Self-testing of binary Pauli measurements requiring neither entanglement nor any dimensional restriction

Shiladitya
QFort,NCKU,NCTS

NONLOCALITY, FOUNDATIONS & INFORMATION

Workshop on QST/Taiwan; 24/08-27/08

Self-testing of binary Pauli measurements requiring neither entanglement nor any dimensional restriction

Phys. Rev. A **103**, 062604 – Published 4 June 2021

Ananda G. Maity,[1,*] Shiladitya Mal,[2,3,†] Chellasamy Jebarathinam,[3,4,‡] and A. S. Majumdar[1,§]

[1] *S. N. Bose National Centre for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700 106, India*
[2] *Harish-Chandra Research Institute, HBNI, Chhatnag Road, Jhunsi, Allahabad 211 019, India*
[3] *Department of Physics and Center for Quantum Frontiers of Research and Technology (QFort), National Cheng Kung University, Tainan 701, Taiwan*
[4] *Center for Theoretical Physics, Polish Academy of Sciences, Aleja Lotników 32/46, 02-668 Warsaw, Poland*

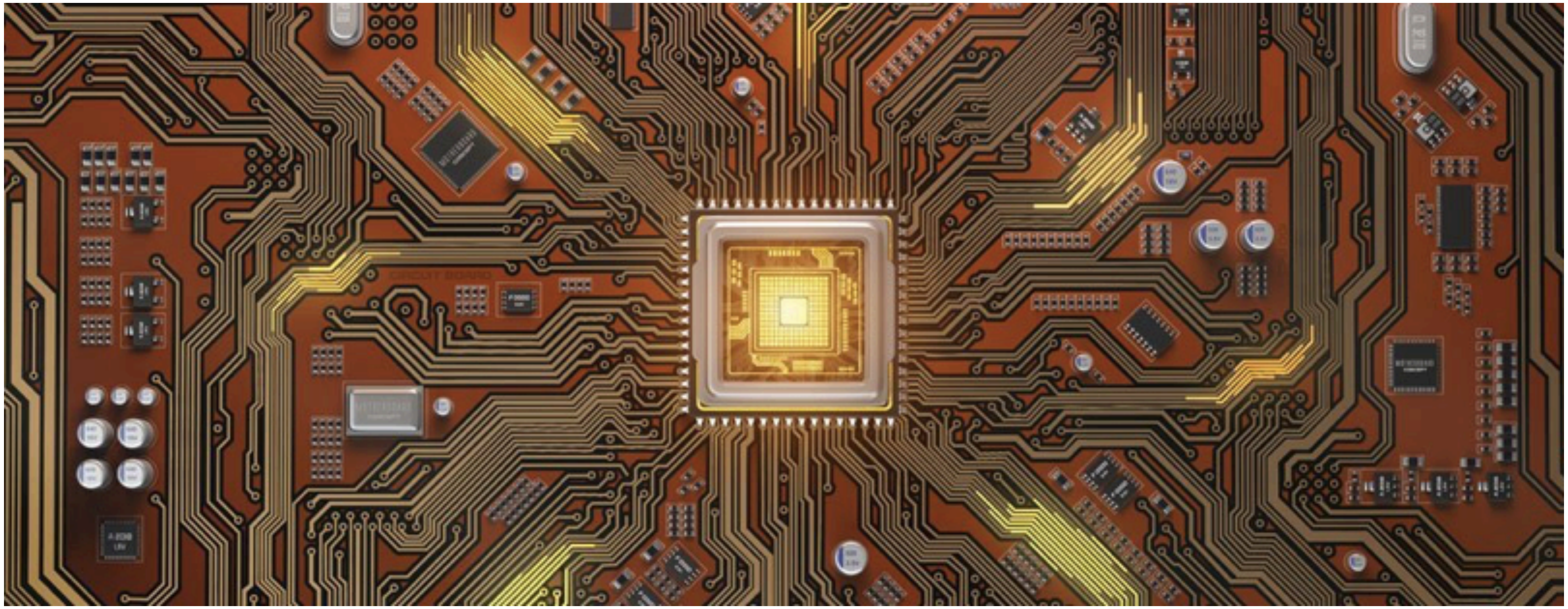
Outline

Motivation

Results

Conclusion

QUANTUM TECHNOLOGY



Certification

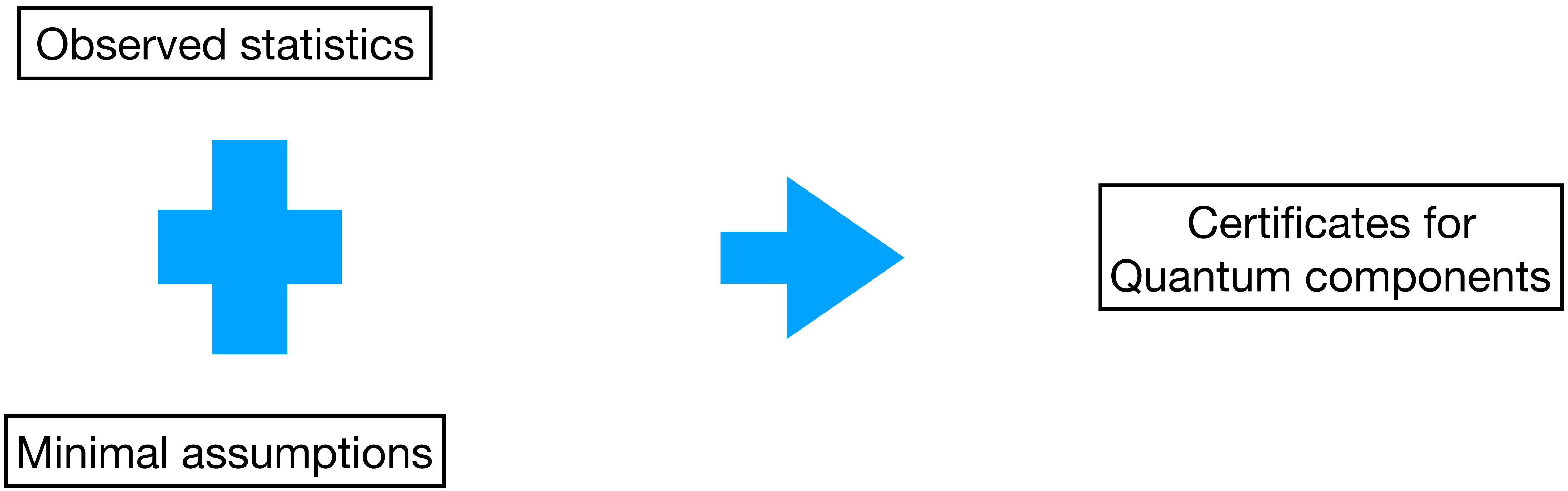
Verification

Self-checking

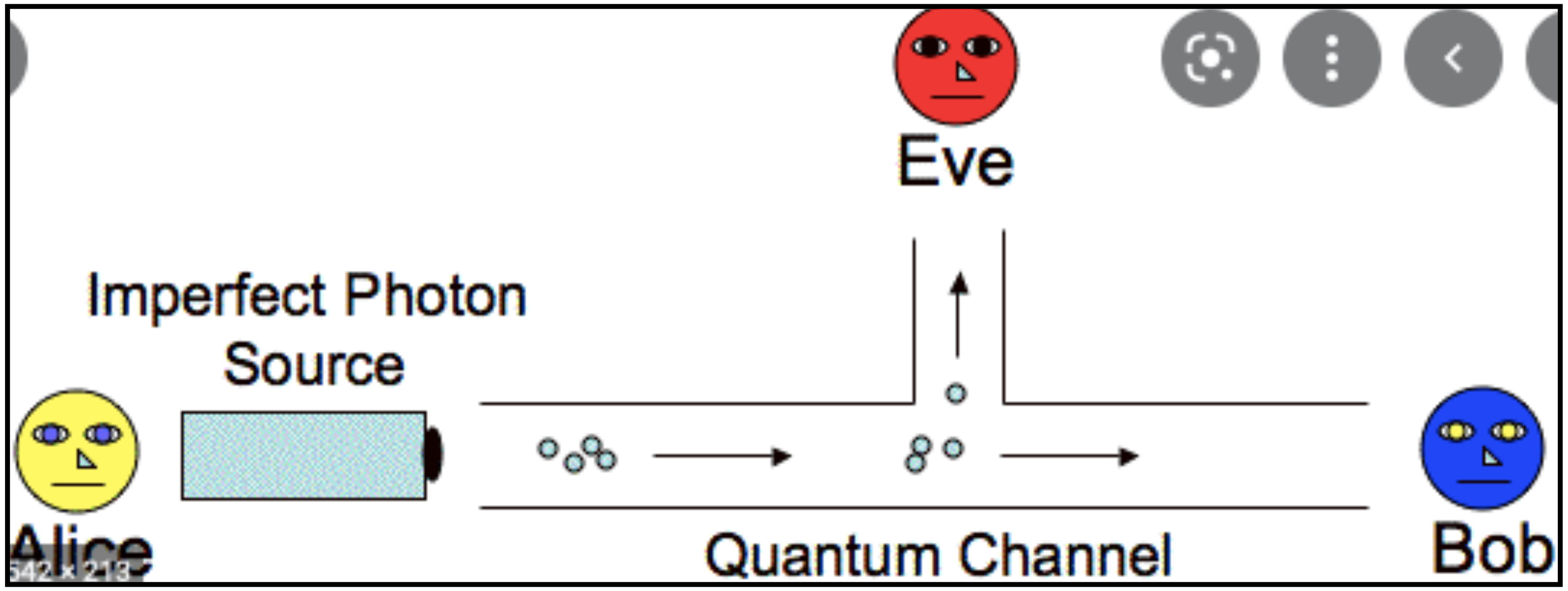
Self-testing

Blind tomography

Self-testing



BB84 is not secure if source is not trusted



$$\boxed{\rho_{AB} = \frac{1}{4}(|00\rangle\langle 00|_z + |11\rangle\langle 11|_z) \otimes (|00\rangle\langle 00|_x + |11\rangle\langle 11|_x).}$$

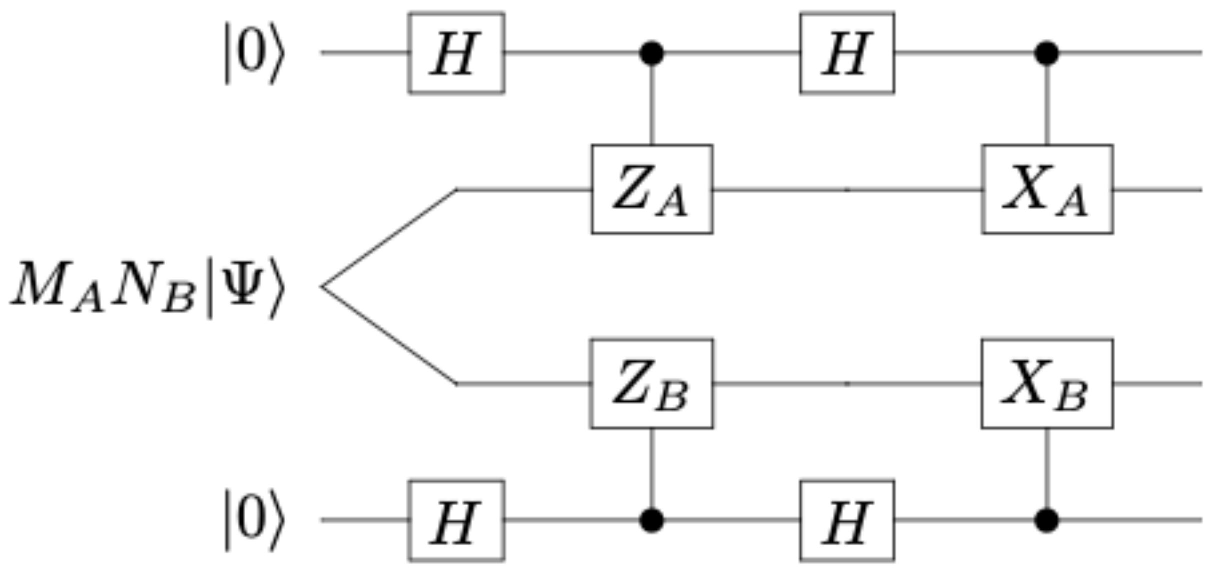
D. Mayers and A. Yao, *Proceedings of the 39th* FOCS (IEEE Computer Society, Washington, DC, 1998), p. 503.

D. Mayers and A. Yao, Quantum Inf. Comput. 4, 273 (2004).

A. Ac´ın, N. Gisin, Ll. Masanes, Phys.Rev.Lett.97,120405 (2006).

$M_A \in \{X_A, Z_A\}$

$N_B \in \{X_B, Z_B, D_B\}$



Theorem 4.2. *Consider five unknown unitary operators* $\{X_A, Z_A; X_B, Z_B, D_B\}$ *binary outcomes labeled* ± 1 *and assumed to fulfill* $[M_A, N_B] = 0$*: if*

$$\begin{aligned}
\langle\Psi|Z_A Z_B|\Psi\rangle = \langle\Psi|X_A X_B|\Psi\rangle &= 1 \\
\langle\Psi|X_A Z_B|\Psi\rangle = \langle\Psi|Z_A X_B|\Psi\rangle &= 0 \\
\langle\Psi|Z_A D_B|\Psi\rangle = \langle\Psi|X_A D_B|\Psi\rangle &= 1/\sqrt{2}
\end{aligned}$$

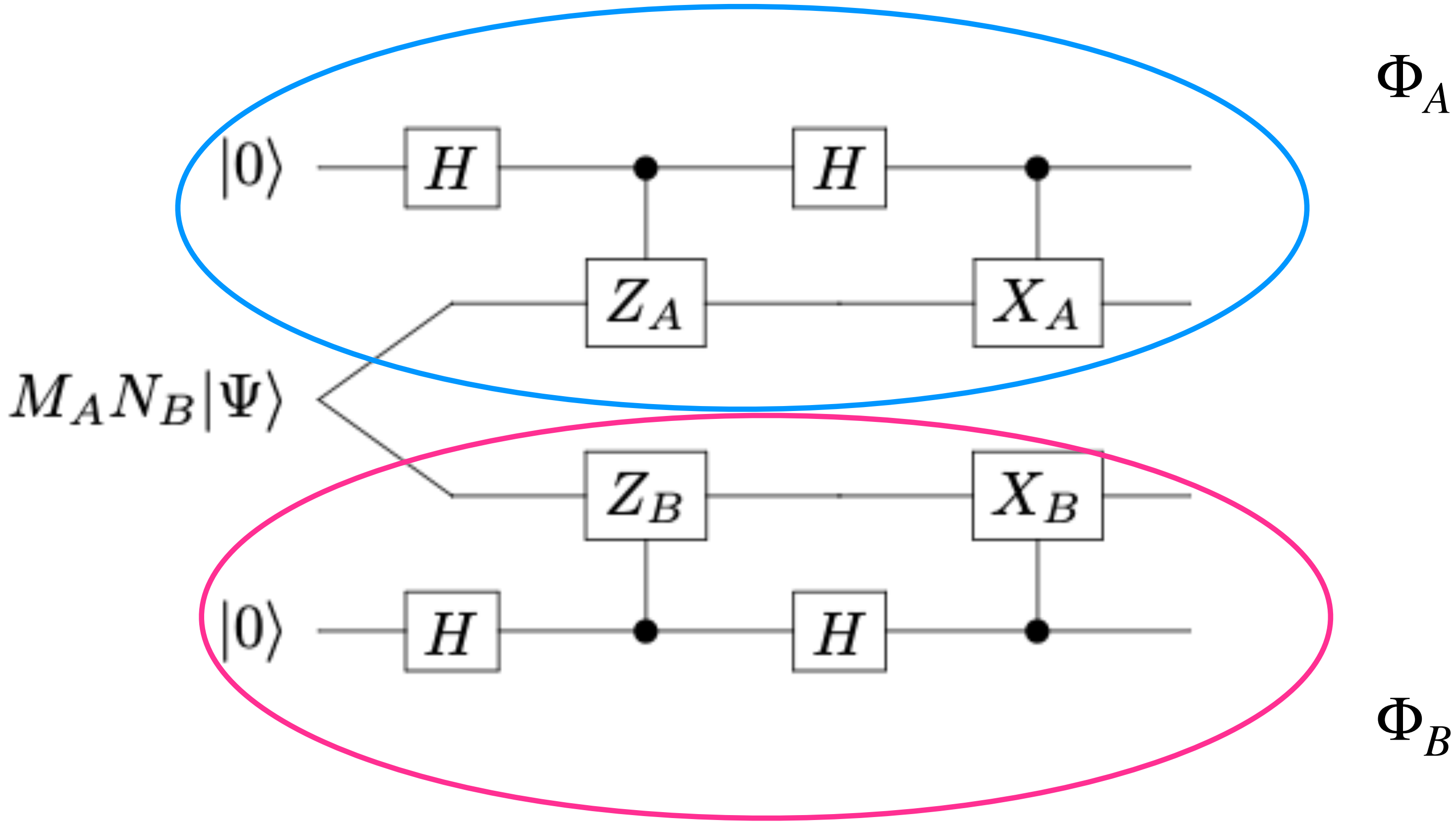
then there exist a local isometry $\Phi = \Phi_A \otimes \Phi_B$ *such that*

$$\begin{aligned}
\Phi|\Psi\rangle_{AB}|00\rangle_{A'B'} &= |\mathrm{junk}\rangle_{AB}|\Phi^+\rangle_{A'B'}, \\
\Phi\, M_A N_B|\Psi\rangle_{AB}|00\rangle_{A'B'} &= |\mathrm{junk}\rangle_{AB}\left(\sigma_m \otimes \sigma_n|\Phi^+\rangle_{A'B'}\right).
\end{aligned}$$

D. Mayers and A. Yao, *Proceedings of the 39th* FOCS (IEEE Computer Society, Washington, DC, 1998), p. 503.

$M_A \in \{X_A, Z_A\}$

$N_B \in \{X_B, Z_B, D_B\}$



Theorem 4.2. *Consider five unknown unitary operators* $\{X_A, Z_A; X_B, Z_B, D_B\}$ *binary outcomes labeled* ± 1 *and assumed to fulfill* $[M_A, N_B] = 0$*: if*

$$\begin{aligned}
\langle\Psi|Z_A Z_B|\Psi\rangle = \langle\Psi|X_A X_B|\Psi\rangle &= 1 \\
\langle\Psi|X_A Z_B|\Psi\rangle = \langle\Psi|Z_A X_B|\Psi\rangle &= 0 \\
\langle\Psi|Z_A D_B|\Psi\rangle = \langle\Psi|X_A D_B|\Psi\rangle &= 1/\sqrt{2}
\end{aligned}$$

then there exist a local isometry $\Phi = \Phi_A \otimes \Phi_B$ *such that*

$$\begin{aligned}
\Phi|\Psi\rangle_{AB}|00\rangle_{A'B'} &= |\text{junk}\rangle_{AB}\left|\Phi^+\right\rangle_{A'B'}, \\
\Phi\, M_A N_B|\Psi\rangle_{AB}|00\rangle_{A'B'} &= |\text{junk}\rangle_{AB}\left(\sigma_m \otimes \sigma_n\left|\Phi^+\right\rangle_{A'B'}\right).
\end{aligned}$$

Self-testing based on Bell theorem

Maximally entangled state

pure bipartite entangled states

Graph state

A. Coladangelo, K. T. Goh, and V. Scarani, Nature Communications 8, 15485 EP (2017).

I. Supic, J. Bowles, Quantum 4, 337 (2020).

Self-testing based on dimension witness

Pure state

PVM

POVM

A. Tavakoli, J. Kaniewski, T. Vertesi, D. Rosset, and N. Brunner, Phys. Rev. A 98, 062307 (2018).

Self-testing based on contextually

Three-dimensional states

measurements

K. Bharti, M. Ray, A. Varvitsiotis, N. A. Warsi, A. Cabello, and L. C. Kwek, Phys. Rev. Lett. 122, 250403 (2019).

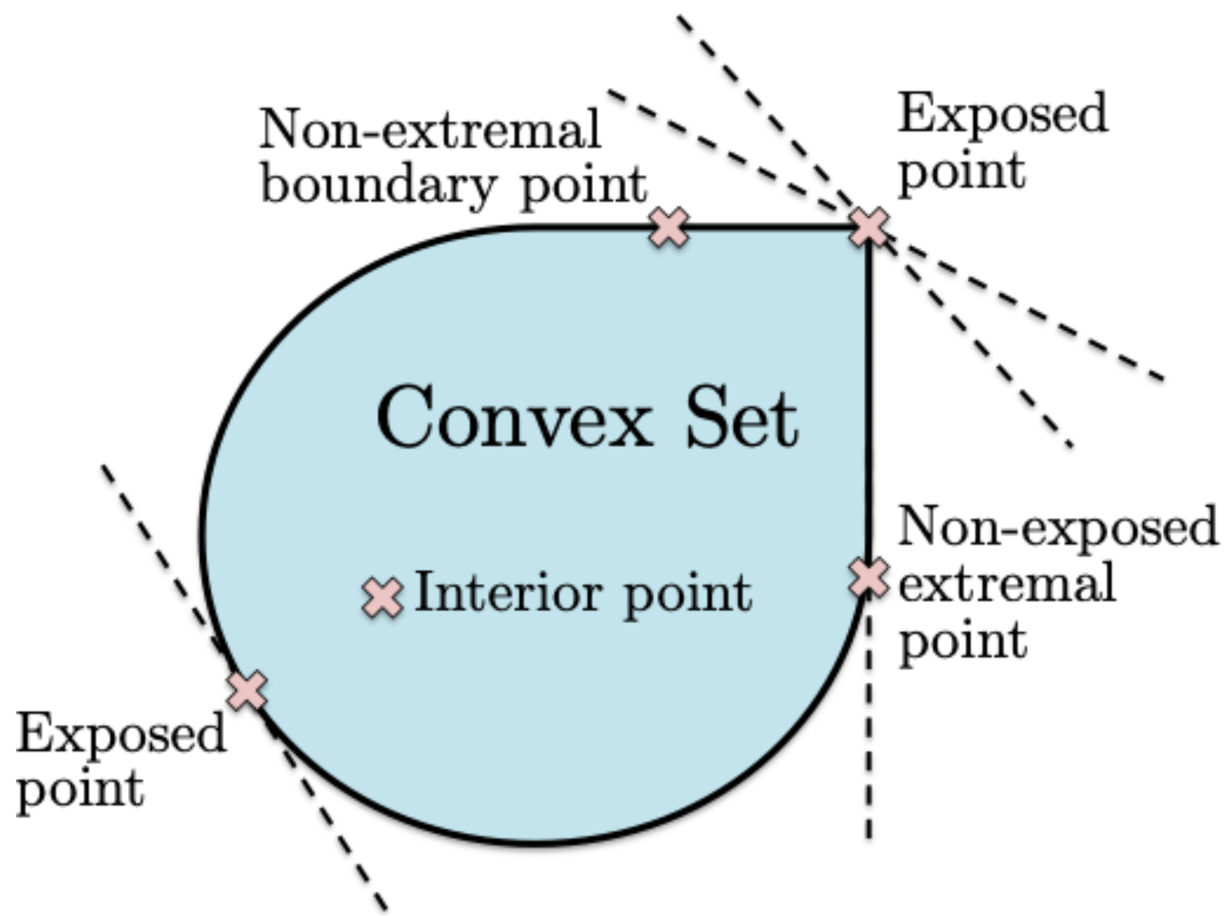
D. Saha, R. Santos, and R. Augusiak, Quantum 4, 302 (2020).

Editors' Suggestion

Geometry of the set of quantum correlations

Koon Tong Goh, Jędrzej Kaniewski, Elie Wolfe, Tamás Vértesi, Xingyao Wu, Yu Cai, Yeong-Cherng Liang, and Valerio Scarani

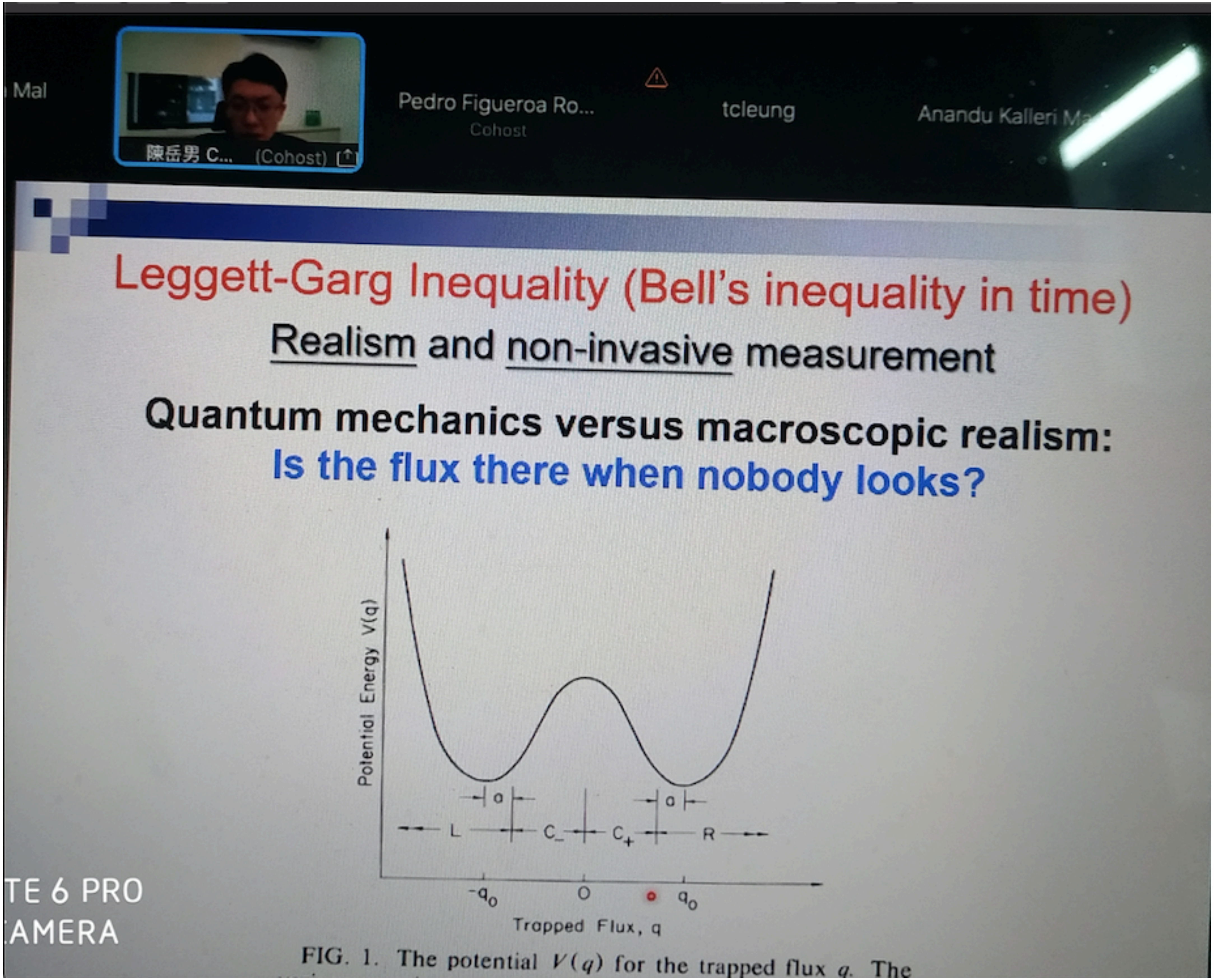
Phys. Rev. A **97**, 022104 – Published 7 February 2018



Limitations that the geometry of the quantum set imposes on the task of self-testing.

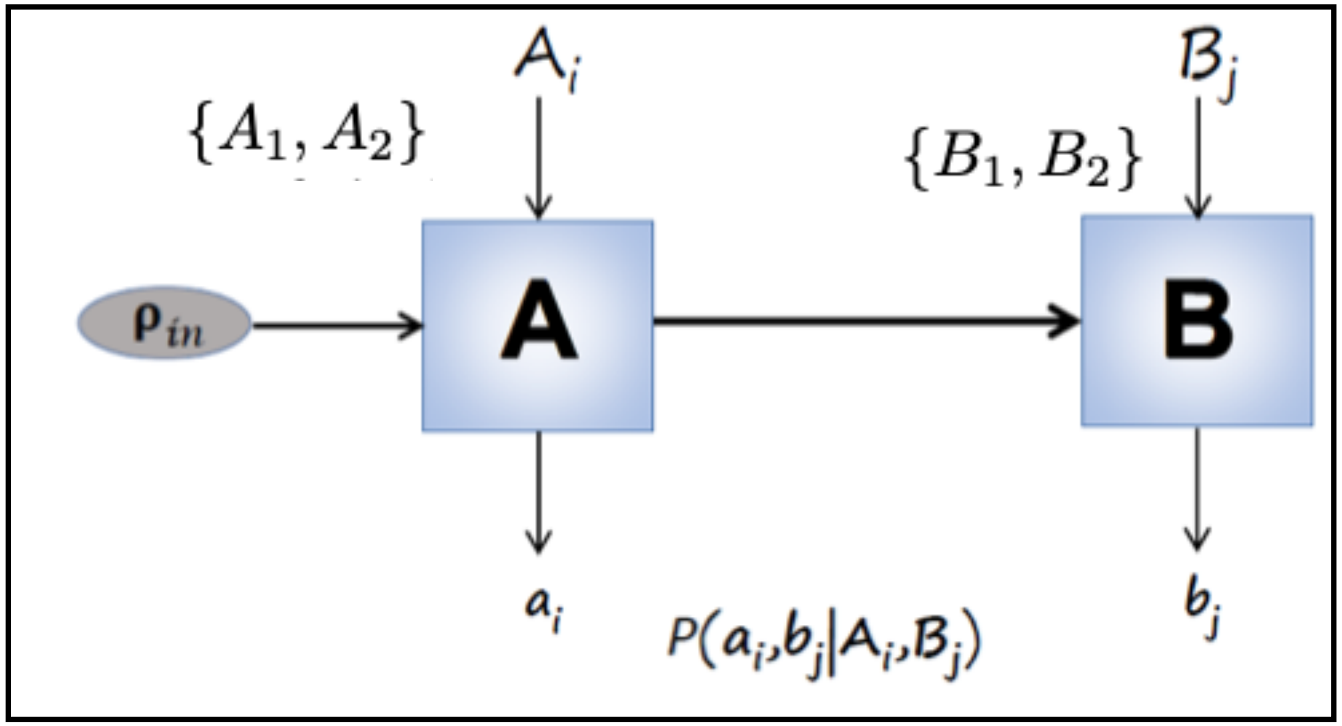
Self-testing measurement in the context of temporal correlation

Exploiting violation of Leggett- Garg inequality



A. J. Leggett and A. Garg, Phys. Rev. Lett. 54, 857 (1985).

C. Emary, N.Lambert, and F.Nori, Rep.Prog.Phys.77,016001(2014).



$$P(a_i, b_j \mid A_i, B_j) = P(a_i \mid A_i) P(b_j \mid a_i, A_i, B_j)$$

Quantum correlation:

$$\mathrm{Tr}\left[\mathcal{P}_{a_i|A_i}\rho_{in}\right] \mathrm{Tr}\left[\mathcal{P}_{b_j|B_j} \frac{\mathcal{P}_{a_i|A_i}\rho_{in}\mathcal{P}^{\dagger}_{a_i|A_i}}{\mathrm{Tr}\left[\mathcal{P}_{a_i|A_i}\rho_{in}\mathcal{P}^{\dagger}_{a_i|A_i}\right]}\right]$$

$$\mathcal{C}_{ij} = \sum_{a_i, b_j} (-1)^{a_i \oplus b_j} P(a_i, b_j \mid A_i, B_j)$$

$$\boxed{\mathcal{K}_4 = C_{11} + C_{21} + C_{22} - C_{12} \leq 2.}$$

Derivation of LGI from operational assumptions

$$\boxed{NSIT \wedge Predictability \Rightarrow LGI.}$$

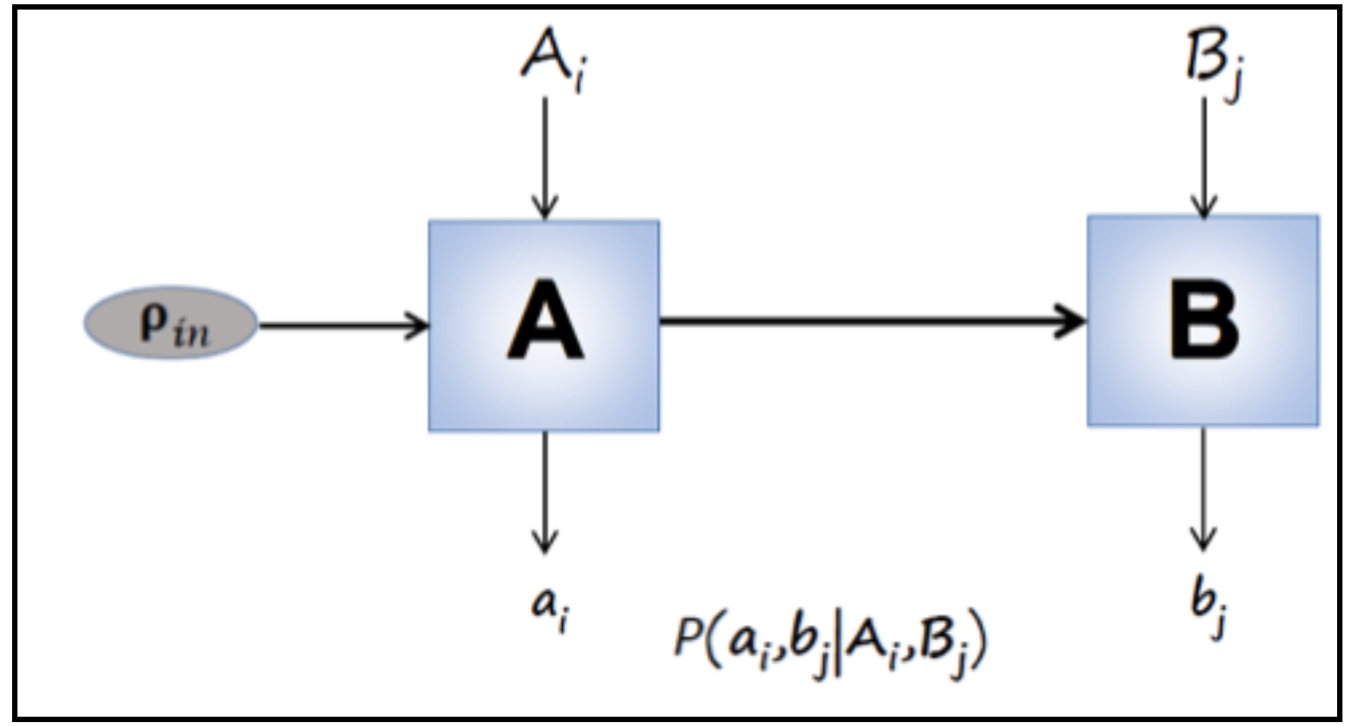
Predictability : A model is said to be predictable if the joint statistics $P(a_i, b_j \mid A_i, B_j) \in \{0,1\} \; \forall a_i, b_j, A_i, B_j$

NSIT : NSIT is defined by the condition that measurement statistics is not influenced by the earlier measurements. Mathematically, $P(b_j \mid B_j) = P(b_j \mid A_i, B_j) \; \forall A_i, B_j, b_j$.

$$\Downarrow$$

$$\boxed{\mathcal{K}_4 = C_{11} + C_{21} + C_{22} - C_{12} \leq 2.}$$

LG test under the Assumption



Assumption : *The measurement device of Alice acts only on the input state prepared by the experimenter, and the measurement device of Bob acts only on the state produced by Alice's measurement, with both returning only the respective post-measurement states.*

Qubit measurements

$$P(a_i, b_j \mid A_i, B_j) = \frac{1}{4}(1+(-1)^{a_i}\hat{a}_i.\hat{n})(1+(-1)^{a_i+b_j}\hat{a}_i.\hat{b_j}).$$

$$\Rightarrow \quad \mathcal{C}_{ij} = \hat{a}_i.\hat{b_j}.$$

$$\boxed{\mathcal{K}_4 = \hat{a}_1.\hat{b_1} + \hat{a}_2.\hat{b_1} + \hat{a}_2.\hat{b_2} - \hat{a}_1.\hat{b_2} \leq 2.}$$

$$\boxed{\begin{aligned} A_1^{\text{ideal}} &= \sigma_z, \\ A_2^{\text{ideal}} &= \sigma_x, \\ B_1^{\text{ideal}} &= \frac{\sigma_x + \sigma_z}{\sqrt{2}}, \\ B_2^{\text{ideal}} &= \frac{\sigma_x - \sigma_z}{\sqrt{2}}, \end{aligned}}$$

Maximal violation =>

$$|\hat{a}_i.\hat{b_j}| = \frac{1}{\sqrt{2}}.$$

NSIT implies :

$$(-1)^{a_1+b_1}\hat{a}_1.\hat{b_1} = (-1)^{a_2+b_1}\hat{a}_2.\hat{b_1} = (-1)^{a_1+b_2}\hat{a}_1.\hat{b_2} = (-1)^{a_2+b_2}\hat{a}_2.\hat{b_2}.$$

Relaxing dimensional restriction

Lemma 2. *The maximum violation of LGI (i.e,* $\mathcal{K}_4^{max} = 2\sqrt{2}$*) implies implementation of the block diagonal measurement, i.e.,* $A_1 = \oplus_i \sigma_z^i, A_2 = \oplus_i \sigma_x^i, B_1 = \oplus_j (\sigma_x^j + \sigma_z^j)/\sqrt{2}, B_2 = \oplus_j (\sigma_x^j - \sigma_z^j)/\sqrt{2}$.

This Allows an isometry

$$\Phi : \mathcal{H}^{\bar{d}} \to \mathcal{C}^2 \otimes \mathcal{H}^d$$

$$\boxed{\begin{aligned} \Phi\,|2m,0\rangle &\to |2m,0\rangle \\ \Phi\,|2m+1,0\rangle &\to |2m,1\rangle \end{aligned}}$$

Theorem 1. *If $\mathcal{K}_4^{max} = 2\sqrt{2}$ is observed in LG-test under Assumption 1, with the measurements of Alice, A_i acting on H_d, producing the post measurement states $\left\{ \frac{\mathcal{P}_{a_i|A_i}\rho_{in}\mathcal{P}^\dagger_{a_i|A_i}}{Tr\left[\mathcal{P}_{a_i|A_i}\rho_{in}\mathcal{P}^\dagger_{a_i|A_i}\right]} \right\}_a$, and the measurements of Bob B_j acting on these post measurement states, then there exists an isometry $\Phi : \mathcal{H}^d \to \mathcal{C}^2 \otimes \mathcal{H}^d$ such that*

$$\Phi \left(B_j \frac{\mathcal{P}_{a_i|A_i}\rho_{in}\mathcal{P}^\dagger_{a_i|A_i}}{Tr\left[\mathcal{P}_{a_i|A_i}\rho_{in}\mathcal{P}^\dagger_{a_i|A_i}\right]} \right) \Phi^\dagger$$
$$= B_j^{\mathtt{ideal}} \left|\psi^{\mathtt{ideal}}_{a|A_i}\right\rangle \left\langle \psi^{\mathtt{ideal}}_{a|A_i}\right| \otimes |\mathtt{junk}\rangle\langle \mathtt{junk}|$$

where $\left|\psi^{\mathtt{ideal}}_{a|A_i}\right\rangle$ are the eigenstates of Alice's ideal measurements and $B_j^{\mathtt{ideal}}$ are Bob's ideal measurements given by Eq. (4) respectively, and $|\mathtt{junk}\rangle$ is a junk state acting on $\mathcal{H}^d$.

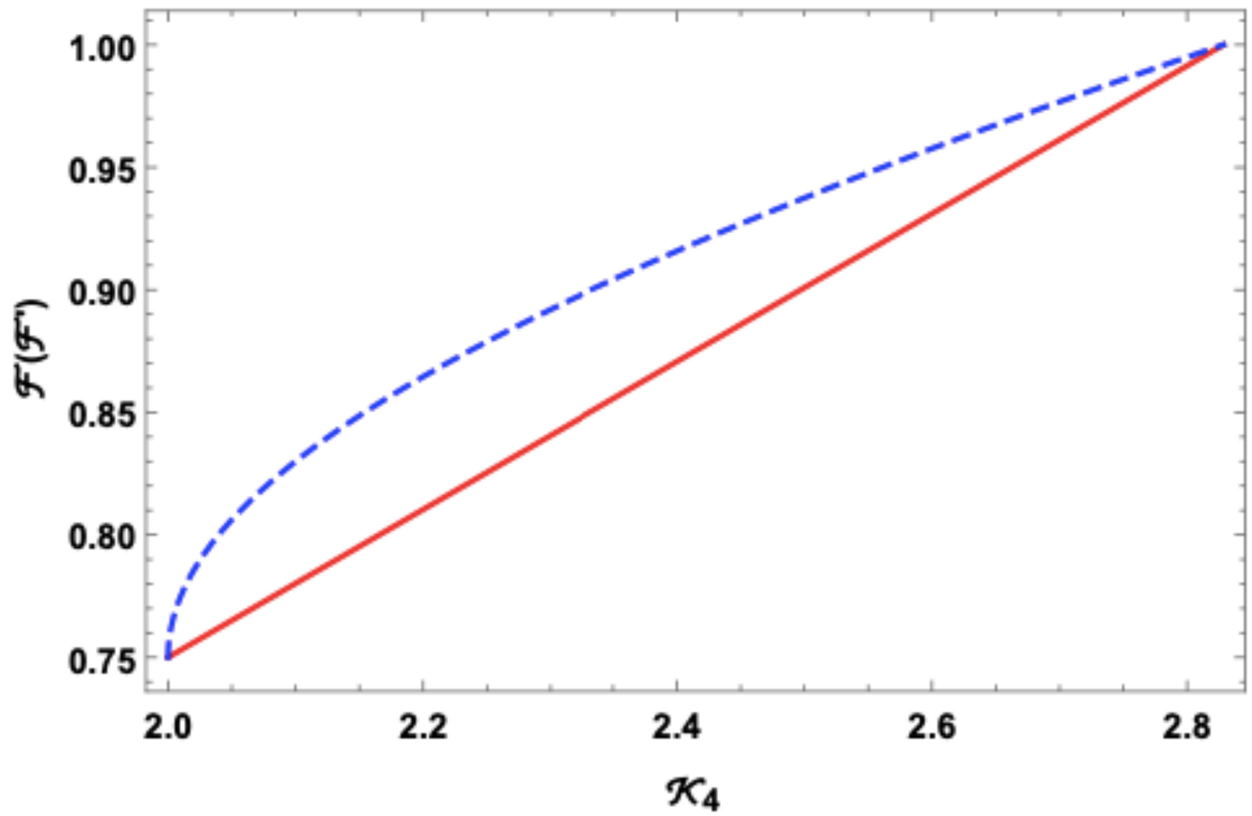
Robustness analysis

Average fidelity with ideal measurements,

$$S(\{\mathcal{P}_{a_i|A_i}\}) = \max_\Lambda \sum_{i,a_i} F(\mathcal{P}^{\text{ideal}}_{a_i|A_i}, \Lambda[\mathcal{P}_{a_i|A_i}])/4.$$

Lower bound on the smallest possible value of fidelity given a particular amount of violation is given by minimising over all sets of measurements,

$$\mathcal{F}(\mathcal{K}_4) = \min_{\mathcal{P}_{a_i|A_i}} S(\{\mathcal{P}_{a_i|A_i}\}).$$



$$\mathcal{F}(\mathcal{K}_4) \geq \frac{(1+\sqrt{2})}{8}\mathcal{K}_4 + \frac{2-\sqrt{2}}{4}.$$

J. Kaniewski, Phys. Rev. Lett. 117, 070402 (2016).

A. Tavakoli, J. Kaniewski, T. Vertesi, D. Rosset, and N. Brunner, Phys. Rev. A 98, 062307 (2018).

Conclusion

Certifying two outcome measurement employing violation of LGI.

No entanglement and no dimensional restriction.

Untrusted measurement devices acts on the input probe state prepared by the trusted experimenter.

Robustness of the protocol allow for experimental realizability.

Thank you