Measurement-device-independent Randomness from local entangled states

ISCQI-2016

Manik Banik

Post Doctoral Fellow
Optics & Quantum Information Group
The Institute of Mathematical Sciences

Colaborator..

Figure: Anubhav Chaturvedi

Colaborator..

Figure: Anubhav Chaturvedi

Link: **Euro. Phys. Lett. 112, 30003 (2015)**
(doi: 10.1209/0295-5075/112/30003)

★ **Random numbers have many practical uses in modern science.**

- Cryptography
- Statistical research
- Numerical Simulation (eg. Monte Carlo method)
- Lotteries and gambling
- PIN number generation
- Mobile prepaid systems

★ **Consider a sequence of two numbers ‘0’ and ‘1’:**

010101010101010101010101010101010101......

with $p(0) = p(1) = \frac{1}{2}$

Randomness Certification...

★ **Consider a sequence of two numbers '0' and '1':**

010101010101010101010101010101010101......

with $p(0) = p(1) = \frac{1}{2}$

★ **Consider another sequence:**

010011101001010011101001010011101001......

with $p(0) = p(1) = \frac{1}{2}$

★ **Consider a sequence of two numbers '0' and '1':**

010101010101010101010101010101010101......

with $p(0) = p(1) = \frac{1}{2}$

★ **Consider another sequence:**

010011101001010011101001010011101001......

with $p(0) = p(1) = \frac{1}{2}$

$\{$**0100111010010**$\}\{$**0100111010010**$\}\{$**0100111010010**$\}$......

Certification: Mathematically impossible...

★ **Using algorithmic information theory it can be shown that true randomness can not exist from a mathematical point of view.** {Chaitin G. J., IBM J. Res. Dev., 21 (1977) 350; Knuth D., The Art of Computer Programming, Semi-numerical Algorithms}

Certification: Mathematically impossible...

★ **Using algorithmic information theory it can be shown that true randomness can not exist from a mathematical point of view.** {Chaitin G. J., IBM J. Res. Dev., 21 (1977) 350; Knuth D., The Art of Computer Programming, Semi-numerical Algorithms}

★ **Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin.**

——John von Neumann

★ **Therefore generation of randomness must rely on unpredictability of physical phenomena, like**

Certification: Impossible in classical physics...

★ **Coin tossing...**

Certification: Impossible in classical physics...

★ **Dice rolling...**

Certification: Impossible in classical physics...

★ **However all classical processes (‘coin tossing’/‘dice rolling’) are deterministic from fundamental point of view.**

★ **This is because, fate of any classical object at any time is completely predictable in Newtonian dynamics.**

★ **Therefore no classical process can be a source of "true" randomness.**

Certification: Impossible in classical physics...

★ However all classical processes (‘coin tossing’/‘dice rolling’) are deterministic from fundamental point of view.

★ This is because, fate of any classical object at any time is completely predictable in Newtonian dynamics.

★ Therefore no classical process can be a source of "true" randomness.

★ So we shift our attention from classical world (CW) to quantum world (QW).

★ **Quantum theory:**

- **State of a system: Vectors,** $|\psi\rangle \in \mathcal{H}$
- **Observables: Hermitian operator,** $\mathcal{A} \in \mathcal{B}(\mathcal{H})$**, acting on** $\mathcal{H}$
  $$\mathcal{A} = \sum_i a_i |\alpha_i\rangle\langle\alpha_i|$$
- **Possible measurement results: Eigenvalues of the given observable**
- **Outcome probability:** $p(a_1) = |\langle\psi|\alpha_i\rangle|^2$ **(Born rule)**

★ **Due to the Born's rule, in QW we can obtain our desired randomness.**

Certification: Possible in QW (?) {an example}...

★ **Consider a spin-1/2 system ($\mathcal{H} \equiv \mathbb{C}^2$)**

- **State:'up' eigenstate ($| \uparrow\rangle$) of the Pauli σ_z**
- **Measurement:Pauli σ_x observable, whose eigenstate are denoted as $| \rightleftarrows\rangle = \frac{1}{\sqrt{2}}(| \uparrow\rangle \pm | \downarrow\rangle)$.**
- **Outcome probability:** $p(| \rightarrow\rangle) = \frac{1}{2}$ **and also** $p(| \leftarrow\rangle) = \frac{1}{2}$

Certification: Possible in QW (?) {an example}...

★ **Consider a spin-1/2 system ($\mathcal{H} \equiv \mathbb{C}^2$)**

- **State:**'up' eigenstate ($|\uparrow\rangle$) of the Pauli σ_z
- **Measurement:**Pauli σ_x observable, whose eigenstate are denoted as $|\rightleftarrows\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle \pm |\downarrow\rangle)$.
- **Outcome probability:** $p(|\rightarrow\rangle) = \frac{1}{2}$ and also $p(|\leftarrow\rangle) = \frac{1}{2}$

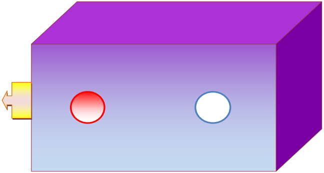
★ **If we associate '0' ('1') with $|\uparrow\rangle$ ($|\downarrow\rangle$), then we obtain a sequence of '0' and '1' with $p(0) = p(1) = \frac{1}{2}$ and there will be no pattern in the sequence $\Longrightarrow$ Randomness**

QRNG...

★ **Such QRNG already exists:**

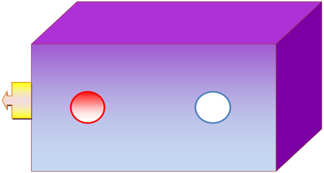
DI Certification...

★ **Consider that we are ignored about the internal working of the device, i.e., the device is like a black box with just input and output.**



DI Certification...

★ Consider that we are ignored about the internal working of the device, i.e., the device is like a black box with just input and output.

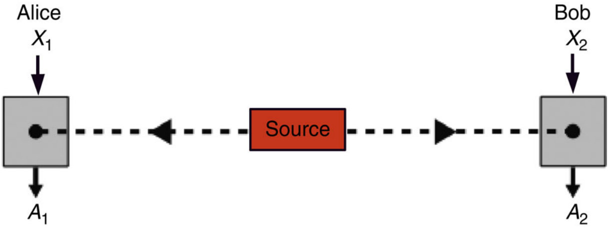


★ In this situation, is it still possible to be certain that the device is producing the outcomes without following any particular pattern?

DI Certification...

★ **In a recent result it has been shown that DI randomness certification is possible.**

★ **"Random Numbers Certified by Bell's Theorem"**, S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, C. Monroe, **Nature 464, 1021 (2010)**



★ **Local Realism (LR):**

$$P(A_1, A_2|X_1, X_2) = \sum_{\lambda \in \Lambda} \rho(\lambda) P(A_1|X_1, \lambda) P(A_2|X_2, \lambda)$$

★ **Bell inequality:** $|\langle X_1 X_2 \rangle + \langle X_1 X_2' \rangle + \langle X_1' X_2 \rangle - \langle X_1' X_2' \rangle| \leq 2$

★ **Bell inequality can also be derived under two operational assumptions, namely 'predictability' and 'signal-locality'**

★ **Determinism $\wedge$ Locality $\Rightarrow$ factorizability $\Rightarrow$ Bell's inequality (BI)**
i.e., $P(A_1, A_2|X_1, X_2, \psi) = \int_{\lambda\in\Lambda} \mu(\lambda|\psi) P(A_1|X_1, \psi, \lambda) P(A_2|X_2, \psi, \lambda) d\lambda$

- **Determinism (D)** $\Rightarrow P(A_1, A_2|X_1, X_2, \psi, \lambda) \in \{0, 1\}$
- **Locality (L)** $\Rightarrow P(A_1|X_1, X_2, \psi, \lambda) = P(A_1|X_1, \psi, \lambda)$
  $P(A_2|X_1, X_2, \psi, \lambda) = P(A_2|X_2, \psi, \lambda)$
- **Proof:**

$$\begin{aligned} P(A_1, A_2|X_1, X_2, \psi, \lambda) &= P(A_1|A_2, X_1, X_2, \psi, \lambda) P(A_2|X_1, X_2, \psi, \lambda) \\ &= P(A_1|X_1, X_2, \psi, \lambda) P(A_2|X_1, X_2, \psi, \lambda); \; [D] \\ &= P(A_1|X_1, \psi, \lambda) P(A_2|X_2, \psi, \lambda); \; [L] \end{aligned}$$

★ **Predictability $\wedge$ Signal Locality $\Rightarrow$ factorizability $\Rightarrow$ BI**
i.e., $P(A_1, A_2|X_1, X_2, \psi) = \int_{\lambda\in\Lambda} \mu(\lambda|\psi) P(A_1|X_1, \psi, \lambda) P(A_2|X_2, \psi, \lambda) d\lambda$

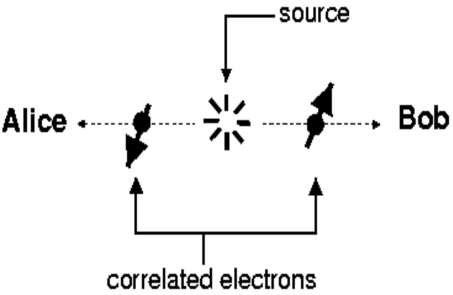
- **Predictability (P)** $\Rightarrow P(A_1, A_2|X_1, X_2, \psi) \in \{0, 1\}$
- **Signal Locality (SL)** $\Rightarrow P(A_1|X_1, X_2, \psi) = P(A_1|X_1, \psi)$
  $P(A_2|X_1, X_2, \psi) = P(A_2|X_2, \psi)$

★ **Predictability $\wedge$ Signal Locality $\Rightarrow$ factorizability $\Rightarrow$ BI**
i.e., $P(A_1, A_2|X_1, X_2, \psi) = \int_{\lambda\in\Lambda} \mu(\lambda|\psi) P(A_1|X_1, \psi, \lambda) P(A_2|X_2, \psi, \lambda) d\lambda$

- **Predictability (P)** $\Rightarrow P(A_1, A_2|X_1, X_2, \psi) \in \{0, 1\}$
- **Signal Locality (SL)** $\Rightarrow P(A_1|X_1, X_2, \psi) = P(A_1|X_1, \psi)$
  $P(A_2|X_1, X_2, \psi) = P(A_2|X_2, \psi)$

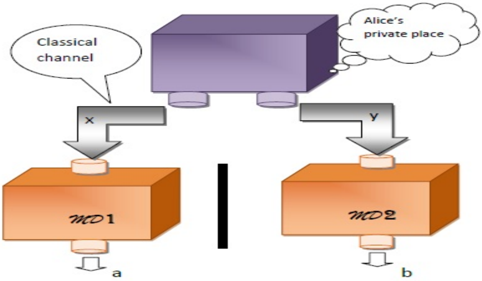
★ $\neg$ **BI** $\wedge$ **Signal Locality** $\Rightarrow$ $\neg$ **Predictability**

★ **Quantum correlation violates BI:**



★ **Using nonlocal correlation DI randomness certification is possible.**

DI Randomness Certification......



★ **Randomness associated with $\{P(ab|xy)\}$, quantified as** $H_\infty = -\log_2 \max_{a,b} P(ab|xy)$.

★ **Which physical correlation shows this nonlocal properties?**

★ **Which physical correlation shows this nonlocal properties?**

★ **Entanglement:**

- **Bipartite quantum system** $\rightarrow \mathcal{H}_A \otimes \mathcal{H}_B$
- **Product state:** $|\psi\rangle_A \otimes |\psi\rangle_B \in \mathcal{H}_A \otimes \mathcal{H}_B$
- **Non product States are called entangled:** $|\psi\rangle_{AB} = \sum_i c_i |\psi^i\rangle_A \otimes |\psi^i\rangle_B$
- **Separable states:** $\rho_{AB} = \sum_i p_i \sigma^i_A \otimes \sigma^i_B$**; with** $p_i \geq 0$ & $\sum \liminf_i p_i = 1$

★ **Example: Werner class of states**

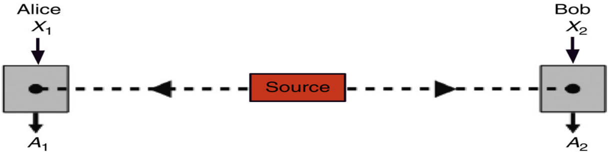
$$W_p = p|\psi^-\rangle\langle\psi^-| + (1-p)\frac{\mathbb{I}}{2} \otimes \frac{\mathbb{I}}{2}$$

with $0 \leq p \leq 1$ **and** $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle|\downarrow\rangle - |\downarrow\rangle|\uparrow\rangle)$

- $p > \frac{1}{\sqrt{2}}$: **Violates BI (useful for DI certification)**
- $p \leq \frac{1}{2}$: **LHV for PV**
- $p \leq \frac{5}{12}$: **LHV for POVM**
- $p \geq \frac{1}{3}$: **Entangled**

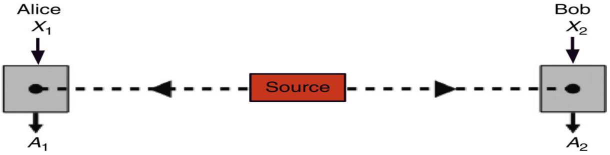
★ **Local entangled states are not useful for DI randomness certification**

★ **Semi-quantum game (F. Buschemi):**



- **Instead of classical inputs, 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, are sent**
- **For every entangled state quantum inputs can be chose in such a way that the produced correlation cannot be achieved by local operation and shared randomness**

★ **Semi-quantum game (F. Buschemi):**



- **Instead of classical inputs, 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, are sent**
- **For every entangled state quantum inputs can be chosen in such a way that the produced correlation cannot be achieved by local operation and shared randomness**

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

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

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**

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

- **Using the above quantum-input classical-output statistics one can construct the following MDI-entanglement witness (Branciard et al.):**

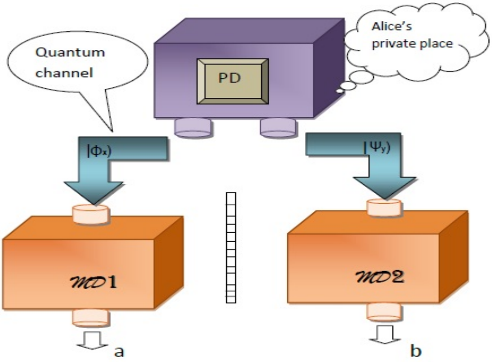
$$I(P) = \frac{5}{8}\sum_{x=y} p(1,1||\phi^x\rangle,|\psi^y\rangle) - \frac{1}{8}\sum_{x\neq y} p(1,1||\phi^x\rangle,|\psi^y\rangle).$$

  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**,** $I(P_\rho) = 0$

MDI Randomness Certification......

★ **Measurement-DI (MDI) randomness certification:**



⋆ MDI min-entropic source

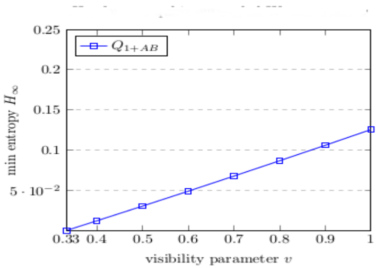
To find the minimum randomness associated with the probability distribution $P = \{p(ab|xy)\}$ one has to solve the following optimization problem,

$$
\begin{aligned}
p^*(ab|xy) \quad = \quad & \textbf{max} \quad p(ab|xy) \\
& \textbf{subject to} \quad I(P) = \frac{1-3v}{16} \\
& p(ab|xy) \in Q,
\end{aligned}
$$

- where $I(P) = \frac{5}{8}\sum_{x=y} p(1,1||\phi^x\rangle,|\psi^y\rangle) - \frac{1}{8}\sum_{x\neq y} p(1,1||\phi^x\rangle,|\psi^y\rangle)$
- the minimum random bits is therefore $H_\infty(AB|XY) = -\log_2 \max_{ab} p_q^*(ab|xy)$.
- While the optimization problem is computationally tough, we solve for a relaxed condition $p(ab|xy) \in Q_{1+AB}$ using SDP.

★ MDI min-entropic source

- **we find zero min-entropy against** Q_{1+AB}
- **so we put further conditions on the observed statistics:** $P(0,0|l,l) = P(0,0|m,m)$; $P(0,0|l,l) = P(0,0|m,m)$; $\forall\ l, m \in \{1,2,3,4\}$
- **interestingly positive min entropy is obtained for** $I(P) < 0$



★ MDI min-entropic source

- two qubits entangled Werner class of states also satified the required conditions and hence are useful for MDI min-entropy (randomness) certification
- no seperable state satifies this condition $I(P) < 0$ hence no cheating strategy is possible by sharing seperable correlations
- correlations in semi-quantum scenarion cannot even be simulated by local operation and classical correlation (LOCC) (Rosset et al.)

★ **Summary of the talk:**

- Randomness is a useful resource
- Randomness certification is not possible mathematically and also in classical world
- In quantum world randomness generation is possible
- Bell's theorem: DI certification possible:– nonlocal entangled states are useful
- local entangled states are useful for MDI randomness certification


Thank You!