Self-testing:
device-independent certification of quantum devices

Xingyao Wu

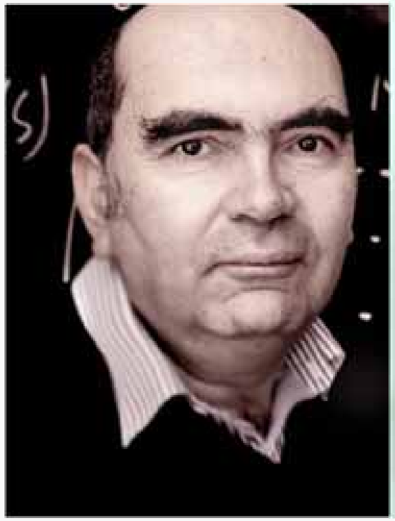
Centre for Quantum Technologies
National University of Singapore

Self-testing:
Basic notions

Definition of self-testing

- Here: DI self-testing of quantum devices: learn about the state, the measurements
  - "Blind tomography"
  - "Black-box characterization of a device"
- Different from other DI tasks, which give bounds for specific parameters
  - QKD: length of a secret key
  - Randomness: min-entropy
  - Entanglement: negativity

On the shoulders of giants




1992 Popescu & Rohrlich

CHSH = 2√2 ➔ singlet, X&Z

In fact, the mathematical result can be read from a 1987 work of Summers and Werner… if you can read algebraic field theory ☺


1998 Mayers & Yao

Other stats ➔ singlet, X&Z

- First to use “self-testing”
- Motivated by what later was called “device-independent QKD”; ended up proving *more* but *less directly useful*.

Ideal self-testing

Some extremal points of the set of correlations achievable with quantum physics can be obtained only from one state and the suitable measurements…

$CHSH = 2\sqrt{2}$ Mayers-Yao

$$U_A \otimes U_B |\Phi^+\rangle \otimes |junk\rangle$$

$$U_A(\sigma_z \otimes I)U_A^\dagger$$

… up to local isometries

Local isometry: pedestrian example

$$\frac{\alpha}{\sqrt{2}}(|00\rangle + |11\rangle) + \frac{\beta}{\sqrt{2}}(|22\rangle + |33\rangle)$$

$$|2n\rangle_A \rightarrow |0\rangle_{A'}|n\rangle_{A''}$$

$$|2n+1\rangle_A \rightarrow |1\rangle_{A'}|n\rangle_{A''}$$

$$\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)_{A'B'} (\alpha|00\rangle + \beta|11\rangle)_{A''B''}$$

Singlet ✓

"junk" (may still contain entanglement)

Is self-testing "useful"?

- Not for QKD, randomness & similar
  - If there is one figure of merit, optimize it directly!
- To test "not-too-big" devices
  - Blind tomography (e.g. stabilizer states)
  - Alleged 1000-qubit quantum computers
- As theoretical primitive
  - Interactive provers:
    - Reichardt-Unger-Vazirani, McKague, Fitzsimons
  - Randomness expansion & amplification
    - Coudron-Yuen, Miller-Shi

What we can certify today

States

–All two-qubit pure entangled states [Bamps, Pironio PRA 2015]

–CGLMP3: two-qutrit non-max entangled state [Yang et al. PRL 2014]

–Multipartite:

•All graph states [McKague TQC'11]

•Some three-qubit non-graph states [Wu et al, Pal et al, PRA 2014]

–Many singlets [Reichardt et al, Nature 2013; McKague arXiv 2015]

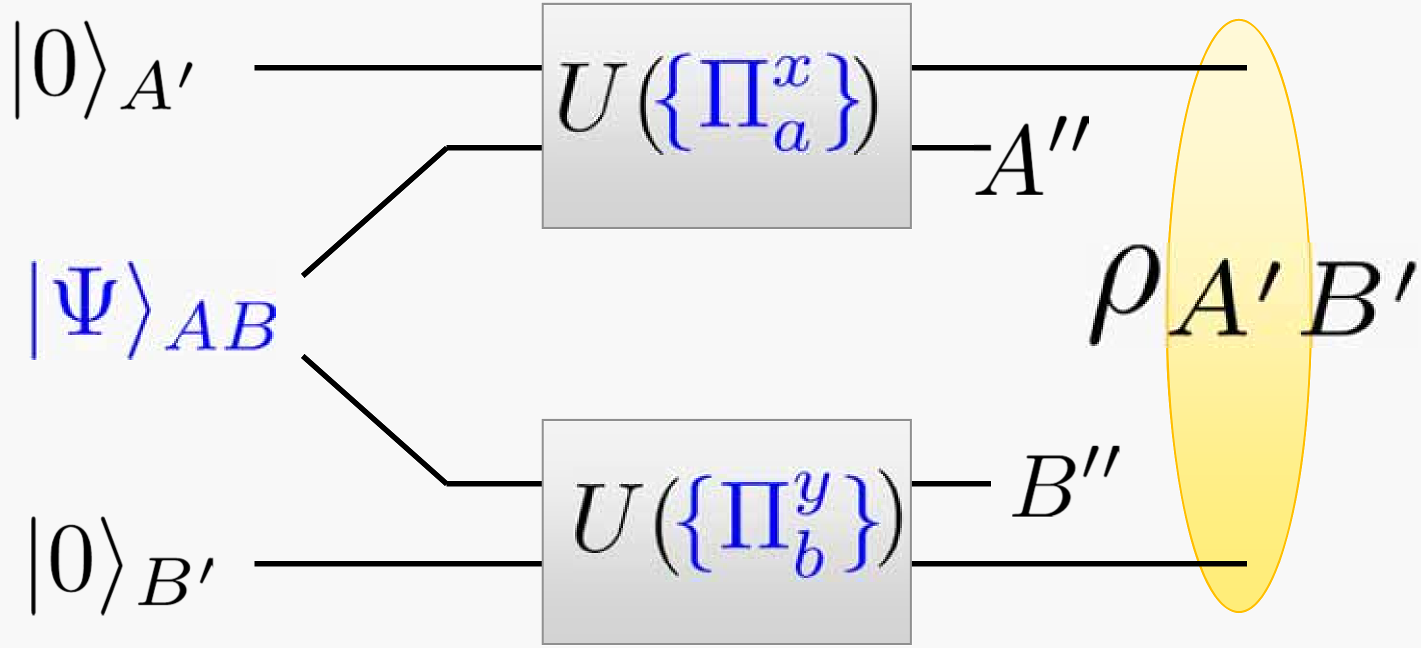
Measurements

–All of the above come with suitable measurements

–Entangling measurements (e.g. Bell basis)

How you do SELF-TESTING (Example: singlet)

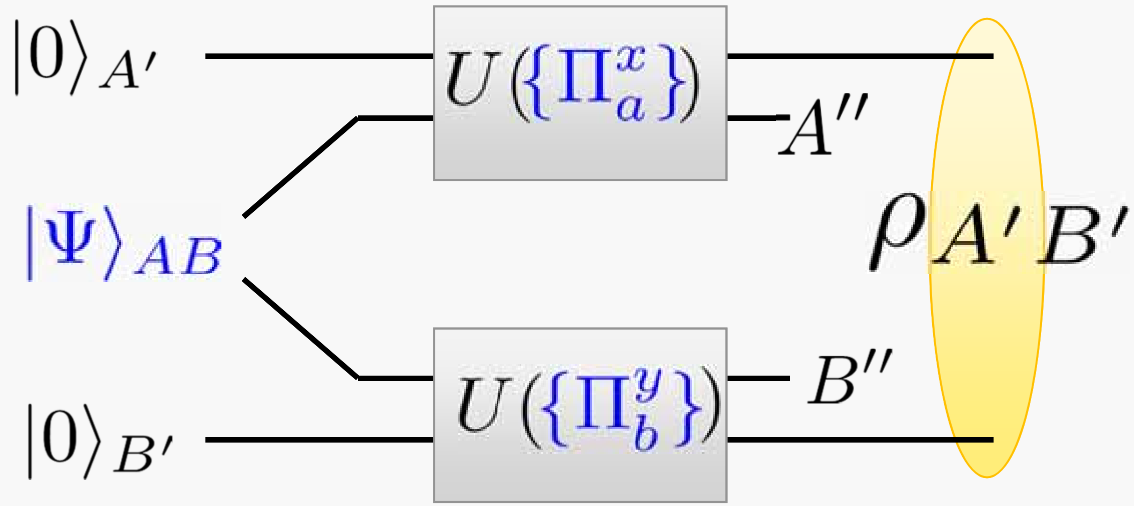
Construct the isometry



Fidelity with the target state (e.g. singlet) $F = \langle \Phi^+ | \rho | \Phi^+ \rangle$

- Intuition: swap out the state you want to self-test
- Important: you don't need to implement this in the lab

Non-deal self-testing: robustness



$$F = \langle\Phi^+|\rho|\Phi^+\rangle$$
$$= f(\langle\Pi_a^x\rangle, \langle\Pi_a^x\Pi_b^y\rangle, \langle\Pi_a^x\Pi_{a'}^{x'}\rangle, \ldots)$$

$min\ f$ constrained by P(a,b|x,y) and quantum correlation

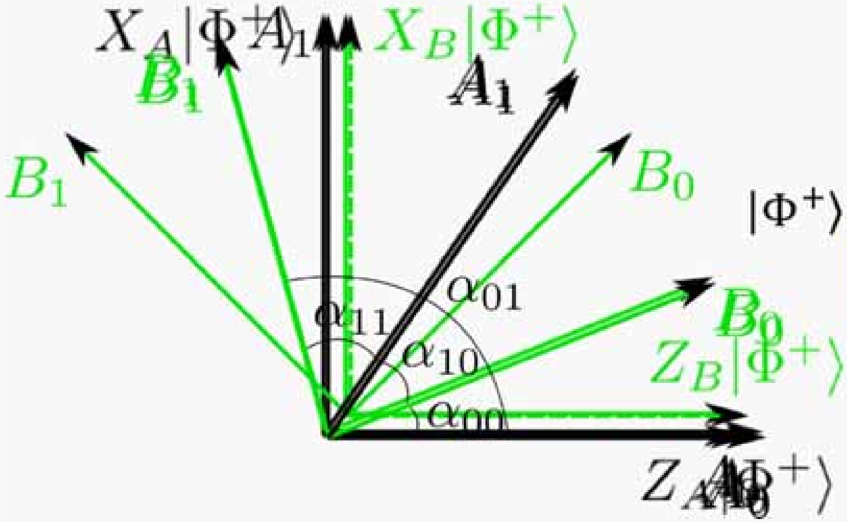
Navascues-Pironio-Acin SDP relaxation of

TWO RECENT RESULTS

- All the self-testing of singlet state
- Parallel self-testing of two singlets

All the self-testing for (2,2;2,2)

Y. Wang, X. Wu and V. Scarani, arxiv:1511.04886(2015)



$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

CHSH

$$A_0B_0 + A_1B_1 + A_1B_0 - A_0B_1 = 2\sqrt{2}$$

$$E_{00} = \langle A_0B_0\rangle = \cos\alpha_{00}$$
$$E_{10} = \langle A_1B_0\rangle = \cos\alpha_{10}$$
$$E_{01} = \langle A_0B_1\rangle = \cos\alpha_{01}$$
$$E_{11} = \langle A_1B_1\rangle = \cos\alpha_{11}$$

↓

Can we self-test a singlet state with these statistics $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$?

Yes

If and only if:

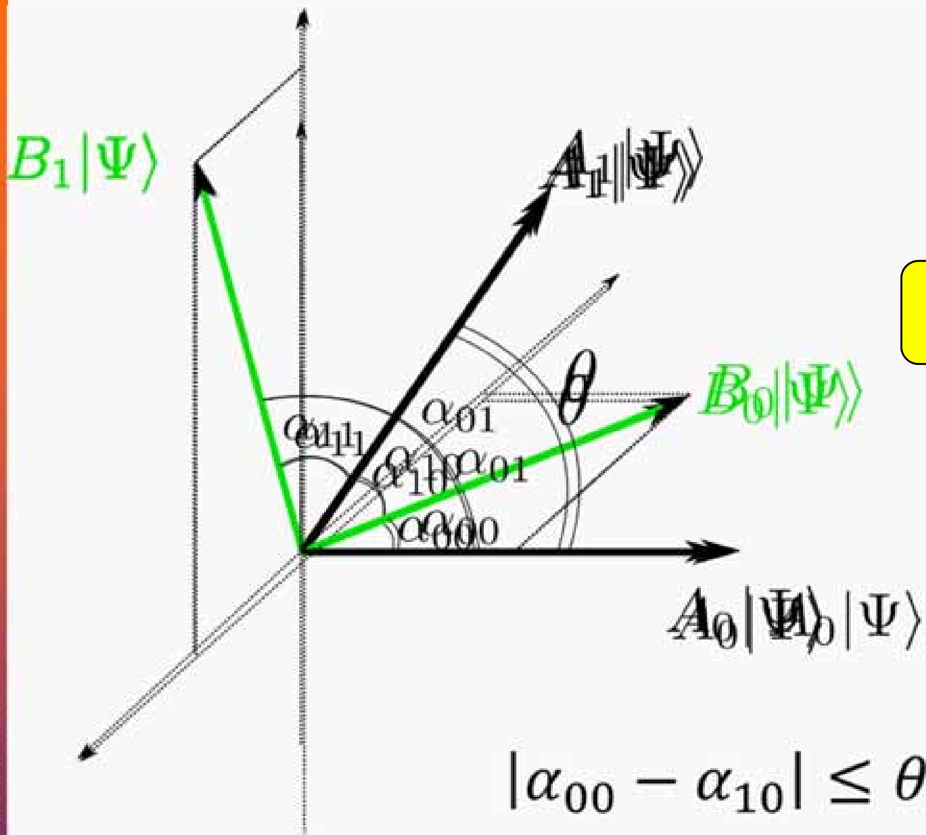
$$|\arcsin E_{00} + \arcsin E_{10} + \arcsin E_{11} - \arcsin E_{01}| = \pi$$

NUS

Centre for Quantum Technologies

All the self-testing for (2,2;2,2)

Y. Wang, X. Wu and V. Scarani, arxiv:1511.04886(2015)



Condition:

$$\alpha_{00} + \alpha_{10} + \alpha_{11} = \alpha_{01}$$

$$\#(\alpha_{ij} = 0) \leq 1$$

$$|\alpha_{00} - \alpha_{10}| \leq \theta \leq \alpha_{00} + \alpha_{10}$$

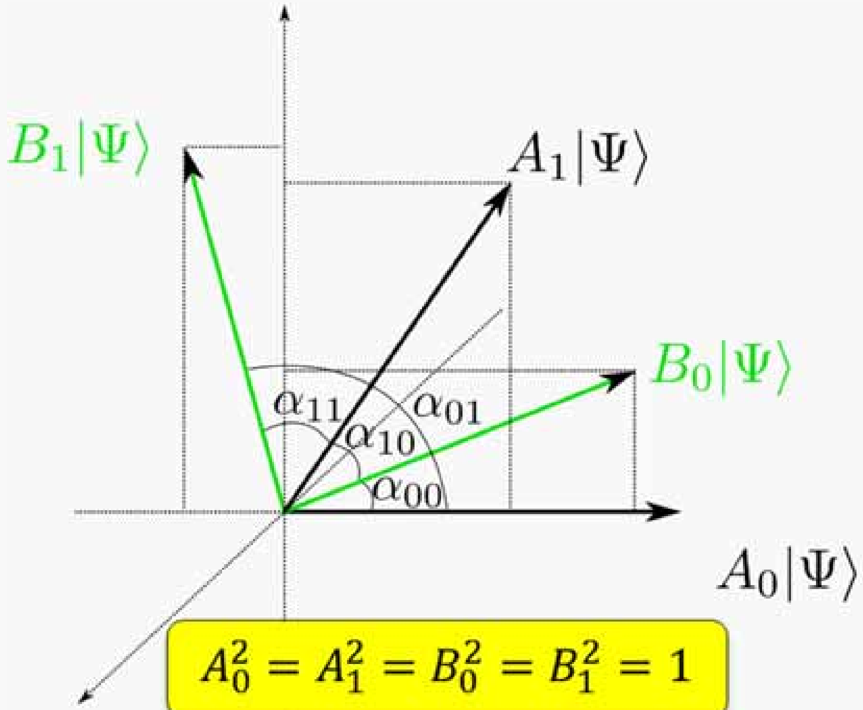
$$\alpha_{01} - \alpha_{11} \leq \theta \leq \alpha_{01} + \alpha_{11}$$

$$\theta = \alpha_{00} + \alpha_{10} = \alpha_{01} - \alpha_{11}$$

Centre for Quantum Technologies

All the self-testing for (2,2;2,2)

Y. Wang, X. Wu and V. Scarani, arxiv:1511.04886(2015)



$$A_0^2 = A_1^2 = B_0^2 = B_1^2 = 1$$

$$B_0|\Psi\rangle = \frac{\sin(\alpha_{00})\, A_1|\Psi\rangle + \sin(\alpha_{10})\, A_0|\Psi\rangle}{\sin(\alpha_{00} + \alpha_{10})}$$

$$A_1|\Psi\rangle = \frac{\sin(\alpha_{11})\, B_1|\Psi\rangle + \sin(\alpha_{10})\, B_0|\Psi\rangle}{\sin(\alpha_{11} + \alpha_{10})}$$

$$(B_0|\Psi\rangle)^2 = \left(\frac{\sin(\alpha_{00})\, A_1|\Psi\rangle + \sin(\alpha_{10})\, A_0|\Psi\rangle}{\sin(\alpha_{00} + \alpha_{10})}\right)^2$$

$$(A_1|\Psi\rangle)^2 = \left(\frac{\sin(\alpha_{11})\, B_1|\Psi\rangle + \sin(\alpha_{10})\, B_0|\Psi\rangle}{\sin(\alpha_{11} + \alpha_{10})}\right)^2$$

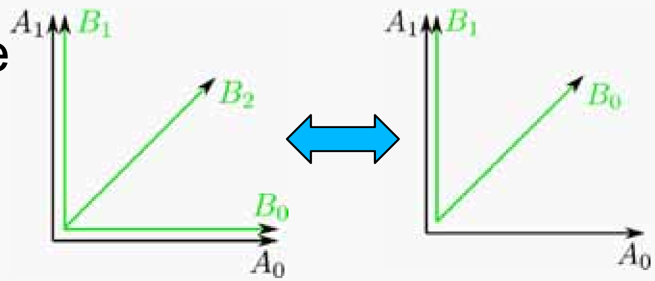
$$\Rightarrow$$

$$(A_1A_0 + A_0A_1)|\Psi\rangle = 2\cos(\alpha_{00} + \alpha_{10})\,|\Psi\rangle$$
$$(B_1B_0 + B_0B_1)|\Psi\rangle = 2\cos(\alpha_{11} + \alpha_{10})\,|\Psi\rangle$$

All the self-testing for (2,2;2,2)

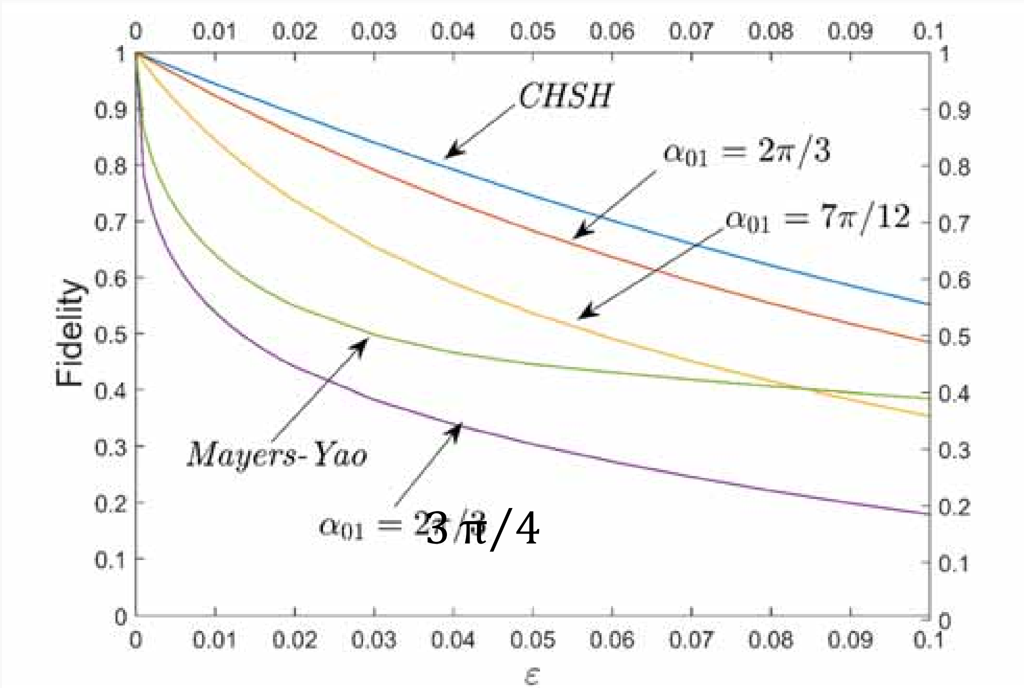
Y. Wang, X. Wu and V. Scarani, arxiv:1511.04886(2015)

- Singlet still can be self-tested without one measurement in Mayers-Yao

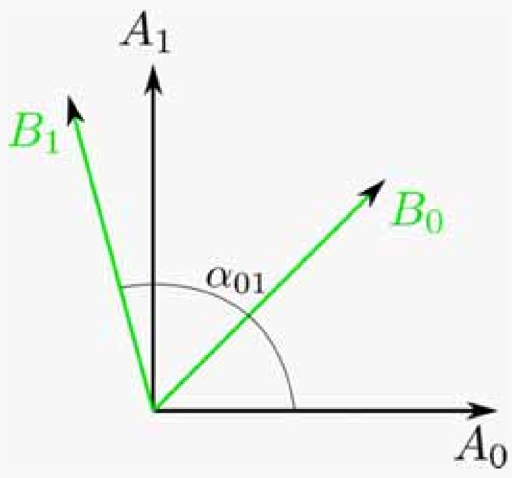


Mayers-Yao Simplification

- Robustness bound of fidelity



$$\left|\langle\Psi|A_x B_y|\Psi\rangle - E_{xy}^{\mathrm{ideal}}\right| \leq \varepsilon$$



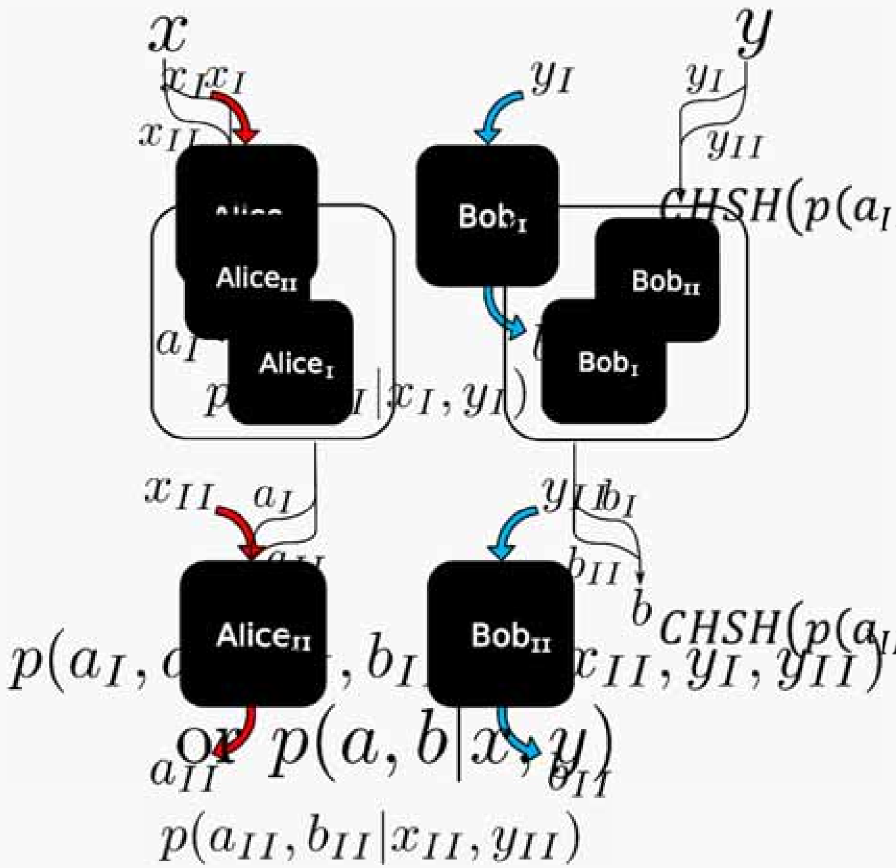
$$\left(\theta = \frac{\pi}{2}, \alpha_{00} = \frac{\pi}{4}\right)$$

NUS

Centre for Quantum Technologies

Parallel self-testing of two singlets

X. Wu, J.-D. Bancal, M. McKague and V. Scarani, arxiv:1511.04886(2015)



$$CHSH(p(a_I, b_I | x_I, y_I)) = 2\sqrt{2} \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- We do not exclude the possibility of the interference between the two subsystems.
- We do not assume sequential measurements. (RUV 2013)

$$CHSH(p(a_{II}, b_{II} | x_{II}, y_{II})) = 2\sqrt{2} \rightarrow \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$CHSH(a_I, b_I, x_I, y_I) = 2\sqrt{2}$$
$$CHSH(a_{II}, b_{II}, x_{II}, y_{II}) = 2\sqrt{2} \overset{?}{\rightarrow} \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes 2}$$

Parallel self-testing of two singlets

X. Wu, J.-D. Bancal, M. McKague and V. Scarani, arxiv:1511.04886(2015)

•***Criterion***:

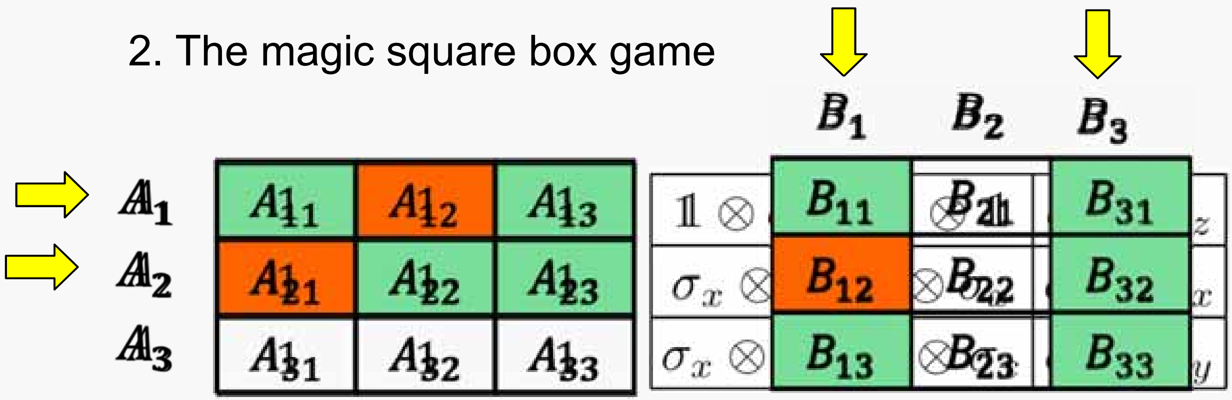
1.The criterion with double violations of CHSH (or the *correlation* from ideal singlets /w ideal optimal measurements)

$$|\psi\rangle = \left(\cos\frac{\pi}{8}|\Phi^+\rangle + \sin\frac{\pi}{8}|\Psi^-\rangle\right)^{\otimes 2}$$

A: $\sigma_z \otimes \sigma_z$
$\sigma_x \otimes \sigma_z$
$\sigma_z \otimes \sigma_x$
$\sigma_x \otimes \sigma_x$

B: $\sigma_z \otimes \sigma_z$
$\sigma_x \otimes \sigma_z$
$\sigma_z \otimes \sigma_x$
$\sigma_x \otimes \sigma_x$

2. The magic square box game

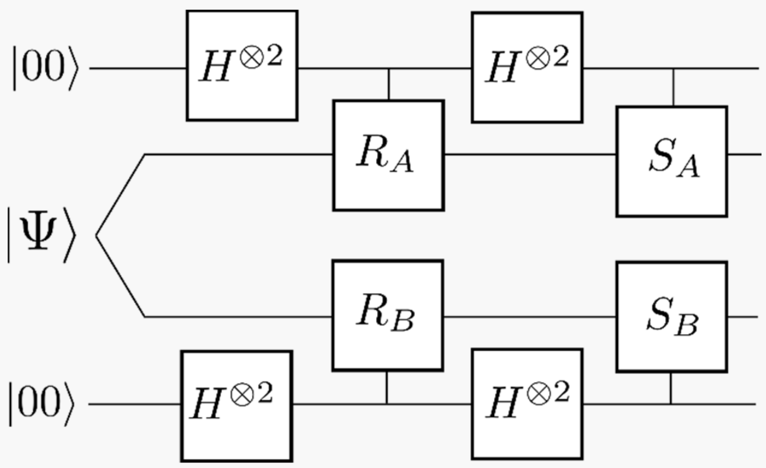


$$|\psi\rangle = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes 2}$$

Parallel self-testing of two singlets

X. Wu, J.-D. Bancal, M. McKague and V. Scarani, arxiv:1511.04886(2015)

•***Swap***: A proper construction of swap based on the measurements from the box. (*<u>Unitary</u>*)



R_A: $|00\rangle$ $\mathbb{I}\otimes\mathbb{I}$
$|01\rangle$ $\mathbb{I}\otimes\sigma_z$
$|10\rangle$ $\sigma_z\otimes\mathbb{I}$
$|11\rangle$ $\sigma_z\otimes\sigma_z$

$\Pi_{0|0}-\Pi_{1|0}+\Pi_{2|0}-\Pi_{3|0}$

$f(\{\Pi_{a|x}\})$

S_A: $|00\rangle$ $\mathbb{I}\otimes\mathbb{I}$
$|01\rangle$ $\mathbb{I}\otimes\sigma_x$
$|10\rangle$ $\sigma_x\otimes\mathbb{I}$
$|11\rangle$ $\sigma_x\otimes\sigma_x$

$\Pi_{0|3}+\Pi_{1|3}-\Pi_{2|3}-\Pi_{3|3}$

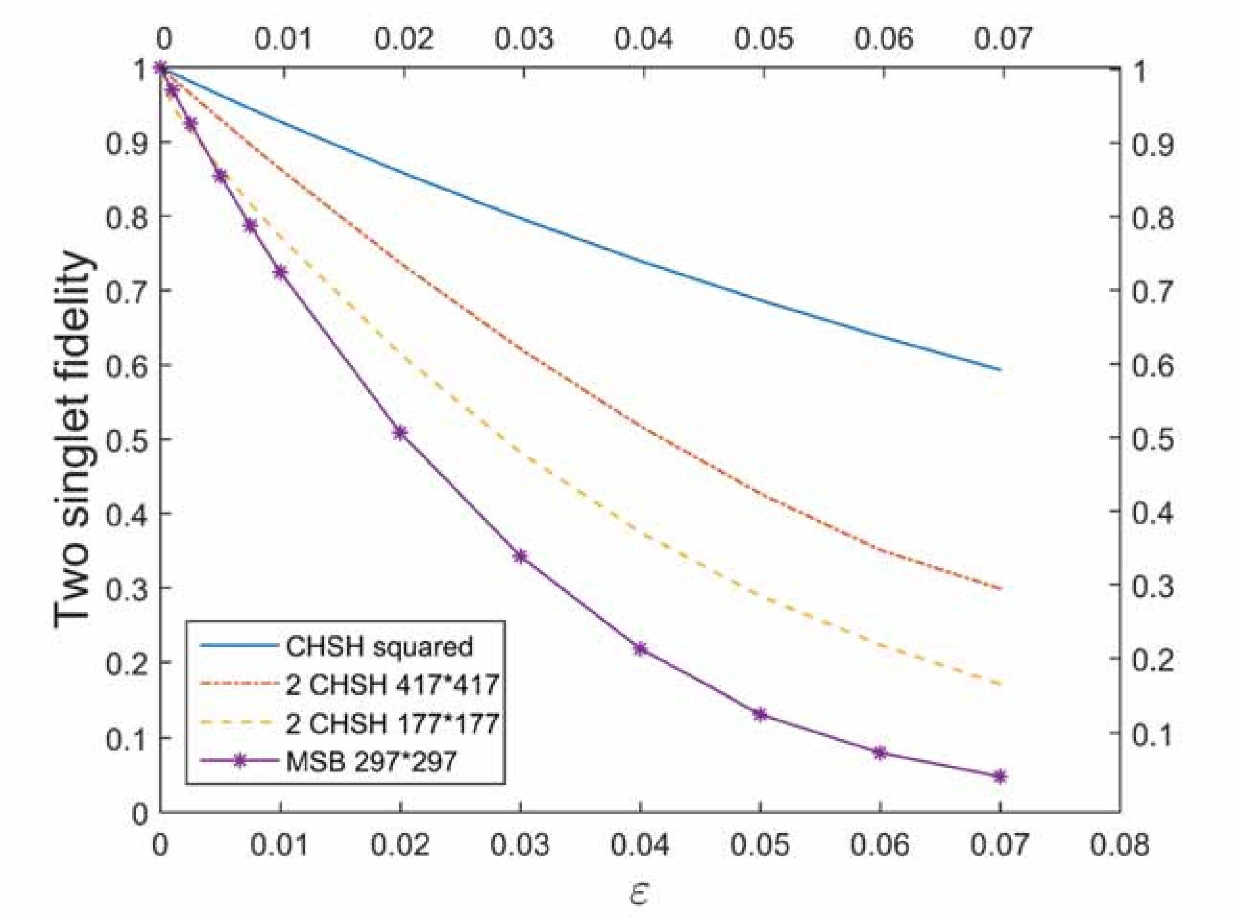
A: $\{\Pi_{a\|x}\}$	B: $\{\Pi_{b\|y}\}$
$\{\Pi_{a\|0}\}\longrightarrow\sigma_z\otimes\sigma_z$	$\{\Pi_{b\|0}\}\longrightarrow\sigma_z\otimes\sigma_z$
$\{\Pi_{a\|1}\}\longrightarrow\sigma_x\otimes\sigma_z$	$\{\Pi_{b\|1}\}\longrightarrow\sigma_x\otimes\sigma_z$
$\{\Pi_{a\|2}\}\longrightarrow\sigma_z\otimes\sigma_x$	$\{\Pi_{b\|2}\}\longrightarrow\sigma_z\otimes\sigma_x$
$\{\Pi_{a\|3}\}\longrightarrow\sigma_x\otimes\sigma_x$	$\{\Pi_{b\|3}\}\longrightarrow\sigma_x\otimes\sigma_x$

$$p(a,b|x,y) = \mathrm{Tr}\Big(|\psi\rangle\langle\psi|(\sigma_i\otimes\sigma_j)\Big)$$

Parallel self-testing of two singlets

X. Wu, J.-D. Bancal, M. McKague and V. Scarani, arxiv:1511.04886(2015)

•Bounding the fidelity with NPA hierarchy



arxiv:1512.02074(2015)

OPEN Questions & SUMMARY

NUS
National University of Singapore

Centre for Quantum Technologies

Summary

•Self-testing = “the signature of a quantum state” (and measurements)

•Device independent

•Recent:

–All the self-testing of singlet

–Parallel self-testing of two singlets

•Open questions:

–More self-testing ?

–Use it to certify experiments.

– MANY! Just ask me if you are interested ☺

Summary

Thank you!

Our group

NUS National University of Singapore

Centre for Quantum Technologies