

Quantum private comparison of arbitrary single qubit states based on swap test

Xi Huang(黄曦), Yan Chang(昌燕), Wen Cheng(程稳), Min Hou(侯敏), and Shi-Bin Zhang(张仕斌)

Citation: Chin. Phys. B, 2022, 31 (**4**): 040303. DOI: 10.1088/1674-1056/ac4103
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Semi-quantum private comparison protocol of size relation with *d*-dimensional GHZ states

Bing Wang(王冰), San-Qiu Liu(刘三秋), and Li-Hua Gong(龚黎华)
Chin. Phys. B, 2022, 31 (**1**): 010302. DOI: 10.1088/1674-1056/ac1413

New semi-quantum key agreement protocol based on high-dimensional single-particle states

Huan-Huan Li(李欢欢), Li-Hua Gong(龚黎华), and Nan-Run Zhou(周南润)
Chin. Phys. B, 2020, 29 (**11**): 110304. DOI: 10.1088/1674-1056/abaedd

Coherent attacks on a practical quantum oblivious transfer protocol

Guang-Ping He(何广平)
Chin. Phys. B, 2018, 27 (**10**): 100308. DOI: 10.1088/1674-1056/27/10/100308

Two-step quantum secure direct communication scheme with frequency coding

Xue-Liang Zhao(赵学亮), Jun-Lin Li(李俊林), Peng-Hao Niu(牛鹏皓), Hong-Yang Ma(马鸿洋), Dong Ruan(阮东)
Chin. Phys. B, 2017, 26 (**3**): 030302. DOI: 10.1088/1674-1056/26/3/030302

Probabilistic direct counterfactual quantum communication

Sheng Zhang(张盛)
Chin. Phys. B, 2017, 26 (**2**): 020304. DOI: 10.1088/1674-1056/26/2/020304

Quantum private comparison of arbitrary single qubit states based on swap test

Xi Huang(黄曦)[1,2], Yan Chang(昌燕)[1,2], Wen Cheng(程稳)[1,2], Min Hou(侯敏)[1,2], and Shi-Bin Zhang(张仕斌)[1,2,†]

[1] *School of Cybersecurity, Chengdu University of Information Technology, Chengdu* 610225, *China*
[2] *Sichuan Key Laboratory of Advanced Cryptography and System Security, Chengdu* 610225, *China*

(Received 9 September 2021; revised manuscript received 20 October 2021; accepted manuscript online 8 December 2021)

By using swap test, a quantum private comparison (QPC) protocol of arbitrary single qubit states with a semi-honest third party is proposed. The semi-honest third party (TP) is required to help two participants perform the comparison. She can record intermediate results and do some calculations in the whole process of the protocol execution, but she cannot conspire with any of participants. In the process of comparison, the TP cannot get two participants' private information except the comparison results. According to the security analysis, the proposed protocol can resist both outsider attacks and participants' attacks. Compared with the existing QPC protocols, the proposed one does not require any entanglement swapping technology, but it can compare two participants' qubits by performing swap test, which is easier to implement with current technology. Meanwhile, the proposed protocol can compare secret integers. It encodes secret integers into the amplitude of quantum state rather than transfer them as binary representations, and the encoded quantum state is compared by performing the swap test. Additionally, the proposed QPC protocol is extended to the QPC of arbitrary single qubit states by using multi-qubit swap test.

Keywords: quantum private comparison, arbitrary single qubit states, swap test, quantum cryptography

PACS: 03.67.–a, 03.67.Dd **DOI:** 10.1088/1674-1056/ac4103

1. Introduction

The quantum information science has made considerable progress, especially in the quantum cryptography field, so far. Quantum cryptography based on the principle of quantum mechanics rather than the computational complexity of solving mathematical problems has a considerable advantage of security over classical cryptography. Since the first quantum cryptographic protocol was proposed by Bennett and Brassard[1] and its unconditional security was proved in 1984, numerous quantum cryptographic protocols have been proposed to solve various cryptographic tasks, such as quantum key distribution (QKD),[1–4] quantum key agreement (QKA),[5–7] quantum secret sharing (QSS),[8–11] quantum secure direct communication (QSDC),[12–14] and quantum private query (QPQ).[15–18]

Secure multiparty computation (SMC) aims to calculate a function in a distributed network of mutual distrust without disclosing the raw content of each party's private inputs. As an important branch of SMC, the first private comparison was proposed by Yao[19] in the millionaires' problem to compare two millionaires who are richer without revealing their actual property. According to Yao's millionaires' problem, Boudot *et al.*[20] suggested a private comparison protocol to compare the equality of two millionaires' actual property. However, the existing private comparison protocols that are based on the computational complexity of solving mathematical problems have security vulnerabilities due to the strong capability of quantum computing. To solve this problem, some researchers began to combine the classical private comparison and quantum mechanics to perform the private comparison. In 2009, Yang and Wen[21] proposed the first QPC protocol, which encodes Hash values into EPR pairs to compare two participants' private inputs. Since then, many QPC protocols based on various quantum states have been proposed, for example, the QPC protocols based on single particle,[22–26] Bell states,[21,27–31] multi-particle entangle states,[32–37] and cluster state.[38–42] Since Lo[43] pointed out that it is impossible to evaluate the equality function in a two-party scenario securely, a semi-honest third party (TP) was introduced in QPC protocols to guarantee security. Except for comparing whether two parties' private inputs are equal, some scholars set out to compare the size relationship of secret integers, which means that multi-participants can compare the size of their secret inputs. Lin *et al.*[44] successfully proposed a QPC protocol of size relation with d-level Bell states. Guo *et al.*[45] presented a QPC protocol of size relation based on entanglement swapping of d-level Bell states. Yu *et al.*[46] put forward a QPC protocol of size relation by using d-level single-particle states. Ye and Ye[47] proposed two multiparty quantum private comparison (MQPC) protocols of size relation with two semi-honest TPs and one semi-honest TP by using d-level single-particle states. Song *et al.*[48] proposed an MQPC by using single-particle states.

Furthermore, the swap test,[49] as a simple and basic algorithm in quantum computing, which was used to put forward

[†]Corresponding author. E-mail: cuitzsb@cuit.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

a quantum cryptographic protocol, is a research focus. The goal of swap test is to evaluate the similarity of the two qubits. By measuring the probability that the ancilla qubit is in state $|1\rangle$ or $|0\rangle$, the square of the inner product of two qubits is obtained. Based on the idea of swap test, quantum signature,[50] quantum neural networks,[51–53] have been proposed.

To the best of our knowledge, all existing QPC protocols are mainly based on entangled states, and the proposed QPC protocol based on swap test has not yet appeared. Moreover, the previous QPC protocols mainly focus on the comparison of secret integers. This paper proposes a QPC protocol of arbitrary single qubit states by using swap test for the first time. Two participants' qubits can be compared by executing this protocol. In this protocol, two participants encrypt their qubits by using rotation operation and sent it to TP. By performing the swap test, the TP can obtain the comparison result of two participants' encrypted qubits. If the measurement result is 0, it indicates that two participants' private inputs are equal. Otherwise, it is not identical. Security analysis shows that our protocol possesses good performance in resisting both outside attacks and participants' attacks. Compared with the existing QPC protocols, the proposed one can compare the equality of two participants' qubits and secret integers. Besides, it does not require any entanglement swapping technology, and qubits are compared by performing swap test, which is easier to implement with current technology. Finally, the proposed protocol is extended to QPC of arbitrary single qubit states by using multi-qubit swap test.

The rest of this paper is organized as follows. Swap test is introduced in Section 2. The detailed description of the proposed QPC of arbitrary single qubit states based on swap test is given in Section 3. Multi-qubit swap test and the proposed QPC of arbitrary single qubit states by using multi-qubit swap test are described in Section 4. Finally, some conclusions are drawn in Section 5.

2. Swap test

Swap test was firstly introduced in Ref. [49]. It aims to evaluate the similarity between arbitrary two qubits. By measuring the probability that the ancilla qubit is in state $|1\rangle$ or $|0\rangle$, we can obtain the square of the inner product of two qubits. The quantum circuit of swap test is shown in Fig. 1.

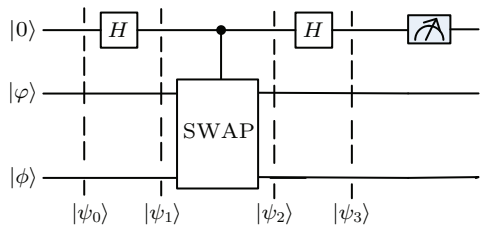


Fig. 1. Quantum circuit of the swap test.

Supposing that there are two qubits $|\varphi\rangle$ and $|\phi\rangle$, as well as an ancilla qubit $|0\rangle$, which constitute an initial quantum state

$$|\psi_0\rangle = |0\rangle \otimes |\varphi\rangle \otimes |\phi\rangle = |0,\varphi,\phi\rangle, \tag{1}$$

and applying the Hadamard gate to the ancilla qubit, the initial state $|\psi_0\rangle$ is transformed into $|\psi_1\rangle$,

$$\begin{aligned} |\psi_1\rangle &= (H\otimes I\otimes I)|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes|\varphi\rangle\otimes|\phi\rangle \\ &= \frac{1}{\sqrt{2}}(|0,\varphi,\phi\rangle+|1,\varphi,\phi\rangle). \end{aligned} \tag{2}$$

Then, by performing the controlled-swap gate, the above state $|\psi_1\rangle$ is changed into $|\psi_2\rangle$,

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{\sqrt{2}}|0\rangle\otimes|\varphi\rangle\otimes|\phi\rangle+\frac{1}{\sqrt{2}}|1\rangle\otimes|\phi\rangle\otimes|\varphi\rangle \\ &= \frac{1}{\sqrt{2}}(|0,\varphi,\phi\rangle+|1,\phi,\varphi\rangle). \end{aligned} \tag{3}$$

By applying another Hadamard gate to the ancilla qubit again, we can obtain $|\psi_3\rangle$,

$$\begin{aligned} |\psi_3\rangle &= (H\otimes I\otimes I)\,|\psi_3\rangle \\ &= \frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\otimes|\varphi\rangle\otimes|\phi\rangle+\frac{|0\rangle-|1\rangle}{\sqrt{2}}\otimes|\phi\rangle\otimes|\varphi\rangle\right) \\ &= \frac{1}{2}|0\rangle\otimes|\varphi\rangle\otimes|\phi\rangle+\frac{1}{2}|1\rangle\otimes|\varphi\rangle\otimes|\phi\rangle \\ &\quad+\frac{1}{2}|0\rangle\otimes|\phi\rangle\otimes|\varphi\rangle-\frac{1}{2}|1\rangle\otimes|\phi\rangle\otimes|\varphi\rangle \\ &= \frac{1}{2}|0\rangle(|\varphi,\phi\rangle+|\phi,\varphi\rangle)+\frac{1}{2}|1\rangle(|\varphi,\phi\rangle-|\phi,\varphi\rangle). \end{aligned} \tag{4}$$

Finally, by performing projection measurement with the measurement operator $M = |1\rangle\langle 1|$ on the ancilla qubit, the probability of the ancilla qubit in state $|1\rangle$ can be written as

$$\begin{aligned} &P(|1\rangle) = \langle\psi_3|M|\psi_3\rangle \\ &= \frac{1}{4}(\langle 1,\varphi,\phi|-\langle 1,\phi,\varphi|)\,|1\rangle\langle 1|\,(|1,\varphi,\phi\rangle-|1,\phi,\varphi\rangle) \\ &= \frac{1}{4}(\langle\varphi,\phi|-\langle\phi,\varphi|)\,(|\varphi,\phi\rangle-|\phi,\varphi\rangle) \\ &= \frac{1}{2}-\frac{1}{2}|\langle\varphi|\phi\rangle|^2. \end{aligned} \tag{5}$$

Thus, we can obtain the square of the inner product of two qubits $|\varphi\rangle$ and $|\phi\rangle$, *i.e.*, $|\langle\varphi|\phi\rangle|^2 = 1-2P(|1\rangle)$.

If two qubits $|\varphi\rangle$ and $|\phi\rangle$ are the same, equation (4) becomes $|0\rangle(|\varphi,\phi\rangle+\langle\phi,\varphi|)$. The measurement result of the ancilla qubit is $|0\rangle$. However, if two qubits $|\varphi\rangle$ and $|\phi\rangle$ are not the same, the measurement result of the ancilla qubit will be either $|0\rangle$ with a probability of $(1/2)+(1/2)|\langle\varphi|\phi\rangle|^2$ or $|1\rangle$ with a probability of $(1/2)-(1/2)|\langle\varphi|\phi\rangle|^2$. Therefore, two qubits $|\varphi\rangle$ and $|\phi\rangle$ are different if the measurement result of the ancilla qubit is $|1\rangle$. We cannot make sure that two qubits $|\varphi\rangle$ and $|\phi\rangle$ are the same if the measurement result of the ancilla qubit is $|0\rangle$. Further, the error probability of the swap test for n qubits can be given by

$$P_{\mathrm{e}} \leq \prod_{i=1}^{n}\left(\frac{1+|\langle\varphi|\phi\rangle|^2}{2}\right). \tag{6}$$

The error probability of the swap test can be reduced to any $\delta > 0$ by performing the swap test λ times, resulting in an error probability below δ, where $\lambda \in O(\log_2 1/\delta)$.

Theorem 1 Let $|\varphi\rangle = \cos\alpha_0|0\rangle + \sin\alpha_0|1\rangle$ and $|\phi\rangle = \cos\alpha_1|0\rangle + \sin\alpha_1|1\rangle$ be arbitrary qubits, by performing swap test on them, the probability of the ancilla qubit in state $|1\rangle$ is $(1/2) - (1/2)\cos^2(\alpha_0 - \alpha_1)$.

Proof By performing swap test on $|\varphi\rangle = \cos\alpha_0|0\rangle + \sin\alpha_0|1\rangle$ and $|\phi\rangle = \cos\alpha_1|0\rangle + \sin\alpha_1|1\rangle$, the probability of the ancilla qubit in state $|1\rangle$ can be given by

$$\begin{aligned} P_0(|1\rangle) &= \frac{1}{2} - \frac{1}{2}|\langle\varphi|\phi\rangle|^2 \\ &= \frac{1}{2} - \frac{1}{2}\Big|(\cos\alpha_0\langle 0| + \sin\alpha_0\langle 1|) \\ &\quad \times (\cos\alpha_1|0\rangle + \sin\alpha_1|1\rangle)\Big|^2 \\ &= \frac{1}{2} - \frac{1}{2}(\cos\alpha_0\cos\alpha_1 + \sin\alpha_0\sin\alpha_1). \end{aligned} \tag{7}$$

Theorem 2 Let

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

be the rotation operation, which is used to encrypt $|\varphi\rangle$ and $|\phi\rangle$. By performing swap test on the encrypted $|\varphi\rangle$ and $|\phi\rangle$, the probability of the ancilla qubit in state $|1\rangle$ is $(1/2) - (1/2)\cos^2(\alpha_0 - \alpha_1)$.

Proof Using the rotation operation

$$R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

to encrypt $|\varphi\rangle$ and $|\phi\rangle$, the following equations can be obtained

$$\begin{aligned} R(\theta)|\phi\rangle &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\alpha_0 \\ \sin\alpha_0 \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta\cos\alpha_0 - \sin\theta\sin\alpha_0 \\ \sin\theta\cos\alpha_0 + \cos\theta\sin\alpha_0 \end{pmatrix} \\ &= \begin{pmatrix} \cos(\alpha_0+\theta) \\ \sin(\alpha_0+\theta) \end{pmatrix} \\ &= \cos(\alpha_0+\theta)|0\rangle + \sin(\alpha_0+\theta)|1\rangle, \end{aligned} \tag{8}$$

$$\begin{aligned} R(\theta)|\phi\rangle &= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}\begin{pmatrix} \cos\alpha_1 \\ \sin\alpha_1 \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta\cos\alpha_1 - \sin\theta\sin\alpha_1 \\ \sin\theta\cos\alpha_1 + \cos\theta\sin\alpha_1 \end{pmatrix} \\ &= \begin{pmatrix} \cos(\alpha_1+\theta) \\ \sin(\alpha_1+\theta) \end{pmatrix} \\ &= \cos(\alpha_1+\theta)|0\rangle + \sin(\alpha_1+\theta)|1\rangle. \end{aligned} \tag{9}$$

By performing swap test on the encrypted $|\varphi\rangle$ and $|\phi\rangle$, the probability of the ancilla qubit in state can be written as

$$\begin{aligned} P_1(|1\rangle) &= \frac{1}{2} - \frac{1}{2}|\langle R(\theta)|\varphi\rangle|R(\theta)|\phi\rangle\rangle|^2 \\ &= \frac{1}{2} - \frac{1}{2}\Big|(\cos(\alpha_0+\theta)\langle 0| + \sin(\alpha_0+\theta)\langle 1|) \\ &\quad \times (\cos(\alpha_1+\theta)|0\rangle + \sin(\alpha_1+\theta)|1\rangle)\Big|^2 \\ &= \frac{1}{2} - \frac{1}{2}\big(\cos(\alpha_0+\theta)\cos(\alpha_1+\theta) \\ &\quad + \sin(\alpha_0+\theta)\sin(\alpha_1+\theta)\big) \\ &= \frac{1}{2} - \frac{1}{2}\cos^2(\alpha_0-\alpha_1). \end{aligned} \tag{10}$$

According to Theorem 1 and Theorem 2, it can be concluded that the same rotation operation $R(\theta)$ applied to $|\varphi\rangle$ and $|\phi\rangle$ does not change the probability for the ancilla qubit to reside in state $|1\rangle$ by performing swap test.

3. Proposed QPC of arbitrary single qubit states based on swap test

3.1. QPC protocol description

Suppose that there are two participants, says Alice and Bob, who want to compare whether their secret qubits $|\varphi_i\rangle = \cos\alpha_i|0\rangle + \sin\alpha_i|1\rangle$ and $|\phi_i\rangle = \cos\beta_i|0\rangle + \sin\beta_i|1\rangle$ are equal under the semi-honest third party TP), where $\alpha_i, \beta_i \in [0, \pi]$. The TP may behave improperly, but she is not allowed to conspire with any participant. Assume that the protocol runs in ideal conditions (*i.e.*, there are no technical errors and the transmission channels are lossless and noiseless), then the proposed QPC of arbitrary single qubit states based on swap test will be able to be described as follows.

Step 1 Alice and Bob share a secret key θ_i via a secure QKD protocol like BB84 protocol[1] in advance. The TP and Alice (Bob) share a secret key γ_i (ω_i) through a secure QKD protocol as well. Here, $0 \le \theta_i \le \pi$, $0 \le \gamma_i \le \pi$, and $0 \le \omega_i \le \pi$.

Step 2 Alice (Bob) uses θ_i and γ_i (ω_i) to encrypt her (his) own qubits $|\varphi_i\rangle$ ($|\phi_i\rangle$) to form a new sequence $|\chi_i^{\mathrm{A}}\rangle$ ($|\chi_i^{\mathrm{B}}\rangle$). The encrypting process can be written as

$$\begin{aligned} |\chi_i^{\mathrm{A}}\rangle &= R(\gamma_i)R(\theta_i)|\phi_i\rangle \\ &= \cos(\alpha_i+\theta_i+\gamma_i)|0\rangle + \sin(\alpha_i+\theta_i+\gamma_i)|1\rangle, \end{aligned} \tag{11}$$

$$\begin{aligned} |\chi_i^{\mathrm{B}}\rangle &= R(\omega_i)R(\theta_i)|\phi_i\rangle \\ &= \cos(\beta_i+\theta_i+\omega_i)|0\rangle + \sin(\beta_i+\theta_i+\omega_i)|1\rangle. \end{aligned} \tag{12}$$

Then, Alice (Bob) prepares δ decoy photons randomly chosen in one of four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and inserts the δ decoy photons into $|\chi_i^{\mathrm{A}}\rangle$ ($|\chi_i^{\mathrm{B}}\rangle$) at random position to generate a new sequence $|\chi_i^{\mathrm{A}}\rangle^*$ ($|\chi_i^{\mathrm{B}}\rangle^*$). Finally, Alice (Bob) sends $|\chi_i^{\mathrm{A}}\rangle^*$ ($|\chi_i^{\mathrm{B}}\rangle^*$) to TP.

Step 3 When TP receives each particle of $|\chi_i^{\mathrm{A}}\rangle^*$ ($|\chi_i^{\mathrm{B}}\rangle^*$) that Alice (Bob) sends to her, she first stores it in quantum memory. After the TP has received the whole sequence $|\chi_i^{\mathrm{A}}\rangle^*$ ($|\chi_i^{\mathrm{B}}\rangle^*$), the TP sends an acknowledgment to Alice (Bob). Then, Alice (Bob) and TP check the security of the qubits' transmission. Alice (Bob) announces the positions and the corresponding bases of decoy photons to the TP, and the TP measures the decoy photons by using the right

bases and returns the measurement results to Alice (Bob). Alice (Bob) checks whether the qubit transmission is secure by comparing the measurement result of decoy photons with the initial prepared states. If the error rate is less than a predetermined threshold, it indicates that the qubits' transmission is secure, and the protocol will proceed to the next step. Otherwise, the protocol will be aborted.

Step 4 After removing the decoy photons in $\left|\chi_i^{\mathrm{A}}\right\rangle^*$ $\left(\left|\chi_i^{\mathrm{B}}\right\rangle^*\right)$, the TP uses the secret key $\gamma_i(\omega_i)$ to decrypt $\left|\chi_i^{\mathrm{A}}\right\rangle$ $\left(\left|\chi_i^{\mathrm{B}}\right\rangle\right)$ to obtain a new sequence $\left|\lambda_i^{\mathrm{A}}\right\rangle$ $\left(\left|\lambda_i^{\mathrm{B}}\right\rangle\right)$. The decrypting process can be written as

$$\begin{aligned}\left|\lambda_i^{\mathrm{A}}\right\rangle &= R(-\gamma_i)\left|\chi_i^{\mathrm{A}}\right\rangle \\ &= \cos(\alpha_i+\theta_i)\left|0\right\rangle+\sin(\alpha_i+\theta_i)\left|1\right\rangle, \qquad (13)\\ \left|\lambda_i^{\mathrm{B}}\right\rangle &= R(-\omega_i)\left|\chi_i^{\mathrm{B}}\right\rangle \\ &= \cos(\beta_i+\theta_i)\left|0\right\rangle+\sin(\beta_i+\theta_i)\left|1\right\rangle. \qquad (14)\end{aligned}$$

Then, the TP performs swap test on $\left|\lambda_i^{\mathrm{A}}\right\rangle$ and $\left|\lambda_i^{\mathrm{B}}\right\rangle$ to obtain the measurement results of the ancilla qubit.

Step 5 By performing Steps 1–4 λ times, if in the measurement results of the ancilla qubit there exists $|1\rangle$, TP announces Alice's (Bob's) qubits are different. If the measurement results of the ancilla qubit are all $|0\rangle$, the TP announces that Alice's (Bob's) qubits are equal.

3.2. Security analysis

In this subsection, the security of the proposed QPC protocol is analyzed from the prospect of both outsider attacks and participants' attacks.

3.2.1. Outsider attacks

Since the confidentiality of Alice (Bob's) qubits are encrypted with rotation operation and the decoy photons technology is adopted to guarantee the security of qubit transmission, besides, the corresponding rotation operations are unknown to Eve, she cannot learn anything about Alice's (Bob's) qubits. Thus, Eve has to adopt some common attack strategies to steal something about Alice's (Bob's) qubits as much as possible, such as the intercept-resend attack, the direct measurement attack, the entangle–measure attack, the man-in-the-middle attack, and the Trojan horse attacks.

Case 1 Intercept–resend attack

The only way for Eve to steal something about Alice's (Bob's) qubits by performing the intercept–resend attack is the transmission of $\left|\chi_i^{\mathrm{A}}\right\rangle^*$ $\left(\left|\chi_i^{\mathrm{B}}\right\rangle^*\right)$ in Step 2. We consider that Eve adopts the intercept–resend attack strategy on Alice (Bob) as follows. Eve intercepts the sequence $\left|\chi_i^{\mathrm{A}}\right\rangle^*$ $\left(\left|\chi_i^{\mathrm{B}}\right\rangle^*\right)$, and then she prepares the corresponding fake sequence and sends it to TP. However, Alice (Bob) prepares δ decoy photons randomly chosen in one of four states $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$, and inserts the δ decoy photons into $\left|\chi_i^{\mathrm{A}}\right\rangle$ $\left(\left|\chi_i^{\mathrm{B}}\right\rangle\right)$ at a randomly chosen position. Without knowing the positions of decoy photons, Eve cannot distinguish between decoy particles and carrier particles. The probability of the intercept–resend attack to be detected can be given by

$$P = 1-[P(C)P(S|C)+P(M)P(S|M)]^{\delta}, \qquad (15)$$

where $P(C)$ denotes the probability of choosing the correct measurement basis, $P(S|C)$ the conditional probability of passing the eavesdropping detection by selecting the correct measurement basis, $P(M)$ the probability of choosing the mismatched measurement basis, $P(S|M)$ the conditional probability of passing the eavesdropping detection by selecting the mismatched measurement basis, and δ the number of decoy photons used in eavesdropping check. Since Eve does nothing about the measurement bases of decoy photons, she can only guess the correct measurement basis and the mismatched one of each decoy particle with the same probability of 0.5. If Eve selects the correct measurement basis, the conditional probability of passing the eavesdropping detection is 1. If Eve chooses the mismatched measurement basis, the conditional probability of passing the eavesdropping detection is 0.5. Therefore, for a decoy photon, the probability of passing the eavesdropping detection by performing the intercept-resend attack is 0.75 $(=0.5\times1+0.5\times0.5)$ according to Eq. (15). For δ decoy photons, the probability of the intercept–resend attack being detected is $1-(0.75)^{\delta}$. When the number of decoy photons, δ is large enough, the probability of the intercept–resend attack being detected will be approximately 1. Besides, the reduced density of Alice's (Bob's) encrypted qubits $\left|\chi_i^{\mathrm{A}}\right\rangle$ $\left(\left|\chi_i^{\mathrm{B}}\right\rangle\right)$ is

$$\begin{aligned}\rho^{\mathrm{A}} &= \mathrm{tr}\left(\left(\cos(\alpha_i+\theta_i+\gamma_i)\left|0\right\rangle+\sin(\alpha_i+\theta_i+\gamma_i)\left|1\right\rangle\right)\left(\left(\cos(\alpha_i+\theta_i+\gamma_i)\left\langle0\right|+\sin(\alpha_i+\theta_i+\gamma_i)\left\langle1\right|\right)\right)\\ &= \cos^2(\alpha_i+\theta_i+\gamma_i)\left|0\right\rangle\left\langle0\right|+\sin(\alpha_i+\theta_i+\gamma_i)\left|1\right\rangle\left\langle1\right|, \qquad (16)\\ \rho^{\mathrm{B}} &= \mathrm{tr}\left(\left(\cos(\beta_i+\theta_i+\omega_i)\left|0\right\rangle+\sin(\beta_i+\theta_i+\omega_i)\left|1\right\rangle\right)\left(\left(\cos(\beta_i+\theta_i+\omega_i)\left\langle0\right|+\sin(\beta_i+\theta_i+\omega_i)\left\langle1\right|\right)\right)\\ &= \cos^2(\beta_i+\theta_i+\omega_i)\left|0\right\rangle\left\langle0\right|+\sin(\beta_i+\theta_i+\omega_i)\left|1\right\rangle\left\langle1\right|. \qquad (17)\end{aligned}$$

That is to say, the reduced density of $\left|\chi_i^{\mathrm{A}}\right\rangle$ $\left(\left|\chi_i^{\mathrm{B}}\right\rangle\right)$ is in the same state, and Eve cannot distinguish these states perfectly. Therefore, Eve cannot learn anything about Alice's (Bob's) qubits without being detected by performing the intercept–resend attack.

Case 2 Direct measurement attack

The direct measurement attack is that Eve intercepts the sequence $\left|\chi_i^{\mathrm{A}}\right\rangle^*\left(\left|\chi_i^{\mathrm{B}}\right\rangle^*\right)$ and measures it directly. Without knowing the positions of decoy photons, Eve cannot distinguish between decoy particles and carrier particles. Suppose that Eve knows the position of decoy photons, and she can measure these particles to obtain the measurement outcome MA_i (MB_i),

$$MA_i = \left|\chi_i^{\mathrm{A}}\right\rangle|1\rangle\langle 1|\left|\chi_i^{\mathrm{A}}\right\rangle = \sin^2(\alpha_i+\theta_i+\gamma_i), \quad (18)$$

$$MB_i = \left|\chi_i^{\mathrm{B}}\right\rangle|1\rangle\langle 1|\left|\chi_i^{\mathrm{B}}\right\rangle = \sin^2(\beta_i+\theta_i+\omega_i). \quad (19)$$

However, the measurement outcome MA_i (MB_i) is encrypted with the secret key θ_i and γ_i (ω_i and γ_i), she cannot infer the confidentiality of Alice (Bob's) qubits without knowing θ_i (ω_i or γ_i).

Case 3 Entangle–measure attack

The entangle-measure attack is that Eve intercepts the transmitted qubits and performs the unitary operation U to entangle the prepared ancilla qubits in state $|E\rangle$ and the intercepted qubits. The unitary operation U is given by

$$U(|0\rangle|E\rangle) = a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle, \quad (20)$$

$$U(|1\rangle|E\rangle) = c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle, \quad (21)$$

$$\begin{aligned} U|+\rangle|E\rangle &= \frac{1}{\sqrt{2}}(U|0\rangle|E\rangle + U|1\rangle|E\rangle) \\ &= \frac{1}{\sqrt{2}}\big(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle \\ &\quad + c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle\big) \\ &= \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle + c|e_{10}\rangle + d|e_{11}\rangle)] \\ &\quad + \frac{1}{2}[|-\rangle(a|e_{00}\rangle - b|e_{01}\rangle + c|e_{10}\rangle - d|e_{11}\rangle)] \\ &= |+\rangle|e_{++}\rangle + |-\rangle|e_{+-}\rangle, \end{aligned} \quad (22)$$

$$\begin{aligned} U|-\rangle|E\rangle &= \frac{1}{\sqrt{2}}(U|0\rangle|E\rangle - U|1\rangle|E\rangle) \\ &= \frac{1}{\sqrt{2}}\big(a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle \\ &\quad - c|0\rangle|e_{10}\rangle - d|1\rangle|e_{11}\rangle\big) \\ &= \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle)] \\ &\quad + \frac{1}{2}[|-\rangle(a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle)] \\ &= |+\rangle|e_{-+}\rangle + |-\rangle|e_{--}\rangle, \end{aligned} \quad (23)$$

where $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$, $|e_{11}\rangle$ are pure states uniquely determined by the unitary operation U and the coefficients satisfy $|a|^2+|b|^2=1$, $|c|^2+|d|^2=1, |a|^2=|d|^2=F$, and $|b|^2=|c|^2=D$. Here F is the fidelity, and D is the quantum bit error rate (QBER). If the decoy photon is $\{|0\rangle,|1\rangle\}$, the correct result can be obtained with the probability of F. If the decoy photon is $\{|+\rangle,|-\rangle\}$, the correct result can be obtained with a probability of $1/2$. For a decoy photon, the valid state can be known to possess the probability of $p=(1/2)(F+(1/2))$, where F is the fidelity when the decoy state is in $\{|0\rangle,|1\rangle\}$, and $1/2$ is the fidelity when the decoy state is in $\{|+\rangle,|-\rangle\}$. Additionally, both the two cases can occur with the probability of $1/2$. Therefore, the probability of the detection of Eve is $1-p^{\delta}$, where δ is the number of decoy photons. The probability of the detection of Eve will be approximately 1 when δ is sufficiently large. Without loss of generality, suppose that Eve applies the entangle–measure attack to the intercepted single qubit states $\left|\chi_1^{\mathrm{A}}\right\rangle\left(\left|\chi_1^{\mathrm{B}}\right\rangle\right)$, then she will be able to acquire no information about Alice's (Bob's) secret qubits. From Eqs. (22) and (23), we have

$$\begin{aligned} &U\left(\left|\chi_1^{\mathrm{A}}\right\rangle|E\rangle\right) \\ &= U(\cos(\alpha_1+\theta_1+\gamma_1)|0\rangle + \sin(\alpha_1+\theta_1+\gamma_1)|1\rangle)|E\rangle \\ &= |0\rangle(a\cos(\alpha_1+\theta_1+\gamma_1)|e_{00}\rangle + c\sin(\alpha_1+\theta_1+\gamma_1)|e_{10}\rangle) \\ &\quad + |1\rangle\big(b\cos(\alpha_1+\theta_1+\gamma_1)|e_{01}\rangle \\ &\quad + d\sin(\alpha_1+\theta_1+\gamma_1)|e_{11}\rangle\big), \end{aligned} \quad (24)$$

$$\begin{aligned} &U\left(\left|\chi_1^{\mathrm{B}}\right\rangle|E\rangle\right) \\ &= U(\cos(\beta_1+\theta_1+\omega_1)|0\rangle + \sin(\beta_1+\theta_1+\omega_1)|1\rangle)|E\rangle \\ &= |0\rangle(a\cos(\beta_1+\theta_1+\omega_1)|e_{00}\rangle + c\sin(\beta_1+\theta_1+\omega_1)|e_{10}\rangle) \\ &\quad + |1\rangle\big(b\cos(\beta_1+\theta_1+\omega_1)|e_{01}\rangle \\ &\quad + d\sin(\beta_1+\theta_1+\omega_1)|e_{11}\rangle\big). \end{aligned} \quad (25)$$

To pass the eavesdropping check, Eve must set $b=c=0$, $a=d=1$. At the same time, equations (24) and (25) change into

$$\begin{aligned} U\left(\left|\chi_1^{\mathrm{A}}\right\rangle|E\rangle\right) &= |0\rangle(\cos(\alpha_1+\theta_1+\gamma_1)|e_{00}\rangle) \\ &\quad + |1\rangle(\sin(\alpha_1+\theta_1+\gamma_1)|e_{11}\rangle), \end{aligned} \quad (26)$$

$$\begin{aligned} U\left(\left|\chi_1^{\mathrm{B}}\right\rangle|E\rangle\right) &= |0\rangle(\cos(\beta_1+\theta_1+\omega_1)|e_{00}\rangle) \\ &\quad + |1\rangle(\sin(\beta_1+\theta_1+\omega_1)|e_{11}\rangle). \end{aligned} \quad (27)$$

However, without knowing the secret key θ_1 or γ_1 (ω_1 or θ_1), she cannot derive Alice's (Bob's) qubits by performing the entangle–measure attack.

Case 4 Man-in-the-middle attack

It is supposed that Eve intercepts the sequence $\left|\chi_i^{\mathrm{A}}\right\rangle^*$ and prepares the fake sequence $\left|\chi_i^{E}\right\rangle$ and sends it to TP instead of $\left|\chi_i^{\mathrm{A}}\right\rangle^*$. Without knowing the relevant information about decoy photons, Eve can only prepare the decoy photons in $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ base to reduce the detection probability. Let the i-th decoy photon be denoted by D_i^{A}, which is the j-th qubit of the sequence $\left|\chi_i^{\mathrm{A}}\right\rangle^*$. The D_i^{A} is prepared in basis B. Let the j-th qubit of $\left|\chi_i^{E}\right\rangle$ be represented by $D_i^{\mathrm{A}'}$, where $D_i^{\mathrm{A}'}$ is prepared in basis B'. It must be noted that B and B' are $\{|0\rangle,|1\rangle\}$or $\{|+\rangle,|-\rangle\}$. In the security check process, when Alice announces the preparation basis of D_i^{A}, then TP measures $D_i^{\mathrm{A}'}$ in basis B and obtains $D_i^{\mathrm{A}''}$. The probability of $D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}$ can be calculated as follows.

(i) If $B=B'$ and $D_i^{\mathrm{A}}=D_i^{\mathrm{A}'}$, then $D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}$ with a probability of 1.

(ii) If $B=B'$ and $D_i^{\mathrm{A}}\neq D_i^{\mathrm{A}'}$, then $D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}$ with a probability of 0.

(iii) If $B\neq B'$, then $D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}$ with a probability of $1/2$.

Thus, for a decoy photon, the probability that Eve can derive the secret qubits is

$$
\begin{aligned}
P\left(D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}\right) &= P\left(D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}|B=B'\right)P\left(B=B'\right)+P\left(D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}|B\neq B'\right)P\left(B\neq B'\right)\\
&= \frac{1}{2}\left(P\left(D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}|B=B'\right)+P\left(D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}|B\neq B'\right)\right)\\
&= \frac{1}{2}\left(P\left(D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}|B=B',D_i^{\mathrm{A}}=D_i^{\mathrm{A}'}\right)P\left(D_i^{\mathrm{A}}=D_i^{\mathrm{A}'}\right)+P\left(D_i^{\mathrm{A}''}=D_i^{\mathrm{A}}|B\neq B',D_i^{\mathrm{A}}\neq D_i^{\mathrm{A}'}\right)P\left(D_i^{\mathrm{A}}\neq D_i^{\mathrm{A}'}\right)+\frac{1}{2}\right)\\
&= \frac{1}{2}\left(1\times\frac{1}{2}+0\times\frac{1}{2}+\frac{1}{2}\right)=\frac{1}{2}. \qquad (28)
\end{aligned}
$$

The man-in-the-middle attack can be detected in the security check process with a probability of $1-(1/2)^{\delta}$, where δ is the number of decoy photons. The probability that Eve is detected is approximate to 1 when δ is sufficiently large. Therefore, the man-in-the-middle attack is invalid. Similarly, the same method can show that Eve cannot derive Bob's qubits by performing the man-in-the-middle attack either.

Case 5 Trojan horse attacks

The Trojan horse attacks mainly include the invisible photon eavesdropping attack and the delay-photon attack.[54] To prevent it, wavelength quantum filters and photon number splitters must be equipped.[16,17] However, the proposed QPC protocol is a one-way communication protocol, the Trojan horse attacks does not work, and it can be prevented automatically.

According to the above analysis, it can be deduced that the proposed protocol possesses good performance in resist outsider attacks.

3.2.2. Participants' attacks

Participants' attacks are more powerful than outsider attacks and the participants have more opportunities and advantages to attack the QPC protocol because they know partial information and can legally utilize this information. Two cases are considered as follows.

Case 1 Security against malicious Alice (Bob)

There is no qubit transmission between Alice and Bob in the proposed QPC protocol except for the secret key θ_i. The decoy photon technology and rotation operation are adopted to guarantee the security of the qubit transmission between Alice (Bob) and TP. Without loss of generality, Alice's role is the same as Bob's. Suppose that Alice intercepts the sequence $\left|\chi_i^{\mathrm{B}}\right\rangle^*$ sent by Bob and then she prepares the corresponding fake sequence to TP. When Bob announces the positions and the corresponding bases of decoy photons, Alice can remove the decoy particles from the intercepted sequence $\left|\chi_i^{\mathrm{B}}\right\rangle^*$ according to the information published by Bob and she can perform rotation operator $R(-\theta_i)$ on $\left|\chi_i^{\mathrm{B}}\right\rangle^*$. However, the sequence $\left|\chi_i^{\mathrm{B}}\right\rangle^*$ is encrypted by θ_i and ω_i, Alice cannot derive Bob's secret qubits without knowing the pre-shared secret key ω_i between TP and Bob. Similarly, Bob cannot infer any information about Alice's privacy either. Therefore, the proposed QPC protocol is secure against malicious Alice (Bob).

Case 2 Security against malicious TP

TP, as a semi-honest third party, is not allowed to conspire with Alice or Bob. Although TP knows $\left|\chi_i^{\mathrm{A}}\right\rangle$ ($\left|\chi_i^{\mathrm{B}}\right\rangle$) that Alice (Bob) sends to her and she can measure $\left|\chi_i^{\mathrm{A}}\right\rangle$ ($\left|\chi_i^{\mathrm{B}}\right\rangle$) directly, she cannot derive Alice's (Bob's) privacy without knowing the secret key θ_i shared between Alice and Bob beforehand. From this perspective, the proposed QPC protocol is secure against malicious TP.

3.3. Comparison

The comparison mainly focuses on the following aspects: quantum state used, quantum measurement, need of entanglement swapping, quantum communication, the technology used and content of comparison. The comparison results between the presented QPC protocol and several representative QPC protocols are shown in Table 1.

Table 1. Comparison results between proposed QPC protocol and several representative QPC protocols.

	Ref. [21]	Ref. [24]	Ref. [26]	Ref. [27]	Ref. [31]	Ref. [44]	The proposed protocol
Quantum state used	Bell states	single particles	single particles	Bell states	Bell states	d-dimensional Bell state	arbitrary single qubit states
Quantum measurement	Bell-basis measurement	$\{\|+\rangle,\|-\rangle,$ $\|+y\rangle,\|-y\rangle\}$ basis measurement	single-particle measurement	Bell-basis measurement	$\{0,1\}$ basis measurement	single-particle measurement	projection measurement
Need of entanglement swapping	No	No	No	Yes	Yes	No	No
Quantum communication	two ways	one way	one way	one way	two ways	one way	one way
Technology used	unitary operations and Hash function	phase plates and Hash function	hash function	entanglement swapping technology	quantum SWAP gate	unitary operations	rotation operations and swap test
Content of comparison	secret integers	secret integers	secret integers	secret integers	secret integers	secret integers	secret qubits and secret integers

Compared with other representative QPC protocols, the propose QPC protocol has many advantages as follows. (i) It provides a new method to compare two participants' qubits and it can compare the equality of two participants' qubits and secret integers. (ii) It does not require any entanglement swapping technology, and it only needs rotation operations and swap test, which is easier to implement with current technology. (iii) It is a one-way communication protocol, and it cannot equip wavelength quantum filters or photon number splitters to resist the Trojan horse attack.

4. Expansibility

4.1. Multi-qubit swap test

To perform swap test on multiple pairs of qubits, (*e.g.* $|\varphi_i\rangle|\phi_i\rangle$, $i=1,2,\ldots,n$), multiple ancilla qubits are used as control qubits to jointly control each qubit pairs $(|\varphi_i\rangle,|\phi_i\rangle)$. For n qubit pairs $(|\varphi_i\rangle,|\phi_i\rangle)$, it takes $k=\lceil\log_2 N\rceil+1$ ancilla qubits. By measuring the probability that each ancilla qubit is in state $|1\rangle$or $|0\rangle$, the square of the inner product of all qubit pairs $(|\varphi_i\rangle,|\phi_i\rangle)$ is obtained. The quantum circuit of multi-qubit swap test is shown in Fig. 2.

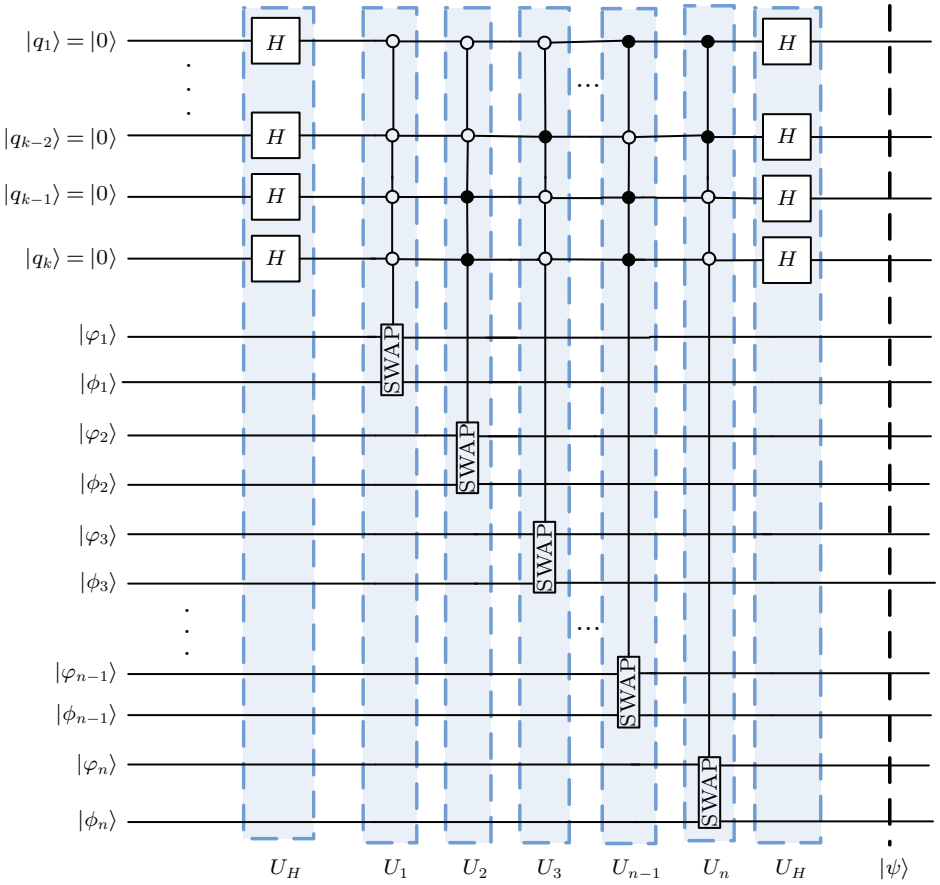


Fig. 2. Quantum circuit of the multi-qubit swap test.

In Fig. 2, the unitary operators corresponding to the quantum circuit of the multi-qubit swap test in each box are shown as follows:

$$\begin{cases} U_H = H^{\otimes k}\otimes I^{\otimes 2n}, \\ U_1 = \left(\text{swap}\oplus I^{\otimes 2}\oplus I^{\otimes 3}\oplus I^{\otimes 4}\oplus\cdots\otimes I^{\otimes(k+1)}\right)\otimes I^{\otimes 2(N-1)},\ldots, \\ U_n = I^{\otimes(2n+k-1)}\oplus\left(\left(I^{\otimes 2(n+1)}\oplus\left(\left(I^{\otimes 2(n-1)}\otimes\text{swap}\right)\oplus I^{\otimes 2n}\oplus I^{\otimes 2(n+1)}\right)\right)\oplus\cdots\right). \end{cases} \tag{29}$$

Let $U=U_HU_nU_{n-1}\ldots U_2U_1U_H$, $M=H^{\otimes k}$, $g(x)=\lceil(x+1)/2\rceil$, $h(x)=2[x+\bmod(x,2)]-3\bmod(x,2)-1$, and $f(x)=(x^2-3x+2)/2$. By performing the multi-qubit swap test on all qubit pairs $(|\varphi_i\rangle,|\phi_i\rangle)$, the output state $|\psi\rangle$ can be written as

$$|\psi\rangle = U|0\rangle^{\otimes(2n+k)} = U_HU_nU_{n-1}\cdots U_2U_1U_H|0\rangle^{\otimes k}\bigotimes_{i=1}^{n}(|\varphi_i\rangle|\phi_i\rangle)$$

$$= \frac{1}{\sqrt{2^k}} \sum_{s=0}^{2^k-1} |s\rangle \left(\begin{array}{l} \sum_{t=0}^{h(n)} M(s+1,t) \bigotimes_{i=1}^{g(t)-1} (|\varphi_i\rangle |\phi_i\rangle) \\ \otimes \mathrm{swap}^{f(\bmod(t,4))} \left(|\varphi_{g(t)}\rangle |\phi_{g(t)}\rangle \right) \bigotimes_{i=g(t)+1}^{n} (|\varphi_i\rangle |\phi_i\rangle) \\ + M(s+1,t) \sum_{t=h(n)+1}^{2^k-1} \bigotimes_{i=1}^{N} (|\varphi_i\rangle |\phi_i\rangle) \end{array} \right). \tag{30}$$

By performing projection measurement on each control qubit $|q_i\rangle$ $(i = 1,2,\ldots,k)$, the probability that all the control qubit reside in state $|1\rangle$ can be written as

$$\begin{aligned} P(|q_i\rangle = |1\rangle) = & \frac{\min\left(n - 2^{k-i-1}\left\lfloor (n-1)/2^{k-i} \right\rfloor, 2^{k-i-1}\left\lceil N/2^{k-i} \right\rceil\right)}{2^k} \\ & - \frac{1}{2^k} \left(\sum_{s=1}^{\lfloor n/2^{k-i} \rfloor} \sum_{t=(s-1)2^{k-i-1}+1}^{(2s-1)2^{k-i-1}} |\langle \varphi_i|\phi_i\rangle|^2 \left| \langle \varphi_{t+2^{k-i-1}}|\phi_{t+2^{k-i-1}}\rangle \right|^2 \right) - \frac{1}{2^k} \left(\sum_{t=\lfloor n/2^{k-i} \rfloor 2^{k-i}+1}^{\min\left(\lfloor n/2^{k-i} \rfloor 2^{k-i}+2^{k-i-1}, n\right)} |\langle \varphi_i|\phi_i\rangle|^2 \right) \\ & - \frac{1}{2^k} \left(\sum_{t=\lfloor n/2^{k-i} \rfloor 2^{k-i}+2^{k-i-1}+1}^{\min\left(\lfloor n/2^{k-i} \rfloor 2^{k-i}+2^{k-i}-1, n\right)} \left| \langle \varphi_{t-2^{k-i-1}}|\phi_{t-2^{k-i-1}}\rangle \right|^2 |\langle \varphi_i|\phi_i\rangle|^2 - \left| \langle \varphi_{t-2^{k-i-1}}|\phi_{t-2^{k-i-1}}\rangle \right|^2 \right). \end{aligned} \tag{31}$$

According to Eq. (31), the probability that $|q_{k-1}\rangle$ and $|q_k\rangle$ stay in state $|1\rangle$ is given by

$$P_0(|q_{k-1}\rangle = |1\rangle) = P(|q_k\rangle = |1\rangle) = \frac{n}{2^k} - \frac{\sum_{i=1}^{n} |\langle \varphi_i|\phi_i\rangle|^2}{2^k}. \tag{32}$$

If n qubit pairs $(|\varphi_i\rangle, |\phi_i\rangle)$ are the same, the measurement result of the ancilla qubit is $|0\rangle$. However, if n qubit pairs $(|\varphi_i\rangle, |\phi_i\rangle)$ are not the same, the measurement result of the ancilla qubit will either be $|0\rangle$ with a probability of

$$\frac{n}{2^k} + \frac{\sum_{i=1}^{n} |\langle \varphi_i|\phi_i\rangle|^2}{2^k}$$

or $|1\rangle$ with a probability of

$$\frac{n}{2^k} - \frac{\sum_{i=1}^{n} |\langle \varphi_i|\phi_i\rangle|^2}{2^k}.$$

Therefore, n qubit pairs $(|\varphi_i\rangle, |\phi_i\rangle)$ are different if the measurement result of the ancilla qubit is $|1\rangle$. We cannot make sure that n qubit pairs $(|\varphi_i\rangle, |\phi_i\rangle)$ are the same if the measurement result of the ancilla qubit is $|0\rangle$. Further, the error probability can be given by

$$P_{\mathrm{e}} \leq \frac{n}{2^k} - \frac{\sum_{i=1}^{n} |\langle \varphi_i|\phi_i\rangle|^2}{2^k}. \tag{33}$$

The error probability of the swap test can be reduced to any $\delta > 0$ by performing the swap test γ times, resulting in an error probability below δ, where $\gamma \in O(\log_2 1/\delta)$.

Theorem 3 Let $|\varphi_i\rangle = \cos\alpha_i |0\rangle + \sin\alpha_i |1\rangle$ and $|\phi_i\rangle = \cos\beta_i |0\rangle + \sin\beta_i |1\rangle$ be arbitrary qubits, and perform the multi-qubit swap test on them, the probability that the ancilla qubit $|q_{k-1}\rangle$ and $|q_k\rangle$ are in state $|1\rangle$ will be

$$\frac{n}{2^k} - \frac{1}{2^k} \left(\sum_{i=1}^{n} \cos^2(\alpha_i - \beta_i) \right).$$

Proof By performing swap test on $|\varphi_i\rangle = \cos\alpha_i |0\rangle + \sin\alpha_i |1\rangle$ and $|\phi_i\rangle = \cos\beta_i |0\rangle + \sin\beta_i |1\rangle$, the probability that the ancilla qubit $|q_{k-1}\rangle$ and $|q_k\rangle$ are in state $|1\rangle$ can be given by

$$\begin{aligned} & P(|q_{k-1}\rangle = |1\rangle) \\ = & P(|q_k\rangle = |1\rangle) = \frac{n}{2^k} - \frac{\sum_{i=1}^{n} |\langle \varphi_i|\phi_i\rangle|^2}{2^k} = \frac{n}{2^k} - \frac{\left(|\langle \varphi_1|\phi_1\rangle|^2 + |\langle \varphi_2|\phi_2\rangle|^2 + \cdots + |\langle \varphi_n|\phi_n\rangle|^2 \right)}{2^k} \\ = & \frac{n}{2^k} - \frac{1}{2^k} \big(|(\cos\alpha_1 \langle 0| + \sin\alpha_1 \langle 1|)(\cos\beta_1 |0\rangle + \sin\beta_1 |1\rangle)|^2 + |(\cos\alpha_2 \langle 0| + \sin\alpha_2 \langle 1|)(\cos\beta_2 |0\rangle + \sin\beta_2 |1\rangle)|^2 \\ & + \cdots + |(\cos\alpha_n \langle 0| + \sin\alpha_n \langle 1|)(\cos\beta_n |0\rangle + \sin\beta_n |1\rangle)|^2 \big) \\ = & \frac{n}{2^k} - \frac{1}{2^k} \left(\cos^2(\alpha_1 - \beta_1) + \cos^2(\alpha_2 - \beta_2) + \cdots + \cos^2(\alpha_n - \beta_n) \right) = \frac{n}{2^k} - \frac{1}{2^k} \left(\sum_{i=1}^{n} \cos^2(\alpha_i - \beta_i) \right). \end{aligned} \tag{34}$$

Theorem 4 Let $R(\theta_i)=\begin{pmatrix}\cos\theta_i & -\sin\theta_i\\ \sin\theta_i & \cos\theta_i\end{pmatrix}$ be the rotation operations, which are used to encrypt $|\varphi_i\rangle$ and $|\phi_i\rangle$ and perform the multi-qubit swap test on the encrypted $|\varphi_i\rangle$ and $|\phi_i\rangle$, then the probability that the ancilla qubit $|q_{k-1}\rangle$ and $|q_k\rangle$ stay in state $|1\rangle$ will be

$$\frac{n}{2^k}-\frac{1}{2^k}\left(\sum_{i=1}^{n}\cos^2(\alpha_i-\beta_i)\right).$$

Proof Using the rotation operation

$$R(\theta_i)=\begin{pmatrix}\cos\theta_i & -\sin\theta_i\\ \sin\theta_i & \cos\theta_i\end{pmatrix}$$

to encrypt $|\varphi_i\rangle$ and $|\phi_i\rangle$ the following equations can be obtained:

$$\begin{aligned}R(\theta_i)|\varphi_i\rangle &= \begin{pmatrix}\cos\theta_i & -\sin\theta_i\\ \sin\theta_i & \cos\theta_i\end{pmatrix}\begin{pmatrix}\cos\alpha_i\\ \sin\alpha_i\end{pmatrix}\\ &= \begin{pmatrix}\cos\theta_i\cos\alpha_i-\sin\theta_i\sin\alpha_i\\ \sin\theta_i\cos\alpha_i+\cos\theta_i\sin\alpha_i\end{pmatrix}\\ &= \begin{pmatrix}\cos(\alpha_i+\theta_i)\\ \sin(\alpha_i+\theta_i)\end{pmatrix}\\ &= \cos(\alpha_i+\theta_i)|0\rangle+\sin(\alpha_i+\theta_i)|1\rangle, \qquad (35)\\ R(\theta_i)|\phi_i\rangle &= \begin{pmatrix}\cos\theta_i & -\sin\theta_i\\ \sin\theta_i & \cos\theta_i\end{pmatrix}\begin{pmatrix}\cos\beta_i\\ \sin\beta_i\end{pmatrix}\\ &= \begin{pmatrix}\cos\theta_i\cos\beta_i-\sin\theta_i\sin\beta_i\\ \sin\theta_i\cos\beta_i+\cos\theta_i\sin\beta_i\end{pmatrix}\\ &= \begin{pmatrix}\cos(\beta_i+\theta_i)\\ \sin(\beta_i+\theta_i)\end{pmatrix}\\ &= \cos(\beta_i+\theta_i)|0\rangle+\sin(\beta_i+\theta_i)|1\rangle. \qquad (36)\end{aligned}$$

By performing the multi-qubit swap test on the encrypted $|\varphi_i\rangle$ and $|\phi_i\rangle$, the probability that the ancilla qubit $|q_{k-1}\rangle$ and $|q_k\rangle$ reside in state $|1\rangle$ can be written as

$$\begin{aligned}P_1(|q_{k-1}\rangle=|1\rangle) &= P(|q_k\rangle=|1\rangle)=\frac{n}{2^k}-\frac{\sum_{i=1}^{n}|\langle R(\theta_i)|\varphi_i\rangle|R(\theta_i)|\phi_i\rangle\rangle|^2}{2^k}\\ &= \frac{n}{2^k}-\frac{\left(|\langle R(\theta_1)|\varphi_1\rangle|R(\theta_1)|\phi_1\rangle\rangle|^2+|\langle R(\theta_2)|\varphi_2\rangle|R(\theta_2)|\phi_2\rangle\rangle|^2+\cdots+|\langle R(\theta_n)|\varphi_n\rangle|R(\theta_n)|\phi_n\rangle\rangle|^2\right)}{2^k}\\ &= \frac{n}{2^k}-\frac{1}{2^k}\big(|(\cos(\alpha_1+\theta_1)\langle 0|+\sin(\alpha_1+\theta_1)\langle 1|)(\cos(\beta_1+\theta_1)|0\rangle+\sin(\beta_1+\theta_1)|1\rangle)|^2\\ &\quad+|(\cos(\alpha_2+\theta_1)\langle 0|+\sin(\alpha_2+\theta_1)\langle 1|)(\cos(\beta_2+\theta_2)|0\rangle+\sin(\beta_2+\theta_2)|1\rangle)|^2\\ &\quad+\cdots+|(\cos\langle 0|+\sin(\alpha_n+\theta_n)\langle 1|)(\cos(\alpha_n+\theta_n)|0\rangle+\sin(\alpha_n+\theta_n)|1\rangle)|^2\big)\\ &= \frac{n}{2^k}-\frac{1}{2^k}\left(\left(\cos^2(\alpha_1-\beta_1)+\cos^2(\alpha_2-\beta_2)+\cdots+\cos^2(\alpha_n-\beta_n)\right)\right)\\ &= \frac{n}{2^k}-\frac{1}{2^k}\left(\sum_{i=1}^{n}\cos^2(\alpha_i-\beta_i)\right). \qquad (37)\end{aligned}$$

According to Theorems 3 and 4, it can be concluded that the same rotation operation $R(\theta_i)$ applied to $|\varphi_i\rangle$ and $|\phi_i\rangle$ does not change the probability that the ancilla qubit $|q_{k-1}\rangle$ and $|q_k\rangle$ stay in state $|1\rangle$ by performing the multi-qubit swap test.

4.2. QPC protocol of arbitrary single qubit states by using multi-qubit swap test

The proposed QPC protocol of arbitrary single qubit states based on the swap test needs to perform i rounds of comparison in the worse condition. To reduce comparison times and perform one comparison, the proposed QPC protocol is extended to the QPC of arbitrary single qubit states by using the multi-qubit swap test. The only difference between these two protocols lies in Step 4. Here, the QPC protocol of arbitrary single qubit states based on the multi-qubit swap test is described. Steps 1–3 are the same as those in the proposed QPC protocol of arbitrary single qubit states based on the swap test.

Step 4* After removing the decoy photons from $\left|\chi_i^{\mathrm{A}}\right\rangle^*\left(\left|\chi_i^{\mathrm{B}}\right\rangle^*\right)$, TP uses the secret key $\gamma_i(\omega_i)$ to decrypt $\left|\chi_i^{\mathrm{A}}\right\rangle\left(\left|\chi_i^{\mathrm{B}}\right\rangle\right)$ to obtain a new sequence $\left|\lambda_i^{\mathrm{A}}\right\rangle\left(\left|\lambda_i^{\mathrm{B}}\right\rangle\right)$ and she performs the multi-qubit swap test on multiple pairs of qubits $\left(\left|\lambda_i^{\mathrm{A}}\right\rangle,\left|\lambda_i^{\mathrm{B}}\right\rangle\right)$ to obtain the measurement result of the ancilla qubit $|q_{k-1}\rangle$ and $|q_k\rangle$.

Step 5* By performing Steps 1–4 γ times, if the measurement results of the ancilla qubit $|q_{k-1}\rangle$ and $|q_k\rangle$ both possess $|1\rangle$, it is indicated that Alice's (Bob's) qubits are different. If the measurement results of the ancilla qubit $|q_{k-1}\rangle$ and $|q_k\rangle$ are both $|0\rangle$, it is implied that Alice's (Bob's) qubits are equal. Finally, TP announces the comparison results to Alice and Bob.

Now we come to discuss the security of the proposed QPC protocol of arbitrary single qubit states based on the multi-qubit swap test. In these two protocols, rotation operations and the decoy particle technology are used to guarantee the security of qubits transmission, and Steps 1–3 in these two protocols are identical. Hence, their security analysis is identical. Security analysis in Subsection 3.2 shows that the proposed QPC of arbitrary single qubit states based on the swap

test can resist both the outsider attacks and the participants' attacks. Therefore, the proposed QPC of arbitrary single qubit states based on the multi-qubit swap test can resist both the outsider attacks and the participants' attacks as well.

5. Conclusions

To sum up, in this paper, by using the swap test, the first quantum private comparison of arbitrary single qubit states is proposed. The participants can compare their secrets by performing the proposed QPC protocol without revealing their private information. In this protocol, Alice and Bob use rotation operations and decoy particle technology to guarantee the security of qubits transmission. Their qubits are encrypted by performing rotation operations and are sent to TP. After the TP performs the swap test on the encrypted qubits, the TP can know whether their secrets are equal and she announces the comparison results to the participants. Additionally, the proposed protocol can compare secret integers as well. It encodes secret integers into the amplitude of quantum state, and the encoded quantum state is compared by performing this protocol. In the process of comparison, TP cannot learn anything about Alice's (Bob's) qubits except the comparison results. The security analysis demonstrates that the proposed QPC protocol is secure against both the outsider attacks and the participants' attacks. Finally, to reduce comparison times, the proposed QPC protocol is extended to the QPC of arbitrary single qubit states by using the multi-qubit swap test.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. 62076042), the Key Research and Development Project of Sichuan Province, China (Grant Nos. 2020YFG0307 and 2021YFSY0012), the Key Research and Development Project of Chengdu Municipality, China (Grant No. 2019-YF05-02028-GX), the Innovation Team of Quantum Security Communication of Sichuan Province, China (Grant No. 17TD0009), and the Academic and Technical Leaders Training Funding Support Projects of Sichuan Province, China (Grant No. 2016120080102643).

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on ComputersSystems and Signal Processing*, Bangalore, India, pp. 175–179
[2] Jiang C, Yu Z W and Wang X B 2016 *Phys. Rev. A* **94** 062323
[3] Bai D Y, Huang P and Zhu Y Q and Ma H X 2020 *Quantum Inf. Process.* **19** 53
[4] Li L L, Li J, Chang Y, Yang Y G and Chen X B 2020 *Sci. China Inf. Sci.* **63** 169501
[5] Yang Y G, Li B R, Li D, Chen X B, Zhou Y H and Shi W M 2019 *Quantum Inf. Process.* **18** 322
[6] Li H H, Gong L H and Zhou N R 2020 *Chin. Phys. B* **29** 110304
[7] Huang X, Zhang S B, Chang Y, Qiu C, Liu D M and Hou M 2021 *Int. J. Theor. Phys.* **60** 838
[8] Zhao D, Xu G, Chen X B, Liu X and Yang X X 2018 *Sci. China Inf. Sci.* **61** 022501
[9] Du Y T and Bao W S 2018 *Chin. Phys. B* **27** 080304
[10] Gao Z K, Li T and Li Z H 2020 *Sci. China Phys. Mech. Astron.* **63** 120311
[11] Wang T Y, Wang X X and Cai X Q, Wei C Y and Zhang R L 2021 *Quantum Inf. Process.* **20** 7
[12] Liu L, Niu J L and Fan C R and Feng X T 2020 *Quantum Inf. Process.* **19** 404
[13] Zhou Z R, Sheng Y B, Niu P H, Yin L G, Long G L and Hanzo L 2020 *Sci. China Phys. Mech. Astron.* **63** 230362
[14] Rong Z B, Qiu D. W, Mateus P and Zou X F 2021 *Quantum Inf. Process.* **20** 58
[15] Gao X, Chang Y, Zhang S B, Yang F and Zhang Y 2018 *Int. J. Theor. Phys.* **57** 1983
[16] Chang Y, Zhang S B, Wan G, Yan L L, Zhang Y and L X Y 2019 *Int. J. Theor. Phys.* **58** 2069
[17] Zheng T, Zhang S B, Gao X and Yan C 2019 *Mod. Phys. Lett. A* **34** 1950196
[18] Liu D M, Yan L L, Xu S H, Qiu C and Huang X 2021 *Quantum Inf. Process* **20** 49
[19] Yao A C 1982 *Proceedings of 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82)*, Washington, DC, USA, p. 160
[20] Boudot F, Schoenmakers B and Traore J 2001 *Discrete Appl. Math.* **111** 23
[21] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305
[22] Yang Y G, Cao W F and Wen Q Y 2009 *Phys. Script.* **80** 065002
[23] Yang Y G, Xia J, Jia X, Shi L and Zhang H 2012 *Int. J. Quantum Inf.* **10** 1250065
[24] Liu B, Gao F, Jia H Y, Huang W, Zhang W W and Wen Q Y 2013 *Quantum Inf. Process.* **12** 887
[25] Chen X B, Su Y, Niu X X and Yang Y X 2014 *Quantum Inf. Process.* **13** 101
[26] He G P 2016 *Int. J. Quantum Inf.* **15** 1750014
[27] Wen L, Wang Y B and Wei C 2012 *Commun. Theor. Phys.* **57** 583
[28] Tseng H Y, Lin J and Hwang T 2012 *Quantum Inf. Process.* **11** 373
[29] Yan L L, Zhang S B, Chang Y, Sheng Z W and Sun Y H 2019 *Int. J. Theor. Phys.* **58** 3852
[30] Jiang L Z 2020 *Quantum Inf. Process.* **19** 1
[31] Wang F, Luo M X, Li H R, Qu Z G and Wang X J 2016 *Sci. China Inf. Sci.* **59** 112501
[32] Chen X B, Xu G, Niu X X, Wen Q Y and Yang Y X 2010 *Opt. Commun.* **283** 1561
[33] Lin S, Guo G D and Liu X F 2013 *Int. J. Theor. Phys.* **52** 4185
[34] Ji Z X and Ye T Y 2016 *Commun. Theor. Phys.* **65** 711
[35] Ye T Y and Ji Z X 2017 *Int. J. Theor. Phys.* **56** 1517
[36] Ji Z X, Zhang H G and Wang H Z 2019 *IEEE Access* **7** 44613
[37] Ji Z X, Zhang H G and Fan P R 2019 *Mod. Phys. Lett. A* **34** 1950229
[38] Xu G A, Chen X B and Wei Z H, Li M J and Yang Y X 2012 *Int. J. Quantum. Inf.* **10** 1250045
[39] Sun Z W and Long D Y 2013 *Int. J. Theor. Phys.* **52** 212
[40] Chang Y, Zhang W B, Zhang S B, Wang H C, Yan L L, Han G H, Sheng Z W, Huang Y Y, Suo W and Xiong J X 2016 *Commun. Theor. Phys.* **66** 621
[41] Zha X W, Yu X Y. Cao Y and Wang S K 2018 *Int. J. Theor. Phys.* **57** 3874
[42] Li C, Chen X B, Li H, Yang Y G and Li J 2019 *Quantum Inf. Process.* **18** 158
[43] Lo H K 1997 *Phys. Rev. A* **56** 1154
[44] Lin S, Sun Y, Liu X F and Yao Z Q 2013 *Quantum Inf. Process.* **12** 559
[45] Guo F Z, Gao F, Qin S J, Zhang J and Wen Q Y 2013 *Quantum Inf. Process.* **12** 2793
[46] Yu C H, Guo G D and Lin S 2013 *Phys. Scripta* **88** 065013
[47] Ye C Q and Ye T Y 2018 *Quantum Inf. Process.* **17** 252
[48] Song X L, Wen A J and Gou R 2019 *IEEE Access* **7** 142507
[49] Buhrman H, Cleve R Watrous J and Wolf R 2001 *Phys. Rev. Lett.* **87** 167902
[50] Kang M S, Choi H W, Pramanik T, Han S W and Moon S 2018 *Quantum Inf. Process.* **17** 254
[51] Zhao J, Zhang Y H, Shao C P, Wu Y C, Guo G C and Guo G P 2019 *Phys. Rev. A* **100** 012334
[52] Shao C 2020 *Quantum Inf. Process.* **19** 102
[53] Li P C and Wang B 2020 *Neural Networks* **130** 152
[54] Li Z H, Wang L J, Xu J P, Yang Y P, M Al-Amri and M Zubairy 2020 *Phys. Rev. A* **101** 022336