J. Math. Math. Sci. (2024) 103–122

Secure direct message exchange based on simultaneous usage of two different degrees of freedom

Nguyen Ba An (Hanoi, Vietnam)

(Received Jan. 8, 2024)

Abstract. In the era of information explosion supplied with a very high level of technology as of today, the loss or leakage of information is one of the most severe problems. Security in communication has thus become more important than ever. In this paper, two protocols for quantum secure direct exchange of messages are proposed using hyperentangled photon pairs as resource for exchanging informative bits and single photons in hyperstates as resource for detecting eavesdroppers. In both the protocols the photons need to be transmitted only once from one to the other communicating party. However, the ways to transmit photons are different in the two proposed protocols. The first protocol employs block transmission of photons. Although its security is unconditional, it compulsorily requires quantum memories at both communicating stations. Contrasting to the first protocol, in the second protocol single photons are transmitted one by one and subject to immediate processing without the need of any quantum memories. The security of the second protocol is asymptotic in the sense that the chance for eavesdroppers to pass is approaching zero in the limit of long messages. Comparison with other protocols is also given.

1. Introduction

Secure and faithful telecommunication is an indispensable primary demand in human society in all fields, especially in diplomatic missions, military tasks

Key words and phrases: Secure direct message exchange, P-DOF, S-DOF, hyperentanglement, hyperstate.
2020 Mathematics Subject Classification: 81P40 Quantum coherence, entanglement, quantum correlations, 81P45 Quantum information, communication, networks

and important commercial business. At present, confidential telecommunication is done within the framework of the public key cryptosystem [1] whose security is based on extreme mathematical difficulty in reversing one-way functions (also called hash functions). Although such a cryptosystem cannot be broken by the most powerful available classical supercomputers in a reasonable finite time, it is threatened by quantum computers that can, say, by a quantum algorithm [2], break the system in a surprisingly short period of time. In other words, the public key cryptosystem is secure conditionally only. To have an unconditional secure way to telecommunicate, people resort to the laws of quantum mechanics. The key to be shared among the communicating parties can be now created remotely in quantum manner in the nose of eavesdroppers whose attacks should be detected because any unauthorized intervene leaves behind observable tracks. This is the so-called quantum key distribution (QKD) protocols [3, 4, 5]. The thus created key is then used to form the ciphertext to be transmitted as in the private key cryptosystem or one-time pad which has been proven absolutely secure [6].

In practice there appear situations when a message is urgently demanded to be sent but no keys are available and no time left to perform a QKD protocol at that moment. Regarding these situations, a new kind of quantum protocols was put forward. These protocols enable sending the message directly yet securely without prior encryption through appropriate quantum channel and thus they are referred to as quantum secure direct communication (QSDC) protocols [7, 8] (see also, *e.g.*, [9] - [20] and many other references for both theoretical and experimental aspects).

It is noted that all the above-mentioned QSDC protocols are unidirectional. The first bidirectional QSDC protocol was proposed in [21] which allows two remote authorized parties to directly and securely exchange their messages without any keys shared beforehand. Later, a great deal of papers have been published addressing diverse aspects of the bidirectional QSDC problem (see, *e.g.*, [22] - [35] and the references therein).

During a few last years hyperentangled states [36, 37], *i.e.*, states possessing simultaneous entanglement in more than one degree of freedom (DOF), are produced providing high-capacity quantum resources for various global tasks such as teleportation of a photon state encoded in multiple DOFs [38, 39, 40], breaking the communication barrier in superdense coding [41, 42, 43], hyper remote state preparation [44, 45, 46], hyper joint remote state preparation [47], hyper remote implementation of operators [48, 49, 50] and so on. As for QSDC, hyperentanglement was also exploited to boost the quantum channel capacity and the communication efficiency [51, 52]. Moreover, compared to the case of using conventional entanglement, the hyperentanglement-based QSDC protocol is deterministic instead of probabilistic and only requires to transmit the photon once instead of twice, thereby ensuring the effectivity of performance,

economizing the quantum resource and lowering the chance for the eavesdropper to attack [53]. Of late, multiple DOFs have also been leveraged to tailor a protocol within the cloud office model that accelerates the processing of huge data amounts, enabling robust network services with mutual authentication among remote parties [54].

In this paper we are going to propose two protocols (Protocol 1 and Protocol 2) for two remote parties (Alice and Bob) to directly exchange their messages in a secure and efficient way. In our protocols photon pairs hyperentangled at the same time in both polarization degree of freedom (P-DOF) and spatial-path degree of freedom (S-DOF) are used to transmit the message bits, while single photons also encoded in both P-DOF and S-DOF serve as decoys to detect the eavesdropper (Eve). Each of the two protocols properly consists of a number of elementary rounds which are specifically designed for the purpose of exchanging useful information and checking the possible presence of Eve. Section 2 describes two kinds of the elementary rounds that constitute the main protocols. Section 3 and Section 4 are respectively reserved for detailing Protocol 1 and Protocol 2, whose advantages/disadvantages are highlighted. The final section, Section 5, provides the conclusion with some discussion and comparison with other protocols.

2. Elementary rounds

There are two kinds of elementary rounds: message round and control round.

2.1. Message round

Suppose that Alice has an informative bit $a \in \{0,1\}$ while Bob has his informative bit $b \in \{0,1\}$ and they wish to securely exchange their bits directly, *i.e.*, without any secret keys shared in advance. The exchange of the bits a and b can be achieved in a quantum way in several steps as follows.

Step 1. Alice prepares a photon pair in a hyperentangled state, which may be, say, of the following particular form

$$\begin{aligned} |\Psi\rangle_{AB} &= \frac{1}{2}(|H,a0\rangle_A |H,b0\rangle_B + |H,a1\rangle_A |H,b1\rangle_B \\ &\quad + |V,a0\rangle_A |V,b0\rangle_B + |V,a1\rangle_A |V,b1\rangle_B), \end{aligned} \tag{2.1}$$

where A, B label the photon, $|H\rangle$ ($|V\rangle$) denotes state of a horizontally (ver-

tically) polarized photon and $|aj\rangle$ ($|bj\rangle$) with $j = \{0, 1)$ indicates state of a corresponding photon propagating along spatial path aj (bj). The notation $|H, a0\rangle_A$ implies state of photon A that is horizontally polarized and propagates along path $a0$. Similar meanings hold for the other notations $|H, a1\rangle_A$, $|H, b0\rangle_B$, ... The particular state (2.1) can be simplified to

$$|\Psi\rangle_{AB} = \frac{1}{2}(|H\rangle_A |H\rangle_B + |V\rangle_A |V\rangle_B)(|a0\rangle_A |b0\rangle_B + |a1\rangle_A |b1\rangle_B), \tag{2.2}$$

Step 2. Alice next generates a random bit $r \in \{0, 1\}$ and encodes a, r on photon A by acting on it the operator

$$E_{ar} = (-1)^a |a\rangle_A \langle a \oplus r| + |a \oplus 1\rangle_A \langle a \oplus r \oplus 1|, \tag{2.3}$$

with $\oplus$ an addition mod 2 and $|0\rangle$ ($|1\rangle$) denoting $|H\rangle$ ($|V\rangle$) for convenience. Explicitly,

$$\begin{cases} E_{00} = |H\rangle_A \langle H| + |V\rangle_A \langle V|, \\ E_{01} = |H\rangle_A \langle V| + |V\rangle_A \langle H|, \\ E_{10} = |H\rangle_A \langle H| - |V\rangle_A \langle V|, \\ E_{11} = |H\rangle_A \langle V| - |V\rangle_A \langle H|. \end{cases} \tag{2.4}$$

This encoding operation transforms the initial state $|\Psi\rangle_{AB}$ to

$$\begin{aligned} |\Phi_{ar}\rangle_{AB} &= \frac{1}{2}[(E_{ar} |H\rangle_A) |H\rangle_B + (E_{ar} |V\rangle_A) |V\rangle_B] \\ &\quad (|a0\rangle_A |b0\rangle_B + |a1\rangle_A |b1\rangle_B). \end{aligned} \tag{2.5}$$

Alice keeps photon A with herself but forwards photon B to Bob.

As will soon be made clear, although Alice does nothing on photon B, Bob is still able to obtain Alice's encoded bits. This is because photon B is quantumly correlated with photon A. Furthermore, the correlation due to hyperentanglement between photon A and photon B allows the decoding process to be done deterministically and nonlocally, *i.e.*, each of the two parties can manipulate his/her photon locally at their own station without the need for either party to possess both the photons at hand.

Step 3. Right after Bob confirms receipt of photon B, the two parties independently proceed to their sequential actions (from left to right in the figure) by means of the optical devices arranged as in Fig. 1, where PBS is a polarization beam splitter which transmits horizontally polarized photons but reflects vertically polarized photons, HWP is a half-wave plate which converts $|H\rangle$ ($|V\rangle$) to $(|H\rangle + |V\rangle)/\sqrt{2}$ ($(|H\rangle - |V\rangle)/\sqrt{2}$) and A_{ij} (B_{ij}) with $i, j \in \{0, 1\}$ are single-photon photodetectors at Alice's (Bob's) station.

It is obvious that photon A may hit only one of Alice's four photodetectors, while photon B behaves the same way with Bob's four photodetectors. Here, of

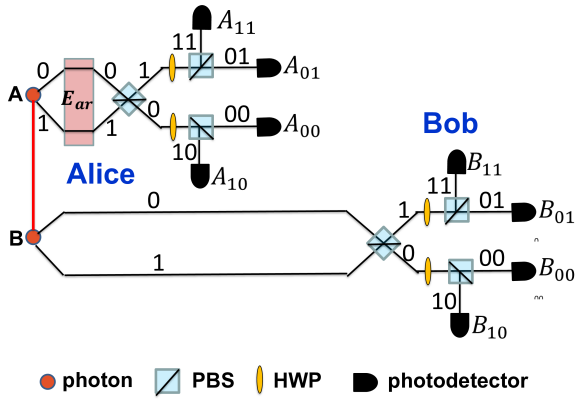

Figure 1. Message round. Alice encodes her informative bit a and random bit r on photon A of a hyperentangled state $|\Psi\rangle_{AB}$ given by Eq. (2.2), then sends photon B to Bob. Alice (Bob) detects photon A (B) by a set of photodetectors $\{A_{ij}\}$ with $i,j \in \{0,1\}$ ($\{B_{kl}\}$ with $k,l \in \{0,1\}$). The encoded bits and detection results are bound by the relationships $a = i \oplus k$ and $r = j \oplus l$. PBS is polarization beam splitter and HWP is half-wave plate. The spatial path labels 0, 1, 00, 01, 10 and 11 respectively imply $a0$, $a1$, $a00$, $a01$, $a10$ and $a11$ ($b0$, $b1$, $b00$, $b01$, $b10$ and $b11$) if the paths belong to photon A (B).

importance is the fact that, thanks to the hyperentanglement there exists non-classical correlations between Alice's encoded bits a, r and the corresponding combination of clicks of Alice's and Bob's photodetectors, despite the distance between them. In other words, which ones of the photodetectors would click are dictated by both the informative bit a and the random bit r. Such spooky distance-independent correlations provide Bob the ability to decode Alice's bits with certainty. To derive the decoding rule it is necessary to consider in detail all the four possible cases of a and r, namely, $\{a = 0, r = 0\}$, $\{a = 0, r = 1\}$, $\{a = 1, r = 0\}$ and $\{a = 1, r = 1\}$. For a given pair of $\{a, r\}$, after being acted in sequence by the devices shown in Fig. 1, the state $|\Phi_{ar}\rangle_{AB}$ in Eq. (2.5) of photons A and B becomes $|\Omega_{ar}\rangle_{AB}$ before hitting the photodetectors. Explicit expressions of $|\Omega_{ar}\rangle_{AB}$ can be derived (the detailed steps of derivation not shown to save the space) in the forms

$$
\begin{aligned}
|\Omega_{00}\rangle_{AB} \;=\; & \frac{1}{2}[|H,a00\rangle_A\,|H,b00\rangle_B + |H,a01\rangle_A\,|H,b01\rangle_B \\
& + |V,a10\rangle_A\,|V,b10\rangle_B + |V,a11\rangle_A\,|V,b11\rangle_B],
\end{aligned} \tag{2.6}
$$

$$|\Omega_{01}\rangle_{AB} = \frac{1}{2}[|H,a00\rangle_A|H,b01\rangle_B + |H,a01\rangle_A|H,b00\rangle_B - |V,a10\rangle_A|V,b11\rangle_B - |V,a11\rangle_A|V,b10\rangle_B], \tag{2.7}$$

$$|\Omega_{10}\rangle_{AB} = \frac{1}{2}[|H,a00\rangle_A|V,b10\rangle_B + |H,a01\rangle_A|V,b11\rangle_B + |V,a10\rangle_A|H,b00\rangle_B + |V,a11\rangle_A|H,b01\rangle_B], \tag{2.8}$$

$$|\Omega_{11}\rangle_{AB} = \frac{1}{2}[-|H,a00\rangle_A|V,b11\rangle_B - |H,a01\rangle_A|V,b10\rangle_B + |V,a10\rangle_A|H,b01\rangle_B + |V,a11\rangle_A|H,b00\rangle_B], \tag{2.9}$$

with aij (bij) denoting the spatial path along which photon A (B) is heading to photodetector A_{ij} (B_{ij}) and $|H,a00\rangle_A \equiv |H\rangle_A|a00\rangle_A$, $|H,b01\rangle_B \equiv |H\rangle_B|b01\rangle_B$, *etc.*.

Equations (2.6) - (2.9) reveal important relations between a, r and the combination of photodetectors' clickings. Namely, as followed from Eq. (2.6), whenever either two photodetectors $\{A_{00}$ and $B_{00}\}$ or $\{A_{01}$ and $B_{01}\}$ or $\{A_{10}$ and $B_{10}\}$ or $\{A_{11}$ and $B_{11}\}$ co-click (each event occurs with an equal probability of 1/4), Alice's encoded bits can be retrodicted as $a = 0$ and $r = 0$. Alternatively, as followed from Eq. (2.7), whenever two photodetectors $\{A_{00}$ and $B_{01}\}$ or $\{A_{01}$ and $B_{00}\}$ or $\{A_{10}$ and $B_{11}\}$ or $\{A_{11}$ and $B_{10}\}$ co-click (each event also occurs with an equal probability of 1/4), Alice's encoded bits can be retrodicted as $a = 0$ and $r = 1$. Similar retrodictions apply to Eqs. (2.8) and (2.9) too. It is interesting that by a closer inspection of Eqs. (2.6) - (2.9) we are able to work out a simple general decoding rule as follows. Suppose that Alice's photodetector A_{ij} and Bob's photodetector B_{kl} co-click. Then the mentioned quantum correlations relate the detection outcomes such that $k = i \oplus a$ and $l = j \oplus r$. Hence, if Alice lets Bob know i, j via a reliable classical communication channel, then Bob can easily infer Alice's informative bit a as well as her random bit r by the following simple rule:

$$a = i \oplus k \,\text{and}\, r = j \oplus l. \tag{2.10}$$

Step 4. Alice and Bob detect their photons by their photodetectors. Then Alice publicly announces which one of her photodetectors clicks. This public announcement allows Bob to decode Alice's bits using his own photodetection outcome, in accordance to the rule (2.10).

By the way, it is worth noting that if ordinary entanglement in terms only of P-DOF is exploited (*i.e.*, the entangled state that Alice initially prepares is of the form $(|H\rangle_A|H\rangle_B + |V\rangle_A|V\rangle_B)/\sqrt{2}$), then Bob is unable to obtain full

information of Alice by just manipulating photon B. In this scenario, in order for Bob to decode, Alice after encoding her information must also send photon A to Bob. That is, photon transmission is required twice: the earlier transmission is for photon B and the later one is for photon A. Only when Bob possesses at hand both photons B and A, he would perform a Bell-state measurement, which is a joint measurement on the two photons, to infer the two bits a and r. Unfortunately, the complete Bell-state measurement is impossible by means of linear-optics toolbox [55]. Therefore, Bob is unable to obtain Alice's two bits deterministically since the Bell-state measurement only succeeds probabilistically. Here, hyperentanglement is employed and the two Alice's bits (a and r) can at the same time be conveyed by sending only one photon (photon B), because complete resolution of the four Bell states in P-DOF can be done nonlocally and unambiguously with the help of the additional entanglement in S-DOF. This is a pronounced advantage of using hyperentanglement over using ordinary entanglement. In this connection, we note that the fact that two bits (a and r) are communicated by sending one photon does not violate the Holevo's bound [56] at all because a photon in the hyperentangled state (2.5) is worth of two qubits: one is associated with the polarization and the other one with the spatial path.

Step 5. After applying the rule (2.10) in the previous step to decode a and r Bob can communicate his informative bit b with Alice by making use of the random bit r. Concretely, Bob forms a bit x which is determined by $x = r \oplus b$ and makes x public. Since Alice knew r she is able, after having heard x from Bob's public announcement, to decode Bob's informative bit as $b = r \oplus x$. Since r is random (but known to Alice) and so is x, only Alice but no one else is able to learn the value of b. That is, no useful information is leaked out to third parties.

The above-described five-step procedure constitutes a round called message round by which one informative bit of Alice (bit a) and one informative bit of Bob (bit b) are exchanged between the two parties.

At this point one might think that Bob could communicate with Alice one more informative bit, say bit b', by forming and publicly publishing a new bit x' such that $x' = b' \oplus a$. As Alice knew bit a, she can know b' too, by adding (mod 2) a and x', *i.e.*, $b' = a \oplus x'$. Although no third parties can precisely infer the value of each of the two bits b' and a but they know for free x' which is the classical correlation between Alice's and Bob's informative bits. According to information-theoretic security assessment this amounts to a partial leakage of useful information [57, 58] (that is also the reason why in the private key cryptosystem the key should not be used twice and so the name one-time pad). Therefore, only the bit r is relevant for Bob to use to encode his informative bit b because both r and $x = r \oplus b$ are random bits containing no information and thus ensuring confidentiality of the informative bit b.

2.2. Control round

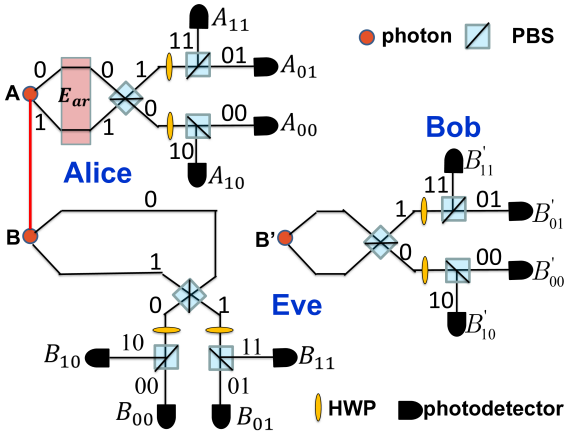

Figure 2. The capture-replace-and-resend #1 attack. Eve prepares photon B' in a hyperstate, then captures photon B of Alice's hyperentangled state $|\Psi\rangle_{AB}$ when it is travelling from Alice to Bob, replaces photon B by photon B' and sends photon B' to Bob. Alice detects photon A by a set of photodetectors $\{A_{ij}\}$, Eve detects photon B by a set of photodetectors $\{B_{kl}\}$ while Bob detects photon B' by a set of photodetectors $\{B'_{k'l'}\}$. When Alice discloses ij Eve is able to correctly decode Alice's bits, but Bob is unable to do so. PBS, HWP and the spatial path labels are same as in Fig. 1.

The message round would work perfectly in the absence of Eve who aims to attack the quantum channel with an attempt to eavesdrop the communication between the two authorized parties Alice and Bob. In practice Eve is most likely present and tries her best to steal any useful information. In principle, Eve is most powerful and may attack in many ways during the time the photon (photon B) travels from Alice to Bob. One Eve's possible strategy, which is named here the "capture-replace-and-resend #1" attack, goes like this (see Fig. 2). After photon B leaves Alice and is traveling midway to Bob, Eve captures photon B and replaces it by another fake photon B' which she prepares in a hyperstate and sends it on to Bob. As Bob cannot distinguish photon B' from photon B so he treats B' as B. Both Eve and Bob proceed to do the necessary actions as detailed in the message round: Eve with the right photon B (which was hyperentangled with photon A) while Bob with the fake one B' (which was prepared by Eve and had no correlations with photon A). When Alice broadcasts her detection results, only Eve is able to obtain the correct bits of Alice but Bob is not. Moreover, because the bits decoded by Bob in

this situation are wrong, Bob's classical encoding is wrong too and hence Alice cannot obtain the faithful informative bit of Bob.

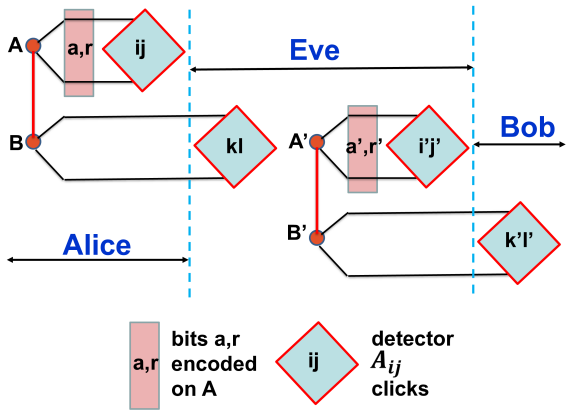

Figure 3. The capture-replace-and-resend #2 attack. Eve prepares her own hyperentangled state $|\Psi\rangle_{A'B'}$ and encodes her bits a' and r' on photon A'. When Alice's photon B is being on the way to Bob, Eve captures photon B but sends her photon B' to Bob. Hence, Alice holds photon A, Eve possesses photons A' and B, while photon B' is with Bob. Alice detects photon A by a set of photodetectors $\{A_{ij}\}$, Eve detects photon B by a set of photodetectors $\{B_{kl}\}$ and photon A' by a set of photodetectors $\{A'_{i'j'}\}$ while Bob detects photon B' by a set of photodetectors $\{B'_{k'l'}\}$. When Alice broadcasts her detection outcome ij Eve is able to steal both Alice's and Bob's bits but Alice and Bob themselves cannot exchange their bits faithfully (see text). A rectangular with a, r (a', r') implies that bíts a and r (a' and r') are encoded on photon A (A') and a diamond with ij (kl, $i'j'$ and $k'l'$) indicates that photon A (B, A' and B') is detected by photodetector A_{ij} (B_{kl}, $A'_{i'j'}$ and $B'_{k'l'}$).

A more complicated but very dangerous strategy, named the "capture-replace-and-resend #2" attack, can be deployed as follows (see Fig. 3). Eve prepares a pair of hyperentangled photons in the form $|\Psi\rangle_{A'B'}$ of Eq. (2.2) and encodes two bits a', r' on photon A'. She then captures Alice's photon B when it is being on the way to Bob, replaces it by photon B' and sends photon B' on to Bob. As a consequence, now Alice holds photon A, Eve possesses photon A' and photon B, while photon B' is with Bob. Each of the three parties operates on their photon as in the message round. As results, photon A is detected by Alice's photodetector A_{ij}, photon B and photon A' are respectively detected by Eve's photodetectors B_{kl} and $A'_{i'j'}$, while photon B' is detected by Bob's photodetector $B'_{k'l'}$. When Alice publicly publishes her detection results ij, Eve

can correctly decode Alice's bits as $a = i \oplus k$ and $r = j \oplus l$, but Bob cannot because his decoding yields $i \oplus k' = a'' \neq a$ and $j \oplus l' = r'' \neq r$. To communicate his informative bit b, Bob publicly publishes a bit $x'' = r'' \oplus b$. Having heard x'', Alice's decoding gives $x'' \oplus r = r'' \oplus b \oplus r$ which is not Bob's bit b since $r'' \neq r$ as seen above. As opposed to Alice, Eve is able to obtain Bob's bit by making use of x'' together with j (announced by Alice) and r', j' (Eve's decoded bit and detection outcome) as $x'' \oplus j \oplus r' \oplus j' = b$. In short, by the "capture-replace-and-resend #2" attack Eve succeeds in stealing both Alice's and Bob's bits while the bits exchanged between Alice and Bob are wrong ones!

To counteract against such and other kinds of attack of Eve, Alice and Bob must comply some efficient method to control the process of exchanging their messages. Here decoy photons come into play. Alice simultaneously uses both P-DOF and S-DOF to prepare a single photon in a double-DOF state that we call single-photon hyperstate (or just hyperstate for short). Afterwards, Alice sends the photon in the prepared hyperstate to Bob. Concretely, Alice prepares a photon, say, photon C, which is randomly chosen in one of the sixteen hyperstates of the forms

$$\left\{\begin{array}{c} |H\rangle_C |c0\rangle_C, |H\rangle_C |c1\rangle_C, |V\rangle_C |c0\rangle_C, |V\rangle_C |c1\rangle_C, \\ |H\rangle_C |S_+\rangle_C, |H\rangle_C |S_-\rangle_C, |V\rangle_C |S_+\rangle_C, |V\rangle_C |S_-\rangle_C, \\ |P_+\rangle_C |c0\rangle_C, |P_+\rangle_C |c1\rangle_C, |P_-\rangle_C |c0\rangle_C, |P_-\rangle_C |c1\rangle_C, \\ |P_+\rangle_C |S_+\rangle_C, |P_+\rangle_C |S_-\rangle_C, |P_-\rangle_C |S_+\rangle_C, |P_-\rangle_C |S_-\rangle_C, \end{array}\right. \tag{2.11}$$

with $|P_\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$ and $|S_\pm\rangle = (|c0\rangle \pm |c1\rangle)/\sqrt{2}$. The above sixteen hyperstates are composed of four groups, each contains four members listed in a line of (2.11). The first, second, third and fourth group are prepared in the combination of bases $\{|H\rangle, |V\rangle\} \otimes \{|c0\rangle, |c1\rangle\}$, $\{|H\rangle, |V\rangle\} \otimes \{|S_+\rangle, |S_-\rangle\}$, $\{|P_+\rangle, |P_-\rangle\} \otimes \{|c0\rangle, |c1\rangle\}$ and $\{|P_+\rangle, |P_-\rangle\} \otimes \{|S_+\rangle, |S_-\rangle\}$, respectively. Due to the obvious equalities $|\langle H|\ P_\pm\rangle|^2 = |\langle V|\ P_\pm\rangle|^2 = |\langle c0|\ S_\pm\rangle|^2 = |\langle c1|\ S_\pm\rangle|^2 = 1/2$, any pair of hyperstates belonging to different groups are not orthogonal to each other, implying impossibility of distinguishing them with certainty. These non-orthogonalities of the hyperstates serve as the clue for detecting Eve. Namely, after Bob confirms his receipt of a photon (which may be the right one prepared by Alice or the fake one prepared by Eve in the "capture-replace-and-resend" attacks), Alice is aware of the right time for her to safely declare that the photon Bob received is a decoy one for checking possible eavesdroppers. Next, she openly reveals the combination of bases in which she prepared her photon. Bob then measures his photon in the combination of bases announced by Alice and lets Alice informed of the measurement outcome. If there are no eavesdroppers, the photon hyperstate that Bob finds in his measurement should match that of the photon prepared by Alice. Since Alice's decoy photon is not in any way entangled with Eve's photon, a mismatch most likely happens between the hyperstate measured by Bob on Eve's photon and the hyperstate

prepared by Alice. So, any mismatch mentioned above signals the presence of Eve. Such procedure for checking eavesdroppers constitutes a round called control round in which Eve is detectable with a high probability. This control technique based on decoy photon in hyperstate is also valid for other kinds of Eve's attacks. In our protocols to be presented in the next section many control rounds will be carried out. In fact, Eve might pass one or several first control rounds but must eventually be catched because the detection probability is quickly increasing with the number of control rounds made [21, 22].

3. Quantum protocols for secure direct message exchange

In this section we are interested in secure exchanging of entire long messages. Now Alice's message MA is exhibited in terms of a list of N informative bits, *i.e.*, $MA = \{a_1, a_2, ..., a_N\}$ with $a_n \in \{0, 1\}$ $\forall n$, while the message of Bob is another list of the same number of informative bits, *i.e.*, $MB = \{b_1, b_2, ..., b_N\}$ with $b_n \in \{0, 1\}$ $\forall n$. The goal of Alice and Bob is to exchange their messages securely and directly though a quantum channel combined with reliable classical communications. We shall propose two protocols to achieve that goal. The first protocol, Protocol 1, is unconditionally secure but requires quantum memories. The second protocol, Protocol 2, does not need quantum memories but its security is asymptotic.

3.1. Protocol 1

This protocol goes step by step as follows.

Step 1. Alice prepares N hyperentangled states $\{|\Psi_1\rangle_{A_1B_1}, |\Psi_2\rangle_{A_2B_2}, ..., |\Psi_N\rangle_{A_NB_N}\}$ with

(3.1)
$$|\Psi_n\rangle_{A_nB_n} = \frac{1}{2}(|H\rangle_{A_n}|H\rangle_{B_n} + |V\rangle_{A_n}|V\rangle_{B_n})(|a0\rangle_{A_n}|b0\rangle_{B_n} + |a1\rangle_{A_n}|b1\rangle_{B_n})$$

and a list $LR = \{r_1, r_2, ..., r_N\}$, with $r_n \in \{0, 1\}$ $\forall n$ a random bit. She also prepares a separate long enough sequence S_C of M decoy photons in hyperstates $\{|\Delta_m\rangle_{C_m}; m = 1, 2, ..., M\}$, with $|\Delta_m\rangle_{C_m}$ being randomly one of the sixteen hyperstates of the forms

(3.2)
$$\begin{cases} |H\rangle_{C_m}|c0\rangle_{C_m}, |H\rangle_{C_m}|c1\rangle_{C_m}, |V\rangle_{C_m}|c0\rangle_{C_m}, |V\rangle_{C_m}|c1\rangle_{C_m}, \\ |H\rangle_{C_m}|S_+\rangle_{C_m}, |H\rangle_{C_m}|S_-\rangle_{C_m}, |V\rangle_{C_m}|S_+\rangle_{C_m}, |V\rangle_{C_m}|S_-\rangle_{C_m}, \\ |P_+\rangle_{C_m}|c0\rangle_{C_m}, |P_+\rangle_{C_m}|c1\rangle_{C_m}, |P_-\rangle_{C_m}|c0\rangle_{C_m}, |P_-\rangle_{C_m}|c1\rangle_{C_m}, \\ |P_+\rangle_{C_m}|S_+\rangle_{C_m}, |P_+\rangle_{C_m}|S_-\rangle_{C_m}, |P_-\rangle_{C_m}|S_+\rangle_{C_m}, |P_-\rangle_{C_m}|S_-\rangle_{C_m}. \end{cases}$$

She then for each $n \in \{1, 2, ..., N\}$ encodes a_n and r_n on the pair $|\Psi_n\rangle_{A_nB_n}$ by acting on photon A_n the operator

$$E_{a_n r_n} = (-1)^{a_n} |a_n\rangle_{A_n} \langle a_n \oplus r_n| + |a_n \oplus 1\rangle_{A_n} \langle a_n \oplus r_n \oplus 1| . \tag{3.3}$$

After the encoding Alice splits the N hyperentangled photon pairs $\{|\Psi_n\rangle_{A_nB_n}; n = 1, 2, ..., N\}$ into two sequences S_A and S_B, with S_A containing N photons $A_1, .., A_N$ and S_B containing N photons $B_1, .., B_N$, *i.e.,* $S_A = \{A_1, A_2, ..., A_N\}$ and $S_B = \{B_1, B_2, ..., B_N\}$. She stores the sequence S_A in her quantum memory for later use. As for the sequence S_B, she enlarges it by inserting within it the M decoy photons from the sequence S_C in random positions, which are unknown to anyone but Alice. The resulting sequence of $N + M$ photons denoted by S_{BC} is sent to Bob by means of block transmission (see, *e.g.* [9, 11]).

Step 2. Alice has to wait a while until Bob confirms her his receipt of a block of $N + M$ photons (among them there might be fake photons which are prepared by Eve to replace Alice's original photons during the photon block transmission from Alice to Bob). Only after hearing from Bob, Alice unveils the exact positions of the M decoy photons according to which Bob splits the obtained block of $N + M$ photons into two sequences: sequence S'_B of N photons and the remaining sequence S'_C of M photons. He stores the sequence S'_B in his quantum memory for later use and the two parties run M control rounds for each photon of the sequence S'_C. If the number of mismatches in the M control rounds exceeds a preset value corresponding to a desired security level, the two parties realize Eve's presence and abort the protocol to restart from the beginning. Otherwise, it implies that there was no eavesdropping and the sequence S'_B would be identical to Alice's original sequence S_B. The two parties thus continue on to the next step.

Step 3. Alice and Bob restore the photon sequences S_A and $S'_B \equiv S_B$ from their quantum memories, respectively. Afterwards, they run N message rounds for each of the N photon pairs A_nB_n $(n = 1, 2, ..., N)$ of the sequences S_A and S_B. After an n^{th} message round Alice is able to communicate with Bob her informative bit a_n while Bob at the same time is able to communicate with Alice his informative bit b_n. Therefore, when all N message rounds are completed, Alive and Bob succeed in exchanging their entire messages $MA = \{a_1, a_2, ..., a_N\}$ and $MB = \{b_1, b_2, ..., b_N\}$. Their direct exchange of messages is absolutely secure.

3.2. Protocol 2

In Protocol 1 Alice and Bob first check the presence of Eve by running M control rounds. Only after they are sure of no Eve present they start to run N message rounds, so Alice's message MA and Bob's message MB are

securely exchanged as a whole upon the completion of the protocol. Protocol 1, however, suffers from two limitations. One limitation concerns the block transmission of photons which might disturb the photon order, especially when N and M are large enough or the route from Alice to Bob is long enough. The other more serious limitation is associated with the compulsory need of having high capacity and long operating time quantum memories at both Alice's and Bob's stations.

In this subsection we shall design another protocol, called Protocol 2, in such a way that neither the block transmission of photons nor the quantum memories are required at all. In contrast to Protocol 1, Protocol 2 will be executed by sending photon by photon, and for each sent photon which kind of round (*i.e.*, message round or control round) to be run is decided by Alice in due time and in a probabilistic fashion. The decided round is processed immediately with the corresponding photon without storing it in a quantum memory. Formally, Protocol 2 is executed as a run of the following programme.

S0. Set $n = 0$

S1. Set $n = n+1$. Alice creates a random bit $s_n \in \{0, 1\}$, then reads its value (approximately, a coin tossing could be done with tail corresponding to $s_n = 0$ and head to $s_n = 1$). If $s_n = 1$ the programme continues to S2. Otherwise, if $s_n = 0$ Alice and Bob perform the control round as described in subsection 2.2 (That is, Alice prepares a single photon C_n randomly in one of the sixteen hyperstates defined by (3.2) and sends C_n to Bob. After Bob responds, Alice tells Bob that this photon is a decoy one, and so on). If mismatch is found in the prepared-by-Alice and measured-by-Bob hyperstates, the two parties return to S0 to restart the programme. Otherwise, they continue to S2.

S2. Alice and Bob perform the message round as described in subsection 2.1 (*i.e.*, Alice prepares a hyperentangled state $|\Psi_n\rangle_{A_nB_n}$ of the form (3.1) of a photon pairs A_n and B_n. Then, she generates a random bit $r_n \in \{0, 1\}$ and encodes a_n, r_n on photon A_n by acting on it the operator $E_{a_n r_n}$. Next, she keeps photon A_n with herself and sends photon B_n to Bob, and so on). As a result, upon the completion of the message round Bob gets Alice's informative bit a_n and, at the same time, Alice gets Bob's informative bit b_n, *i.e.*,. they succeed in exchanging their n^{th} informative bits.

S3. If $n < N$ the programme goes to S1. Otherwise, if $n = N$ the programme stops, implying that Protocol 2 is completed: Alice and Bob have exchanged all the informative bits of their messages.

According to the above design, in each message round (from the 1^{st} to the N^{th} message round) Alice can be looked upon as "asking" an informative bit and Bob as "answering" by another informative bit. Such "asking" and "answering" much resembles a dialogue being going on between the two parties. That is why the name "quantum dialogue" has come for protocols of the type

of Protocol 2 [21]. As for the security, whenever a mismatch is encountered in a control round, Protocol 2 is re-initiated. Eve may luckily pass several first control rounds but she will eventually be caught" when the number of control rounds is sufficiently large, that is necessary for exchanging sufficiently long messages. In this sense, Protocol 2 is secure asymptotically [21, 22]. Regarding this security issue, to avoid any possible partial leakage of useful information to Eve, it is advised to construct the messages MA and MB such that their precisely useful meaning is obtained only when all the bits or a large enough number of bits of the messages are successfully exchanged (*i.e.*, no useful information is contained in a number of the initial bits of the messages that Eve might get).

4. Conclusion

We have proposed two quantum protocols for two remote parties to exchange their secret messages. The quantum resources used are quantum-correlated photon pairs and single photons, both are encoded simultaneously in both P-DOF and S-DOF. The most outstanding advantage is the use of hyperentangled photon pairs that features our protocols over many previous protocols based on conventionally entangled photons. The hyperentanglement enables exchanging messages directly without sharing any keys in advance. This also deterministically provides full high capacity of the quantum channel for information transmission because the resolution of all Bell states is 100% executable by linear-optic tools. Of particular importance is the fact that the Bell states' resolution can be done in a nonlocal manner (*i.e.*, only by means of local operations and classical communication), requiring to transmit the photon (photon block in Protocol 1 or single photons in Protocol 2) only once from one to the other party, as opposed to many other previous protocols which are based on conventional entanglement and need to transmit the photon twice between the two parties. This fact plays a significant role since it reduces eavesdropping chance by 50% as well as greatly saves the protocols' performance time. Security of our protocols is guaranteed by control rounds where single photons as decoys are exploited. Note that here the decoy photons are prepared in non-orthogonal hyperstates rather than in non-orthogonal conventional states as in [3], thus boosting the probability of Eve's detection.

At first, our Protocol 1 seems somewhat resembling to that in [53]. Nevertheless, there are sharp differences. In [53] only the message of one party (say, Alice) is conveyed to the other party (say, Bob), *i.e.*, the information flows only one-way and no exchange of messages happens. To convey information in the

opposite direction (say, from Bob to Alice) the protocol in [53] must be done one more time with Alice's and Bob's roles interchanged (*i.e.*, two separate protocols to be performed: one for Alice to transmit her message to Bob and the other for Bob to transmit his message to Alice). In our Protocol 1 the messages of the two parties are simultaneously exchanged in one and the same protocol which is much more convenient. Moreover, the protocol in [53] uses hyperentangled photon pairs for both message transmission and eavesdropping check, whereas in ours the photon pairs are used only in the message rounds. In the control rounds, which are devised to check eavesdropping, we only utilize single photons as decoy ones, thereby cutting the quantum resource cost (half the photon number for detecting Eve in [53] is economized yet maintaining the same security level) and, at the same time, simplifying the quantum operations (preparation of single photons is easier than preparation of entangled pairs and measurement on a single photon by one party as in our control rounds is simpler than measurements on two separate photons of a hyperentangled pair by both the parties as in [53]).

In conclusion, as our protocols do not demand nonlinear-optic devices, they would be realizable experimentally within the present technology levels and thus promise diverse applications in quantum information processing and quantum computing.

References

[1] **Rivest R., Shamir A. and Adleman L.**, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems.* Communications of the ACM **21** (1978), 120.

[2] **Shor P. W.**, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring.* Proc. 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press. (1994) 124

[3] **Bennett C. H. and Brassard G.,** *Quantum Cryptography: Public Key Distribution and Coin Tossing.* Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing (Bangalore) (1984) 175.

[4] **Ekert A. K.**, *Quantum cryptography based on Bell's theorem.* Phys. Rev. Lett. **67** (1991) 661.

[5] **Bennett C. H.**, *Quantum cryptography using any two nonorthogonal states*. Phys. Rev. Lett. **68** (1992) 3121.

[6] **Shannon C.**, *Communication theory of secrecy systems*. Bell System Technical Journal **28** (1949) 656.

[7] **Bostrom K. and Felbinger T. F.**, *Deterministic Secure Direct Communication Using Entanglement.* Phys. Rev. Lett. **89** (2002) 187902.

[8] **Beige A., Englerta B. G., Kurtsieferc Ch.and Weinfurter H.**, *Secure communication with a publicly known key*. Acta Phys. Pol. A **101** (2002) 357.

[9] **Deng F. G., Long G. L. and Liu X. S.,** *Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block*. Phys. Rev. A **68** (2003) 042317.

[10] **Deng F. G. and Long G. L.**, *Secure direct communication with a quantum one-time pad*. Phys. Rev. A **69** (2004) 052319.

[11] **Li X. H., Zhou P., Liang Y. J., Li C. Y., Zhou H. Y. and Deng F. G.**, *Quantum Secure Direct Communication Network with Two-Step Protocol*. Chin. Phys. Lett. **23** (2006) 1080.

[12] **Hu J. Y., Yu B., Jing M. Y., Xiao L. T., Jia S. T., Qin G. Q. and Long G. L.**, *Experimental quantum secure direct communication with single photons*. Light: Sci. & Appl. **5** (2016) e16144.

[13] **Zhang W., Ding D. S., Sheng Y. B., Zhou L., Shi B. S. and Guo G. C.**, *Quantum Secure Direct Communication with Quantum Memory*. Phys. Rev. Lett. **118** (2017) 220501.

[14] **Zhu F., Zhang W., Sheng Y. B. and Huang Y. D.**, **Experimental long-distance quantum secure direct communication.** Sci. Bull. **62** (2017) 1519.

[15] **Pan D., Lin Z. S., Wu J. W., Zhang H. R., Sun Z., Ruan D., Yin L. G. and Long G. L.**, *Experimental free-space quantum secure direct communication and its security analysis*. Photon. Res. **8** (2020) 1522.

[16] **Srikara S., Thapliyal K. and Pathak A.,** *Continuous variable direct secure quantum communication using Gaussian states*. Quant. Inf. Process. **19** (2020) 132.

[17] **Nayana D. and Goutam P.**, *Cryptanalysis of quantum secure direct communication protocol with mutual authentication based on single photons and Bell states*. Europhys. Lett. **138** (2022) 48001.

[18] **Zhang H. R., Sun Z., Qi R. Y., Yin L. G., Long G. L. and Lu J. H.**, *Realization of quantum secure direct communication over 100 km fiber with time-bin and phase quantum states.* Light Sci. & Appl. **11** (2022) 83.

[19] **Pan D., Song X. T. and Long G. L.**, *Free-space quantum secure direct communication: basics, progress, and outlook.* Advanced Devices & Instrunentation **4** (2023) 0004.

[20] **Panda S. S., Yasir P. A. A. and Chandrashekar C. M.**, *Quantum direct communication protocol using recurrence in k-cycle quantum walks.* Phys. Rev. A **107** (2023) 022611.

[21] **Nguyen B. A.**, *Quantum dialogue.* Phys. Lett. A **328** (2004) 6.

[22] **Nguyen B. A.**, *Secure dialogue without a prior key distribution.* J. Kor. Phys. Soc. **47** (2005) 562.

[23] **Yan C., Man Z. X. and Xia Y. J.**, *Quantum Bidirectional Secure Direct Communication via Entanglement Swapping.* Chin. Phys. Lett. **24** (2007) 19.

[24] **Shi G. F., Xi X. Q. and Tian X. L.**, *Bidirectional quantum secure communication based on a shared private Bell state.* Opt. Commun. **282** (2009) 2460.

[25] **Shan C. J., Liu J. B., Cheng W. W., Liu T. K., Huang Y. X. and Li H.**, *Bidirectional quantum secure direct communication in driven cavity QED.* Mod. Phys. Lett. B **23** (2009) 3225.

[26] **Shi G. F., Xi X. Q. and Hu M. L.**, *Quantum secure dialogue by using single photons.* Opt. Commun. **283** (2010) 1984.

[27] **Gao G.**, *Two quantum dialogue protocols without information leakage.* Opt. Commun. **283** (2010) 2288.

[28] **Shi G. F.**, *Bidirectional quantum secure communication scheme based on Bell states and auxiliary particles.* Opt. Commun. **283** (2010) 5275.

[29] **Pathak A.**, *Efficient protocols for unidirectional and bidirectional controlled deterministic secure quantum communication: different alternative approaches.* Quant. Inf. Process. **14** (2015) 2195.

[30] **Zhou N. R., Li J. F., Yu Z. B., Gong L. H. and Farouk A.**, *New quantum dialogue protocol based on continuous-variable two-mode squeezed vacuum states.* Quant. Inf. Process. **16** (2017) 4.

[31] **Chauhan S. and Gupta N. L.**, *Bidirectional Quantum Secure Direct Communication Using Dense Coding of Four Qubit Cluster States*. J. Sci. Res. **14** (2022) 179.

[32] **Nguyen B. A.**, *Quantum dialogue by nonselective measurements.* Adv. Nat. Sci. Nanosci. Nanotech. **9** (2018) 025001.

[33] **Nguyen B. A.**, *Quantum dialogue mediated by EPR-type entangled coherent states*. Quant. Inf. Process. **20** (2021) 100.

[34] **Lang Y. F.**, *Efficient Quantum Dialogue Using a Photon in Double Degrees of Freedom*. Int. J. Theor. Phys. **61** (2022) 105.

[35] **Ramachandran M. and Balakrishnan S.**, *Significance of Bell States Over Four-Qubit Entangled States in Quantum Bidirectional Direct Communication Protocols*. Int. J. Theor. Phys. **62** (2023) 180.

[36] **Paul G. and Kwiat J.**, *Hyper-entangled states*. Mod. Opt. **44** (1997) 2173.

[37] **Deng F. G., Ren B. C. and Li X. H.**, *Quantum hyperentanglement and its applications in quantum information processing*. Sci. Bull. **62** (2017) 46.

[38] **Wang X. L., Cai X. D., Su Z. E., Chen M. C., Wu D., Li L., Liu N. L., Lu C. Y. and Pan J. W**., *Quantum teleportation of multiple degrees of freedom of a single photon*. Nature **518** (2015) 516.

[39] **Graham T. M., Bernstein H. J., Wei T. C., Junge M. and Kwiat P. G.**, *Superdense teleportation using hyperentangled photons.* Nat. Commun. **6** (2015) 7185.

[40] **Luo M. X., Li H. R., Lai H. and Wang X.**, *Teleportation of a ququart system using hyperentangled photons assisted by atomic-ensemble memories*. Phys. Rev. A **93** (2016) 012332.

[41] **Walborn S. P.**, *Breaking the communication barrier*. Nat. Phys. **4** (2008) 268.

[42] **Barreiro J. T., Wei T. C. and Kwiat P. G.**, *Beating the channel capacity limit for linear photonic superdense coding*. Nat. Phys. **4** (2008) 282.

[43] **Williams B. P., Sadlier R. J. and Humble T. S.**, *Superdense Coding over Optical Fiber Links with Complete Bell-State Measurements*. Phys. Rev. Lett. **118** (2017) 050501.

[44] **Nawaz M., ul-Islam R. and Ikram M.**, *Remote state preparation through hyperentangled atomic state*. J. Phys. B: At. Mol. Opt. Phys. **51** (2018) 075501.

[45] **Zhou P., Jiao X. F. and Lv S. X.**, *Parallel remote state preparation of arbitrary single-qubit states via linear-optical elements by using hyperentangled Bell states as the quantum channel*. Quant. Inf. Process. **17** (2018) 298.

[46] **Jiao X. F., Zhou P., Lv S. X. and Wang Z. Y.**, *Remote preparation for single-photon two-qubit hybrid state with hyperentanglement via linear-optical elements*. Sci. Rep. **9** (2019) 4663.

[47] **Zhou P. and Lv L.**, *Joint remote preparation of single-photon three-qubit state with hyperentangled state via linear-optical elements*. Quant. Inf. Process. **19** (2020) 283.

[48] **Jiao X. F., Zhou P. and Lv S. X**., *Remote implementation of single-qubit operations via hyperentangled states with cross-Kerr nonlinearity*. J. Opt. Soc. Am. B **36** (2019) 867.

[49] **Nguyen B. A. and Cao T. B.**, *Controlled remote implementation of operators via hyperentanglement*. J. Phys. A: Math. Theor. **55** (2022) 225307.

[50] **Nguyen B. A.**, *Joint remote implementation of operators*. J. Phys. A: Math. Theor. **55** (2022) 395304

[51] **Wu X. D., Zhou L., Zhong W. and Sheng Y. B.**, *High-capacity measurement-device-independent quantum secure direct communication*. Quant. Inf. Process. **19** (2020) 354.

[52] **Gao C. Y., Guo P. L. and Ren B. C.**, *Efficient quantum secure direct communication with complete Bell-state measurement*. Quantum Eng. **3** (2021) e83.

[53] **Sheng Y. B., Zhou L. and Long G. L.**, *One-step quantum secure direct communication*. Sci. Bull. **67** (2022) 367.

[54] **Meng Y., Qu Z., Muhammad G. and Tiwari P.**, *Secure and efficient data transmission based on quantum dialogue with hyperentangled states in cloud office*. Internet of Things **24** (2023) 100911.

[55] **Calsamiglia J. and Lutkenhaus N.**, *Maximum efficiency of a linear-optical Bell-state analyzer*. App. Phys. B **72** (2001) 67.

[56] **Holevo A. S.**, *Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel*. Problems of Information Transmission **9** (1973) 177.

[57] **Gao F., Guo F. Z., Wen Q. Y. and Zhu F. C.**, *Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication.* Sci. Chin. Ser. G: Phys., Mech. Astr. **51** (2008) 559.

[58] **Tan Y. G. and Cai Q. Y.**, *Classical Correlation in Quantum Dialogue.* Int. J. Quant. Inf. **6** (2008) 325.

Nguyen Ba An
Thang Long Institute of Mathematics and Applied Sciences
Thang Long University, Nghiem Xuan Yem, Hoang Mai
Hanoi
Vietnam
annb@thanglong.edu.vn