Quantum Information Processing (2021) 20:100
https://doi.org/10.1007/s11128-021-03007-1

Quantum dialogue mediated by EPR-type entangled coherent states

Nguyen Ba An[1,2]

Received: 20 July 2020 / Accepted: 20 January 2021 / Published online: 8 March 2021

Abstract
Talking with each other on the telephone is convenient but insecure because the conversation content can be eavesdropped perfectly. Quantum dialogue protocols have thus been devised to enable two parties to talk with a reasonable level of security suited to urgent situations without the need of a prior quantum key distribution. Existing protocols use either discrete-variable or continuous-variable entangled states each of which has its own pros and cons. Here we employ Einstein–Podolky–Rosen-type entangled coherent states with fixed and large enough amplitudes which are intermediate between discrete- and continuous-variable states. The outstanding pros is the possibility of unambiguous and efficient identification of a given entangled coherent state which is necessary for the decoding process. Single-mode gates required for the encoding process are executable as well, possibly with the assistance of additional resources. Two types of control methods are introduced to protect the quantum dialogue from outsider's attacks. The information leakage problem is also discussed showing that it hardly influences the protocol security for a long enough dialogue.

Keywords Quantum dialogue · Entangled coherent states · Communication round · Eve in the line · Two types of control round · Information leakage

1 Introduction

Nowadays, talking with each other on mobile smartphones is pleasant and so convenient. However, the whole content of such conversations could be wiretapped by an unauthorized outsider without even knowing it because any classical communi-

✉ Nguyen Ba An
nban@iop.vast.ac.vn; annb@thanglong.edu.vn

1 Thang Long Institute of Mathematics and Applied Sciences, Thang Long University, Nghiem Xuan Yem, Hoang Mai, Hanoi, Vietnam

2 Center for Theoretical Physics, Institute of Physics Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet, Cau Giay, Hanoi, Vietnam

cation can be perfectly eavesdropped. Therefore, secure dialogue or, more generally, secure exchange of information is highly demanded and a good solution proves to be by means of quantum resources' manipulation dictated by laws of Nature. In fact, unconditional secure quantum key distribution (QKD) protocols were designed theoretically and implemented successfully in practice [1–3]. In those protocols, secret keys are beforehand created among remote agents exploiting the laws of quantum physics such as impossibility of cloning an unknown quantum state and collapse of measured states. If any unauthorized agent somehow intervenes in the QKD process, the interference will inevitably leave traces behind that the authorized agents could detect by an appropriate checking method. It is worth mentioning that such QKD protocols are not at all threatened by quantum computers, in contrast with the presently used public key system [4] whose security is based on mathematical difficulty and is breakable in the near future by quantum algorithms on quantum computers. The QKD protocols are indeed absolutely secure like in the proven private key system [5] and, at the same time, get rid of the inconvenience of necessity of authorized agents' gathering in one place for preparing common secret keys.

As a necessary prerequisite, before actually exchanging confidential messages the authorized agents have to perform a QKD protocol that consumes time and much quantum resource. Then, a question arises: "Can they, say, in an urgent situation, still be able to securely exchange their messages without a prior quantum distribution of secret key?" The answer turns out "yes, they can," via the so-called quantum dialogue protocol. The terminology 'quantum dialogue' first appeared in Ref. [6], and since then, a good deal of papers related to this topic have been published addressing wide range of interesting aspects. Not only bipartite entanglement as in the original protocols [6,7], but also multipartite ones have been utilized for the quantum dialogue [9–12]. Hyperentanglement has also been exploited [13], while fault-tolerant asymmetric quantum dialogue protocols [14] and measurement device-independent quantum dialogue [15] as well as affects of quantum field [16] have been investigated. **S**emi-quantum protocols allowing some of the authorized participants to remain classical have also been put forward for secure communication tasks including dialogue [17]. And, recently, nonselective measurements have been shown to be useful in a novel quantum dialogue protocol [18]. The above-cited references deal with discrete-variable quantum states which suffer from certain restrictions regarding processes of their generation and discrimination by means of current technologies. Alternatively, continuous-variable quantum states can also be exploited for quantum information processing which may have some advantages. In fact, new quantum dialogue protocols based on continuous-variable squeezed states have been reported [19–24].

In this paper, we are going to employ entangled coherent states (ECSs) which are intermediate between continuous- and discrete-variable states. They are continuous states because their amplitudes are continuous. However, if the amplitude is fixed to a certain value, they can be looked upon as discrete ones. So far ECSs have not yet been considered for quantum dialogue due to difficulty in direct and feasible performance of single-mode gates. With the techniques developed in [25], (near-)deterministic and efficient coherent-state-based quantum gates can be indirectly implemented inline by means of available linear-optics devices, motivating the idea of considering quantum dialogue which is mediated by ECSs. For pedagogical purpose, we briefly

review in Sect. 2 various types of ECSs with emphasis on the so-called Einstein–Podolsky–Rosen-type (EPR-type) ECSs. In Sect. 3, scheme for discrimination of the four EPR-type ECSs is given. Communication round, i.e., a round of the quantum dialogue protocol in which two authorized parties, Alice and Bob, can exchange their secret bits, is described in Sect. 4, which consists of three Sects. 4.1, 4.2, and 4.3 in order to deal with the details. Section 5 introduces a powerful outsider, Eve, whose aim is to disturb or eavesdrop the conversation between Alice and Bob. In that same Sect. 5, two types of control rounds are proposed to detect Eve: type-1 control round in Sect. 5.1 and type-2 control round in Sect. 5.2. How the protocol of quantum dialogue runs is presented in Sect. 6 with a discussion on the problem of possible information leakage. Finally, we conclude in Sect. 7.

2 Entangled coherent states

Coherent states and entangled coherent states are very important not only in nonlinear and quantum optics, but also in quantum information processing and quantum computing [26,27]. Generally, ECSs are those that entangle $N \geq 2$ different modes which are in coherent states. For $N > 2$ modes, they are referred to as multipartite ECSs. Typical multipartite ECSs are GHZ-type ECSs [28–30], W-type ECSs [31–35], and cluster-type ECSs [36–40]. For $N = 2$ modes when one mode is a coherent state while the other mode is the vacuum state, the corresponding ECS is of the form (up to a normalization factor) $|\alpha\rangle_A |0\rangle_B + |0\rangle_A |\alpha\rangle_B$, with $|\alpha\rangle_{A(B)}$ being a coherent state of mode A (B) with amplitude α and $|0\rangle_{A(B)}$ the vacuum state containing no photons [41]. Such states are in fact composed of infinite superpositions of the so-called NOON states $|N\rangle_A |0\rangle_B + |0\rangle_A |N\rangle_B$ with $|N\rangle_{A(B)}$ a Fock state containing $N > 0$ photons [42], so they can be named NOON-type ECSs. The general two-mode ECSs have the form $\propto |\alpha\rangle_A |\beta\rangle_B + |\gamma\rangle_A |\delta\rangle_B$. In this paper, we are concerned with a special kind of the two-mode ECSs called EPR-type ECSs [43], which consist of the following four states

$$|E_{mn}\rangle_{AB} = N_n[|\alpha\rangle_A \left|(-1)^m\alpha\right\rangle_B + (-1)^n |-\alpha\rangle_A \left|(-1)^{m+1}\alpha\right\rangle_B], \tag{1}$$

where $m, n \in \{0, 1\}$ and

$$N_n = \frac{1}{\sqrt{2\,[1 + (-1)^n \langle\alpha\,|-\alpha\rangle]}} \tag{2}$$

is the normalization factor guaranteeing ${}_{AB}\langle E_{mn}\,|E_{mn}\rangle_{AB} = 1$. For simplicity, here we assume that α is real and large enough (say, $\alpha \geq 2$) so that the scalar product $\langle\alpha\,|-\alpha\rangle = \exp(-2\alpha^2)$ is negligible and N_n can be well approximated to $1/\sqrt{2}$ for both $n = 0$ and $n = 1$. That is, explicitly we shall work with

$$|E_{00}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|\alpha\rangle_A |\alpha\rangle_B + |-\alpha\rangle_A |-\alpha\rangle_B\right), \tag{3}$$

$$|E_{01}\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|\alpha\rangle_A |\alpha\rangle_B - |-\alpha\rangle_A |-\alpha\rangle_B\right), \tag{4}$$

$$|E_{10}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\alpha\rangle_A|-\alpha\rangle_B + |-\alpha\rangle_A|\alpha\rangle_B\right) \tag{5}$$

and

$$|E_{11}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\alpha\rangle_A|-\alpha\rangle_B - |-\alpha\rangle_A|\alpha\rangle_B\right). \tag{6}$$

A certain EPR-type ECS can be produced by superimposing on a balanced beam splitter (BBS) the vacuum state of light $|0\rangle$ and a proper Schrodinger cat state [44]

$$|\text{cat}_\pm\rangle = \frac{1}{\sqrt{2}}\left(\left|\alpha\sqrt{2}\right\rangle \pm \left|-\alpha\sqrt{2}\right\rangle\right), \tag{7}$$

where $|\text{cat}_+\rangle$ ($|\text{cat}_-\rangle$) is called even (odd) cat because it contains only even (odd) photon numbers. Namely, adopting the following transformation for the BBS's action [30]

$$\text{BBS}_{AB}|\alpha\rangle_A|\beta\rangle_B = \left|\frac{\alpha+\beta}{\sqrt{2}}\right\rangle_A\left|\frac{\alpha-\beta}{\sqrt{2}}\right\rangle_B, \tag{8}$$

we have

$$\text{BBS}_{AB}|\text{cat}_\pm\rangle_A|0\rangle_B = \frac{1}{\sqrt{2}}\left(|\alpha\rangle_A|\alpha\rangle_B \pm |-\alpha\rangle_A|-\alpha\rangle_B\right), \tag{9}$$

which are exactly the ECSs $|E_{00}\rangle_{AB}$ or $|E_{00}\rangle_{AB}$, whereas

$$\text{BBS}_{AB}|0\rangle_A|\text{cat}_\pm\rangle_B = \frac{1}{\sqrt{2}}\left(|\alpha\rangle_A|-\alpha\rangle_B \pm |-\alpha\rangle_A|\alpha\rangle_B\right), \tag{10}$$

which are exactly the ECSs $|E_{10}\rangle_{AB}$ or $|E_{11}\rangle_{AB}$.

A cat state $|\text{cat}_+\rangle$ or $|\text{cat}_-\rangle$ with a small amplitude $\alpha \leq 1$, which appears as a kitten state, can be produced by several methods (see, e.g., Refs. [45–47]). Furthermore, a kitten can be "fed" to grow to a cat of desired amplitude $\alpha \geq 2$ [48–50]. Hence, EPR-type ECSs of large enough amplitudes which we are interested in can be considered available to us. Although separable coherent states are the most classical states, ECSs in general and EPR-type ECSs in particular are quantum ones exhibiting 'spooky' nonclassical correlations which promise advantageous applications in various classically impossible tasks. Here we use EPR-type ECSs as carriers of information during the process of quantum dialogue. An important task in running the protocol is the unambiguous discrimination between the EPR-type ECSs which is the content of the next section.

3 Discrimination of the EPR-type ECSs

The two-photon EPR states $\{(|H\rangle_A|H\rangle_B \pm |V\rangle_A|V\rangle_B)/\sqrt{2}, (|H\rangle_A|V\rangle_B \pm |V\rangle_A|H\rangle_B)/\sqrt{2}\}$, with $|H\rangle$ ($|V\rangle$) the horizontally (vertically) polarized single-photon state, were used for quantum dialogue, but the efficiency is low because photons do not talk with each another so these states cannot be distinguished with certainty by means of linear-optics tools [51,52]. The main cause of employing EPR-type ECSs (instead

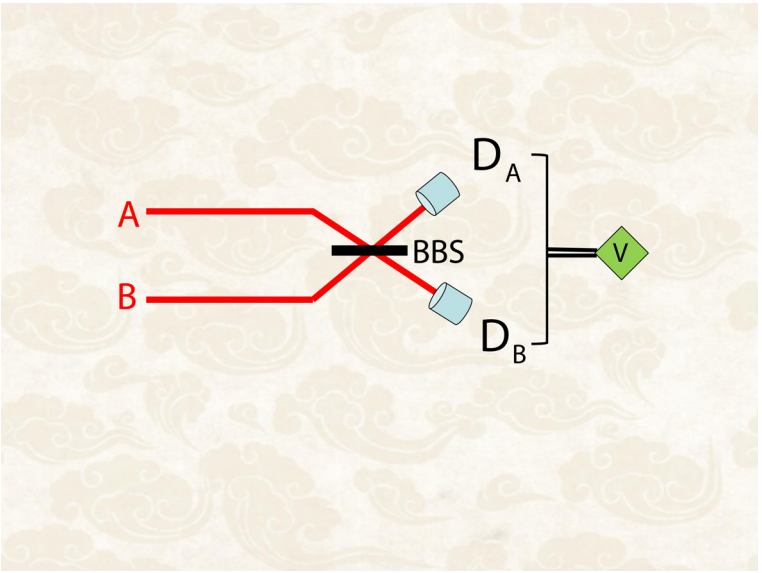

Fig. 1 (Color online) Scheme for identification of a given EPR-type ECS $|E_{mn}\rangle_{AB}$, Eqs. (3)–(6), with BBS a balanced beam splitter and D_A, D_B photon number-resolving detectors. The double line represents the numbers of photon counted by the photo-detectors depending on which the values of m, n are verified in box V

of two-photon EPR states) in the quantum dialogue protocol is the highly simple yet (near-)deterministic and unambiguous discrimination of the four states $|E_{mn}\rangle_{AB}$ defined in Eqs. (3)–(6), which is compulsorily needed for information decoding during the course of quantum dialogue.

Given any one of the four states $|E_{mn}\rangle_{AB}$, Eqs. (3)–(6), with unknown $m.n$, we can easily determine the values of m and n by mixing modes A and B on a BBS and counting the photon numbers of each outgoing mode by two photon-number-resolving detectors D_A, D_B set behind the BBS (see Fig. 1). Applying the formula (8) yields

$$\begin{aligned}\mathrm{BBS}_{AB}\,|E_{mn}\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(&\left|\delta_{m0}\alpha\sqrt{2}\right\rangle_A\left|\delta_{m1}\alpha\sqrt{2}\right\rangle_B \\ &+(-1)^n\left|-\delta_{m0}\alpha\sqrt{2}\right\rangle_A\left|-\delta_{m1}\alpha\sqrt{2}\right\rangle_B\Big),\end{aligned} \tag{11}$$

with δ_{mn} the Kronecker delta function. Expressing Eq. (11) in terms of the cat states (7), we have for concrete values of m and n the following explicit transformations

$$\mathrm{BBS}_{AB}\,|E_{00}\rangle_{AB} \rightarrow |\mathrm{cat}_+\rangle_A\,|0\rangle_B\,, \tag{12}$$
$$\mathrm{BBS}_{AB}\,|E_{01}\rangle_{AB} \rightarrow |\mathrm{cat}_-\rangle_A\,|0\rangle_B\,, \tag{13}$$
$$\mathrm{BBS}_{AB}\,|E_{10}\rangle_{AB} \rightarrow |0\rangle_A\,|\mathrm{cat}_+\rangle_B\,, \tag{14}$$
$$\mathrm{BBS}_{AB}\,|E_{11}\rangle_{AB} \rightarrow |0\rangle_A\,|\mathrm{cat}_-\rangle_B\,. \tag{15}$$

Transparently, if D_A registers an even (odd) number of photons while there are no photons coming in D_B, then the input ECS was $|E_{00}\rangle_{AB}$ ($|E_{01}\rangle_{AB}$) definitely. However, if D_A does not click but an even (odd) number of photons comes in D_B, then we know with no doubt that the ECS $|E_{10}\rangle_{AB}$ ($|E_{11}\rangle_{AB}$) was inputted to the BBS. As we have assumed α sufficiently large, the probability that both D_A and D_B are silent can be set to zero. Therefore, the four ECSs $|E_{mn}\rangle_{AB}$ are distinguishable deterministically and unambiguously. Quantum dialogue is taking place through a sequence of rounds with specific functions. In what follows, we shall describe different types of rounds which are needed for secure quantum dialogue.

4 Communication round

Suppose that Alice wishes to inform Bob two her secret bits k, l and, at the same time, Bob wishes to let Alice know two his secret bits p, q. In order to exchange their pairs of bits securely, Bob prepares one of the four ECSs $|E_{mn}\rangle_{AB}$ and then sends mode A to Alice but keeps mode B with himself. Without loss of generality, we assume for concreteness that $m = n = 0$, i.e., the state $|E_{00}\rangle_{AB}$ is to be prepared by Bob.

Communication round is a round of the many-round quantum dialogue protocol in which Alice and Bob can exchange two secret bits. It includes three kinds of operation: Alice encodes her bits, Bob decodes Alice's bits then encodes his, and Alice decodes Bob's bits.

4.1 Alice's encoding

To encode her secret bits k and l in such a way that only Bob is able to decode, Alice should do an appropriate local operation which we call operation C_{kl}. The aim of the operation C_{kl} is to make Alice and Bob share a two-mode ECS $|E_{kl}\rangle$, one mode of which is with Alice and the other one is with Bob. Such operation C_{kl} is implemented differently depending on the actual values of k and l. As will be seen, for $k, l = 0, 1$ or $k, l = 1, 1$ the encoding operation is nontrivial, requiring additional resources.

Most trivial is the case when $k = l = 0$. In this case, Alice does nothing but returning mode A intact to Bob, i.e., Bob will have at his hand again both modes A and B which remain in the initial entangled state $|E_{00}\rangle_{AB}$.

The case when $k = 0$ and $l = 1$ is, however, not trivial since no unitary operations exist that directly acts on mode A and transforms $|E_{00}\rangle_{AB}$to $|E_{01}\rangle_{AB}$. In this case, to execute the operation C_{01} Alice needs extra resources. Namely, she prepares her own ECS $|E_{00}\rangle_{XY}$, where X and Y denote two auxiliary modes. Hence, the total state of Alice and Bob is $|\Psi_0\rangle_{XYAB} = |E_{00}\rangle_{XY}|E_{00}\rangle_{AB}$, of which modes X, Y and A belong to Alice while mode B is at Bob's possession. Then, Alice combines mode Y and mode A on a BBS, bringing the total state $|\Psi_0\rangle_{XYAB}$ to

$$|\Psi\rangle_{XYAB} = \frac{1}{2}\left(|\alpha\rangle_X \left|\alpha\sqrt{2}\right\rangle_Y |0\rangle_A |\alpha\rangle_B + |\alpha\rangle_X |0\rangle_Y \left|\alpha\sqrt{2}\right\rangle_A |-\alpha\rangle_B\right.$$

$$+ |-\alpha\rangle_X |0\rangle_Y \left|-\alpha\sqrt{2}\right\rangle_A |\alpha\rangle_B$$
$$+ |-\alpha\rangle_X \left|-\alpha\sqrt{2}\right\rangle_Y |0\rangle_A |-\alpha\rangle_B \Big). \quad (16)$$

Behind the BBS two photon number-resolving detectors D_A and D_Y are arranged (see Fig. 2). If detector D_A registers n_A photons while detector D_Y registers n_Y photons, then the state $|\Psi\rangle_{XYAB}$ collapses into $|n_A\rangle_A |n_Y\rangle_Y |\Phi\rangle_{XB}$, with $|\Phi\rangle_{XB}$ being of the (unnormalized) form

$$|\Phi\rangle_{XB} = \frac{1}{2}\Big\{\delta_{n_A,0}\,\langle n_Y \left|\alpha\sqrt{2}\right\rangle \left[|\alpha\rangle_X |\alpha\rangle_B + (-1)^{n_Y} |-\alpha\rangle_X |-\alpha\rangle_B\right]$$
$$+ \langle n_A \left|\alpha\sqrt{2}\right\rangle \delta_{n_Y,0} \left[(-1)^{n_A} |-\alpha\rangle_X |\alpha\rangle_B + |\alpha\rangle_X |-\alpha\rangle_B\right]\Big\}, \quad (17)$$

where the equalities $\langle n|\, 0\rangle = \delta_{n,0}$ and $\langle n \left|-\alpha\sqrt{2}\right\rangle = (-1)^n \langle n \left|\alpha\sqrt{2}\right\rangle$ have been taken into account.

If $n_A = 0$ and n_Y is nonzero even then, with a probability

$$P_{0,\text{even}} = \frac{1}{2}\sum_{n=1}^{\infty} \left|\langle 2n \left|\alpha\sqrt{2}\right\rangle\right|^2 = e^{-2\alpha^2} \sinh^2(\alpha^2), \quad (18)$$

the state (17) becomes

$$\frac{1}{\sqrt{2}} (|\alpha\rangle_X |\alpha\rangle_B + |-\alpha\rangle_X |-\alpha\rangle_B) = |E_{00}\rangle_{XB}, \quad (19)$$

which is not what Alice wants. However, the initial kind of entanglement between Alice and Bob is not lost, just being transferred from between A and B to between X and B. This allows Alice to repeat the same process some more times until obtaining the desired state $|E_{01}\rangle_{ZB}$, where Z is a new auxiliary mode. The fact that mode Z is not the initial mode A does not matter. The matter at this point is that mode Z is with Alice, mode B is with Bob, and more importantly, the two modes are in the desired ECS $|E_{01}\rangle_{ZB}$. To economize notations, let us relabel $|E_{01}\rangle_{ZB}$ as $|E_{01}\rangle_{XB}$, just to indicate that the correctly obtained kind of entanglement is not between B and the original mode A but between B and an auxiliary mode.

If $n_A = 0$ and n_Y is odd then, with a probability

$$P_{0,\text{odd}} = \frac{1}{2}\sum_{n=0}^{\infty} \left|\langle 2n+1| \left|\alpha\sqrt{2}\right\rangle\right|^2 = \frac{1}{2} e^{-2\alpha^2} \sinh(2\alpha^2), \quad (20)$$

the state (17) becomes

$$\frac{1}{\sqrt{2}} (|\alpha\rangle_X |\alpha\rangle_B - |-\alpha\rangle_X |-\alpha\rangle_B) = |E_{01}\rangle_{XB}, \quad (21)$$

which is what Alice wants.

If n_A is nonzero even and $n_Y = 0$ then, with the probability $P_{even,0} = P_{0,\text{even}}$, the state (17) becomes

$$\frac{1}{\sqrt{2}}\left(|\alpha\rangle_X|-\alpha\rangle_B + |-\alpha\rangle_X|\alpha\rangle_B\right) = |E_{10}\rangle_{XB}\,, \tag{22}$$

which is undesired. Worse still, the initial nonclassical correlation between Alice and Bob has changed. Fortunately, Alice can first π-phase-shifts mode X (i.e., she lets mode X go through a phase-shifter PS(π), with PS(φ) acting on a coherent state $|\alpha\rangle$ as $\text{PS}(\varphi)|\alpha\rangle = \left|e^{i\varphi}\alpha\right\rangle$) to transform $|E_{10}\rangle_{XB}$ to $|E_{00}\rangle_{XB}$ and then proceed as in the case when $n_A = 0$ and n_Y is nonzero even until obtaining $|E_{01}\rangle_{XB}$.

If n_A is odd and $n_Y = 0$ then, with the probability $P_{odd,0} = P_{0,\text{odd}}$, the state (17) becomes

$$\frac{1}{\sqrt{2}}\left(|\alpha\rangle_X|-\alpha\rangle_B - |-\alpha\rangle_X|\alpha\rangle_B\right) = |E_{11}\rangle_{XB}\,, \tag{23}$$

which can easily be transformed to the desired $|E_{01}\rangle_{XB}$ by π-phase-shifting mode X.

There might be that $n_A = n_Y = 0$, in which case the state (17) factorizes as $(|\alpha\rangle_X + |-\alpha\rangle_X)(|\alpha\rangle_B + |-\alpha\rangle_B)/2$, i.e., no entanglement exists between Alice and Bob, implying failure. But this event happens with a probability $P_{0,0} = \left|\langle 0|\left|\alpha\sqrt{2}\right\rangle\right|^2 = e^{-2\alpha^2}$, which is vanishingly small for large enough α. So the failure event can be excluded.

For $k = 1$ and $l = 0$, the operation C_{10} is simple, without consuming any extra resources. In fact, Alice just needs to π-phase-shift mode A to change the state $|E_{00}\rangle_{AB}$ to the desired ECS $|E_{10}\rangle_{AB}$.

Finally, if $k = l = 1$, the job Alice needs to do is formally similar to the case with $k = 0$ and $l = 1$, but the details differ. Concretely, after preparing an additional ECS $|E_{00}\rangle_{XY}$ and combining modes Y and A on a BBS, followed by counting photon numbers n_A and n_Y of the combined modes, the state of modes X and B will be of the same form given by Eq. (17). However, Alice's job differs from that for the case with $k = 0$ and $l = 1$ as will be detailed below.

If $n_A = 0$ and n_Y is nonzero even then, with a probability $P_{0,\text{even}}$, modes X and B are projected on $|E_{00}\rangle_{XB}$,which requires Alice to repeat the same procedure some more times until obtaining the desired state $|E_{11}\rangle_{ZB}$ which, for the purpose of economizing notations mentioned above, will be again labeled as $|E_{11}\rangle_{XB}$.

If $n_A = 0$ and n_Y is odd then, with a probability $P_{0,\text{odd}}$, modes X and B are projected onto $|E_{01}\rangle_{XB}$, which after π-phase-shifting mode X becomes the desired state $|E_{11}\rangle_{XB}$.

If n_A is nonzero even and $n_Y = 0$, then, with the probability $P_{even,0}$, modes X and B are projected onto $|E_{10}\rangle_{XB}$, which is not the desired state and cannot directly be transformed to $|E_{00}\rangle_{XB}$. In this situation, Alice needs first to π-phase-shift mode X of the ECS $|E_{10}\rangle_{XB}$ to transform it to $|E_{00}\rangle_{XB}$ and then repeat the above-described procedure until obtaining the desired state $|E_{11}\rangle_{XB}$.

If n_A is odd and $n_{Y_1} = 0$, then, with the probability $P_{odd,0}$, modes X and B are projected on the desired ECS $|E_{11}\rangle_{XB}$ without any additional efforts.

We see that the operations C_{00} and C_{10} are executed without any extra quantum resources. As for the operations C_{01} and C_{11}, they require at least one additional ECS (on average, two additional ECSs), but are always successfully executed. In this sense Alice is able to encode her secret bits deterministically.

4.2 Bob's decoding and encoding

After Alice has encoded her secret bits k, l by executing the operation C_{kl} she sends mode A (in cases no extra resources are needed) or mode X (in cases extra resources are required) to Bob. No matter which Alice's mode is (i.e., A or X), it is entangled with Bob's mode B in the right state (i.e., either in $|E_{kl}\rangle_{AB}$ or in $|E_{kl}\rangle_{XB}$). So Bob follows the scheme sketched in Fig. 1 to identify the ECS he has at hand and easily decodes Alice's bits k and l. Only Bob is able to do that because he is the only one who possesses the two modes which are entangled in the right state. Next, to encode his secret bits p and q, Bob adds (addition mod 2) them to k and l, respectively, to create two new bits $u = p \oplus k$ and $v = q \oplus l$, where $\oplus$ denotes addition mod 2. Afterwards, Bob publicly announces u and v through a reliable classical channel.

4.3 Alice's decoding

From the public announcement, Alice can straightforwardly decodes Bob's bits as $p = u \oplus k$ and $q = v \oplus l$. Anyone who listens to the announcement knows both u and v but cannot get p and q since they have no idea about k and l. Only Alice can!

The operations to be done in a communication round when Alice's bits are $k, l = 0, 1$ or $1, 1$ are shown in Fig. 2. In a communication round Alice "talks" to Bob by two bits and Bob "responds" to Alice by another pair of bits. If many such communication rounds are run one after another, the whole process can be looked upon as a dialogue, which is quantum because it is executed in terms of quantum states and by means of quantum operations. However, such a quantum dialogue is threatened by attacks from a malicious outsider named Eve who is supposed to be capable of doing anything allowable by Nature.

5 Eve in the line

Recall that in the communication round one of the two entangled modes is traveling back and forth, first from Bob to Alice and then back from Alice to Bob, while the other mode always stays with Bob. Eve can access the traveling mode, but she is wise enough to not directly measure that mode because she knows that its density matrix is $\rho = (|-\alpha\rangle\langle-\alpha| + |\alpha\rangle\langle\alpha|)/2$, which is maximally mixed containing no information.

Instead, Eve may disturb by applying on the traveling mode an unitary operator to cause unaware errors in the process of Alice's encoding and Bob's decoding. For instance, as illustrated in Fig. 3a, *en route* from Bob to Alice, Eve makes a π-phase-shift on mode A changing the intended ECS $|E_{00}\rangle_{AB}$ to $|E_{10}\rangle_{AB}$ so that the operation C_{kl} which Alice makes would encode erroneous bits $k \oplus 1$ and l instead of the should-

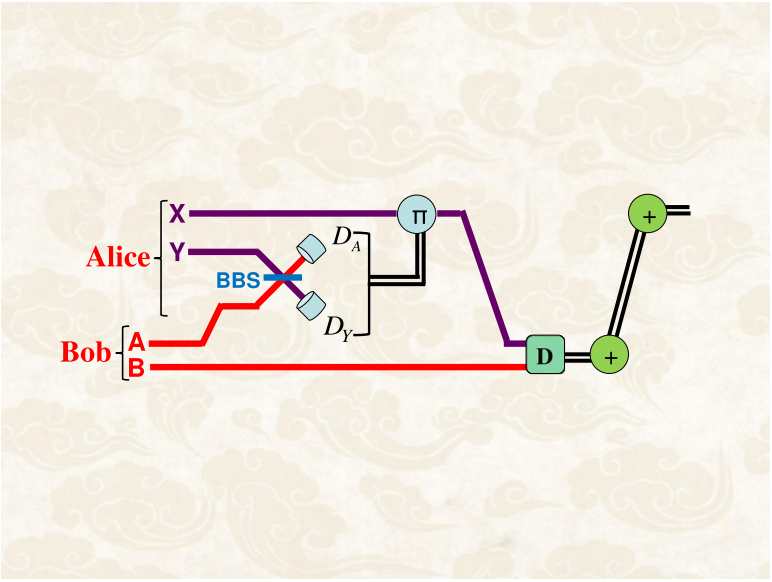

Fig. 2 (Color online) Operations in a communication round when Alice's bits are $k, l = 0, 1$ or $1, 1$. Initially modes A and B (X and Y) are in the ECS $|E_{00}\rangle_{AB}$ ($|E_{00}\rangle_{XY}$). BBS is a balanced beam-splitter and D_A, D_Y photon-number-resolving detectors. Depending on the concrete values of k, l and the photon numbers counted by the photo-detectors (represented by a double line after the detectors), Alice makes or does not make a π-phase-shift (represented by a circle with a π) on mode X before sending it back to Bob. Having both modes X and B at hand, Bob decodes Alice's bits k, l (Bob's decoding is represented by a box with letter D and the values of k, l by a double line going out from the box) and then encodes his bits p, q (represented by the first circle with a plus sign) in two new bits $u = k \oplus p$, $v = l \oplus q$ (represented by a double line going out from the first circle). Afterwards, via a classical communication channel (represented by a double line connecting the two circles) Bob sends u, v to Alice who decodes Bob's bits (represented by the second circle with a plus sign) as $p = k \oplus u$, $q = l \oplus v$ (represented by a double line going out from the second circle)

be ones k and l. Alternatively, as illustrated in Fig. 3b, Eve may let the mode traveling from Bob to Alice intact (i.e., Alice's encoding remains alright), but π-phase-shifts the mode traveling back from Alice to Bob after Alice's correct encoding. In doing so, after Alice returns the encoded mode to Bob, Bob will have the wrong ECS $\left|E_{k\oplus 1,l}\right\rangle_{AB}$ instead of the correct one $|E_{kl}\rangle_{AB}$, and thus, Bob will incorrectly decode Alice's bits. That leads later to Bob's wrong encoding of his bits and therefore also leads to Alice's wrong decoding of Bob's bits. In other words, these kind of attacks can be referred to as disturbance attack or denial-of-service attack because it makes the quantum dialogue protocol totally ambiguous.

Another very wise kind of attack by which Eve perfectly eavesdrops the dialogue can be designed as follows (see Fig. 4). Eve prepares her own ECS $|E_{00}\rangle_{A'B'}$, keeps it in a quantum memory for later use, and ambushes on the way between Bob and Alice. When Bob sends mode A of his ECS $|E_{00}\rangle_{AB}$ to Alice, Eve captures and stores this mode A in a quantum memory and sends her mode A' to Alice. Alice, unaware of Eve's action, takes A' for A and encodes her secret bits k, l on that mode A' and then returns it to Bob (in fact, as presented in Sect. 4.1, here the encoded mode may be the

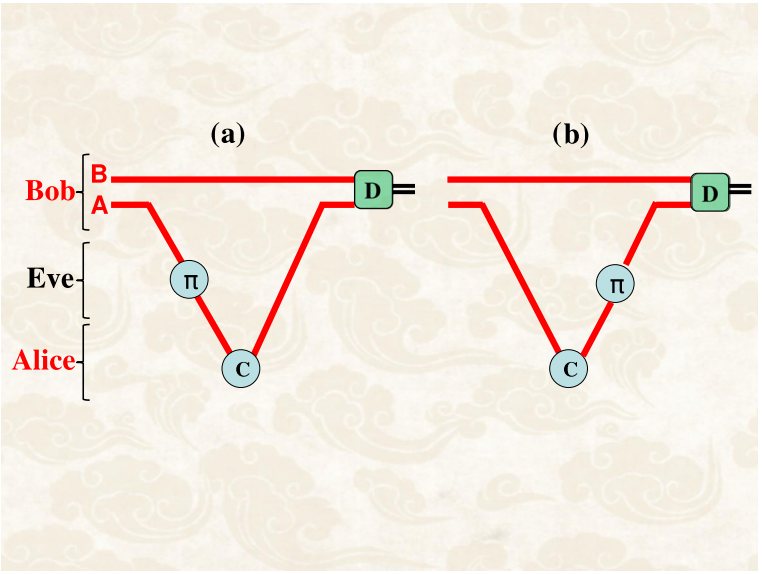

Fig. 3 (Color online) Eve's disturbance attack on **a** the Bob-to-Alice direction and **b** the Alice-to-Bob direction. Modes A and B are initially entangled with each other in the ECS $|E_{00}\rangle_{AB}$. The circle with a π implies a π-phase-shift made by Eve, the circle with letter C (the box with letter D) represents Alice's encoding (Bob's decoding) operation, and the double line carries classical results obtained after Bob's decoding

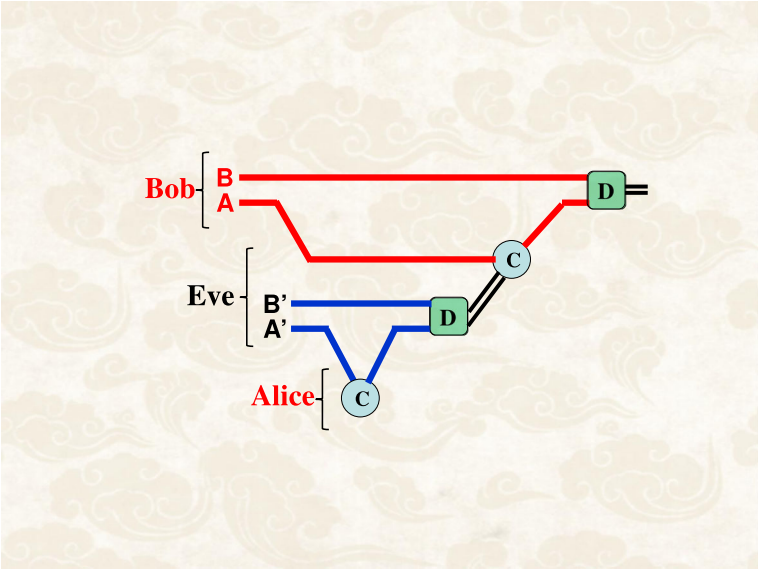

Fig. 4 (Color online) Eve's eavesdropping attack. Modes A and A' are entangled with modes B and B' in the ECSs $|E_{00}\rangle_{AB}$ and $|E_{00}\rangle_{A'B'}$, respectively. The circle with letter C (the box with letter D) represents the encoding (decoding) operation of Alice and Eve (Eve and Bob), and the double lines carry classical results of the decoding operations. This kind of attack allows Eve eavesdrop the whole content of Alice–Bob dialogue

same mode A' or an auxiliary mode X, depending on the case, but we keep calling that encoded mode A' for convenience). Still waiting in the line, Eve again captures the mode sent to Bob by Alice after she performs the operation C_{kl} and then together with her mode B' (which she has stored) decodes Alice's bits k, l correctly. Having known the precise values of k, l, Eve is fully capable of performing the operation C_{kl} on mode A (which has been stored in Eve's quantum memory). Afterward, Eve returns the encoded mode A to Bob, who will perfectly decode Alice's bits. Finally, upon public announcement of Bob's encrypted bits u and v, not only Alice but also Eve can easily infer Bob's bits p, q. Therefore, by such an eavesdropping attack Eve eavesdrops the whole conversation between Alice and Bob.

To protect from Eve's attacks, Alice and Bob should apply certain control methods. Concretely, to detect the above-mentioned disturbance attack and eavesdropping attack, two types of control rounds must be run.

5.1 Type-1 control round

The mode that Alice receives to do her encoding may be the right one which was traveling safely and thus correctly entangled with Bob's mode, i.e., their shared state is the ECS $|E_{00}\rangle_{AB}$. Yet, it may have been acted on by Eve as described in the disturbance attack so that the ECS shared between Alice and Bob is not the right one $|E_{00}\rangle_{AB}$ but the wrong one $|E_{10}\rangle_{AB}$. Also, it may be a new mode A' unentangled with mode B since the original mode A was captured by Eve as described in the eavesdropping attack. Therefore, after Alice receives a mode the two parties may wish to check whether they share the right ECS $|E_{00}\rangle_{AB}$. For this purpose, they publicly agree with each other to execute this round as a control one. With such a choice, Alice does not perform the C_{kl} operation as in a communication round but prepares an ancillary coherent state $|\alpha\rangle_a$ and lets mode a and mode A be mixed on a BBS. As for Bob, he also prepares an ancillary coherent state $|\alpha\rangle_b$ and lets mode B and mode b be mixed on another BBS. Behind each BBS, there are two threshold photo-detectors: D_A, D_a behind Alice's BBS and D_b, D_B behind Bob's BBS. If Eve is absent, the total state $|\alpha\rangle_a |E_{00}\rangle_{AB} |\alpha\rangle_b$ after passing the two BBSs becomes

$$\frac{1}{\sqrt{2}}\left(\left|\alpha\sqrt{2}\right\rangle_a |0\rangle_A \left|\alpha\sqrt{2}\right\rangle_B |0\rangle_b + |0\rangle_a \left|\alpha\sqrt{2}\right\rangle_A |0\rangle_B \left|-\alpha\sqrt{2}\right\rangle_b\right). \tag{24}$$

Regarding the photo-detectors' clicking, the expression (24) indicates that

$$\left.\begin{array}{c} \text{either} \\ D_a \text{and} D_B \text{simultaneously click} \\ \textit{or} \\ D_A \text{and} D_b \text{simultaneously click} \end{array}\right\} \tag{25}$$

The combinations (25) of the photo-detectors' clicking reflect the specific should-be type of quantum correlation in the ECS $|E_{00}\rangle_{AB}$. The control round just described is illustrated in Fig. 5 and takes the name 'type-1 control round' which is distinct from 'type-2 control round' to be introduced later.

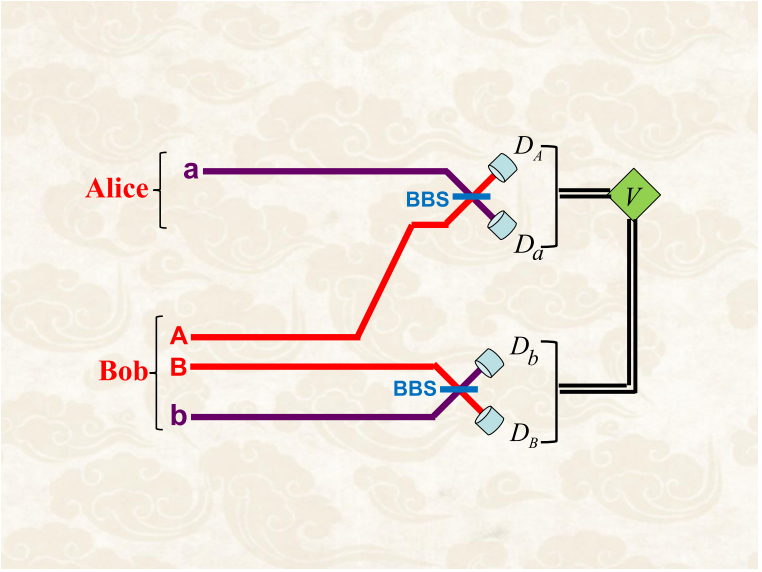

Fig. 5 (Color online) Operations for Alice and Bob to do in the type-1 control round. BBSs are balanced beam splitters, and D_A, D_a, D_b, D_B are threshold photo-detectors. The double lines represent the outcomes of the photo-detectors' clickings which are classically communicated between Alice and Bob and analyzed in the box with letter V. If initially the ECS was $|E_{00}\rangle_{AB}$, the separable coherent states were $|\alpha\rangle_a$, $|\alpha\rangle_b$ and Eve did not attack, the photo-detectors should click in accordance with the combination (25)

Suppose that Eve sits in the line and attempts to disturb by π -phase-shifting mode A when it is traveling from Bob to Alice. By doing so, Eve purposely transforms the initial shared ECS $|E_{00}\rangle_{AB} = (|\alpha\rangle_A\,|\alpha\rangle_B + |-\alpha\rangle_A\,|-\alpha\rangle_B)/\sqrt{2}$ to $\mathrm{PS}_A(\pi)\,|E_{00}\rangle_{AB} = (|-\alpha\rangle_A\,|\alpha\rangle_B + |\alpha\rangle_A\,|-\alpha\rangle_B)/\sqrt{2} = |E_{10}\rangle_{AB}$. The initial total state $|\alpha\rangle_a\,|E_{00}\rangle_{AB}\,|\alpha\rangle_b$ thus changes to $|\alpha\rangle_a\,|E_{10}\rangle_{AB}\,|\alpha\rangle_b$ which after passing the two BBSs will be of the form

$$\frac{1}{\sqrt{2}}\left(|0\rangle_a\left|\alpha\sqrt{2}\right\rangle_A\left|\alpha\sqrt{2}\right\rangle_B|0\rangle_b + \left|\alpha\sqrt{2}\right\rangle_a|0\rangle_A\,|0\rangle_B\left|-\alpha\sqrt{2}\right\rangle_b\right). \tag{26}$$

Regarding the photo-detectors' clicking, the expression (26) indicates that

$$\left.\begin{array}{c}\text{either}\\ D_A \text{and} D_B \text{simultaneously click}\\ \textit{or}\\ D_a \text{and} D_b \text{simultaneously click}\end{array}\right\} \tag{27}$$

Clearly, the combinations (27) of the photo-detectors' clicking differ from the should-be ones specified in (25), indicating the presence of Eve. The operations in the type-1 control round for detecting Eve's disturbance attack on the Bob-to-Alice direction are displayed in Fig. 6.

Now, suppose that Eve attempts to eavesdrop. She, as outlined above, prepares an ECS $|E_{00}\rangle_{A'B'}$ by herself, then captures mode A, keeps it together with mode B' in a quantum memory, and sends mode A' to Alice. Alice, unaware of Eve's attack,

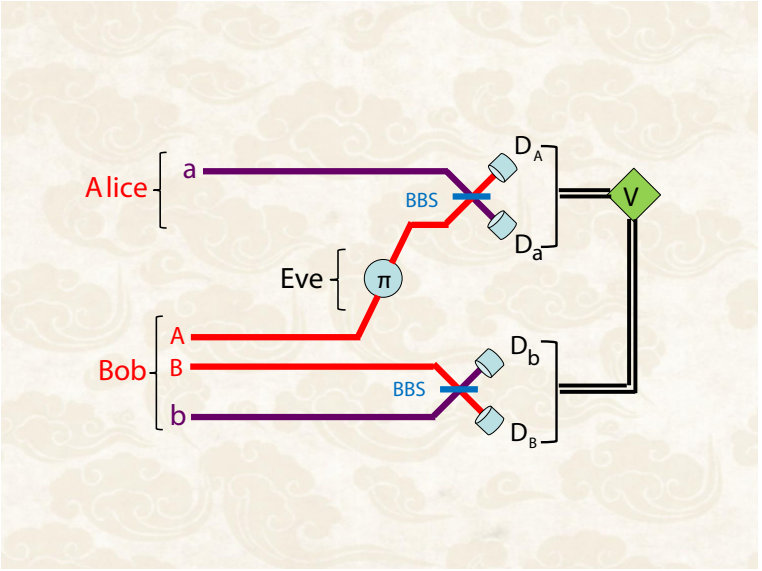

Fig. 6 (Color online) Operations in the type-1 control round to detect Eve's disturbance attack on the Bob-to-Alice direction. Initially modes A and B are in the ECS $|E_{00}\rangle_{AB}$, while modes a and b are separable coherent states. The circle with a π denotes a π-phase-shift made by Eve on mode A when this mode is traveling from Bob to Alice. BBSs are balanced beam splitters, and D_A, D_a, D_b, D_B are threshold photo-detectors. Combinations of the photo-detectors' clickings represented by double lines are verified in the box with letter V which in this case disagree with those in (25)

takes A' for A and follows the procedure of the type-1 control round. Because mode A' and mode B are not entangled with each other, after the two BBSs the total state $|\alpha\rangle_a |E_{00}\rangle_{A'B'} |E_{00}\rangle_{AB} |\alpha\rangle_b$ turns out to be

$$\begin{aligned}\frac{1}{2}\Big(&\left|\alpha\sqrt{2}\right\rangle_a |0\rangle_{A'} |\alpha\rangle_{B'} |\alpha\rangle_A \left|\alpha\sqrt{2}\right\rangle_B |0\rangle_b \\ &+ |0\rangle_a \left|\alpha\sqrt{2}\right\rangle_{A'} |-\alpha\rangle_{B'} |\alpha\rangle_A \left|\alpha\sqrt{2}\right\rangle_B |0\rangle_b \\ &+ \left|\alpha\sqrt{2}\right\rangle_a |0\rangle_{A'} |\alpha\rangle_{B'} |-\alpha\rangle_A |0\rangle_B \left|-\alpha\sqrt{2}\right\rangle_b \\ &+ |0\rangle_a \left|\alpha\sqrt{2}\right\rangle_{A'} |-\alpha\rangle_{B'} |-\alpha\rangle_A |0\rangle_B \left|-\alpha\sqrt{2}\right\rangle_b\Big). \end{aligned} \tag{28}$$

As is easy to recognize from the expression (28), there are four equally possible combinations of outcomes: either $\{D_a$ and $D_B\}$ or $\{D_{A'}$ and $D_B\}$ or $\{D_a$ and $D_b\}$ or $\{D_{A'}$ and $D_b\}$ fire. Clearly, if $\{D_{A'}$ and $D_B\}$ or $\{D_a$ and $D_b\}$, which are different from (25), click Alice and Bob know that Eve was in the line. The operations in the type-1 control round to detect Eve's eavesdropping attack are displayed in Fig. 7. Since the eavesdropper's detection rate is 50%, Eve, on average, could not hide her traces after a pair of such type-1 control rounds.

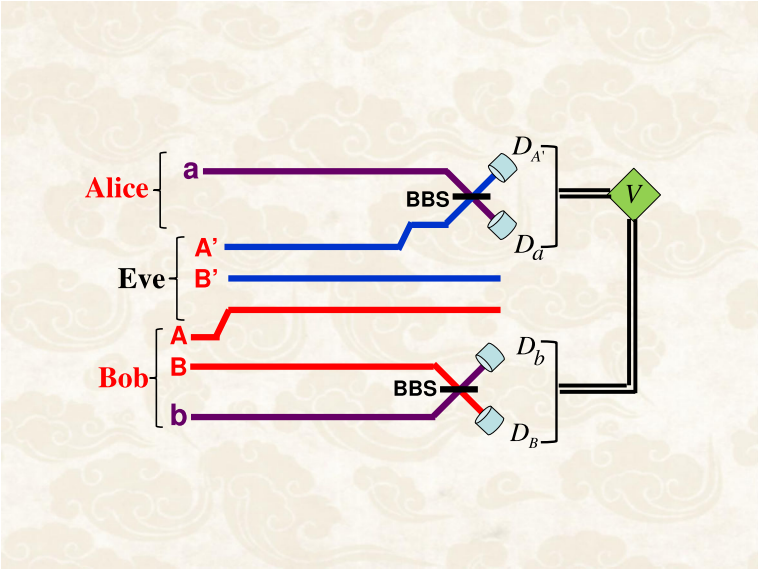

Fig. 7 (Color online) Operations in the type-1 control round for detecting Eve's eavesdropping attack. Initially modes A and B (A' and B') are in the ECS $|E_{00}\rangle_{AB}$, ($|E_{00}\rangle_{A'B'}$), while modes a and b are separable coherent states. BBSs are balanced beam-splitters and $D_{A'}$, D_a, D_b, D_B are threshold photo-detectors. The double lines represent the results of the photo-detectors' clickings which are collected and compared with those in (25) in the box with letter V to examine whether Eve eavesdropped or not

5.2 Type-2 control round

The above type-1 control round could not fully protect from the disturbance attack. For example, if Eve does not disturb on the Bob-to-Alice direction, but does on the Alice-to-Bob direction as shown in Fig. 3b, her disturbance is undetectable. That is, when mode A is traveling back to Bob from Alice after Alice's encoding operation, Eve phase-shifts mode A by π. One can see that even though Alice's encoding remains alright, Bob's decoding will be wrong, leading to full failure of the dialogue protocol. To catch Eve in such a way of disturbance, Alice and Bob should control the Alice-to-Bob direction as well. This will be the type-2 control round with its operations different from those in the type-1 control round. Namely, in the type-2 control round, after Alice encodes her bits on mode A and sends it back to Bob, Bob carries out a joint measurement on the encoded mode A and his mode B to identify the type of their shared entanglement. After that, instead of proceeding as in a communication round, Bob asks Alice to announce via a classical channel her encoded bits which will be compared with Bob's measurement outcome. Any mismatch between those data signals the presence of Eve. Operations in the type-2 control round are displayed in Fig. 8.

As has been elucidated in detail, by applying both the type-1 and type-2 control rounds Eve's attacks should be disclosed: disturbance attack on the Bob-to-Alice direction and eavesdropping attack by the type-1 control round, while disturbance attack on the Alice-to-Bob direction by the type-2 control round. Because both the

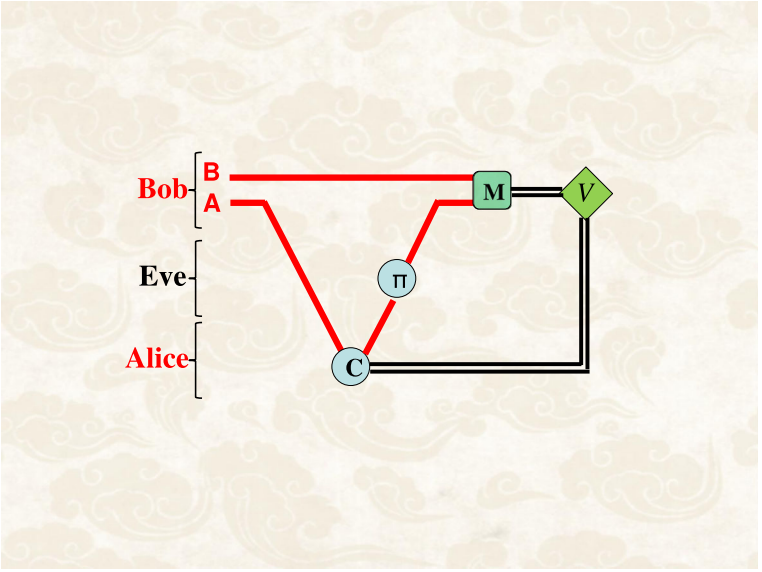

Fig. 8 (Color online) Operations in the type-2 control round for detecting Eve's disturbance attack on the Alice-to-Bob direction. Initially modes A and B are in the ECS $|E_{00}\rangle_{AB}$. The circle with letter C represents Alice's encoding operation, the circle with a π is the phase-shifter PS(π) used by Eve and the box with letter M means Bob's measurement to identify the entanglement type of the final ECS. The double line going out from M carries Bob's measurement outcome, while that going out from C carries the values of bits that Alice has encoded. Their data are communicated and compared in the box with letter V to check the presence of Eve

possible routes (Bob-to-Alice and Alice-to-Bob) are under control, Eve would be also caught by other types of attacks.

6 Running the quantum dialogue

The quantum dialogue protocol runs through a finite sequence of steps. In each step, after Alice receives a mode (which might be sent to her by Bob or by Eve), Bob and Alice together decide (in fact, randomly choose) via a classical channel whether this step will be a communication round or type-1 control round. In case the type-1 control round is chosen, they do the measurement procedure and compare their outcomes as described in Sect. 5.1. If Eve is found (no matter she performed disturbance attack or eavesdropping attack), they abort the protocol, otherwise they redo the step. In case the communication round is chosen, Alice encodes her bits on the mode she received as described in Sect. 4.1 and returns this mode to Bob. Upon receipt of the mode, the two parties publicly decide whether communication round or type-2 control round will be processed. If the type-2 control round is chosen, they follow the operations as described in Sect. 5.2 to check the presence of Eve. If Eve was present (in this case Eve's disturbance attack was done), they abort the protocol; otherwise, they repeat the previous step. In case it is the communication round Bob decodes Alice's bits, then

encodes his bits and announces the encrypted bits u, v as described in Sect. 4.2 for Alice to decode Bob's bits as described in Sect. 4.3.

The rates at which the type-1 and type-2 control rounds are chosen depend on the confidential level of the dialogue. As derived in [6,18], such kind of quantum dialogue is secure asymptotically and is advised to be used in urgent situations when not enough time can be found to first do QKD and then send encrypted messages.

Before drawing the conclusion, some delicate discussion is in order. Returning to Sect. 4.2 where Bob encodes his bits p (q) by adding (addition mod 2) them to Alice's bits k (l) to obtain new bits $u = p \oplus k$ ($v = q \oplus l$) which will be openly published. It is true that Eve can also know u (v) from the public announcement without taking any active attacks. From the information theory point of view, this implies an unconscious leakage of information to Eve (or any other outsiders). To cope with that information leakage problem, a number of improved protocols have been put forward [53–59] by employing more quantum resource (e.g., multiqubit entanglement, logical qubits, ancillas, …) and applying more quantum operations in order to parallelly create a common key bit in a communication round. Similar information leakage-free protocols could also be constructed in terms of ECSs and coherent states, but, in our opinions, it is not really necessary because of the following explanation. In each communication round, each of Alice and Bob can send to his/her partner two secret bits. A quantum dialogue as a whole comprises many communication rounds to exchange Alice's bits $\{k_1 l_1, k_2 l_2, \ldots, k_N l_N\}$ and Bob's bits $\{p_1 q_1, p_2 q_2, \ldots, p_N q_N\}$, with N the dialogue length. In what follows, for simplicity and without loss of generality, we shall consider only the bit sequences $\{k_1, k_2, \ldots, k_N\}$ and $\{p_1, p_2, \ldots, p_N\}$ (similar arguments also hold for $\{l_1, l_2, \ldots, l_N\}$ and $\{q_1, q_2, \ldots, q_N\}$). If $N = 1$ and $u_1 = k_1 \oplus p_1 = 0$, for example, then Eve has two equally weighted choices to guess Alice's and Bob's bits: either $\{k_1 = 0, p_1 = 0\}$ or $\{k_1 = 1, p_1 = 1\}$. If $N = 2$ and $\{u_1 = k_1 \oplus p_1 = 0, u_2 = k_2 \oplus p_2 = 1\}$, for example, then Eve has four equally weighted choices to guess Alice's and Bob's bits: either $\{k_1 k_2 = 00, p_1 p_2 = 01\}$ or $\{k_1 k_2 = 01, p_1 p_2 = 00\}$ or $\{k_1 k_2 = 10, p_1 p_2 = 11\}$ or $\{k_1 k_2 = 11, p_1 p_2 = 10\}$ and so on. Hence, for a finite N and certain values of $\{u_1 = k_1 \oplus p_1, u_2 = k_2 \oplus p_2, \ldots, u_N = k_N \oplus p_N\}$ Eve has 2^N equally weighted choices to guess Alice's and Bob's messages $\{k_1 k_2 \ldots k_N, p_1 p_2 \ldots p_N\}$. Obviously, if N is big enough, Eve can hardly infer content of the conversation. Therefore, practically the mentioned information leakage problem can be regarded as creating no (or having very little) affect on security of the quantum dialogue as a whole.

7 Conclusion

We have exploited EPR-type ECSs for Alice and Bob to talk with each other in a quantum manner. Each time one mode of a two-mode EPR-type ECS is mediated between Alice and Bob enabling the two to exchange their two secret bits in a communication round thanks to the specific type of shared entanglement. The security of the quantum dialogue is ensured also thanks to the type of shared entanglement. Any kind of action of Eve in the Alice-to-Bob or/and the Bob-to-Alice directions changes the type of shared entanglement so that Alice and Bob are able to detect Eve's presence by alter-

natively executing the two types of control rounds: the type-1 control round that guards the Bob-to-Alice direction and the type-2 control round that guards the Alice-to-Bob direction. The main advantage of using EPR-type ECSs over two-photon EPR states is the simple yet unambiguous and deterministic discrimination between the four types of entanglement of the EPR-type ECS by balanced beam-splitters and photo-detectors that makes the decoding process 100% efficient. The encoding process by single-mode gates, though being nontrivial, can be surpassed also by balanced beam splitters and photo-detectors, sometimes with additional resources. A remaining challenge is the use of photon number-resolving detectors that commonly cannot be avoided in many optical quantum information tasks. However, this problem is expected to be solved in future since the concerned technology development is getting great attention and achievements in recent years [60,61].

Acknowledgements This work is supported by the National Foundation for Science and Technology Development (NAFOSTED) under Project No. 103.01-2019.313.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Vol. **175**, New York, p. 8 (1984). See also Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theoret. Comput. Sci. **560**, 7 (2014). https://doi.org/10.1016/j.tcs.2014.05.025
2. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, 661 (1991). https://doi.org/10.1103/PhysRevLett.67.661
3. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121 (1992). https://doi.org/10.1103/PhysRevLett.68.3121
4. Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM **21**, 120 (1978). https://doi.org/10.1145/359340.359342
5. Bellovin, S.M.: Frank Miller: inventor of the one-time pad. Cryptologia **35**, 203 (2011). https://doi.org/10.1080/01611194.2011.583711
6. An, N.B.: Quantum dialogue. Phys. Lett. A **328**, 6 (2004). https://doi.org/10.1016/j.physleta.2004.06.009
7. An, N.B.: Secure dialogue without a prior key distribution. J. Kor. Phys. Soc. **47**, 562 (2005)
8. Chang, C.H., Yang, C.W., Hzu, G.R., Hwang, T., Kao, S.H.: Quantum dialogue protocols over collective noise using entanglement of GHZ state. Quantum Inf. Process. **15**, 2971 (2016). https://doi.org/10.1007/s11128-016-1309-9
9. Qi, J.M., Xu, G., Chen, X.B., Wang, T.Y., Cai, X.Q., Yang, Y.X.: Two authenticated quantum dialogue protocols based on three-particle entangled states. Quantum Inf. Process. **17**, 247 (2018). https://doi.org/10.1007/s11128-018-2005-8
10. Li, W., Zha, X.W., Yu, Y.: Secure quantum dialogue protocol based on four-qubit cluster state. Int. J. Theor. Phys. **57**, 371 (2018). https://doi.org/10.1007/s10773-017-3569-2
11. Zha, X.W., Yu, X.Y., Cao, Y., Wang, S.K.: Quantum private comparison protocol with five-particle cluster states. Int. J. Theor. Phys. **57**, 3874 (2018). https://doi.org/10.1007/s10773-018-3900-6
12. Liu, Z., Chen, H.: Analyzing and improving the secure quantum dialogue protocol based on four-qubit cluster state. Int. J. Theor. Phys. **59**, 2120 (2020). https://doi.org/10.1007/s10773-020-04485-2
13. Wang, R.J., Li, D.F., Zhang, F.L., Qin, Z., Baaguere, E., Zhan, H.: Quantum dialogue based on hypertanglement against collective noise. Int. J. Theor. Phys. **55**, 3607 (2016). https://doi.org/10.1007/s10773-016-2989-8
14. Zhang, M.H., Cao, Z.W., Peng, J.Y.: Fault-tolerant asymmetric quantum dialogue protocols against collective noise. Quantum Inf. Process. **17**, 204 (2018). https://doi.org/10.1007/s11128-018-1966-y

15. Maitra, A.: Measurement device-independent quantum dialogue. Quantum Inf. Process. **16**, 305 (2017). https://doi.org/10.1007/s11128-017-1757-x
16. Huang, Z., Situ, H.: Protection of quantum dialogue affected by quantum field. Quantum Inf. Process. **18**, 37 (2019). https://doi.org/10.1007/s11128-018-2152-y
17. Chitra, S., Thapliyal, K., Pathak, A.: Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf. Process. **16**, 295 (2017). https://doi.org/10.1007/s11128-017-1736-2
18. An, N.B.: Quantum dialogue by nonselective measurements. Adv. Nat. Sci. Nanosci. Nanotechnol. **9**, 025001 (2018). https://doi.org/10.1088/2043-6254/aab811
19. Yu, Z.B., Gong, L.H., Zhu, Q.B., Cheng, S., Zhou, N.R.: Efficient three-party quantum dialogue protocol based on the continuous variable GHZ states. Int. J. Theor. Phys. **55**, 3147 (2016). https://doi.org/10.1007/s10773-016-2944-8
20. Zhou, N.R., Li, J.F., Yu, Z.B., Gong, L.H., Farouk, A.: New quantum dialogue protocol based on continuous-variable two-mode squeezed vacuum states. Quantum Inf. Process. **16**, 4 (2017). https://doi.org/10.1007/s11128-016-1461-2
21. Gong, L., Tian, C., Li, J., Zou, X.: Quantum network dialogue protocol based on continuous-variable GHZ states. Quantum Inf. Process. **17**, 331 (2018). https://doi.org/10.1007/s11128-018-2103-7
22. Gong, L.H., Li, J.F., Zhou, N.R.: Continuous variable quantum network dialogue protocol based on single-mode squeezed states. Laser Phys. Lett. **15**, 105204 (2018). https://doi.org/10.1088/1612-202X/aadaa4
23. Zhang, M.H., Cao, Z.W., He, C., Qi, M., Peng, J.Y.: Quantum dialogue protocol with continuous-variable single-mode squeezed states. Quantum Inf. Process. **18**, 83 (2019). https://doi.org/10.1007/s11128-019-2188-7
24. Zhang, M.H., Peng, J.Y., Cao, Z.W.: Quantum dialogue protocol with four-mode continuous variable GHZ state. Modern Phys. Lett. B **33**, 1950033 (2019). https://doi.org/10.1142/S0217984919500337
25. An, N.B., Kim, K., Kim, J.: Near-deterministic efficient all-optical quantum computation. Phys. Lett. A **375**, 245 (2011). https://doi.org/10.1016/j.physleta.2010.11.034
26. Sanders, B.C.: Entangled coherent states. Phys. Rev. A **45**, 6811 (1992). https://doi.org/10.1103/PhysRevA.45.6811
27. Sanders, B.C.: Review of entangled coherent states. J. Phys. A: Math. Theor. **45**, 244002 (2012). https://doi.org/10.1088/1751-8113/45/24/244002
28. Wang, X.: Quantum teleportation of entangled coherent states. Phys. Rev. A **64**, 022302 (2001). https://doi.org/10.1103/PhysRevA.64.022302
29. Wang, X.: Bipartite entangled non-orthogonal states. J. Phys. A: Math. Gen. **35**, 165 (2002). https://doi.org/10.1088/0305-4470/35/1/313
30. An, N.B.: Teleportation of coherent-state superpositions within a network. Phys. Rev. A **68**, 022321 (2003). https://doi.org/10.1103/PhysRevA.68.022321
31. An, N.B.: Optimal processing of quantum information via W-type entangled coherent states. Phys. Rev. A **69**, 022315 (2004). https://doi.org/10.1103/PhysRevA.69.022315
32. Jeong, H., An, N.B.: Greenberger–Horne–Zeilinger-type and W-type entangled coherent states: generation and Bell-type inequality tests without photon counting. Phys. Rev. A **74**, 022104 (2006). https://doi.org/10.1103/PhysRevA.74.022104
33. Guo, Y., Kuang, L.M.: Near-deterministic generation of four-mode W-type entangled coherent states. J. Phys. B: At. Mol. Opt. Phys. **40**, 3309 (2007). https://doi.org/10.1088/0953-4075/40/16/011
34. Guo, Y., Deng, H.L.: Near-deterministic generation of three-mode W-type entangled coherent states in free-travelling optical fields. J. Phys. B: At. Mol. Opt. Phys. **42**, 215507 (2009). https://doi.org/10.1088/0953-4075/42/21/215507
35. Liu, T., Su, Q.P., Xiong, S.J., Liu, J.M., Yang, C.P., Nori, F.: Generation of a macroscopic entangled coherent state using quantum memories in circuit QED. Sci. Rep. **6**, 32004 (2016). https://doi.org/10.1038/srep32004
36. Munhoz, P.P., Semiao, F.L., Vidiella-Barranco, A., Roversi, J.A.: Cluster-type entangled coherent states. Phys. Lett. A **372**, 3580 (2008). https://doi.org/10.1016/j.physleta.2008.02.009
37. Becerra-Castro, E.M., Cardoso, W.B., Avelar, A.T., Baseia, B.: Generation of a 4-qubit cluster of entangled coherent states in bimodal QED cavities. J. Phys. B: At. Mol. Opt. Phys. **41**, 085505 (2008). https://doi.org/10.1088/0953-4075/41/8/085505
38. An, N.B., Kim, J.: Cluster-type entangled coherent states: generation and application. Phys. Rev. A **80**, 042316 (2009). https://doi.org/10.1103/PhysRevA.80.042316

39. Munhoz, P.P., Roversi, J.A., Vidiella-Barranco, A., Semiao, F.L.: Bipartite quantum channels using multipartite cluster-type entangled coherent states. Phys. Rev. A **81**, 042305 (2010). https://doi.org/10.1103/PhysRevA.81.042305
40. An, N.B., Kim, J., Kim, K.: Generation of cluster-type entangled coherent states using weak nonlinearities and intense laser beams. Quantum Inf. Comput. **11**, 0124 (2011). https://doi.org/10.5555/2011383.2011392
41. Israel, Y., Cohen, L., Song, X.B., Joo, J., Eisenberg, H.S., Silberberg, Y.: Entangled coherent states created by mixing squeezed vacuum and coherent light. Optica **6**, 753 (2009). https://doi.org/10.1364/OPTICA.6.000753
42. Gerry, C.C., Mimih, J., Benmoussa, A.: Maximally entangled coherent states and strong violations of Bell-type inequalities. Phys. Rev. A **80**, 022111 (2009). https://doi.org/10.1103/PhysRevA.80.022111
43. van Enk, S.J., Hirota, O.: Entangled coherent states: teleportation and decoherence. Phys. Rev. A **64**, 022313 (2001). https://doi.org/10.1103/PhysRevA.64.022313
44. Schrödinger, E.: Die gegenwärtige Situation in der Quantenmechanik. Naturwissenschaften **23**, 807 (1935). https://doi.org/10.1007/BF01491891
45. Ourjoumtsev, A., Tualle-Brouri, R., Laurat, J., Grangier, P.: Generating optical Schrödinger Kittens for quantum information processing. Science **312**, 83 (2006)
46. Neergaard-Nielsen, J.S., Melholt Nielsen, B., Hettich, C., Mølmer, K., Polzik, E.S.: Generation of a superposition of odd photon number states for quantum information networks. Phys. Rev. Lett. **97**, 083604 (2006). https://doi.org/10.1103/PhysRevLett.97.083604
47. Gerrits, T., Glancy, S., Clement, T.S., Calkins, B., Lita, A.E., Miller, A.J., Migdall, A.L., Nam, S.W., Mirin, R.P., Knill, E.: Generation of optical coherent-state superpositions by number-resolved photon subtraction from the squeezed vacuum. Phys. Rev. A **82**, 031802(R) (2010). https://doi.org/10.1103/PhysRevA.82.031802
48. Lund, A.P., Jeong, H., Ralph, T.C., Kim, M.S.: Conditional production of superpositions of coherent states with inefficient photon detection. Phys. Rev. A **70**, 020101R (2004). https://doi.org/10.1103/PhysRevA.70.020101
49. Sychev, D.V., Ulanov, A.E., Pushkina, A.A., Richards, M.W., Fedorov, I.A., Lvovsky, A.I.: Nat. Photonics **11**, 379 (2017). https://doi.org/10.1038/nphoton.2017.57
50. Mikheev, E.V., Pugin, A.S., Kuts, D.A., Podoshvedov, S.A., An, N.B.: Efficient production of large-size optical Schrödinger cat states. Sci. Rep. **9**, 14301 (2019). https://doi.org/10.1038/s41598-019-50703-1
51. Vaidman, L., Yoran, N.: Phys. Rev. A **59**, 116 (1999)
52. Lütkenhaus, N., Calsamiglia, J., Suominen, K.A.: Bell measurements for teleportation. Phys. Rev. A **59**, 3295 (1999). https://doi.org/10.1103/PhysRevA.59.3295
53. Gao, G.: Two quantum dialogue protocols without information leakage. Opt. Commun. **283**, 2288 (2010). https://doi.org/10.1016/j.optcom.2010.01.022
54. Ye, T.Y.: Large payload bidirectional quantum secure direct communication without information leakage. Int. J. Quantum. Inf. **11**, 1350051 (2013). https://doi.org/10.1142/S0219749913500512
55. Zhou, N.R., Wu, G.T., Gong, L.H., Liu, S.Q.: Int. J. Theor. Phys. **52**, 3204 (2013). https://doi.org/10.1007/s10773-013-1615-2
56. Ye, T.Y., Jiang, L.Z.: Quantum dialogue without information leakage based on the entanglement swapping between any two Bell states and the shared secret Bell state. Phys. Scr. **89**, 015103 (2014). https://doi.org/10.1088/0031-8949/89/01/015103
57. Wang, H., Zhang, Y.Q., Liu, X.F., Hu, Y.P.: Efficient quantum dialogue using entangled states and entanglement swapping without information leakage. Quantum Inf. Process. **15**, 2593 (2016). https://doi.org/10.1007/s11128-016-1294-z
58. Liu, Z.H., Chen, H.W.: Cryptanalysis and improvement of efficient quantum dialogue using entangled states and entanglement swapping without information leakage. Quantum Inf. Process. **16**, 229 (2017). https://doi.org/10.1007/s11128-017-1668-x
59. Liu, Z.H., Chen, H.W.: Analyzing and revising quantum dialogue without information leakage based on the entanglement swapping between any two bell states and the shared secret bell state. Int. J. Theor. Phys. **58**, 575 (2019). https://doi.org/10.1007/s10773-018-3955-4
60. Provazník, J., Lachman, L., Filip, R., Marek, P.: Benchmarking photon number resolving detectors. Opt. Express **28**, 14839 (2020). https://doi.org/10.1364/OE.389619

61. Young, S.M., Sarovar, M., Léonard, F.: Design of high-performance photon-number-resolving photodetectors based on coherently interacting nanoscale elements. ACS Photonics **7**, 821 (2020). https://doi.org/10.1021/acsphotonics.9b01754