# Device-independent quantum information

**Valerio Scarani**
Centre for Quantum Technologies
National University of Singapore

# Looking for post-doc

*Commitment to fairness: in case of otherwise equally competent candidates, the best soccer player will be chosen.*

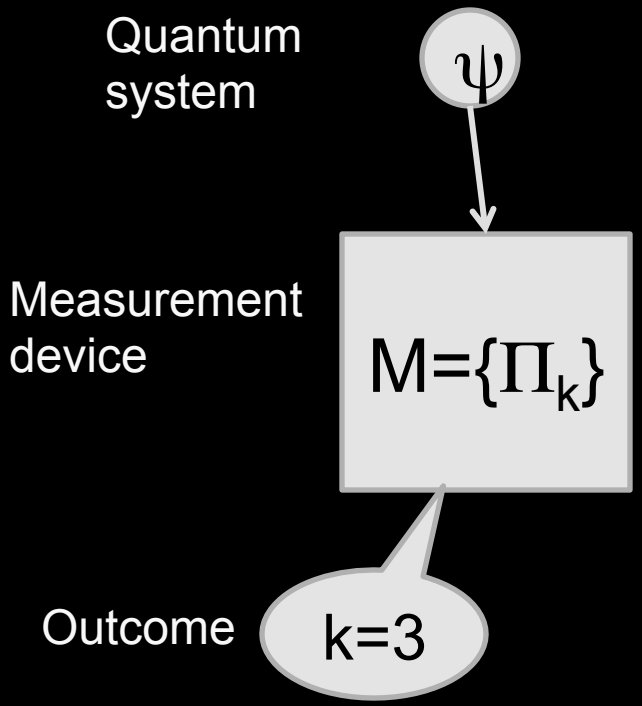
NUS
National University of Singapore

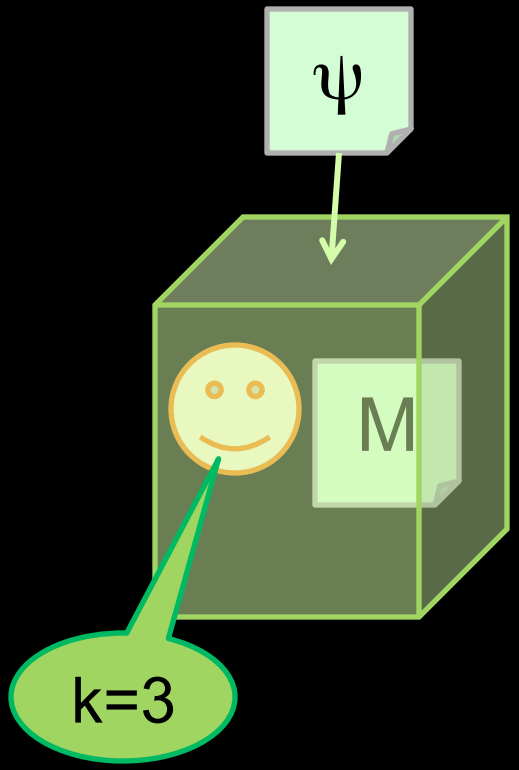
# THE NOTION OF DEVICE-INDEPENDENT

Centre for Quantum Technologies

# Something obvious

Simulation of quantum statistics with competent students

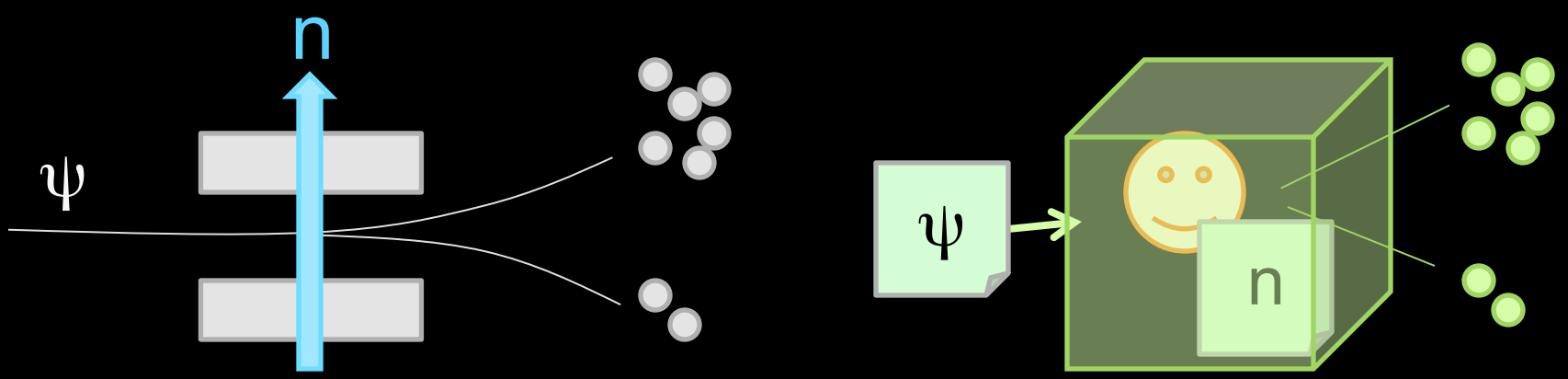



$P(k|M)=Tr(\Pi_k P_\psi)$

$P(k|M)=Tr(\Pi_k P_\psi)$

# Indulge in the obvious



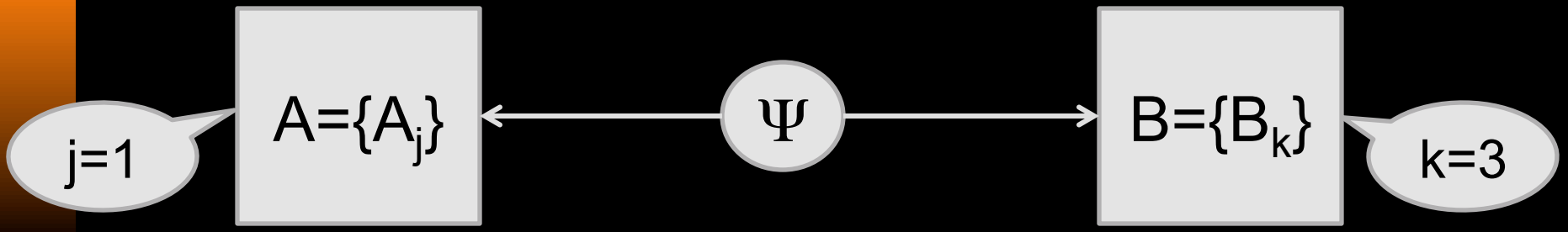

Why then Stern-Gerlach is “quantum” and can be used to derive the quantum formalism?

Because here we know much more than the statistics!
We know that:

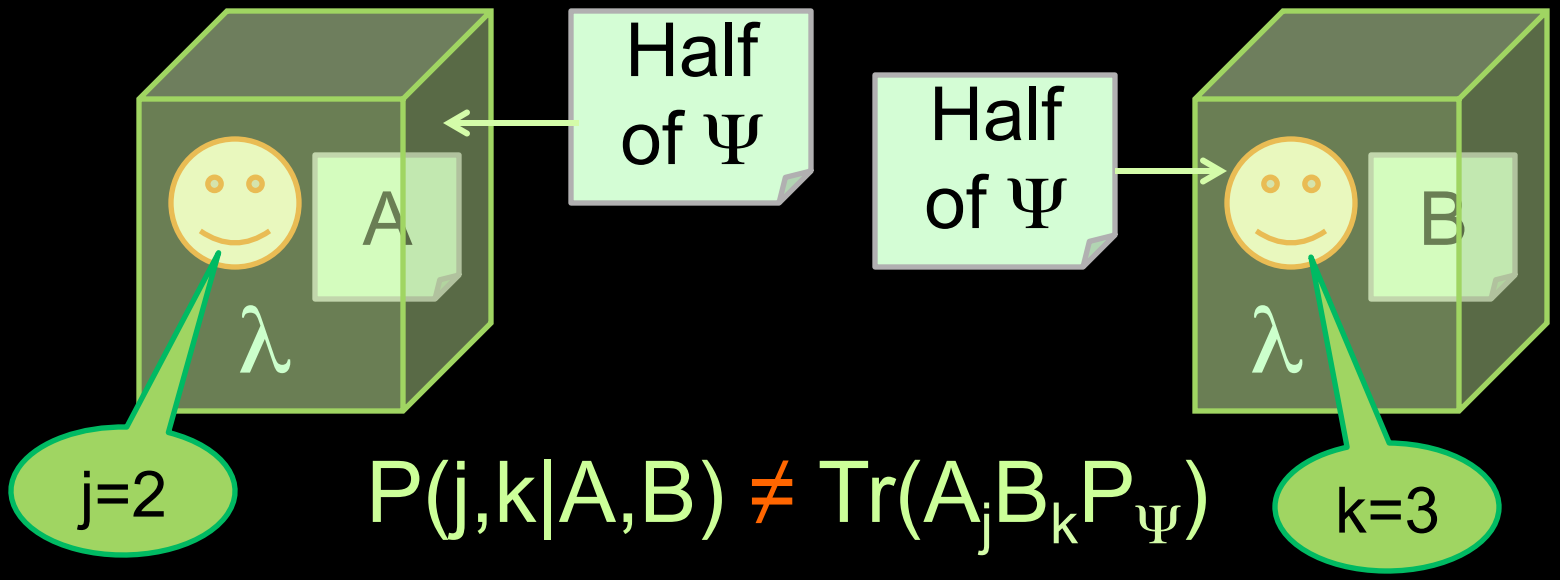
- a magnetic moment is being measured
- a measurement is associated to a direction in space

and no classical magnetic moment can behave that way!

# Something less obvious




$$P(j,k|A,B)=Tr(A_jB_kP_\Psi)$$




$$P(j,k|A,B) \neq Tr(A_jB_kP_\Psi)$$

The students cannot simulate this experiment, even if they have shared in advance some common strategy λ.

# Indulge in the obvious again

## How comes?

Because the quantum statistics may violate Bell inequalities – whose most operational, interpretation-free definition is precisely “criteria that must not be violated when a simulation of that type is possible”.

## Why can students compute joint probabilities in exams?

Because they are given BOTH measurements A and B; while in the simulation, one is given only A, the other only B (“locality constraint”)

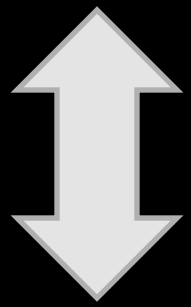
## How could the students cheat to win?

They could use their mobile phone (signaling) or ask to be allowed not to answer sometimes (“detection loophole”).

# And now, the flash of the obvious!

## Loophole-free Bell violation

Be sure there is no cheating



The criterion is quantitative

## Device-independent proof of entanglement

No need to know what I am measuring or how

NUS National University of Singapore

Centre for Quantum Technologies

# And a bit of motivation

## Why are you not happy with Stern-Gerlach?

- For physics, I am perfectly happy (I trust that nature is not trying to cheat me).
- But if I buy (say) a QKD device from a vendor, how can I check that this device is really Q?
- Or, how can experimentalists convince us that they have excluded all side channels (cf. hacking)?

## And above all…

Is it not really fascinating, that quantitative tests of "quantumness" can be based only on input-output statistics? ☺

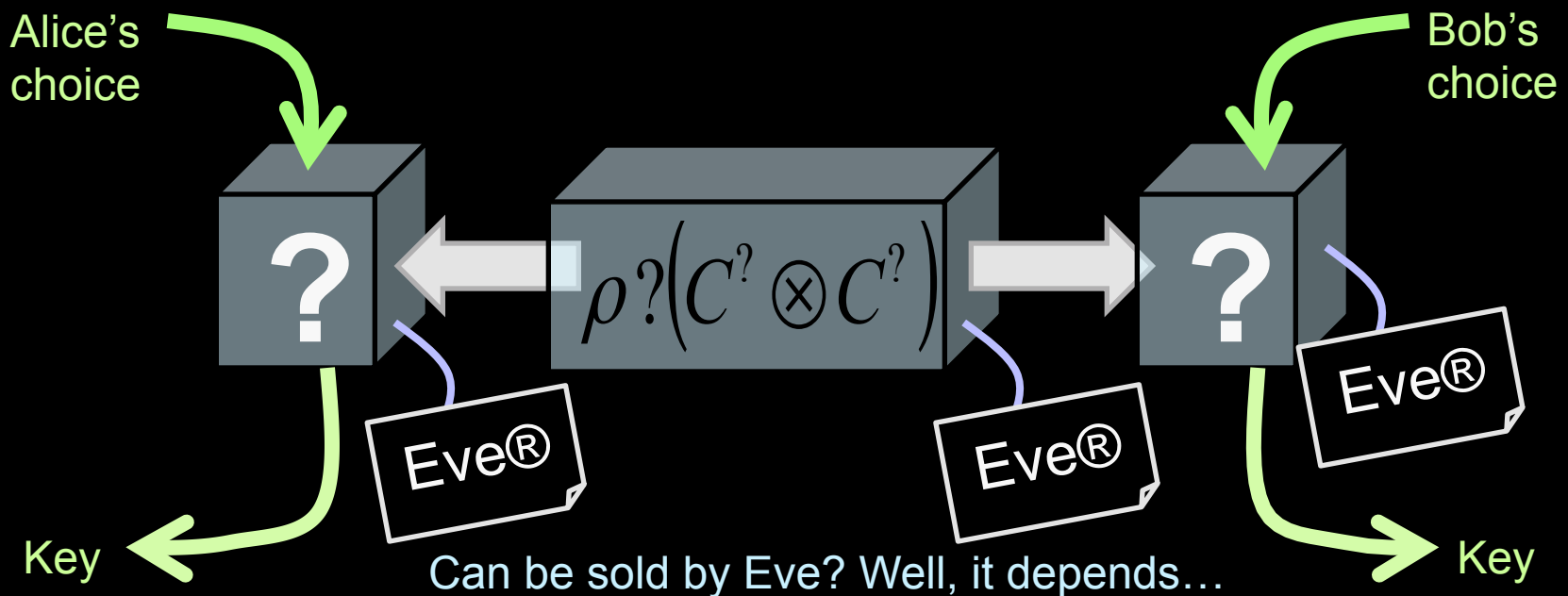
NUS
National University of Singapore

Centre for Quantum Technologies

# THEORETICAL HORS-D'OEUVRE

An overview of tasks, results and open problems

# Task 1: key distribution

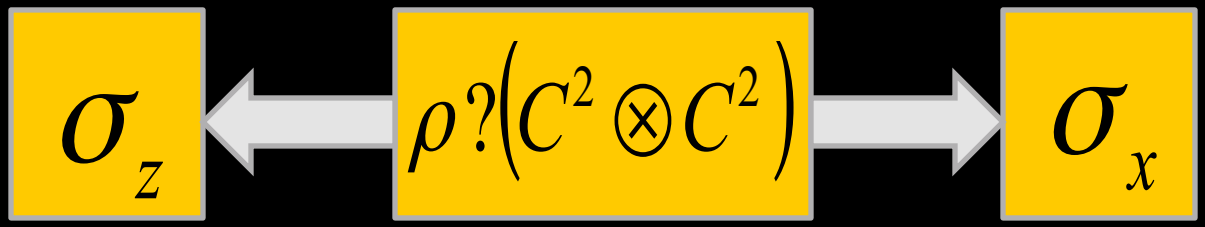



- Protocol: BB84-BBM fully insecure in DI, need to use Ekert or similar.
- Violation of Bell quantifies the information leaked to the eavesdropper.
- State of the art: security bound under assumption of "no-signaling" between repetitions.

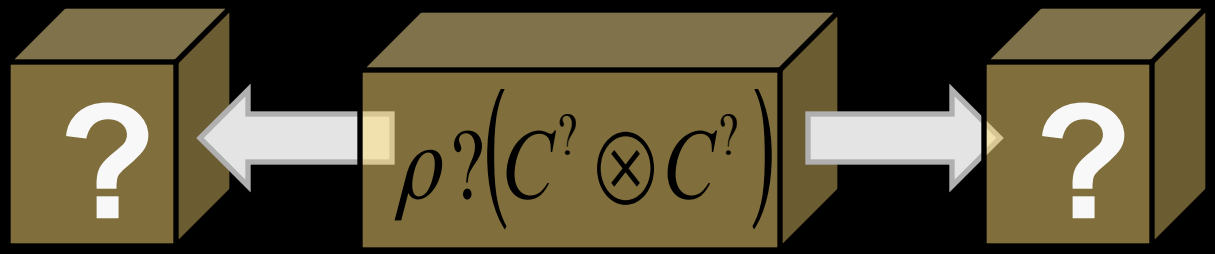
Precursors: Ekert 1991; Barrett, Hardy, Kent 2005; Acin, Gisin, Masanes 2006
Bound for collective attacks: Acin, Brunner, Gisin, Massar, Pironio, Scarani 2007
State of the art: Masanes, Pironio, Acin 2011; Haenggi, Renner 2010

# Task 2: test entanglement sources

Usual tomography: we know the system and how to measure it
⇒ Reconstruct ρ



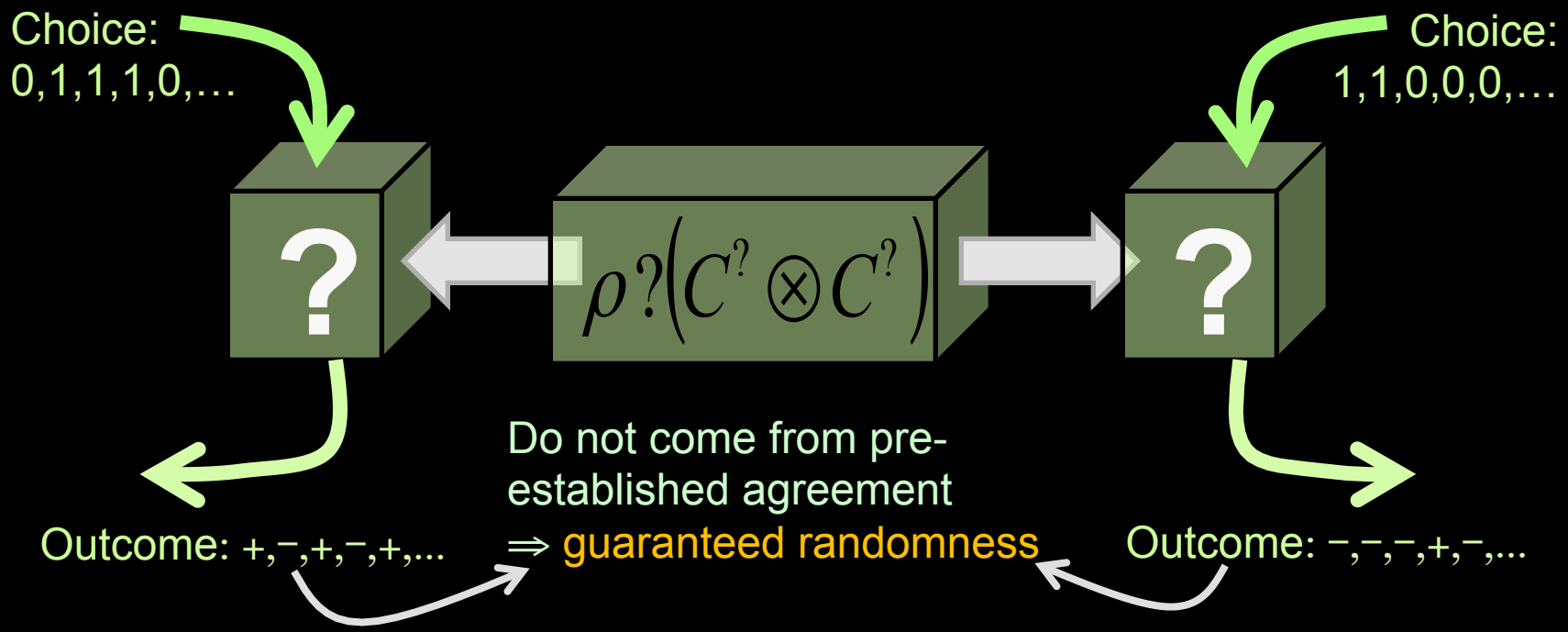

DI: "jealous vendor". How far is ρ from an "ideal" state (S=2√2)?




- Violation of Bell quantifies the trace distance between the source and the closest state which would lead to a maximal violation.
- State of the art: analytical bound for CHSH under further assumptions (pure state, or qubits); numerical evidence that it is general.
- Genuine multipartite entg: inequalities, no quantitative estimate

Bipartite CHSH: Bardyn, Liew, Massar, McKague, Scarani 2009
Multipartite: Bancal, Gisin, Liang, Pironio 2011
Related idea "self-testing": Mayers, Yao 2004; McKague 2010

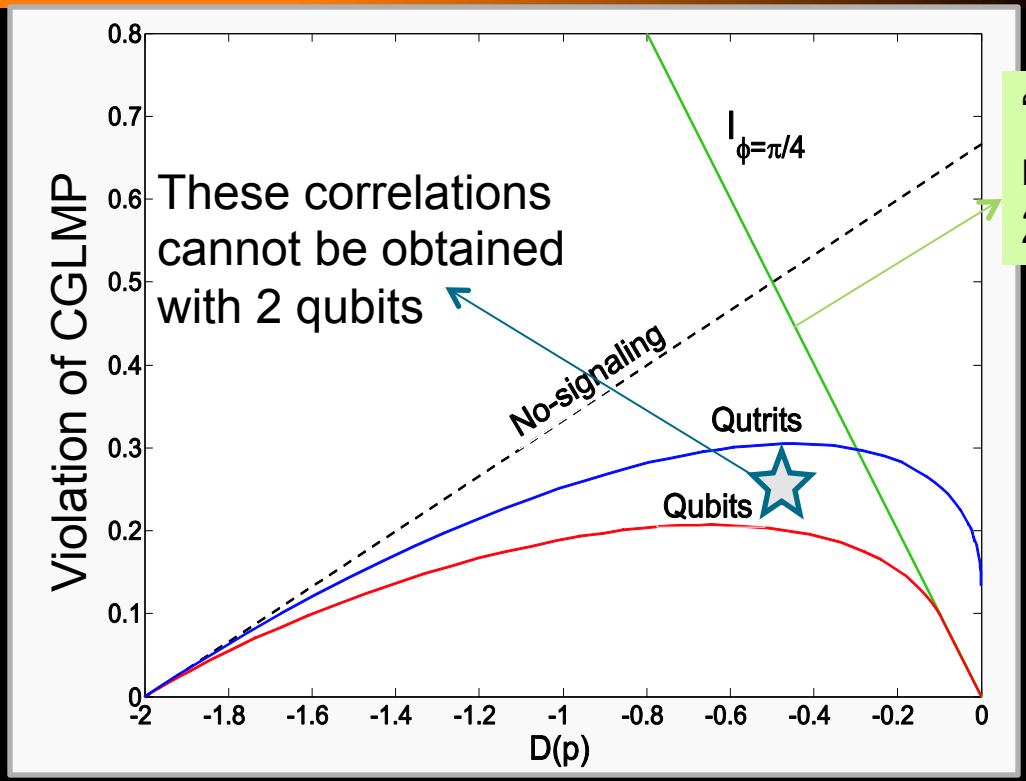
# Task 3: randomness expansion




- Violation of Bell quantifies the min-entropy of the generated strings.
- Moreover, the randomness is private (no third person can share those lists)
- Experiment performed with atoms (closed detection loophole, not locality but ok…)

Initial theory and experiment: Pironio, Acin, Massar, Boyer de la Giraudy, Matsukevich, […], Monroe 2010

# Task 4: dimension witness




"Tilted" ineq, never violated by 2 qubits

- Violation of some Bell inequalities gives a lower bound on the dimension of the Hilbert space.
- State of the art: several examples

Using Bell inequalities: Pironio, Acin, Gisin, Methot, Scarani 2008
Other approach: Wehner, Christandl, Doherty 2008
Further results: Vertesi, Pal; Briet, Buhrman, Toner 2009
Experiments (detection loophole): Dada et al 2011 (assumes a family of states); Cai et al in preparation

# Semi-DI friends

Remove some of the typical assumptions, even if not all:

1. Simpler implementations
2. Obtain more refined information

- Assume the dimension of the Hilbert space, no knowledge of state and measurement
  - Quantify entanglement: Liang, Vertesi, Brunner 2011;
- Bound the dimension even classically
  - Dimension: Gallego, Brunner, Hadley, Acin 2010; Experiments: Hendrych et al., Ahrens et al. 2011
  - QKD: Pawlowski, Brunner 2011
- Assume that the source is fully characterized, while the measurement process is not
  - Lo, Curty, Qi 2011, Branciard et al. 2011

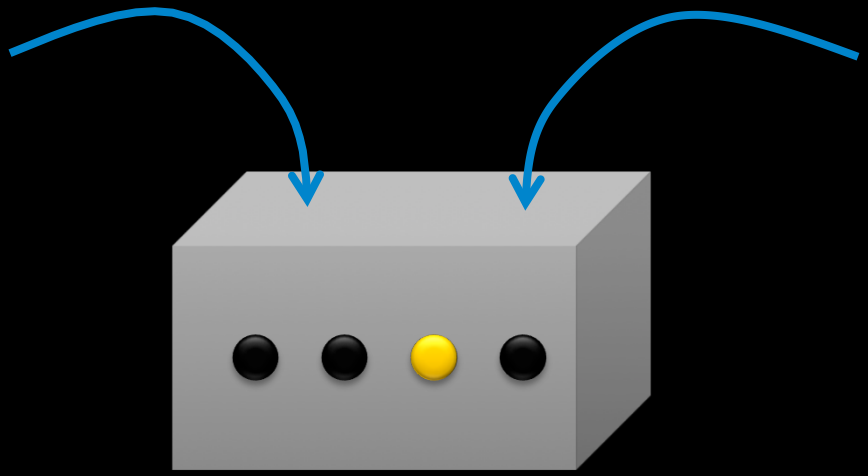
# SPECIAL TOPIC: ENTANGLED MEASUREMENT

Rabelo, Ho, Brunner, Cavalcanti, Scarani PRL 2011

Related (not fully DI): Vertesi, Navascues PRA 2011

# Motivation: circuit testing

A vendor sells allegedly quantum devices: you can buy “sources of entangled pairs”, “local unitaries”…



Is this box performing a Bell-state measurement?

- A perfect one? Certainly not!
- What is a BSM if I don’t know the dimensionality of the signals?

How close is this box from performing a Bell-state measurement on some 2-dimensional sub-systems in the incoming signals?

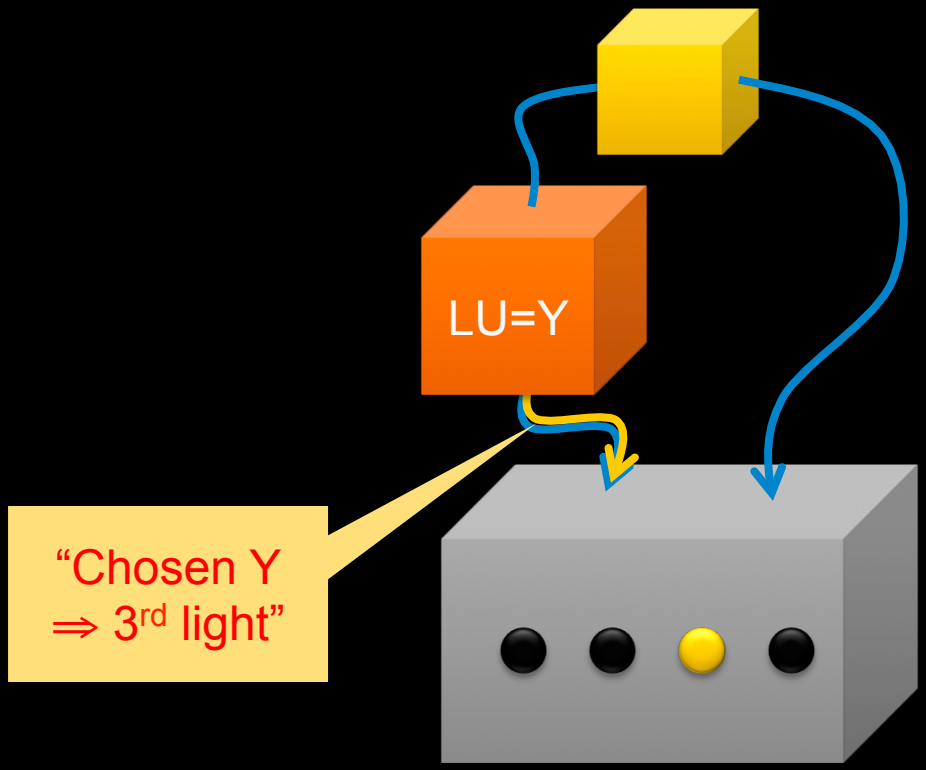
Of course, everything must be checked with the same vendor’s products!

# What does not work

0. Buy a “source”, “local measurements”, a “local unitary” and a “BSM”

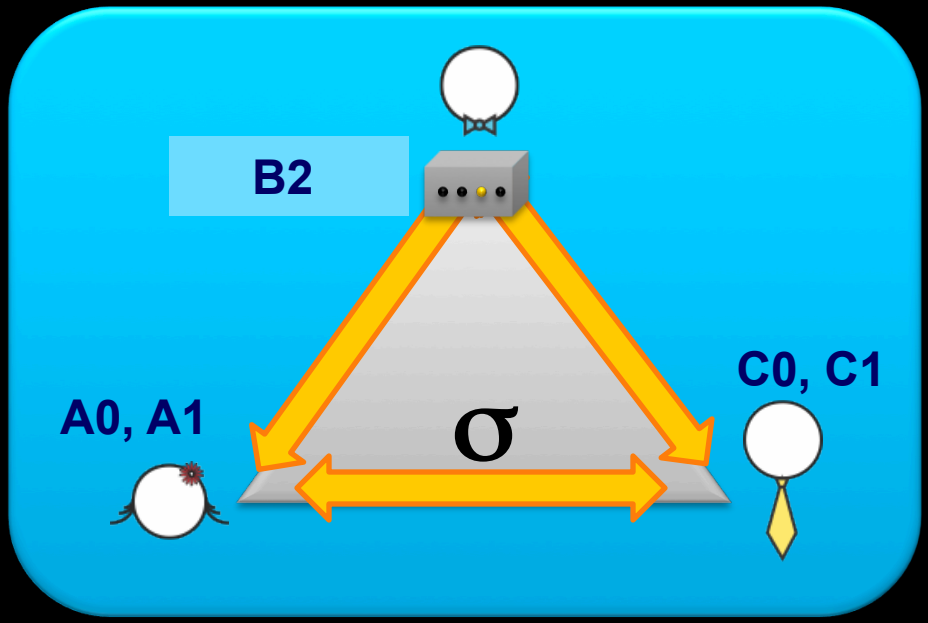
1. Check the entanglement of the source (e.g. Bardyn et al PRA 2009)

2. Set the local unitary to I, X, Y, Z and check that one light clicks deterministically for each



# A three-partite strategy

Local measurements: A0,A1,C0,C1: 2 outputs; B0,B1,B2: four outputs



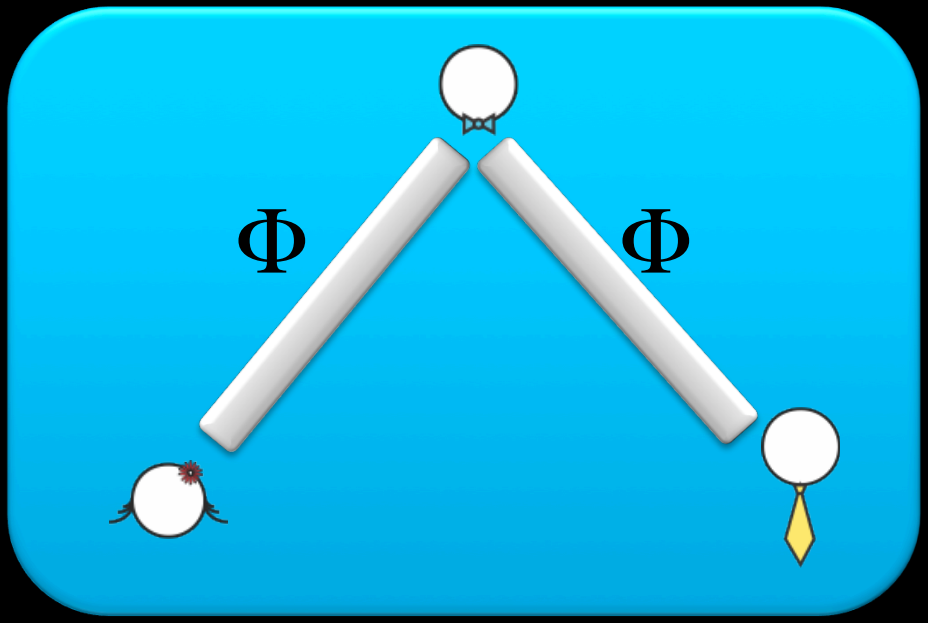

1a. Check CHSH (A0,A1;B0,B1)

1b. Check CHSH (C0,C1;B0,B1)

2. Check CHSH (A0,A1;C0;C1) conditioned on B2 = b2

# Intuition

**What QM can do:** entanglement swapping of two singlets




CHSH(A,B) = 2√2
CHSH(C,B) = 2√2

If B2 = perfect BSM:
CHSH(A,C|b2) = 2√2

If B2 = separable:
CHSH(A,C|b2) < √2

**This last bound is device-independent!**
CHSH(A,B)=2√2 ⇒ A is measuring on an effective qubit, max entg with something in B (Popescu-Rohrlich, McKague) ⇒ not entg with C before B2.

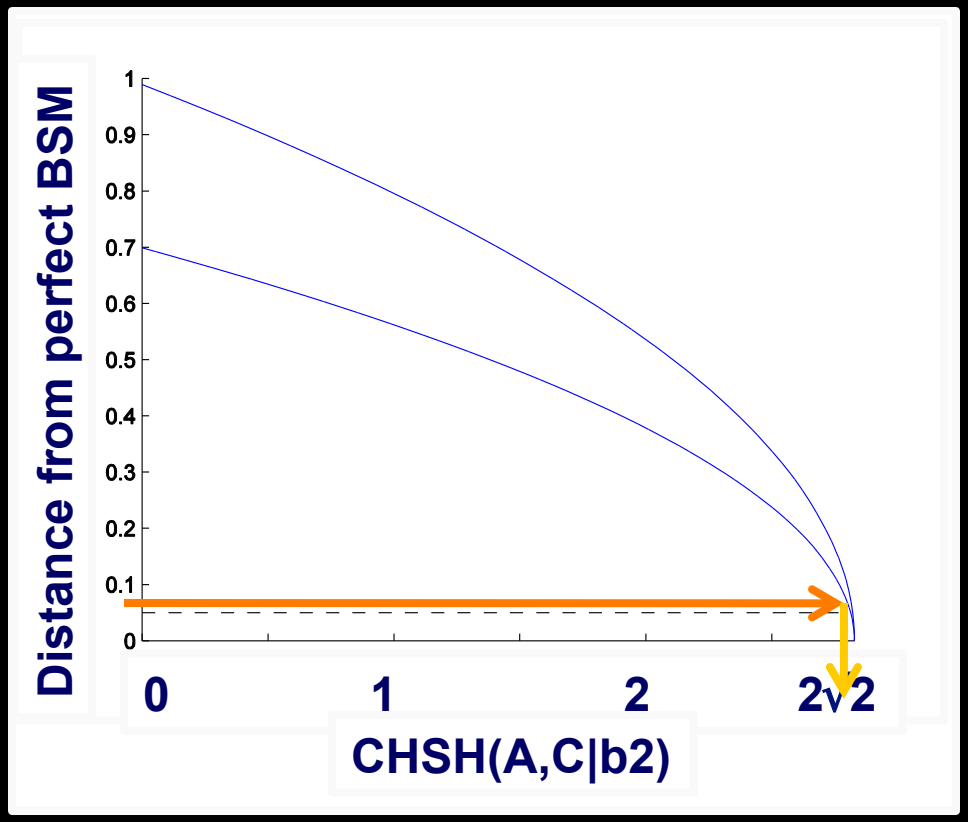
DI gap between "separable measurement" and "BSM"
⇒ a competent company CAN convince you to buy their BSM

# Three remarks

(1) One needs CHSH(A,B) and CHSH(B,C): the condition CHSH(A,C|b2) = 2√2 alone can be met without any BSM.

(2) So far, quantitative bounds only under the assumption that either CHSH(A,B) or CHSH(B,C) is exactly 2√2.

(3) In a qubit model (i.e. not DI) one can see that this test is going to be very demanding on the company:




Certify BSM at 5% of failure probability

⇓

CHSH ≥ 2√2− 0.5%

Centre for Quantum Technologies

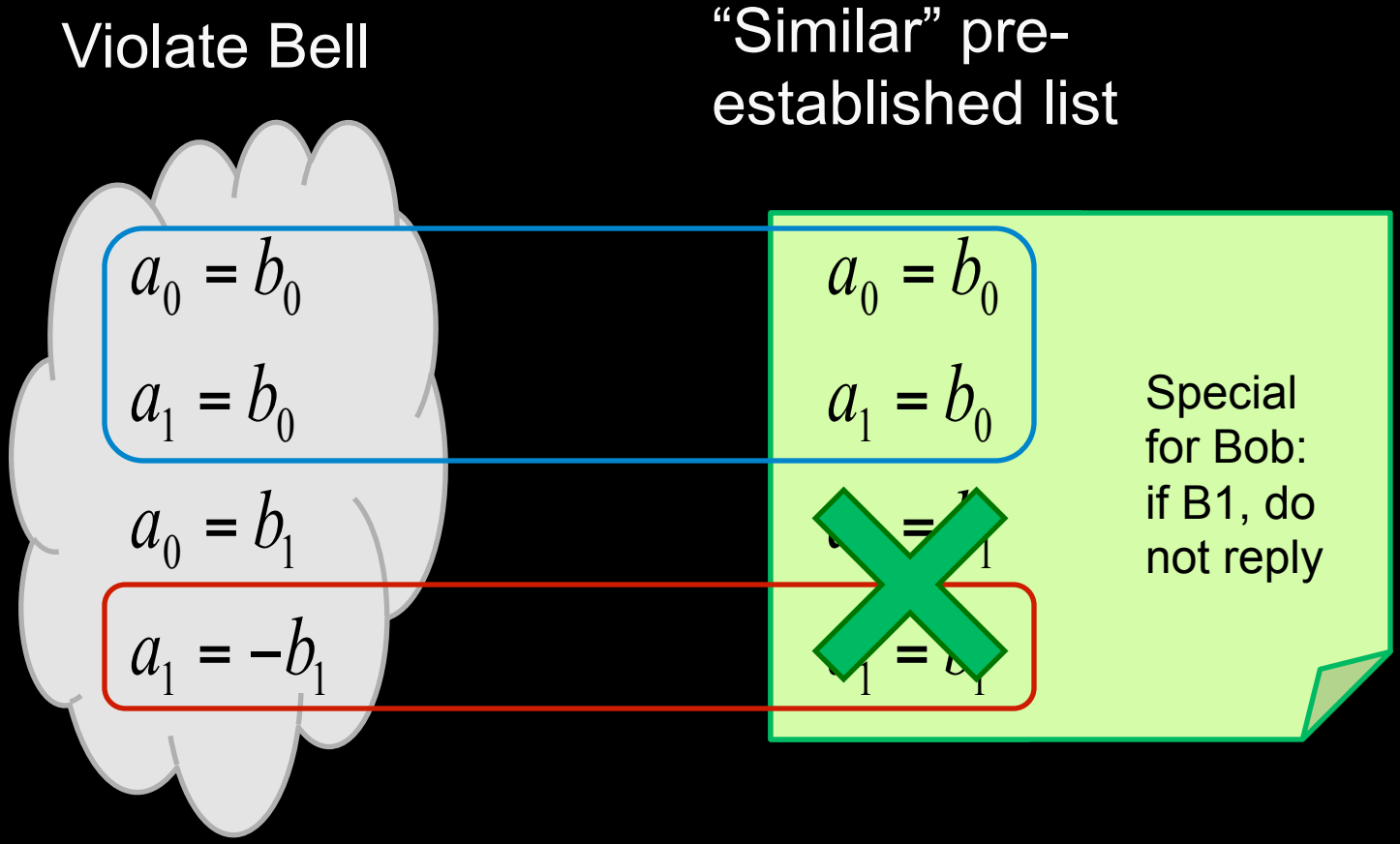
NUS
National University of Singapore

Centre for Quantum Technologies

# TOWARDS THE MAIN COURSE

## Challenges for experiments

# Detection loophole

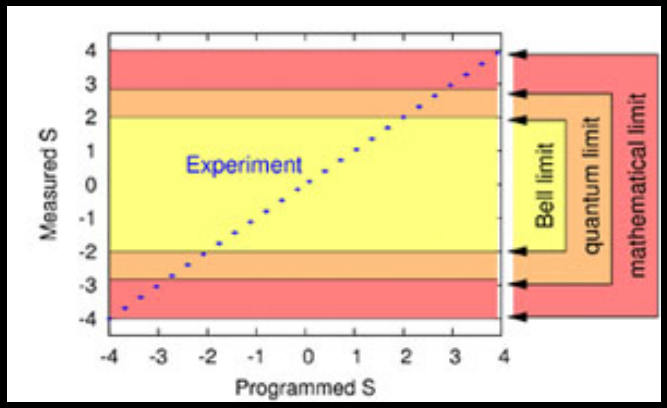


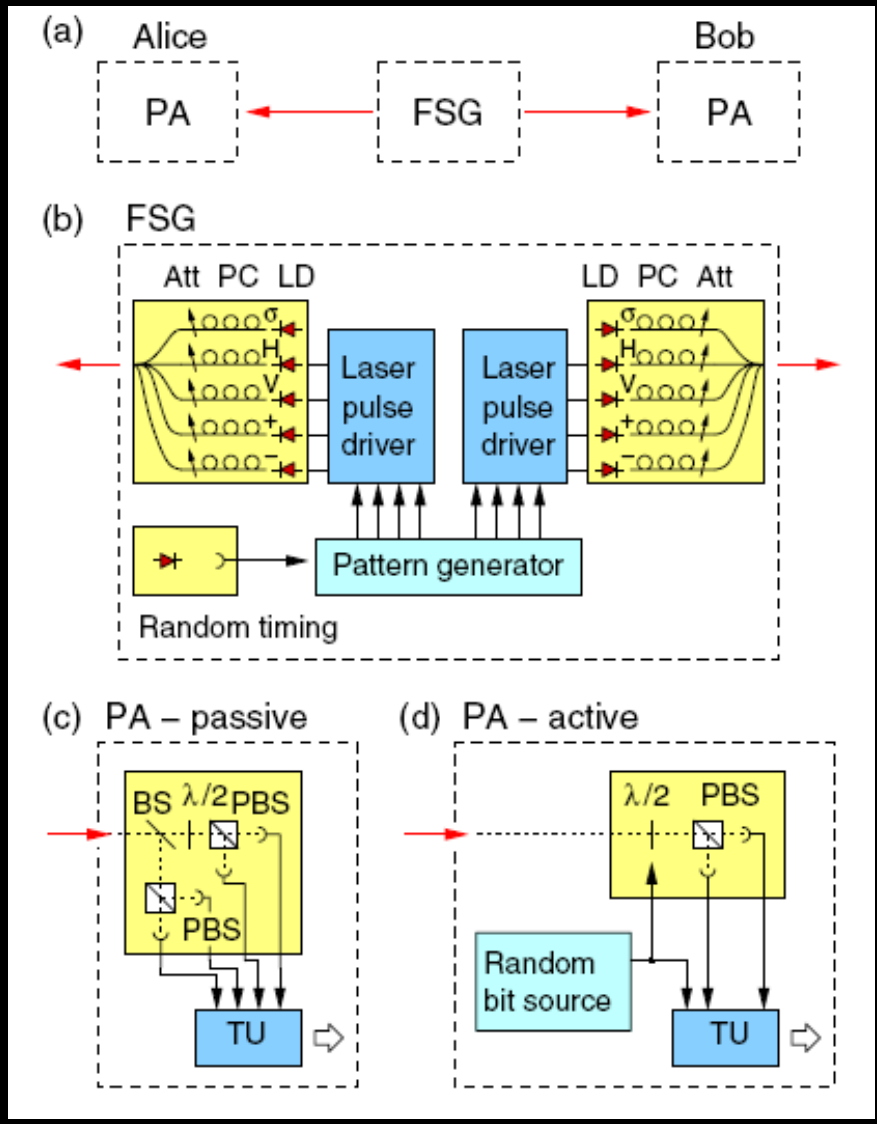

- This example has 50% losses on Bob, none on Alice. Symmetric thresholds are around 70-80%.
- Losses = inefficiency of detectors & losses in the channel (unless QND)

# What the hack??

## Faking the violation of Bell inequalities with "faked states"

- By exploiting the physics of some detectors, the FSG can choose which polarization is going to be detected.
- In an active choice of basis, if the other basis is chosen, no detector will fire: 50% detection loophole.




Gerhardt, Liu, Lamas-Linares, Skaar, Scarani, Kurtsiefer, Makarov, 2011

# Conclusion

- Loophole-free Bell violation ⇔ device-independent assessment of entanglement
- Quantitative assessment:
  - How long a secret key…
  - How many random bits…
  - How far from an ideal source…
- Challenges for theorists: not easy to prove results without knowing the Hilbert space
- Challenges for experiments: loophole-free tests
- Bell inequalities are not only “conceptual”, they are also “applied”.

# Q&A


Question

Further information

Answer
(hopefully not too random)

Group website
conneqt.quantumlah.org

Blog
Spreadquantum.wordpress.com

NUS National University of Singapore

Centre for Quantum Technologies