Pramana – J. Phys. (2021) 95:155
https://doi.org/10.1007/s12043-021-02194-x

Catalysing quantum information processing task using LOCC distinguishability

SUMIT NANDI

Institute of Physics, Sachivalaya Marg, Bhubaneswar 751 005, India
E-mail: sumit.enandi@gmail.com

MS received 22 January 2021; revised 13 April 2021; accepted 21 May 2021

Abstract. Entanglement is a key ingredient for performing information processing protocols. On the other hand, it is known that there may exist non-locality without entanglement. Distinguishing a set of unknown states by local operation and classical communication (LOCC) can be recast as a manifestation of non-locality. Motivated by this fact, we have explored a novel relation between entanglement and LOCC distinguishability of an ensemble of entangled states. We have shown explicitly that an ensemble of LOCC distinguished states is more efficient for quantum information processing protocol than those states which cannot be discriminated deterministically by LOCC.

Keywords. Local operation and classical communication distinguishability; controlled quantum key distribution; non-locality without entanglement.

PACS Nos 03.67.−a; 03.67.Bg; 03.67.Dd

1. Introduction

Quantum mechanics of a compound system allows non-local correlation known as entanglement and it has bestowed privilege on us to perform information processing protocols such as teleportation, quantum key distribution, secret sharing etc. Entanglement cannot be described by a local hidden variable. So it reveals non-locality [1]. However, non-locality arises when we discuss the issue of distinguishing a set of orthogonal state vectors by means of local operation and classical communication (LOCC) [2] and this astonishing aspect of non-locality has been referred to as non-locality without entanglement. In this connection, interesting phenomenon like more non-locality with less entanglement had been described while discussing LOCC indistinguishability of a set of pure states of Hilbert space with dimension $3 \otimes 3$ [3]. They had shown that a complete orthogonal basis cannot be discriminated if it contains at least one entangled state. The context of discrimination of finite-dimensional multipartite quantum states and its underlying connection with non-locality had been studied by many [4–6].

Two given orthogonal quantum state vectors can always be distinguished unambiguously by constructing a suitable measurement set-up. But it is not so obvious for a compound system, in particular when it is distributed between many observers and the observers are allowed to perform LOCC only to run the machinery of discrimination. The situation even becomes worse if the states carry entanglement with them. Quantum mechanics rules out the possibility of distinguishing the states in the ensemble unambiguously. It had been elegantly shown that among four Bell states, only two of them can be distinguished when one copy of a state is provided and only LOCC is allowed to the observers [5]. However, all the Bell states can be discriminated if two copies of a state is provided [7]. Indeed, two orthogonal multipartite states can always be distinguished without further ado. In this regard, the authors also presented a quantitative criterion of distinguishing two orthogonal multipartite states by LOCC. Contrarily, two non-orthogonal entangled states can also be discriminated conclusively with probability less than unity [8,9]. Although entanglement as a resource does not play any role in distinguishing between a finite set of states [10], we shall show quantitatively that such a discrimination sometimes may be crucial to make quantum information processing protocol more efficient. It had been widely believed that, apart from entanglement it is possible to manifest non-local

Published online: 13 September 2021

aspect of quantum mechanics by LOCC distinguishability [11]. Thus, it is of no wonder that it can be exploited for the betterment of certain quantum information processing protocols (QIP). In this work, we shall devote on this very issue and show how LOCC distinguishability can catalyse QIP task. We shall also discuss the scenario of LOCC distinguishability of an ensemble comprising orthogonal separable and entangled states to show that on its own this criterion would not be sufficient to perform a QIP successfully.

The main aim of this paper is to show a comprehensive relation between entanglement and LOCC distiguishability of a set of states in a given ensemble. We shall show that an ensemble of LOCC distinguishable entangled states ensures the success of a QIP protocol by considering controlled quantum key distribution [12] as a paradigmatic situation. Interestingly, we show that the states are more suitable for establishing secret key [13] whenever the collapsed states are LOCC distinguishable with larger probability. We have also presented a specific paradigm in which the scope of the protocol is broadened by appropriately choosing a set of LOCC distinguishable states. We organise the text as follows: in §2 we shall present our main result and subsequently we conclude in §3.

2. LOCC disitinguishability and controlled key distribution protocol

The problem of distinguishing an ensemble of states of a compound system depends on the operational approach that may arise during the execution of certain quantum information protocols. In a controlled key distribution protocol, Charlie intends to assist in establishing a secret key between Alice and Bob and the former acts as a controller. Therefore, it suffices to assume that the tripartite state shared between the trio is genuinely entangled. So, we shall consider the following class of states $|\Psi\rangle \in \mathcal{C}_2 \otimes \mathcal{C}_2 \otimes \mathcal{C}_2$ which is given as

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\big[\,|i\rangle_C\,|\phi\rangle_{AB} + |j\rangle_C\,|\tilde{\phi}\rangle_{AB}\,\big], \tag{1}$$

where $|i\rangle$, $|j\rangle$ constitute an orthonormal basis spanned by the bases $\{e_l\}_{l=0,1}$ respectively. Referring to the paradigmatic situation of distant labs scenario, Charlie measures his subsystem in the same basis as in eq. (1) and subsequently after the measurement, Alice and Bob jointly hold the subsystems $|\phi\rangle$ and $|\tilde{\phi}\rangle$ which are not necessarily orthogonal. It is worth mentioning that Charlie does not disclose his measurement setting to his partners leaving them no choice but to guess the states between $|\phi\rangle$ and $|\tilde{\phi}\rangle$. Here we note that $|\phi\rangle$'s are normalised state vectors and write those explicitly in computational basis as

$$|\phi\rangle = \sqrt{a}\,|00\rangle + \sqrt{1-a}\,|11\rangle\,, \tag{2}$$

$$|\tilde{\phi}\rangle = \sqrt{1-a}\,|00\rangle - e^{i\alpha}\sqrt{a}\,|11\rangle\,, \tag{3}$$

where $0 \le a \le 1$ and $0 \le \alpha \le \pi$. It can be easily realised that for $a = \frac{1}{2}$ and $\alpha = 0$, the collapsed states can be made Bell states. With this choice of parameters, the state $|\Psi\rangle$ becomes local unitary equivalent [14] to the well-known GHZ state in C-AB bipartition. But in general, Alice and Bob find partially entangled states at their disposal to carry out the protocol. However, in the particular situation $a = \frac{1}{2}$ and $\alpha = 0$, the collapsed states can be distinguished as two Bell states, one of them can always be determined unambiguously.

As the collapsed states are not orthogonal for the given choice of Charlie's measurement basis, the states cannot be distinguished deterministically either globally or by LOCC. We also mention that the states have the same entanglement as quantified by von Neumann entropy of an arbitrary individual subsystem and it turns out to be

$$S(\rho_B) = -a\log_2 a - (1-a)\log_2(1-a), \tag{4}$$

where ρ_B is Bob's subsystem obtained after tracing over Alice's subsystem. However, it does not allow one to perceive that $|\phi\rangle$ would be as compatible in establishing a secret key between Alice and Bob as $|\tilde{\phi}\rangle$. It will be evident in our discussion as we proceed. We restrict the protocol in a sense that they agree to measure their subsystems with the given projectors $\Pi_{0/1}$ and $\Pi_{\pm}$ where

$$\Pi_{0/1} = \mathcal{M}_{0/1}^{\dagger}\mathcal{M}_{0/1}, \quad \Pi_{\pm} = \mathcal{M}_{\pm}^{\dagger}\mathcal{M}_{\pm} \tag{5}$$

and

$$\mathcal{M}_0 = |0\rangle\langle 0|,$$
$$\mathcal{M}_1 = |1\rangle\langle 1|,$$
$$\mathcal{M}_{\pm} = |\pm\rangle\langle\pm|$$

and

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle).$$

As the collapsed states (2) and (3) are partially entangled states for arbitrary values of α and a, quantum key distribution cannot be carried out perfectly. At this point, it would be convenient to find out the efficacy of the protocol. As the resource states are not maximally entangled, there would be no perfect correlation of measurement outcomes as obtained by Alice and Bob inducing an inherent error in the protocol. Now, we shall find out quantum bit error rate (QBER) of the QKD protocol which is defined as the probability that Alice and Bob would obtain uncorrelated outcomes for a given

choice of measurement basis [15]. With partially entangled states, the key cannot be generated with perfect authenticity. However, the observers can fix a standard level of error that can be tolerated for the purpose and it is estimated by QBER of the protocol.

In our protocol, QBER ($\mathcal{Q}$) can be computed as

$$\mathcal{Q} = \frac{1}{2}\mathrm{Tr}(\Pi_0 \otimes \Pi_1.\rho) + \mathrm{Tr}(\Pi_1 \otimes \Pi_0.\rho) + \mathrm{Tr}(\Pi_+ \otimes \Pi_-.\rho) + \mathrm{Tr}(\Pi_- \otimes \Pi_+.\rho). \quad (6)$$

After plugging in the resource states (2) and (3) respectively, we obtain

$$\mathcal{Q}_{|\phi\rangle} = \frac{(\sqrt{1-a} - \sqrt{a})^2}{4} \quad (7)$$

$$.\mathcal{Q}_{|\tilde{\phi}\rangle} = \frac{1 - 2\sqrt{a(1-a)}\cos\alpha}{4}. \quad (8)$$

Thus, we have obtained an ensemble of two non-orthogonal pure entangled states $|\phi\rangle$ and $|\tilde{\phi}\rangle$ respectively, out of which equal number of Bell states can be distilled. It is much expected that QBER would be identical for both the collapsed states. But, we observe that $\mathcal{Q}_{|\tilde{\phi}\rangle}$ can be made larger than $\mathcal{Q}_{|\phi\rangle}$ by varying the parameter α. A close inspection reveals that the parameter α plays an important role in this protocol. The non-trivial phase factor makes collapsed states non-orthogonal. As a consequence, the resource states cannot be discriminated by LOCC deterministically. However, the given ensemble of states can be differentiated in a conclusive way. The collapsed state is either $|\phi\rangle$ or $|\tilde{\phi}\rangle$, or 'none of these' with some probability [8]. The success probability that can be achieved to distinguish the ensemble unambiguously is given by

$$P_{\mathrm{succ}} = 1 - |\langle\phi|\tilde{\phi}\rangle| = \sqrt{1 - 2\varepsilon(1-\cos\alpha) + 2\varepsilon^2(1-\cos\alpha)}, \quad (9)$$

where $\varepsilon = \sqrt{a(1-a)}$. Interestingly we observe that P_{succ} is less than unity except $\alpha = 0$.

We have plotted figures 1a and 1b to describe the behaviour of QBER and success probability of LOCC discrimination with the emerging parameter α. Figure 1a is produced for the given value $a = \frac{1}{2}$ while figure 1b shows almost the same behaviour for specific values of a. Both the figures suggest that P_{succ} is maximal and QBER vanishes when $\alpha = 0$. It also shows that whenever P_{succ} decreases, QBER tends to increase.

We observe that, when α vanishes, the given ensemble of states is mutually orthogonal and hence, can be discriminated deterministically. At this point, we also note that bit error rate of the state $|\tilde{\phi}\rangle$ is the least which signifies that the protocol can be made more efficient. Due to this non-trivial phase factor, the collapsed states become LOCC undistinguished and hence, QBER takes larger value making the protocol less and less secure. As security lies in the heart of any variant of key distribution protocol, arguably α influences the protocol considerably. The parameter can be used to estimate the validity of the protocol, and it can potentially make entanglement consuming protocol less efficient no matter how entangled the states may be. We also emphasise that the states in the ensemble have the same amount of entanglement but not LOCC distinguished for arbitrary α. LOCC distinguishability is ensured when phase difference strictly vanishes and it makes key distribution protocol more authentic. It would be interesting to find out the success probability to distinguish the states locally. We have found the expression for optimal discrimination locally $P_{\mathrm{succ}}^{\mathrm{local}}$ [9] as

$$P_{\mathrm{succ}}^{\mathrm{local}} = 1 - 2\sqrt{a(1-a)}. \quad (10)$$

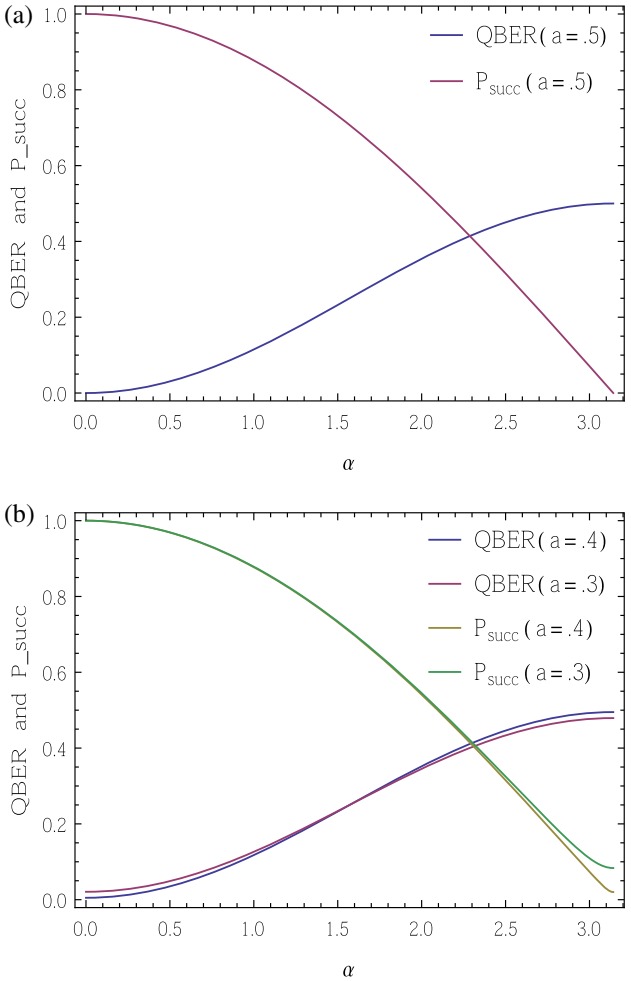

Figure 1. Behaviour of QBER and success probability of LOCC discrimination with α for given values of $a = 0.5, 0.4$ and 0.3. It is evident from the figure that P_{succ} is maximal and QBER vanishes when $\alpha = 0$. It is also depicted that as P_{succ} decreases, QBER tends to increase.

It is interesting to note that, for a given value of a, $P_{\text{succ}}^{\text{local}}$ does not depend on the parameter α, and entanglement being a potential resource, helps Bob to identify his subsystem.

Usually, in QKD protocols, information is encoded in two-level systems which propagate in quantum channel. It forces qubits to interact with the environment. One can analyse the discussion from this more general perspective. It makes the ensemble of the collapsed states an ensemble of mixed states. As the states are entangled, it suffices to consider only rank-2 states. Without loss of generality, we presume the collapsed states to pass through white noise and thus we obtain an ensemble of mixed states $\eta|\phi\rangle\langle\phi| + (1-\eta)|01\rangle\langle 01|$ and $\eta|\tilde{\phi}\rangle\langle\tilde{\phi}| + (1-\eta)|01\rangle\langle 01|$ respectively where η is a positive integer between $\{0, 1\}$. Indeed, the ensemble is not LOCC distinguishable. The proof is straightforward; if it happens then the states in the ensemble must be spanned by separable states only, but $|\phi\rangle$ and $|\tilde{\phi}\rangle$ are entangled which is antithetical. We also note that the states in the ensemble have same concurrence [16] as given by $2\eta\sqrt{a(1-a)}$. As we observed earlier, entanglement scarcely plays any role in LOCC discrimination between pure states, it also holds for mixed states.

Now we discuss the paradigm when the ensemble would contain orthogonal product and entangled states which are indeed LOCC distinguishable. We revisit the protocol, but this time taking the resource state given by

$$|\Phi\rangle = \sqrt{1/2}\big(|0\rangle_C|\zeta\rangle_{AB} + |1\rangle_C|\zeta'\rangle_{AB}\big), \tag{11}$$

where

$$|\zeta\rangle = \sqrt{\beta}\left(\frac{|00\rangle + |1\eta\rangle}{\sqrt{2}}\right) + \sqrt{1-\beta}\,|01\rangle$$

and

$$|\zeta'\rangle = |1\eta^{\perp}\rangle\,.$$

We take the explicit form of the normalised vectors, $|\eta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\eta'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ respectively. With these choices, it is straightforward to verify that $|\zeta\rangle$ and $|\zeta'\rangle$ are orthogonal, i.e. $\langle\zeta|\zeta'\rangle = 0$. However, we shall restrict our protocol as earlier in this section, Charlie measures his subsystem in computational basis and Alice and Bob establish secret key between them by using previously mentioned measurement settings. The ensemble comprises the collapsed states given by the following equation:

$$|\omega_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |1\eta\rangle) \tag{12}$$

$$|\omega_2\rangle = |01\rangle \tag{13}$$

$$|\omega_3\rangle = |1\eta^{\perp}\rangle\,. \tag{14}$$

We note that the states are collapsed with the probabilities $\beta/2$, $(1-\beta)/2$ and $1/2$ respectively. Interestingly, two of the collapsed states are separable. We observe that the collapsed states are mutually orthogonal, i.e. $\langle\omega_i|\omega_j\rangle = 0$ and it was shown in [17] that the ensemble is LOCC distinguishable deterministically. Nevertheless, $|\Phi\rangle$ is not suitable for Co-Qkd, as two of the collapsed states are separable, and those outcomes cannot be used as the resource for the proposed protocol. However, an entangled state $|\omega_1\rangle$ would be obtained with probability $\beta/2$, but we are seeking to establish key in each turn of Charlie's operation. So, $|\Phi\rangle$ seems to be incongruous for the controlled key distribution protocol. It also sets a counter-example that non-locality arising out of LOCC distinguishability cannot alone guarantee the success of a QIP. We have shown that though the collapsed states are LOCC distinguishable, $|\Phi\rangle$ cannot be used as a suitable resource for the protocol. Thus, we have obtained a tighter criterion for the protocol to succeed, and an ensemble of LOCC distinguishable entangled collapsed states are required to establish secret key in the mentioned scheme. However, we shall discuss one specific scheme of sharing secret between Alice and Bob under the supervision of Charlie. It may happen that Charlie intends no communication between the other two. Charlie must have that provision for whatever reason, and it also makes the whole protocol strictly under the control of Charlie. We observe that it is attainable if one of the collapsed states is separable. As the ensemble is LOCC distinguishable, the task is feasible for Charlie. Key distribution protocol would not work for either of the outcomes $|\omega_2\rangle$ and $|\omega_3\rangle$ and Charlie makes it always possible by measuring his subsystem in appropriate basis.

3. Conclusion

We have studied the effect of LOCC distinguishability of an ensemble of non-orthogonal quantum states on controlled QKD protocol. It has been shown that quantum bit error rate to which security of the protocol relies on, increases as the collapsed states become undistinguished by LOCC. We have shown explicitly that the resource states are more effective as determined by the parameter QBER when collapsed states between Alice and Bob remain distinguished in a conclusive manner. More importantly, we have shown that an ensemble of resource states having the same amount of entanglement as measured by von Nuemann entropy can have different effectiveness in quantum key distribution and it can be declassified by the LOCC distinguishability of the states. In our case, it turns out to be of utmost requirement to have zero phase difference to make LOCC distinguishability certain between two collapsed states.

Earlier, it was shown that entanglement is neither necessary nor sufficient to discriminate between the states. Nevertheless, such a discrimination can be an important factor for protocols like controlled quantum key distribution. It is an interesting observation as it may seem that entanglement of the resource states is the only determining factor for successful information processing protocols. However, we believe that non-locality emerging out of LOCC distinguishability of an ensemble of states may be important as well. We have shown it explicitly by illustrating that distinguishability can enhance the performance of controlled key distribution protocol.

Acknowledgements

The authors would like to thank Prof. Pankaj Agrawal for valuable discussions and comments which helped a lot to develop this work.

References

[1] A Einstein, B Podolsky and N Rosen, *Phys. Rev*. **47**, 777 (1935)
[2] C H Bennett, D P Di Vincenzo, C A Fuchs, T Mor, E Rains, P W Shor, J A Smolin and W K Wootters, *Phys. Rev. A* **59**, 1070 (1999)
[3] M Horodecki, A Sen(De), U Sen and K Horodecki, *Phys. Rev. Lett*. **90**, 047902 (2003)
[4] A Chefles, *Phys. Rev. A* **69**, 050307(R) (2004)
[5] S Ghosh, G Kar, A Roy, A Sen(De) and U Sen, *Phys. Rev. Lett*. **87**, 277902 (2001)
[6] M Hayashi, D Markham, M Murao, M Owari and S Virmani, *Phys. Rev. Lett*. **96**, 040501 (2006)
[7] J Walgate, A J Short, L Hardy and V Vedral, *Phys. Rev. Lett*. **85**, 4972 (2000)
[8] G Jaeger and A Shimony, *Phys. Lett. A* **197**, 83 (1995)
[9] S Virmani, M F Sacchi, M B Plenio and D Markhama, *Phys. Lett. A* **288**, 62 (2001)
[10] S Bandyopadhyay, *Phys. Rev. A* **85**, 042319 (2012)
[11] P-X Chen and C-Z Li, *Phys. Rev. A* **68**, 062107 (2003)
[12] A Das *et al*, *Eur. Phys. J. D* **74**, 91 (2020)
[13] A K Ekert, *Phys. Rev. Lett.* **67**, 661 (1991)
[14] B Krauss, *Phys. Rev. A* **82**, 032121 (2010)
[15] M Epping, H Kampermann, C Macchiavello and D Bruß, *New J. Phys.* **19**, 093012 (2017)
[16] W Wootters, *Phys. Rev. Lett.* **80**, 2245 (1998)
[17] J Walgate and L Hardy, *Phys. Rev. Lett.* **89**, 147901 (2002)