Measurement-device-independent randomness from local entangled states

Anubhav Chaturvedi[1], Manik Banik[2,3]

(1) Center for Computational Natural Sciences and Bio-informatics, IIIT-Hyderabad, Hyderabad 500032, India.
(2) The Institute of Mathematical Sciences, CIT Campus, Tharamani, Chennai 600113, India.
(3) Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 B.T. Road, Kolkata 700108, India.

*** Missing PACS ***

Abstract –Nonlocal correlations are useful for device independent (DI) randomness certification [Nature (London) **464**, 1021 (2010)]. The advantage of this DI protocol over the conventional quantum protocol is that randomness can be certified even when experimental apparatuses are not trusted. Although quantum entanglement is the necessary physical source for nonlocal correlation, these two are distinct concepts. There exist entangled states which produce no nonlocal correlation and hence are not useful for the DI randomness certification task. Here we introduce the measurement-device-independent randomness certification task and show that entangled states, having local description, can be useful resource in such task which otherwise are useless in corresponding DI scenario.

Introduction. – Randomness is a valuable resource for various important tasks ranging from cryptographic applications [1] to numerical simulations such as *Monte Carlo* method [2]. Algorithmic information theory shows that true randomness cannot exist from a mathematical point of view [3, 4]. Thus generation of randomness must be based on unpredictability of physical phenomena so that the random nature is guaranteed by the laws of physics. Classical physics being fundamentally deterministic in nature cannot guarantee such randomness [5]. on the other hand, though the outcomes of measurement performed on quantum system are intrinsically random (due to Born rule) [6, 7], but real-life implementation of such randomness generation procedures [8–10] further demand idealized modeling and detailed knowledge about the internal working process of the devices used for generating randomness. To overcome this issue, nonlocality based [11–13] and device independent (DI) technique [14–17] has been applied for generating randomness. In Ref. [18], Pironio *et al.* have shown that the correlation of entangled quantum particles can be used to certify the presence of genuine randomness and they have designed cryptographically secure random number generator which does not require any assumption on the internal working of the devices. The key point is that randomness in the outcomes of measurements performed on the separated parts of the entangled quantum systems can be certified in DI way if the correlation obtained from the entangled state violates a Bell inequality (BI). But, it is well known that nonlocality [22] and entanglement [23] are two distinct concepts. Not all entangled states violate BI, rather there exists entangled states for which measurement statistics can be simulated locally [24]. Therefore, such *local* entangled states are not useful resource for DI randomness certification. In this work we first introduce the measurement-device-independent (MDI) randomness certification protocol, where the quantum state preparation device behave quantum mechanically but the measurement device is completely untrusted. In such scenario we show that *local* entangled states can be potentially useful resource for randomness certification task which otherwise are not useful for DI randomness certification.

The concept of MDI information processing scenario has been independently introduced in Ref. [25] and Ref. [26], where the authors have presented the idea of MDI-quantum key distribution (MDI-QKD) protocol. Recently, Branciard *et al.* have shown that presence of entanglement can be demonstrated in MDI way [29]. To arrive at their conclusion Branciard *et al.* have used a recent result of Buscemi [31], which shows that all entangled states provide an advantage over the separable states for some a *semi quantum* game.

In this work we first introduce the MDI randomness certification task. Using the result of [29] we then show

that entangled states which are not useful for DI randomness certification can be useful resource in this scenario. More precisely we consider the two-qubit entangled Werner states $\varrho^v = v|\psi^-\rangle\langle\psi^-| + (1-v)\frac{\mathbb{I}}{2}\otimes\frac{\mathbb{I}}{2}$. It is known that Werner states with visibility parameter $v > 1/3$ are entangled and a subclass of these states (states with $v > 1/\sqrt{2}$) violates BI and hence are useful for DI randomness certification. On the other hand Werner states with $v \leq 1/2$ and $v \leq 5/12$ have local description for projective measurement and positive operator valued measurement (POVM), respectively and thus cannot be useful for DI randomness certification. We show that all these entangled Werner states are useful for MDI randomness certification.

Bell scenario and DI randomness. – A bipartite Bell scenario with m different measurements per subsystem, each measurement having d possible results, is characterized by the joint probabilities $P_{AB|XY} = \{p(ab|xy)\}$, with measurement results denoted by $a, b \in \{1, 2, ..., d\}$ and measurements denoted by $x, y \in \{1, 2, ..., m\}$. The quantum distribution $P^Q_{AB|XY}$ is of the form

$$p(ab|xy) = \mathrm{Tr}[M_{a|x} \otimes M_{b|y}\rho] \tag{1}$$

where ρ is a quantum state (density operator) in some tensor product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\{M_{a|x} \mid M_{a|x} \geq 0\ \forall a;\ \sum_a M_{a|x} = \mathbb{I}_{\mathcal{H}_A}\}$, $\{M_{b|y} \mid M_{b|y} \geq 0\ \forall b;\ \sum_b M_{b|y} = \mathbb{I}_{\mathcal{H}_B}\}$ are positive operator valued measures (POVMs) [33]. A Bell expression $I = \sum_{abxy} c_{abxy}p(ab|xy)$ is a linear combination of the probabilities specified by the coefficients $\{c_{abxy}\}$. Correlations which can be expressed as $P(ab|xy) = \int_\lambda d\lambda\rho(\lambda)P(a|x,\lambda)P(b|y,\lambda)$ with λ being the shared random variable, admit *local realistic* description and satisfy the condition $I \leq I_L$, where I_L is called the local bound of the BI. Interestingly, there exists entangled quantum states which violate BI and such correlations are called nonlocal correlations (see [22] for a review on Bell's nonlocality). Note that BI is derived under conjunction of the assumptions called *reality* and *locality* (along with *measurement independence*). Violation of BI by quantum correlations implies that quantum mechanics is not reconcilable with these assumptions. As these assumptions refer to properties of a ontological (hidden-variable) model [37], thus from the observed BI violation it is impossible to conclude which one of these assumptions is violated. Interestingly, the BI can be derived under two operational assumptions, namely, *predictability* and *signal locality* [38]. As the operational assumption of signal locality is an empirically testable (and well-tested) consequence of relativity, thus BI violation implies that events are unpredictable. This alternative derivation of BI from operational assumptions plays important role in the practical question of randomness certification even when the experimental devices are not trusted.

In DI randomness certification scenario one (Say Alice) has a private place which is completely inaccessible from the outside i.e., no illegitimate system may enter in this place. From a cryptographic point of view assumption of such private place is admissible. Alice choses classical inputs $x \in X$ and $y \in Y$ with probability distributions $\mathcal{P}_X(x)$ and $\mathcal{P}_Y(y)$, respectively, and sends them to two measurement devices ($\mathcal{MD}1$ and $\mathcal{MD}2$ respectively) through some secure classical communication channels. The inputs prescribe the measurement devices to perform some POVM $\{M_{a|x} \mid M_{a|x} \geq 0\ \forall a;\ \sum_a M_{a|x} = \mathbb{I}_{\mathcal{H}_A}\}$ and $\{M_{b|y} \mid M_{b|y} \geq 0\ \forall b;\ \sum_b M_{b|y} = \mathbb{I}_{\mathcal{H}_B}\}$ on some quantum state ρ, shared between the two devices. Once the inputs are received, no classical communication between the measurement devices $\mathcal{MD}1$ and $\mathcal{MD}2$ is allowed. Alice collects the input-output statistics $P(AB|XY) = \{p(ab|xy)\}$. Since no communication between two measurement devices is allowed (i.e signal locality assumption is satisfied) hence BI violation implies that operational statistic must be unpredictable. Therefore randomness can be certified without specifying the detail of the experimental device. The setup for DI randomness certification is depicted in Fig.1.

The amount of randomness associated with the measurement outcome is quantified by guessing probability $G(x, y, \mathcal{K}) = \max_{a,b} p(ab|xy, \mathcal{K})$ [19]. Here $p(ab|xy, \mathcal{K})$ are the joint outcome probabilities and $\mathcal{K}$ denotes the shared resources between the two spatially separated system. As for example if we are in the quantum domain then $\mathcal{K}$ is any bipartite quantum state. On the other hand, if no signaling (NS) scenario is considered then $\mathcal{K}$ can be any correlation satisfying NS principle. The quantity G corresponds to the probability to guess correctly the outcome pair (a, b), since the best guess is simply to output the most probable pair. The guessing probability can be expressed in bits and is then known as the min-entropy, $H_\infty(x, y, \mathcal{K}) = -\log_2 G(x, y, \mathcal{K})$ [39]. In [18], Pironio *et al.* have shown that whenever a bipartite input-output probability distributions violates BI there is nonzero min-entropy associated with the outputs. To obtain the minimum randomness in quantum theory one has to perform the following optimization problem:

$$\begin{aligned} p^*_q(ab|xy) \quad = \quad & \max \quad p(ab|xy) \\ & \text{subject to} \quad \sum_{abxy} c_{abxy}p(ab|xy) = I \\ & p(ab|xy) \text{ is quantum.} \end{aligned} \tag{2}$$

The last condition ensures that the obtained correlation is quantum one. Adapting a straightforward way of technique of semi-definite-programing (SDP) introduced in [40], one can efficiently check whether a given correlation is obtainable via quantum means or not. The minimum random bits obtained in quantum theory corresponding to BI violation I is thus $H_\infty(AB|XY) = -\log_2 \max_{ab} p^*_q(ab|xy)$. One may, however, be interested in the amount of minimum randomness obtained in NS theory; which mean that instead of the quantum state any correlation satisfying NS condition is allowed to share between the measurement devices (see [18] for NS analy-

sis).

Semi-quantum nonlocal game scenario. – Recently, Buschemi generalizes the standard Bell game scenario into semi quantum scenario [31]. In this case Alice chooses classical inputs $x \in X$ and $y \in Y$ with probability distributions $\mathcal{P}_X(x)$ and $\mathcal{P}_Y(y)$, respectively. But, instead of sending these classical inputs to the measurement devices she encodes the information of these inputs into sets of quantum states $\{|\phi^x\rangle_{\alpha'}\}_{x\in X}$ and $\{|\psi^y\rangle_{\beta'}\}_{y\in Y}$, chosen from Hilbert spaces $\mathcal{H}_{\alpha'}$ and $\mathcal{H}_{\beta'}$, respectively. The quantum states $|\phi^x\rangle$ and $|\psi^y\rangle$ are then send to the measurement devices $\mathcal{MD}1$ and $\mathcal{MD}2$, respectively, through quantum channels. Given these quantum states the respective measurement device $\mathcal{MD}1$ and $\mathcal{MD}2$ produce outcomes a and b, respectively, by performing POVMs on the composite system i.e. the system obtained from Alice and the part of a bipartite state $\rho_{\alpha\beta}$, shared between the two measurement devices $\mathcal{MD}1$ and $\mathcal{MD}2$. The output probability is

$$p_{\rho_{\alpha\beta}}(ab||\phi^x\rangle_{\alpha'}, |\psi^y\rangle_{\beta'}) = \mathrm{tr}[(\mathcal{M}_a^{\alpha'\alpha} \otimes \mathcal{M}_b^{\beta\beta'}) (|\phi^x\rangle_{\alpha'}\langle\phi^x| \otimes \rho_{\alpha\beta} \otimes |\psi^y\rangle_{\beta'}\langle\phi^y|)], \quad (3)$$

where $\mathcal{M}_a^{\alpha'\alpha}$ ($\mathcal{M}_b^{\beta\beta'}$) is the element of the POVM performed on the composite system $\mathcal{H}_{\alpha'} \otimes \mathcal{H}_{\alpha}$ ($\mathcal{H}_{\beta} \otimes \mathcal{H}_{\beta'}$) to produce the outcomes a and b. In this generalized framework Buscemi proved that if the shared state between the measurement devices $\mathcal{MD}1$ and $\mathcal{MD}2$ is entangled one then Alice can choose the input quantum states in such way that the produced correlation cannot be achieved by local operation and shared randomness (LOSR). Later it has been shown that in this scenario any entangled state can generate correlations that cannot be simulated by local operation and classical correlation (LOCC) even if there is no restriction on the amount of classical communication [32], but that such correlations can be simulated if the distribution of the shared variables depends on the input quantum states i.e., it the measurement independence assumptions have been reduced [41]. Using these semi quantum game framework, in the following, we explicitly show that all two-qubit entangled Werner states are useful for MDI randomness certification.

We consider the following particular semi-quantum game. The input quantum states are chosen from a regular tetrahedron on the Bloch sphere i.e.,

$$|\phi^x\rangle\langle\phi^x| = \frac{\mathbb{I} + \vec{v}_x.\vec{\sigma}}{2}, \quad |\psi^y\rangle\langle\psi^y| = \frac{\mathbb{I} + \vec{v}_y.\vec{\sigma}}{2}, \quad (4)$$

for $x, y = 1, .., 4$ we have $\vec{v}_1 = \frac{(1,1,1)}{\sqrt{3}}$, $\vec{v}_2 = \frac{(1,-1,-1)}{\sqrt{3}}$, $\vec{v}_3 = \frac{(-1,1,-1)}{\sqrt{3}}$ and $\vec{v}_4 = \frac{(1,-1,-1)}{\sqrt{3}}$; and $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ with σ_i $(i = 1, 2, 3)$ being the Pauli matrices. The POVM $\{\mathcal{M}_a^{\alpha'\alpha}\}_{a\in\{0,1\}}$ is given by

$$\mathcal{M}_1^{\alpha'\alpha} = |\phi^+\rangle\langle\phi^+|, \quad \mathcal{M}_0^{\alpha'\alpha} = \mathbb{I} - |\phi^+\rangle\langle\phi^+|, \quad (5)$$

where $|\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Same POVM is considered at Bob's end $\{\mathcal{M}_b^{\beta\beta'}\}_{b\in\{0,1\}}$. It is known that $W = \frac{\mathbb{I}}{2} - |\psi^-\rangle\langle\psi^-|$ is an entanglement witness for the two-qubit Werner state ϱ^v [30]. For Werner state ϱ^v, $\mathrm{tr}[\varrho^v W] = \frac{1-3v}{4}$, which is negative for $v > \frac{1}{3}$ and $\mathrm{tr}[\rho W] > 0$ for any separable state ρ. From this entanglement witness operator Branciard *et al.* have constructed the following MDI-entanglement witness [29]:

$$I(P) = \frac{5}{8}\sum_{x=y} p(1,1||\phi^x\rangle, |\psi^y\rangle) - \frac{1}{8}\sum_{x\neq y} p(1,1||\phi^x\rangle, |\psi^y\rangle) \quad (6)$$

here P denotes the probability distribution $\{p(a,b||\phi^x\rangle, |\psi^y\rangle)|a,b = 0,1; x,y = 1,..,4\}$. For the Werner states the above expression becomes $I(P_{\varrho^v}) = \frac{1-3v}{16}$, which is negative for $v > \frac{1}{3}$. For any separable state ρ, $I(P_\rho) = 0$, as separable states are the end points of the semi-quantum game relation '$\succcurlyeq_{sq}$' defined in [31].

MDI randomness certification. – We are now in the position to show that randomness can be certified by all two-qubit entangled Werner states when the measurement apparatuses are not trusted. The set up for MDI randomness certification is depicted in Fig.2. Here, in contrast to the DI randomness certification scenario (Fig.1), Alice has a perfect state preparation device at her private place. The quantum states, chosen from the set described in Eq.(4) are prepared by Alice and are sent to measurement devices $\mathcal{MD}1$ and $\mathcal{MD}2$ through quantum channels. No leakage of the information about the classical index x (or y) is allowed. In DI scenario, after sending the classical index x and y to the respective measurement devices no classical communication is allowed between the measurement devices. In this case no such restriction is required. But after receiving the quantum states from Alice any kind of quantum state transfer is prohibited between the two measurement devices. When the quantum states reach to the measurement devices, both the devices produce classical outcomes $a, b \in \{1, 0\}$. Alice collects the input-output statistics and tests whether the the collected data satify certain condition.

Resut:

Discussion. – Device independent randomness certification and generation are intense area of research which draws much attention in recent time. The key ingredient of these tasks is the presence of nonlocal correlation which is physically obtained from quantum entangled states. But not all entangled states produce such nonlocal correlation and hence have no use in DI randomness certification. In this work we introduce the concept of MDI randomness certification task and using a recently proposed novel concept of *semi-quantum nonlocal game* we show that all two-qubit entangled Werner states are useful in MDI randomness certification where some of these states are indeed useless in DI randomness certification. However, we have considered single shot scenario and the protocol presented

here is not optimal one. It is interesting to find the optimal protocol. On the other, it is also interesting to study the MDI randomness certification task with other classes of *Bell local* entangled states. In Ref. [43] the authors have shown that relaxation of 'measurement independence' assumption in Bell's theorem potentially enhance the adversary's capabilities in the task of randomness expansion. On the other hand in Ref. [41] the author has shown that correlations achieved in SG can be simulated by reducing 'measurement independence'. In light of these two results it will be interesting to study the effect of reduced 'measurement independence' in MDI randomness certification task.

Acknowledgments. – The author likes to thank G. Kar for simulating discussions. Discussions with D. Rosset at ISI-Kolkata and comments of A. Acín in a private communication are gratefully acknowledged. It is a great pleasure to thank T. Chakraborty for helping in improving the presentation of the manuscript.

REFERENCES

[1] D. E. Denning, *Cryptography and Data Security* (Addison-Wesley Publishing Company) 1982.
[2] M. H. Kalos and P.A. Whitlock, *Monte Carlo Methods* (John Wiley & Sons) 1986.
[3] GL. Chaitin, *IBM Journal of Research and Development*, **21** (1977) 350-359.
[4] D. Knuth, *The Art of Computer Programming Vol. 2, Semi-numerical Algorithms* (Addison-Wesley Publishing Company) 1981.
[5] J. Butterfield, *Routledge Encyclopedia of Philosophy*, **3** (1998) 33-39.
[6] M. Born, *Z. Phys.*, **38** (1926) 803-827.
[7] J. Von-Neumann, *Mathematical Foundations of Quantum Mechanics* (Princeton University Press) 1955.
[8] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter and A. Zeilinger, *Rev. Sci. Instrum.*, **71** (2000) 1675.
[9] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard and H. Zbinden, *J. Mod. Opt.*, **47** (2000) 595-598.
[10] U. Atsushi *et al.*, *Nature Photon.*, **2** (2008) 728-732.
[11] A.K. Ekert, *Phys. Rev. Lett.*, **67** (1991) 661-663.
[12] J. Barrett, L. Hardy and A. Kent, *Phys. Rev. Lett.*, **95** (2005) 010503-010507.
[13] L. Masanes, *Phys. Rev. Lett.*, **102** (2009) 140501.
[14] D. Mayers and A. Yao, *In FOCS'98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science: Washington DC, USA, IEEE Computer Society pages 503-509, 1998*, () .
[15] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, *Phys. Rev. Lett.*, **98** (2007) 230501.
[16] R. Colbeck, *PhD Dissertation* (University of Cambridge) 2007. (See arXiv:0911.3814).
[17] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar and V. Scarani, *New J. Phys.*, **11** (2009) 045021.
[18] S. Pironio *et al.*, *Nature (London)*, **464** (2010) 1021-1024.
[19] A. Acín, S. Massar and S. Pironio, *Phys. Rev. Lett.*, **108** (2012) 100402.
[20] S. Fehr, R. Gelles and C. Schaffner, *Phys. Rev. A*, **87** (2013) 012335.
[21] S. Pironio and S. Massar, *Phys. Rev. A*, **87** (2013) 012336.
[22] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, *Rev. Mod. Phys.*, **86** (2014) 419.
[23] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, *Rev. Mod. Phys.*, **81** (2009) 865.
[24] R.F. Werner, *Phys. Rev. A*, **40** (1989) 4277; J. Barrett, *Phys. Rev. A*, **65** (2002) 042302; A. Rai, MD R. Gazi, M. Banik, S. Das and S. Kunkri, *J. Phys. A: Math. Theor.*, **45** (2012) 475302.
[25] S. L. Braunstein and S. Pirandola, *Phys. Rev. Lett.*, **108** (2012) 130502.
[26] H. K. Lo, M. Curty M and B. Qi, *Phys. Rev. Lett.*, **108** (2012) 130503.
[27] H. Inamori, N. Lütkenhaus and D. Mayers, *Eur. Phys. J. D*, **41** (2007) 599-627.
[28] D. Gottesman, H. K. Lo, N. Lütkenhaus and J. Preskill, *Quantum Inf. Comput.*, **4** (2004) 325.
[29] C. Branciard, D. Rosset, Y. C. Liang and N. Gisin, *Phys. Rev. Lett.*, **110** (2013) 060405.
[30] G. Tóth and O. Gühne, *Phys. Rev. Lett.*, **94** (2005) 060501.
[31] F. Buscemi, *Phys. Rev. Lett.*, **108** (2012) 200401.
[32] D. Rosset, C. Branciard, N. Gisin and Y. Liang, *New J. Phys.*, **15** (2013) 053025.
[33] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press) 2000.
[34] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press) 2004.
[35] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, *Phys. Rev. Lett.*, **23** (1969) 880.
[36] S. Popescu and D. Rohrlich, *Fond. Phys.*, **24** (1994) 379-385.
[37] T. Rudolph, arXiv:quant-ph/0608120; N. Harrigan and R. W. Spekkens, *Found. Phys.*, **40** (2010) 125-157.
[38] E. G. Cavalcanti and H. M. Wiseman, *Found. Phys.*, **42** (2012) 1329-1338.
[39] R. Koenig, R. Renner and C.Schaffner, *IEEE Trans. Inf. Theory*, **55** (2009) 4337.
[40] M. Navascués, S. Pironio and A. Acín, *New J. Phys.*, **10** (2008) 073013.
[41] M. Banik, *Phys. Rev. A*, **88** (2013) 032118.
[42] A. Chees, *Phys. Lett. A*, **239** (1998) 339.
[43] D. E. Koh *et al.*, *Phys. Rev. Lett.*, **109** (2012) 160404.

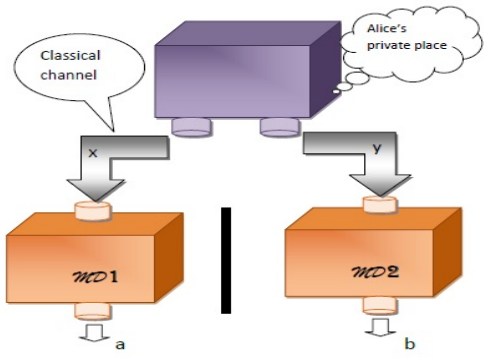

Fig. 1: Setup for DI randomness certification. Classical inputs are sent from Alice's private place to the measurement devices ($\mathcal{MD}1$ and $\mathcal{MD}2$) through secure classical channels. Classical communication is not allowed between two measurement devices.

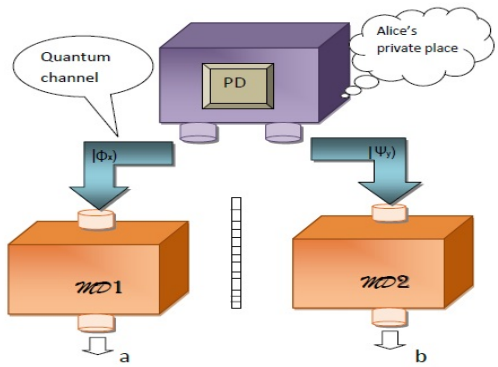

Fig. 2: Setup for MDI randomness certification. Alice has perfect state preparation device (PD) at her private place. Quantum states are sent from Alice's private place to the measurement devices through secure quantum channels. Classical communication is allowed between two measurement devices but no quantum state transfer is allowed.