Physics Letters A 381 (2017) 897–902

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Preservation of a lower bound of quantum secret key rate in the presence of decoherence

Shounak Datta *, Suchetana Goswami, Tanumoy Pramanik, A.S. Majumdar

S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700098, India

ARTICLE INFO

Article history:
Received 25 August 2016
Received in revised form 3 January 2017
Accepted 12 January 2017
Available online 16 January 2017
Communicated by A. Eisfeld

Keywords:
Quantum key distribution
Quantum steering
Weak measurement
Non-locality
Quantum decoherence

ABSTRACT

It is well known that the interaction of quantum systems with the environment reduces the inherent quantum correlations. Under special circumstances the effect of decoherence can be reversed, for example, the interaction modelled by an amplitude damping channel can boost the teleportation fidelity from the classical to the quantum region for a bipartite quantum state. Here, we first show that this phenomenon fails to preserve the quantum secret key rate derived under individual attack. We further show that the technique of weak measurement can be used to slow down the process of decoherence, thereby helping to preserve the quantum secret key rate when one or both systems are interacting with the environment via an amplitude damping channel. Most interestingly, in certain cases weak measurement with post-selection where one considers both success and failure of the technique is shown to be more useful than without it when both systems interact with the environment.

© 2017 Elsevier B.V. All rights reserved.

1. Introduction

Correlations between quantum systems can not always be explained by local causal theory [1,2]. This nature of quantum correlations helps to perform certain information processing tasks, for example, quantum teleportation [3], super dense coding [4] and quantum key distribution [5,6], which are not possible using classical correlations. However, in practice, quantum systems are continuously interacting with the environment, and this interaction weakens the correlations between observed quantum systems. Hence, the most crucial task in quantum information processing is to protect quantum correlations from diminishing due to the effect of the ubiquitous environment.

Under special circumstances, interaction between systems and a common environment can generate entanglement [7]. For example, when two or more atoms are consecutively passing through a cavity, they become entangled [8,9]. Although, for a specific information processing task, *viz.* quantum teleportation, the environmental interaction modelled by an amplitude damping channel (ADC) can enhance the fidelity of quantum teleportation of those bipartite states whose teleportation fidelity lies just below the quantum region [10], this improvement of fidelity is found to be possible only for a certain class of bipartite states [11,12].

Moreover, one can use the technique of weak measurements to protect the fidelity of quantum teleportation when systems are interacting with the environment modelled by an amplitude damping channel [12–19]. The idea of weak measurements was originally proposed [20] on the basis of weak coupling between the observed system and the measurement device, thereby making possible for the measurement outcomes to be amplified compared to the eigenvalue spectrum of original system, for suitable post-selected ensembles. This technique has been implemented in many different ways, such as in the study of the spin Hall effect [21], superluminal propagation of light [22], wave particle duality using cavity-QED experiments [23], direct measurement of the quantum wave function [24], measurement of ultrasmall time delays of light [25], and observing Bohmian trajectories of photons [26,27].

In the present work, we study the possibility of preservation of the quantum secret key rate for a bipartite state shared between Alice and Bob where Alice's system is not trusted as a quantum system. More specifically, we discuss a way to protect the one-sided device independent quantum key distribution (1s-DIQKD) [28] scenario[1] when the system interacts with the en-

* Corresponding author.
E-mail addresses: shounak.datta@bose.res.in (S. Datta), suchetana.goswami@bose.res.in (S. Goswami), tanu.pram99@bose.res.in (T. Pramanik), archan@bose.res.in (A.S. Majumdar).

http://dx.doi.org/10.1016/j.physleta.2017.01.019
0375-9601/© 2017 Elsevier B.V. All rights reserved.

[1] In the present work we are concerned with the security analysis when one of the parties does not trust her device, rather than details of the actual protocol, and hence, we use the terminology of "1s-DIQKD scenario", instead of the "1s-DIQKD protocol".

vironment modelled by ADC. Comparing the preservation of 1s-DIQKD with the preservation of the fidelity of quantum teleportation, we observe that ADC cannot improve the optimal secret key rate in 1s-DIQKD, which is derived using the steering inequality [29] based on the fine-grained uncertainty relation [30], though it can improve the teleportation fidelity for states having teleportation fidelity just below the quantum region [10,11]. We show that improvement of the secret key rate becomes possible using the technique of weak measurement and its reversal, which may be used to suppress the effect of the amplitude damping decoherence [13–18].

This paper is organized as follows. In Sec. 2, we briefly recapitulate the technique of weak measurement and its reversal in the presence of an interaction of the system with the environment as modelled by ADC. In Sec. 3 we discuss the connection of steerability with quantum key distribution for the case of the 1s-DIQKD scenario [29]. In Sec. 4 we demonstrate the effect of the amplitude damping decoherence on the steerability and secret key rate. In Sec. 5 we show how the technique of weak measurement and its reversal can be used to protect the secret key rate. Finally, in Sec. 6 we summarize the main results of this work.

2. Weak and reverse weak measurement in the presence of an amplitude damping channel

Let us consider photon loss when the photon is passing through the environment, which can be regarded as amplitude damping decoherence. The environmental interaction with the state of a two level system, ρ can be written as a positive and trace preserving map Λ given by

$$\Lambda(\rho) = W_{S,0}\,\rho\,W_{S,0}^{\dagger} + W_{S,1}\,\rho\,W_{S,1}^{\dagger}, \tag{1}$$

where

$$W_{S,0} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\overline{D_S}} \end{pmatrix}; \qquad W_{S,1} = \begin{pmatrix} 0 & \sqrt{D_S} \\ 0 & 0 \end{pmatrix}, \tag{2}$$

and $\sum_{i=0}^{1} W_{S,i}^{\dagger} W_{S,i} = I$. D_S is considered as the strength of the system with environment and $\sqrt{\overline{D_S}} = 1 - D_S$, where the subscript S denotes Alice's system ($S = A$) and Bob's system ($S = B$). Here, the matrices $W_{S,0}$ and $W_{S,1}$ are written in the photon number basis with the zero photon state denoted as $|0\rangle$ $\left(= \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right)$ and the one photon state denoted as $|1\rangle$ $\left(= \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right)$. Alice and Bob are regarded here to be well separated, and thus the environments for A and B are not connected, though for simplicity we take the same values of the decoherence strength for both. Hence, we do not consider any memory effect here.

It has been shown in earlier works [13–17] that the technique of weak measurement and its reverse can suppress the environmental effect modelled by ADC. Here, before allowing interaction with the environment, the system is measured using a scheme of weak quantum measurement, with strength p_S. More specifically, the detector detects the system with probability p_S if and only if the system is in the state $|1\rangle_S$. When the detector detects, the corresponding Kraus operator in the photon number basis is given by

$$M_{S,1} = \begin{pmatrix} 0 & 0 \\ 0 & \sqrt{p_S} \end{pmatrix}, \tag{3}$$

which does not have any inverse. Hence, this operation, i.e., the detection is irreversible. The operator when the system is not detected has the following form in the photon number basis

$$M_{S,0} = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{\overline{p_S}} \end{pmatrix}. \tag{4}$$

The operator $M_{S,0}$ is reversible, i.e., the application of its inverse restores the system to its initial state. The case where the system is detected will be discarded. Hence, weak measurement is associated with a success probability.

After performing weak measurement, the system is allowed to interact with the environment and at the end, to reduce the effect of environment, reverse weak measurement is performed. The operator corresponding the case when the system is not detected, can be written in the photon number basis as

$$N_{S,0} = \begin{pmatrix} \sqrt{\overline{q_S}} & 0 \\ 0 & 1 \end{pmatrix}, \tag{5}$$

where q_S is the strength of the reverse weak measurement.

3. Steering and its connection with 1s-DIQKD

Non-local quantum correlations between two systems, say A and B, can be categorized separately by entanglement, steering and Bell non-local correlation [31], respectively. In the case of entanglement, both A and B are trusted as quantum systems, whereas, none of them is trusted as a quantum system in Bell non-local correlation. In the intermediate case of steering, one of them is trusted as a quantum system and the shared state, ρ_{AB} is said to be entangled if it cannot be described by a local hidden state model (LHS) [31]. The security of quantum key distribution scenario is verified through the demonstration of one of the above forms of nonlocal correlations. So, for example, violation of Bell's inequality is required for the security of a fully device independent key distribution scenario since none of the two parties are trusted in this scenario. In case of a one-sided device independent scenario, the device of one of the two parties is not trusted, and hence, here the security is directly connected with the demonstration of quantum steering. There are different steering criteria based on different uncertainty relations [32–34]. In the present work we use the optimal fine-grained steering criteria to study the quantum secret key rate of steerable states [29].

To discuss fine-grained steering, let us consider the following game. Alice prepares a large number of bipartite quantum states ρ_{AB}. She then sends all the systems B to Bob and keeps the systems A with her. Bob only trusts that the system B is quantum, but agrees that the prepared state is entangled if and only if Alice has control on the state of systems B. In other words, ρ_{AB} is said to be steerable when it cannot be explained a by local hidden state model [31]. To check whether the state is steerable, Bob asks Alice to control the state of his system B in one of the eigenstates of the observable chosen randomly from the set $\{\sigma_z, \sigma_x\}$. Next, Alice measures a suitable observable chosen from the set $\{\mathcal{A}_1, \mathcal{A}_2\}$ and communicates her choice and outcome. The shared state ρ_{AB} is steerable when the conditional probability distribution $P(b_{\sigma_{z\,(x)}}|a_{\mathcal{A}_i})$ (where b and a are measurement outcomes at Bob's and Alice's side) violates the relation [29]

$$\frac{1}{2}\left[P(b_{\sigma_z}|a_{\mathcal{A}_1}) + P(b_{\sigma_x}|a_{\mathcal{A}_2})\right] \leq \frac{3}{4}. \tag{6}$$

It has been further shown that if the shared state ρ_{AB} between systems A and B is maximally steerable, then none of these systems can be quantumly correlated, or steerable with any other system – this phenomenon is called monogamy of steerable states. Let us consider ρ_{ABC} to be a shared state between Alice, Bob and Charlie. The monogamy relation is given by

$$\frac{1}{2}\left(\Sigma_{A,B} + \Sigma_{B,C}\right) \leq \frac{3}{4}, \tag{7}$$

where $\Sigma_{A,B} = \frac{1}{2}\left[P(b_{\sigma_z}|a_{\mathcal{A}_1}) + P(b_{\sigma_x}|a_{\mathcal{A}_2})\right]$ and $\Sigma_{B,C} = \frac{1}{2}\left[P(b_{\sigma_z}|c_{\mathcal{C}_1}) + P(b_{\sigma_x}|c_{\mathcal{C}_2})\right]$. Here, Charlie measures the observable $\mathcal{C}_1$ ($\mathcal{C}_2$)

Download English Version:

https://daneshyari.com/en/article/5496551

Download Persian Version:

https://daneshyari.com/article/5496551

Daneshyari.com