Study on the security of discrete-variable quantum key distribution over non-Markovian channels

2012 J. Phys. B: At. Mol. Opt. Phys. 45 135501

(http://iopscience.iop.org/0953-4075/45/13/135501)

J. Phys. B: At. Mol. Opt. Phys. **45** (2012) 135501 (6pp) doi:10.1088/0953-4075/45/13/135501

Study on the security of discrete-variable quantum key distribution over non-Markovian channels

Peng Huang, Jun Zhu, Guangqiang He and Guihua Zeng

State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200240, People's Republic of China

E-mail: peakeagle1985@hotmail.com

Received 10 February 2012, in final form 4 May 2012
Published 30 May 2012
Online at stacks.iop.org/JPhysB/45/135501

Abstract
The dynamic of the secret key rate of the discrete-variable quantum key distribution (QKD) protocol over the non-Markovian quantum channel is investigated. In particular, we calculate the secret key rate for the six-state protocol over non-Markovian depolarizing channels with coloured noise and Markovian depolarizing channels with Gaussian white noise, respectively. We find that the secure secret key rate for the non-Markovian depolarizing channel will be larger than the Markovian one under the same conditions even when their upper bounds of tolerable quantum bit error rate are equal. This indicates that this coloured noise in the non-Markovian depolarizing channel can enhance the security of communication. Moreover, we show that the secret key rate fluctuates near the secure point when the coupling strength of the system with the environment is high. The results demonstrate that the non-Markovian effects of the transmission channel can have a positive impact on the security of discrete-variable QKD.

(Some figures may appear in colour only in the online journal)

1. Introduction

Quantum key distribution (QKD) [1–7] provides a novel way to allow two distant authorized parties, the sender Alice and the receiver Bob, to remotely establish a secret key through quantum and classical channels. Generally, the classical channel needs to be authenticated, i.e. the legitimated parties identify themselves and a third party may listen to the communication but cannot participate in it. However, the quantum channel is open so that the third party can manipulate the communication. The security of QKD originates from the fundamental principles of quantum mechanics. More precisely, the legitimated parties can estimate the security after communication, since the leakage of information in a quantum channel to eavesdropper, Eve, is quantitatively related to the degradation of communication [3].

The unconditional security of QKD schemes with the ideal system [8, 9] and practical system [10] has been proved for several years. However, the ignorance of imperfection of the practical QKD system still exists and limits Eve's attack strategy. So the unconditional security should be reconsidered under more powerful attacks introduced by Eve. To avoid the leakage of information from the loopholes of the imperfect practical QKD system, many potential attacks [11–20] have been proposed recently. The known considerations of the imperfection of the practical QKD system are focused on the practical system devices, and the quantum channels are usually approximately considered to be Markovian, i.e. the correlation time between the system and environment is infinitely short so that the memory effects can be neglected. In practice, the correlations between the system and environment exist for a small finite period of time, which leads to the quantum channel with memory [21]. In recent years, non-Markovian effects have been investigated in the dynamics of entanglement [22–24], quantum correlation [25], quantum channel capacity [26] and the security of continuous-variable QKD [27]. Moreover, the optical non-Markovian signatures in semiconductor quantum wires have been achieved in an

experiment [28]. Interestingly, it is shown in [27] that the non-Markovian effects may be exploited to enhance the security of continuous-variable QKD and detect eavesdropping along the transmission line. However, the security analysis is addressed in Gaussian individual attacks, whereas Eve's collective attacks are not being considered.

In this paper, we explore the security of discrete-variable QKD schemes over non-Markovian quantum channels. In particular, we investigate the dynamics of the secret key rates for the six-state protocol [29, 30] by restricting consideration to collective attacks, where the transmission quantum channels are specified as non-Markovian depolarizing channels with coloured noise and the Markovian one with Gaussian white noise [21]. In contrast, we show that the secure secret key rate for the non-Markovian channels may always be larger than the Markovian ones. Moreover, we find that the nosier the channels are, the more effectively the non-Markovian effects will enhance the security of transmission. When the coupling strength of the system with the environment is high enough, the secret key rate fluctuates near the secure point.

This paper is organized as follows. In section 2, we introduce the physical model we will investigate and construct the non-Markovian depolarizing quantum channel with coloured noise. We then briefly introduce the six-state protocol, and calculate and analyse contrastively the dynamics of the secret key rates and quantum bit error rate (QBER) of the six-state protocol under collective attack for the non-Markovian and Markovian depolarizing channels in section 3. Finally, the conclusions are drawn in section 4.

2. The non-Markovian depolarizing channel with coloured noise

In this section, we introduce the physical model under study, i.e. the non-Markovian depolarizing channel with coloured noise. As known, the evolution of the quantum system can be described as a completely positive map (CPM) [31]. A known depolarizing quantum channel can be expressed as the CPM $\mathcal{N}(\rho) = (1-p)\rho + (p/3)(\sigma_1\rho\sigma_1 + \sigma_2\rho\sigma_2 + \sigma_3\rho\sigma_3)$, where $0 \leqslant p \leqslant 1$, and σ_i for $i = 1, 2, 3$ are Pauli operators. This CPM defines a depolarizing channel with white noise, which comes from the Markovian master equation. However, the Markovian master equation that describes the time evolution of the quantum system is an approximation, since the correlation time between the quantum system and environment is seen to be infinitely short so that the memory effects can be neglected. In practice, the correlation time is a small finite period of time, which leads to the non-Markovian master equation. In the following, we review the derivation of the depolarizing channel with coloured noise [21].

A prevailing memory kernel master equation can be described by

$$\dot{\rho} = K\mathcal{L}\rho, \tag{1}$$

where K is an integral operator that depends on time acting as the form $K\mathcal{N} = \int_0^t k(t-t')\mathcal{N}(t')\mathrm{d}t'$, $\mathcal{L}$ is a Lindblad superoperator describing the dynamics due to the interaction of the system and environment and ρ is the density operator of the small system of interest. The solution to the master equation (1) defines a completely positive and trace-preserving linear map $\mathcal{N}_t : \rho \to \rho_t$ that describes the evolution of a system coupled to an environment.

A master equation of the form of equation (1) arises when considering any two-level quantum system that interacts with an environment possessing random telegraph signal noise. It is possible to write a time-dependent Hamiltonian for this kind of system,

$$H(t) = \hbar \sum_{i=1}^{3} \Gamma_i(t)\sigma_i, \tag{2}$$

where $\Gamma_i(t)$ are independent random variables. Each random variable can be defined as $\Gamma_i(t) = a_i n_i(t)$. The random variable $n_i(t)$ has a Poisson distribution with a mean equal to $t/2\tau_i$, while a_i is an independent coin-flip random variable assuming the values $\pm a_i$. A model like this describes, for instance, a spin-1/2 particle in the presence of three orthogonal magnetic fields, each of which has a constant magnitude a_i and inverts randomly in time with a distribution given by n_i.

By using the von Neumann equation $\dot{\rho} = -(\mathrm{i}/\hbar)[H, \rho] = -\mathrm{i}\sum_k(t)[\sigma_k, \rho]$, one can obtain the solution for the density operator of the form

$$\rho(t) = \rho(0) - \mathrm{i}\int_0^t \sum_k \Gamma_k(s)[\sigma_k, \rho(s)]\,\mathrm{d}s. \tag{3}$$

Applying the correlation functions of the random telegraph signal $\langle\Gamma_j(t)\Gamma_k(t')\rangle = a_k^2 e^{-|t-t'|/\tau_k}\delta_{jk}$, and substituting equation (3) back into the von Neumann equation and performing a stochastic average, one obtains the memory kernel master equation

$$\dot{\rho}(t) = -\int_0^t \sum_k \mathrm{e}^{-(t-t')/\tau_k} a_k^2[\sigma_k, [\sigma_k, \rho(t')]]\,\mathrm{d}t'. \tag{4}$$

It can be seen from equation (4) that the state of the system at time t depends on its past history. It is known that the Fourier transform of the correlation function gives the power spectrum of the environment. For white noise, the delta-function correlation in time leads to a flat power spectrum for the environment, and the system is equally coupled to all frequencies of environment, while for the coloured noise, the system prefers certain frequencies and a gives the coupling strength of the system with environment while τ determines the most preferred frequencies.

By assuming that the fluctuations τ_i are equal, one can obtain the solution to equation (4) as a linear map $\mathcal{N}_t : \rho \to \rho_t$ on $\mathcal{M}_2$ [21]. This map is a generalization of the depolarizing channel to the case of coloured noise, which can be written in the form of Kraus decomposition $\mathcal{N}_t(\rho) = \sum_k A_k^\dagger \rho A_k$ with Kraus operators given by $A_1 = \sqrt{\xi_1(\nu)}\sigma_1$, $A_2 = \sqrt{\xi_2(\nu)}\sigma_2$, $A_3 = \sqrt{\xi_3(\nu)}\sigma_3$ and $A_4 = \sqrt{\xi_4(\nu)}I$, provided that the following conditions are all satisfied:

$$\begin{aligned}
\xi_1 &= \tfrac{1}{4}(1 + \Lambda_1 - \Lambda_2 - \Lambda_3),\\
\xi_2 &= \tfrac{1}{4}(1 - \Lambda_1 + \Lambda_2 - \Lambda_3),\\
\xi_3 &= \tfrac{1}{4}(1 - \Lambda_1 - \Lambda_2 + \Lambda_3),\\
\xi_4 &= \tfrac{1}{4}(1 + \Lambda_1 + \Lambda_2 + \Lambda_3),
\end{aligned} \tag{5}$$

where $\nu = t/2\tau$ is the dimensionless time and $\Lambda_i(\nu) = e^{-\nu}[\cos(\mu_i\nu) + \sin(\mu_i\nu))/\mu_i]$ are damped harmonic oscillators having frequencies $\mu_i = \sqrt{(4\kappa_i\tau_i)^2 - 1}$ with $\kappa_i^2 = a_j^2 + a_k^2$ for $i \neq j \neq k$. The restrictions in equation (5) assure that the linear map $\mathcal{N}_t$ is completely positive. By assuming $\tau \to 0$ and $a \to \infty$, the random telegraph signal reduces to a Gaussian white noise and equation (4) becomes $\dot{\rho}(t) = -\int_0^t \delta(t-t')\sum_k 2a_k^2\tau[\sigma_k, [\sigma_k, \rho(t')]]\,dt'$. This leads to $\Lambda_i(t) = e^{-\gamma_i t}$ in equation (5) with inverse lifetimes $\gamma_i = 4\kappa_i^2\tau$. It should be pointed out that, whether in the case of coloured noise or white noise, there are examples of maps that are positive but not completely [32–34]. The map is completely positive if and only if the linear combinations in equation (5) are non-negative.

3. Unconditional security of the six-state protocol over a non-Markovian depolarizing channel

The six-state protocol is similar to the well-known BB84 four-state protocol, but with an additional basis [29, 30]. In the six-state protocol, Alice first generates a random bit $k = -1, 1$ and chooses one basis Θ randomly out of the three bases X, Y and Z. Then Alice prepares and sends over a quantum channel a qubit with the $|\Theta_k\rangle$ state, which is the eigenstate of the Θ basis with the eigenvalue of $k/2$. Bob randomly chooses one basis out of the three bases and measures the states along the chosen direction. Alice and Bob compare the bases they used via a public channel, and keep the bit value if the bases match; otherwise they discard it. Lastly, Alice and Bob repeat the above steps and apply bit error correction and privacy amplification to obtain a shared key string.

The unconditional security bounds for the six-state protocol [30] have been found in [35, 36] for the case where the quantum signals are single qubits. As usual, the proof for this prepare-and-measure (P&M) six-state scheme can be performed by an entanglement-based (EB) scheme: Alice produces the state $|\Phi^+\rangle_{AB} = (1/\sqrt{2})(|00\rangle_{AB} + |11\rangle_{AB})$; then she keeps the first qubit and sends the other one to Bob. This state shows perfectly correlated outcomes in the X and Z bases and perfectly anti-correlated outcomes in the Y basis. Bob may flip his results when he measures with Y basis. Without loss of generality, the symmetry of the six-state protocol implies that one can compute the unconditional security bound by restricting the consideration to collective attacks, and even further, to those cases such that the final state of Alice and Bob is Bell diagonal [3, 35, 36],

$$\rho_{AB} = \lambda_1|\Phi^+\rangle\langle\Phi^+| + \lambda_2|\Phi^-\rangle\langle\Phi^-| + \lambda_3|\Psi^+\rangle\langle\Psi^+| + \lambda_4|\Psi^-\rangle\langle\Psi^-|, \tag{6}$$

where $\sum_i \lambda_i = 1$ and $|\Phi^\pm\rangle_{AB} = (1/\sqrt{2})(|00\rangle_{AB} \pm |11\rangle_{AB})$, $|\Psi^\pm\rangle_{AB} = (1/\sqrt{2})(|01\rangle_{AB} \pm |10\rangle_{AB})$. It should be emphasized that the restriction for calculating the unconditional security bound does not depend on the type of the quantum channel, i.e. whether the quantum channel is with or without quantum memory, the restriction is feasible. In particular, λ_i acts as a function of time for the quantum channel with memory. It can be seen that $|\Phi^\pm\rangle$ give perfect correlation in the Z basis, $|\Phi^+\rangle$, $|\Psi^+\rangle$ give perfect correlation in the X basis, and $|\Phi^+\rangle$, $|\Psi^-\rangle$ show perfect correlation in the Y basis. Thus, the QBER for the three bases are given by

$$\begin{aligned} \varepsilon_x &= \lambda_2 + \lambda_4, \\ \varepsilon_y &= \lambda_2 + \lambda_3, \\ \varepsilon_z &= \lambda_3 + \lambda_4. \end{aligned} \tag{7}$$

Eve's information I_E is given by the Holevo bound

$$I_E = S(\rho_E) - \sum_a p(a)S(\rho_{E|a}), \tag{8}$$

where S is von Neumann entropy, a is a symbol of Alice's classical alphabet distributed with probability $p(a)$, $\rho_E = \sum_a p(a)\rho_{E|a}$ is Eve's partial state, with $\rho_{E|a}$ being the corresponding state of Eve's ancilla state. Eve can purify the state of ρ_{AB} such that $S(\rho_E) = S(\rho_{AB}) = H(\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\})$, and the bit a values 0 or 1 equiprobably in this attack. So we obtain

$$I_E = H(\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}) - \tfrac{1}{2}S(\rho_{E|0}) - \tfrac{1}{2}S(\rho_{E|1}). \tag{9}$$

The detailed computation of $\rho_{E|b}$ [2] shows that $S(\rho_{E|0}) = S(\rho_{E|1}) = h(\varepsilon_z)$, where h is binary entropy. For the six-state protocol, all the error rates are measured, and equation (9) can be rewritten as

$$I_E = \varepsilon_z h\left(\frac{1 + (\varepsilon_x - \varepsilon_y)/\varepsilon_z}{2}\right) + (1 - \varepsilon_z) \times h\left(\frac{1 - (\varepsilon_x + \varepsilon_y + \varepsilon_z)/2}{1 - \varepsilon_z}\right). \tag{10}$$

Now we calculate the evolution of the transmission state over the non-Markovian depolarizing channel with coloured noise. Having derived the Kraus operators of the depolarizing channel with coloured noise, the evolution of the state ρ_{AB} with the second qubit interacting with environment can be written as

$$\mathcal{N}_t(\rho_{AB}) = \sum_k I^{(A)} \otimes A_k^{(B)} \rho_{AB} A_k^{(B)\dagger} \otimes I^{(A)\dagger}. \tag{11}$$

For the case of the non-Markovian depolarizing channel with coloured noise, the error rates can be calculated as

$$\begin{aligned} \varepsilon_x(\nu) &= \tfrac{1}{2}[1 - \Lambda_1(\nu)], \\ \varepsilon_y(\nu) &= \tfrac{1}{2}[1 - \Lambda_2(\nu)], \\ \varepsilon_z(\nu) &= \tfrac{1}{2}[1 - \Lambda_3(\nu)], \end{aligned} \tag{12}$$

where $\Lambda_i(\nu) = e^{-\nu}[\cos(\mu_i\nu) + \sin(\mu_i\nu))/\mu_i]$. Now we consider the dynamics of the secret key rates for the non-Markovian case of state evolution. Under the assumption of depolarizing channels, i.e. $\varepsilon_x(\nu) = \varepsilon_y(\nu) = \varepsilon_z(\nu) = Q(\nu)$; hence $a_1 = a_2 = a_3$, the secret key rates for the non-Markovian case can be derived as

$$r^N(\nu) = 1 - Q(\nu) - h[Q(\nu)] - [1 - Q(\nu)] \times h\left[\frac{1 - 3Q(\nu)/2}{1 - Q(\nu)}\right], \tag{13}$$

while for the case of the Markovian depolarizing channel with Gaussian white noise, $\Lambda_i(\nu)$ in error rates should be valued as $e^{-\gamma_i t}$, and hence, $Q(t) = \frac{1}{2}[1 - e^{-\gamma_i t}]$. The secret key rate for the case of the Markovian channel is denoted as $r^M(t)$. It should be pointed out that the secret key rate here is derived under

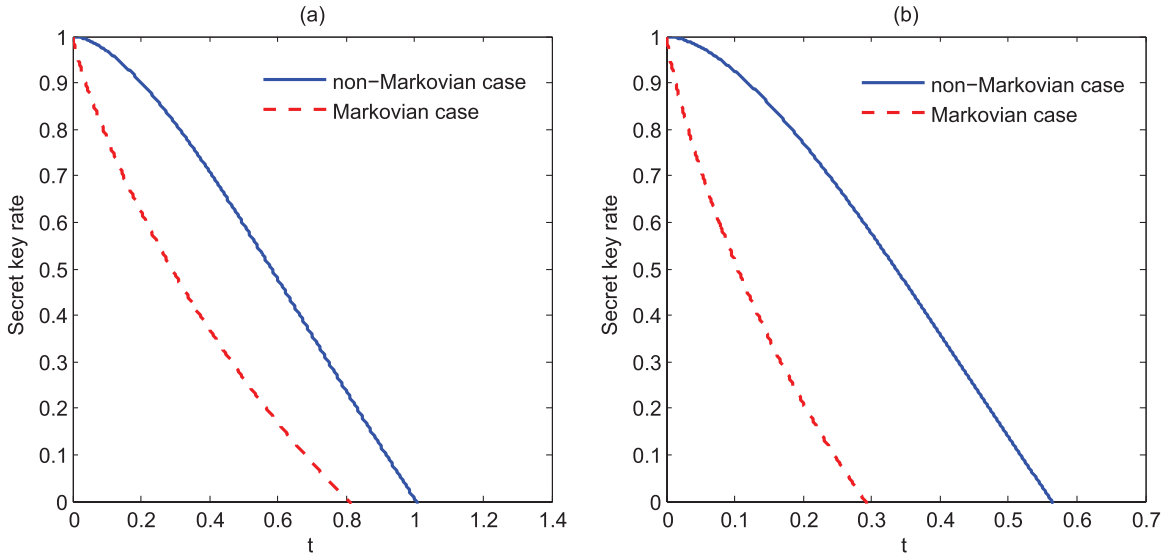

Figure 1. The comparison of the dynamics of secret key rates of the six-state protocol over the non-Markovian and Markovian depolarizing quantum channels under the conditions (a) $\tau = 1$, $|a_1| = |a_2| = |a_3| = 0.3$ and (b) $\tau = 1$, $|a_1| = |a_2| = |a_3| = 0.5$. The blue solid and red dashed curves correspond, respectively, to the secure secret key rate in the case of non-Markovian and Markovian depolarizing channels.

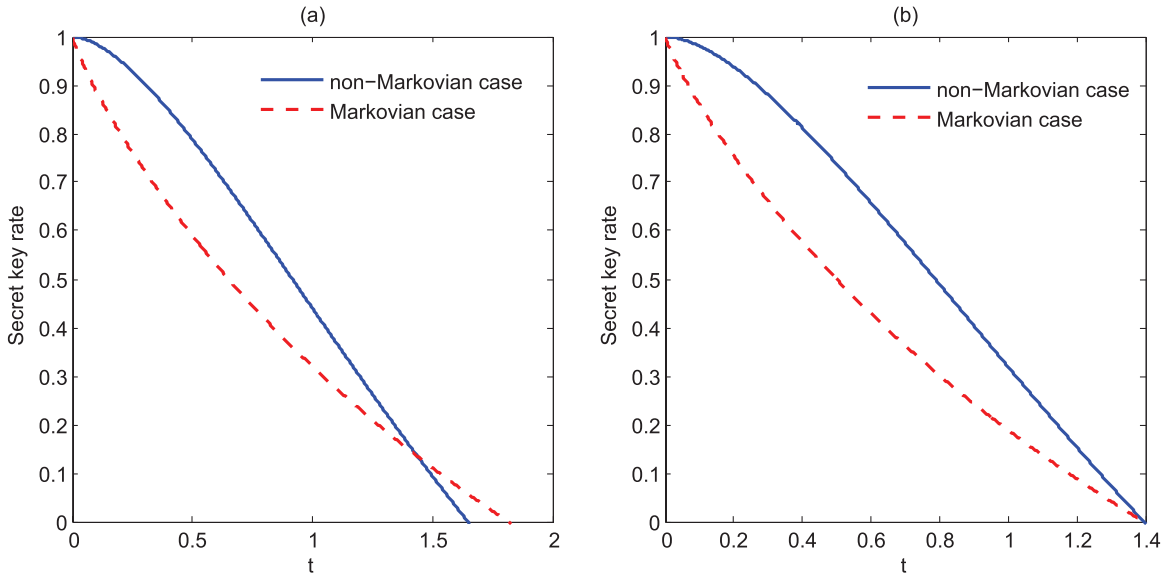

Figure 2. The comparison of the dynamics of secret key rates of the six-state protocol over the non-Markovian and Markovian depolarizing quantum channels under the conditions (a) $\tau = 1$, $|a_1| = |a_2| = |a_3| = 0.2$ and (b) $\tau = 1$, $|a_1| = |a_2| = |a_3| = |a^*|$. The blue solid and red dashed curves correspond, respectively, to the secure secret key rate in the case of the non-Markovian and Markovian depolarizing channels.

the assumption of one-way post-processing, no pre-processing and perfect error correction.

In what follows, we check whether the non-Markovian quantum channel can exhibit higher security of transmission of classical information under the same conditions. In figure 1, we plot the dynamics of the secret key rates for the cases of non-Markovian and Markovian depolarizing quantum channels under the same conditions for some different parameters $|a_i|$. It can be seen that the secure secret key rate for the non-Markovian case is larger than the Markovian case. Also, the difference between the two cases is much clearer for the more noisy channel, since the secure secret key rate for the Markovian channel is more sensitive to the increase in noise. However, when the coupling strength of the system with the external system, which can be measured by the parameters $|a_i|$, becomes small, the secure secret key rate for the non-Markovian case will not always be larger than the Markovian case. By setting $\tau = 1$, we find $r^N(v) \geqslant r^M(t)$ always exists for secure communication in the regime of $0.2282 \leqslant |a_i| \leqslant |a^*|$, where $|a^*| = \sqrt{[(\pi/\ln 3)^2 + 1]/32}$, is the upper bound to keep the linear map $\mathcal{N}_t$ completely positive for all times. Figure 2 presents the case that the secure secret key rate for the Markovian depolarizing channel may be larger than the non-Markovian one for some time when $|a_i| \leqslant |a^*|$.

It should be mentioned that the time parameter t denotes the duration of the processing of the quantum channel. Thus,

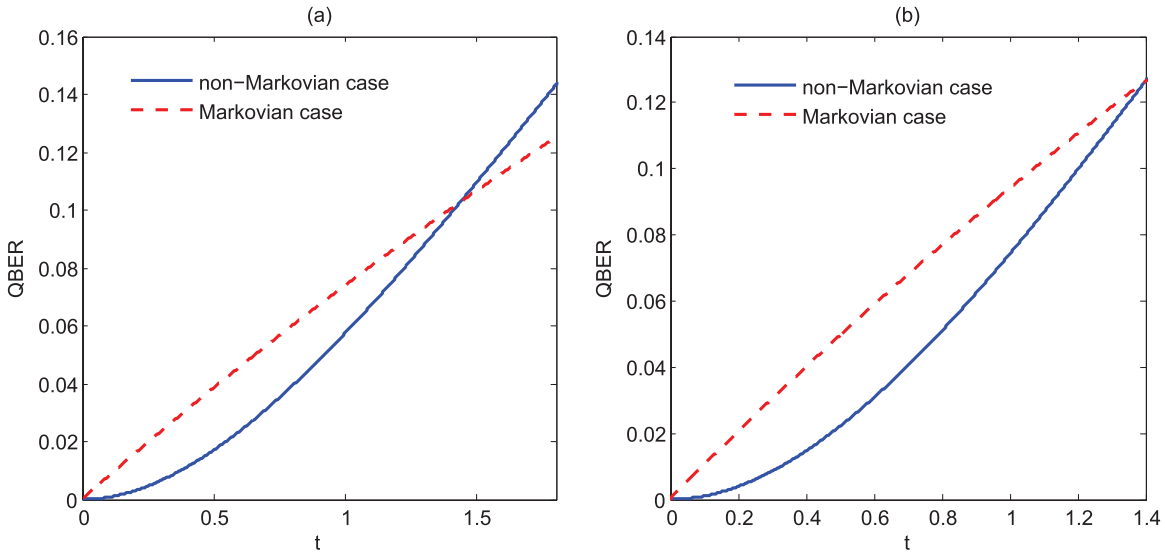

Figure 3. The comparison of the dynamics of QBER for the six-state protocol over the non-Markovian and Markovian depolarizing quantum channels under the conditions (a) $\tau = 1$, $|a_1| = |a_2| = |a_3| = 0.2$ and (b) $\tau = 1$, $|a_1| = |a_2| = |a_3| = |a^*|$. The blue solid and red dashed curves correspond, respectively, to the QBER in the case of the non-Markovian and Markovian depolarizing channels.

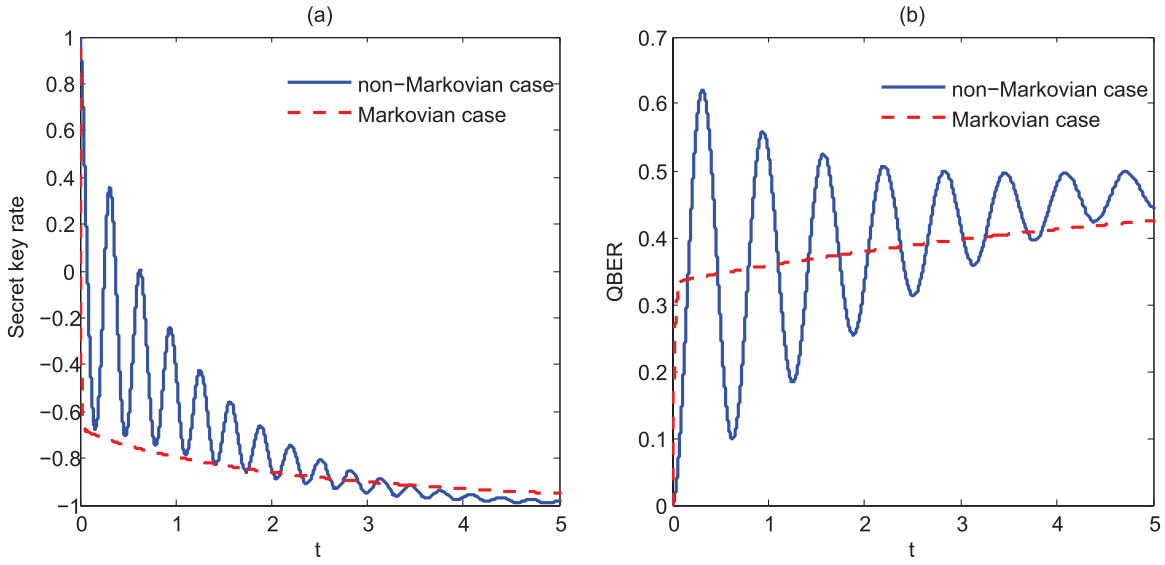

Figure 4. The comparison of the dynamics of (a) secret key rate, (b) QBER, for the six-state protocol over the non-Markovian and Markovian depolarizing quantum channels under the conditions $\tau = 1$, $|a_1| = |a_2| = 0.2$, $|a_3| = 5$. The blue solid and red dashed curves correspond, respectively, to the QBER in the case of the non-Markovian and Markovian depolarizing channels.

to guarantee the absolutely secure communication, one should limit the processing time of the quantum channel. Actually, the control of the processing time corresponds to the restriction of the QBER, and the unconditional security bounds of the QBER for the non-Markovian and Markovian depolarizing channels are equal to 12.61%. However, the dynamics of the QBER for the non-Markovian and Markovian depolarizing channels are different. Correspondingly, we find that the QBER for the Markovian case is always larger than the non-Markovian case under the same conditions in the regime $0.2282 \leqslant |a_i| \leqslant |a^*|$ when setting $\tau = 1$. Figure 3 shows the dynamics of the QBER for two different parameters $|a_i|$.

Now we extend to the generalized depolarizing channel. Assuming the coupling strengths of the system with the external system in three directions are different, i.e. a_i for $i = 1, 2, 3$ are not equal, the restriction $|a_i| \leqslant |a^*|$ to keep $\mathcal{N}_t$ completely positive for all times can be broken. We find that the secret key rate will fluctuate near the secure point along time when the coupling strength of the system with the environment is high enough. This effect originates from the convergent oscillation of the QBER in the case of the non-Markovian depolarizing channel, which has not been found in the case of the Markovian channel. Figure 4 shows this effect when setting a high coupling strength in one direction. Since the secret key rate is positive in only some ranges of time, one application is that the legitimate parties can guarantee security communication by controlling the processing time of the non-Markovian quantum channel. It should be noted that

the non-Markovian effects of the constructed quantum channel act along the quantum signals passing through the quantum channel. Moreover, it can be seen from the physical model that the former transmission of the quantum state will not affect the next transmission, i.e. the correlations between the subsequent quantum signals do not exist in this model.

Our results for the non-Markovian channel have shown something very different from the Markovian case. The non-Markovian channel has a better performance than the Markovian one to resist the leakage of information with the increasing of noise. Actually, the non-Markovian effects can be useful to enhance the security of quantum communication. This advantage originates from the small period of correlation time between the system and environment of the non-Markovian channel, which leads to a smaller QBER in transmission than the Markovian channel. Therefore, we can combine the application of the non-Markovian and Markovian quantum channel to achieve optimally secure QKD.

4. Summary and conclusions

We have investigated the dynamics of the secret key rate of the discrete-variable QKD protocol over the quantum channel with non-Markovian effects. In particular, we have introduced the physical model of the non-Markovian depolarizing channel with coloured noise, and calculated the secret key rate for the six-state protocol over non-Markovian and Markovian quantum channels under the same conditions. Moreover, we numerically compare the performances of the information transmissions over these two types of quantum channels. We find that the secure secret key rate will always be larger for non-Markovian channels than Markovian ones when the coupling strength of the system with the environment is strong enough. In particular, we obtain the lower bound of the coupling strength a_i when the parameter τ is specified as $\tau = 1$. It should be mentioned that we focus on the study of the value of the secure secret key rate as the function of processing time of the quantum channel. In practice, the transmission distance for secure QKD is also an important parameter, which is directly related to the transmission speeds of the quantum states over the Markovian and non-Markovian channels. However, the secure transmission distances over the Markovian and non-Markovian channels are out of our discussions.

Since the upper bounds of tolerable QBER for secure QKD are equal over the non-Markovian and Markovian depolarizing channels, we demonstrate that the better performance of the non-Markovian depolarizing quantum channel for the six-state protocol originates from the different dynamics of QBER. Furthermore, we consider the generalized non-Markovian depolarizing channel and show that the secret key rate will fluctuate near the secure point when the coupling strength of the system with the environment is high. This indicates that the coloured noise in the non-Markovian quantum channels can enhance the security of communication. The results demonstrate that the non-Markovian effects of the transmission channel can have a positive impact on the security of discrete-variable QKD.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (grant nos 61 102 053, 61 170 228, 60 970 109 and 60 801 051).

References

[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* pp 175–9
[2] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95
[3] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[4] Wang X-B 2005 *Phys. Rev.* A **72** 012322
[5] Wang X-B 2007 *Phys. Rev.* A **75** 052301
[6] Cai Q-Y and Tan Y-G 2006 *Phys. Rev.* A **73** 032305
[7] Shen Y, Peng X, Yang J and Guo H 2011 *Phys. Rev.* A **83** 052304
[8] Lo H-K and Chau H F 1999 *Science* **283** 2050
[9] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[10] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 *Quantum Inf. Comput.* **4** 325–60
[11] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691
[12] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320
[13] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev.* A **74** 022313
[14] Lamas-Linares A and Kurtsiefer C 2007 *Opt. Express* **15** 9388
[15] Fung C-H F, Qi B, Tamaki K and Lo H-K 2007 *Phys. Rev.* A **75** 032314
[16] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 042333
[17] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nature Photon.* **4** 686
[18] Xu F, Qi B and Lo H-K 2010 *New J. Phys.* **12** 113026
[19] Sun S H, Jiang M S and Liang L M 2011 *Phys. Rev.* A **83** 062331
[20] Liu W T, Sun S H, Liang L M and Yuan J M 2011 *Phys. Rev.* A **83** 042326
[21] Daffer S, Wódkiewicz K, Cresser J D and McIver J K 2004 *Phys. Rev.* A **70** 010304
[22] Maniscalco S, Olivares S and Paris M G A 2007 *Phys. Rev.* A **75** 062119
[23] Liu K-L and Goan H-S 2007 *Phys. Rev.* A **76** 022312
[24] Vasile R, Olivares S, Paris M G A and Maniscalco S 2009 *Phys. Rev.* A **80** 062324
[25] Vasile R, Giorda P, Olivares S, Paris M G A and Maniscalco S 2010 *Phys. Rev.* A **82** 012313
[26] Huang P, He G, Lu Y and Zeng G 2011 *Phys. Scr.* **83** 015005
[27] Vasile R, Olivares S, Paris M G A and Maniscalco S 2011 *Phys. Rev.* A **83** 042321
[28] Lopez-Richard V, Gonzalez J C, Matinaga F M, Trallero-Giner C, Ribeiro E, Dias M R, Villegas-Lelovsky L and Marques G E 2009 *Nano Lett.* **9** 3129
[29] Bruß D 1998 *Phys. Rev. Lett.* **81** 3018
[30] Lo H-K 2001 *Quantum Inf. Comput.* **1** 81–94
[31] Kraus K 1983 *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Berlin: Springer)
[32] Gorini V, Kossakowski A and Sudarshan E C G 1976 *J. Math. Phys.* **17** 821
[33] Kimura G 2002 *Phys. Rev.* A **66** 062113
[34] Daffer S, Wódkiewicz K and McIver J K 2003 *Phys. Rev.* A **67** 062312
[35] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501
[36] Renner R, Gisin N and Kraus B 2005 *Phys. Rev.* A **72** 012332