Detection of genuine multipartite entanglement and its applications in secure communication

Ramij Rahaman

Department of Mathematics

Presidency University

Kolkata-700073

OUTLINE

- **INTRODUCTION**
  - Tasks/problems & possible applications.
  - Non-locality test (without any inequality).
- **OUR WORKS:**
  - Detection of true multipartite entanglement.
  - DI-Quantum Key Distribution with measurement inputs.
  - Quantum Digital Signatures.
  - DI Quantum Liar Detection & Byzantine Agreement.
  - DI Quantum Random Number Generator, etc.

Tasks/Problems

Let $H = H_1 \otimes H_2$; $n \times m$ dim. Hilber space.

$$\begin{pmatrix} a_1 \\ a_2 \end{pmatrix} \otimes \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$$

Hilbert Space:	H_1	H_2	$H = H_1 \otimes H_2$
Orthonormal basis:	$\{\lvert\eta_i\rangle_1\}_{i=1}^{n}$	$\{\lvert\chi_j\rangle_2\}_{j=1}^{m}$	$\{\lvert\eta_i\rangle_1 \otimes \lvert\chi_j\rangle_2\}_{i=1,2,..,n}^{j=1,2,..,m}$

Any $|\psi\rangle_{12} \in H$ can be expressed as $\displaystyle\sum_{i=1,2,..,n}^{j=1,2,..,m} \alpha_{ij}\, |\eta_i\rangle_1 |\chi_j\rangle_2$

Product state: $|\psi\rangle_{12} = |\eta\rangle_1 \otimes |\chi\rangle_2$

Entangled state: $|\psi\rangle_{12} \neq |\eta\rangle_1 \otimes |\chi\rangle_2$ **[A key feature, exists in quantum correlations.]**

Tasks/Problems cont...

Consider a system $H = H_1 \otimes H_2 \otimes \ldots \otimes H_n$; $\text{Dim.}(H) = d_1 . d_2 \ldots d_n$

$|\Psi\rangle \in H$ is called:

i) fully product if, $|\Psi\rangle = |\eta\rangle_1 |\chi\rangle_2 \ldots |e\rangle_n$

ii) bi-separable/product if, $|\Psi\rangle = |\phi\rangle_K |\xi\rangle_{\bar{K}}$; $K \subset \{1, 2, \ldots, n\}$

iii) genuine entangled if, $|\Psi\rangle \neq |\phi\rangle_K |\xi\rangle_{\bar{K}}$

E. g. : $\alpha\, |0\rangle_1 |0\rangle_2 \ldots |0\rangle_n + \beta |1\rangle_1 |1\rangle_2 \ldots |1\rangle_n$ is genuinely entangled.

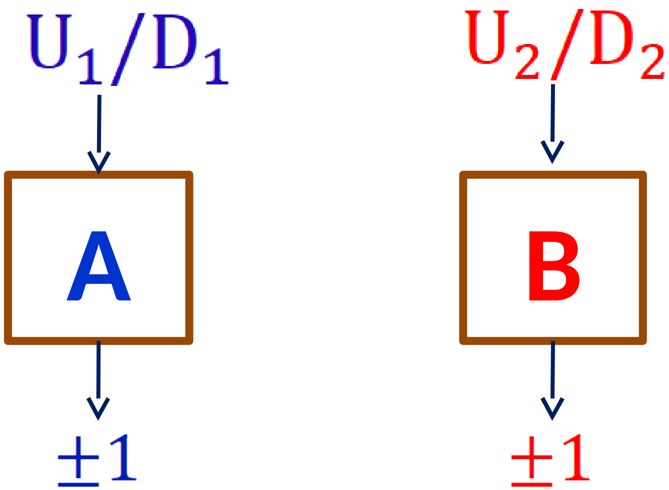
Problems:

- General witness for bi-separable & genuine entangled states.
- Non-classicality & monogamous characteristics of $|\Psi\rangle \in H$

Applications

- Provides secure quantum protocols for various cryptographic & communication tasks. E.g.,
  - Key distribution
  - Digital signatures
  - Secret sharing
  - Byzantine agreement
  - Random number generator
  - Oblivious transfer
  - Dining cryptographers
  - Anonymous veto etc.
- Quantum algorithms & computation.
- Quantum simulation & metrology, etc.

Hardy's Paradox *[L. Hardy PRL 1992]*



$$P(+,+|U_1,U_2) = q > 0$$
$$P(+,+|U_1,D_2) = 0$$
$$P(+,+|D_1,U_2) = 0$$
$$P(-,-|D_1,D_2) = 0$$

P(a,b|X,Y) is the joint probability of getting the outcome (a,b) for the given input (X,Y).

This set of conditions cannot be satisfied by any Local-Realistic (LR) Theory (Classical Theory).

HARDY'S PARADOX & QM

$\mathrm{P}(\mathrm{a},\mathrm{b}|\mathrm{X},\mathrm{Y}) = |\langle\psi|(|\mathrm{X}=\mathrm{a}\rangle|\mathrm{Y}=\mathrm{b}\rangle)|^2$ for the quantum state $|\psi\rangle$.

$|\mathrm{X}=\mathrm{a}\rangle$ is the eigenstate corresponding to the eigenvalue **a**.

$$\mathrm{P}(+,+|\mathrm{U}_1,\mathrm{U}_2) = \mathrm{q} > 0 \qquad |\phi_4\rangle = |U_1 = +1\rangle|U_2 = +1\rangle$$
$$\mathrm{P}(+,+|\mathrm{U}_1,\mathrm{D}_2) = 0 \qquad |\phi_3\rangle = |U_1 = +1\rangle|D_2 = +1\rangle$$
$$\mathrm{P}(+,+|\mathrm{D}_1,\mathrm{U}_2) = 0 \qquad |\phi_2\rangle = |D_1 = +1\rangle|U_2 = +1\rangle$$
$$\mathrm{P}(-,-|\mathrm{D}_1,\mathrm{D}_2) = 0 \qquad |\phi_1\rangle = |D_1 = -1\rangle|D_2 = -1\rangle$$

Let $|\mathbf{D_j} = +\mathbf{1}\rangle = \mathbf{a_j}|\mathbf{U_j} = +\mathbf{1}\rangle + \mathbf{b_j}|\mathbf{U_j} = -\mathbf{1}\rangle, \mathbf{j} = \mathbf{1}, \mathbf{2}$; with $|\mathbf{a_j}|^2 + |\mathbf{b_j}|^2 = \mathbf{1}$ & $\mathbf{0} < |\mathbf{a_j}| < \mathbf{1}$.

$|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle, |\phi_4\rangle$ are linearly independent.

If $\mathbf{S} = \{|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle\}$, then $\dim(\mathbf{S}) = \mathbf{3}$.

Hardy state $|\Psi\rangle \perp \mathbf{S}$ & $\dim(\mathrm{H_A} \otimes \mathrm{H_B}) = \mathbf{2} \times \mathbf{2}$.

$\therefore |\Psi\rangle$ is unique [Ref. G Kar, PLA 97].

HARDY STATE

$$|\phi_1\rangle = |D_1 = -1\rangle|D_2 = -1\rangle \quad |\phi_3\rangle = |U_1 = +1\rangle|D_2 = +1\rangle$$

$$|\phi_2\rangle = |D_1 = +1\rangle|U_2 = +1\rangle \quad |\phi_4\rangle = |U_1 = +1\rangle|U_2 = +1\rangle$$

By Gram-Schmidt orthogonalization procedure

$$|\phi_1'\rangle = |\phi_1\rangle;$$

$$|\phi_i'\rangle = \frac{|\phi_i\rangle - \sum_{j=1}^{i-1}\langle\phi_j'|\phi_i\rangle|\phi_j'\rangle}{\sqrt{1 - \sum_{j=1}^{i-1}|\langle\phi_j'|\phi_i\rangle|^2}}; i = 2,3,4$$

$\therefore$ Hardy state $|\Psi\rangle = |\phi_4'\rangle$

PROBABILITY OF SUCCESS

Probability of Success $q = |\langle\Psi|\phi_4\rangle|^2 = \dfrac{|a_1a_2|^2|b_1b_2|^2}{1-|a_1a_2|^2}$.

Its maximum is $\dfrac{5\sqrt{5}-11}{2} = 0.09$, where $|a_1| = |a_2| = \sqrt{\frac{\sqrt{5}-1}{2}}$.

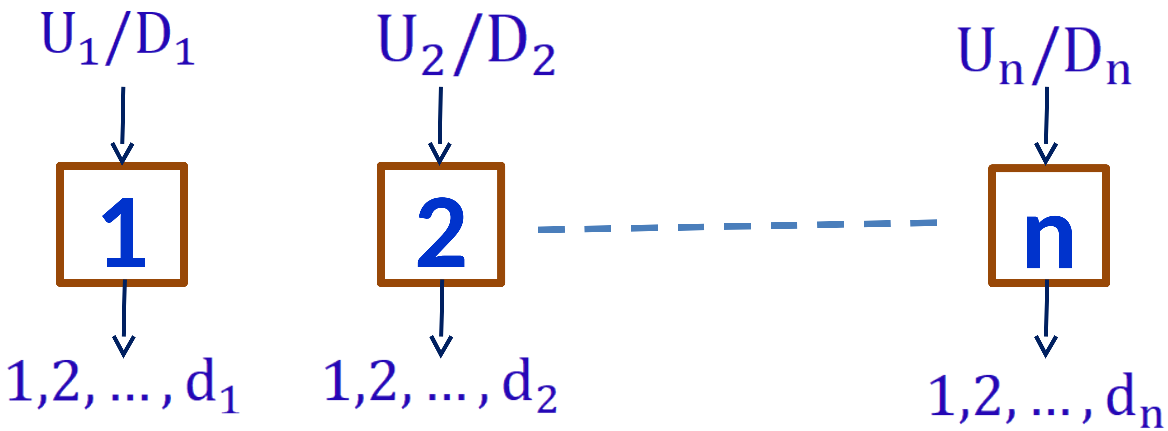
$\therefore U_1 \equiv U_2$ & $D_1 \equiv D_2$.

For **q=0.09** (max.), associated Hardy state $|\psi\rangle$ is ***device-independent*** *[Rabelo et al. PRL 2012]*.

For $q_{\max} = \dfrac{5\sqrt{5}-11}{2}$ the state is equivalent to $|\psi_{\max}\rangle_{12} \otimes |\eta_{1'2'}\rangle$.

NON-LOCALITY TEST FOR GENUINE ENTANGLEMENT.

Consider a system $H = H_1 \otimes H_2 \otimes \ldots \otimes H_n$; $\mathrm{Dim.}(H) = d_1 . d_2 \ldots d_n$



$$P(11 \ldots 1 | D_1 D_2 \ldots D_n) = 0$$

$$P(a_r 1 | D_r U_{r+1}) = 0 \quad a_r \neq 1$$

$$P(11 \ldots 1 | U_1 U_2 \ldots U_n) = q > 0$$

Again cannot be satisfied by any LR theory

Also, states of the form $|\phi\rangle_K \otimes |\xi\rangle_{\bar{K}}$; $K \subset \{1,2, \ldots, n\}$ cannot.

That is, **only genuine entangled states** can satisfy.

[Rahaman et al., Phys. Rev. A 2014]

Proof: If is ρ not a genuine entangled state then all joint probabilities can be expressed as,

$$P_\rho(x_1x_2 \ldots x_n|X_1X_2 \ldots X_n) = \sum_m p_m Q(x_1x_2 \ldots x_m|X_1X_2 \ldots X_m) R(x_{m+} \ldots x_n|X_{m+1} \ldots X_n)$$

$P_\rho(11 \ldots 1|U_1U_2 \ldots U_n) > 0$ implies, for some $\mathrm{m} \in \{\mathrm{m}\}$,

$\mathrm{Q}(11 \ldots 1|\mathrm{U}_1\mathrm{U}_2 \ldots \mathrm{U}_\mathrm{m})\ \mathrm{R}(11 \ldots 1|\mathrm{U}_{\mathrm{m}+1}\mathrm{U}_{\mathrm{m}+2} \ldots \mathrm{U}_\mathrm{n}) = \mathrm{q}' > 0$,

Middle conditions: $\mathrm{Q}(\mathrm{a_m} \neq 1|\mathrm{D_m})\mathrm{R}(1|\mathrm{U_{m+1}}) = 0\ \&\ \mathrm{R}(\mathrm{a_n} \neq 1|\mathrm{D_n})\mathrm{Q}(1|\mathrm{U_1}) = 0$.

$\because \mathrm{R}(1|\mathrm{U_{m+1}}) \neq 0$, so $\mathrm{Q}(\mathrm{a_m} \neq 1|\mathrm{D_m}) = 0$. Thus, $\mathrm{Q}(1|\mathrm{D_m}) = 1$.

$\therefore\ Q(x_1x_2 \ldots x_m|X_1X_2 \ldots X_m) = Q'(x_1x_2 \ldots x_{m-1}|X_1X_2 \ldots X_{m-1})\mathrm{Q}(\mathrm{x_m}|\mathrm{X_m})$.

Also middle conditions give us, $\mathrm{Q}'(\mathrm{a_{m-1}} \neq 1|\mathrm{D_{m-1}})\mathrm{Q_m}(1|\mathrm{U_m}) = 0$.

Again, $\mathrm{Q_m}(1|\mathrm{U_m}) > 0$, so $\mathrm{Q}'(\mathrm{a_m} \neq 1|\mathrm{D_{m-1}})$ i.e., $\mathrm{Q}'(1|\mathrm{D_{m-1}}) = 1$.

Proceeding like this we show that Q fully factorizes.

Following the same steps, we can show that R is fully factorized with the help of $\mathbf{R(a_n \neq 1|D_n)Q(1|U_1) = 0}$

Thus the state representing the considered term is fully factorizable.

Such states admit local hidden variable models, and as such **cannot** satisfy the mentioned set of joint probability conditions for **q'> 0**.

For qubits system: $\text{Dim.}\,(H) = 2 \times 2 \times \ldots \times 2$

$$P(11\ldots 1|D_1 D_2 \ldots D_n) = 0;\ |\phi_-\rangle = |D_1 = 1\rangle|D_2 = 2\rangle \ldots |D_n = 1\rangle$$

$$P(a_r 1|D_r U_{r+1}) = 0\,;\ |\phi_{k_r}\rangle = |..\rangle \ldots |D_r = 2\rangle|U_{r+1} = 1\rangle \ldots |..\rangle$$

$$P(11\ldots 1|U_1 U_2 \ldots U_n) = q;\ |\phi_+\rangle = |U_1 = 1\rangle|U_2 = 1\rangle \ldots |U_n = 1\rangle$$

Define a new basis: $|00\ldots 0\ldots 0\rangle = |\phi_+\rangle,$

$$|00\ldots 01_l 0\ldots 0\rangle = \frac{1}{\beta_l}\left[|\phi_k(0,\ldots,0,+_l,0,\ldots,0)\rangle - \alpha_l|\phi_+\rangle\right], \forall\ l,$$

$$\begin{aligned}|0\ldots 01_l 0\ldots 01_m 0\ldots 0\rangle = \frac{1}{\beta_l\beta_m}&[|\phi_k(0,\ldots,0,+_l,0,\ldots,0,+_m,0,\ldots,0)\rangle - \alpha_l\alpha_m|\phi_+\rangle\\ &- \beta_l\alpha_m|00\ldots 01_l 0\ldots 0\rangle - \alpha_l\beta_m|00\ldots 01_m 0\ldots 0\rangle], \forall\, l \neq m,\end{aligned}$$

$$\begin{aligned}|0\ldots 01_l 0\ldots 01_m 0\ldots 01_k 0\ldots 0\rangle = \frac{1}{\beta_l\beta_m\beta_k}&[|\phi_k(0,\ldots,0,+_l,0,\ldots,0,+_m,0,\ldots,0,+_k,0,\ldots,0)\rangle\\ &- \alpha_l\alpha_m\alpha_k|\phi_+\rangle - \alpha_l\alpha_m\beta_k|00\ldots 01_k 0\ldots 0\rangle\\ &- \alpha_l\beta_m\alpha_k|00\ldots 01_m 0\ldots 0\rangle - \beta_l\alpha_m\alpha_k|00\ldots 01_l 0\ldots 0\rangle\\ &- \alpha_l\beta_m\beta_k|00\ldots 01_m 0\ldots 01_k 0\ldots 0\rangle\\ &- \beta_l\alpha_m\beta_k|00\ldots 01_l 0\ldots 01_k 0\ldots 0\rangle - \beta_l\beta_m\alpha_k|00\ldots 01_l 0\ldots 01_m 0\ldots 0\rangle],\\ &\forall\, l \neq m \neq k \neq l, \ldots\end{aligned}$$

$$\begin{aligned}|11\ldots 1\ldots 1\rangle = \frac{(-1)^N}{\prod_{i=1}^N \alpha_i^*}\Bigg[&|\phi_0\rangle - \Bigg\{\left(\prod_{j=1}^N \beta_j^*\right)|\phi_+\rangle + (-1)^1\sum_{i=1}^N \alpha_i^*\left(\prod_{j=1, j\neq i}^N \beta_j^*\right)|00\ldots 01_i 0\ldots 0\rangle\\ &+ (-1)^2\sum_{i,l=1, i\neq l}^N \alpha_i^*\alpha_l^*\left(\prod_{j=1, j\neq i,l}^N \beta_j^*\right)|00\ldots 01_i 0\ldots 01_l 0\ldots 0\rangle\\ &+ \cdots + (-1)^{N-1}\sum_{j=1}^N \beta_j^*\left(\prod_{i=1, i\neq j}^N \alpha_i^*\right)|11\ldots 10_j 1\ldots 1\rangle\Bigg\}\Bigg],\end{aligned}$$

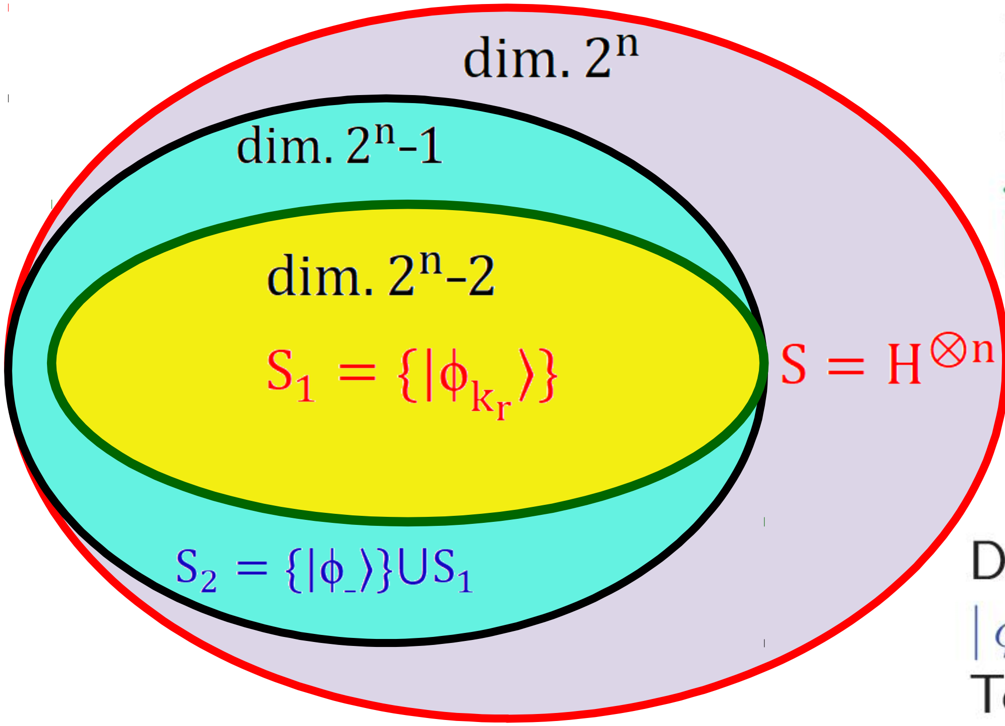
where $|+\rangle_j = \alpha_j|0\rangle_j + \beta_j|1\rangle_j$, and $|-\rangle_j = \beta_j^*|0\rangle_j - \alpha_j^*|1\rangle_j$

For qubits system: $\mathrm{Dim.}(\mathrm{H}) = 2 \times 2 \times \ldots \times 2$

$P(11\ldots1|D_1D_2\ldots D_n) = 0$; $|\phi_-\rangle = |D_1 = 1\rangle|D_2 = 2\rangle \ldots |D_n = 1\rangle$

$P(a_r1|D_rU_{r+1}) = 0$; $|\phi_{k_r}\rangle = |..\rangle \ldots |D_r = 2\rangle|U_{r+1} = 1\rangle \ldots |..\rangle$

$P(11\ldots1|U_1U_2\ldots U_n) = q$; $|\phi_+\rangle = |U_1 = 1\rangle|U_2 = 1\rangle \ldots |U_n = 1\rangle$



Let $\mathcal{S}_1 = \{|\phi_{k_r}\rangle\}$
$|\phi_-\rangle \perp \{\mathcal{S}_1\}$ and $|\phi_-\rangle \not\perp |\phi_+\rangle$.
$\therefore \quad |\phi_+\rangle \notin \{\mathcal{S}_1\}$
$|\phi_+\rangle \neq |\phi_-\rangle$, $\therefore$ dim.$(\mathcal{S}_1) = 2^n - 2$

Define: $\mathcal{S}_2 = \{|\phi_-\rangle\} \cup \mathcal{S}_1$.
$|\phi_+\rangle \notin \mathcal{S}_2$, $\therefore$ dim.$(\mathcal{S}_2) = 2^n - 1$.
To satisfy Hardy conditions: $|\psi\rangle \perp \mathcal{S}_2$.

Hardy state $|\psi\rangle$ **is** unique & genuinely entangled

[Rahaman et al., Phys. Rev. A 2014]

Relaxed Hardy type test for genuine multiparty entangled states

$$P(11\ldots1|D_1D_2\ldots D_n)=0$$

$$P(1\ldots\neg1\ldots1|U_1\ldots D_r\ldots U_n)=0$$

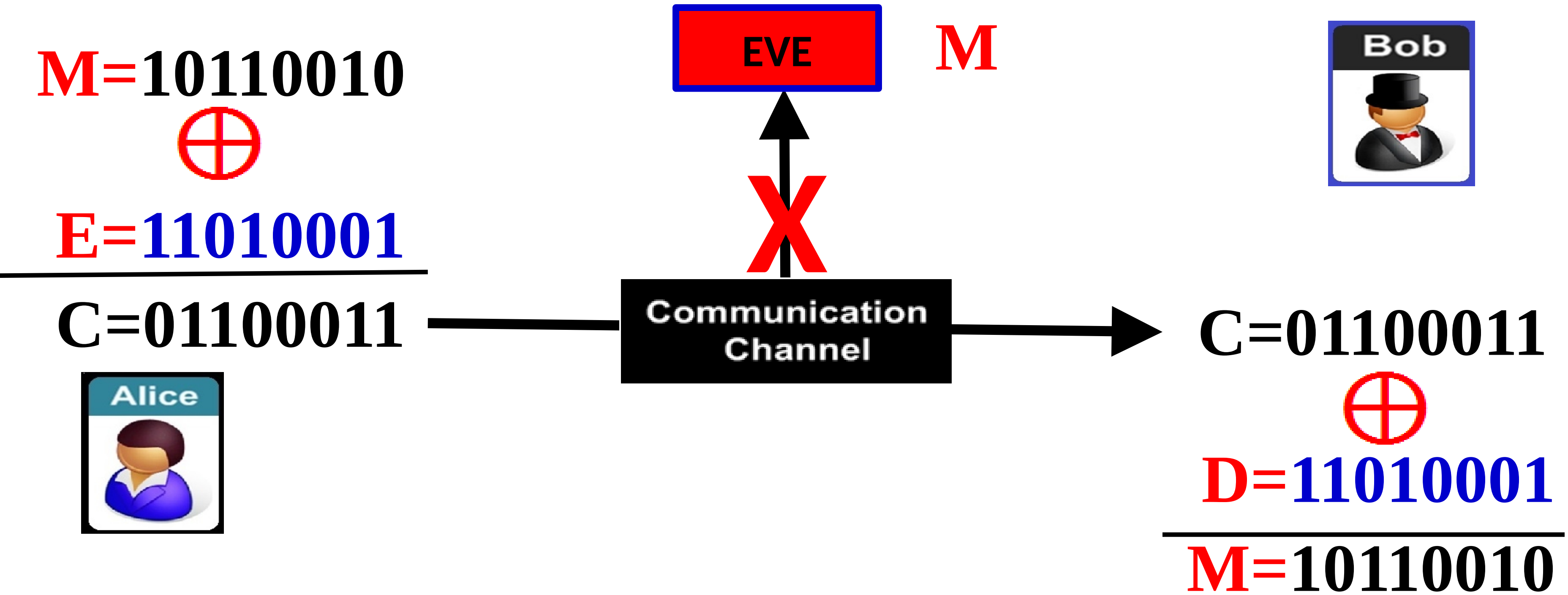
$$P\left(1..1\ldots1\ldots1\middle|U_1\ldots D_i\ldots D_j\ldots U_n\right)=q$$

Only **genuine** multiparty entangled states can satisfy

[S. S. Bhattacharya, A. Roy, A. Mukherjee & R. Rahaman, Phys. Rev. A, 92, 012111 (2015)]

KEY DISTRIBUTION PROTOCOL

Private key cryptography



Difficulties in Private Key

- The key bits cannot be reused for any future protocol.
- Key bits must be delivered in advance, guarded assiduously until used.

Public key cryptosystems-

- W. Diffie and M. Hellman (1976).
- R. Rivest, A. Shamir and L. Adleman (1978) [RSA].

Possible attacks:

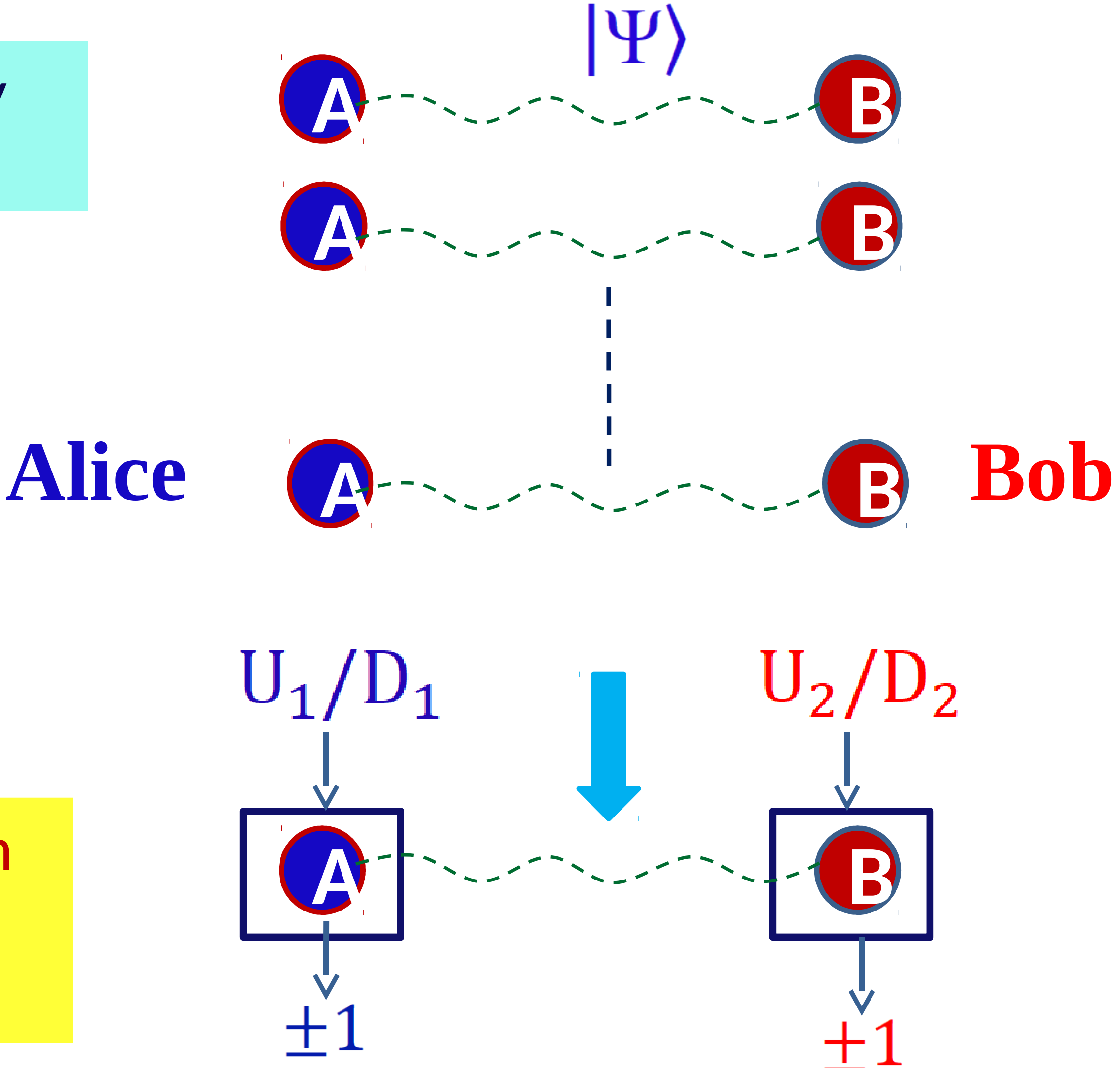
- If you able to factor n.
  - Security based on computational hardness
  - Can be broken by quantum computers!

Possible Solution:-

- Quantum cryptography
  - Security based on Laws of Physics

DI-QKD PROTOCOL [*Rahaman et al. PRA 92, 062304 (2015)*]

Alice & Bob share many copies of Hardy State.



Measures own qubits in the basis chosen randomly from {U,D}.

DI-QKD [*Rahaman et al. PRA 2015*] CONT…

Since, $\langle\Psi|(|D_1 = +1\rangle|D_2 = +1\rangle) \neq 0$

For $|\psi\rangle$; $P(+,+|D_1,D_2) > 0.$

Thus, $P(+,+|U_1,U_2) > 0$

& $P(+,+|D_1,D_2) > 0.$

Remember Hardy's Paradox

$$P(+,+|U_1,U_2) = q > 0$$
$$P(+,+|U_1,D_2) = 0$$
$$P(+,+|D_1,U_2) = 0$$
$$P(-,-|D_1,D_2) = 0$$

\ For (+,+) outcome local inputs are correlated [(U,U) or (D,D)].

Key assign: U → 0 & D → 1.

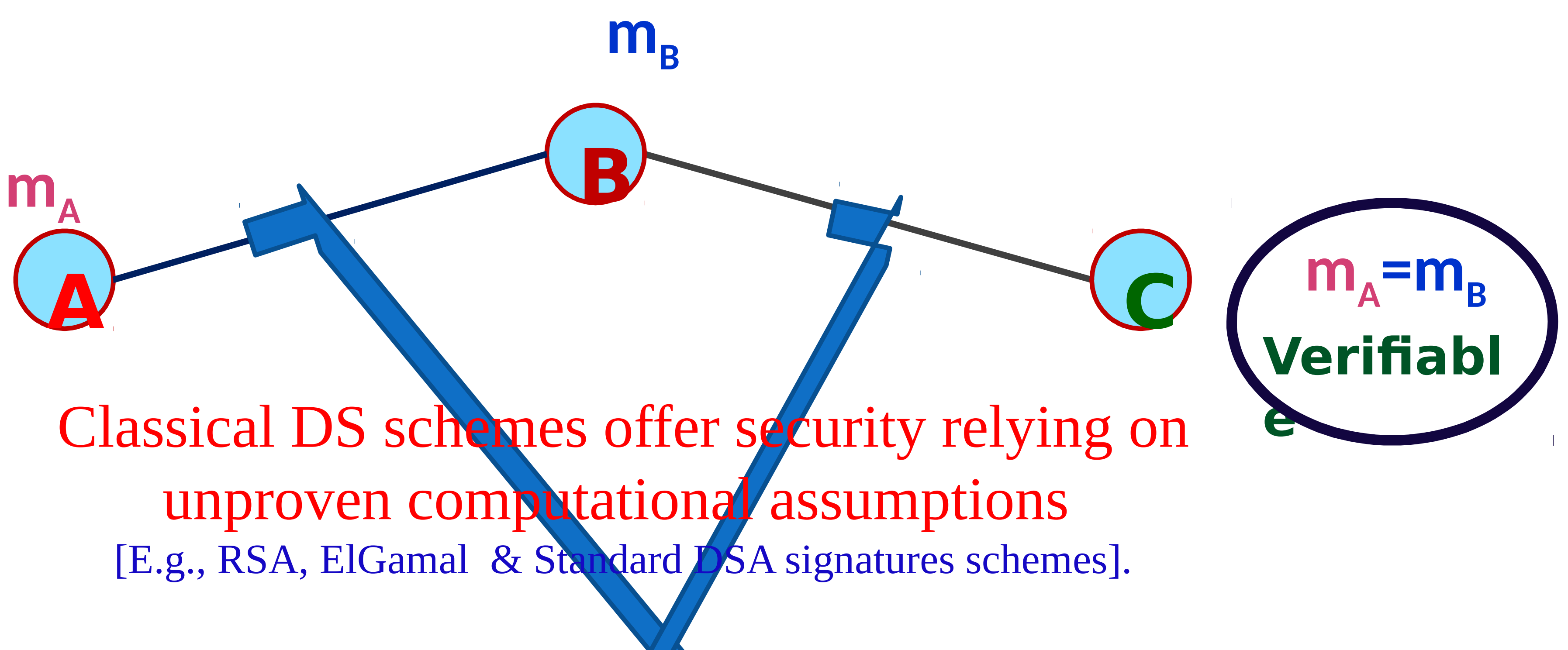
For **q=0.09** (max.), associated Hardy state $|\Psi\rangle$ is device-independent *[Rabelo et al. PRL 2012]*.

⊗ Our QKD also DI in this case.

DIGITAL SIGNATURES (DS) PROBLEM

Digital signature (DS)

- DS allows to send authentic message(s) from one sender to multiple recipients.
- In a DS the known sender cannot deny having sent the message.
- Also, the message was not altered in transit.



Classical DS schemes offer security relying on unproven computational assumptions

[E.g., RSA, ElGamal & Standard DSA signatures schemes].

QUANTUM DIGITAL SIGNATURES(QDS) PROTOCOL

Existing QDS schemes

- In 2001, Gottesman & Chuang, arXiv:quant-ph/0105032.

- Experimental demonstration with coherent states:

  (i) E. Andersson et. al., PRA 2006.

  (ii) P. J. Clarke et. al., Nature Com. 2012.

- QDS schemes without Quantum Memory:

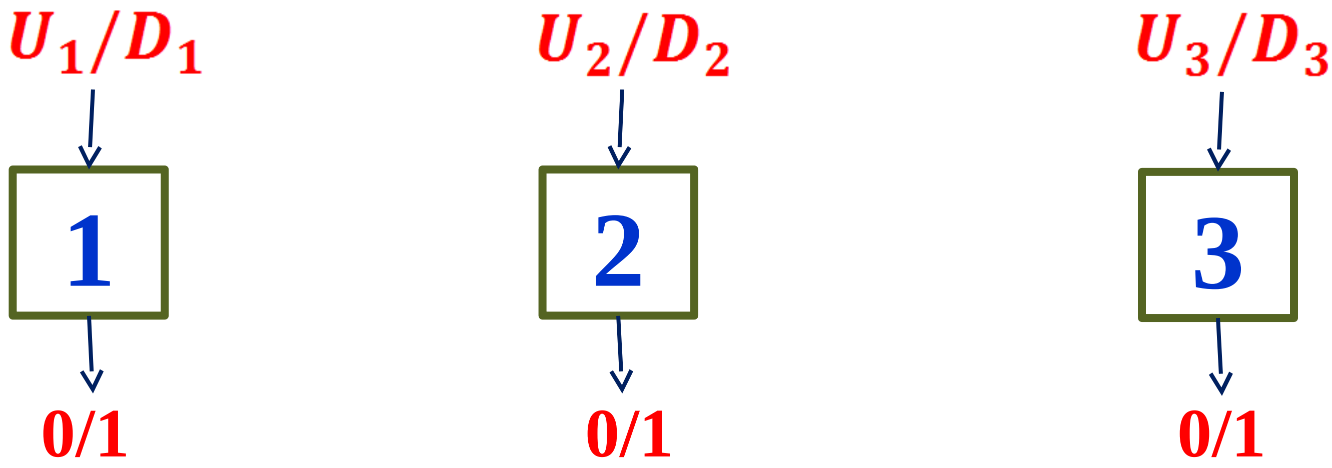
  (i) V. Dunjko et. al., PRL 2014.

  (ii) R. J. Collins et. al., PRL 2014.

THREE QUBITS HARDY PARADOX

Consider a system $H = H_1 \otimes H_2 \otimes H_3$

Dim.(H)=2x2x2=8



$$P(000|U_1U_2U_3) = q > 0$$

$$P(00|U_iD_j) = 0 \quad i \neq j$$

$$P(111|D_1D_2D_3) = 0$$

Again cannot be satisfied by any LR theory

For 3-qubits system: **Dim.(H)=2x2x2=8.**

Let us assign:

$$P(000|U_1U_2U_3) = q \quad |\phi_+\rangle = |0\rangle|0\rangle|0\rangle$$

$$P\left(00\middle|U_iD_j\right) = 0 \quad \left|\phi_{k_r}\right\rangle = |..\rangle|0_i\rangle|0_j'\rangle$$

$$P(111|D_1D_2D_3) = 0 \quad |\phi_-\rangle = |1'\rangle|1'\rangle|1'\rangle$$

Let $S_1 = \left\{\backslash\phi_{k_r}\right\} \cup \{|\phi_-\}.$

Then $dim.\,(S_1) = 2^3 - 1$

Hardy state $|\Psi\rangle \perp S_1$

Hardy state |❓⚕ **is** unique & genuinely entangled

[Rahaman et al., Phys. Rev. A 2014].

3-QUBIT HARDY STATE

Probability of success **q= 0.0181938.**

$$P(000|U_1U_2U_3) = q > 0$$
$$P(00|U_iD_j) = 0 \quad i \neq j$$
$$P(111|D_1D_2D_3) = 0$$

In this case also, $U_1 \cong U_2 \cong U_3 \cong U$ & $D_1 \cong D_2 \cong D_3 \cong D$

Hardy State: $|\Psi\rangle = c_0|000\rangle + c_1P[|001\rangle] + c_2P[|011\rangle] + c_3|111\rangle$

$$c_0 = \frac{|\alpha|^3|\beta|^3}{\sqrt{1-|\alpha|^6}}, c_1 = \frac{-\beta|\alpha|^4|\beta|}{\sqrt{1-|\alpha|^6}}, c_2 = \frac{\beta^2|\alpha|^5}{|\beta|\sqrt{1-|\alpha|^6}}, c_3 = \frac{\beta^3\sqrt{1-|\alpha|^6}}{|\beta|^3}$$

$$|0'\rangle = \alpha|0\rangle + \beta|1\rangle \;\&\; |1'\rangle = \beta^*|0\rangle - \alpha^*|1\rangle$$

Device Independent Hardy Test (3-qubit):-

For q= 0.0181938, state is equivalent to $|\Psi\rangle_{123} = |\psi_{\max}\rangle_{123} \otimes |\eta_{1'2'3'}\rangle$.

Quantum digital signatures protocol

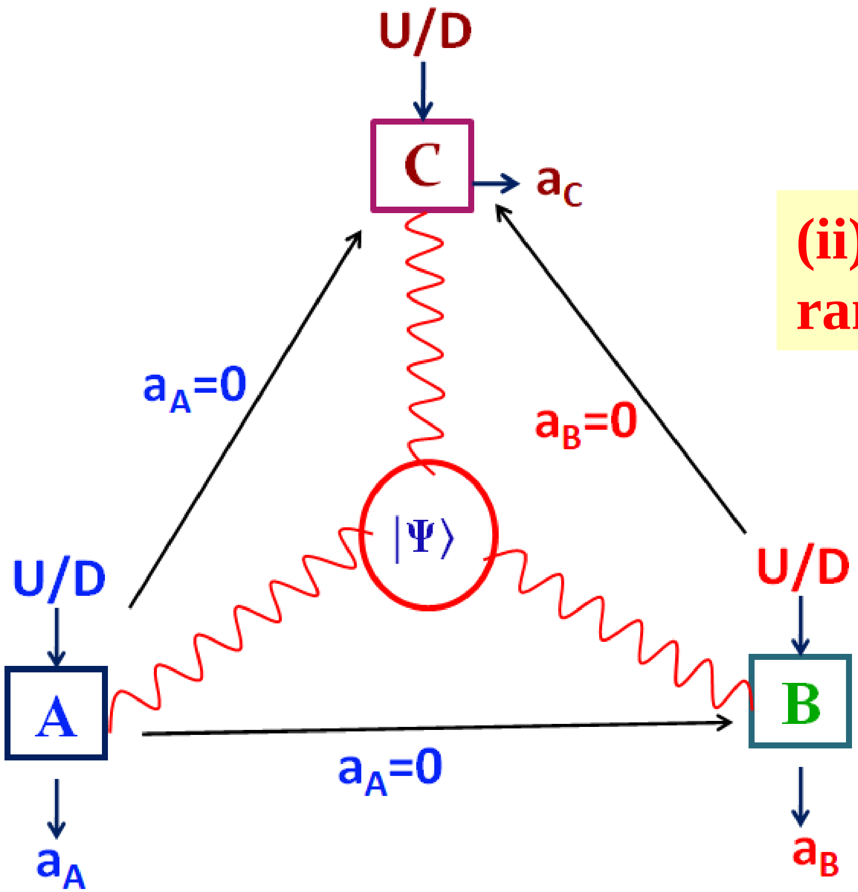
- **S1. Distribution of resources:** '**A**' prepares and shares a large number of 3-qubits Hardy state $|\psi\rangle$ **with B and C.**

$$|\Psi\rangle = c_0|000\rangle + c_1 P[|001\rangle] + c_2 P[|011\rangle] + c_3|111\rangle$$

$$c_0 = \frac{|\alpha|^3|\beta|^3}{\sqrt{1-|\alpha|^6}}, c_1 = \frac{-\beta|\alpha|^4|\beta|}{\sqrt{1-|\alpha|^6}}, c_2 = \frac{\beta^2|\alpha|^5}{|\beta|\sqrt{1-|\alpha|^6}}, c_3 = \frac{\beta^3\sqrt{1-|\alpha|^6}}{|\beta|^3}$$

$$|0'\rangle = \alpha|0\rangle + \beta|1\rangle \;\&\; |1'\rangle = \beta^*|0\rangle - \alpha^*|1\rangle$$

S2. Actions: (i) **A** measures all his qubits in the message basis he want to convey. *[U for m=0 and D for m=1].*



P(000|UUU)=q
P(00|UD)=0
P(111|DDD)=0

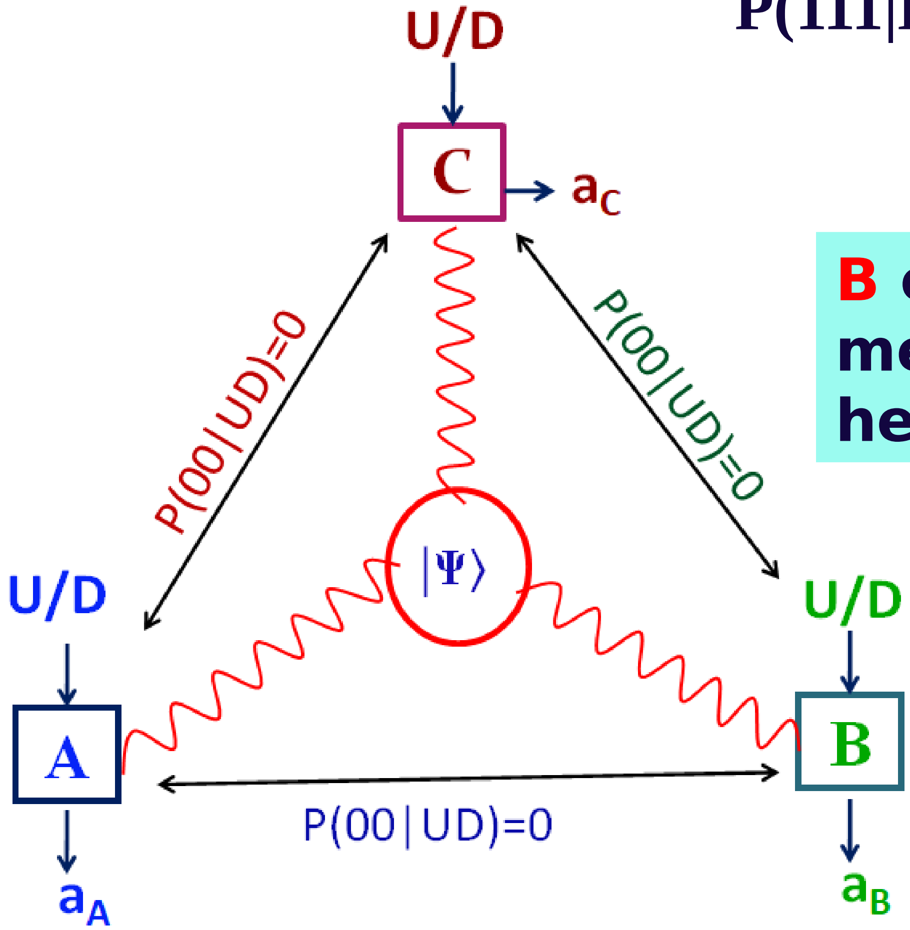
(ii) B(C) measures all his qubits in random basis U/D.

(iii) A sends the list of runs to B & C when a_A=0.

(iv) B sends the list of runs to C when a_B=0.

They discards the runs when A gets outcome 1.

$P(000|UUU)=q$
$P(00|UD)=0$
$P(111|DDD)=0$



$P(00|DD)>0$
$P(00|UU)>0$
$P(00|DU)=0$
$P(00|UD)=0$

B can easily figure out the message basis [m] of A with help of Hardy's conditions.

C can also easily verify B's claim with help of Hardy's conditions.

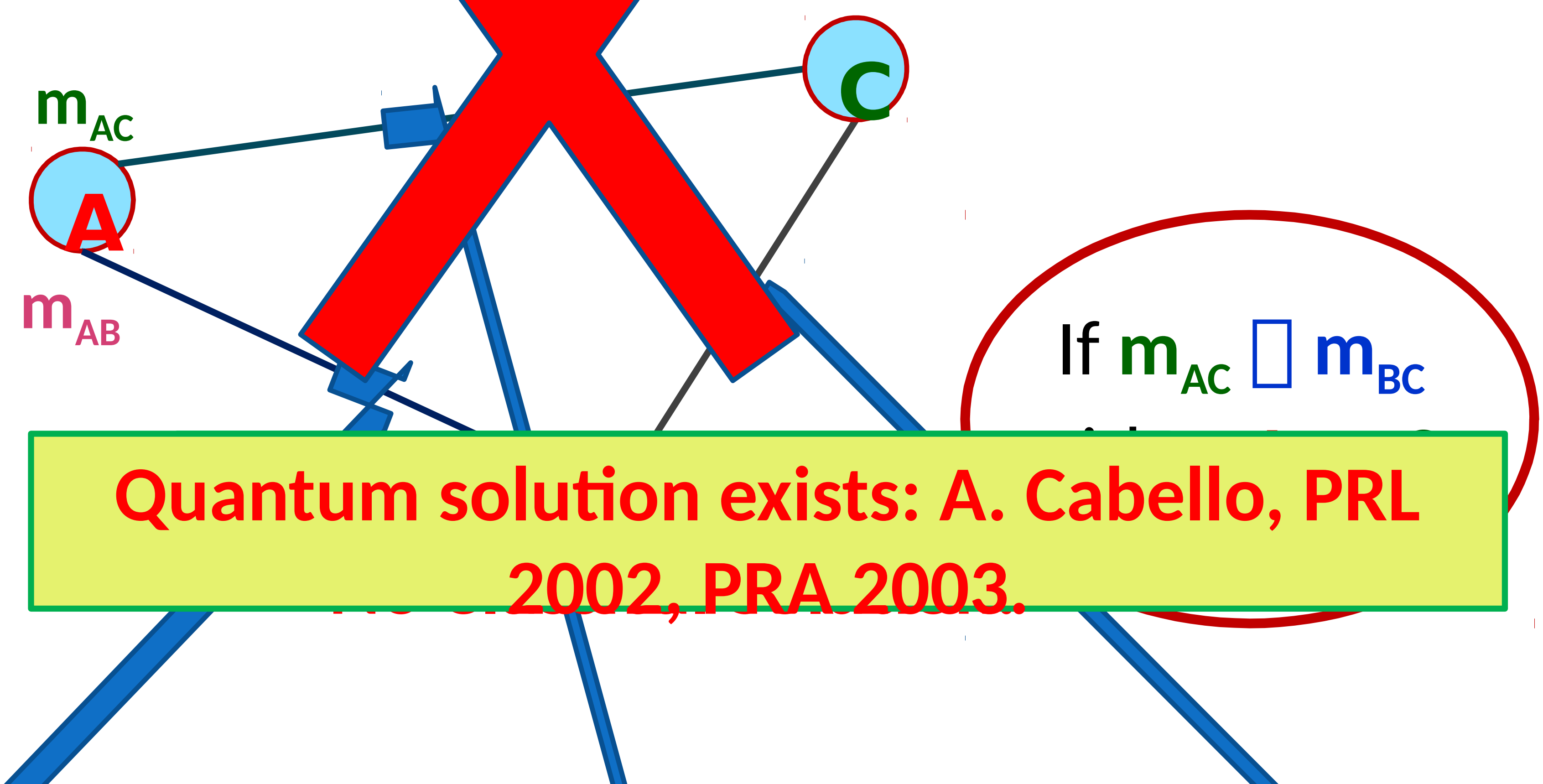
LIAR DETECTION (LD) PROBLEM

Liar Detection

'C' receives a message from A in two different paths:

(i) Directly … A [messa… m_{AC}]

(ii) Via B [mes… m…



Quantum solution exists: A. Cabello, PRL 2002, PRA 2003.

Quantum solution for Liar Detection (QLD) Problem

- **S1. Distribution of resources:**

  (i) ‘C’ shares a large number ($\approx 6N$) of maximally entangled states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|uu\rangle + |u^\perp u^\perp\rangle]$$

  (ii) Conversion from $|\Phi^+\rangle$ *to* $|\psi^H\rangle$ between ‘C and A’ and ‘C and B’.

$$(\mathbb{U}^{c1} \otimes \mathbb{I}^2)|u\rangle_c|\Phi^+\rangle_{12} = \frac{1}{\sqrt{2}}|u\rangle_c|\psi^H\rangle_{12} + \frac{1}{\sqrt{2}}|u^\perp\rangle_c|\psi'\rangle_{12},$$

$$|\psi^H\rangle = x_{00}|u\rangle_1|u\rangle_2 + x_{01}\left(|u\rangle_1|u^\perp\rangle_2 + |u^\perp\rangle_1|u\rangle_2\right) + x_{11}|u^\perp\rangle_1|u^\perp\rangle_2,$$

$$|\psi'\rangle = x_{01}^*|uu\rangle - x_{00}^*|uu^\perp\rangle + x_{11}^*|u^\perp u\rangle - x_{01}^*|u^\perp u^\perp\rangle.$$

$$\mathbb{U}|uu\rangle = x_{00}|uu\rangle + x_{01}|uu^\perp\rangle + x_{01}^*|u^\perp u\rangle + x_{11}^*|u^\perp u^\perp\rangle,$$
$$\mathbb{U}|uu^\perp\rangle = x_{01}|uu\rangle + x_{11}|uu^\perp\rangle - x_{00}^*|u^\perp u\rangle - x_{01}^*|u^\perp u^\perp\rangle$$

Quantum solution for Liar Detection (QLD)

- **S1. Distribution of resources:**

(iii) Conversion from $|\Phi^+\rangle$ *to* $|\psi^H\rangle$ between '**A** and **B**'.

C applies a two outcome joint measurement **{M, I−M}** on her two qubits.

$$M = |\psi^{H^*}\rangle\langle\psi^{H^*}|$$

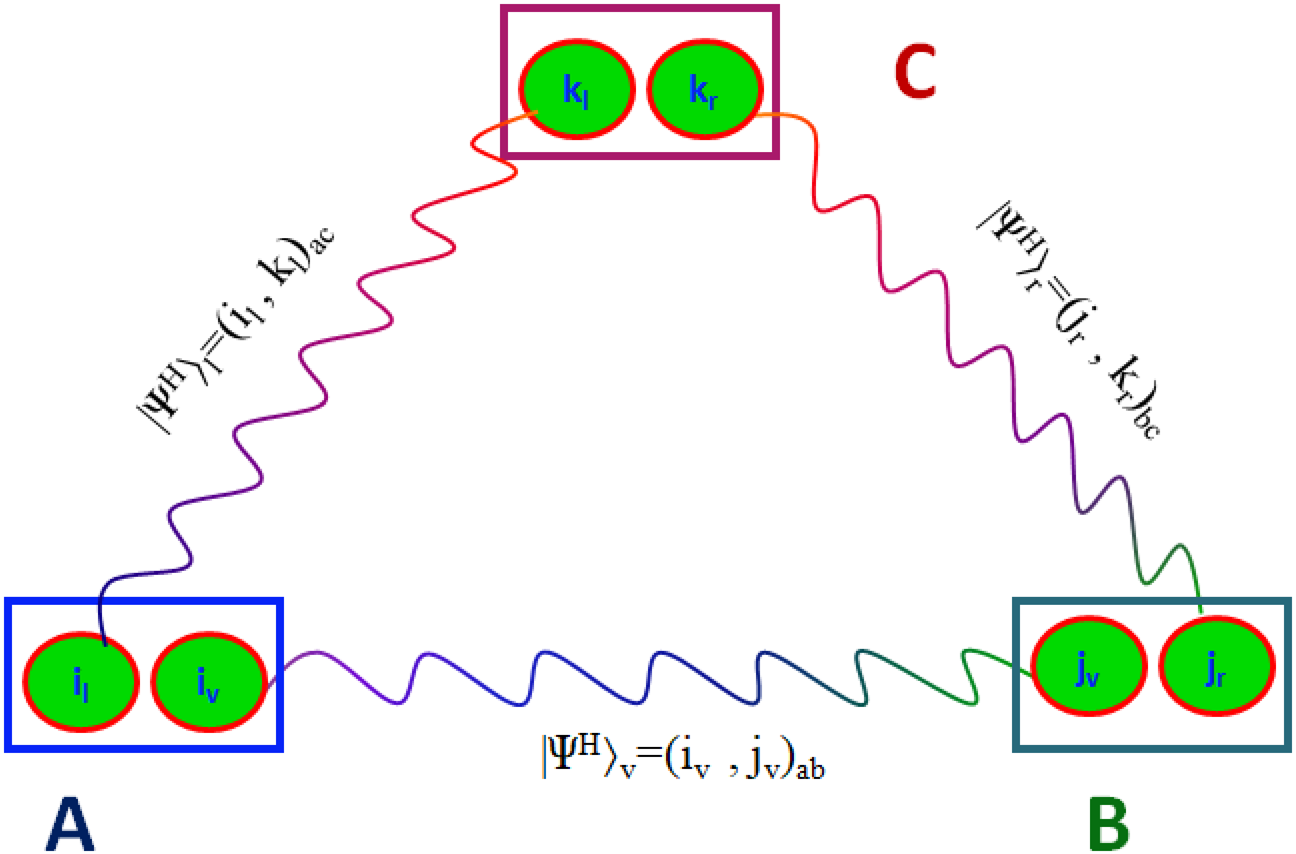
$$|\psi^{H^*}\rangle = x_{00}^*|uu\rangle + x_{01}^*\left(|uu^\perp\rangle + |u^\perp u\rangle\right) + x_{11}^*|u^\perp u^\perp\rangle.$$

$$(M^{13} \otimes \mathbb{I}^{24})|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}|\psi^{H^*}\rangle_{13} \otimes |\psi^H\rangle_{24}.$$

(iv) '**C**' prepares a list $\mathbf{L_B = \{(j_v, k_v)_{AB}\}_{v=1}^{t}}$ for **'B'** and sends to him.

Neither **B** nor **C** reveal the inform of $\mathbf{L_B}$ to **A.**

After a successful distribution of qubits



each party shares ≈N copies of Hardy state with others.

QLD Protocol …………

S2. Actions on qubits distributed by C :

(i) Action by 'A': **A** measures all his qubits in the message basis he want to convey.

[Measurement U for the message m=0 and D for m=1].

(ii) Action by 'B': (a) **B** measures qubits of $\mathbf{L_B}$ in random bases U/D.

B can easily figure out the message basis [$\mathbf{m_{AB}}$] of **A** by comparing his measurement data and the results of **A** with Hardy's conditions.

(b) **B** measures rest of his qubits in the message basis and sends the results to **C**.

QLD Protocol …………
[S2. Actions on qubits distributed by C]

(iii) Action by '**C**': **C** measures all his qubits in the random bases **U/D**.

(a) '**C**' can easily figure out the message basis [$\mathbf{m}_{AC}$] of **A** by comparing his measurement data and the results of **A** with Hardy's conditions.

(b) Similarly, '**C**' can find out the message basis [$\mathbf{m}_{BC}$] of **B** with comparing the data and Hardy's conditions.

$$P(11 \mid D_1 D_2) = 0$$

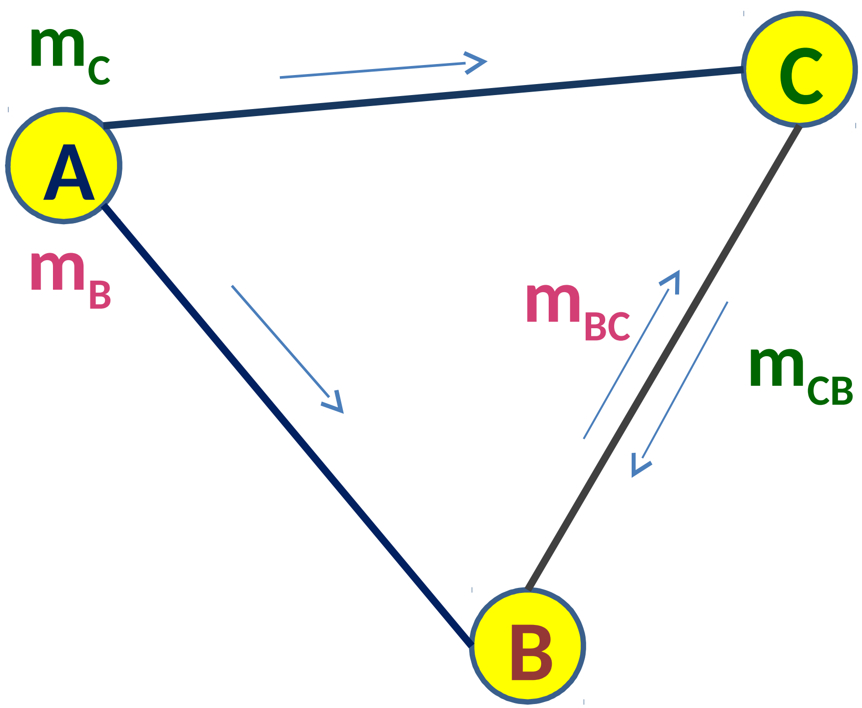
$$P(00 \mid D_1 U_2) = 0$$

$$P(00 \mid U_1 D_2) = 0$$

$$P(00 \mid U_1 U_2) = q > 0$$

Byzantine Agreement (BA)

Generals of the Byzantine Army communicating with each other



If $m_{CB} = m_{BC}$, all are loyal.

The generals must reach a consensus among themselves whether to attack or retreat based on the messages exchanged.

But some generals can be traitors; they may send conflicting messages to the other generals.

Byzantine Agreement

The solution to the problem must allow

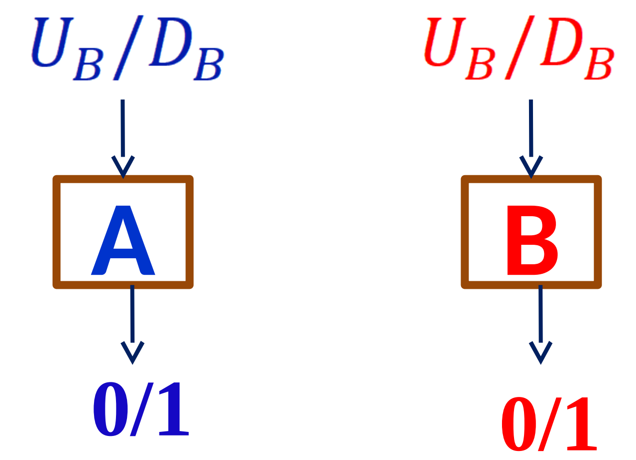
- (i) all the loyal generals to agree upon a common plan of action.
- (ii) if the commanding general (A) is loyal then all the loyal generals must obey the order (s)he sends.
- No Classical solution *[Fitzi et. al. CRYPTO 2001]*

QUANTUM RANDOM NUMBER GENERATION

Randomness of a measurement's outcomes:

Randomness of the measurement outcomes (a,b) for the inputs (x,y) estimated by the min-entropy function
[R. Koenig et al., IEEE Trans. Inf. Theory, 09]

$$H_\infty(a,b|x,y) \equiv -\log_2[\mathrm{Max}_{\{a,b\}} P(a,b|x,y)]$$



$U \overset{\times}{\times\circ} 0$ & $D \overset{\times}{\times\circ} 1$

Device-independent Case: Used semidefinite programming (SDP)

Minimize: $\mathrm{Max}_{\{a,b\}} P(a,b|U_A,U_B)$

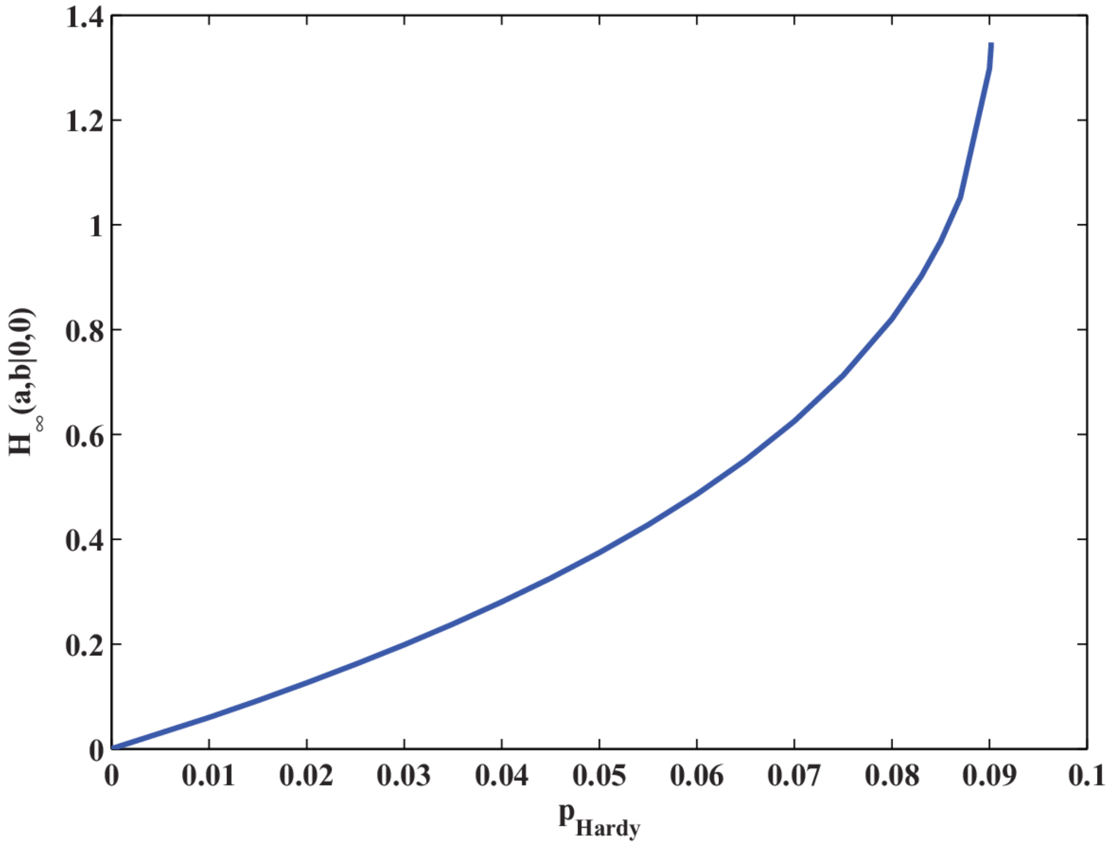
Subject to: $\Delta_{Hardy} = [\Delta_{ij}] \geq 0,$ where $\Delta_{ij} = \mathrm{Tr}\left(E_i^\dagger E_j \rho\right)$

$$P(0,0|U_A,U_B) = 0,$$
$$P(0,1|D_A,U_B) = 0,$$
$$P(1,0|U_A,U_B) = 0,$$
$$P(0,0|D_A,D_B) = p_{Hardy}.$$

$$E_i, E_j \in \{I, A_{a|x}, B_{b|y}, A_{a|x}B_{b|y}\}$$

POVM $\{A_{0|x}, A_{1|x}\} \rightarrow X \in \{U_A, D_A\}$

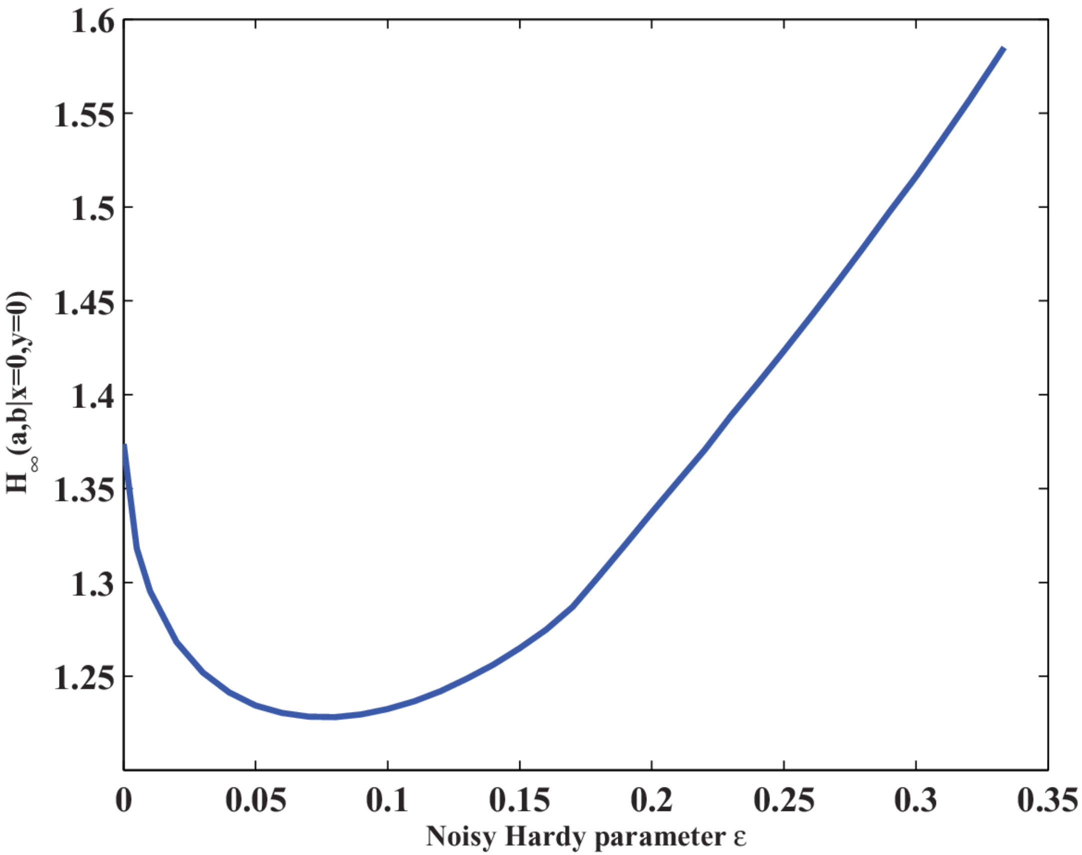
A lower bound on min-entropy $H_\infty(a,b|0,0)$
as a function of Hardy's parameter $q = p_{Hardy}$.



$$
\begin{aligned}
P(0,0|U_A,U_B) &= 0,\\
P(0,1|D_A,U_B) &= 0,\\
P(1,0|U_A,U_B) &= 0,\\
P(0,0|D_A,D_B) &= p_{Hardy}.
\end{aligned}
$$

Maximal randomness can reach up to 1.35 if the corresponding Hardy probability obtains its maximal value.

Noisy Case: A lower bound on min-entropy $H_\infty(a,b|0,0)$ as a function noise parameter ϵ.



SDP Scheme

Minimize: $\mathrm{Max}_{\{a,b\}} P(a,b|U_A,U_B)$

Subject to: $\Delta_{\mathrm{noisyHardy}} \geq 0,$

$$P(0,0|U_A,U_B) \leq \epsilon,$$
$$P(0,1|D_A,U_B) \leq \epsilon,$$
$$P(1,0|U_A,U_B) \leq \epsilon,$$
$$P(0,0|D_A,D_B) \geq q \geq 3\epsilon.$$

Maximal randomness can reach up to 1.58 for ϵ=0.333.

Cabello scenario: A lower bound on min-entropy

SDP Scheme

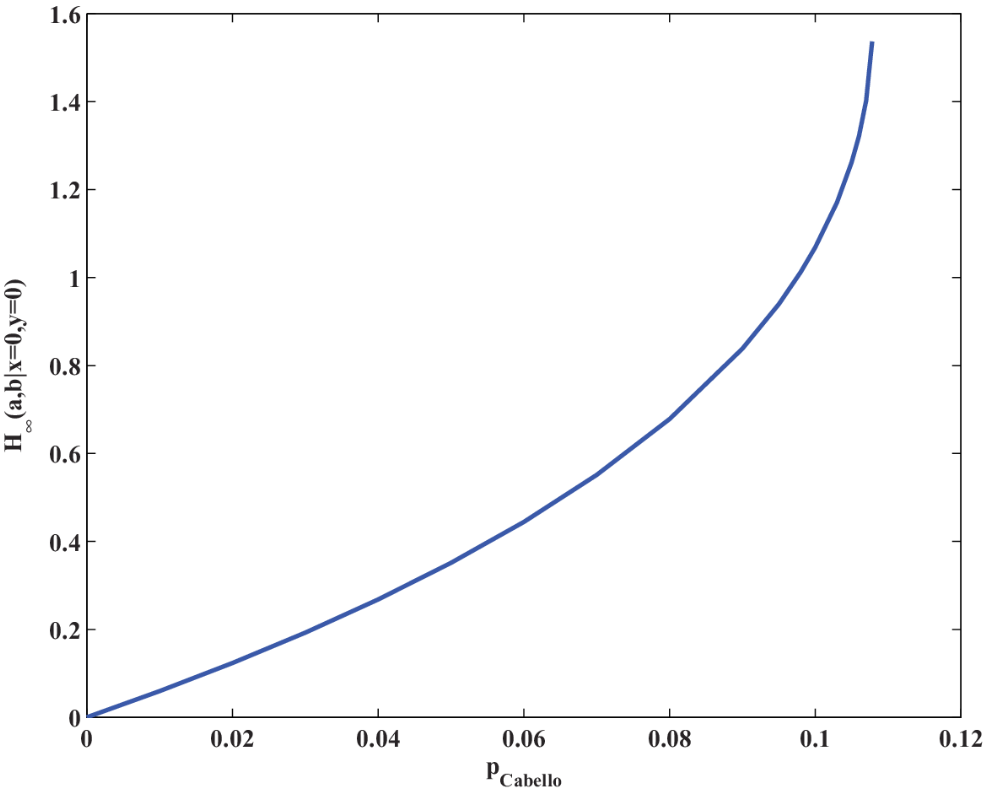
Minimize: $\mathrm{Max}_{\{a,b\}} P(a, b|U_A, U_B)$

Subject to: $\Delta_{\mathrm{Cabello}} = [\Delta_{ij}] \geq 0,$

$P(0,1|D_A, U_B) = 0,$

$P(1,0|U_A, U_B) = 0,$

$P(0,0|D_A, D_B) - P(0,0|U_A, U_B) = p.$



Maximal randomness can reach up to 1.56 when Cabello parameter (p) reaches its maximal value 0.10784.

Semi-Device Independent scenario

SDP Scheme

Minimize: $\text{Max}_{\{a,b\}} P(b|U_A, a, U_B)$

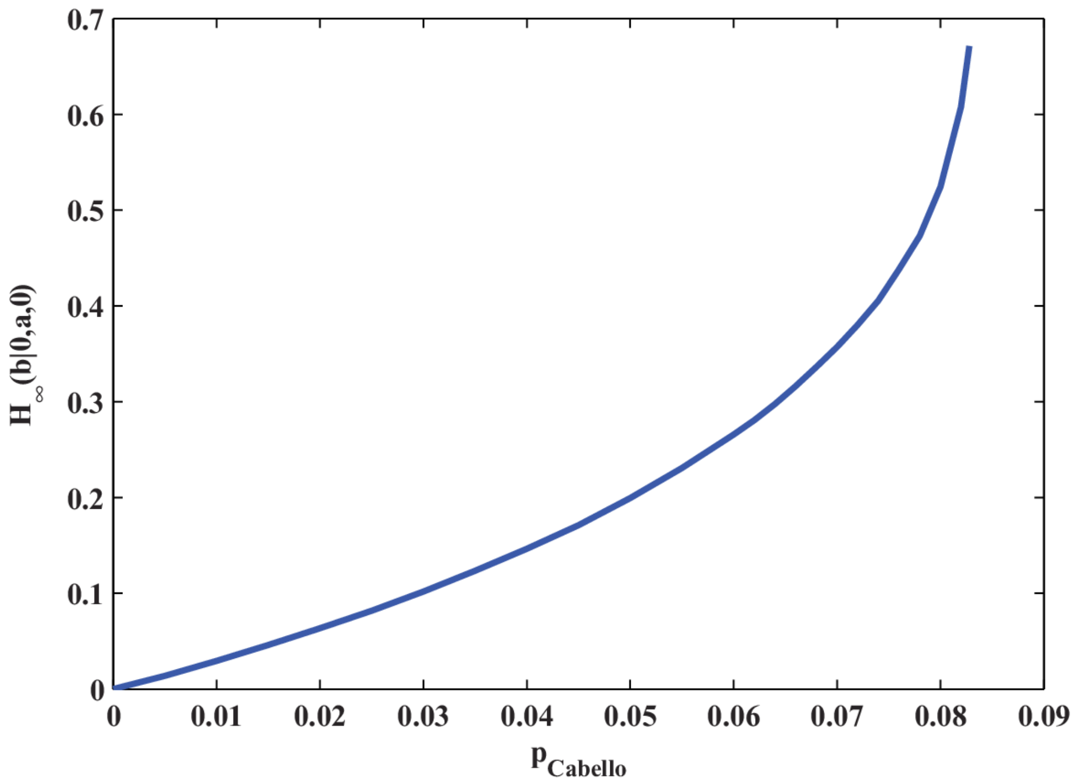
Subject to: $\Delta_{\text{Cabello}} = [\Delta_{ij}] \geq 0,$

$P(0,1|D_A, U_B) = 0,$

$P(1,0|U_A, U_B) = 0,$

$P(a|x) = P(a|x, y) = \frac{1}{2};\ x \in \{U, D\},$

$P(0,0|D_A, D_B) - P(0,0|U_A, U_B) = p.$



Maximal randomness can reach up to 0.68. Other existing protocols can generate a maximum 0.23 bit randomness.

CONCLUSIONS

- Proposed generalized Hardy type test for detection of multiparty entanglement.
- Based on Hardy correlations, we have proposed Device-Independent quantum protocols for
  - Key Distribution.
  - Liar Detection & Byzantine Agreement
  - Random Number Generator
  - Quantum Digital Signatures etc.

References:-

- ***R. Rahaman***, M. G. Parker, P. Mironowicz & M. Pawlowski, *'Device-independent quantum key distribution based on measurement inputs'*, Phys. Rev. A, 92, 062304(2015).
- ***R. Rahaman***, M. Wiesniak & M. Zukowski, *'Quantum Byzantine agreement via Hardy correlations and entanglement swapping'*, Phys. Rev. A, 92, 042302(2015).
- H.-W. Li, M. Pawłowski, ***R. Rahaman***, G. Guo & Z.-F. Han, *'Device- and semi–device-independent random numbers based on noninequality paradox'*, Phys. Rev. A 92, 022327(2015).
- S. S. Bhattacharya, A. Roy, A. Mukherjee & ***R. Rahaman***, *'All-versus-nothing violation of local realism from the Hardy paradox under no-signaling'*, Phys. Rev. A 92, 012111(2015).
- ***R. Rahaman***, M. Wiesniak & M. Zukowski, *'True Multipartite Entanglement Hardy Test'*, Phys. Rev. A, 90, 062338(2014).
- ***R. Rahaman***, *'Quantum digital signatures based non-locality test'* (Under Preparation).

Thank You