NUS
National University of Singapore

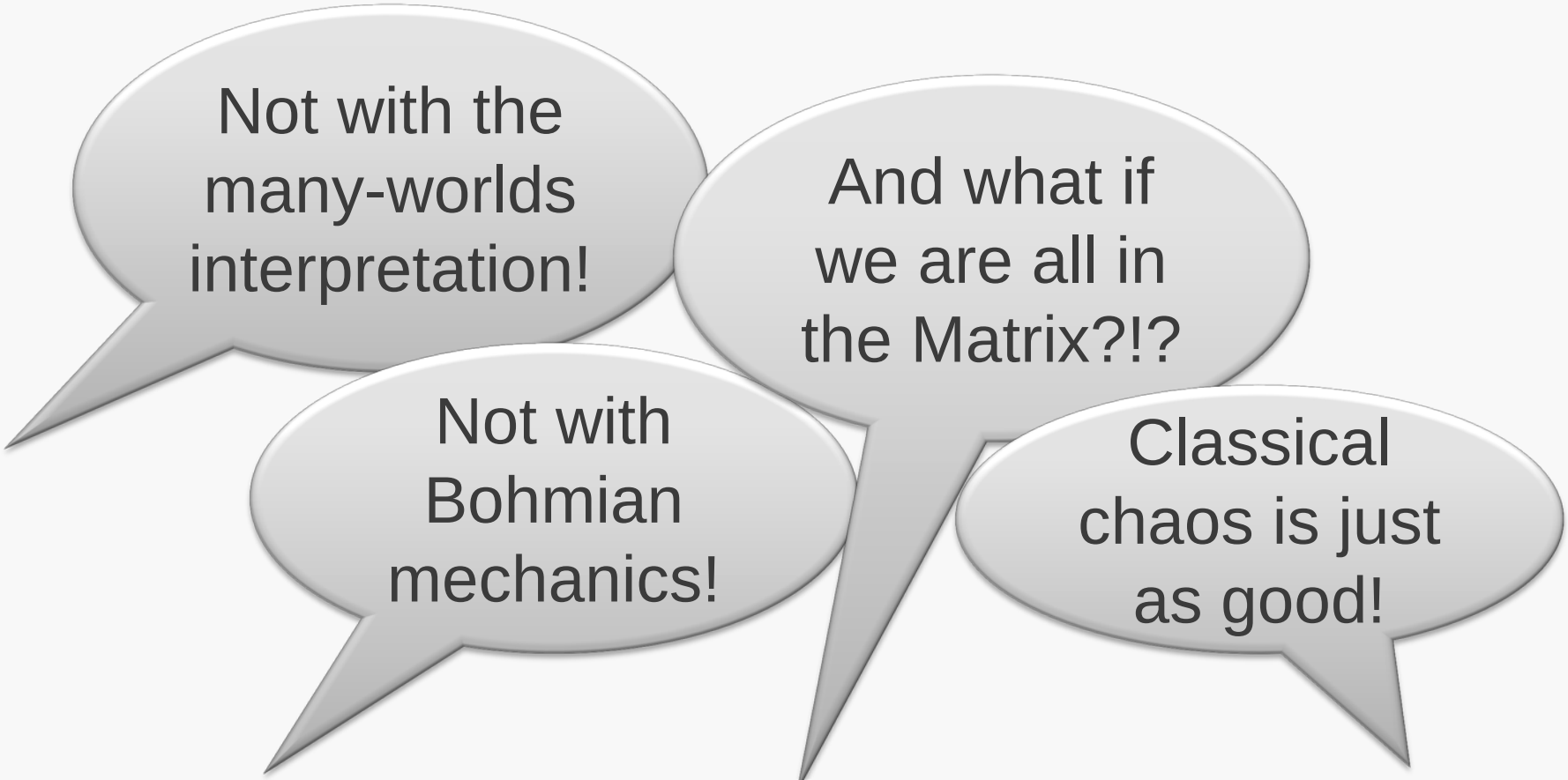
Randomness from quantum systems – a guided tour

Valerio Scarani

Centre for Quantum Technologies

Random = not fully predictable

Quantum physics ⇒ intrinsic randomness




KEEP
CALM
AND
RANDOM
FOR WHOM?
KeepCalmAndPosters.com

For a being in our universe?

NO

- For a being stretched across the multiverse, no randomness
- For a being capable of reading the pilot wave, no randomness
- For the robots controlling the Matrix, no randomness

YES

With limited computational power?

NO

Only quantum systems are random

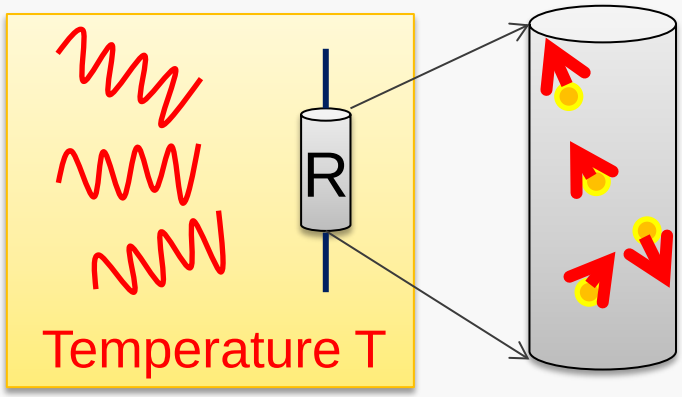
YES

- Classical processes can also be random, provided they are “happening” then and there (not pre-recorded).
- Quantum physics allows for device-independent certification of no pre-recording

Is classical just as good?

Classical

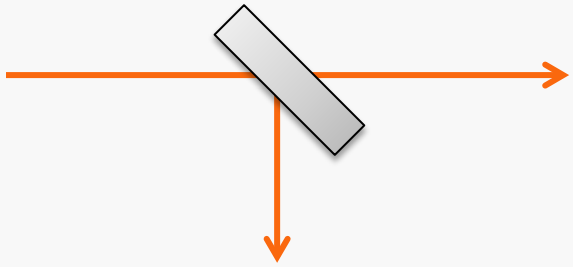
Example: thermal noise



Quantum

Example: photon on a beam-splitter

(or: prepare $|+z\rangle$, measure σ_x)

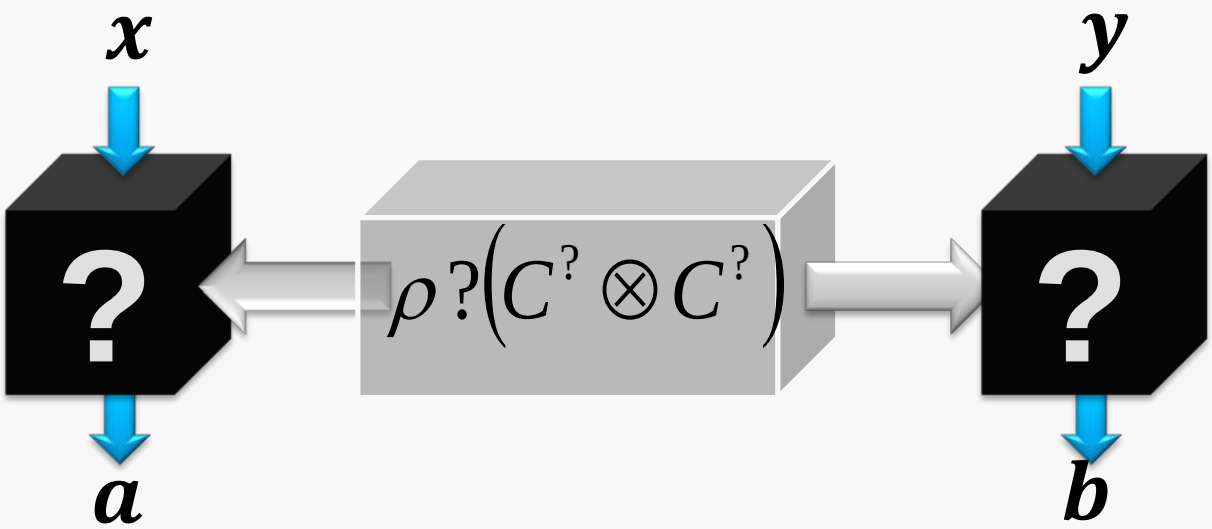


	Classical	Quantum	Comment
Random for whom?	Limited computational power	Also for Laplace's demon ("intrinsic")	Identical FAPP
Characterization	Mechanism to be known	Mechanism to be known	

$\Rightarrow$ At this level, the choice will be based on practical considerations: rate, stability, price…

BUT QM allows for <u>black-box certification</u> in more complex setups (Bell tests)

Bell = device-independent



$S_{obs} > S_L \Rightarrow$ "no LHV"

(a, b) random $\quad H_\infty(P) \geq f(S_{obs})$

Requirements:
- Entanglement ✓
- Close detection loophole
- No-signaling ✓
- Random choice of (x,y)

???

Centre for Quantum Technologies

Plan of the talk

- Systematic review
  - Random for whom: who is your adversary?
  - Characterization: what do you need to know about your devices?
- Our focus: theory to work with trusted experimentalists
  - More randomness from the same data
  - Not-very-useful experimental designs

NUS
National University of Singapore

Centre for Quantum Technologies

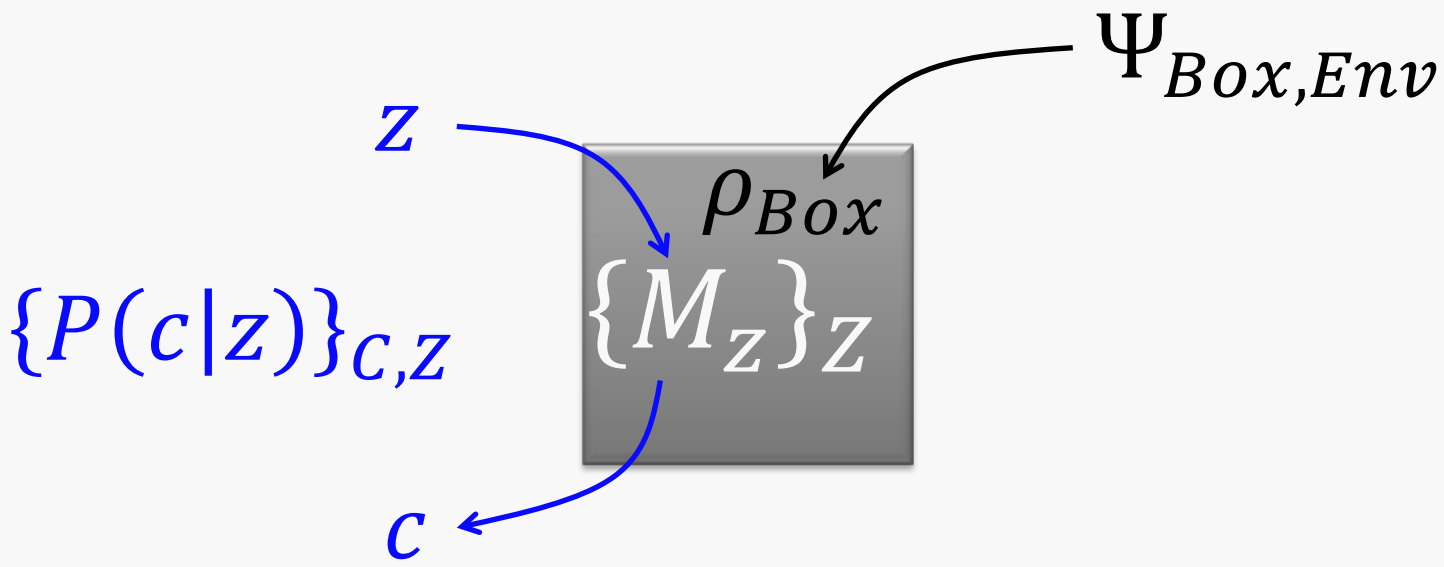
PART 1: SYSTEMATIC REVIEW OF SCENARIOS

LAW Yun Zhi, LE Phuc Thinh, Jean-Daniel BANCAL

Submitted to J. Phys. A (2014)

Who's who in randomness

USER wants to have certified randomness
ADVERSARY wants to know the user's data
PROVIDER builds the apparatus, does not care about learning the user's data

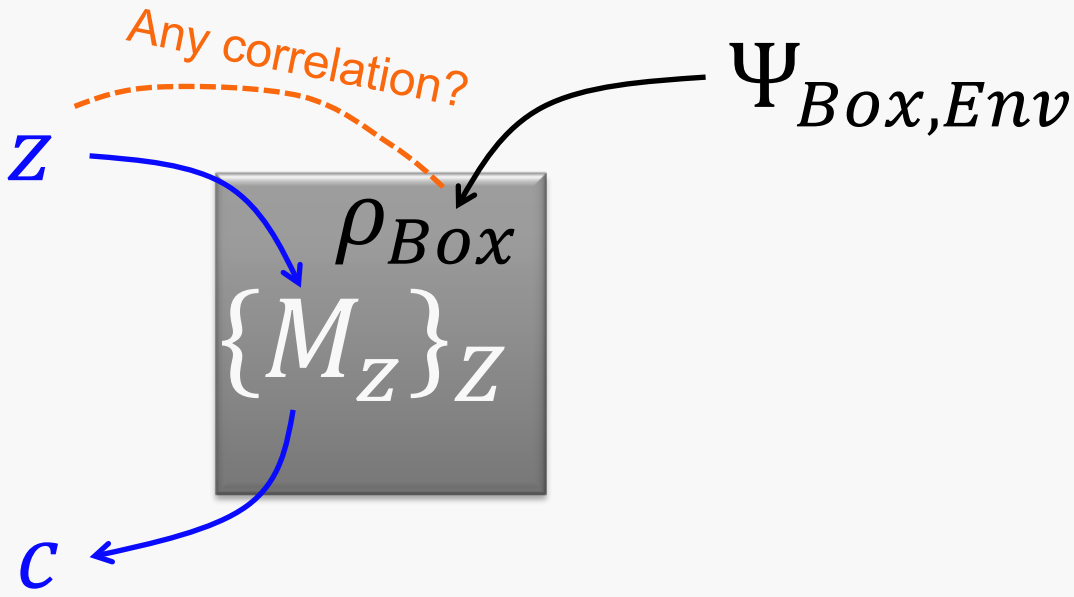


Goal of user: the adversary must not have full information about some of the c

- Where is the adversary?
- What does the user know about the device, i.e. $\rho, \{M_z\}$?

Centre for Quantum Technologies

Measurement (in)dependence

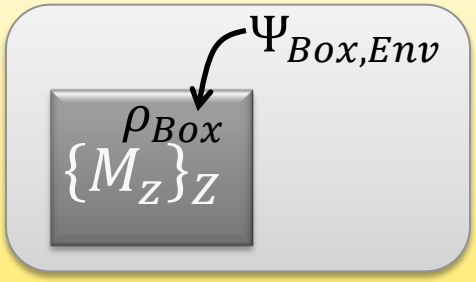


- Full correlation ⇒ impossible to certify any randomness
- Partial correlation ⇒ "randomness amplification"
- No correlation ("measurement independence"): usual scenario
  This talk: measurement independence assumed

IMPORTANT: measurement independence means that z must be random <u>for the process that chooses ρ</u>, not necessarily for the adversary (whom we have not introduced yet)

3 adversarial classes

Class I "trusted provider"

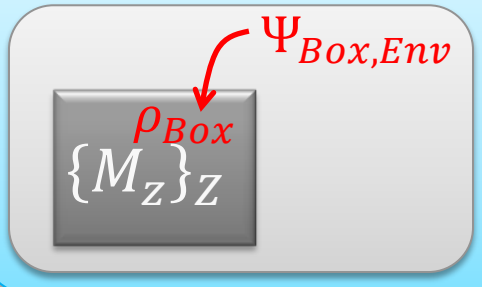


ϕ^{λ}_{Box} $\{M_z\}_z$

Adv

- Has the best possible classical knowledge of the state in each run and of the set of measurements
- Has not tampered with the lab in the past and has no access to it

Class II inspired by QKD

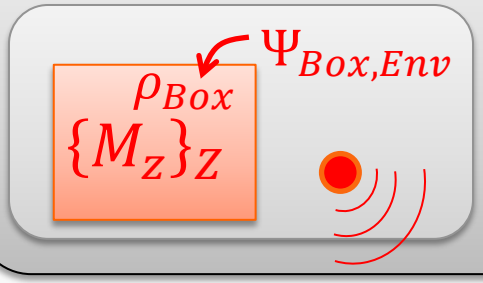


$\{M_z\}_z$

Adv

- Has the best possible classical knowledge of the set of measurements
- Is distributing the state in each run, and keeping a purification

Class III adversarial provider



User can still certify "quantumness" by running a loophole-free Bell test…
… however, a not-too-stupid provider has put an emitter in the box, to broadcast c at the end: no secure task is possible

Centre for Quantum Technologies

User's level of characterization

ρ_{Box}

$\{M_z\}_z$

"Tomography"

- Dimension of Hilbert space of ρ_{Box} known
- All the M_z known

$\Rightarrow$ Possible to reconstruct ρ_{Box}, then choose the M_z that gives the largest amount of randomness

"Device-independent"

- The devices are black boxes for the user
- As mentioned above, one needs:
  - Entanglement
  - Close detection loophole
  - No-signaling

  But the boxes don't need to be in separate labs, like in QKD

Anything in-between!

- Dimension bounded, M_z unknown
- "Steering": one black box, one tomography box
- Etc…

Example

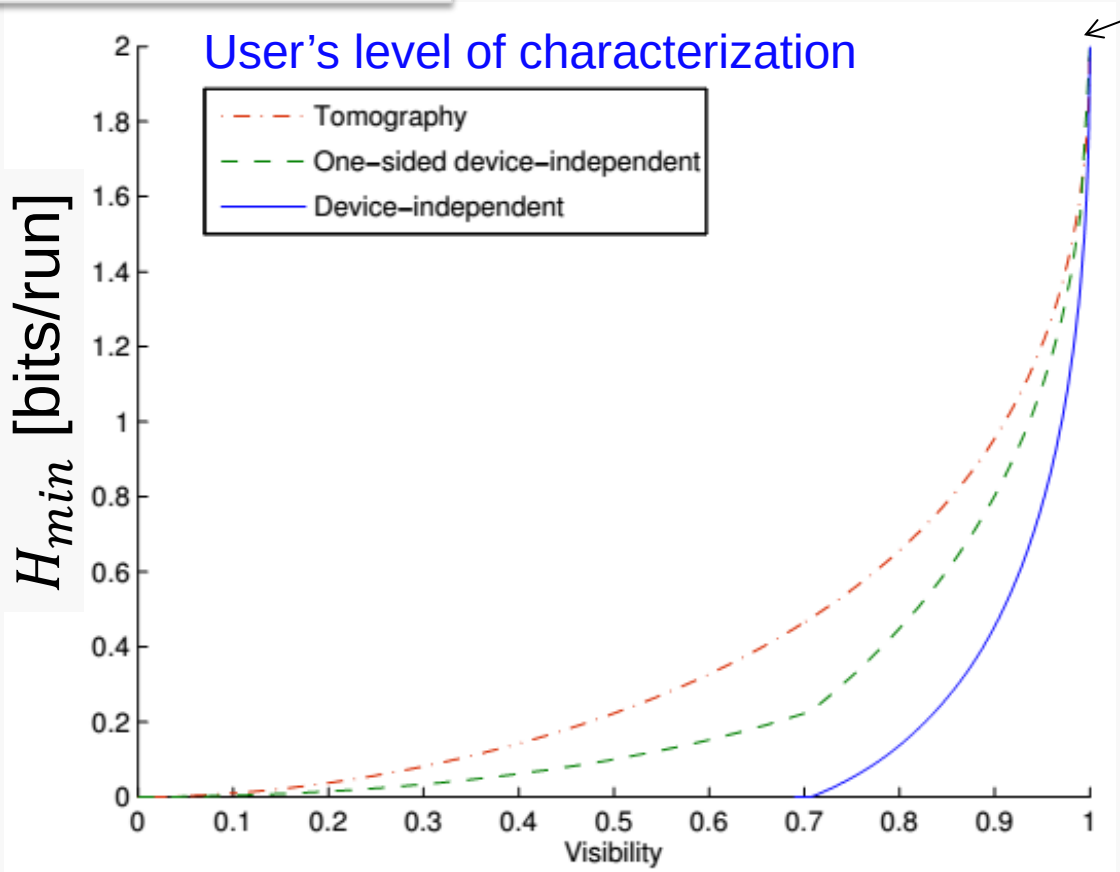
"Observed" data:
Asymptotic stats obtained from

$$\rho_V = V\,|\Phi\rangle\langle\Phi| + \frac{(1-V)I}{4}$$

Alice: $\{Z, X\}$, Bob: $\{Z, X, +, -\}$

Adversarial class I
(trusted provider)

V=1: two bits of randomness per run for all levels



Centre for Quantum Technologies

Take-away messages

- Recipe
  - Pick an adversarial class
  - Pick a user's characterization level
  - Compute the guessing probability (min-entropy)
    - I skipped this part, technicalities in the papers
- Avoid confusions:
  - "Device-independent" is about the characterization of the devices by the user, not about the power of the adversary
  - Adversarial provider: one can certify quantumness, entanglement, violation of local realism… but can't guarantee any secure task

PART 2: SOME RECENT RESULTS

Tailored for assessment of experiments

Adversarial class I ("trusted provider")

Various levels of characterization

More randomness from the same data /1

Previous works

$$\{P(a,b|x,y)\} \longrightarrow CHSH(P) = S$$

$$P_{guess} \equiv \max_{a,b} P(a,b|0,0;\lambda) = f(S)$$

First improvement: no need to pass through an inequality

$$P_{guess} \equiv \max_{a,b} P(a,b|0,0;\lambda) = f(\{P(a,b|x,y)\})$$

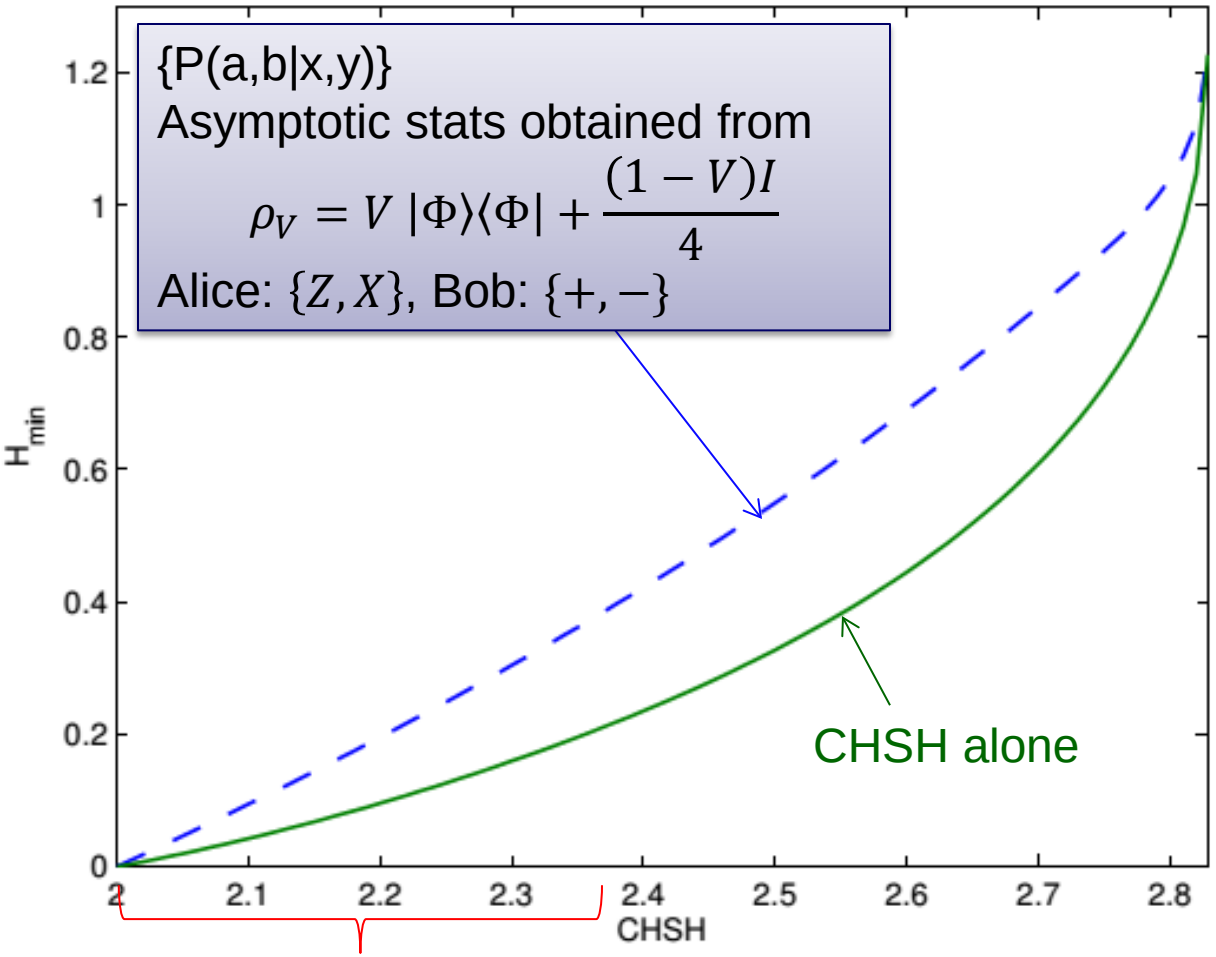
Second improvement: "trusted provider" $\Rightarrow$ better to use all settings

$$P_{guess} \equiv \sum_{x,y} p(x,y) \max_{a,b} P(a,b|x,y;\lambda)$$

Bancal, Sheridan, VS, New J. Phys. 16, 033011 (2014).
Similar: Nieto-Silleras, Pironio, Silman, New J. Phys. 16, 013035 (2014)

More randomness from the same data /2

Second improvement



Any experiment with SPDC is restricted to this region [Caprara Vivoli et al, arXiv:1405.1939]: our method gives twice as much randomness.

Randomness & ancillas /1

Tomography level of characterization (in device-independent, the box is black, so we have no ideas whether ancillas are there or not)

Case study: tomography yields $\rho = I/2$: can one extract intrinsic randomness?

One projective measurement (say Z): no randomness
Proof: ρ could be prepared by mixing the eigenstates of Z, and the adversary has maximal knowledge of which state is used in each run.

Two or more projective measurements:

randomness if adversary does not hold a purification
Proof: "uncertainty relations": in no run the state can be both eigenstate of Z and X (but if adversary has purification, she can steer later)

One POVM:

randomness… but not more than what is in the ancilla (so just as well measure the ancilla alone)
Proof: Law, Le, Bancal, VS, arXiv:1401.4243

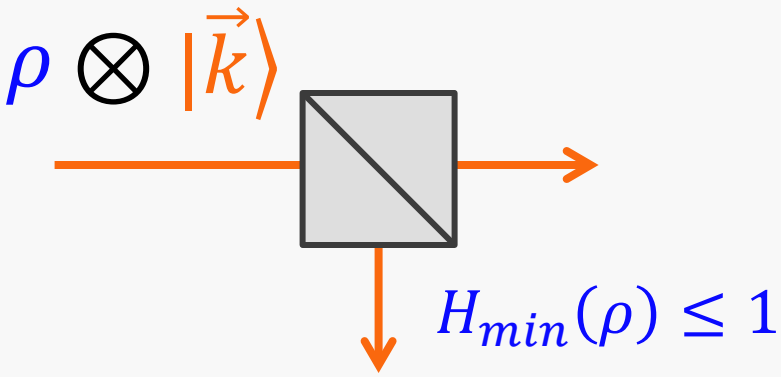
Randomness & ancillas /2

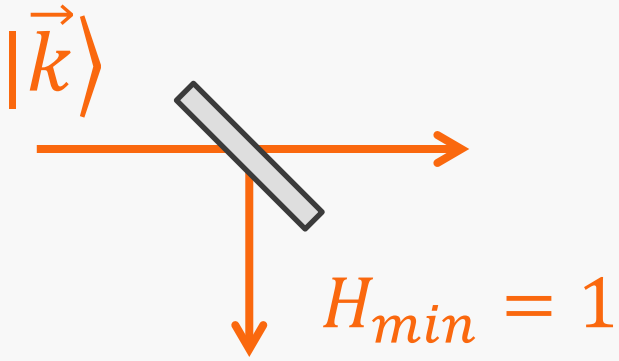
Tomography level of characterization (in device-independent, the box is black, so we have no ideas whether ancillas are there or not)

Case study: pointer measurements

Initial goal: randomness from degree of freedom A, with ρ_A known
BUT if A can be measured only by coupling to a pointer… the pointer is initially in a well-defined state…
… so think if you can't get more randomness by measuring directly the pointer in a conjugated basis, ignoring A.

Example: A = polarization





For the referee ☺