

Efficient quantum private comparison protocol utilizing single photons and rotational encryption

Tian-Yi Kou(寇天翊), Bi-Chen Che(车碧琛), Zhao Dou(窦钊), Xiu-Bo Chen(陈秀波), Yu-Ping Lai(赖裕平), and Jian Li(李剑)

Citation: Chin. Phys. B, 2022, 31 (**6**): 060307. DOI: 10.1088/1674-1056/ac65f0
Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

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

Efficient quantum private comparison protocol utilizing single photons and rotational encryption

Tian-Yi Kou(寇天翊), Bi-Chen Che(车碧琛), Zhao Dou(窦钊), Xiu-Bo Chen(陈秀波), Yu-Ping Lai(赖裕平), and Jian Li(李剑)
Chin. Phys. B, 2022, 31 (**6**): 060307. DOI: 10.1088/1674-1056/ac65f0

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)
Chin. Phys. B, 2022, 31 (**4**): 040303. DOI: 10.1088/1674-1056/ac4103

Channel parameters-independent multi-hop nondestructive teleportation

Hua-Yang Li(李华阳), Yu-Zhen Wei(魏玉震), Yi Ding(丁祎), and Min Jiang(姜敏)
Chin. Phys. B, 2022, 31 (**2**): 020302. DOI: 10.1088/1674-1056/ac1330

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

Optimal entanglement concentration for three-photon W states with parity check measurement

Zhou Lan, Sheng Yu-Bo, Zhao Sheng-Mei
Chin. Phys. B, 2013, 22 (**2**): 020307. DOI: 10.1088/1674-1056/22/2/020307

Efficient quantum private comparison protocol utilizing single photons and rotational encryption

Tian-Yi Kou(寇天翊)[1], Bi-Chen Che(车碧琛)[1], Zhao Dou(窦钊)[1,†], Xiu-Bo Chen(陈秀波)[1], Yu-Ping Lai(赖裕平)[2], and Jian Li(李剑)[2]

[1] *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[2] *Information Security Center, School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

(Received 7 February 2022; revised manuscript received 7 April 2022; accepted manuscript online 11 April 2022)

As a branch of quantum secure multiparty computation, quantum private comparison is applied frequently in many fields, such as secret elections, private voting, and identification. A quantum private comparison protocol with higher efficiency and easier implementation is proposed in this paper. The private secrets are encoded as single polarized photons and then encrypted with a homomorphic rotational encryption method. Relying on this method and the circular transmission mode, we implement the multiplexing of photons, raising the efficiency of our protocol to 100%. Our protocol is easy to realize since only single photons, unitary operation, and single-particle measurement are introduced. Meanwhile, the analysis shows that our protocol is also correct and secure.

Keywords: quantum private comparison, rotational encryption, polarized single photons, efficiency

PACS: 03.67.Dd, 03.67.Hk, 03.67.Ac **DOI:** 10.1088/1674-1056/ac65f0

1. Introduction

Secure multiparty computation (SMPC) problems are cryptographic tasks that enable joint computation using private input from all parties without revealing them. In the traditional secure two-party computation scenario, Alice, who has secret input x, and Bob, who has secret input y, are willing to calculate $f(x,y)$. The origin of SMPC problems can be traced back to Yao's millionaire problem,[1] where two millionaires try to compare who is richer without information leaking. Based on Yao's research, a variant of the millionaire problem named the socialist millionaire problem[2,3] was proposed. On this condition, two millionaires wish to compare whether they are equally rich. However, Lo[4] pointed out that constructing an equality function with only two-party is not secure. Thus, a semi-honest third party (TP) should exist to complete the task.

With the advancement of quantum mechanics, laws such as the Heisenberg uncertainty principle and the quantum no-cloning theorem were discovered. They endow quantum computing with absolute security. With this advantage, a huge number of quantum cryptography protocols have been proposed to solve cryptography challenges, embracing quantum secure direct communication (QSDC),[5–8] quantum secret sharing (QSS),[9–12] and quantum key distribution (QKD),[13–17] as well as quantum secure multiparty computation (QSMPC),[18–24] *etc.*

As one essential type of QSMPC, quantum private comparison (QPC) has gotten much attention. In QPC protocols, the purpose of participants is to determine whether the respective secrets are equal. According to the number of participants, the types of QPC protocols can be divided into two-party and multi-party. The two-party QPC protocols are taken for example. The inputs are their secrets x and y. The output is $x = y$ or $x \neq y$. Yang and Wen[18] proposed the first QPC protocol with a dishonest TP. Two parties compare their secrets based on decoy photons and EPR pairs, and the one-way hash function ensures the security of the protocol. Before long, Chen *et al.*[19] introduced a more efficient QPC protocol based on triplet entangled states and single-particle measurement. Then, Tseng *et al.*[20] proposed a QPC protocol with EPR pairs, facilitating implementation and improving qubit efficiency to 50%. After that, Jia *et al.*[21] suggested another QPC protocol based on χ-type genuine four-particle entangled states, whose efficiency is equal to 100%. In 2014, Chen *et al.*[22] proposed a protocol using a class of maximally entangled states as the information carriers. The implementation of this protocol can rely on a variety of particles, so it has more freedom in selecting quantum states than all prior protocols. To further improve efficiency, Xu *et al.*[25] proposed a QPC protocol based on four-particle GHZ states. Three secret bits can be compared at one time, which reduces the rounds of the protocol. In addition, some participants without quantum capabilities were considered by Chou *et al.*[26] in their QPC protocol firstly. Such protocols are called semi-quantum private comparison (SQPC) protocols. They are closer to reality because some participants may not be able to afford quantum equipment. Recently, Zhou *et al.*[27] and Wang *et al.*[28] proposed SQPC protocols with d-dimensional Bell states and

†Corresponding author. E-mail: dou@bupt.edu.cn

© 2022 Chinese Physical Society and IOP Publishing Ltd

GHZ states, respectively, improving efficiency and ensuring security.

After analyzing existing QPC protocols, we observe the extensive utilization of entangled states. However, some unfavorable conditions, such as the difficulty in preparing entangled states[29] and the security vulnerabilities,[30] limit the application of entangled states. Thus, protocols based on single photons have received widespread attention.[31–34] As a significant method to ensure the correctness and security of single-photon based protocols, rotational encryption is introduced in various types of quantum protocols, such as quantum key exchange,[35] quantum designated verifier signature,[36] quantum image encryption,[37] *etc.* Additionally, rotational encryption can be applied to design QPC protocols[38,39] because the mapping of rotational encryption is homomorphic.

In this paper, we propose an efficient QPC protocol with polarized single photons, which is efficient and easy to realize. In our protocol, two players encrypt their secret integers with rotational encryption and single photons, and then they can privately compare their secrets with a semi-honest TP, who may misbehave alone but cannot conspire with other players.[40–43] The TP should initialize a quantum sequence at the beginning of the protocol and decrypt it at the end of the protocol. Two players' core operation is encoding the secret into the quantum sequence.

In comparison to existing QPC protocols, our protocol provides the following advantages. First, without pre-shared keys, the qubit efficiency of our protocol is 100% on account of the application of the circular transmission mode.[44,45] In this mode, the photons will be transmitted along the circular path TP-player1-player2-TP. Second, our protocol has simple technical requirements. The complex technology, such as entangled states, joint measurement, and entanglement swapping, are replaced by single photons, single-particle measurement, and unitary operation. As a consequence, the efficiency of our protocol achieves the theoretical maximum, and our protocol is easy to realize.

The rest of this paper is organized as follows. In Section 2, the encryption and decryption method with the rotational encryption is elaborated as a core. In Section 3, we propose a new QPC protocol. In Section 4, the correctness, security, and efficiency are analyzed. In Section 5, we compare our protocol with others and discuss its extended application. In Section 6, we summarize the characteristics of the protocol.

2. The encryption and decryption method of the protocol

The encryption and decryption method with the rotational encryption is the core of our protocol. The classical binary data "0" can be encoded to the horizontally polarized photon $|0\rangle$, and the classical binary data "1" can be encoded to the vertically polarized photon $|1\rangle$.

The rotational encryption operator, drawing support from Jones matrix,[46] can be expressed in the following form:

$$R(\theta)=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}. \tag{1}$$

The symbol $E_K[|\varphi\rangle]$ represents the process of encryption with the photon $|\varphi\rangle$ and the rotation angle $K\in[0,2\pi)$ that acts as a key. Similarly, the decryption process is described by the symbol $D_K[|\varphi\rangle]$. Suppose a binary message $P=0$ is encoded to $|\varphi\rangle=|0\rangle$, and the key is θ. Then the encrypted $|\varphi'\rangle$ can be represented as follows:

$$\begin{aligned}|\varphi'\rangle=E_\theta[|\varphi\rangle]=R(\theta)|\varphi\rangle&=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\\&=\begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}=\cos\theta|0\rangle+\sin\theta|1\rangle.\end{aligned} \tag{2}$$

After encryption, the original polarization of $|\varphi\rangle$ is disguised. As for decryption, we only need to change the key θ to $-\theta$. $|\varphi'\rangle$ is taken for example:

$$\begin{aligned}&D_\theta[|\varphi'\rangle]=R(-\theta)|\varphi'\rangle\\&=\begin{pmatrix}\cos(-\theta) & -\sin(-\theta)\\ \sin(-\theta) & \cos(-\theta)\end{pmatrix}\begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}\\&=\begin{pmatrix}1\\0\end{pmatrix}=|0\rangle=|\varphi\rangle.\end{aligned} \tag{3}$$

This encryption and decryption method has two features.

Lemma 1 The mapping $\theta\to R(\theta)$ is homomorphic, *i.e.*,

$$\prod_{i=1}^{n}R(\theta_i)=R\left(\sum_{j=1}^{n}\theta_j\right), \tag{4}$$

for $n=2,3,4,\ldots$

Proof When $n=2$,

$$\begin{aligned}R(\theta_1)R(\theta_2)&=\begin{pmatrix}\cos\theta_1 & -\sin\theta_1\\ \sin\theta_1 & \cos\theta_1\end{pmatrix}\begin{pmatrix}\cos\theta_2 & -\sin\theta_2\\ \sin\theta_2 & \cos\theta_2\end{pmatrix}\\&=\begin{pmatrix}\cos(\theta_1+\theta_2) & -\sin(\theta_1+\theta_2)\\ \sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2)\end{pmatrix}\\&=R(\theta_1+\theta_2).\end{aligned} \tag{5}$$

Thus, Lemma 1 holds when $n=2$.

We assume that

$$\prod_{i=1}^{k}R(\theta_i)=R\left(\sum_{j=1}^{k}\theta_j\right)$$

when $n=k$, $k=2,3,4,\ldots$

From this hypothesis, when $n=k+1$,

$$\begin{aligned}\prod_{i=1}^{k+1}R(\theta_i)&=\left(\prod_{i=1}^{k}R(\theta_i)\right)R(\theta_{k+1})\\&=R\left(\sum_{j=1}^{k}\theta_j\right)R(\theta_{k+1})\end{aligned}$$

$$= R\left(\left(\sum_{j=1}^{k}\theta_j\right)+\theta_{k+1}\right)$$
$$= R\left(\sum_{j=1}^{k+1}\theta_j\right). \quad (6)$$

Hence, Lemma 1 holds when $n=k+1$.

In summary, we prove the correctness of

$$\prod_{i=1}^{n}R(\theta_i)=R\left(\sum_{j=1}^{n}\theta_j\right),\quad n=2,3,4,\ldots$$

Owing to this feature, we can ignore the order of each key if the data are encrypted more than once. For this reason, we can simply add all the keys as a new key and then perform the decryption operation only once.

Lemma 2 The following equation holds:

$$R(\theta)|\alpha\oplus\beta\rangle = E_{(\pi/2)\alpha+(\pi/2)\beta}\left[R(\theta)|0\rangle\right], \quad (7)$$

for $\alpha,\beta\in\{0,1\}$.

Proof We can transform $E_{(\pi/2)\alpha+(\pi/2)\beta}\left[R(\theta)|0\rangle\right]$ as follows:

$$E_{(\pi/2)\alpha+(\pi/2)\beta}\left[R(\theta)|0\rangle\right] = R\left(\frac{\pi}{2}\alpha+\frac{\pi}{2}\beta\right)\left[R(\theta)|0\rangle\right]$$
$$= R(\theta)\left[R\left(\frac{\pi}{2}\alpha+\frac{\pi}{2}\beta\right)|0\rangle\right]. \quad (8)$$

The relationship among α, β, $\alpha\oplus\beta$, $|\alpha\oplus\beta\rangle$, and $R((\pi/2)\alpha+(\pi/2)\beta)|0\rangle$ is shown in Table 1.

Table 1. The relationship among α, β, $\alpha\oplus\beta$, $|\alpha\oplus\beta\rangle$, and $R((\pi/2)\alpha+(\pi/2)\beta)|0\rangle$.

α	β	$\alpha\oplus\beta$	$\lvert\alpha\oplus\beta\rangle$	$R((\pi/2)\alpha+(\pi/2)\beta)\lvert0\rangle$
0	0	0	$\lvert0\rangle$	$\lvert0\rangle$
0	1	1	$\lvert1\rangle$	$\lvert1\rangle$
1	0	1	$\lvert1\rangle$	$\lvert1\rangle$
1	1	0	$\lvert0\rangle$	$\lvert0\rangle$

From Table 1, we can discover that $|\alpha\oplus\beta\rangle$ and $R((\pi/2)\alpha+(\pi/2)\beta)|0\rangle$ are always equal. Thus,

$$R(\theta)|\alpha\oplus\beta\rangle = R(\theta)\left[R((\pi/2)\alpha+(\pi/2)\beta)|0\rangle\right]$$
$$= E_{(\pi/2)\alpha+(\pi/2)\beta}\left[R(\theta)|0\rangle\right]. \quad (9)$$

The Lemma 2 follows.

It means that $R(\theta)|\alpha\oplus\beta\rangle$ can be expressed as the form $E_{(\pi/2)\alpha+(\pi/2)\beta}\left[R(\theta)|0\rangle\right]$, *i.e.*, we can realize the bitwise XOR operation with the rotational encryption.

3. The two-party quantum private comparison protocol

There are two distrustful players, Alice and Bob, who want to compare whether their secrets are equal with the aid of a semi-honest TP named Charlie.

It is supposed Alice and Bob hold private integers $N_{\rm A}$ and $N_{\rm B}$, respectively. Alice converts her secret $N_{\rm A}$ to an n-bit string $N_{{\rm A},n-1}\ldots N_{{\rm A},1}N_{{\rm A},0}$ meeting the condition $N_{\rm A}=\sum_{i=0}^{n-1}2^iN_{{\rm A},i}$. Similarly, Bob transforms his $N_{\rm B}$ to an n-bit string $N_{{\rm B},n-1}\ldots N_{{\rm B},1}N_{{\rm B},0}$.

Step 1 Charlie initializes an n-length single quantum sequence S filled by $|0\rangle$ and generates his secret key $K_{\rm C}=\{k_{{\rm C},i}:0\le k_{{\rm C},i}<2\pi, i=n-1,\ldots,1,0\}$. After that, he obtains $S_{\rm init}$ by operating on S as follows:

$$S_{\rm init}=\left\{\left|\varphi_{{\rm init},i}\right\rangle:\left|\varphi_{{\rm init},i}\right\rangle=E_{k_{{\rm C},i}}\left[|0\rangle\right], i=n-1,\ldots,1,0\right\}. \quad (10)$$

Step 2 Charlie chooses m photons from $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ as decoy photons randomly. Then he inserts them into $S_{\rm init}$ randomly and records their states and locations. After that, he sends the new $(m+n)$-length sequence $S'_{\rm init}$ to Alice.

Step 3 After confirming that Alice has received $S'_{\rm init}$, Charlie announces the locations and measurement bases. For $|0\rangle$ or $|1\rangle$, Alice's measurement basis is Z-basis. For $|+\rangle$ or $|-\rangle$, it is X-basis. Charlie and Alice can find the existence of an eavesdropper and reboot this protocol if the error rate exceeds the agreed threshold. If not, Alice discards the photons inserted in Step 2 and then executes Step 4.

Step 4 Alice generates her secret key $K_{\rm A}=\{k_{{\rm A},i}:0\le k_{{\rm A},i}<2\pi, i=n-1,\ldots,1,0\}$ randomly. Then she gets $S_{\rm A}$ by handling $S_{\rm init}$ with her binary string $N_{{\rm A},n-1}\ldots N_{{\rm A},1}N_{{\rm A},0}$ and the key $K_{\rm A}$. The process can be written in the following form:

$$S_{\rm A}=\left\{\left|\varphi_{{\rm A},i}\right\rangle:\left|\varphi_{{\rm A},i}\right\rangle=E_{(\pi/2)N_{{\rm A},i}+k_{{\rm A},i}}\left[\left|\varphi_{{\rm init},i}\right\rangle\right], i=n-1,\ldots,1,0\right\}. \quad (11)$$

Step 5 Similar to Step 2 and Step 3, Alice inserts decoy photons, sends the sequence to Bob, and executes an eavesdropping check with Bob. If they find the eavesdropper, the protocol will be restarted.

Step 6 Bob performs what Alice does in Step 4. He generates the key $K_{\rm B}$ randomly and uses his key and private binary to acquire $S_{\rm B}$:

$$S_{\rm B}=\left\{\left|\varphi_{{\rm B},i}\right\rangle:\left|\varphi_{{\rm B},i}\right\rangle=E_{(\pi/2)N_{{\rm B},i}+k_{{\rm B},i}}\left[\left|\varphi_{{\rm A},i}\right\rangle\right], i=n-1,\ldots,1,0\right\}. \quad (12)$$

Bob starts the eavesdropping check with Charlie when $S_{\rm B}$ is received by Charlie, which is similar to Step 5.

Step 7 Alice and Bob announce their keys $K_{\rm A}$ and $K_{\rm B}$, and then Charlie logs them.

Step 8 Charlie decrypts $S_{\rm B}$ with his private key $K_{\rm C}$ and the published keys $K_{\rm A}$, $K_{\rm B}$. He computes $S_{\rm C}$ adhering to the following rule:

$$S_{\rm C}=\left\{|\varphi_{{\rm C},i}\rangle:|\varphi_{{\rm C},i}\rangle=D_{k_{{\rm A},i}+k_{{\rm B},i}+k_{{\rm C},i}}\left[|\varphi_{B,i}\rangle\right],i=n-1,\ldots,1,0\right\}. \tag{13}$$

He calculates the result string $N_{\rm C}=N_{{\rm C},n-1}\ldots N_{{\rm C},1}N_{{\rm C},0}$ from $S_{\rm C}$ with the following regulation:

$$N_{{\rm C},i}=\begin{cases}0,\ |\varphi_{{\rm C},i}\rangle=|0\rangle,\\ 1,\ |\varphi_{{\rm C},i}\rangle=|1\rangle.\end{cases} \tag{14}$$

Charlie knows $N_{\rm A}\neq N_{\rm B}$ if he gets a result $N_{{\rm C},i}=1$ or $N_{\rm A}=N_{\rm B}$ if he gains an all-zero string $N_{{\rm C},n-1}\ldots N_{{\rm C},1}N_{{\rm C},0}$. Then he broadcasts the result.

4. Analysis

In this section, we shall demonstrate the correctness and security of our proposed protocol.

4.1. Correctness

In this subsection, we give a general proof of the correctness of the protocol. In our analysis, decoy photons are ignored since they are only applied to detect eavesdroppers.

For any $|\varphi_{{\rm C},i}\rangle$ in $S_{\rm C}$, we can rewrite it into the following form according to the operation rules of Alice, Bob, and Charlie:

$$\begin{aligned}|\varphi_{{\rm C},i}\rangle &= R\left(-k_{{\rm A},i}-k_{{\rm B},i}-k_{{\rm C},i}\right)|\varphi_{{\rm B},i}\rangle\\ &= R\left(-k_{{\rm A},i}-k_{{\rm B},i}-k_{{\rm C},i}\right)\\ &\quad\times R\left(\frac{\pi}{2}N_{{\rm B},i}+k_{{\rm B},i}\right)|\varphi_{{\rm A},i}\rangle\\ &= R\left(-k_{{\rm A},i}-k_{{\rm B},i}-k_{{\rm C},i}\right)R\left(\frac{\pi}{2}N_{{\rm B},i}+k_{{\rm B},i}\right)\\ &\quad\times R\left(\frac{\pi}{2}N_{{\rm A},i}+k_{{\rm A},i}\right)|\varphi_{{\rm init},i}\rangle\\ &= R\left(-k_{{\rm A},i}-k_{{\rm B},i}-k_{{\rm C},i}\right)R\left(\frac{\pi}{2}N_{{\rm B},i}+k_{{\rm B},i}\right)\\ &\quad\times R\left(\frac{\pi}{2}N_{{\rm A},i}+k_{{\rm A},i}\right)R\left(k_{{\rm C},i}\right)|0\rangle.\end{aligned} \tag{15}$$

According to Lemma 1, we can combine the four Jones matrices[46] in the equation

$$|\varphi_{{\rm C},i}\rangle=R\left(-k_{{\rm A},i}-k_{{\rm B},i}-k_{{\rm C},i}+\frac{\pi}{2}N_{{\rm B},i}+k_{{\rm B},i}+\frac{\pi}{2}N_{{\rm A},i}+k_{{\rm A},i}+k_{{\rm C},i}\right)|0\rangle=R\left(\frac{\pi}{2}N_{{\rm B},i}+\frac{\pi}{2}N_{{\rm A},i}\right)|0\rangle. \tag{16}$$

Then we can infer that $|\varphi_{{\rm C},i}\rangle=|N_{{\rm A},i}\oplus N_{B,i}\rangle$ in the light of Lemma 2.

For simplicity, the string $N_{{\rm A},n-1}\oplus N_{{\rm B},n-1},\ldots,N_{{\rm A},1}\oplus N_{{\rm B},1},N_{{\rm A},0}\oplus N_{{\rm B},0}$ will be recorded in $N_{\rm A}\oplus N_{\rm B}$. Obviously, $N_{\rm C}=N_{\rm A}\oplus N_{\rm B}$ holds based on Eq. (14). For this reason, an all-zero $N_{\rm C}$ represents that $N_{\rm A}=N_{\rm B}$, and other cases signify that $N_{\rm A}\neq N_{\rm B}$. Thus, TP can determine the comparison result by figuring the string $N_{\rm C}$.

4.2. Security analysis

We analyze the security of our proposed protocol. Firstly, we prove that our protocol can resist outside attacks. Secondly, we show that inside attacks are ineffective to our protocol.

4.2.1. Outside attack

Suppose Eve is the outside attacker. She cannot discover the difference between target and decoy photons. Therefore, she has to implement the same operation $U_{\rm E}$ to all of them. Her most general operation is to induce the sample photons to interact coherently with an auxiliary quantum system $|\varphi^{\rm E}\rangle$. Hence, her behavior can be expressed as Eq. (17):

$$\begin{cases}U_{\rm E}|0\rangle|\varphi^{\rm E}\rangle=a_0|0\rangle|\varphi^{\rm E}_{00}\rangle+b_0|1\rangle|\varphi^{\rm E}_{01}\rangle,\\ U_{\rm E}|1\rangle|\varphi^{\rm E}\rangle=a_1|0\rangle|\varphi^{\rm E}_{10}\rangle+b_1|1\rangle|\varphi^{\rm E}_{11}\rangle.\end{cases} \tag{17}$$

Obviously, $|a_i|^2+|b_i|^2=1$ $(i=0,1)$. If Eve does not introduce an error in the eavesdropping check, the overall operation must meet the following requirements:

$$\begin{cases}U_{\rm E}|+\rangle|\varphi^{\rm E}\rangle=|+\rangle|\varphi^{\rm E}_{+}\rangle,\\ U_{\rm E}|-\rangle|\varphi^{\rm E}\rangle=|-\rangle|\varphi^{\rm E}_{-}\rangle,\\ U_{\rm E}|0\rangle|\varphi^{\rm E}\rangle=|0\rangle|\varphi^{\rm E}_{0}\rangle,\\ U_{\rm E}|1\rangle|\varphi^{\rm E}\rangle=|1\rangle|\varphi^{\rm E}_{1}\rangle.\end{cases} \tag{18}$$

Taking the $U_{\rm E}|+\rangle|\varphi^{\rm E}\rangle=|+\rangle|\varphi^{\rm E}_{+}\rangle$ as an example, we can expand it on both sides in this way:

$$\begin{aligned}&U_{\rm E}|+\rangle|\varphi^{\rm E}\rangle=|+\rangle|\varphi^{\rm E}_{+}\rangle,\\ \Rightarrow\ &\frac{1}{\sqrt{2}}U_{\rm E}|0\rangle|\varphi^{\rm E}\rangle+\frac{1}{\sqrt{2}}U_{\rm E}|1\rangle|\varphi^{\rm E}\rangle\\ &=\frac{1}{\sqrt{2}}|0\rangle|\varphi^{\rm E}_{+}\rangle+\frac{1}{\sqrt{2}}|1\rangle|\varphi^{\rm E}_{+}\rangle,\\ \Rightarrow\ &\frac{1}{\sqrt{2}}\left(a_0|0\rangle|\varphi^{\rm E}_{00}\rangle+b_0|1\rangle|\varphi^{\rm E}_{01}\rangle\right)\\ &+\frac{1}{\sqrt{2}}\left(a_1|0\rangle|\varphi^{\rm E}_{10}\rangle+b_1|1\rangle|\varphi^{\rm E}_{11}\rangle\right)\\ &=\frac{1}{\sqrt{2}}|0\rangle|\varphi^{\rm E}_{+}\rangle+\frac{1}{\sqrt{2}}|1\rangle|\varphi^{\rm E}_{+}\rangle,\end{aligned}$$

$$
\begin{aligned}
&\Rightarrow \frac{1}{\sqrt{2}}|0\rangle\left(a_0\left|\varphi_{00}^{\mathrm{E}}\right\rangle+a_1\left|\varphi_{10}^{\mathrm{E}}\right\rangle-\left|\varphi_{+}^{\mathrm{E}}\right\rangle\right)\\
&\quad+\frac{1}{\sqrt{2}}|1\rangle\left(b_0\left|\varphi_{01}^{\mathrm{E}}\right\rangle+b_1\left|\varphi_{11}^{\mathrm{E}}\right\rangle-\left|\varphi_{+}^{\mathrm{E}}\right\rangle\right)=\mathbf{0},\\
&\Rightarrow \begin{cases} a_0\left|\varphi_{00}^{\mathrm{E}}\right\rangle+a_1\left|\varphi_{10}^{\mathrm{E}}\right\rangle-\left|\varphi_{+}^{\mathrm{E}}\right\rangle=\mathbf{0}, \\ b_0\left|\varphi_{01}^{\mathrm{E}}\right\rangle+b_1\left|\varphi_{11}^{\mathrm{E}}\right\rangle-\left|\varphi_{+}^{\mathrm{E}}\right\rangle=\mathbf{0}. \end{cases}
\end{aligned}
\tag{19}
$$

Here, $\mathbf{0}$ denotes a column zero vector. For the same reason, we can infer

$$
\begin{cases}
a_0\left|\varphi_{00}^{\mathrm{E}}\right\rangle+a_1\left|\varphi_{10}^{\mathrm{E}}\right\rangle-\left|\varphi_{+}^{\mathrm{E}}\right\rangle=\mathbf{0}, \\
b_0\left|\varphi_{01}^{\mathrm{E}}\right\rangle+b_1\left|\varphi_{11}^{\mathrm{E}}\right\rangle-\left|\varphi_{+}^{\mathrm{E}}\right\rangle=\mathbf{0}, \\
a_0\left|\varphi_{00}^{\mathrm{E}}\right\rangle-a_1\left|\varphi_{10}^{\mathrm{E}}\right\rangle-\left|\varphi_{-}^{\mathrm{E}}\right\rangle=\mathbf{0}, \\
b_0\left|\varphi_{01}^{\mathrm{E}}\right\rangle-b_1\left|\varphi_{11}^{\mathrm{E}}\right\rangle+\left|\varphi_{-}^{\mathrm{E}}\right\rangle=\mathbf{0}, \\
a_0\left|\varphi_{00}^{\mathrm{E}}\right\rangle-\left|\varphi_{0}^{\mathrm{E}}\right\rangle=\mathbf{0}, \\
b_0\left|\varphi_{01}^{\mathrm{E}}\right\rangle=\mathbf{0}, \\
a_1\left|\varphi_{10}^{\mathrm{E}}\right\rangle=\mathbf{0}, \\
b_1\left|\varphi_{11}^{\mathrm{E}}\right\rangle-\left|\varphi_{1}^{\mathrm{E}}\right\rangle=\mathbf{0}.
\end{cases}
\tag{20}
$$

Then we can deduce the following results: $\left|\varphi_{00}^{\mathrm{E}}\right\rangle=\left|\varphi_{11}^{\mathrm{E}}\right\rangle=\left|\varphi_{0}^{\mathrm{E}}\right\rangle=\left|\varphi_{1}^{\mathrm{E}}\right\rangle$, $a_1=b_0=0$ and $a_0=b_1=1$ from Eq. (20). Substituting these results into Eq. (17), we gain the following Eq. (21):

$$
\begin{aligned}
U_{\mathrm{E}}|0\rangle\left|\varphi^{\mathrm{E}}\right\rangle&=|0\rangle\left|\varphi_{00}^{\mathrm{E}}\right\rangle,\\
U_{\mathrm{E}}|1\rangle\left|\varphi^{\mathrm{E}}\right\rangle&=|1\rangle\left|\varphi_{00}^{\mathrm{E}}\right\rangle,
\end{aligned}
\tag{21}
$$

i.e., Eve cannot distinguish $\{|0\rangle,|1\rangle\}$ without introducing errors. Once an error exists, it will be found in the eavesdropping check. Then the protocol will be restarted without information disclosure, so Eve's attack will never succeed.

Some special cases of the above attack, such as measurement-resend attack, intercept-resend attack, and entanglement-measurement attack, can be discovered in eavesdropping check.[47]

4.2.2. Inside attack

In our setting, Alice, Bob (players), and Charlie (a TP) may try to steal the private information. Generally, distrustful inside participants are more destructive while launching attacks and should be paid more regard.[48]

In this protocol, quantum channels are established in Step 2 (Charlie sends S_{init} to Alice), Step 5 (Alice sends S_{A} to Bob), and Step 6 (Bob sends S_{B} to Charlie). Each $\left|\varphi_{\mathrm{init},i}\right\rangle$ in S_{init}, $|\varphi_{\mathrm{A},i}\rangle$ in S_{A}, and $|\varphi_{\mathrm{B},i}\rangle$ in S_{B} ($i=n-1,\ldots,1,0$) can be rewritten as Eqs. (22)–(24):

$$
\left|\varphi_{\mathrm{init},i}\right\rangle=E_{k_{\mathrm{C},i}}\left[|0\rangle\right]=R\left(k_{\mathrm{C},i}\right)|0\rangle, \tag{22}
$$

$$
\begin{aligned}
|\varphi_{\mathrm{A},i}\rangle&=E_{(\pi/2)N_{\mathrm{A},i}+k_{\mathrm{A},i}}\left[\left|\varphi_{\mathrm{init},i}\right\rangle\right]\\
&=R\left(\frac{\pi}{2}N_{\mathrm{A},i}+k_{\mathrm{A},i}\right)R\left(k_{\mathrm{C},i}\right)|0\rangle\\
&=R\left(k_{\mathrm{A},i}+k_{\mathrm{C},i}\right)\left|N_{\mathrm{A},i}\right\rangle,
\end{aligned}
\tag{23}
$$

$$
\begin{aligned}
|\varphi_{\mathrm{B},i}\rangle&=E_{(\pi/2)N_{\mathrm{B},i}+k_{\mathrm{B},i}}\left[|\varphi_{\mathrm{A},i}\rangle\right]\\
&=R\left(\frac{\pi}{2}N_{\mathrm{B},i}+k_{\mathrm{B},i}\right)|\varphi_{\mathrm{A},i}\rangle\\
&=R\left(k_{\mathrm{A},i}+k_{\mathrm{B},i}+k_{\mathrm{C},i}\right)\left[R\left(\frac{\pi}{2}N_{\mathrm{A},i}+\frac{\pi}{2}N_{\mathrm{B},i}\right)|0\rangle\right]\\
&=R\left(k_{\mathrm{A},i}+k_{\mathrm{B},i}+k_{\mathrm{C},i}\right)\left|N_{\mathrm{A},i}\oplus N_{\mathrm{B},i}\right\rangle.
\end{aligned}
\tag{24}
$$

Unlike the security ensured by decoy photons in outside attacks, the inside security depends on the safety of the rotational encryption method, which is explained as follows.

We can infer that an attacker cannot identify the correct key for only an intercepted photon because when the photon is measured, it collapses to $|0\rangle$ or $|1\rangle$, and the rotation angle is lost. Additionally, the measurement result cannot be guaranteed to be completely true once the attacker chooses a key unequal to the correct key. For example, the attacker chooses $\gamma\neq\theta$ to decrypt $R(\theta)|0\rangle$. The result is $R(\theta-\gamma)|0\rangle=\cos(\theta-\gamma)|0\rangle+\sin(\theta-\gamma)|1\rangle$. Thus, the probability p that the attacker gets the correct result $|0\rangle$ by measuring $R(\theta-\gamma)|0\rangle$ with Z-basis is $\cos^2(\theta-\gamma)$. Since γ and θ are unequal, p cannot reach 100%, which means that a wrong key cannot decrypt the completely correct result.

Hence, we can analyze the inside attacks by judging whether participants can obtain a quantum sequence and the corresponding key simultaneously. Based on this idea, we will analyze the following four cases one by one: Alice wants to get N_{B}, Bob wants to get N_{A}, and Charlie wants to get N_{A} or N_{B}.

Case 1 Alice wants to get N_{B}

N_{B} only exists in S_{B}. However, the key $(k_{\mathrm{A},i}+k_{\mathrm{B},i}+k_{\mathrm{C},i})$ to decrypt S_{B} is unavailable for Alice since $k_{\mathrm{C},i}$ is only held by Charlie and never published during the whole period.

Another way for Alice to steal N_{B} is to pass a fake S_{A} to Bob, such as a sequence filled by $|0\rangle$. While Bob sends S_{B} to Charlie, Alice intercepts it and passes another fake sequence to Charlie. If Bob announces his secret key, Alice can obtain S_{B} and K_{B} at the same time, so N_{B} will be leaked to Alice. However, this way is ineffective in our protocol. Once Alice intercepts S_{B}, her eavesdropping behavior must be detected in the eavesdropping check before Bob publishes his secret key. Then the protocol will be rebooted with three refreshed keys so Alice can never have Bob's available key.

In summary, Alice cannot obtain N_{B}.

Case 2 Bob wants to get N_{A}

Calculating N_{A} from S_{A} or S_{B} are equivalent to Bob because it is Bob who encrypts S_{A} to S_{B}. The former is taken for example. Bob cannot steal $k_{\mathrm{C},i}$ to decrypt the sequence S_{A} for the same reason as Alice.

Similar to the above, Bob can replace S_{init} with a fake sequence filled by $|0\rangle$ in Step 2. After Alice adds her secret to the fake sequence, Bob intercepts S_{A} and then gives Charlie another random fake sequence. He may calculate N_{A} after the

announcement of Alice's key since the state of each photon in S_A is in this form: $|\varphi_{A,i}\rangle = E_{(\pi/2)N_{A,i}+k_{A,i}}[|0\rangle] = R(k_{A,i})|N_{A,i}\rangle$. Nevertheless, the attack from Bob in this way is failed either. His eavesdropping will come to light after the check between Charlie and Alice.

To sum up, Bob cannot gain N_A.

Case 3 Charlie wants to get N_A

Once Charlie intercepts the sequence S_A, his eavesdropping will be identified. Then Alice will execute this protocol again with a refreshed key. Without the new key, Charlie cannot determine N_A even if he intercepts S_A. As for the sequence S_B, Charlie can compute $N_A \oplus N_B$ from it legally, but N_A and N_B are invisible to him.

So, Charlie will fail to decrypt S_A or S_B to steal N_A.

Case 4 Charlie wants to get N_B

As already stated, N_B has never been transmitted separately when the protocol is executed normally. It only coexists with N_A in S_B and never be divulged unless N_A is known. However, N_A is unavailable for Charlie from the analysis in Case 3.

In another way, Charlie can replace S_A with a fake sequence filled by $|0\rangle$. Then he may calculate N_B from S_B after K_B is published by Bob. Nevertheless, this behavior can also be discovered due to the check between Alice and Bob.

Therefore, N_B will not be disclosed to Charlie.

According to the above study, this protocol can withstand outside and inside attacks without revealing the players' private integers.

4.3. Efficiency analysis

The definition of qubit efficiency $\eta = \eta_c/\eta_t$ is given in Refs. [20,40]. In the above equation, η_c represents the number of the compared classical bits and η_t represents the total number of particles in the comparison protocol except for decoy particles used in the eavesdropping check.[20,40] Particularly, $\eta_t = \eta_k + \eta_s$. Here, η_k refers to the number of quantum particles applied to pre-shared keys, such as in QKD protocols, and η_s refers to the number of qubits carrying information in the sequence.

For our protocol, pre-shared keys do not exist, *i.e.*, $\eta_k = 0$. Moreover, the comparison of each classical bit in this protocol needs to be completed by one quantum bit, *i.e.*, $\eta_s = \eta_c$. Therefore, the efficiency of our protocol is 100%.

5. Discussion

In this section, we will compare our protocol with other similar protocols, and then discuss the extra application of our protocol.

In Table 2, we compare protocols in Refs. [21,32,49,50] with our protocol. Our protocol has the following characteristics: First, it is unnecessary to utilize extra particles during the key distribution process. Thus, our protocol has no quantum resources consumption of key distribution compared to a series of QKD-based QPC protocols.[32,49,50] Second, the quantum resources in our protocol are multiplexed. It means that the same quantum sequence carries two players' secret integers. However, in some protocols[49,50] without this feature, players have to prepare more particles to execute the protocols, which increases the consumption of quantum resources. Third, our protocol not only achieves the maximum theoretical efficiency as Jia *et al.*'s protocol,[21] but can be realized more easily. Jia *et al.*'s protocol[21] has more technical constraints, such as preparing four-particle χ-type states, entanglement swapping, and joint measurement.[44] On the contrary, our protocol is realized with single photons, unitary operation, and single-particle measurement.

Table 2. Comparison among our protocol and some existing QPC protocols.

Protocol	Quantum source	Qubit efficiency	Need for QKD protocols	Quantum resource multiplexing	Measurement manner
The protocol in Ref. [21]	particles in χ-type states	100%	No	Yes	joint measurement
The protocol in Ref. [49]	particles in Bell states	25%	Yes	No	single-particle measurement
The protocol in Ref. [32]	single photons	33%	Yes	Yes	single-particle measurement
The protocol in Ref. [50]	single photons	33%	Yes	No	single-particle measurement
Our protocol	single photons	100%	No	Yes	single-particle measurement

Furthermore, our proposed protocol can also be extended to perform additional tasks. For example, the protocol can accomplish a comparison of two sets. Every player arranges the set elements from small to large, and then concatenates the binary values. Another example is quantum secret sharing. Assume that the boss split a secret integer N_C into a random N_A and $N_B = N_A \oplus N_C$, and then sent N_A to Alice and N_B to Bob. Alice and Bob can execute our protocol to calculate the secret N_C.

6. Conclusion

We propose an efficient QPC protocol with single photons and rotational encryption. With the help of a TP, the players can safely determine the size relations for two private integers N_A and N_B. For efficiency, the secret keys in our protocol are distributed through classic channels instead of QKD protocols, so extra particles are not consumed for sharing keys. Additionally, the circular transmission mode allows players to implement the multiplexing of quantum resources, reducing

the number of photons utilized in our protocol. According to these two characteristics, the qubit efficiency of our protocol reaches 100%, the theoretical maximum. For technical constraints, the utilization of single photons, unitary operation, and single-particle measurement allows our protocol to be realized under current technical conditions.

Acknowledgments

Project supported by the National Key Research and Development Program of China (Grant No. 2020YFB1805405), the 111 Project (Grant No. B21049), the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant No. 2019BDKFJJ014), and the Fundamental Research Funds for the Central Universities (Grant No. 2020RC38).

References

[1] Yao A C 1982 *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, November 3–5, 1982, Chicago, USA, p. 160
[2] Jakobsson M and Yung M 1996 *Annual International Cryptology Conference*, August 18–22, 1996, Santa Barbara, USA, p. 186
[3] Boudot F, Schoenmakers B and Traore J 2001 *Discrete Appl. Math.* **111** 23
[4] Lo H K 1997 *Phys. Rev. A* **56** 1154
[5] Yang J, Wang C and Zhang R 2010 *Chin. Phys. B* **19** 110306
[6] Gu B, Huang Y G, Fang X and Zhang C Y 2011 *Chin. Phys. B* **20** 100309
[7] Chang Y, Zhang S B, Yan L L and Han G H 2015 *Chin. Phys. B* **24** 050307
[8] Zhao X L, Li J L, Niu P H, Ma H Y and Ruan D 2017 *Chin. Phys. B* **26** 030302
[9] Wang C and Zhang Y 2009 *Chin. Phys. B* **18** 3238
[10] Zhu Z C, Zhang Y Q and Fu A M 2011 *Chin. Phys. B* **20** 040306
[11] Zhang Z R, Liu W T and Li C Z 2011 *Chin. Phys. B* **20** 050309
[12] Du Y T and Bao W S 2018 *Chin. Phys. B* **27** 080304
[13] Tan Y G and Liu Q 2016 *Chin. Phys. Lett.* **33** 090303
[14] Liu C Q, Zhu C H, Wang L H, Zhang L X and Pei C X 2016 *Chin. Phys. Lett.* **33** 100301
[15] Li J J, Wang Y, Li H W and Bao W S 2020 *Chin. Phys. B* **29** 030303
[16] He Y Q, Mao Y, Zhong H, Huang D and Guo Y 2020 *Chin. Phys. B* **29** 050309
[17] Li X, Yuan H W, Zhang C M and Wang Q 2020 *Chin. Phys. B* **29** 070303
[18] Yang Y G and Wen Q Y 2009 *J. Phys. A: Math. Theor.* **42** 055305
[19] Chen X B, Xu G, Niu X X, Wen Q Y and Yang Y X 2010 *Opt. Commun.* **283** 1561
[20] Tseng H Y, Lin J and Hwang T 2012 *Quantum Inf. Process.* **11** 373
[21] Jia H Y, Wen Q Y, Li Y B and Gao F 2012 *Int. J. Theor. Phys.* **51** 1187
[22] Chen X B, Dou Z, Xu G, Wang C and Yang Y X 2014 *Quantum Inf. Process.* **13** 85
[23] Shi R H, Mu Y, Zhong H, Cui J and Zhang S 2016 *Sci. Rep.* **6** 19655
[24] Peng Z W, Shi R H, Zhong H, Cui J and Zhang S 2017 *Quantum Inf. Process.* **16** 316
[25] Xu Q D, Chen H Y, Gong L H and Zhou N R 2020 *Int. J. Theor. Phys.* **59** 1798
[26] Chou W H, Hwang T and Gu J 2016 arXiv: 1607.07961 [cs.CR]
[27] Zhou N R, Xu Q D, Du N S and Gong L H 2021 *Quantum Inf. Process.* **20** 124
[28] Wang B, Liu S Q and Gong L H 2022 *Chin. Phys. B* **31** 010302
[29] Shannon K, Towe E and Tonguz O K 2020 arXiv: 2003.07907 [cs.CR]
[30] Wen Q Y, Qin S J and Gao F 2014 *J. Cryptol.* **1** 200 (in Chinese)
[31] Yang Y G, Xia J, Jia X, Shi L and Zhang H 2012 *Int. J. Quantum Inf.* **10** 1250065
[32] Liu B, Gao F, Jia H Y, Huang W, Zhang W W and Wen Q Y 2013 *Quantum Inf. Process.* **12** 887
[33] Li Y B, Ma Y J, Xu S W, Huang W and Zhang Y S 2014 *Int. J. Theor. Phys.* **53** 3191
[34] Liu B, Xiao D, Huang W, Jia H Y and Song T T 2017 *Quantum Inf. Process.* **16** 180
[35] Goswami P S, Chakraborty T and Chattopadhyay A 2021 *International Conference on Electrical, Computer and Communication Technologies*, September 15–17, 2021, Erode, The Republic of India, p. 1
[36] Xin X J, Ding L, Li C Y, Sang Y X, Yang Q L and Li F G 2022 *Quantum Inf. Process.* **21** 33
[37] Zhang J L, Huang Z J, Li X, Wu M Q, Wang X Y and Dong Y M 2021 *Int. J. Theor. Phys.* **60** 2930
[38] Song X L, Wen A J and Gou R 2019 *IEEE Access* **7** 142507
[39] Wu W Q, Zhou G L, Zhao Y X and Zhang H G 2020 *Int. J. Theor. Phys.* **59** 1866
[40] Ye T Y and Ji Z X 2017 *Int. J. Theor. Phys.* **56** 1517
[41] Ye T Y 2017 *Commun. Theor. Phys.* **67** 147
[42] Zha X W, Yu X Y, Cao Y and Wang S K 2018 *Int. J. Theor. Phys.* **57** 3874
[43] Pan H M 2017 *Int. J. Theor. Phys.* **56** 3340
[44] Ji Z X, Fan P R, Zhang H G and Wang H Z 2020 *Opt. Commun.* **459** 124911
[45] Ye C Q, Li J, Chen X B and Tian Y 2021 *Quantum Inf. Process.* **20** 262
[46] Jones R C 1941 *J. Opt. Soc. Am.* **31** 488
[47] Zi W, Guo F Z, Luo Y, Cao S H and Wen Q Y 2013 *Int. J. Theor. Phys.* **52** 3212
[48] Gao F, Qin S J, Wen Q Y and Zhu F C 2007 *Quantum Inf. Comput.* **7** 329
[49] Yan L L, Zhang S B, Chang Y, Sheng Z W and Sun Y H 2019 *Int. J. Theor. Phys.* **58** 3852
[50] Sun Z W, Yu J P, Wang P, Xu L L and Wu C H 2015 *Quantum Inf. Process.* **14** 2125