Quantum Information and Computation, Vol. 11, No. 11&12 (2011) 0913–0924

PASSIVELY SELF-ERROR-REJECTING QUBIT TRANSMISSION OVER A COLLECTIVE-NOISE CHANNEL

FU-GUO DENG [a]
Department of Physics, Applied Optics Beijing Area Major Laboratory
Beijing Normal University, Beijing 100875, China

XI-HAN LI
Department of Physics, Chongqing University, Chongqing 400044, China

HONG-YU ZHOU
College of Nuclear Science and Technology, Beijing Normal University
Beijing 100875, China

Received November 30, 2010
Revised July 30, 2011

We propose a passively self-error-rejecting single-qubit transmission scheme for an arbitrary polarization state of a single qubit over a collective-noise channel, without resorting to additional qubits and entanglement. By splitting a single qubit into some wavepackets with some Mach-Zehnder interferometers, we can obtain an uncorrupted state with a success probability approaching 100% via postselection in different time bins, independent of the parameters of collective noise. It is simpler and more flexible than the schemes utilizing decoherence-free subspace and those with additional qubits. One can directly apply this scheme to almost all quantum communication protocols based on single photons or entangled photon systems against a collective noise.

Keywords: faithful single-qubit transmission, self-error-rejecting, collective-noise channel, Mach-Zehnder interferometer, quantum communication
Communicated by: S Braunstein & R Laflamme

1 introduction

Quantum key distribution (QKD) supplies a secure way for two parties, say the sender Alice and the receiver Bob, to generate a shared key, provided that they initially share a short secret key (for identity authentication) and that they possess an unprotected quantum channel (an optical fiber). Different from classical crypto-system in which the security of key depends on computation difficulty with a limited computation power, the security of QKD comes from the laws of quantum mechanics such as the uncertainty relation (non-cloning theorem), the coherence of entangled systems, quantum measurement, and so on. As an unknown quantum state cannot be cloned, the vicious actions done by an eavesdropper, say Eve will inevitably disturb the quantum system and leave a trace in the outcomes obtained by the two authorized parties. Eve's action will be detected by analyzing the error rate of samples chosen randomly. Since Bennett and Brassard published the original QKD protocol [1] in 1984 (called BB84),

[a]Author to whom correspondence should be addressed. Email address: fgdeng@bnu.edu.cn

QKD attracts a great deal of attention [2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17] and has been proven unconditionally secure [18, 19]. Recently, some groups demonstrated successfully long-distance quantum cryptography [20, 21, 22, 23] and its network [24, 25, 26, 27, 28, 29].

Implementations of practical QKD rely on either the polarization or the differential phases of photons. Preventing Eve from eavesdropping by disguising her action as noise with a better quantum channel requires the two legitimate users to reduce the influence of the noise in their quantum channels. Otherwise, they can only distill a short shared key from a large raw string with privacy amplification [2]. When the noise in the quantum channels is too large, secure key generation is impossible. For overcoming the birefringence of the optical fiber which alters the polarization state of photons, some QKD schemes are proposed with Mach-Zehnder interferometers (MZIs) and a Faraday mirror which is used to compensate polarization mode dispersion, such as the "plug and play" QKD system [30] and its modifications [31, 32]. However, these two-way quantum communication schemes are vulnerable to the Trojan horse attack [33]. Also, it is not easy for the two legal users in quantum communication to reduce the noise effect caused by the thermal fluctuation, vibration, and the imperfection of the fiber. Recently, some novel techniques are developed for protecting quantum information transmission, such as decoherence-free subspaces (DFS) [34, 35, 36, 37], error-correcting codes [38, 39], faithful qubit distribution [40, 41], faithful qubit transmission [42], error-rejecting codes [43], and so on. In DFS, a single logical qubit can be encoded in two physical qubits [44], i.e., $|\bar{0}\rangle \rightarrow |HV\rangle \equiv |H\rangle_{A_1}|V\rangle_{A_2}$, $|\bar{1}\rangle \rightarrow |VH\rangle \equiv |V\rangle_{A_1}|H\rangle_{A_2}$. Here $|H\rangle$ and $|V\rangle$ represent the horizontal polarization and the vertical polarization, respectively. Usually, there is a time delay Δt between the qubit A_1 and the qubit A_2. This code makes the logical qubits be immune to a collective-dephasing noise which is described with a transformation [34]: $|H\rangle \rightarrow |H\rangle$, $|V\rangle \rightarrow e^{i\phi}|V\rangle$ (the additional phase ϕ is unknown to any one). Under this transformation, the states of two physical qubits $|HV\rangle$, $|VH\rangle$, and $\frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle)$ all are immune to this collective-dephasing noise, and can be used for quantum communication perfectly [34]. Wang showed that DFS can also used for QKD over a collective- random-unitary-noise channel by checking parity and sacrificing a proportion of qubits [45]. In error-correcting codes [38], at least five entangled physical qubits are encoded for a single logical qubit against the noise. In 2005, Yamamoto *et al.* [40] introduced a good way for faithful qubit distribution with one additional qubit against a collective noise. Their scheme can be perfectly used for secure key generation with two quantum channels. The proportion of uncorrupted qubits to those transmitted approaches 1/8 (it depends on the coefficients of the noise [41]). More recently, a scheme [42] for faithful qubit transmission without additional qubits is proposed with two quantum channels. Its proportion of uncorrupted qubits to those transmitted approaches 1/2 in a passive way. With some delayers, the proportion can be improved to 1. In the error-rejecting codes [43], at least two fast polarization modulators (Pockels cell), whose synchronization makes it difficult to be implemented with current technology [46], are employed [42]. In the quantum error-rejection code protocol proposed by Wang [47] against bit-flipping errors with entanglement, the user should exploit a parity-check tool to read out the qubit probabilistically.

In this paper, we introduce a scheme for passively self-error-rejecting single-qubit transmission over a collective-noise channel with a success probability approaching 100%, several times of other schemes. For example, the success probability in the present scheme is about eight

times as that in the scheme proposed by Yamamoto *et al.* [40] in a passive way. Moreover, it is independent of the parameters of a collective noise. Unlike other schemes [34, 35, 36, 45, 47], it does not require entanglement. Different from Yamamoto's scheme [40], the present scheme needs no additional qubits and it also works for the transmission of one photon in an entangled photon pair. Moreover, our scheme works with one quantum channel, not two [40, 42] or more, and its implement is based on some simple optical devices. All these good features make it easy to apply for almost all quantum communication protocols existing, such as the quantum cryptography protocols based on single photons or entangled photon systems.

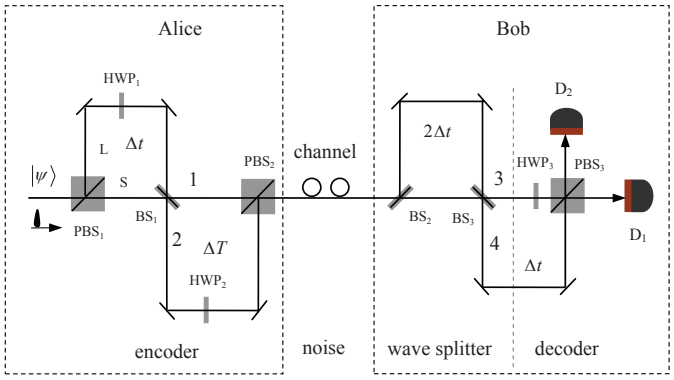

Fig. 1. Schematic representation of the present self-error-rejecting single-qubit transmission scheme over a collective-noise channel. PBS_i $(i = 1, 2, 3)$, HWP, and BS_i represent a polarizing beam splitter, a half wave plate, and a beam splitter (50/50), respectively. The intervals between the long path and the short path in the two unbalanced Mach-Zehnder interferometers are Δt and ΔT, respectively.

2 Passively self-error-rejecting single-qubit transmission protocol

The principle of our self-error-rejecting single-qubit transmission scheme over a collective-noise channel is shown in Fig.1. It comprises an encoder, a collective-noise channel, a wave splitter, and a decoder. The fluctuation in the collective-noise channel is slow in time so that the alteration of the polarization is considered to be the same over the sequence of several photons (or wavepackets) [40]. The encoder is made up of two unbalanced Mach-Zehnder interferometers (MZIs) with different intervals, i.e., Δt ($\Delta t \equiv t_L - t_S$) and ΔT. A single qubit, whose original state is $|\psi\rangle_0 = \alpha|H\rangle + \beta|V\rangle$, is split into two parts by the first polarizing beam splitter (PBS), which transmits $|H\rangle$ and reflects $|V\rangle$. A half wave plate (HWP) rotates the polarization of the photons in the path L by 90^o, i.e., $|H\rangle \leftrightarrow |V\rangle$. Before the first beam splitter (BS_1:50/50), the state of the single qubit can be described as $|\psi\rangle_B = \alpha|H\rangle_S + \beta|H\rangle_L \equiv \alpha|H\rangle_0 + \beta|H\rangle_{\Delta t}$. Therefore, the single qubit before it enters the collective-noise channel is in the state

$$|\psi\rangle_C = \frac{1}{\sqrt{2}}(\alpha|H\rangle_0 + i\beta|H\rangle_{\Delta t} + i\alpha|V\rangle_{\Delta T} + \beta|V\rangle_{\Delta T+\Delta t}) \equiv \frac{1}{\sqrt{2}}(|\psi\rangle_H + |\psi\rangle_V), \quad (1)$$

where

$$|\psi\rangle_H \quad = \quad \alpha|H\rangle_0 + i\beta|H\rangle_{\Delta t}, \quad (2)$$

$$|\psi\rangle_V \quad = \quad i\alpha|V\rangle_{\Delta T} + \beta|V\rangle_{\Delta T+\Delta t}. \tag{3}$$

The complex coefficient i comes from the phase shift aroused by the BS_1 reflection (we assume that the surface of the BS_1 has the phase shift i between the wave packet reflected and that transmitted), and the subscripts represent the signal time slots arrived.

Suppose that the collective noise in an optical fiber transforms the polarization states of a photon as

$$|H\rangle \quad \rightarrow \quad \delta_1|H\rangle + \eta_1|V\rangle, \tag{4}$$
$$|V\rangle \quad \rightarrow \quad \delta_2|H\rangle + \eta_2|V\rangle, \tag{5}$$

where

$$|\delta_1|^2 + |\eta_1|^2 = |\delta_2|^2 + |\eta_2|^2 = 1. \tag{6}$$

The four parameters δ_1, η_1, δ_2, and η_2 vary with the time t slowly, which means that only the photons transmitted close to each other suffer from the same noise. The decoherence channels represented by the unitary transformations shown in Eqs.(4) and (5) indicate that a photon is in a pure polarization state when it is emitted from the noisy channel although it is rotated and its state is unknown to us accurately (for a large number of single photons, we should use a mixed state to describe the state of a photon statistically).

The states shown in Eqs.(2) and (3) have the same form but different parameters, and so do the rotations arisen from the noisy channels shown in Eqs.(4) and (5). That is, Bob can distill an uncorrupted state from the states $|\psi\rangle_H$ and $|\psi\rangle_V$ with the same principle. We first discuss the principle of the decoder for distilling an uncorrupted state from the state $|\psi\rangle_H$ in detail as follows and then generalize it from the state $|\psi\rangle_V$.

The rotation by the collective-noise channel on the state $|\psi\rangle_H$ will transform it into the state $|\psi'\rangle_H$, i.e.,

$$\begin{aligned} |\psi\rangle_H \xrightarrow{noise} |\psi'\rangle_H \quad &= \quad \delta_1(\alpha|H\rangle_0 + i\beta|H\rangle_{\Delta t}) + \eta_1(\alpha|V\rangle_0 + i\beta|V\rangle_{\Delta t}) \\ &\equiv \quad \delta_1[\alpha + i\hat{D}(\Delta t)\beta]|H\rangle_0 + \eta_1[\alpha + i\hat{D}(\Delta t)\beta]|V\rangle_0 \\ &\equiv \quad \delta_1|\phi\rangle_H + \eta_1|\phi\rangle_V. \end{aligned} \tag{7}$$

Here

$$\begin{aligned} |\phi\rangle_H \quad &= \quad [\alpha + i\hat{D}(\Delta t)\beta]|H\rangle_0, \\ |\phi\rangle_V \quad &= \quad [\alpha + i\hat{D}(\Delta t)\beta]|V\rangle_0, \end{aligned} \tag{8}$$

and $\hat{D}(\Delta t)$ is a time-delay operator. That is,

$$\begin{aligned} \hat{D}(\Delta t)|\psi\rangle_0 \quad &= \quad |\psi\rangle_{\Delta t}, \\ \hat{D}(\Delta t_1)\hat{D}(\Delta t_2) \quad &= \quad \hat{D}(\Delta t_1 + \Delta t_2). \end{aligned} \tag{9}$$

Bob uses a wave splitter and a decoder to distill an uncorrupted state, shown in Fig.1. The time interval between the two paths of the wave splitter is $2\Delta t$. The wave splitter and the decoder has the same role for the states $|\phi\rangle_H$ and $|\phi\rangle_V$ but different outports of the PBS_3.

The combination of the wave splitter and the decoder will complete the transformation on the state $|\phi\rangle_H$ as follows,

$$\begin{aligned} |\phi\rangle_H \to |\phi'\rangle_H &= \{\hat{\sigma}_x + i\hat{D}(\Delta t) + \hat{D}(2\Delta t)[i^2\hat{\sigma}_x + i\hat{D}(\Delta t)]\}|\phi\rangle_H \\ &= \{\hat{\sigma_x}\alpha + i\hat{D}(\Delta t)[\hat{\sigma}_x\beta + \alpha] + i^2\hat{D}(2\Delta t)[\beta + \hat{\sigma}_x\alpha] \\ &\quad + i\hat{D}(3\Delta t)[i^2\hat{\sigma}_x\beta + \alpha] + i^2\hat{D}(4\Delta t)\beta\}|H\rangle_0 \\ &\equiv \hat{K}|H\rangle_0, \end{aligned} \tag{10}$$

where $\hat{K}$ is a quantum operator used for describing the principle of the reconstruction of the unknown state $|\psi\rangle_0$ and $\hat{\sigma}_x = |H\rangle\langle V| + |V\rangle\langle H|$ is a bit-flip operation. Bob can get an uncorrupted state $|\psi\rangle_0$ from the outport D_2 of the PBS_3 at the time slots Δt, $2\Delta t$, and $3\Delta t$ with the unitary operations I, $\hat{\sigma}_x$, and $\hat{\sigma}_z$, respectively, which takes place with the success probability 3/4, shown in Fig.2. That is,

$$\begin{aligned} \Delta t: &\quad (\alpha + \hat{\sigma}_x\beta)|H\rangle = \alpha|H\rangle + \beta|V\rangle \xrightarrow{I} \alpha|H\rangle + \beta|V\rangle, \\ 2\Delta t &: (\hat{\sigma}_x\alpha + \beta)|H\rangle = \alpha|V\rangle + \beta|H\rangle \xrightarrow{\hat{\sigma}_x} \alpha|H\rangle + \beta|V\rangle, \\ 3\Delta t &: (\alpha + i^2\hat{\sigma}_x\beta)|H\rangle = \alpha|H\rangle - \beta|V\rangle \xrightarrow{\hat{\sigma}_z} \alpha|H\rangle + \beta|V\rangle. \end{aligned} \tag{11}$$

Here $I = |H\rangle\langle H| + |V\rangle\langle V|$ and $\hat{\sigma}_z = |H\rangle\langle H| - |V\rangle\langle V|$.

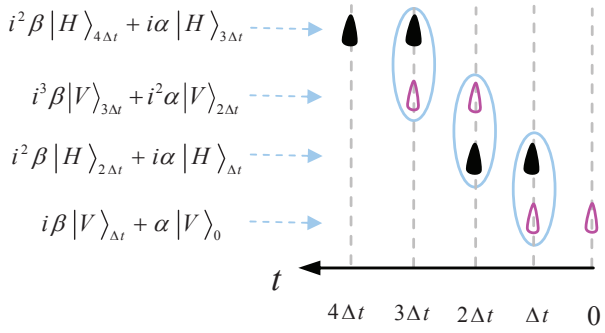

Fig. 2. Schematic representation for the reconstruction of the original state $|\psi\rangle_0 = \alpha|H\rangle + \beta|V\rangle$ from the state $|\phi\rangle_H$. The two wavepackets closed in an ellipse represent the fact that they will emerge at the PBS_3 at the same time and interfere with each other, which takes place with a success probability of 3/4.

Bob can also distill an uncorrupted state from the state $|\phi\rangle_V$ at the outport D_1 of the PBS_3, similar to the case from the state $|\phi\rangle_H$. In detail, the combination of the wave splitter and the decoder will complete the transformation on the state $|\phi\rangle_V$ as follows,

$$\begin{aligned} |\phi\rangle_V \to |\phi'\rangle_V &= \{\hat{\sigma_x}\alpha + i\hat{D}(\Delta t)[\hat{\sigma}_x\beta + \alpha] + i^2\hat{D}(2\Delta t)[\beta + \hat{\sigma}_x\alpha] \\ &\quad + i\hat{D}(3\Delta t)[i^2\hat{\sigma}_x\beta + \alpha] + i^2\hat{D}(4\Delta t)\beta\}|V\rangle_0. \end{aligned} \tag{12}$$

Bob can also get an uncorrupted state $|\psi\rangle_0$ from the outport D_1 at the time slots Δt, $2\Delta t$, and $3\Delta t$ with the unitary operations $\hat{\sigma}_x$, I, and $\hat{\sigma}_y$, respectively. That is,

$$\Delta t: \quad (\alpha + \hat{\sigma}_x\beta)|V\rangle = \alpha|V\rangle + \beta|H\rangle \xrightarrow{\hat{\sigma}_x} \alpha|H\rangle + \beta|V\rangle,$$

$$\begin{aligned} 2\Delta t &: (\hat{\sigma}_x\alpha+\beta)|V\rangle=\alpha|H\rangle+\beta|V\rangle \xrightarrow{I}\alpha|H\rangle+\beta|V\rangle, \\ 3\Delta t &: (\alpha+i^2\hat{\sigma}_x\beta)|V\rangle=\alpha|V\rangle-\beta|H\rangle \xrightarrow{\hat{\sigma}_y}\alpha|H\rangle+\beta|V\rangle. \end{aligned} \quad (13)$$

Here $-i\hat{\sigma}_y = |V\rangle\langle H| - |H\rangle\langle V|$. In this way, Bob can get the uncorrupted state $|\psi\rangle_0 = \alpha|H\rangle+\beta|V\rangle$ from the states $|\phi\rangle_H$ and $|\phi\rangle_V$ at the time slots Δt, $2\Delta t$, and $3\Delta t$. At the time slots 0 and $4\Delta t$, Bob will lose the useful information about the unknown state $|\psi\rangle_0 = \alpha|H\rangle+\beta|V\rangle$ as he can not distill the parameters α and β, which takes place with the probability 1/4.

We have discuss the principle that Bob distills an uncorrupted state from the state $|\psi\rangle_H$ shown in Eq. (2). The principle that Bob distills an uncorrupted state from the state $|\psi\rangle_V$ shown in Eq. (3) is similar to that from the state $|\psi\rangle_H$. The rotation by the noisy channel on the state $|\psi\rangle_V$ will transform it into the state $|\psi'\rangle_V$, i.e.,

$$\begin{aligned} |\psi\rangle_V \xrightarrow{noise} |\psi'\rangle_V &= \delta_2[i\alpha+\hat{D}(\Delta t)\beta]|H\rangle_{\Delta T}+\eta_2[i\alpha+\hat{D}(\Delta t)\beta]|V\rangle_{\Delta T} \\ &\equiv \delta_2|\Phi\rangle_H+\eta_2|\Phi\rangle_V. \end{aligned} \quad (14)$$

Here

$$\begin{aligned} |\Phi\rangle_H &= [i\alpha+\hat{D}(\Delta t)\beta]|H\rangle_{\Delta T}, \\ |\Phi\rangle_V &= [i\alpha+\hat{D}(\Delta t)\beta]|V\rangle_{\Delta T}. \end{aligned} \quad (15)$$

The combination of the wave splitter and the decoder will complete the transformation on the state $|\Phi\rangle_H$ as follows,

$$\begin{aligned} |\Phi\rangle_H \to |\Phi'\rangle_H &= \{i\hat{\sigma_x}\alpha+i^2\hat{D}(\Delta t)[-\hat{\sigma}_x\beta+\alpha]-i^3\hat{D}(2\Delta t)[\beta-\hat{\sigma}_x\alpha] \\ &\quad +i^2\hat{D}(3\Delta t)[\hat{\sigma}_x\beta+\alpha]+i\hat{D}(4\Delta t)\beta\}|H\rangle_{\Delta T}. \end{aligned} \quad (16)$$

Bob can get an uncorrupted state $|\psi\rangle_0$ from the outport D_2 at the time slots $\Delta T+\Delta t$, $\Delta T+2\Delta t$, and $\Delta T+3\Delta t$ with the unitary operations $\hat{\sigma}_z$, $\hat{\sigma}_y$, and I, respectively. That is,

$$\begin{aligned} \Delta T+\Delta t &: (\alpha-\hat{\sigma}_x\beta)|H\rangle=\alpha|H\rangle-\beta|V\rangle \xrightarrow{\hat{\sigma}_z}\alpha|H\rangle+\beta|V\rangle, \\ \Delta T+2\Delta t &: (\hat{\sigma}_x\alpha-\beta)|H\rangle=\alpha|V\rangle-\beta|H\rangle \xrightarrow{\hat{\sigma}_y}\alpha|H\rangle+\beta|V\rangle, \\ \Delta T+3\Delta t &: (\alpha+\hat{\sigma}_x\beta)|H\rangle=\alpha|H\rangle+\beta|V\rangle \xrightarrow{I}\alpha|H\rangle+\beta|V\rangle. \end{aligned} \quad (17)$$

With the same way, Bob can also distill an uncorrupted state from the wavepacket in the state $|\Phi\rangle_V$. In detail, the combination of the wave splitter and the decoder will complete the transformation on the state $|\Phi\rangle_V$ as follows,

$$\begin{aligned} |\Phi\rangle_V \to |\Phi'\rangle_V &= \{i\hat{\sigma_x}\alpha+i^2\hat{D}(\Delta t)[-\hat{\sigma}_x\beta+\alpha]-i^3\hat{D}(2\Delta t)[\beta-\hat{\sigma}_x\alpha] \\ &\quad +i^2\hat{D}(3\Delta t)[\hat{\sigma}_x\beta+\alpha]+i\hat{D}(4\Delta t)\beta\}|V\rangle_{\Delta T}. \end{aligned} \quad (18)$$

Bob can get an uncorrupted state $|\psi\rangle_0$ from the outport D_1 at the time slots $\Delta T+\Delta t$, $\Delta T+2\Delta t$, and $\Delta T+3\Delta t$ with the unitary operations $\hat{\sigma}_y$, $\hat{\sigma}_z$, and $\hat{\sigma}_x$, respectively. That is,

$$\begin{aligned} \Delta T+\Delta t &: (\alpha-\hat{\sigma}_x\beta)|V\rangle=\alpha|V\rangle-\beta|H\rangle \xrightarrow{\hat{\sigma}_y}\alpha|H\rangle+\beta|V\rangle, \\ \Delta T+2\Delta t &: (\hat{\sigma}_x\alpha-\beta)|V\rangle=\alpha|H\rangle-\beta|V\rangle \xrightarrow{\hat{\sigma}_z}\alpha|H\rangle+\beta|V\rangle, \\ \Delta T+3\Delta t &: (\alpha+\hat{\sigma}_x\beta)|V\rangle=\alpha|V\rangle+\beta|H\rangle \xrightarrow{\hat{\sigma}_x}\alpha|H\rangle+\beta|V\rangle. \end{aligned} \quad (19)$$

In this way, Bob can get the uncorrupted state $|\psi\rangle_0 = \alpha|H\rangle + \beta|V\rangle$ from the states $|\Phi\rangle_H$ and $|\Phi\rangle_V$ at the time slots $\Delta T + \Delta t$, $\Delta T + 2\Delta t$, and $\Delta T + 3\Delta t$, which takes place with the success probability 3/4.

In order to distinguish the uncorrupted state coming from the state $|\psi\rangle_H$ or $|\psi\rangle_V$ when the photon emits from the outports D_1 or D_2, ΔT should not be zero. That is, Bob should make the wavepackets from $|\psi\rangle_H$ and $|\psi\rangle_V$ attain the PBS_3 in different time slots and they do not interfere with each other. For simplification, Bob can choose $\Delta T = \frac{\Delta t}{2}$.

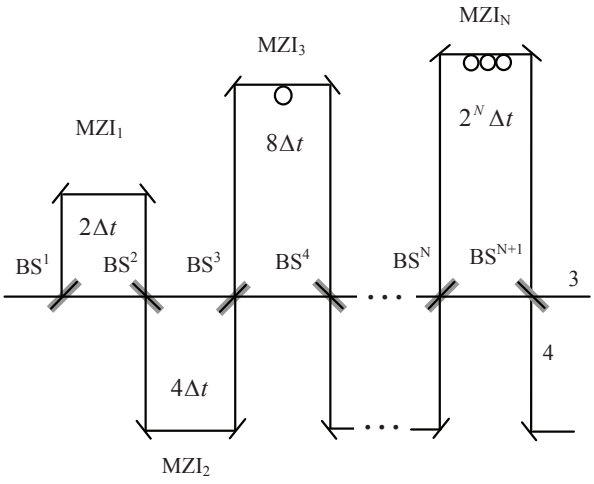

Fig. 3. A time-divisioned multiplexing for splitting a single qubit into 2^N wavepackets with N unbalanced MZIs.

From the discussion above, one can see that Bob can get an uncorrupted state with the success probability 75% if he exploits the wave splitter shown in Fig.1 to split the wave pockets of the single photon. Of course, Bob can improve the success probability by using a time-divisioned multiplexing [48, 49, 50] to split the single photon into more wavepackets, shown in Fig.3. In this time, the quantum operator $\hat{K}$ in Eq. (10) will be replaced with $\hat{K}'$. Here

$$\begin{aligned}
\hat{K}' \equiv \quad & \{ \quad a_0\hat{\sigma}_x\alpha \\
& + \quad i\sum_{m=0}^{2^{N-1}-1} a_{2m}\hat{D}[(2m+1)\Delta t](\alpha + \hat{\sigma}_x\beta) \\
& + \quad \sum_{m=1}^{2^{N-1}} \hat{D}(2m\Delta t)(a_{2m}\hat{\sigma}_x\alpha - a_{2m-2}\beta) \\
& - \quad i\sum_{m=2^{N-1}}^{2^N-1} a_{2m}\hat{D}[(2m+1)\Delta t](\alpha - \hat{\sigma}_x\beta) \\
& + \quad \sum_{m=2^{N-1}+1}^{2^N-1} \hat{D}(2m\Delta t)(a_{2m}\hat{\sigma}_x\alpha + a_{2m-2}\beta)
\end{aligned}$$

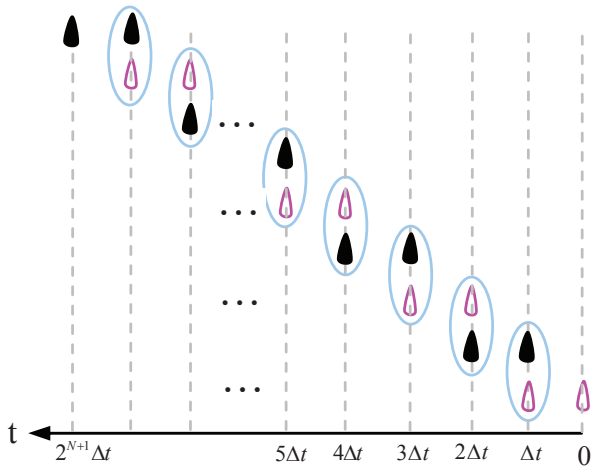

Fig. 4. Schematic representation for the reconstruction of the original state $|\psi\rangle_0 = \alpha|H\rangle + \beta|V\rangle$ with 2^{N+2} wavepackets. The success probability for obtaining an uncorrupted state is, in principle, improved to be $P_S = \frac{2^{N+1}-1}{2^{N+1}}$.

$$+ \quad a_{2^{N+1}-2}\hat{D}(2^{N+1}\Delta t)\beta\}, \tag{20}$$

where $a_j \in \{1, -1\}$ and can be determined when the number of MZIs in the wave splitter N is given. Also, Eq. (10) will be transformed into

$$|\phi\rangle_H \to |\phi''\rangle_H = \hat{K}' |H\rangle_0 . \tag{21}$$

With the same way as the case in which Bob chooses his wave splitter shown in Fig.1, Bob can distill an uncorrupted state $|\psi\rangle_0 = \alpha|H\rangle + \beta|V\rangle$ with the success probability $P_S = \frac{2^{N+1}-1}{2^{N+1}}$, shown in Fig.4. Moreover, this success probability is independent of the noise parameters δ_1, η_1, δ_2, and η_2.

3 discussion and summary

In a practical application in quantum communication (such as QKD), the qubit is measured immediately and no extra operations are required for recovering the original state as the receiver can judge the time when the qubit is detected and then he can compensate for the effect of the extra operations by flipping the measured bit value or not. That is, the present scheme is completely passive when it is used as a part of a QKD protocol. Of course, this is the main goal of the present scheme. Certainly, there are some other problems when the present scheme is used in a practical quantum cryptography. One is the effect of the channel losses and detection dark counts. The other is the requirement that the delays by Δt and $2\Delta t$ should be done accurately, which means that the two parties should possess some stable Mach-Zehnder interferometers. The present scheme will suffer from the channel losses and detection dark counts, the same as other faithful qubit transmission schemes [40, 41, 42, 43] and quantum communication protocols [2]. In fact, the detection dark counts will decease

the key-generation rate as its effect equals to lose a portion of the single photons transmitted over a noisy channel. This is a general problem in quantum communication. On the other hand, the channel losses has two effects. One is that it decreases the key-generation rate if the photon is lost before it arrives the side of the receiver. The other is that it will decrease the success probability of the present faithful qubit transmission scheme if only some wavepackets of the single photon are lost. In the present scheme, the wavepackets of a single photon is so close (not more than $\frac{3\Delta t}{2}$) that we can assume that the wavepackets are lost or not as a whole system. Under this assumption, the channel losses will decrease the key-generation rate only, not the success probability. At present, it is not easy for us to maintain the stabilization of a Mach-Zehnder interferometer for a long time with only linear optical elements such as PBSs and BSs. On one hand, this feature will improve the difficulty of the implementation of the present scheme in a practical application. On the other hand, the two parties in quantum communication can use some reference signals to analyze periodically the stability of the Mach-Zehnder interferometers and compensate the fluctuation with feedback. With the improvement of technology, the parties can also use some interferometers with optical integrations in chips to depress the fluctuation of time difference.

When the present scheme is used in some coherent quantum communication protocols in which the qubits are not measured immediately but stored, it does not work in a passive way. For example, if the present scheme is used to distribute an entangled photon pair for a quantum repeater (not for generating a key immediately in long-distance QKD), the two photons with a high fidelity will be stored for a period of time. At this time, the parties should exploit some kinds of non-destructive quantum measurements to detect the presence of the photons. It is not necessary for the two parties to perform extra operations for restoring the original state, just get the map of the correlation between the unitary operations and the measured bit values obtained later as they can also compensate for the effect of the extra operations by flipping the measured bit value or not in the end of quantum communication.

We have described a passively self-error-rejecting single-qubit transmission scheme over a collective-noise channel. Compared with the scheme proposed by Yamamoto *et al.* [40] for faithful qubit distribution assisted by one additional qubit and the scheme without additional qubit [42], the present scheme has some interesting features as follows: (1) The success probability for obtaining an uncorrupted state $P_S = \frac{2^{N+1}-1}{2^{N+1}}$ approaches 100% in principle if the number of wavepackets is large enough (when $N = 3$, $P_S = 93.75\%$), which is about eight times of that in the scheme introduced by Yamamoto *et al.* [40]. At the aspect of success probability, the present scheme is an optimal one. Of course, the bigger the number of the wavepackets, the more time slots that Bob should pay for reconstructing the original state, which maybe decrease the key-generation rate in quantum communication. (2) The present scheme does not require an additional qubit against a collective noise, just the single qubit itself, which makes the present scheme have some good applications in quantum communication. In detail, one can easily apply this scheme to almost all quantum communication protocols existing, such as the quantum cryptography protocols with single photons or entanglement [2]. (3) The present scheme requires only one quantum channel, not two or more [40, 42]. (4) This scheme does not require fast polarization modulators (Pockels cell) [43] when it is used in quantum cryptography, i.e., it works in a completely passive way for quantum cryptography with postselection. (5) It is easy to implement this scheme with some simple

optical devices in principle. (6) The success probability does not depend on the extent of the collective noise, i.e., it is independent of the noise parameters (δ_1, η_1, δ_2, and η_2), which is different from those in Refs.[40, 45]. As shown in Eq.(7) and Fig. 2, the wavepackets interfere with only those with the same parameter of collective noise, and the success probability for each part with the same noise parameter is $P_S = \frac{2^{N+1}-1}{2^{N+1}}$. This good feature makes the present scheme more efficient than other schemes [40, 42]. (7) As the single qubit transmitted is in an arbitrary state $|\psi\rangle_0 = \alpha|H\rangle + \beta|V\rangle$, the present scheme can also be used to accomplish the faithful transmission of one particle in an entangled quantum system as an entangled pure state $\alpha'|H\rangle_h|H\rangle_t + \beta'|V\rangle_h|V\rangle_t$ can be rewritten as $\alpha''|H\rangle_t + \beta'|V\rangle_t$ (here the subscript h and t represent the home particle and the traveling particle, respectively).

In summary, we have presented a passively self-error-rejecting single-qubit transmission scheme for polarization states of photons, which is immune to the collective noise in a quantum channel (such as an optical fiber). The success probability for obtaining an uncorrupted state, in principle, approaches 100% via postselection in different time bins with some Mach-Zehnder interferometers, independent of the parameters of collective noise, and the present scheme can be implemented with some simple optical devices and photon detectors in a completely passive way. The present scheme does not employ an entangled state in DFS, and it does not resort to additional qubits. One can directly apply this scheme to almost all quantum communication protocols against a collective noise, including the quantum cryptography protocols based on single photons [1, 2] and those based on entangled photon systems [3, 4, 5, 6].

Acknowledgements

This work is is supported by the National Natural Science Foundation of China under Grant Nos. 10974020 and 11174039, A Foundation for the Author of National Excellent Doctoral Dissertation of P. R. China under Grant No. 200723, the Beijing Natural Science Foundation under Grant No. 1082008, and the Fundamental Research Funds for the Central Universities.

References

1. C. H. Bennett and G. Brassard (1984), *Quantum cryptography: public key distribution and coin tossing*, in *Proceedings of IEEE international conference on computers, systems and signal Processing, Bangalore, India* (IEEE, New York), pp. 175-179.
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden (2002), *Quantum crytography*, Rev. Mod. Phys., **74**, pp. 145-195.
3. A. K. Ekert (1991), *Quantum cryptography based on Bells theorem*, Phys. Rev. Lett., **67**, pp. 661-663.
4. C. H. Bennett, G. Brassard, and N. D. Mermin (1992), *Quantum cryptography without Bells theorem*, Phys. Rev. Lett., **68**, pp. 557-559.
5. G. L. Long and X. S. Liu (2002), *Theoretically efficient high-capacity quantum-key-distribution scheme*, Phys. Rev. A, **65**, 032302.
6. F. G. Deng and G. L. Long (2003), *Controlled order rearrangement encryption for quantum key distribution*, Phys. Rev. A, **68**, 042315.
7. F. G. Deng and G. L. Long (2004), *Bidirectional quantum key distribution protocol with practical faint laser pulses*, Phys. Rev. A, **70**, 012311.
8. W. Y. Hwang (2003), *Quantum key distribution with high loss: toward global secure communication* Phys. Rev. Lett., **91**, 057901.
9. X. B. Wang (2005), *Beating the photon-number-splitting attack in practical quantum cryptography*,

Phys. Rev. Lett., **94**, 230503.
10. H. K. Lo, X. F. Ma, and K. Chen (2005), *Decoy state quantum key distribution*, Phys. Rev. Lett., **94**, 230504.
11. A. Acin, N. Gisin, and L. Masanes (2006), *From Bell's theorem to secure quantum key distribution*, Phys. Rev. Lett., **97**, 120405.
12. I. Ali-Khan, C. J. Broadbent, and J. C. Howell (2007), *Large-alphabet quantum key distribution using energy-time entangled bipartite states*, Phys. Rev. Lett., **98**, 060503.
13. Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto (2007), *Simple and efficient quantum key distribution with parametric down-conversion*, Phys. Rev. Lett., **99**, 180503.
14. L. J. Zhang, C. Silberhorn, and I. A. Walmsley (2008), *Secure quantum key distribution using continuous variables of single photons*, Phys. Rev. Lett., **100**, 110504.
15. V. Scarani and R. Renner (2008), *Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing*, Phys. Rev. Lett., **100**, 200501.
16. R. Garcia-Patron and N. J. Cerf (2009), *Continuous-variable quantum key distribution protocols over noisy channels*, Phys. Rev. Lett., **102**, 130501.
17. N. Gisin, S. Pironio, and N. Sangouard (2010), *Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier*, Phys. Rev. Lett., **105**, 070501.
18. H. K. Lo and H. F. Chau (1999), *Unconditional security of quantum key distribution over arbitrarily long distances*, Science, **283**, 2050.
19. P. W. Shor and J. Preskill (2000), *Simple proof of security of the BB84 quantum key distribution protocol*, Phys. Rev. Lett., **85**, pp. 441-444.
20. D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt (2007), *Long-distance decoy-state quantum key distribution in optical fiber*, Phys. Rev. Lett., **98**, 010503.
21. T. Schmitt-Manderbach, H. Weier, M. Frst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter (2007), *Experimental Demonstration of Free-space decoy-state quantum key distribution over 144 km*, Phys. Rev. Lett., **98**, 010504.
22. C. Z. Peng, J. Zhang, D. Yang, W. B. Gao, H. X. Ma, H. Yin, H. P. Zeng, T. Yang, X. B. Wang, and J. W. Pan (2007), *Experimental long-distance decoy-state quantum key distribution based on polarization encoding*, Phys. Rev. Lett., **98**, 010505.
23. Z. Q. Yin, Z. F. Han, W. Chen, F. X. Xu, Q. L. Wu, and G. C. Guo (2008), *Experimental decoy state quantum key distribution over 120km fibre*, Chin. Phys. Lett., **25**, pp. 3547-3550.
24. H. C. Lim, A. Yoshizawa, H. Tsuchida, and K. Kikuchi (2008), *Distribution of polarization-entangled photon-pairs produced via spontaneous parametric down-conversion within a local-area fiber network: Theoretical model and experiment*, Opt. Express, **16**, pp. 14512-14523.
25. T. Y. Chen, H. Liang, Y. Liu, W. Q. Cai, L. Ju, W. Y. Liu, J. Wang, H. Yin, K. Chen, Z. B. Chen, C. Z. Peng, and J. W. Pan (2009), *Field test of a practical secure communication network with decoy-state quantum cryptography*, Opt. Express, **17**, pp. 6540-6549.
26. W. Chen, Z. F. Han, T. Zhang, H. Wen, Z. Q. Yin, F. X. Xu, Q. L. Wu, Y. Liu, Y. Zhang, X. F. Mo, Y. Z. Gui, G. Wei, and G. C. Guo (2009), *Field experiment on a "star type" metropolitan quantum key distribution network*, IEEE Photonics Tech. Lett., **21**, pp. 575-577.
27. T. Y. Chen, J. A. Wang, H. Liang, W. Y. Liu, Y. Liu, X. A. Jiang, Y. A. Wang, X. Wan, W. Q. Cai, L. Ju, L. K. Chen, L. J. Wang, Y. A. Gao, K. Chen, C. Z. Peng, Z. B. Chen, and J. W. Pan (2010), *Metropolitan all-pass and inter-city quantum communication network*, Opt. Express, **18**, pp. 27217-27225.
28. W. J. Munro, K. A. Harrison, A. M. Stephens, S. J. Devitt, and K. Nemoto (2010), *From quantum multiplexing to high-performance quantum networking*, Nature Photonics, **4**, pp. 792-796.
29. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T.

Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legre, S. Robyr, P. Trinkler, L. Monat, J. B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Langer, M. Peev, and A. Zeilinger (2011), *Field test of quantum key distribution in the Tokyo QKD Network*, Opt. Express, **19**, pp. 10387-10409.

30. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin (1997), *"Plug and play" systems for quantum cryptography*, Appl. Phys. Lett., **70**, pp. 793-795.
31. G. Ribordy, J. D. Gautier, N. Gisin, O. Guinnard, and H. Zbindn (1998), *Automated 'plug & play' quantum key distribution*, Electron. Lett., **34**, pp. 2116-2117.
32. C. Zhou, G. Wu, X. Chen, and H. Zeng (2003), *"Plug and play" quantum key distribution system with differential phase shift*, Appl. Phys. Lett., **83**, pp. 1692-1694.
33. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy (2006), *Trojan-horse attacks on quantum-key-distribution systems*, Phys. Rev. A, **73**, 022320.
34. Z. D. Walton, A. F. Abouraddy, A. V. Sergienko, B. E. A. Saleh, and M. C. Teich (2003), *Decoherence-free subspaces in quantum key distribution*, Phys. Rev. Lett., **91**, 087901.
35. J. C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens (2004), *Robust polarization-based quantum key distribution over a collective-noise channel*, Phys. Rev. Lett., **92**, 017901.
36. J. C. Boileau, R. Laflamme, M. Laforest, and C. R. Myers (2004), *Robust quantum communication using a polarization-entangled photon pair*, Phys. Rev. Lett., **93**, 220501.
37. X. H. Li, F. G. Deng, and H. Y. Zhou (2008), *Efficient quantum key distribution over a collective noise channel*, Phys. Rev. A, **78**, 022321.
38. M. A. Nielsen and I. L. Chuang (2000), *Quantum computation and quantum Information*, Cambridge Univ. Press, (Cambridge, UK).
39. F. G. Deng (2011), *One-step error correction for multipartite polarization entanglement*, Phys. Rev. A, **83**, 062316.
40. T. Yamamoto, J. Shimamura, S. K. Özdemir, M. Koashi, and N. Imoto (2005), *Faithful qubit distribution assisted by one additional qubit against collective noise*, Phys. Rev. Lett., **95**, 040503.
41. X. H. Li, B. K. Zhao, Y. B. Sheng, F. G. Deng, and H. Y. Zhou (2009), *Efficient faithful qubit transmission with frequency degree of freedom*, Opt. Commun., **282**, 4025.
42. X. H. Li, F. G. Deng, and H. Y. Zhou (2007), *Faithful qubit transmission against collective noise without ancillary qubits*, Appl. Phys. Lett., **91**, 144101.
43. D. Kalamidas (2005), *Single-photon quantum error rejection and correction with linear optics*, Phys. Lett. A, **343**, pp. 331-335.
44. G. M. Palma, K. A. Suominen, and A. K. Ekert (1996), *Quantum computers and dissipation*, Proc. R. Soc. London A, **452**, pp. 567-584.
45. X. B. Wang (2005), *Fault tolerant quantum key distribution protocol with collective random unitary noise*, Phys. Rev. A, **72**, 050304(R).
46. D. B. de Brito and R. V. Ramos (2006), *Passive quantum error correction with linear optics*, Phys. Lett. A, **352**, pp. 206-209 .
47. X. B. Wang (2004), *Quantum error-rejection code with spontaneous parametric down-conversion*, Phys. Rev. A, **69**, 022320.
48. M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson (2003), *Photon-number resolution using time-multiplexed single-photon detectors*, Phys. Rev. A, **68**, 043814.
49. D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, I. A. Walmsley, M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson (2004), *Photon-number-resolving detection using time-multiplexing*, J. Mod. Opt., **51**, pp. 1499-1515.
50. K. Laiho, M. Avenhaus, K. N. Cassemiro, and C. Silberhorn (2009), *Direct probing of the Wigner function by time-multiplexed detection of photon statistics*, New J. Phys., **11**, 043012.