$
(\rho_{pubk}^{F(s)})^\otimes t - 1 = \left( \sum_i p_i (H_{F_1(s)}|i\rangle\langle i| H_{F_1(s)}) \right)^\otimes t - 1
$$

refers to the extra \((t - 1)\) public keys the adversary would obtain. For simplicity, we calculate 

\[
\| \sum_F p_F \rho_{0,F}^F \otimes \left( \rho_{pubk}^{F(s)} \right)^{\otimes t - 1} \|_{tr} - \left( \frac{I}{2^n} \right)^{\otimes t} \|_{tr},
\]

and then use the triangle inequality.

Let \( A = \sum_k \sum_{l \neq l'} |l\rangle\langle l'| \), which has a polar decomposition \( A = |A| V \), then \( \text{tr}|A| = \|\text{tr}|A|\| = \|\text{tr}(AV^\dagger)\| \), so the above equation can be written as:

\[
\frac{1}{2^n 2nt} |\text{tr} \left( \sum_k \sum_{l \neq l'} H_k |l\rangle\langle l'| V^\dagger H_k \right) | = \frac{1}{2^n 2nt} \left| \sum_{l \neq l'} \left( \sum_k \langle l'| H_k V^\dagger H_k |l\rangle \right) \right|
\]
\[
\leq \frac{1}{2^n 2^{nt}} \sum_{l,k} \| H_k V^* H_k |l \rangle \| \| \sum_{l'} |l' \rangle \|
\]

\[
< \sqrt{\frac{1}{2^{n-t+1}}}
\]

(15)

Similarly, we can obtain

\[
\| \sum_F p_F \rho_{F(s)}^1 \otimes \left( \rho_{F(s)}^{\text{pubk}} \right)^{\otimes t-1} - \left( \frac{I}{2^n} \right)^{\otimes t} \|_{\text{tr}} < \sqrt{\frac{1}{2^{n-t+1}}};
\]

then we have:

\[
\| \sum_F p_F \rho_{F(s)}^0 \otimes \left( \rho_{F(s)}^{\text{pubk}} \right)^{\otimes t-1} - \sum_F p_F \rho_{F(s)}^1 \otimes \left( \rho_{F(s)}^{\text{pubk}} \right)^{\otimes t-1} \|_{\text{tr}}
\]

\[
\leq \| \sum_F p_F \rho_{F(s)}^0 \otimes \left( \rho_{F(s)}^{\text{pubk}} \right)^{\otimes t-1} - \left( \frac{I}{2^n} \right)^{\otimes t} \|_{\text{tr}}
\]

\[
+ \| \sum_F p_F \rho_{F(s)}^1 \otimes \left( \rho_{F(s)}^{\text{pubk}} \right)^{\otimes t-1} - \left( \frac{I}{2^n} \right)^{\otimes t} \|_{\text{tr}}
\]

\[
< \sqrt{\frac{1}{2^{n-t-1}}}
\]

(16)

If we want

\[
\| \sum_F p_F \rho_{F(s)}^0 \otimes \left( \rho_{F(s)}^{\text{pubk}} \right)^{\otimes t-1} - \sum_F p_F \rho_{F(s)}^1 \otimes \left( \rho_{F(s)}^{\text{pubk}} \right)^{\otimes t-1} \|_{\text{tr}} < \frac{1}{p(n)},
\]

the lower bound of \( t \) is \( o(n) \), which means that the number of bits encrypted by the same public key is larger than that of the private key.

### 2.4.2 Security of private key

Suppose that the attacker, Eve, acquires a user’s public key and then measures it. The public-key state for him is

\[
\rho' = \sum_{F_2} p_{F_2[i]} \sum_{F_1} \sum_i p_i F_1 H F_1(s) |i \rangle \langle i | H F_1(s). \]

(17)

Under the condition including that the output of \( F_1 \) is uniformly distributed, we obtain

\[
\rho' = \frac{1}{2^{2n}} \sum_k \sum_i H_k |i \rangle \langle i | H_k = \frac{I}{2^n}.
\]

(18)

Then, the quantum part of the public key is a totally mixed state for the attacker, so he cannot obtain any information about the private key. From the view of physics, since an attack on the private key is equivalent to an attack on the basis of an unknown state, we have proved [29] that if this attack can be achieved it will lead to superluminal communication; the scheme is secure under an attack on the private key.
3 Multi-bit-oriented schemes

3.1 First scheme

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

(G1) Randomly select a multi-output Boolean function \( F : \{0, 1\}^m \rightarrow \{0, 1\}^n \) as his private key;
(G2) Randomly select \( s_1, s_2 \in \{0, 1\}^m \) 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 an \( n \)-bit message \( j \) to Bob, then she should obtain one of Bob’s public keys \((s_1, s_2, H_k|i\rangle)\) and then:

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

[Decryption] After Bob receives the \((s_1, s_2, Y_j H_k|i\rangle)\) 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.

3.2 Second scheme

[Key generation]

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

[Encryption] If Alice wants to send an \( n \)-bit message \( j \) to Bob, then she should obtain one of Bob’s public keys \((s, H_k|i\rangle)\) and then:

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

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

(D1) Calculate \( k = F_1(s), i = F_2(s) \);
(D2) Apply \( H_k \) to \( Y_j H_k|i\rangle \) and measure on the basis \(|0\rangle, |1\rangle\)^n.

In the two multi-bit-oriented schemes described above, Bob can obtain the message via measuring the result. 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 obtains \(|i \oplus j\rangle\). Because Bob can obtain the exact value of \( i \), he can obtain the message \( j \) successfully.

3.3 Security analysis of both schemes

The security of the QPKE is also analyzed from two perspectives: (1) Security of the encryption and (2) Security of the private key. For security of the encryption, the ciphertext of message \( j \) under private key \( k \) is

\[
\rho_F^j = \sum_F Y_j \left[ H_F(s) \left( \sum_i p_i F |i\rangle \langle i| \right) H_F(s) \right] Y_j = I/2^n.
\]
Then, for any \( j \) and \( j' (j \neq j') \),

\[
D(\rho_F^j, \rho_F^{j'}) = 0,
\]

(20)

and for any \( F \) and \( F' (F \neq F') \),

\[
D(\rho_F^j, \rho_{F'}^{j'}) = 0.
\]

(21)

According to the definition of information-theoretic quantum ciphertext indistinguishability described in 2.2.1, an attacker cannot distinguish any two ciphertexts encrypted by different public keys corresponding to the same private key because of Eq. (20). Moreover, if an attacker intercepts two different ciphertext states encrypted by public keys corresponding to different private keys, he is unable to distinguish them because of Eq. (21).

For security of the private key, similar to the analysis in 2.4.2, suppose that the attacker, Eve, acquires a user’s public key and then measures it. The public-key state for Eve is

\[
\rho' = \frac{1}{2^n} \sum_k \sum_i |H_k| i \rangle \langle i | H_k = \frac{1}{2^n}.
\]

Then, the quantum part of the public key is a totally mixed state for the attacker, so he cannot obtain any information about the private key.

4 Discussions

4.1 Authentication of the encrypted quantum messages

For the schemes in this paper, if the attacker applies certain Pauli gate to the message encrypted by the sender Alice, the measurement result for the receiver Bob in the decryption phase can be changed without being detected. This kind of attack threatens data integrity, altering data in an unauthorized manner after it was created by an authorized source. Like other encryption schemes such as RSA, encryption itself does not ensure data integrity [34], and methods should be taken to resist such attacks to make the scheme work in practice.

As shown in [34], to prevent such an attack, the technique of authentication can be used, which is an important branch in cryptography independent of encryption discussed in this paper. Some discussions on quantum message authentication [35–40] have been proposed, which can be referred to when message authentication of the schemes herein is explored in detail in our future study.

4.2 Authentication of the public key

In classical public-key schemes, to resist man-in-the-middle attack on the public key, the public key is always authenticated before use. In QPKE schemes, the public key also should be authenticated. Consider the way to achieve this by first exploring the classical case. Generally, there are five techniques for distributing classical public keys with guaranteed/verifiable authenticity [34]:

\[ \text{Springer} \]
(1) Point-to-point delivery. To exchange public keys and associated information over an untrusted electronic channel and provide authentication of this information by communicating a hash. Another case is to obtain authentic public keys directly from the associated user over a trusted channel, such as a trusted courier or registered mail.

(2) Direct access to a trusted public file (public-key registry). A public database, the integrity of which is trusted, may be set up to contain the name and authentic public key of each system user. This may be implemented as a public-key registry operated by a trusted party. Users acquire keys directly from this registry.

(3) Use of an online trusted server. An online trusted server provides access to the equivalent of a public file storing authentic public keys, returning requested (individual) public keys in signed transmissions. The requesting party possesses a copy of the servers signature verification public key, allowing verification of the authenticity of such transmissions.

(4) Use of an off-line server and certificates. In a one-time process, each party A contacts an off-line trusted party referred to as a certification authority (CA), to register its public key and obtain the CAs signature verification public key (allowing verification of other users certificates). The CA certifies As public key by binding it to a string identifying A, thereby creating a certificate. Parties obtain authentic public keys by exchanging certificates or extracting them from a public directory.

(5) Use of systems implicitly guaranteeing authenticity of public parameters. In such systems, including identity-based systems and those using implicitly certified keys, by algorithmic design, modification of public parameters results in detectable, non-compromising failure of cryptographic techniques.

For the public-key authentication methods in QPKE, possible ways may include:

On the one hand, the technique of public-key infrastructure (PKI) is adopted. For QPKE schemes with classical public keys such as [15], classical PKI can be used. For QPKE schemes with quantum public keys, which is the case in this paper, quantum PKI needs to be developed. The main issue that should be considered for quantum PKI is to design signature schemes on quantum messages, so that the certification authority can sign on a user’s public key and identity information to produce a certificate. Some signature schemes on quantum messages with computational security such as [17] have been proposed. Signature schemes on quantum messages with information-theoretical security are needed, so as to maintain the security level of the QPKE schemes in this paper, and the one proposed by Buhrman et al. [41] can be an alternative choice among available schemes.

On the other hand, conducting point-to-point authentication of public keys, i.e., if Alice wants to send Bob messages and needs to get authenticated public key of Bob, they can run an authentication protocol for the quantum state of the public key directly between them, using authentication schemes like that in [35–40].

### 4.3 A possible improved scheme

In the schemes provided above, although \( H_k|\rangle \) is unknown to the attacker, he can identify if the private keys are different since \( s \) is obvious. Then, the attacker can acquire several copies of the same \((s, H_k|\rangle)\), with which he may obtain information
about the private key. Thus, to ensure the security of the private key, the amount of public keys with the same \( s \) should be limited. Here, we propose a possible method of improving the security of proposed schemes in this paper such as the one described in Sect. 2.3:

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

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

(G2) Randomly select \( |i\rangle \in \{0, 1\}^n \). Then, select \( s \in \{0, 1\}^m \) randomly, and compute \( (k, p) = F(s) \). If \( p \neq P(i) \), then 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 a one-bit message \( b \) to Bob, then she should obtain one of Bob’s public keys and then:

(E1) Select \( j \) randomly from \( \Omega_b \);

(E2) Apply \( I \otimes Y_j \) to \( |\psi_s\rangle \otimes H_k |i\rangle \) and then send \( |\psi_s\rangle \otimes Y_j H_k |i\rangle \) to Bob.

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

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

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

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

This method is also useful for our multi-bit-oriented schemes. Similarly to the approach described in previous sections, we can prove that the scheme is information-theoretically secure under an attack on the private key and encryption. Furthermore, owing to the basic principles of the quantum mechanism, the information contained in the quantum state (such as \( s \)) cannot be completely obtained. Hence, the information get by attackers from the public key is greatly limited, and he can hardly obtain pairs of \( (s, H_k |i\rangle) \) to deduce the private key. Based on a preliminary analysis, to ensure security of the private key, more public keys with the same \( s \) may be allowed than that in the proposed schemes in this paper, which is to be strictly proved in further study.

## 5 Conclusion

We proposed several QPKE schemes for classical messages based on conjugate coding. The features of our schemes are as follows: (1) The private key is Boolean functions; (2) the public key is classical string-quantum state pairs, and one private key corresponds to an exponential number of public keys; (3) information-theoretic security is ensured under attacks on the private key and the encryption; (4) from a practical point of view, the schemes may be more easily realized using single-photon strings.

**Acknowledgements** This work was supported by National Natural Science Foundation of China (Grant No. 61672517), National Natural Science Foundation of China (Key Program, Grant No. 61732021), National Cryptography Development Fund (Grant No. MMJJ20170108) and Beijing Municipal Science & Technology Commission (Grant No. Z191100007119006).
References

1. Rivest, R.L., Shamir, A., Adleman, L.A.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 120–126 (1978)
2. ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. Inf. Theory 31, 469–478 (1985)
3. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Goldwasser, S. (ed.) Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, pp. 124–134 (1994)
4. Bennett, C.H., Brassard, G.: 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. Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67, (1991)
6. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68, (1992)
7. Wang, L., Zhou, Y., Zhou, X., et al.: New scheme for measurement-device-independent quantum key distribution. Quantum Inf. Process. 17, 231 (2018)
8. Lee, C., Mower, J., Zhang, Z., et al.: Finite-key analysis of high-dimensional time–energy entanglement-based quantum key distribution. Quantum Inf. Process. 14, 1005–1015 (2015)
9. Okamoto, T., Tanaka, K., Uchiyama, S.: Quantum Public-key cryptosystems. In: Bellare, M. (ed.) Advances in Cryptology: Crypto 2000 Proceedings, LNCS, vol. 1880, pp. 147–165 (2000)
10. Gottesman, D.: Quantum public key cryptography with information-theoretic security. In: Workshop on Classical and Quantum Information Security, pp. 15–18 (2005)
11. Kawachi, A., Koshiha, T., Nishimura, H., Yamakami, T.: Computational indistinguishability between quantum states and its cryptographic application. In: Cramer, R. (ed.) Advances in Cryptology: Eurocrypt 2005 Proceedings, LNCS, vol. 3494, pp. 268–284 (2005)
12. Kawachi, A., Koshiha, T., Nishimura, H., Yamakami, T.: Computational indistinguishability between quantum states and its cryptographic application. J. Cryptol. 25(3), 528–555 (2012)
13. Nikolopoulos, G.M.: Applications of single-qubit rotations in quantum public-key cryptography. Phys. Rev. A. 77, 032348 (2008)
14. Nikolopoulos, G.M.: Deterministic quantum-public-key encryption: forward search attack and randomization. Phys. Rev. A. 79, 042327 (2009)
15. Fujita, H.: Quantum McEliece public-key cryptosystem. Quantum Inf. Comput. 12(3–4), 181–202 (2012)
16. Yang, L.: A public-key cryptosystem for quantum message transmission. In: Proceedings of the SPIE vol. 5631(1), pp. 233–236 (2005)
17. Yang, L., Liang, M., Li, B., Hu, L., Feng, D.G.: Quantum public-key cryptosystems based on induced trapdoor one-way transformations, e-print arXiv:1012.5249 (2010)
18. Liang, M., Yang, L.: Public-key encryption and authentication of quantum information. Sci. China Phys. Mech. Astron. 55(9), 1618–1629 (2012)
19. Gao, F., Wen, Q.Y., Qin, S.J., Zhu, F.C.: Quantum asymmetric cryptography with symmetric keys. Sci. China Ser. G Phys. Mech. Astron. 52, 1925–1931 (2009)
20. Yang, L., Yang, B., Pan, J.: Quantum public-key encryption protocols with information-theoretic security. In: Proceedings of the SPIE, vol. 8440, pp. 84400E–1–84400E–7 (2012)
21. Wu, C., Yang, L.: Bit-oriented quantum public-key encryption based on quantum perfect encryption. Quantum Inf. Process. 15(8), 3285–3300 (2016)
22. Wu, C., Yang, L.: Qubit-wise teleportation and its application in public-key secret communication. Sci. China (Inf. Sci.) 3, 183–194 (2017)
23. Wu, W., Cai, Q., Zhang, H., et al.: Quantum public key cryptosystem based on bell states. Int. J. Theor. Phys. (2017)
24. Wang, Y., She, K.: A practical quantum public-key encryption model. In: 2017 3rd International Conference on Information Management (ICIM), Chengdu, pp. 367–372 (2017)
25. Wiesner, S.: Conjugate coding. SIGACT News 15(1), 78–88 (1983)
26. Rabin, M.O.: How to exchange secrets by oblivious transfer. Harvard University: Aiken Computation Laboratory, Technical Report TR-81 (1981)
27. Even, S., Goldreich, O., Lempel, A.: A randomized protocol for signing contracts. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology. Springer, Boston (1983)
28. Deng, F.G., Long, G.L.: Secure direct communication with a quantum one-time pad. Phys. Rev. A 69(5), 052319 (2004)
29. Yang, L., Xiang, C., Li, B.: Quantum probabilistic encryption protocol based on conjugate coding. China Commun. 10(2), 19–26 (2013)
30. Bethune, D.S., Risk, W.P.: An auto-compensating fiber-optic quantum cryptography system based on polarization splitting of light. J. Quantum Electron. 36(3), 100 (2000)
31. Pan, J.Y., Yang, L.: Quantum public-key encryption with information theoretic security, e-print arXiv:1006.0354 (2010)
32. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
33. Hayashi, M., Kawachi, A., Cobayashi, H.: Quantum measurements for hidden subgroup problems with optimal sample complexity. Quantum Inf. Comput. 8, 0345–0358 (2008)
34. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1997)
35. Barnum, H., Crepeau, C., Gottesman, D.: Authentication of quantum messages. In: The 34rd Annual IEEE Symposium on Foundations of Computer Science, November 16, et al.: November 19, 2002, Vancouver, BC, p. 2002. Institute of Electrical and Electronics Engineers Computer Society, Canada (2002)
36. Yang, L., Hu, L., Feng, D.: Quantum message authentication based on algebraic coding theory. In: Guo, G.-C., Lo, H.-K., Sasaki, M., Liu, S. (eds.) Quantum Optics and Applications in Computing and Communications II. Proceedings of SPIE Vol. 5631. SPIE, Bellingham (2005)
37. Garg, S., Yuen, H., Zhandry, M.: New security notions and feasibility results for authentication of quantum data. In: Annual International Cryptology Conference, pp. 342–371. Springer (2017)
38. Broadbent, A., Gutoski, G., Stebila, D.: Quantum one-time programs. In: Advances in Cryptology-CRYPTO 2013, pp. 344–360. Springer (2013)
39. Aharonov, D., Ben-Or, M., Eban, E.: Interactive proofs for quantum computations. In: Proceedings of Innovations in Computer Science. Tsinghua University Press (2010)
40. Broadbent, A., Wainwright, E.: Efficient simulation for quantum message authentication. In: Nascimento, A., Barreto, P. (eds.) Information Theoretic Security. ICITS 2016. Lecture Notes in Computer Science, vol. 10015. Springer
41. Buhman, H., Cleve, R., Watrous, J., De Wolf, R.: Quantum fingerprinting. Phys. Rev.Lett. 87(16), 167902 (2001)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.