Probabilistic direct counterfactual quantum communication*

Sheng Zhang(张盛)†

Department of Electronic Technology, China Maritime Police Academy, Ningbo 315801, *China*

(Received 31 May 2016; revised manuscript received 3 November 2016; published online 20 December 2016)

It is striking that the quantum Zeno effect can be used to launch a direct counterfactual communication between two spatially separated parties, Alice and Bob. So far, existing protocols of this type only provide a deterministic counterfactual communication service. However, this counterfactuality should be payed at a price. Firstly, the transmission time is much longer than a classical transmission costs. Secondly, the chained-cycle structure makes them more sensitive to channel noises. Here, we extend the idea of counterfactual communication, and present a probabilistic-counterfactual quantum communication protocol, which is proved to have advantages over the deterministic ones. Moreover, the presented protocol could evolve to a deterministic one solely by adjusting the parameters of the beam splitters.

Keywords: quantum communication, quantum cryptography, optical implementation of quantum information processing

PACS: 03.67.Dd, 03.67.Hk, 42.50.Ex **DOI:** 10.1088/1674-1056/26/2/020304

1. Introduction

Quantum communication is now widely accepted to be one of the most promising candidates in future quantum technology. Using quantum mechanics, several amazing tasks, such as dense coding,[1,2] teleportation[3,4] and counterfactual quantum key distribution,[5,6] are naturally achieved. Since the invention of quantum key distribution (QKD) protocol, i.e., the BB84 protocol,[7] quantum communication has enjoyed great success with both theoretical and commercial aspects. One of the most significant contributions, which is impossible to be achieved by classical means, is counterfactual quantum communication. It enables two remote parties, Alice and Bob, to exchange messages without transmitting any information carriers.

The idea of counterfactual quantum communication was initialized by interaction-free measurement,[8–10] with the impressive phenomenon that an object can be detected without being intuitively measured. The first example, presented by Noh,[5] was realized in a QKD protocol. Later, we announced a variant adapted to the deterministic key distribution scenario.[11] In sharp contrast to conventional QKD schemes, these protocols are counterintuitive that the quantum states, served as the information carriers, never travel through the channel. A translated no-cloning theorem prevents the eavesdroppers from getting any information of the private key. A strict security proof of Noh's protocol (Noh09 protocol) was presented by Yin *et al.*[12] We further proved that, although this protocol is secure under a general intercept-resend attack in an ideal mode, the practical security could be compromised due to the dark count rate and low efficiency of the detectors.[13] Surprisingly, we also found that Eve could get full information of the key from a real implementation by launching a counterintuitive trojan horse attack.[14] Since the rate of information photons in the Noh09 protocol, only up to 12.5% in an ideal setting, is not satisfactory, Sun and Wen improved it to reach 50% using an iterative module.[6] Experimental verifications of the Noh09 protocol have also been reported.[15,16]

Most interestingly, the topic of counterfactual quantum communication (CQC), has been repainted by Salih *et al.*, who claimed a new protocol (SLAZ2013 protocol) with a better rate, using the quantum Zeno effect.[17,18] They also announced a tripartite counterfactual quantum key distribution protocol,[19] to improve the counterfactuality and security of a previous scheme by Akshata Shenoy *et al.*[20] Other interesting applications, such as semi-counterfactual quantum cryptography,[21] counterfactual quantum-information transfer,[22] are also found in recent papers.[19,20]

Although conventional CQC protocols based on the quantum Zeno effect, such as the SLAZ2013 protocol, are supposed to be more efficient than early versions, there are unexpected side-effects directly induced by the chained-cycle structure. Firstly, the transmission time could be multiplied by the number of the cycles, since a photon pulse should travel through all the cycles before it is detected by the legitimate detectors. In other words, the time taken by transferring a single bit might be much longer than a classical transmission may cost, even though Alice and Bob stand close to each other. Secondly, these schemes seem to be more sensitive to channel noises (concerning only those blocking the channel), since the transmission time is systematically multipled. In Ref. [17], it was estimated that an acceptable noise rate only reaches 0.2%.

Motivated by removing the above side effects, we extend the idea of 'counterfactual', and consider a new paradigm,

*Project supported by the National Natural Science Foundation of China (Grant No. 61300203).

†Corresponding author. E-mail: huoxingren112@163.com

© 2017 Chinese Physical Society and IOP Publishing Ltd

namely probabilistic counterfactual quantum communication (PCQC). Here, we use the word 'probabilistic' to define the purity of the counterfactuality. Specifically, a deterministic counterfactual communication scheme is one in which none of the information-carriers travels through the channel. However, in a probabilistic one, there is a non-zero probability for a carrier passing the channel. The idea mostly contributes to bridging the gaps between the classical and deterministic counterfactual communication schemes. In classical communications, all information carriers must pass the channel. In contrast, they are never allowed to do so in a deterministic counterfactual communication scheme. However, in a PCQC protocol, they might travel through the channel with uncertainty. It naturally follows that existing counterfactual quantum communication schemes fall into the paradigm of deterministic ones. For instance, Noh's protocol[5] is a deterministic one on that no information-carrier goes through the channel, though it produces a probabilistic (or random) key. In this paper, we present a PCQC protocol, in which the chained structure is removed, thus the transmission time is greatly reduced and the sensitivity to channel noises is simultaneously degraded.

The rest of the paper is organized as follows. In Section 2, the definition of probabilistic counterfactual communications is given. Then, we present a probabilistic counterfactual quantum communication protocol in Section 3. Next, the counterfactuality rate and the robustness against channel noises are analyzed to show the advantages over the SLAZ2013 protocol. In Section 5, we have a brief discussion on how to combine the presented protocol with quantum key distribution. Finally, a conclusion is drawn.

2. Definition

Before the protocol is introduced, it is necessary to define the probabilistic counterfactual communications. Figure 1 is a primitive prototype of a communication system, where the quantum channel is presumed to be noiseless for simplicity. Define three binary registers x, y, and z for Alice, Bob, and the channel, respectively. A successful communication procedure is described as follows: the sender, Alice, prepares a signal bit (0 or 1) and stores it in register x; Bob resets his register y for depositing the received signal; Alice and Bob carry out a communication protocol p, which sets $y = z = x$; the procedure ends with the result l. Consequently, the procedure can be written as the function $l = F(x,y,z,p)$, where $l = 1$ for $x = y = z$, and $l = 0$ for otherwise. A successful communication procedure is featured with $l = 1$. We need another binary function $k = N(z)$, where $k = 0(1)$ implies the information carrier (not) passing the channel. Naturally, classical, deterministic counterfactual and probabilistic counterfactual communications can be defined by Table 1, in which Prob$\{k = 0\}$ denotes the probability of the case $k = 0$.

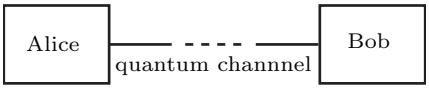


Fig. 1. A primitive prototype of communication systems.

We should note that the information carriers in counterfactual and probabilistic counterfactual communications are supposed to be quantum photons, which are well known for their wave-particle duality.[23] We argue that the counterfactuality should only be referred to the particle-property of the quantum photons. Otherwise, it is difficult to determine whether a protocol is counterfactual or not. There have been controversies around the topic of 'counterfactual' in recent papers.[24–27] For example, the SLAZ2013 protocol seems to be not counterfactual for some results, i.e., logic 0, according to the trace definition proposed by Vaidman.[27] Also, one may argue that Noh's protocol[5] is not counterfactual based on the following fact. As demonstrated by a quantum delayed choice experiment,[28] it is Bob's operation choice (blocking or passing) that determines the path where the photon finally travels. Before he made his choice, the photon, if observed as a wave, would exist in all paths of the interferometer, otherwise, quantum interference would never take place. Therefore, things become more complex than we ever expected, if counterfactuality and wave function are both concerned. Here, in Table 1, I only take into account their classical description, i.e., the particle-property.

Table 1. Definitions of Communication prototypes.

Prototype	l	Prob$\{k = 0\}$
Classical communications	1	0
Deterministic counterfactual communications	1	1
Probabilistic counterfactual communications	1	$p(0 < p < 1)$

In previous schemes,[5,6,17] it is known that projective measurement is important to perform deterministic counterfactual computations and communications, since the information that whether the photon passes the channel can be obtained from the detection results. Figure 2(a) is an analog of the detections in quantum deterministic counterfactual schemes. Obviously, one can confirm that the photon is absent from the channel with certainty, if it reaches the bottom telescope. Therefore, an intuitive way to achieve quantum probabilistic counterfactual communications is to replace the projective measurement device by a photon counter. For example, in Fig. 2(b), where a photon screen is located at point A, it is obvious that one can never confirm the path information from the detection result, which can be expressed by $|\varphi\rangle = \sqrt{R}|0\rangle + \sqrt{1-R}|1\rangle$. Here, $|0(1)\rangle$ represents that the photon is reflected (transmitted) by the BS, and R is the reflectivity of the BS. In this case, the probability of a photon being absent from the channel is R from a classical view. However,

it may be argued that the photon exists in both arms with respect to the wave-property. In this paper, 'probabilistic counterfactual' is only discussed in the classical settings, since it may lead to controversies if it is considered with a quantum description.

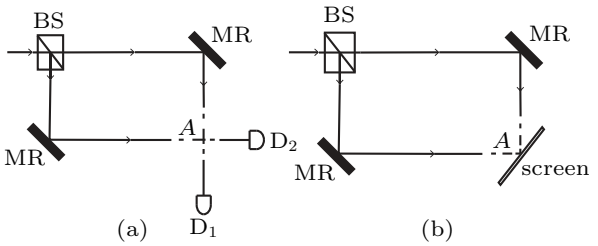


Fig. 2. Two detection modes. Here, BS stands for beam splitter and MR is a mirror. The transmission mode of the BS is supposed to be the quantum channel. (a) Detectors D_1 and D_2, e.g., two telescopes, are placed here to observe incoming photons from the top and the side of the apparatus, respectively. (b) A photon screen is placed at point A to receive photons from both arms.

3. Protocol

First, we give a brief introduction of the SLAZ2013 protocol. To achieve the goal of counterfactuality, a chained quantum Zeno effect, acting as the core principle, is introduced by employing a series of beam splitters and mirrors. Correspondingly, the optical circuit is divided into two types of cycles, i.e., the outer cycle and inner cycle shown in Ref. [17]. At the very beginning, a photon, which has nothing to do with the information bit, is injected by the source, and enters the input port of the outer cycle. The other thing Alice has to do is to observe which of her detectors, D_1 and D_2, clicks. At Bob's end, he just chooses to block (pass) the photon, if logic "1" ("0") is selected to be transmitted. Let us see how Alice knows the transmitted bit. When "0" is selected, two events, denoted by E_1 and E_2 can be observed by Alice:

(i) (E_1) The photon has been caught in detector D_1.

(ii) (E_2) The photon has been caught in detector D_3.

Note that E_2 implies that the photon must have gone through the channel. Therefore, E_2 should be discarded. Similarly, when "1" is selected, events E_3 and E_4 can be observed:

(iii) (E_3) The photon has been caught in detector D_2.

(iv) (E_4) The photon has been caught in detector D_4.

Again, E_4, which goes against the counterfactuality, is discarded. Indeed, the quantum Zeno effect has an important role in both events E_1 and E_3, however, one should note that the chained-cycle structure ievitably increases the time of transmitting a single bit.

The experimental setup shown in Fig. 3, which is adapted from the template of the SLAZ2013 protocol, is presented. It is shown that an iterative module (shown in the dashed rectangle), ever introduced by Refs. [6] and [14], is employed to replace the inner cycle. The length of each optical delay (OD) in this module should be carefully chosen to match each other with respect to interference. Specifically, the following condition should be satisfied,

$$L_{\mathrm{OD}_{i+1}} - L_{\mathrm{OD}_i} = L_0, \tag{1}$$

for $i = 1, 2, \ldots, N-1$. Here, L_{OD_i} and L_0 denote the optical lengths of OD_i, and the interval between two neighboring ODs, respectively. Also, L_{OD_1} is initialized by the optical length of the real channel in terms of matching.

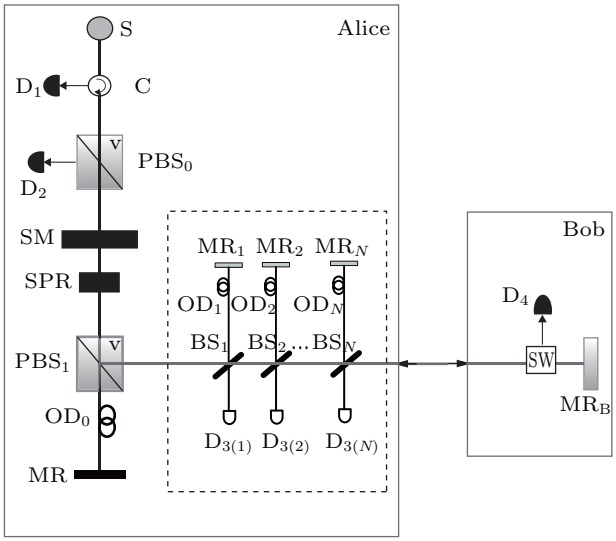


Fig. 3. Experimental setup. In contrast with the SLAZ2013 protocol, an iterative module in the dashed box is introduced to replace the original inner cycle. Here, BS_i stands for a beam splitter, and $\mathrm{D}_{3(i)}$ denotes a photon detector for $i = 1, 2, \ldots, N$. Bob uses a switch (SW) to carry out the blocking operation. SPR and SM stand for switchable polarization rotator and switchable mirror, respectively. Other notations: C is a circulator; D stands for the single-photon detector; S is the single-photon source; PBS stands for the polarizing beam splitter which only reflects vertically polarized photons; OD and MR stand for the optical delay and Mirror, respectively. In real implementations, the MR could be replaced by the Faraday mirror (FM) to offset the side effects induced by the noises and birefringence. The settings of PBS_0, PBS_1, SPR, and SM are the same as those in Ref. [17]. For instance, we have the rotating angle of SPR as $\beta_M = \theta/2 = \pi/4M$.

In Alice's station, a horizontally polarized (H) photon is emitted by the source, and it certainly arrives at SM, which is switched off initially to allow the photon to be transmitted but it then remains on for M cycles, and is turned off again after M cycles are completed. Due to the polarization rotation by SPR, the photon will either be reflected or transmitted by PBS_1. If the photon is not blocked by the SW at Bob's end, it will return to the SM and repeat the travel in a new cycle. Otherwise, the protocol will be restarted. The iterative module and Bob's station comprise a Michelson-type interferometer, in which quantum interference can be observed. Here, the combination of PBS_1 and the SPR cooperate with each other as a beam splitter. Therefore, the presented setup can be translated to a Mach–Zehnder type interferometer shown in Fig. 4, if we technically use a fictitious router to approximate the Michelson-type interferometer mentioned above. Bob's station is simpler: he chooses to block (logic 1) or pass (logic 0) the photon by controlling the SW.

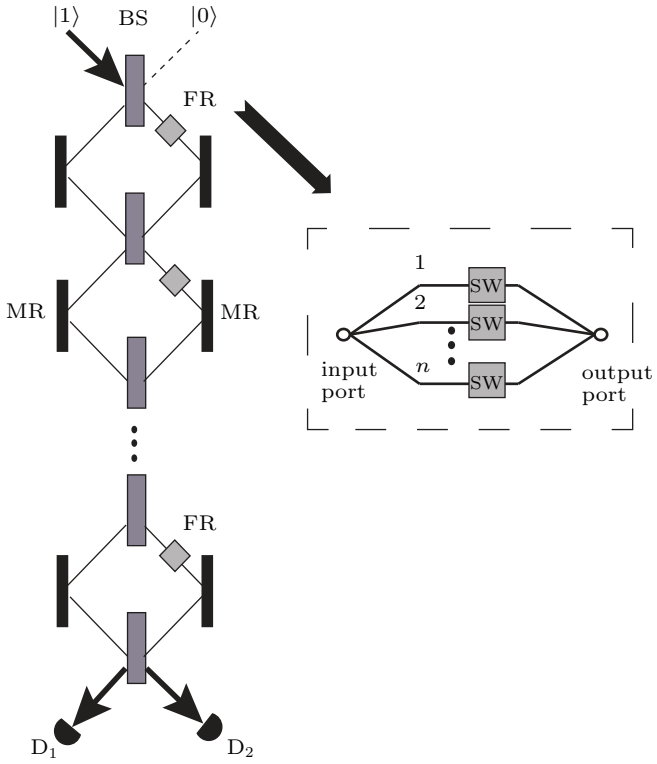


Fig. 4. Principle schematics. Here, FR stands for a fictitious probabilistic router, explicitly shown in the right side dashed box. The input node routes the photon to the output through one of the n paths. Here, we denote the probability that the photon goes through path i as P_{FR_i}. One of the n paths, say path k, corresponds to the real channel, such as path $\mathrm{BS}_N \rightarrow$ SW in Fig. 3.

Now, we explain why this router works and show the principle of the presented protocol in detail. When Bob passes the photon, representing the fact that Bob chooses logic 0, quantum interference immediately takes place in the presented interferometer. Explicitly, in each cycle, if the photon leaving SPR is reflected by PBS_1, it enters the iterative module and returns to PBS_1 with certainty owing to the interference (the phase difference is π radians between the two output paths of each BS). In other words, the photon will neither be detected by Bob nor by the detectors in the iterative module. In this sense, the Michelson-type interferometer is equivalent to the router FR with all its SWs on. From Fig. 3, the conditional probability that the photon was to manifest itself to the channel, i.e., P_{FR_k}, is estimated to be $\prod_{i=1}^{N} t_i$, where t_i is the transmissivity of the i-th BS in Fig. 3. In addition, it naturally follows from Fig. 4 that the initial quantum state $|10\rangle$, implying that the photon enters the first BS from the left hand side arm, ultimately evolves to $\cos M\theta|10\rangle + \sin M\theta|01\rangle$, which equals to $|01\rangle$. Consequently, it means that the photon will trigger detector D_2. Now, let us see how probabilistic counterfactual communication takes place. In each cycle, we see that P_{FR_k} is non-zero. It means that the information carrier, which triggers detector D_2, may have traveled through the channel or not. From Table 1, it immediately implies that this case is of the paradigm of probabilistic counterfactual communications. This property makes the presented scheme distinguished with deterministic counterfactual communication protocols. Interestingly, the presented scheme could easily evolve to a deterministic counterfactual one when $P_{\mathrm{FR}_k} \rightarrow 0$.

When Bob blocks the photon, the interference in the iterative module is destroyed. Therefore, it is most probably that a photon exiting PBS_1 is detected by Bob's detector D_4 or one of the detectors in the iterative module ($\mathrm{D}_{3(1)}$, $\mathrm{D}_{3(2)}$, …, $\mathrm{D}_{3(N)}$). In my previous work,[14] it is shown that the conditional occurrence rate of this event is obtained by

$$P_{\mathrm{ab}} = 1 - \sum_{i=1}^{N} \prod_{j=0}^{i-1} t_j^2 (1 - t_i)^2, \tag{2}$$

which satisfies

$$P_{\mathrm{ab}} \leq 1 - \frac{1}{N}(1 - p_{\mathrm{FR}_k})^2. \tag{3}$$

Here, we define that $t_0 \equiv 1$. Obviously, the P_{ab} approaches 1 asymptotically with $N \rightarrow \infty$. Correspondingly, in Fig. 4, we can also replace the Michelson-type interferometer by the route FR, if the i-th SW is set to be switched off with probability P_{B_i}, such that $\sum_{i=1}^{N} P_{\mathrm{FR}_i} P_{\mathrm{B}_i} = P_{\mathrm{ab}}$. Counterfactual communication here is ensured by the quantum Zeno effect, i.e.,

$$|10\rangle \rightarrow \cos^{M-1}\theta(\cos\theta|10\rangle + \sin\theta|01\rangle) \approx |10\rangle. \tag{4}$$

Consequently, detector D_1 clicks as a result. Note that probabilistic counterfactual communication never takes place in this case, since the photon going through the channel triggers detector D_4 with certainty (this event should be discarded).

4. Performance

Since the equivalent optical distance between Alice and Bob, D_{eq}, is only $M*L$, where L denotes the practical distance, (that is $D_{\mathrm{eq}} = M*N*L$ for SLAZ2013) the transmission time, i.e., $t = D_{\mathrm{eq}}/c$, has been reduced by a factor of N, which is a great step forward to implementing direct quantum counterfactual communication in real-life channels. Here, c denotes the light speed. Intuitively, the sensitivity to channel noises is degraded, since the equivalent communication distance is greatly shortened. Analysis of the robustness against channel noises will be presented in this section. Another advantage is that the counterfactuality rate of the procotol is improved, in contrast with the SLAZ2013 protocol.

4.1. Counterfactuality analysis

Here, the counterfactuality rate, denoted by C, is defined by the probability of a successful communication featured with no transmission of information carriers. In a deterministic scheme, it is usually given by a tuple $\boldsymbol{C} = (C_0, C_1)$. Here, C_0 and C_1 represent the counterfactuality rates for the signals 0 and 1, respectively. Obviously, C_i $(i = 0, 1)$ varies from 0

to 1, and perfect counterfactual communication is available if and only if $C_i = 1$ $(i = 0, 1)$. For the SLAZ2013 protocol, $C_{0(1)}$ equals to the detection rate $P_{1(2)}$, which is given by $|x(y)_M|^2$ (see Ref. [17] for more details). Also, this protocol achieves perfect counterfactuality when N and M approach infinity, leading to $\boldsymbol{C}_1 \to (1, 1)$, i.e., $P_1 \to 1$ and $P_2 \to 1$. However, in the presented protocol, the counterfactual rate C_0 could not be given by the detection rate, due to the absence of projective measurement. Fortunately, it can be estimated from its quantum description, which is a superposition of all possible paths.

Now, we begin to calculate the counterfactuality rates of the presented protocol. When Bob blocks the channel (logic '1'), deterministic counterfactual communication takes place. Therefore, C_1 is directly given by the detection rate of detector D_2, i.e.,

$$C_1 = \cos^{2M}\theta. \tag{5}$$

Obviously, perfect counterfactuality is achievable for signal "1", when M approaches infinity.

In the case of Bob passing the photon (logic '0'), it is impossible to determine C_0 from the detection rate of detector D_1, since there are probabilistic counterfactual events here. Therefore, C_0 should be estimated from the superposition state of each cycle. In Fig. 4, the superposition in the m-th cycle can be expressed by $|\varphi_m\rangle = \cos m\theta|10\rangle + \sin m\theta|01\rangle$, if the router is not taken into account (see Ref. [17]). Now, if the photon is in the right-hand side arm of the BS (the probability is $\sin^2 m\theta$), the photon enters the router, and the conditional probability of it passing the channel is given by P_{FR_k}. In total, C_0 is

$$C_0 = \prod_{m=1}^{M}(1 - \sin^2 m\theta \cdot P_{\mathrm{FR}_k}). \tag{6}$$

Obviously, equations (5) and (6) imply that perfect direct counterfactual communication can also be achieved when M approaches infinity, i.e., $C_0, C_1 \to 1$. One could also obtain $C_0 \to 1$ by setting $P_{\mathrm{FR}_k} \to 0$, keeping M unchanged. In this case, the presented protocol evolves to a deterministic one. More interestingly, the presented protocol could also turn out to be totally classical when $P_{\mathrm{FR}_k} = 1$. In this case, the router in Fig. 4 contains only one path, i.e., the channel. Therefore, this result is consistent with the one referring to Fig. 2(a) in Ref. [17], whose counterfactuality rate C_0 is also equal to 0.

We have loosely plotted the counterfactuality rate C_0, illustrating how it varies as a function of M. In Fig. 5, it is showed that all curves descend as M increases. In other words, the performance becomes worse with a bigger M, since the probability that a photon exposes itself in the channel evidently increases when the number of the cycles grows up. Fortunately, C_0 can be improved by reducing t (or independently increasing N). As is shown in Fig. 5, a curve, marked with a smaller t, locates itself over the others with bigger ones. This shows that high counterfactuality (e.g., $C_0 > 0.9$) is achievable with acceptable Ms, as long as t is chosen to be sufficiently small. In order to show the advantages over the SLAZ2013 protocol, we list some meaningful results, obtained from numerical estimating, in table 1. It is clear that, for the SLAZ2013 protocol, N should be sufficiently large (meanwhile things get worse as M increases), in order to achieve acceptable counterfactuality rates (bigger than 0.9). However, the same rates can be achieved with less resources in the presented protocol, as long as we carefully choose the value of t_j $(j = 1, 2, \ldots, N)$.

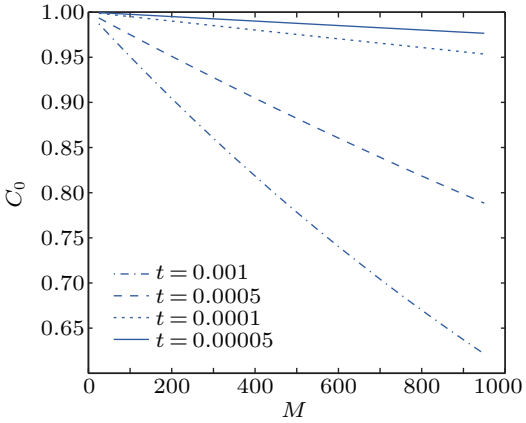


Fig. 5. C_0 as a function of M. Here, $t = P_{\mathrm{FR}_k}$.

Table 2. Numerical estimating results.

		$M = 25$	$M = 50$	$M = 75$	$M = 100$	$M = 150$
(I)[1]	$P_{\mathrm{FR}_k} = 0.001$	0.987	0.975	0.963	0.951	0.927
	$P_{\mathrm{FR}_k} = 0.0005$	0.994	0.987	0.981	0.975	0.963
	$P_{\mathrm{FR}_k} = 0.0001$	0.999	0.997	0.996	0.995	0.992
	$P_{\mathrm{FR}_k} = 0.00005$	0.999	0.999	0.998	0.997	0.996
(II)[2]	$N = 320$	0.912	0.831	0.758	0.693	0.582
	$N = 500$	0.943	0.887	0.836	0.788	0.702
	$N = 1250$	0.977	0.953	0.930	0.908	0.865
	$N = 2500$	0.988	0.976	0.964	0.953	0.930

(I)[1]: The first half of the table, corresponding to the presented protocol. The content units are filled with values of C_0, referring to different p_{FR_k} and M.
(II)[2]: The second half of the table, corresponding to the SLAZ2013 protocol. The content units are filled with values of p_2, referring to different M and N.

At last, we concluded the detector rates, Prob{D_1 clicks} and Prob{D_2 clicks}, which are given by

$$\mathrm{Prob}\{\mathrm{D}_1 \text{ clicks}\} = \cos^{2M}\theta, \tag{7}$$

and

$$\mathrm{Prob}\{\mathrm{D}_2 \text{ clicks}\} = 1. \tag{8}$$

The difference between Eq. (6) and (8) shows the probabilistic-counterfactual property of the protocol.

4.2. Robustness against channel noises

Here, the robustness of the presented protocol is only investigated in a most representative scenario that the channel noise acts as an obstacle which definitely registers an event of "Block". Errors only occur in the case of Bob choosing to pass the photon, where interference is destroyed by noises. Remarkably, for the presented protocol, the presence of noises definitely induces errors as well as an increase of the probability that detector $D_{3(j)}$, $(j = 1,2,\ldots,N)$ clicks, which independently discounts the performance of the protocol.

When Bob passes the photon, it will produce a click of detector D_2 with certainty owing to quantum interference, if the channel is noiseless. Let us see what happens when a "block" in one cycle is triggered by the noise other than Bob. Without loss of generality, we assume that the channel of the i-th cycle is blocked due to the noise. Given that the state of the i-th cycle is $|\varphi\rangle_i = x_i|10\rangle + y_i|01\rangle$, the quantum state after the $(i+1)$-th BS is written as

$$\begin{aligned}|\varphi\rangle_{i+1} &= (x_i\cos\theta - c * y_i\sin\theta)|10\rangle \\ &\quad + (x_i\sin\theta + c * y_i\cos\theta)|01\rangle,\end{aligned} \tag{9}$$

where c denotes the rate that the single-photon pulse in the channel of the i_{th} cycle is not absorbed. For instance, in the SLAZ2013 protocol, $c = 0(1)$, corresponding to Bob's choice "Block(pass)", means that the pulse is fully(never) absorbed by Bob's detector D_4. Interestingly, c varies from 0 to 1 for the presented protocol, since the iterative module also contributes to the benefit that the photon in the right-hand side arm is not absorbed.

Next, it is necessary to fix the rate "c" with given parameters of the module. Suppose that a photon is reflected by PBS_1 in the i-th cycle, it is easy to conclude the probability that it is reflected back to PBS_1 by one of the mirrors in the module as

$$P_{\text{ref}} = \sum_{i=1}^{N}\prod_{j=0}^{i-1} t_j^2(1-t_i)^2, \tag{10}$$

due to the absence of quantum interference. Also, the probability that it is absorbed is

$$P_{\text{abs}} = 1 - \sum_{i=1}^{N}\prod_{j=0}^{i-1} t_j^2(1-t_i)^2 - \prod_{i=o}^{N} t_i. \tag{11}$$

Obviously, we have $c = P_{\text{ref}}$. Moreover, it is seen that a photon will be detected by $D_{3(j)}$, $(j = 1,2,\ldots,N)$ with unit probability, when N approaches infinity.[14] Nevertheless, it is still interesting to investigate the robustness of the presented protocol in finite settings, where c is indeed a non-zero real number less than 1. In order to find how c discounts the rate of detector D_2, we try to correlate Prob{D_2 clicks} with c formally. Assume independently that a single-photon pulse, denoted by an unnormalized quantum state $|\psi\rangle = c|01\rangle$, arrives at the $(i+1)$-th BS in Fig. 4, the final state after the following $M-i$ BSs is written by

$$|\psi\rangle_{\text{final}} = c * (\cos(M-i)\theta|01\rangle - \sin(M-i)\theta|10\rangle), \tag{12}$$

owing to quantum interference. Obviously, it is seen from Eq. (12) that this independent pulse definitely contributes to the rate of detector D_2. Therefore, Prob{D_2 clicks}, which is given by Prob{D_2 clicks} $= (1-(1-c)y_i\cos(M-i)\theta)^2$, directly increases as c increases. Equation (10) shows the balance of c and N, and that $c = 0$ when $N \to \infty$ for the worst case. Now, we use the same technique, that random numbers between 0 and 1 are employed to play the role of noise, to plot the successful rate of the right detector. The curves in Fig. 6(a) are statistically averaged on a 2000-times repetition to achieve better smoothness. Obviously, the protocol outperforms the SLAZ2013 protocol on the tolerance of noise given the same M. Moreover, a smaller M implies a bigger tolerance of B for the presented protocol, which is consistent with the fact that an increase of the number of cycles immediately increases the risk of suffering from channel noises.

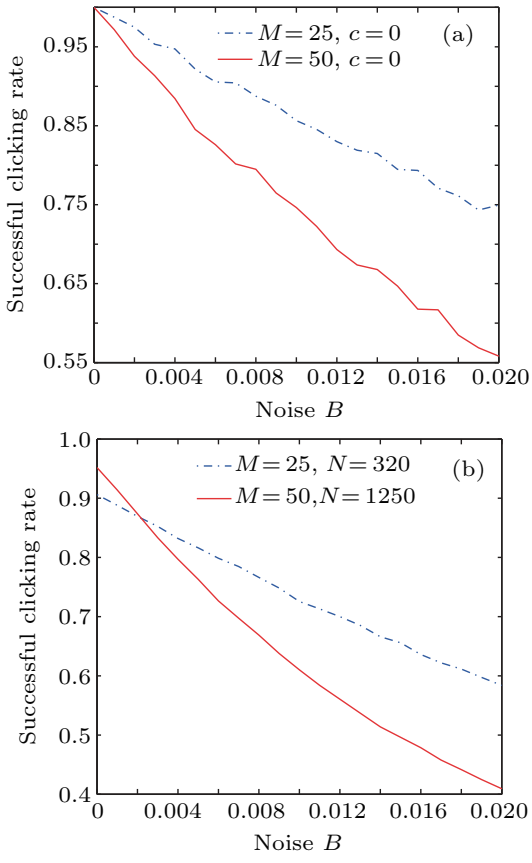


Fig. 6. (color online) Numerical estimating results. (a) Successful clicking rate of the presented protocol as a function of the noise rate B. Here, $c = 0$, corresponding to the worst case, is chosen as a better sample to make a comparison with the SLAZ protocol. The solid (dash–dot) curve is plotted for $M = 25$ (50). (b) Successful clicking rate of the SLAZ2013 protocol as a function of the noise rate B. The solid (dash–dot) curve is plotted for $M = 25$ (50), $N = 320$ (1250).

5. Discussions

Although the side-effect of the chained quantum Zeno effect is greatly reduced by the iterative module, another arises from this component. When Bob chooses to block the photon, it is likely in a single cycle that he cannot capture it, even if it enters the module, since the photon could be reflected by one of the mirrors in the module, i.e., MR_1, $\mathrm{MR}_2,\ldots,\mathrm{MR}_N$, and returns back to PBS_1 (the conditional probability told by Eq. (2) is $\sum_{i=1}^{N}\prod_{j=0}^{i-1}t_j^2(1-t_i)^2$). Fortunately, this effect contributes, though unobviously, to the counterfactualitiy C_1.

It is impossible to directly apply this protocol or SLAZ2013-like ones to secure communications, such as quantum key distribution. The central problem is that a no-cloning theorem is not included in principle. In these protocols, only orthogonal states, say, $|\phi_0\rangle$ and $|\phi_1\rangle$, are employed. Fortunately, it is not difficult to make them secure. All one should do is to change the pure states into nonorthogonal mixed states, i.e., $\mathrm{Tr}[\rho_0\rho_1]\neq 0$. For example, the Noh09 protocol is of this kind. Here, we also highlight an open question that whether it is possible to explore unconditional security directly from the quantum Zeno effect, thus leading to a new paradigm outperforming existing quantum key distribution schemes.

6. Conclusion

In summary, we have opened the door of probabilistic counterfactual quantum communication. Generally, a high counterfactuality rate can be achieved with less resources, in contrast with previous schemes based on the chained quantum Zeno effect. Also, we should point out that this protocol is not symmetrical, since probabilistic counterfactual communication only occurs when the quantum interference remains. It is a challenge whether this symmetry could help to further reduce the transmission time.

References

[1] Bennett C H and Wiesner S J 1992 *Phys. Rev. Lett.* **69** 2881
[2] Mattle K and Weinfurter H and Kwiat P G and Zeilinger A 1996 *Phys. Rev. Lett.* **76** 4656
[3] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 *Phys. Rev. Lett.* **70** 1895
[4] Boschi D, Branca S, De Martini F, Hardy L and Popescu S 1998 *Phys. Rev. Lett.* **80** 1121
[5] Noh T G 2009 *Phys. Rev. Lett.* **103** 230501
[6] Sun Y and Wen Q Y 2010 *Phys. Rev. A* **82** 052318
[7] Bennett C H, Brassard G, *et al.* 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, December 9–12, 1984, Bangalore, India, p. 175
[8] Elitzur A C and Vaidman L 1993 *Found. Phys.* **23** 987
[9] Kwiat P G *et al.* 1999 *Phys. Rev. Lett.* **83** 4725
[10] Noh T G and Hong C K 1999 *Quantum Semiclass. Opt.* **10** 637
[11] Zhang S and Wang J and Tang C J 2013 *Commun. Theor. Phys.* **10** 637
[12] Yin Z Q, Li H W, Chen W, Han Z F and Guo G C 2010 *Phys. Rev. A* **82** 042335
[13] Zhang S, Wang J and Tang C J 2012 *Chin. Phys. B* **21** 060303
[14] Zhang S, Wang J and Tang C J 2012 *Europhys. Lett.* **98** 30012
[15] Liu Y, Ju L, Liang X L, Tang S B, Tu G L, Zhou S, Peng L, Chen C Z, Chen K, Chen T Y, *et al.* 2012 *Phys. Rev. Lett.* **109** 030501
[16] Brida G, Cavanna A, Degiovanni I P, Genovese M and Traina P 2012 *Laser Phys. Lett.* **9** 247
[17] Salih H, Li Z H, Al-Amri M and Zubairy M S 2013 *Phys. Rev. Lett.* **110** 170502
[18] Vaidman L 2007 *Phys. Rev. Lett.* **98** 160403
[19] Salih H 2014 *Phys. Rev. A* **90** 012333
[20] Shenoy A, Srikanth R and Srinivas T 2014 *Phys. Rev. A* **89** 052307
[21] Shenoy H A, Srikanth R and Srinivas T 2013 *Europhysics Lett.* **103** 60008
[22] Guo Q, Cheng L Y, Chen L, Wang H F and Zhang S 2014 arXiv: 1404.6401 [quant-ph]
[23] Greiner W 2001 *Quantum Mechanics: An introduction* (Berlin: Springer)
[24] Hosten O, Rakher M T, Barreiro J T, Peters N A and Kwiat P G 2006 *Nature* **439** 949
[25] Mitchison G Jozsa R 2007 arXiv: quant-ph/0606092v3
[26] Vaidman L 2016 arXiv: 1511.006615v2 [quant-ph]
[27] Vaidman L 2016 arXiv: 1605.02181v1 [quant-ph]
[28] Marlow A R 1978 *Mathematical Foundations of Quantum Theory*. (New York: Academic Press) pp. 36