Journal of Quantum Computing
DOI:10.32604/jqc.2021.019675
Article

Tech Science Press

New Quantum Private Comparison Using Hyperentangled GHZ State

Jerrel Gianni[1] and Zhiguo Qu[2,*]

[1]College of International Students, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[2]School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, 210044, China
[*]Corresponding Author: Zhiguo Qu. Email: qzghhh@126.com
Received: 15 April 2021; Accepted: 10 May 2021

Abstract: In this paper, we propose a new protocol designed for quantum private comparison (QPC). This new protocol utilizes the hyperentanglement as the quantum resource and introduces a semi-honest third party (TP) to achieve the objective. This protocol's quantum carrier is a hyperentangled three-photon GHZ state in 2 degrees of freedom (DOF), which could have 64 combinations. The TP can decide which combination to use based on the shared key information provided from a quantum key distribution (QKD) protocol. By doing so, the security of the protocol can be improved further. Decoy photon technology is also used as another means of security and checks if the transmission in the quantum channel is secure or not before sending the quantum carrier. The proposed protocol is proved to be able to fend off various kinds of eavesdropping attacks. In addition, the new QPC protocol also can compare secret inputs securely and efficiently.

Keywords: GHZ state; hyperentangled state; information security; quantum cryptography; quantum private comparison

1 Introduction

The research on quantum computing has been escalating in recent years. This, in turn, benefits quantum cryptography advancements as new quantum technologies are discovered and applied to improve existing quantum cryptography systems. The field of quantum cryptography was first established by Bennett et al. [1] in 1984, who came up with the first quantum key distribution (QKD) protocol called BB84. They proved that using a quantum channel as a means of transmission could provide unconditional security. Since then, quantum cryptography has been getting more and more attention from researchers because of its potential. Up until now, the field of quantum cryptography has been divided into several branches, namely: QKD, quantum multi-party computation (QSMC), quantum secret sharing (QSS), quantum secure direct communication (QSDC), and others.

Quantum private comparison (QPC) has also been getting attention which led to QPC becoming a vital subfield of quantum cryptography. The general idea of a private comparison protocol is to compare the equality of private information of n ($n \geq 2$) mutual parties without the disclosure of their secret information. The example usage of a private comparison protocol is to solve problems such as the famous "millionaires" problem, introduced by Yao et al. [2]. QPC realizes this idea of private comparison by applying quantum mechanics to the classical protocol, which vastly improves its security. The first QPC protocol was introduced by Yang et al. [3] in 2009, which uses single photons. Soon afterward, many researchers have been proposing QPC designs by utilizing different quantum states and quantum technologies. In the same year, Chen et al. [4] proposed another QPC protocol that uses a triplet entangled state called the Greenberger–Horne–Zeilinger (GHZ) state. Later in 2011, Tseng et al. [5] proposed a QPC protocol which makes use of entanglement of Bell states. Liu et al. [6] proposed a QPC protocol that uses triplet W state with single-particle measurement, and Jia et al. [7] proposed a QPC protocol which is based on χ-type state.

Recently, the more QPC protocols by using highly entangled six-particle state [8–9], maximally entangled seven-particle state [10], and semi-quantumness [11–12] were proposed, respectivley.

However, almost all of the existing QPC protocols only use quantum resources in only one degree of freedom (DOF) as their information carrier. Except for a QPC protocol proposed by Xu et al. [13] in 2019. The quantum resource used in their QPC protocol is a Bell state that possesses three different DOFs. By using this state, they were able to achieve QPC protocol with higher capacity and efficiency. The concept of using simultaneous entanglement of multiple DOFs is called hyperentanglement [14]. Some researchers [15] stated that hyperentanglement could significantly improve the channel capacity of quantum communication and speed up quantum computation. Thus, using the hyperentangled state as a quantum resource is beneficial in designing not only QPC protocol but also other quantum cryptography protocols. However, it has to be noted that distinguishing the different forms of hyperentangled state in different DOFs requires the use of a hyperentangled state analysis (HSA) scheme. Fortunately, other experts have also been coming up with new HSA schemes for different states with hyperentangled bell state analysis (HBSA) and hyperentangled GHZ state analysis (HGSA) schemes at the forefront of the research [16–19].

This paper proposes a QPC protocol using a three-photon hyperentangled GHZ state as the quantum resource. GHZ state is a maximally entangled state with m ($m > 2$) subsystems and having extremely non-classical property. But specific measurements done on the GHZ state could make the state collapse into a mixture or a pure state. The simplest form of a GHZ state is the 3-qubit GHZ state which has the form of $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. The three-photon hyperentangled GHZ state makes use of entanglement in 2 kinds of DOFs, polarization and spatial-mode. References [20–21] show that some researchers have developed schemes that could generate the hyperentangled GHZ state using current technology.

This structure of the paper is as follows: Section 2 introduces the prior knowledge related to the QPC protocol; Section 3 describes the proposed QPC protocol and the main steps of the protocol; Section 4 describes the analysis of the proposed QPC protocol; Section 5 concludes the content of the paper.

2 Preliminary

2.1 Hyperentangled GHZ State in 2 DOF

Generally, an N-photon hyperentangled GHZ state in polarization and spatial-mode DOFs can be written in the following form [16]:

$$|\tau\rangle_{PS} = |\delta_P\rangle_{AB\dots Z} \otimes |\delta_S\rangle_{AB\dots Z} \tag{1}$$

Here, the subscript A, B, …Z denotes the N photons, and the subscript P denotes the polarization DOF while S denotes the spatial-mode DOF. In each of the DOF, there are 2^N maximally entangled GHZ states. These GHZ states can be written in a universal form of [16]

$$\left|\delta^{\pm}_{ab\dots z}\right\rangle_{AB\dots Z} = \frac{1}{\sqrt{2}}\left(|ab\dots z\rangle \pm \left|\bar{a}\bar{b}\dots\bar{z}\right\rangle\right)_{AB\dots Z} \tag{2}$$

Here the $a, b, \dots z \in \{0,1\}$ denotes the bit information, and $\bar{x} = 1 - x$, ($\bar{x} \in \bar{a}\bar{b}\dots\bar{z}$). Based on Eqs. (1) and (2), three-photon hyperentangled GHZ state in polarization DOF can be written as one of the following 8 GHZ states [17–19]:

$$\left|\delta^{\pm}_{000}\right\rangle_P = \frac{1}{\sqrt{2}}(|HHH\rangle \pm |VVV\rangle)$$

$$\left|\delta^{\pm}_{001}\right\rangle_P = \frac{1}{\sqrt{2}}(|HHV\rangle \pm |VVH\rangle)$$

$$\left|\delta^{\pm}_{010}\right\rangle_P = \frac{1}{\sqrt{2}}(|HVH\rangle \pm |VHV\rangle)$$

$$\left|\delta^{\pm}_{100}\right\rangle_P = \frac{1}{\sqrt{2}}(|VHH\rangle \pm |HVV\rangle) \tag{3}$$

Here, $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization modes of the photons where $|H\rangle \equiv |0\rangle$ and $|V\rangle \equiv |1\rangle$. And the three-photon hyperentangled GHZ state in spatial-mode DOF can be written as one of the following 8 GHZ states [17–19]:

$$\left|\delta_{000}^{\pm}\right\rangle_S = \frac{1}{\sqrt{2}}(|a_1b_1c_1\rangle \pm |a_2b_2c_2\rangle)$$
$$\left|\delta_{001}^{\pm}\right\rangle_S = \frac{1}{\sqrt{2}}(|a_1b_1c_2\rangle \pm |a_2b_2c_1\rangle)$$
$$\left|\delta_{010}^{\pm}\right\rangle_S = \frac{1}{\sqrt{2}}(|a_1b_2c_1\rangle \pm |a_2b_1c_2\rangle)$$
$$\left|\delta_{100}^{\pm}\right\rangle_S = \frac{1}{\sqrt{2}}(|a_2b_1c_1\rangle \pm |a_1b_2c_2\rangle) \quad (4)$$

Here $|x_1\rangle$ and $|x_2\rangle$ denote the different spatial modes for each photon where $|x_1\rangle \equiv |0\rangle$, $|x_2\rangle \equiv |1\rangle$, and $x \in a, b, c$. Because of Eqs. (3) and (4), a hyperentangled three-photon GHZ state can have 64 different combinations of GHZ states in polarization and spatial-mode DOF. An example of one of the combinations of the hyperentangled state is shown in Eq. (5)

$$|\tau\rangle_{PS} = |\delta_{000}^{+}\rangle_P \otimes |\delta_{000}^{+}\rangle_S = \frac{1}{\sqrt{2}}(|HHH\rangle + |VVV\rangle)_{ABC} \otimes \frac{1}{\sqrt{2}}(|a_1b_1c_1\rangle + |a_2b_2c_2\rangle)_{ABC} \quad (5)$$

2.2 Bell Measurement in 2 DOF

In this paper, we also utilize Bell measurement (BM) to get the Bell states of each photon, but the form of the Bell states is somewhat different because of the nature of a hyperentangled state. The Bell states in polarization and spatial-mode DOF in this paper will follow the form of [16]

$$\left|\varphi^{\pm}\right\rangle_X = \frac{1}{\sqrt{2}}(|Hx_2\rangle \pm |Vx_1\rangle)$$
$$\left|\psi^{\pm}\right\rangle_X = \frac{1}{\sqrt{2}}(|Hx_1\rangle \pm |Vx_2\rangle) \quad (6)$$

Here, $X \in A, B, \ldots Z$ and $x \in a, b, \ldots z$. These indicate which of the photon is being measured. Using BM on each of the photons of hyperentangled GHZ state will yield one of the following results from Eq. (6). However, each of 64 combinations of the hyperentangled three-photon GHZ state could yield different results based on the measured combination. For example, performing BM on $|\tau\rangle_{PS} = |\delta_{000}^{+}\rangle_P \otimes |\delta_{000}^{+}\rangle_S$ will result in

$$|\gamma\rangle_{PS} = |\delta_{000}^{+}\rangle_P \otimes |\delta_{000}^{+}\rangle_S = \frac{1}{2\sqrt{2}}\begin{pmatrix} |\varphi^{+}\rangle_a|\varphi^{+}\rangle_b|\varphi^{+}\rangle_c + |\varphi^{+}\rangle_a|\varphi^{-}\rangle_b|\varphi^{-}\rangle_c \\ +|\varphi^{-}\rangle_a|\varphi^{+}\rangle_b|\varphi^{-}\rangle_c + |\varphi^{-}\rangle_a|\varphi^{-}\rangle_b|\varphi^{+}\rangle_c \\ +|\psi^{+}\rangle_a|\psi^{+}\rangle_b|\psi^{+}\rangle_c + |\psi^{+}\rangle_a|\psi^{-}\rangle_b|\psi^{-}\rangle_c \\ +|\psi^{-}\rangle_a|\psi^{+}\rangle_b|\psi^{-}\rangle_c + |\psi^{-}\rangle_a|\psi^{-}\rangle_b|\psi^{+}\rangle_c \end{pmatrix} \quad (7)$$

while performing BM on $|\tau\rangle_{PS} = |\delta_{000}^{+}\rangle_P \otimes |\delta_{001}^{+}\rangle_S$ will result in

$$|\gamma\rangle_{PS} = |\delta_{000}^{+}\rangle_P \otimes |\delta_{000}^{+}\rangle_S = \frac{1}{2\sqrt{2}}\begin{pmatrix} |\varphi^{+}\rangle_a|\varphi^{+}\rangle_b|\psi^{+}\rangle_c + |\varphi^{+}\rangle_a|\varphi^{-}\rangle_b|\psi^{-}\rangle_c \\ +|\varphi^{-}\rangle_a|\varphi^{+}\rangle_b|\psi^{-}\rangle_c + |\varphi^{-}\rangle_a|\varphi^{-}\rangle_b|\psi^{+}\rangle_c \\ +|\psi^{+}\rangle_a|\psi^{+}\rangle_b|\varphi^{+}\rangle_c + |\psi^{+}\rangle_a|\psi^{-}\rangle_b|\varphi^{-}\rangle_c \\ +|\psi^{-}\rangle_a|\psi^{+}\rangle_b|\varphi^{-}\rangle_c + |\psi^{-}\rangle_a|\psi^{-}\rangle_b|\varphi^{+}\rangle_c \end{pmatrix} \quad (8)$$

This property will be exploited in the QPC protocol to improve the security of the protocol.

3 The Proposed QPC Protocol

In this section, we present the QPC protocol with a hyperentangled three-photon GHZ state.

3.1 Prerequisites

For simplicity, it is assumed that there are two parties which are conventionally called Alice and Bob. Alice and Bob want to compare the equality of their private information. Alice has the private information X while Bob has the private information Y. The binary representations of X and Y in F_{2^N} are $(x_1,x_2,\ldots,x_N)$ and $(y_1,y_2,\ldots,y_N)$, respectively, where $x_j, y_j \in \{0,1\}, j \in \{1,2,\ldots,N\}$. They employ a third party (TP) who is assumed to be semi-honest which means that the TP may misbehave but will not plot with either party.

Alice (Bob) then divides the binary representation of X (Y) into $[N/2]$ groups: $G_a^1, G_a^2, \dots, G_a^{[N/2]}(G_b^1, G_b^2, \dots, G_b^{[N/2]})$. Each of the group $G_a^i(G_b^i)$ contains two bits. If N mod 2 = 1, Alice (Bob) adds one 0 into the last group $G_a^{[N/2]}(G_b^{[N/2]})$.

Through a secure QKD protocol, Alice and TP generate a shared key sequence K_{AT}. Besides that, Bob and TP also generate the secret key K_{BT}. Here, $K_{AT}, K_{BT} \in \{000, 001, 010, 011, 100, 101, 110, 111\}$. The key sequence is used to determine which of the initial states will be prepared by the TP.

3.2 Detailed Steps of the Protocol

Step 1. TP prepares to generate N number of initial states $|\tau\rangle_{PS}$, which are chosen from the 64 combinations of hyperentangled three-photon GHZ state based on the shared key sequence K_{AT} and K_{BT} for the polarization DOF and spatial-mode DOF, respectively, according to Tab. 1. TP will then form a quantum sequence $S\tau$ using the states $|\tau\rangle_{PS}$.

$$S\tau: [P_A^1, P_B^1, P_C^1, P_A^2, P_B^2, P_C^2, \dots, P_A^N, P_B^N, P_C^N] \quad (9)$$

Next, TP divides the quantum sequence into three new quantum sequences S_A, S_B, and S_C. S_A consists of the first photon of every $|\tau\rangle_{PS}$ in quantum sequence $S\tau$ and is intended to be sent to Alice. S_B consists of the second photon of every $|\tau\rangle_{PS}$ in quantum sequence $S\tau$ and is intended to be sent to Bob. S_C consists of the third photon of every $|\tau\rangle_{PS}$ in quantum sequence $S\tau$ and will be kept by TP.

Table 1: Initial state selection based on shared key sequence

$\|\delta_P\rangle$	$\|\delta_S\rangle$	K_{AT}, K_{BT}
$\|\delta_{000}^+\rangle_P$	$\|\delta_{000}^+\rangle_S$	000
$\|\delta_{000}^-\rangle_P$	$\|\delta_{000}^-\rangle_S$	001
$\|\delta_{001}^+\rangle_P$	$\|\delta_{001}^+\rangle_S$	010
$\|\delta_{001}^-\rangle_P$	$\|\delta_{001}^-\rangle_S$	011
$\|\delta_{010}^+\rangle_P$	$\|\delta_{010}^+\rangle_S$	100
$\|\delta_{010}^-\rangle_P$	$\|\delta_{010}^-\rangle_S$	101
$\|\delta_{100}^+\rangle_P$	$\|\delta_{100}^+\rangle_S$	110
$\|\delta_{100}^-\rangle_P$	$\|\delta_{100}^-\rangle_S$	111

Step 2. After preparing the quantum sequences, TP prepares two sets of decoy photons D_A and D_B selected randomly from the single-photon states $|\sigma\rangle_P \otimes |\sigma\rangle_S$ where $|\sigma\rangle_P \in \left\{|H\rangle, |V\rangle, \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\right\}$, $|\sigma\rangle_S \in \left\{|x_1\rangle, |x_2\rangle, \frac{1}{\sqrt{2}}(|x_1\rangle + |x_2\rangle), \frac{1}{\sqrt{2}}(|x_1\rangle - |x_2\rangle)\right\}$, $x \in \{a, b, c\}$. Then, the sets of decoy photons D_A and D_B are randomly inserted into the quantum sequence S_A and S_B respectively to form a new quantum sequence S'_A and S'_B. TP records each of the decoy photons' positions and measurement bases in each of the quantum sequences. And then, TP sends the quantum sequence S'_A (S'_B) to Alice (Bob).

Step 3. After receiving the quantum sequence S'_A (S'_B), Alice (Bob) notify TP that she (he) has received the quantum sequence, and TP informs Alice (Bob) of the positions and bases of each decoy photons in quantum sequence S'_A (S'_B). According to TP information, Alice (Bob) measures every decoy photons' quantum state with their corresponding measurement bases. Alice and Bob could check the security of the transmission in the quantum channel with the decoy photons' measurement results. If the error rate exceeds the error threshold, they can assume that the quantum channel is compromised, abort the protocol, and retry the protocol from the first step. Otherwise, they continue the protocol to the next step.

Table 2: Encoding table

Bell state	M_a^i, M_b^i	M_c^i
$\|\varphi^+\rangle$	00	00
$\|\varphi^-\rangle$	11	11
$\|\psi^+\rangle$	10	00
$\|\psi^-\rangle$	01	11

Table 3: Encoding table

K_{AT} (K_{BT})	C_P (C_S)
000	00
001	11
010	00
011	11
100	10
101	01
110	10
111	01

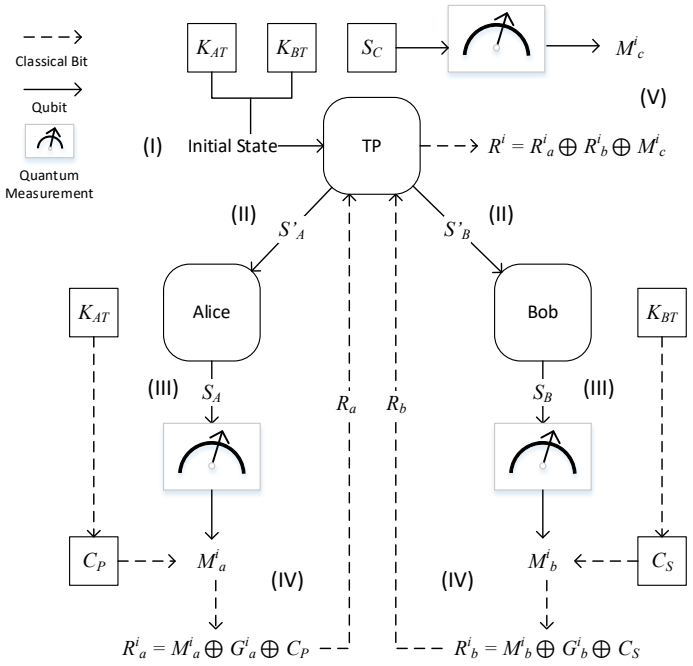

Figure 1: The proposed protocol flowchart

Step 4. After confirming that the quantum channel is secure, Alice (Bob) discards all of the decoy photons D_A (D_B) from the quantum sequence S'_A (S'_B) respectively according to the positions of the decoy photons as informed by the TP. Alice (Bob) then receives the quantum sequence S_A (S_B) and then perform a BM on each of the photons inside the sequence. The result of the measurement is denoted as classical bits according to Tab. 2. Also, based on the shared key K_{AT} (K_{BT}), Alice (Bob) gets the encoding C_P (C_S) according to Tab. 3. Using the measurement result M_a^i (M_b^i), Alice (Bob) computes $R_a^i = M_a^i \oplus G_a^i \oplus C_P$ ($R_b^i = M_b^i \oplus G_b^i \oplus C_S$) and then sends the result of the computation R_a^i (R_b^i) to TP.

Step 5. When TP has received both R_a^i (R_b^i), TP perform BM on the quantum sequence S_C. TP encodes the measurement result M_C^i according to Tab. 2. And finally, TP calculates each of $R^i = R_a^i \oplus R_b^i \oplus M_c^i$. If all of the computation result $R = \sum_{i=1}^{N} R^i = 00$, then X and Y are equal; otherwise, X and Y are not equal. TP announces the comparison result to Alice and Bob.

The graphical representation of the QPC protocol steps are shown in Fig. 1.

4 Analysis

4.1 Correctness

In this section, we will be discussing the correctness of the proposed protocol. According to Tab. 4, we could infer $M_a^i \oplus M_b^i \oplus M_C^i \oplus C_P \oplus C_S = 00$ which means that

$$R^i = R_a^i \oplus R_b^i \oplus M_c^i$$
$$R^i = (M_a^i \oplus G_a^i \oplus C_P) \oplus (M_b^i \oplus G_b^i \oplus C_S) \oplus M_c^i$$
$$R^i = (M_a^i \oplus M_b^i \oplus M_c^i \oplus C_P \oplus C_S) \oplus G_a^i \oplus G_b^i$$
$$R^i = G_a^i \oplus G_b^i \quad (10)$$

From Eq. (10), we can conclude that if $R^i = 00$, G_a^i and G_b^i are equal. Otherwise, G_a^i and G_b^i are not equal. This equation proved that the proposed protocol is correct and works as intended.

Table 4: Two cases of different initial states

G_a^i	G_b^i	$\|\delta_P\rangle$	$\|\delta_S\rangle$	M_a^i	M_b^i	M_c^i	C_P^i	C_S^i	R_a^i	R_b^i	R^i
01	01	$\|\delta_{000}^+\rangle_P$	$\|\delta_{000}^+\rangle_S$	00	00	00	00	00	01	01	00
				00	11	11	00	00	01	10	00
				11	00	11	00	00	10	01	00
				11	11	00	00	00	10	10	00
				10	10	00	00	00	11	11	00
				10	01	11	00	00	11	00	00
				01	10	11	00	00	00	11	00
				01	01	00	00	00	00	00	00
01	01	$\|\delta_{001}^+\rangle_P$	$\|\delta_{100}^-\rangle_S$	00	10	11	00	01	01	10	00
				00	01	00	00	01	01	01	00
				11	10	00	00	01	10	10	00
				11	01	11	00	01	10	01	00
				10	00	11	00	01	11	00	00
				10	11	00	00	01	11	11	00
				01	00	00	00	01	00	00	00
				01	11	11	00	01	00	11	00

4.2 Security

This section will discuss the security of the proposed protocol from two types of attacks: external attacks and participants attacks. First, we show the protocol can withstand attacks from outside of the quantum transmission. Second, we prove that any participants (Alice, Bob, and TP) cannot obtain Alice or Bob's private information.

4.2.1 External Attacks

We assume an external attacker called Eve is trying to get Alice or Bob's private information in every step of the protocol when given the opportunity. The only step with any transmissions of quantum particle sequences is Step 2 of the protocol, which means that this step is the only time Eve could implement the attacks. Other security measures in the protocol are decoy photons technology and QKD protocol. The decoy photons technology is used in the protocol to perform eavesdropping check. This technology has been proven to work against some well-known attacks such as intercept-resend attacks, measurement-resend attacks, and entanglement measurement attacks [22]. The key sequences generated through the QKD protocol are used to select the initial states and used as encodings that could thwart some of the attacks. The following sections will describe some possible attacks that Eve could implement to get the participants' private information.

Intercept-Resend Attack. The intercept-resend attack is an attack in which the attacker intercepts the transmission to get the particles and then resends fake particles prepared beforehand to conceal the interception. In the proposed protocol, Eve can only intercept the transmission of Step 2. Meaning that what Eve can try to do is to obtain the quantum sequences S'_A and S'_B which are filled with decoy photon particles. Eve has to select the measurement basis from $\{|H\rangle, |V\rangle\}$, $\left\{\frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\right\}$, $\{|x_1\rangle, |x_2\rangle\}$, $\left\{\frac{1}{\sqrt{2}}(|x_1\rangle + |x_2\rangle), \frac{1}{\sqrt{2}}(|x_1\rangle - |x_2\rangle)\right\}$ to measure the decoy photons. Thus, she will have a probability of $\frac{3}{4}$ to choose the wrong basis for every photon. The detection rate of this protocol for n decoy photons is $1 - \left(\frac{1}{4}\right)^n$ which approaches 1 if n is large enough. This detection rate means that the eavesdropper will inevitably be exposed during the eavesdropping check. Not to mention that Eve will be unable to generate a fake quantum sequence that could reproduce the decoy photon's quantum states due to the rules of the no-cloning theorem for quantum information. In a minimal chance that Eve can bypass the detection, Eve can get the measurement result M_a^i and M_b^i. However, during Step 4, the computation results are encrypted through the encoding of the shared key sequence (C_P and C_S) generated through QKD. As such, Eve can only get $G_a^i \oplus C_P$ and $G_b^i \oplus C_S$ and since the shared keys are unknown to Eve, Eve would not be able to get either G_a^i and G_b^i. Thus, this type of attack would not work on the proposed protocol.

Measurement-Resend Attack. The measurement-resend attack is an attack in which the attacker intercepts the transmission similar to the previous type of attack and then perform quantum measurements on the intercepted particles. Afterwards, Eve will prepare the same quantum states based on the measurement result and resend the states to Alice and Bob. In this attack, Eve can only intercept the quantum sequences S'_A and S'_B which are filled with decoy photons. Eve cannot differentiate which intercepted particles are decoy photons or particles in the actual hyperentangled GHZ state, resulting in Eve consistently choosing different measurement bases for each particle. By doing so, Eve will be detected during the eavesdropping check, and thus this type of attack will also fail to work against the proposed protocol.

Man in the Middle Attack. In the man in the middle attack, Eve will try to get useful information by pretending to be the participants in the protocol. For example, during Steps 2 and 3, when TP sends the quantum sequence S'_A to Alice, Eve intercepts the particles. Eve then pretends to be Alice and completes the eavesdropping check with TP resulting in Eve being able to get the quantum sequence S_A. Next, Eve replaces the quantum sequence S'_A with a fake quantum sequence by fabricating new hyperentangled GHZ states and decoy photons. Eve then pretends to be TP, sends the fake quantum sequence to Alice, and completes the eavesdropping check with Alice to prevent being detected. Eve could do the same thing to Bob to receive the quantum sequence S_B. By doing so, Eve can get both the measurement result M_a^i and M_b^i. However, similar to the result of the intercept-resend attack, Eve can only get $G_a^i \oplus C_P$ and $G_b^i \oplus C_S$ and she does not know the value of the shared keys generated through QKD. Therefore, Eve will fail to get either G_a^i and G_b^i.

Trojan Horse Attack. In the Trojan horse attack, the proposed protocol adopts the entanglement

swapping approach to QPC. Because of this approach, the transmissions used in the protocol are one-way qubit transmissions. Thus Trojan horse attack would not be effective, and the attack will also fail. In conclusion, based on the analysis, our protocol has no problem withstanding known external attacks.

4.2.2 Participant Attacks

Compared with the previous type of attack, participant attack is more threatening as the participants have more opportunities to attack the protocol. This kind of attack was first introduced by Gao et al. [23]. In this section, we will discuss the possibility of attacks from each party.

Case 1. Alice's (or Bob's) attack: Since Alice and Bob have the same role, analysis on any party would yield the same result. We assume that Alice is trying to get Bob's private information *Y*. The first attack that Alice could try is to intercept the quantum sequence S'_B and extract Bob's private information. However, since she does not know the decoy photons' location and measurement bases, she will be detected as an outside attacker during the eavesdropping check. The second attack that she could try is to intercept R_b^i and try to infer M_b^i from M_a^i but since she does not know C_S^i, she will fail to get any helpful information.

Case 2. TP's attack: The TP in this protocol is assumed to be semi-honest, meaning that the TP will execute the protocol and prepare the initial states. TP can only infer the private information from R_a^i, R_b^i, and M_c^i. Because of not knowing the value of C_P and C_S and the measurement results from BM have the same probability; TP cannot know the definite value of G_a^i and G_b^i. Therefore, TP cannot learn of the private information *X*, *Y*.

4.3 Performance & Efficiency

In this section, we will analyze the performance as well as the efficiency of the proposed protocol. Firstly, there are advantages regarding the protocol's performance: 1) The protocol does not employ unitary operations, which means it doesn't require additional quantum devices. The protocol only uses Bell measurement, which has an easier implementation than unitary operations. 2) The protocol uses decoy photon technology instead of using entangled states for eavesdropping check. 3) The transmissions for quantum particles in the protocol are one-way quantum transmission which improves the security and efficiency of the protocol. 4) Our protocol utilizes the property of entanglement swapping, which produces nonlocal entanglement remotely, reducing the number of required transmissions and providing an easier implementation.

Secondly, to discuss the efficiency of the protocol, let us first define qubit efficiency, which is commonly used to determine the efficiency of a QPC protocol. Generally, the qubit efficiency of a QPC protocol is defined using the following equation, $\eta_e = \frac{\eta_c}{\eta_t}$. In this equation, η_e denotes qubit efficiency, η_c denotes the compared classical bits, and η_t denotes the total number of photons consumed in each comparison phase [10]. The proposed protocol's quantum carrier are three-photon hyperentangled GHZ states. In each comparison, three photons in the hyperentangled state are used to compare 2 bits of classical information. On that account, the qubit efficiency η_e of the proposed protocol is $\frac{2}{3}$ or about 66%. The comparison of this protocol with other previously proposed QPC protocols is shown in Tab. 5.

Table 5: The comparison between our protocol and other existing QPC protocols

Reference	[8]	[9]	[10]	[11]	Our protocol
Quantum Carrier	Entangled GHZ State	Highly Entangled Six-qubit State	Maximally Entangled Seven-qubit State	QED	Hyperentangled GHZ State
Measurement	BM	BM	SPM & BM	SAM	BM
Unitary Operation	No	No	No	No	No

Entanglement Swapping	Yes	No	No	No	Yes
QKD	No	Yes	Yes	Yes	Yes
Decoy Photons	Yes	Yes	Yes	Yes	Yes
Qubit Efficiency	33%	33%	29%	50%	66%

Note: SPM (single-particle measurements), SAM (single-atom measurements), BM (Bell measurements).

5 Discussion and Conclusion

In this paper, the QPC protocol with a hyperentangled three-photon GHZ state in 2 DOFs is proposed. The protocol utilizes a hyperentangled three-photon GHZ state in 2 DOF as a quantum resource. Using a hyperentangled state saves more quantum resources because only one kind of quantum state is needed to be prepared. The hyperentangled state also offers higher capacity and efficiency when compared to regular quantum states. The security analysis shows that the proposed protocol could withstand both external attacks and participant attacks. With the ongoing research on hyperentangled states, there will undoubtedly be more quantum technologies that could make hyperentangled states more accessible, which gives more options in handling hyperentangled states. Hopefully, by introducing this protocol, this paper could inspire other researchers to use hyperentanglement as a quantum resource.

Acknowledgement: We are grateful to the peoples for the support and encouragement.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. of IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179, 1984.

[2] A. C. Yao, "Protocols for secure computations," in *Proc. of the 23rd Annual Sym. on Computer Science*, Chicago, USA, pp. 160–164, 1982.

[3] Y. G. Yang and Q. Y. Wen, "Secure quantum private comparison," *Physica Scripta*, vol. 80, no. 6, pp. 065002–065007, 2009.

[4] X. B. Chen, G. Xu, X. X. Niu, Q. Y. Wen and Y. X. Yang, "An efficient protocol for the private comparison of equal information based on the triplet entangled state and single-particle measurement," *Optics Communications*, vol. 283, no. 7, pp. 1561–1565, 2010.

[5] H. Y. Tseng, J. Lin and T. Hwang, "New quantum private comparison protocol using EPR pairs," *Quantum Information Processing*, vol. 11, no. 2, pp. 373–384, 2012.

[6] W. Liu, Y. B. Wang and Z. T. Jiang, "An efficient protocol for the quantum private comparison of equality with W state," *Optics Communications*, vol. 284, no. 12, pp. 3160–3163, 2011.

[7] H. Y. Jia, Q. Y. Wen, Y. B. Li and F. Gao, "Quantum private comparison using genuine four-particle entangled states," *International Journal of Theoretical Physics*, vol. 51, no. 4, pp. 1187–1194, 2012.

[8] W. Liu and Y. B. Wang, "Quantum private comparison based on GHZ entangled states," *International Journal of Theoretical Physics*, vol. 51, no. 11, pp. 3596–3604, 2012.

[9] Z. X. Ji and T. Y. Ye, "Quantum private comparison of equal information based on highly entangled six-qubit genuine state," *Communications in Theoretical Physics*, vol. 65, no. 6, pp. 711–715, 2016.

[10] Z. X. Ji, H. G. Zhang and P. R. Fan, "Two-party quantum private comparison protocol with maximally entangled seven-qubit state," *Modern Physics Letters A*, vol. 34, no. 28, pp. 1950229–1950234, 2019.

[11] T. Y. Ye, "Quantum private comparison via cavity QED," *Communications in Theoretical Physics*, vol. 67, no. 2, pp. 147–156, 2017.

[12] W. H. Chou, T. Hwang and J. Gu, "Semi-quantum private comparison protocol under an almost-dishonest third party," *arXiv preprint arXiv:1607.07961*, no. 1, pp. 1–19, 2016.

[13] L. Xu and Z. W. Zhao, "High-capacity quantum private comparison protocol with two-photon hyperentangled Bell states in multiple-degree of freedom," *The European Physical Journal D*, vol. 73, no. 3, pp. 1–11, 2019.

[14] P. G. Kwiat, "Hyper-entangled states," *Journal of Modern Optics*, vol. 44, no. 11–12, pp. 2173–2184, 1997.

[15] F. G. Deng, B. C. Ren and X. H. Li, "Quantum hyperentanglement and its applications in quantum information processing," *Science Bulletin*, vol. 62, no. 1, pp. 46–68, 2017.

[16] X. H. Li and S. Ghose, "Self-assisted complete maximally hyperentangled state analysis via the cross-Kerr nonlinearity," *Physical Review A*, vol. 93, no. 2, pp. 022302–022307, 2017.

[17] Y. Xia, Q. Q. Chen, J. Song and H. S. Song, "Efficient hyperentangled Greenberger–Horne–Zeilinger states analysis with cross-Kerr nonlinearity," *JOSA B*, vol. 29, no. 5, pp. 1029–1037, 2012.

[18] M. Wang, F. Yan and T. Gao, "Deterministic state analysis for polarization-spatial-time-bin hyperentanglement with nonlinear optics," *Laser Physics Letters*, vol. 15, no. 12, pp. 125206–125211, 2018.

[19] Z. Zeng and K. D. Zhu, "Complete hyperentangled state analysis using weak cross-Kerr nonlinearity and auxiliary entanglement," *New Journal of Physics*, vol. 22, no. 8, pp. 083051–083056, 2020.

[20] D. Ding and F. L. Yan, "Efficient scheme for three-photon Greenberger–Horne–Zeilinger state generation," *Physics Letters A*, vol. 377, no. 15, pp. 1088–1094, 2013.

[21] A. P. Liu, X. Han, L. Y. Cheng, Q. Guo, S. L. Su *et al.,* "Generation of large scale hyperentangled photonic GHZ states with an error-detected pattern," *The European Physical Journal D*, vol. 73, no. 6, pp. 1–9, 2019.

[22] Z. Ji, P. Fan and H. Zhang, "Security proof of qudit-system-based quantum cryptography against entanglement-measurement attack using decoy photons," *arXiv preprint arXiv:2012.14275*, pp. 1–10, 2020.

[23] F. Gao, S. J. Qin, Q. Y. Wen and F. Z. Zhu, "A simple participant attack on the brádler-dušek protocol," *Quantum Information & Computation*, vol. 7, no. 4, pp. 329–334, 2007.