Direct Counterfactual Quantum Communication with High Efficiency

Sheng Zhang
Department of Electronic Technology, China Maritime Police Academy, Ningbo 315801, China

Xing-tong Liu and Bo Zhang
School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China

(Dated: October 13, 2014)

Recently, a novel direct counterfactual quantum communication protocol was proposed using chained quantum Zeno effect. We found that this protocol is far from being widely used in practical channels, due to the side effect of "Chained". First, the probability that the interference is destroyed by the noise is far bigger than one expects. Second, the efficiency is very low since the total optical distance between the two parties, Alice and Bob, is $M \ast N$ times the original one. Here, we propose an improved protocol, in which the side effect is removed by adding a customized module.

I. 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\cite{1,2}, teleportation\cite{3,4} and counterfactual quantum key distribution\cite{5,6}, are naturally achieved. Since the invention of quantum key distribution(QKD) protocol, i.e., BB84 protocol\cite{7}, quantum communication has enjoyed a 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\cite{8,9,10}, impressive with the phenomenon that an object can be detected without being intuitively measured. The first example, presented by Noh\cite{5}, was realized in a QKD protocol. Later, we announced a variant adapted to deterministic key distribution scenario\cite{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.\cite{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\cite{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\cite{14}. Since the rate of information photons in Noh09 protocol, only up to 12.5% in ideal setting, is not satisfactory, Sun and Wen improved it to reach 50% using an iterative module\cite{6}. Experimental verifications of Noh09 protocol have been made by various authors\cite{13,10}.

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

Here, we argue that it is problematic to apply SLAZ2013 protocol in real channels, unless the side effect of chained quantum Zeno effect is degraded to an acceptable level. Notice that the total optical distance between Alice and Bob, being amplified by $M \ast N$(numbers of the outer and inner cycles) times, is far larger than the original one, though it is good to use chained quantum Zeno effect to achieve perfect counterfactuality. Consequently, the efficiency, on the first hand, turns out to be very low. In other words, transferring one bit might take a long time, even though Alice and Bob stand close to each other. On the second hand, the noise rate is coupled. Thus, even a slight disturbance might stop the system from a normal running.

In this paper, we present a new protocol, which outperforms SLAZ2013 protocol with respect to efficiency. The rest of the paper is organized as follow: In section II, this protocol is introduced. Then, we analyze the counterfactuality of our protocol and SLAZ2013 in the following section, showing the advantage of our protocol. In section IV, we have a brief discussion on how to bridge the presented protocol and quantum key distribution. At last, a conclusion is drawn.

*shengzhcn@gmail.com
II. PROTOCOL

First, we give a brief introduction of SLAZ2013 protocol. To achieve the goal of counterfactuality, 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. At very beginning, a photon, which has nothing to do with the information bit, is injected by the source, and entering the input port of the outer cycle. The rest 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’s 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:

- \( (E_1) \) The photon has been caught in detector \( D_1 \).
- \( (E_2) \) The photon has been caught in detector \( D_3 \).

Note that \( E_2 \) implies that the photon has been traveling through the channel. Therefore, \( E_2 \) should be discarded. Similarly, when ”1” is selected, events \( E_3 \) and \( E_4 \) can be observed:

- \( (E_3) \) The photon has been caught in detector \( D_2 \).
- \( (E_4) \) The photon has been caught in detector \( D_4 \).

Again, \( E_4 \), which goes against the counterfactuality, is discarded. The central problem is that the twisted structure (i.e., outer cycle twisting with inner cycles) directly increases the optical length of the channel.

Now, we introduce our protocol. First, let’s see the setup shown in Fig.1. Compared with SLAZ2013, the only difference is easily found. We put an iterative module (shown in the dashed rectangle), which is as the same as the one in Ref. or except for the mirrors, to replace the original inner cycle. Note that the length of each optical delay (OD) in this module should be carefully chosen to match each other. Specifically, the following condition should be satisfied,

\[
L_{OD_{i+1}} - L_{OD_i} = L_0, \tag{1}
\]

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

Next, let’s see how this protocol works. Not surprisingly, the protocol begins with a vertically polarized photon, i.e., the state \( |V> \), which will be caught in detector \( D_1 \) or \( D_2 \), according to Bob’s choice 1 or 0, respectively. The explanation is presented as follow.

In Fig.2, When Bob passes the photon (all SWs are on), path \( i(i = 1, 2, ..., n) \) corresponds to the optical path \( PBS_i \rightarrow MR_j(j = 1, 2, ..., N) \) or \( PBS_i \rightarrow MR_B \). In this case, our protocol degrades to the first step of SLAZ2013, owing to the interference. Therefore, detector \( D_2 \) clicks with certainty. However, when all SWs are off, the interference is destroyed. Consequently, the photon will be caught in the corresponding detector, i.e., \( D_4 \) or \( D_3(i) \), if it is in the right arm of the BS. In this case, our protocol is also equivalent to the first step of SLAZ2013, excepted that in which detector the photon arrives. In
other words, our protocol shares the same principle with SLAZ2013 in spite of some details.

III. PERFORMANCE

In this section, we first show how our protocol benefits from the iterative module with counterfactuality aspect, and then a comparison with SLAZ2013 protocol is presented using numerical estimation.

Before the analysis begins, the conception "counterfactual rate", denoted by $C$, should be reviewed. Here, it is defined by the probability of a successful communication featured with no transmission. Correspondingly, another conception "abnormality rate" denoted by $A$ is defined by the reverse, so we have $A = 1 - C$. Now, we are able to define the counterfactuality of a given protocol by a pair of counterfactual rates(or abnormality rates), $\vec{C} = (C_0, C_1)$, each representing the counterfactual rate for signal 0 and 1, respectively. Evidently, $C_i (i = 0, 1)$ varies from 0 to 1, and perfect counterfactual communication is available if and only if $C_i = 1 (i = 0, 1)$.

Back to SLAZ2013 protocol, it is easy to find that her counterfactuality, denoted by $\vec{C}'_1$, is given by $P_1$ and $P_2$, so we have

$$\vec{C}'_1 = (P_1, P_2).$$

Certainly, this protocol reaches towards perfect counterfactuality when $N$ and $M$ approach infinity, leading to $\vec{C}'_1 \rightarrow (1, 1)$. Also note that this protocol is achieved in two steps, which appear with the following concern: In the first step, the protocol, referring to Fig.2(a) of Ref.[17], is only partially counterfactual. In this case, we only obtain

$$\vec{C}'_1 \rightarrow (0, 1),$$

for whatever $N$s. Therefore, the second step, in which an inner cycle is employed, is introduced in order to achieve perfect counterfactuality. However, in our scheme, we try to achieve the same goal by replacing the inner cycle with an iterative module.

Now, we begin to calculate the counterfactuality of our protocol, denoted by $\vec{C}_2$, where $\vec{C}_2 = (C_0, C_1)$. Fortunately, it is easy to determine $C_1$, which immediately implies that Bob blocks the channel. From the definition of $C_1$, it is natural to obtain

$$C_1 = \cos^{2M} \theta,$$

which is also the probability that $D_1$ clicks. Here, $\theta = \pi / 2M$.

When Bob passes the photon, i.e., signal 0 is selected, a successful counterfactual communication is established only when there is no photon in the channel in each cycle. Back to Fig[2] the probability that the photon travels through the channel in the $m_{th}$ cycle is given by $t = \prod_{j=1}^{N} t_j$, where $t_j$ is the transmissivity of the $j_{th}$ BS in the module. Therefore, $C_0$ can be written as

$$C_0 = \prod_{m=1}^{M} (1 - \sin^2 m\theta \cdot t).$$

Obviously, Eqs.(4) and (5) imply that perfect direct counterfactual communication is achievable when $N$ approaches infinity. Interestingly, our protocol equals to the first step of SLAZ2013 protocol, given $t = 1$. Therefore, we directly obtain $C_0 = 0$, which is consistent with Eq.(3), as we have expected.

From above analysis, it is known that parameters $N$ and $M$ are crucial to achieve a better performance. We have loosely plotted the counterfactuality rate $C_0$, in order to illustrate how it varies as a function of $M$. In Fig[3] it is showed that all curves descend as $M$ increase. In other words, the performance of our protocol becomes worse with a bigger $M$, since the probability that 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[3] 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 $M$s, as long as $t$ is chosen to be sufficiently small. In order to show our advantages over SLAZ2013 protocol, we list some meaningful results, obtained from numerical estimating, in table 1.

\begin{table} [h]
\centering
\begin{tabular}{|c|c|c|c|}
\hline
$N$ & $C_0$ & $M$ & $t$ \\
\hline
10 & 0.1 & 100 & 0.0001 \\
20 & 0.3 & 100 & 0.0005 \\
30 & 0.5 & 100 & 0.001 \\
40 & 0.7 & 100 & 0.005 \\
\hline
\end{tabular}
\caption{Counterfactuality rates comparison with SLAZ2013 protocol.}
\end{table}

It is clear that, for SLAZ2013 protocol, $N$ should be sufficiently large(things get worse as $M$ increases), in order to achieve acceptable counterfactuality rates(bigger than 0.9). However, the same goal can be achieved, for our protocol, only by choosing an appropriate $t$, keeping $M$ unchanged.
TABLE I. Numerical estimating results

|        | $M = 25$ | $M = 50$ | $M = 75$ | $M = 100$ | $M = 150$ |
|--------|----------|----------|----------|-----------|-----------|
| (I)    |          |          |          |           |           |
| $t = 0.001$ | 0.987    | 0.975    | 0.963    | 0.951     | 0.927     |
| $t = 0.0005$ | 0.994    | 0.987    | 0.981    | 0.975     | 0.963     |
| $t = 0.00001$ | 0.999    | 0.997    | 0.996    | 0.995     | 0.992     |
| (II)   |          |          |          |           |           |
| $N = 320$  | 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    | 0.955    | 0.930    | 0.908     | 0.865     |
| $N = 2500$ | 0.988    | 0.976    | 0.964    | 0.953     | 0.930     |

1 (I): The first half of the table, corresponding to our protocol. The content units are filled with values of $C_0$, referring to different $t$s and $M$s.

2 (II): The second half of the table, corresponding to SLAZ2013 protocol. The content units are filled with values of $p_2$, referring to different $M$s and $N$s.

Since our protocol shares the same template with the simplified SLAZ2013 protocol, i.e., the first-step protocol, it is easy to conclude the detector rates, $P_1$ and $P_2$, which are given by $P_1 = 1$ and $P_2 = \cos^{2M}\theta$.

IV. DISCUSSIONS

Although both our protocol and SLAZ2013 provide us ways to establish counterfactual communication, which is impossible with classical means, we should point out that they always fail in a secure scenario, such as quantum key distribution. The central problem is that no-cloning theorem is not included in their principles. Specifically, in both protocols, only orthogonal states, say, $|\phi_0>$ and $|\phi_1>$, 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., $Tr[|\rho_0><\rho_1|] \neq 0$. For this, Noh09 protocol acts as a good example. In doing so, our protocol immediately evolves to a quantum key distribution scheme. Here, we also highlight an open question that whether it is possible to explore unconditional security directly from quantum Zeno effect, thus leading to a new paradigm outperforming existed quantum key distribution schemes.

V. CONCLUSION

It is interesting that direct counterfactual quantum communication is achievable using quantum Zeno effect. However, the original scheme, i.e., SLAZ2013 protocol, has new problems when applying it in real channels. First, the efficiency is low, compared with conventional schemes. Second, it is too sensitive to noise. We find that those two flaws are resulted from the twisted structure, i.e., the inner cycles and outer cycles. In this paper, we have tried to rule out the twist by replacing the inner cycle with an iterative module, which is the core component of our new protocol. We has also proved that perfect counterfactuality is achievable for our protocol, and numerical estimating shows that our protocol outperforms the original one in that it is easier to reach a high quality of counterfactuality with less cycles. At last, we discussed how to bridge our protocol and quantum key distribution with no-cloning theorem, in order to broaden the view of direct counterfactual quantum communication.

VI. ACKNOWLEDGEMENTS

This work was supported by National Natural Science Foundation of China with the project number 61300203.
[21] Q. Guo, L.-Y. Cheng, L. Chen, H.-F. Wang, and S. Zhang, arXiv preprint arXiv:1404.6401 (2014)