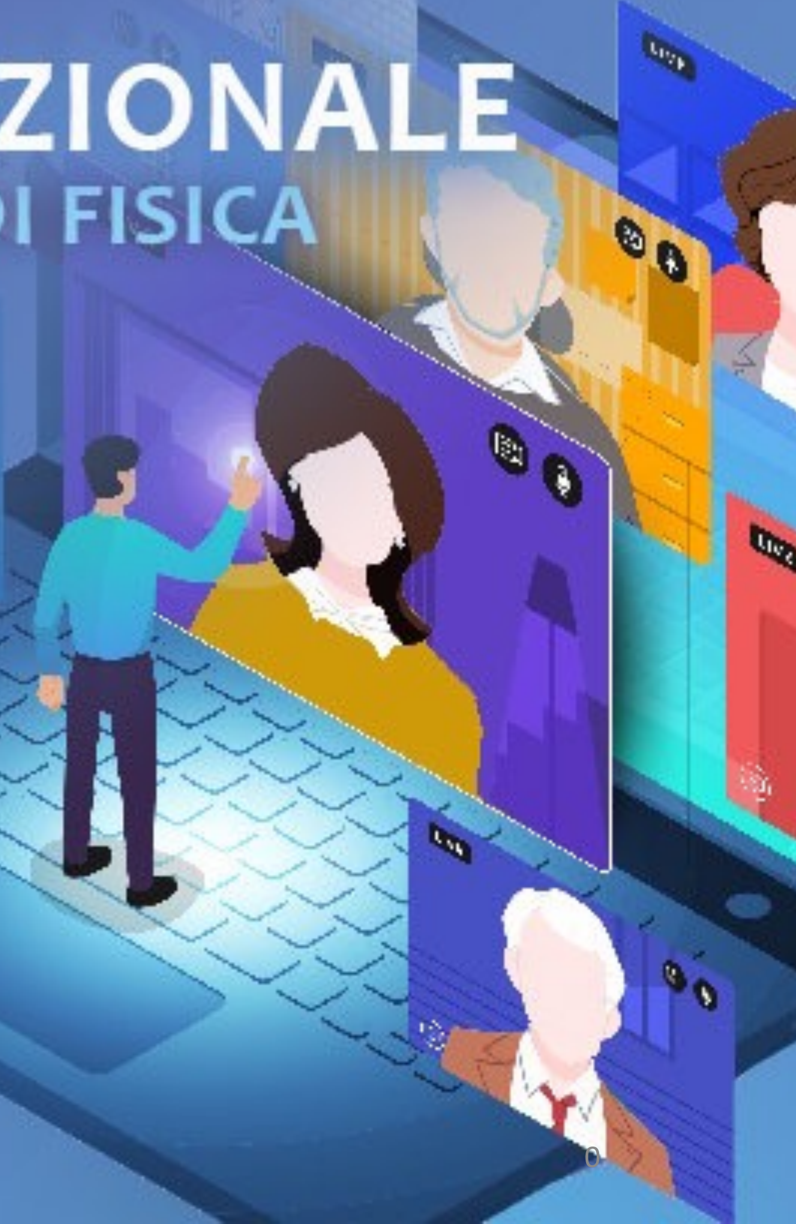
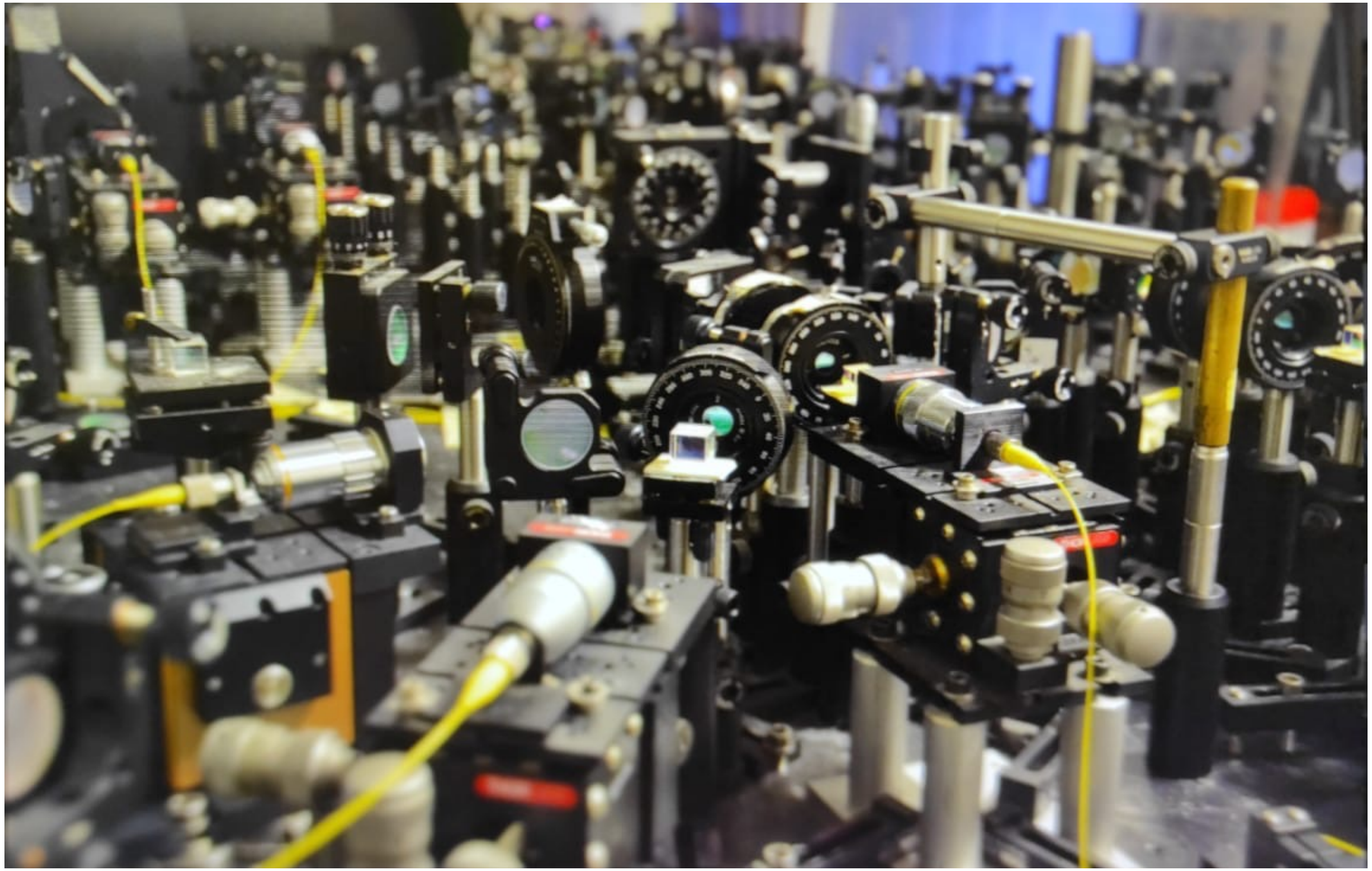
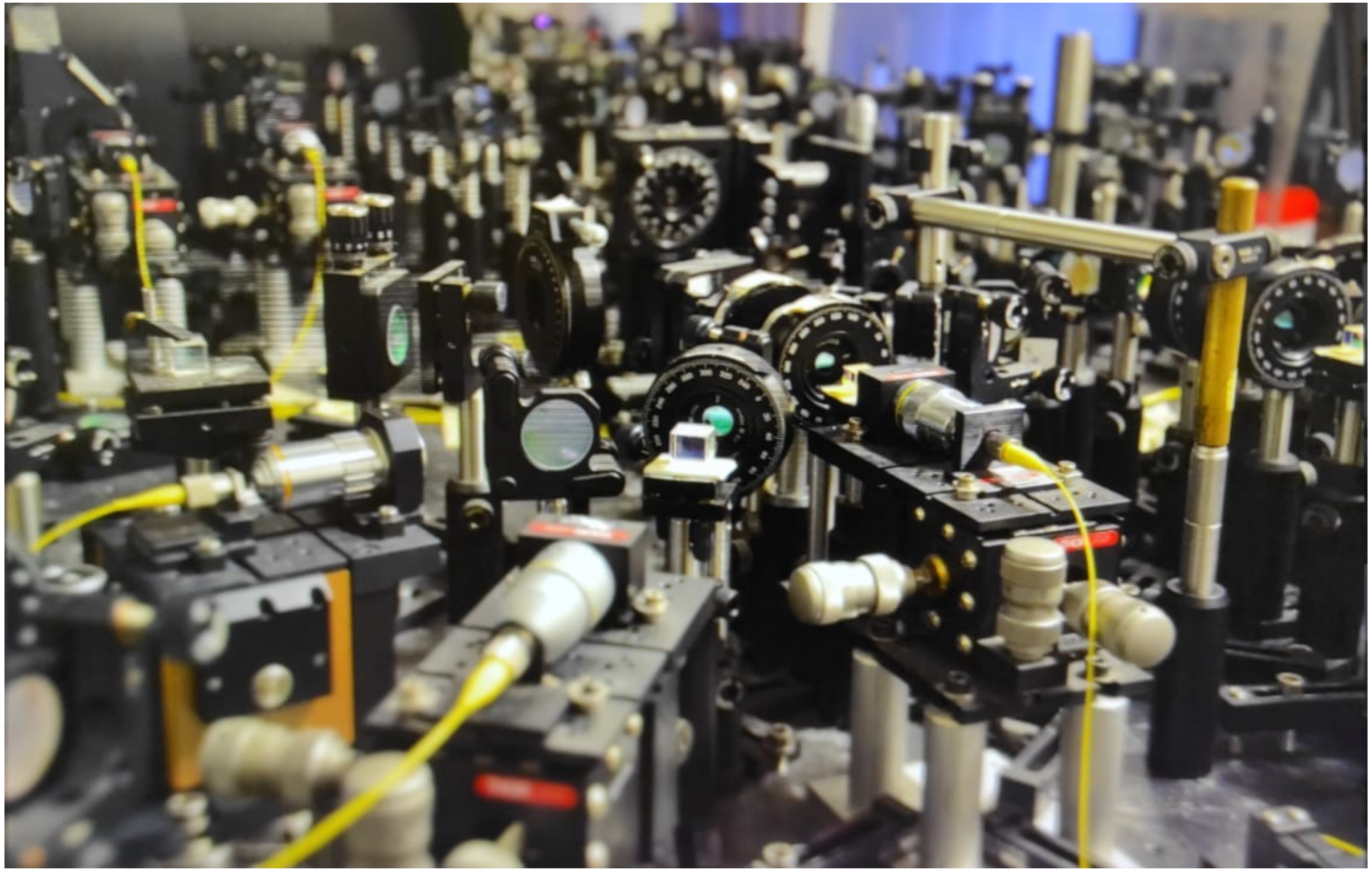
107° CONGRESSO NAZIONALE
della SOCIETÀ ITALIANA DI FISICA

Device-independent certification of quantum protocols

Iris Agresti, La Sapienza university of Rome

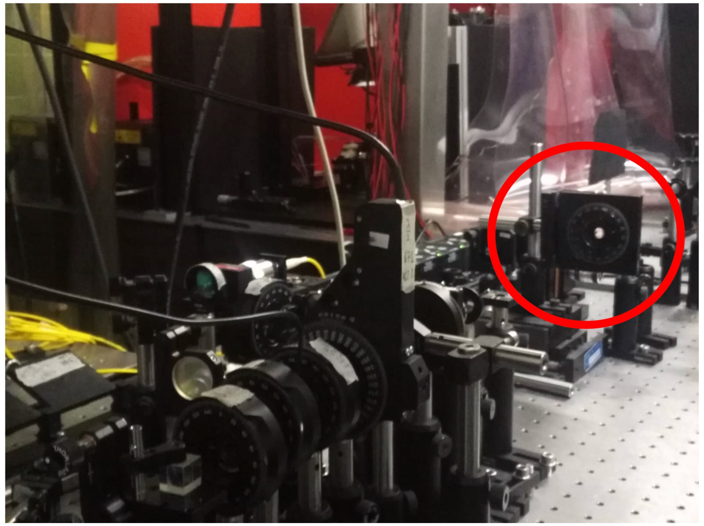


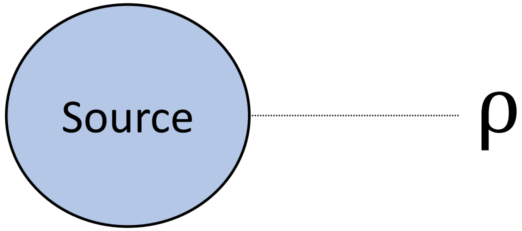




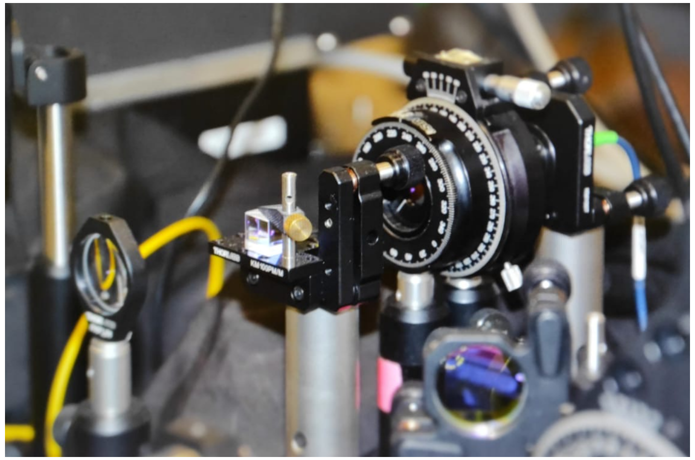
How can I be sure it is working?

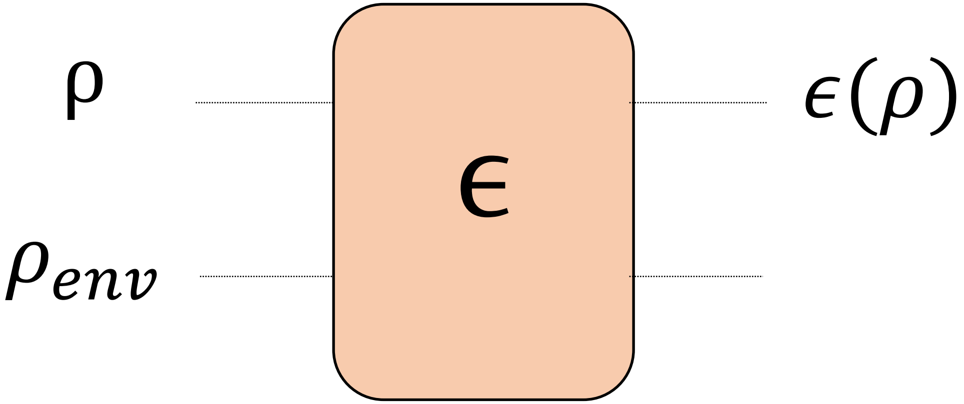
Examples of certification protocols





Quantum state tomography





Quantum process tomography

What are the drawbacks?

Inefficient procedures

The number of required measurements scales exponentially with the size of the system

Full control over the apparatus

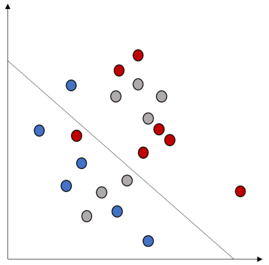
We need to trust that the apparatus is performing the right measurements

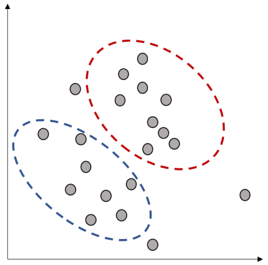
Can we solve these issues?

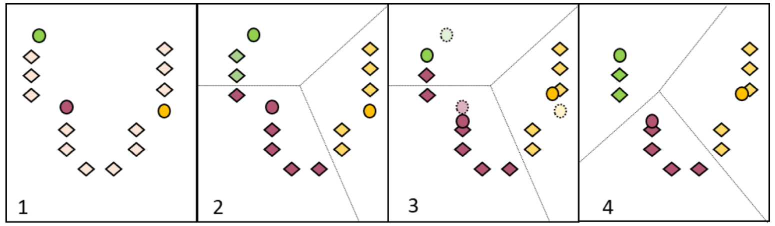
Can we solve these issues?

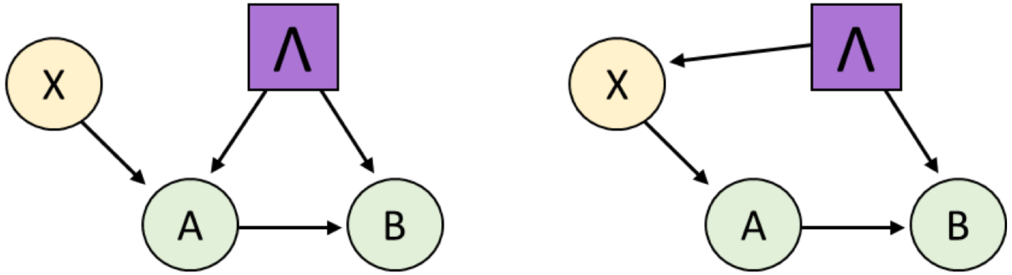
Efficient learning algorithms

Device Independent protocols



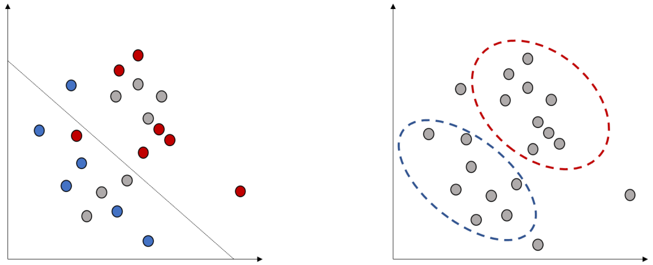


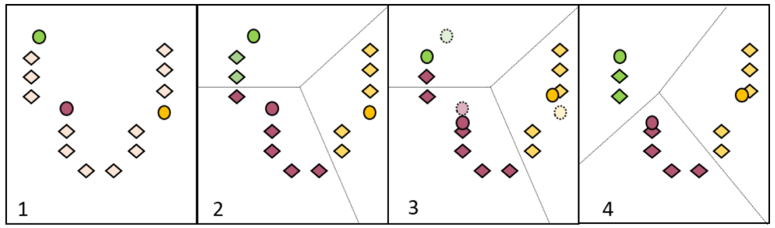




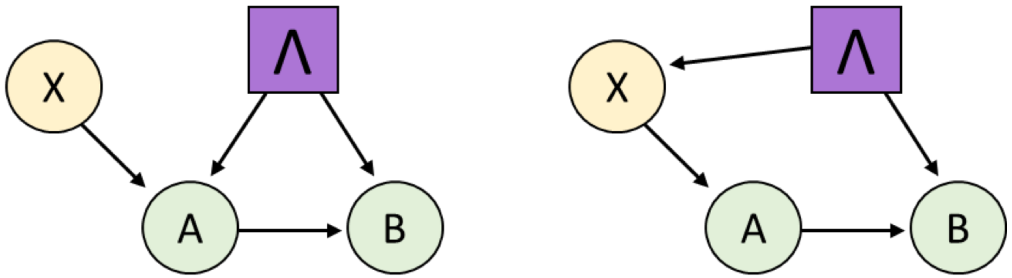
Can we solve these issues?

Efficient learning algorithms





Device Independent protocols



1. I. Agresti et al., Communications Physics, 3, 110 (2020).
2. I. Agresti et al., arXiv:2108.08926 (2021).
3. I. Agresti et al., PRX Quantum 2, 020346 (2021).

Device Independent Protocols

Device Independent Protocols

Device Independent Protocols

Device Independent protocols can be verified, relying solely on the input/output statistics.

Device Independent Protocols

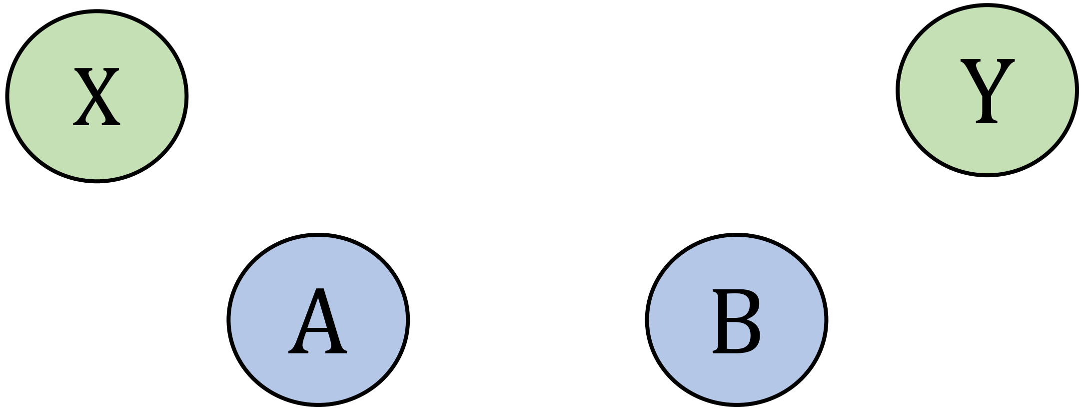
Device Independent protocols can be verified, relying solely on the input/output statistics.

How do we build a DI protocol?

Causal Inference

We can detect non-classical correlations

Device-Independently, exploiting causal inference.



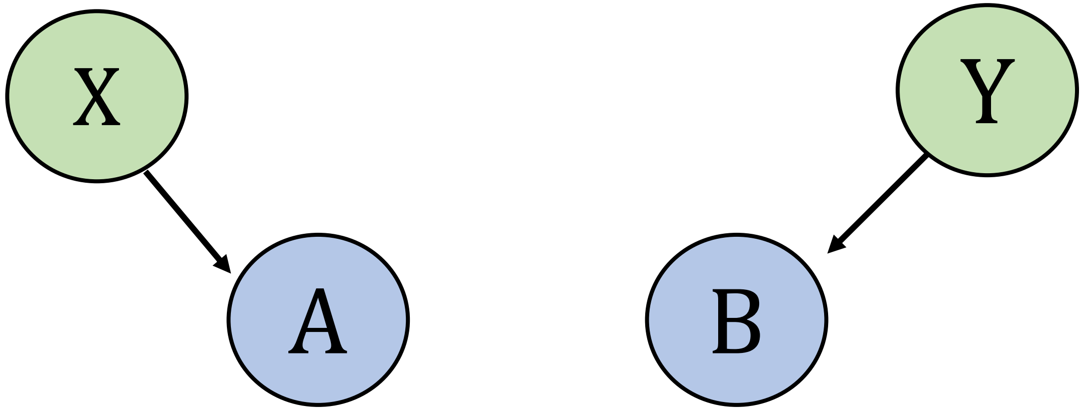
p(a,b,x,y)

collected statistics

J. Pearl, Cambridge University Press, II edition (2009)

Causal Inference

We can detect non-classical correlations
Device-Independently, exploiting causal inference.



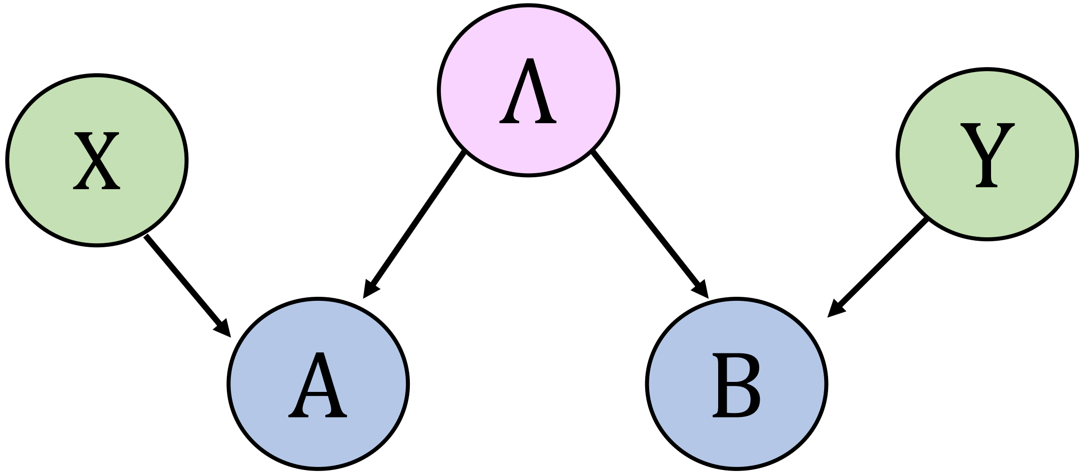
p(a,b|x,y)

collected statistics

J. Pearl, Cambridge University Press, II edition (2009)

Causal Inference

We can detect non-classical correlations Device-Independently, exploiting causal inference.



$p(a,b|x,y)$

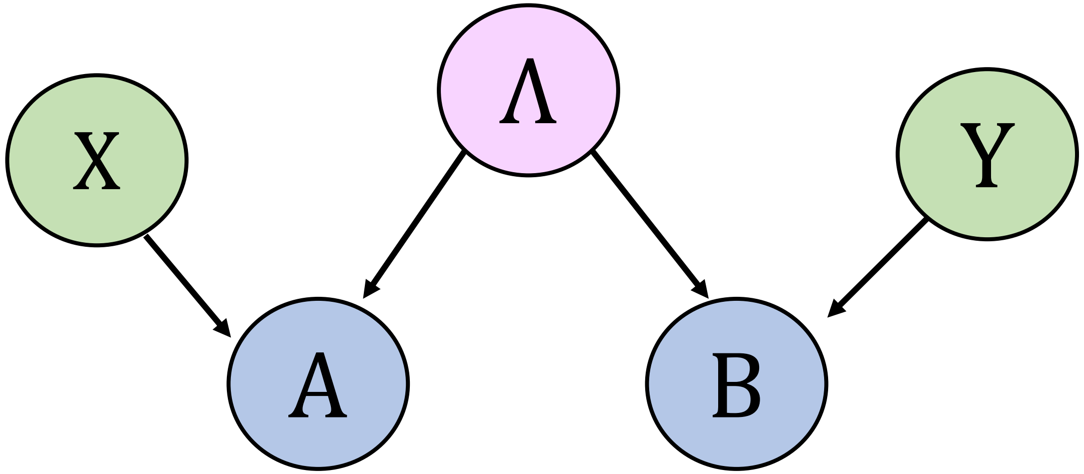
collected statistics

J. Pearl, Cambridge University Press, II edition (2009)

Causal Inference

We can detect non-classical correlations

Device-Independently, exploiting causal inference.



$p(a,b|x,y)$

collected statistics

$$\sum_{a,b,x,y} c_{abxy} p(a,b|xy) \leq 2$$

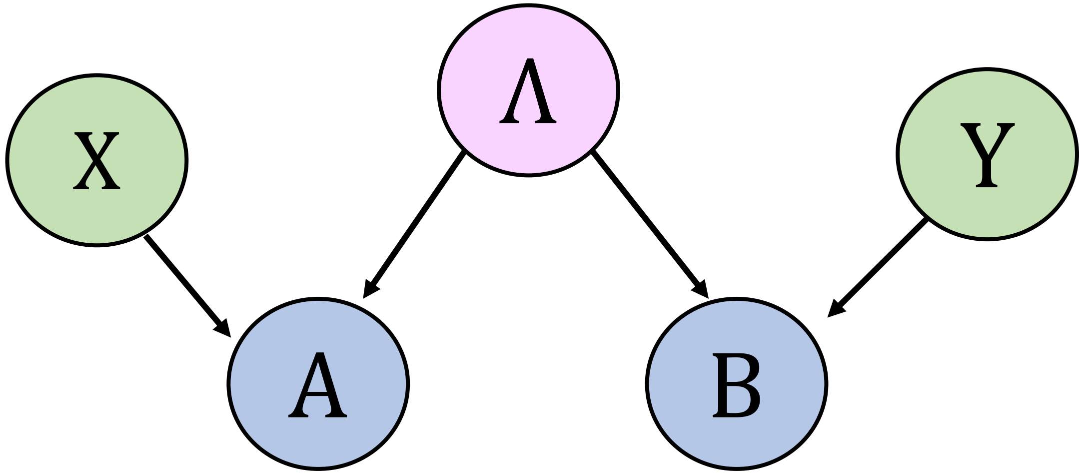
CHSH inequality

J. Pearl, Cambridge University Press, II edition (2009)

Causal Inference

We can detect non-classical correlations

Device-Independently, exploiting causal inference.



$$\sum_{a,b,x,y} c_{abxy} p(a,b|xy) \leq 2$$

p(a,b|x,y)

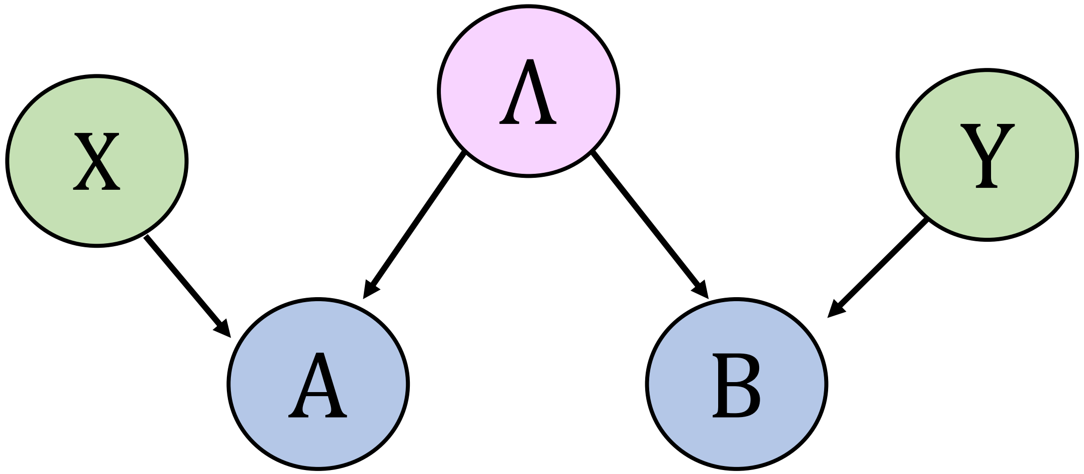
collected statistics

violation

Causal Inference

We can detect non-classical correlations

Device-Independently, exploiting causal inference.



p(a,b|x,y)

collected statistics

$$\sum_{a,b,x,y} c_{abxy} p(a,b|xy) \leq 2$$

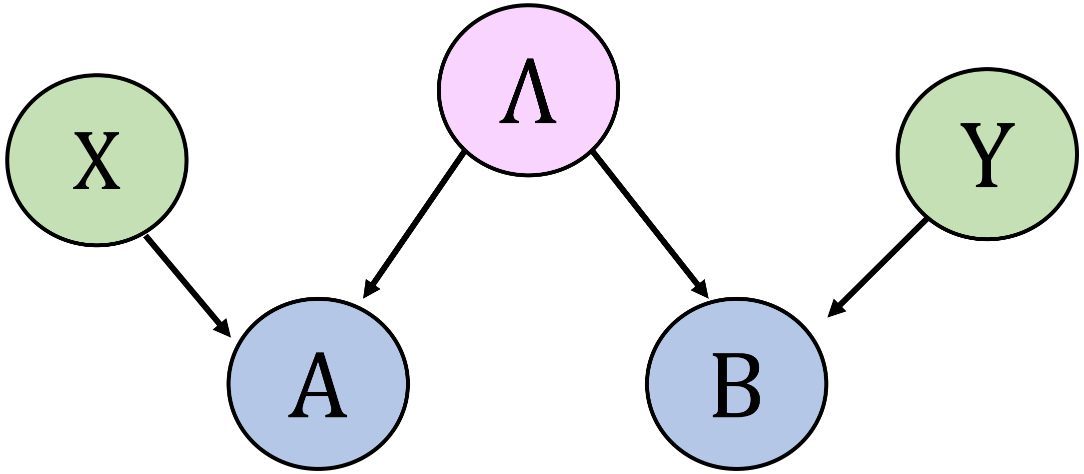
violation

Different underlying causal structure

Causal Inference

We can detect non-classical correlations

Device-Independently, exploiting causal inference.



p(a,b|x,y)

collected statistics

$$\sum_{a,b,x,y} c_{abxy} p(a,b|xy) \leq 2$$

violation

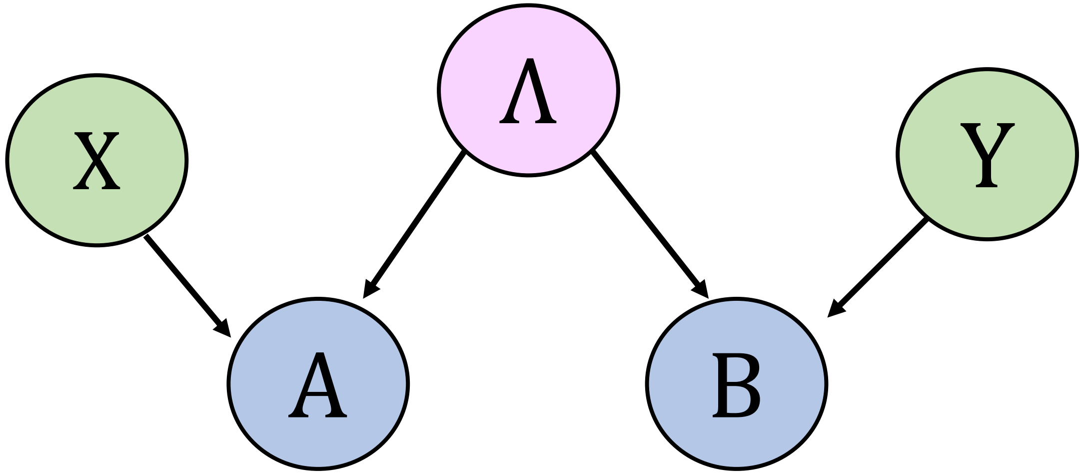
Different underlying causal structure

non-classical correlations

Causal Inference

We can detect non-classical correlations

Device-Independently, exploiting causal inference.



p(a,b|x,y)

collected statistics

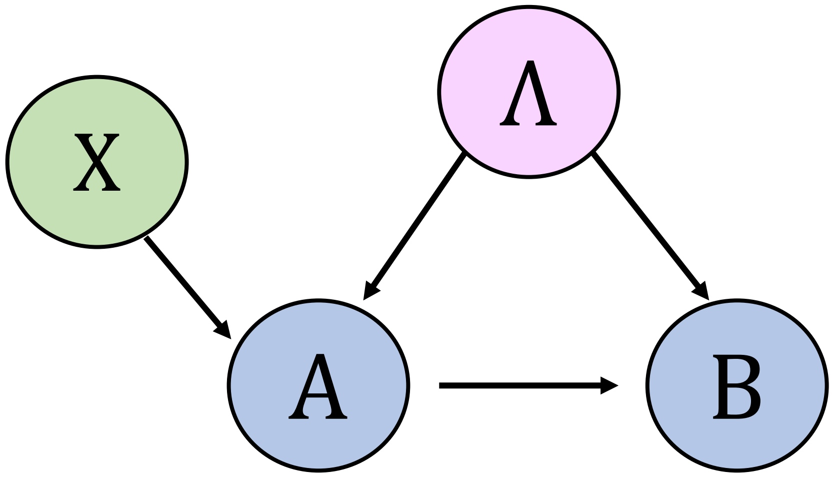
$$\sum_{a,b,x,y} c_{abxy} p(a,b|xy) \leq 2$$

violation

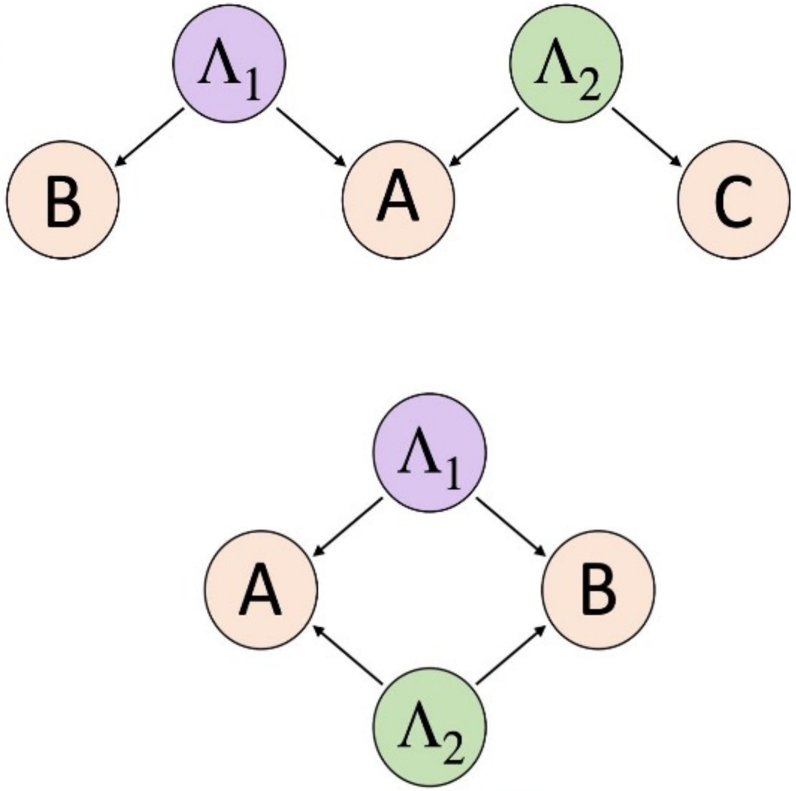
Different underlying causal structure

non-classical correlations ✓

Can we consider different scenarios?

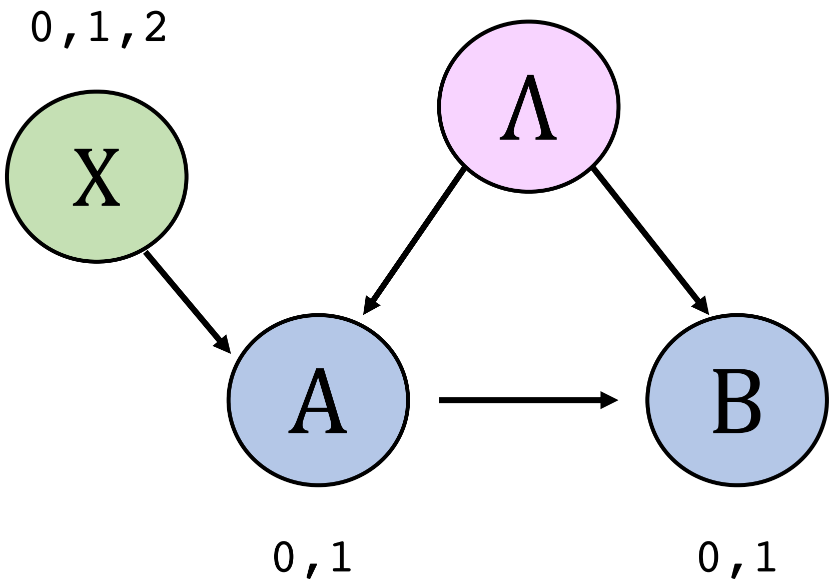


Instrumental process



Quantum network
building blocks

Instrumental process



p(a,b|x)

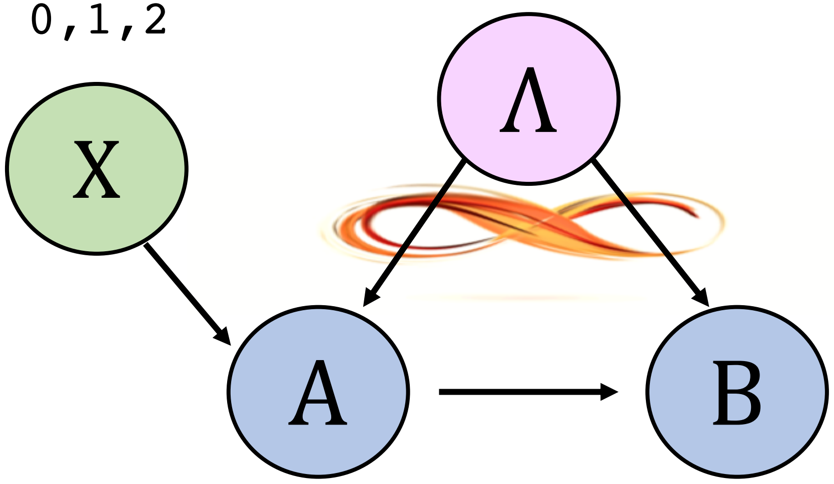
Instrumental Inequality

$$-\langle B\rangle_0 + 2\langle B\rangle_1 + \langle A\rangle_0 - \langle AB\rangle_0 + 2\langle AB\rangle_2 \equiv \mathcal{I} \leq 3$$

with $\langle AB\rangle_x = \sum_{a,b=0,1}(-1)^{a+b}p(a,b|x)$

I. Agresti et al., Communications Physics, **3**, **110** (2020).

Instrumental process



Instrumental Inequality

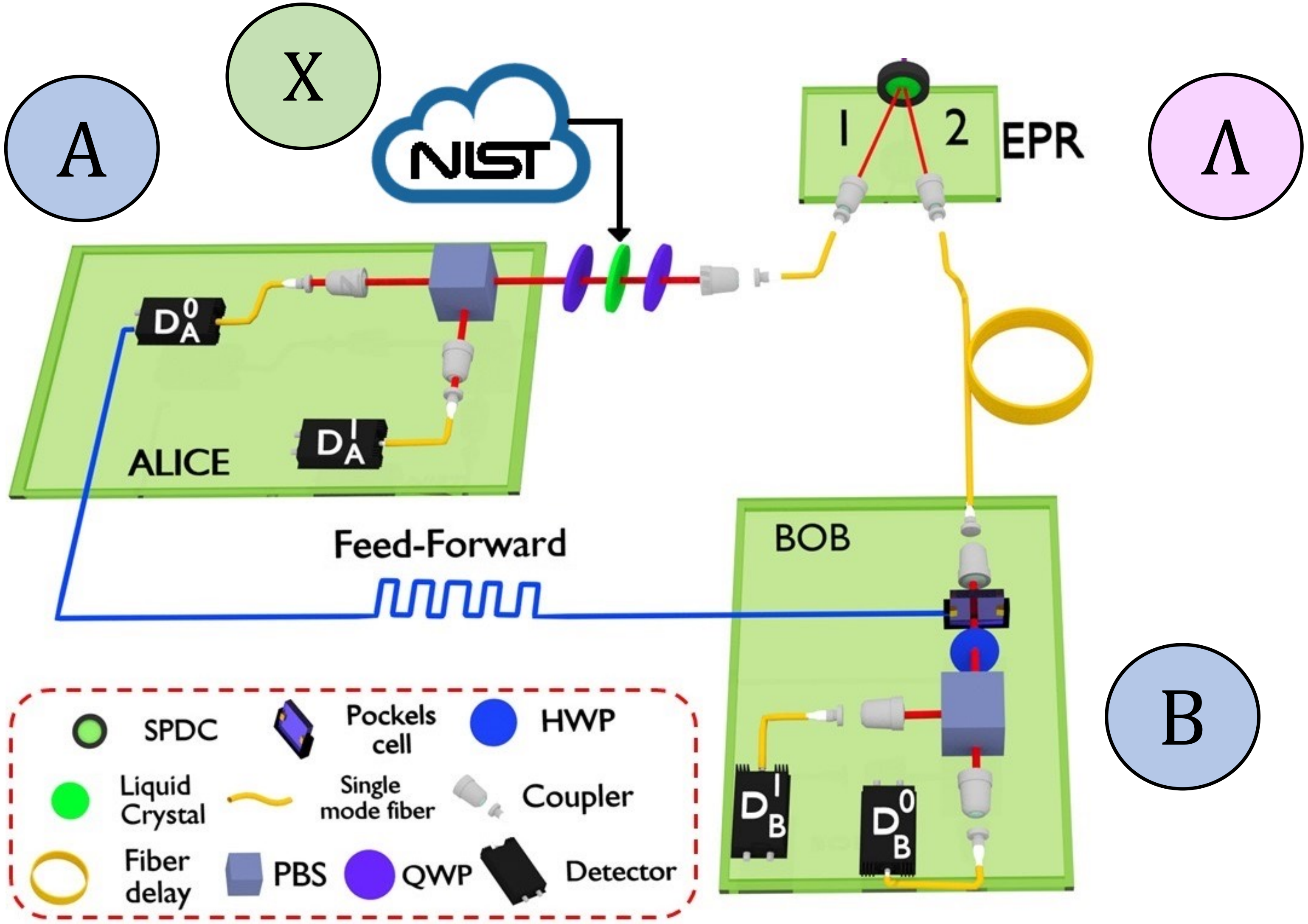
$$-\langle B\rangle_0 + 2\langle B\rangle_1 + \langle A\rangle_0 - \langle AB\rangle_0 + 2\langle AB\rangle_2 \equiv \mathcal{J} \leq 3$$

with $\langle AB\rangle_x = \sum_{a,b=0,1}(-1)^{a+b}p(a,b|x)$

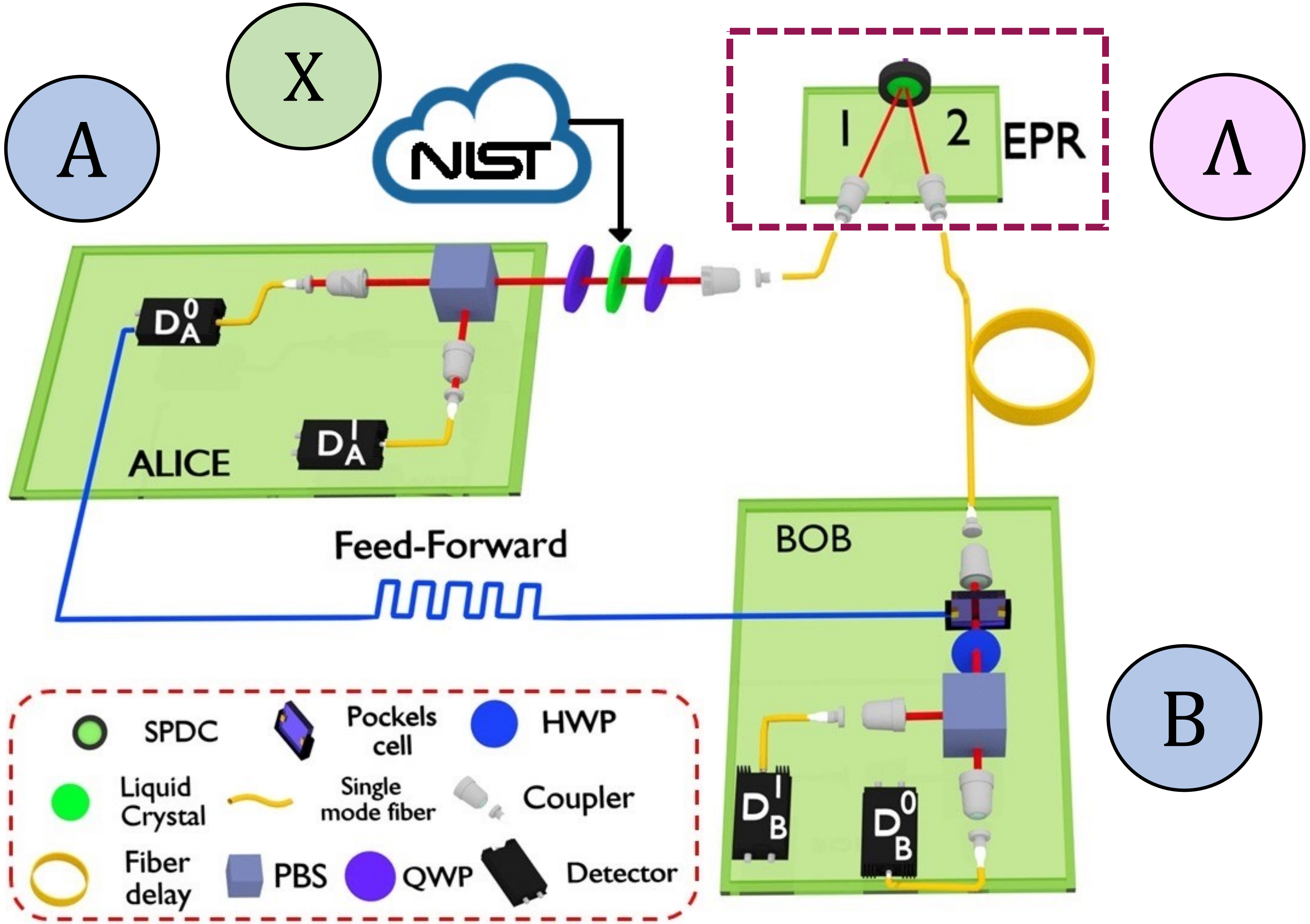
$$\mathcal{J} \leq 1 + 2\sqrt{2} \simeq 3.82$$

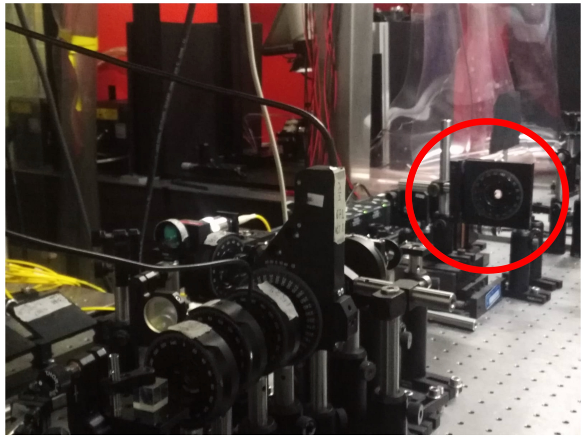
R. Chaves, G. Carvacho, I. Agresti, V. Di Giulio, L. Aolita, S. Giacomini, F. Sciarrino, *Nature Physics* **14**, 291-296 (2018)

Experimental Implementation



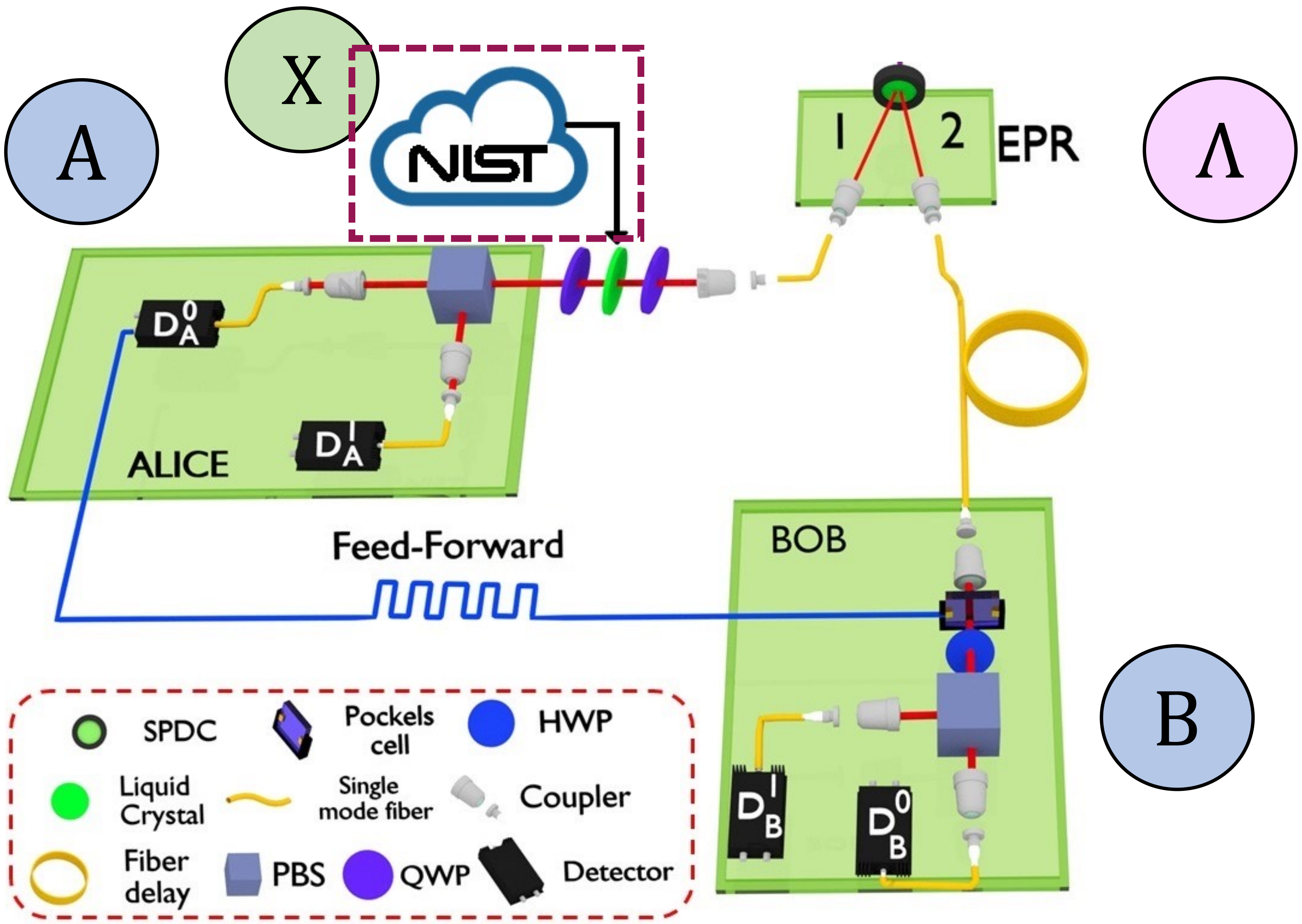
Experimental Implementation





BBO type II crystal

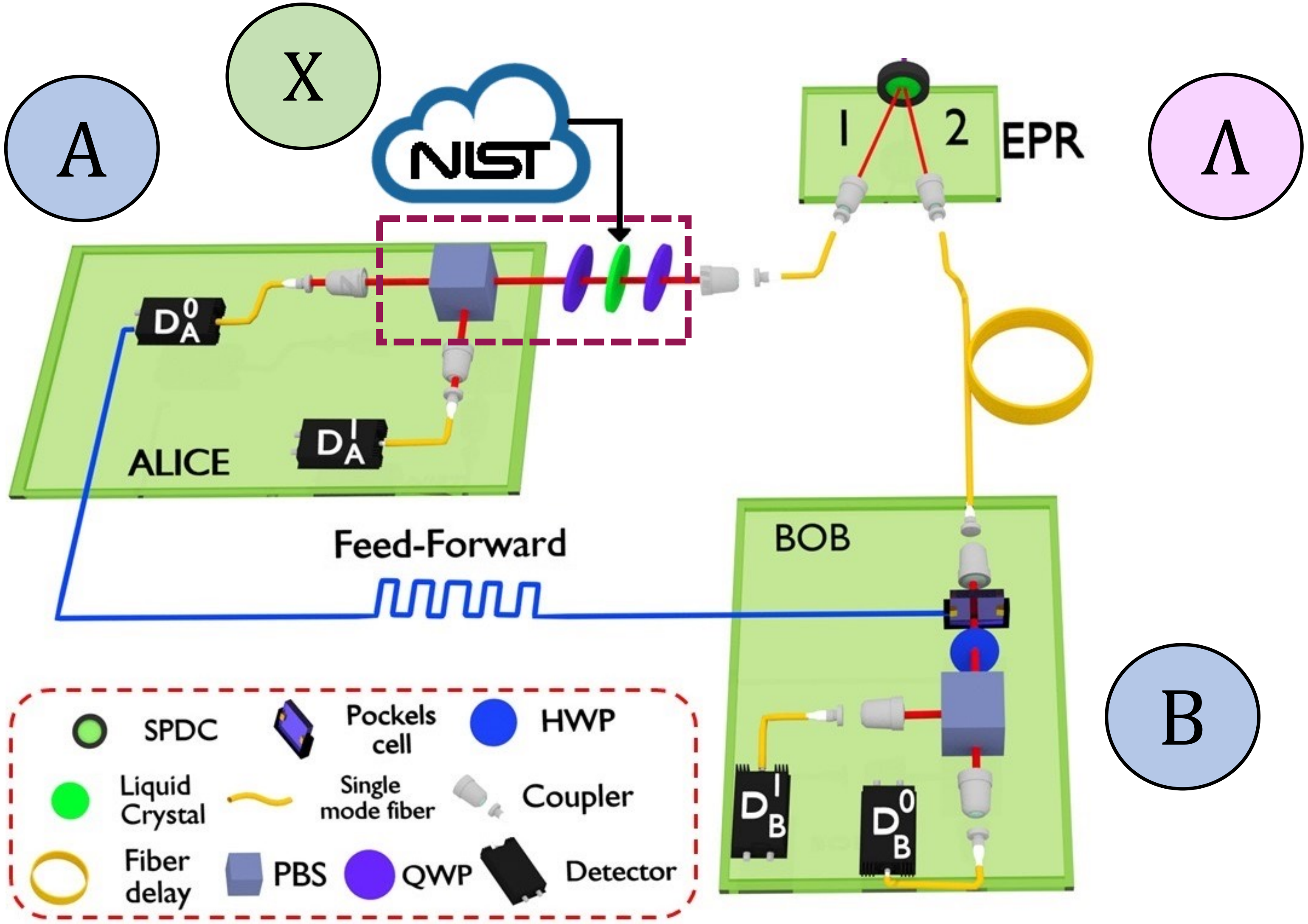
Experimental Implementation

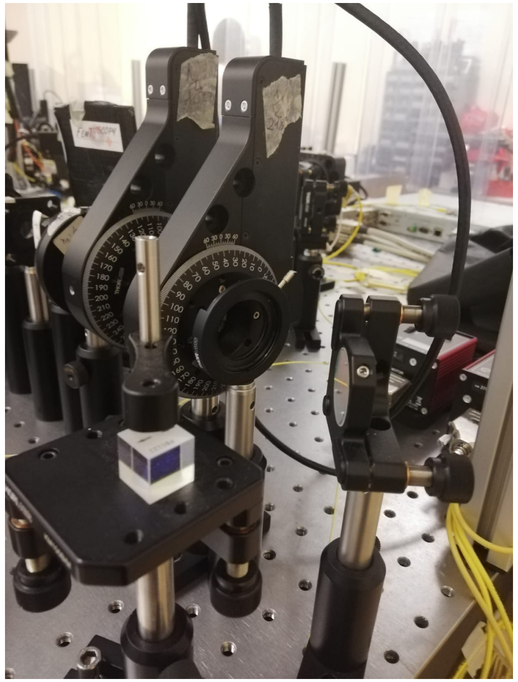


NIST Randomness Beacon
512 bit/minute

M. J. Fischer et al. *Proc. International Conf. on Security and Cryptography* **434-438** (2011)

Experimental Implementation





Measurement station

Experimental Implementation

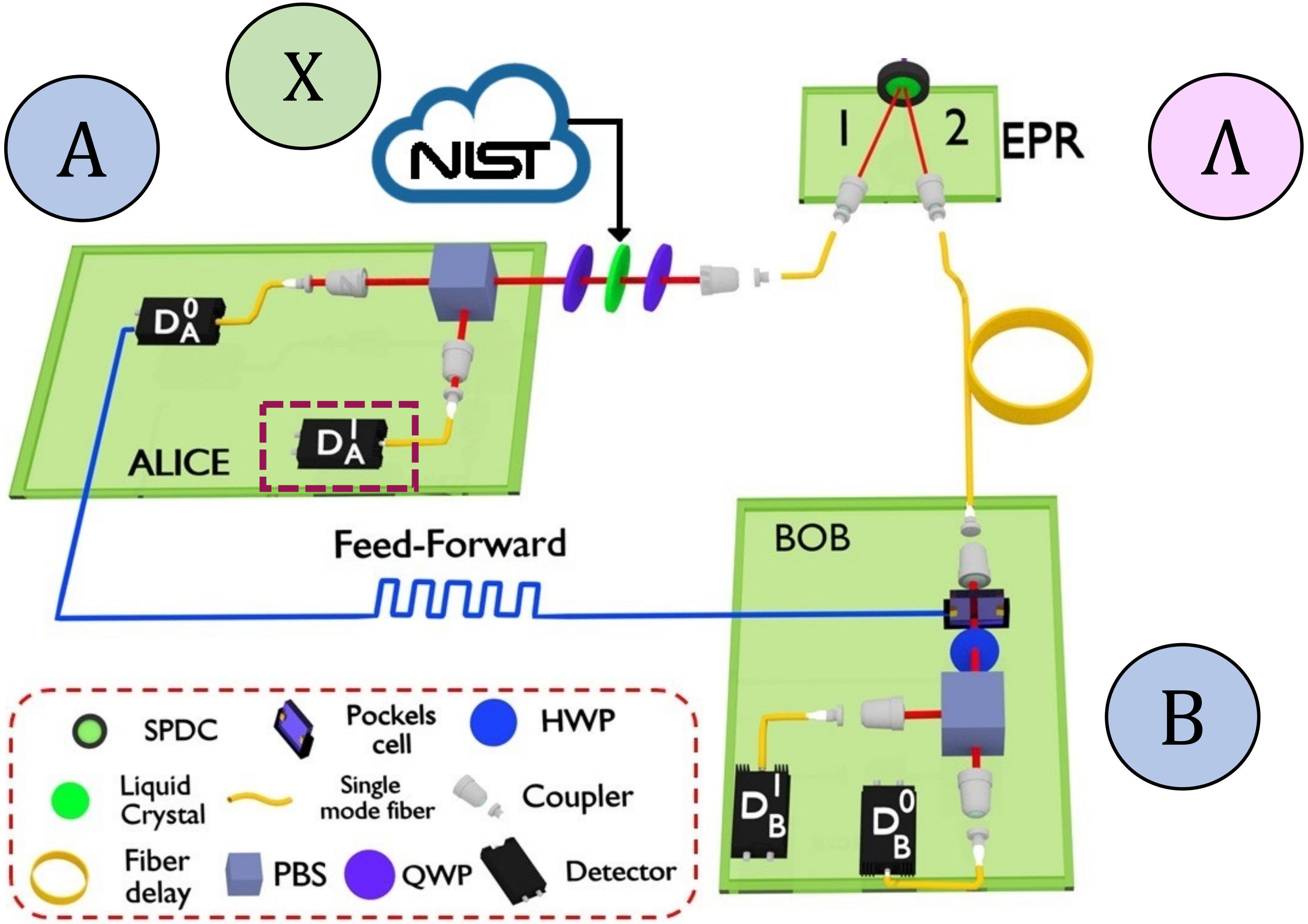
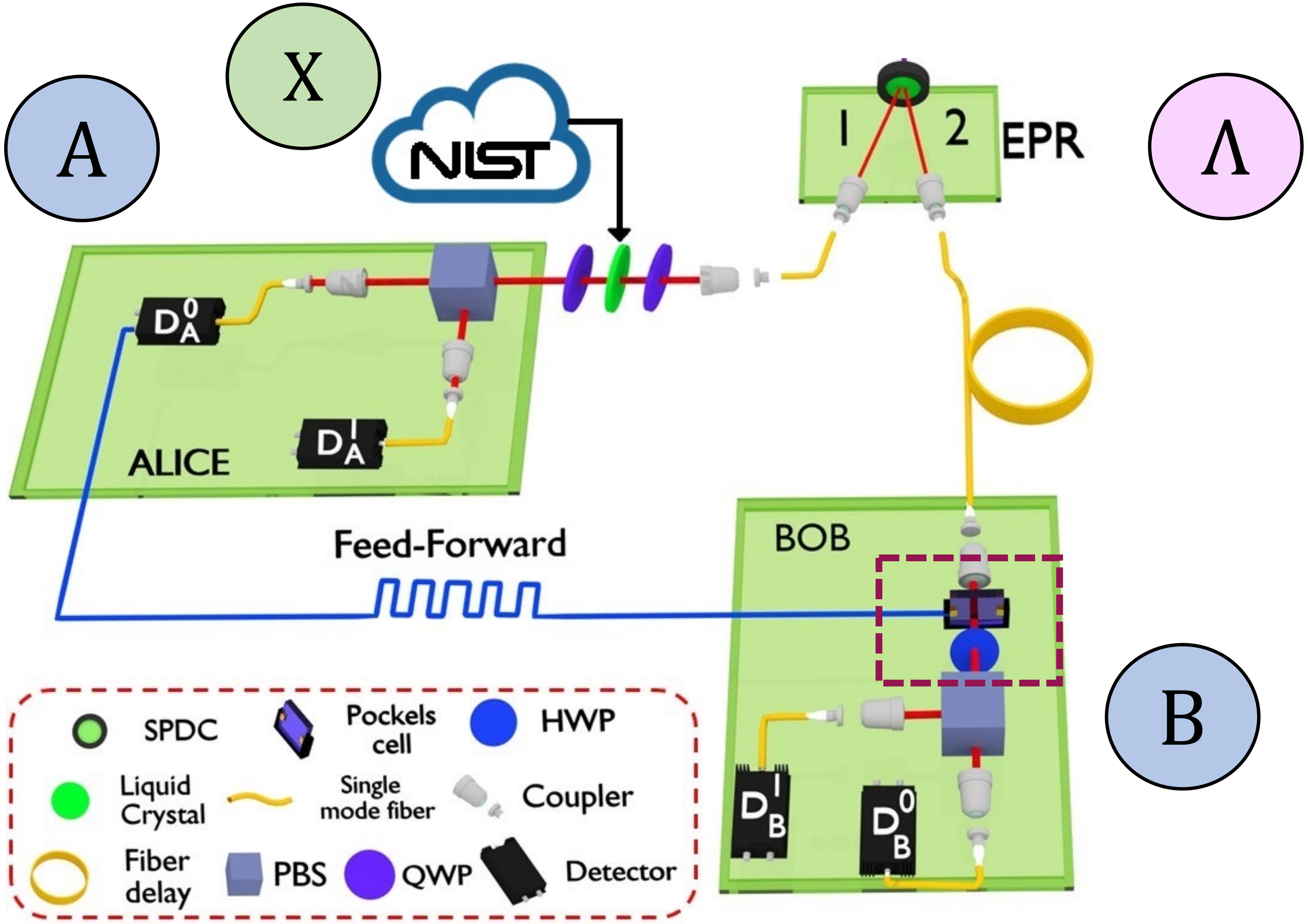
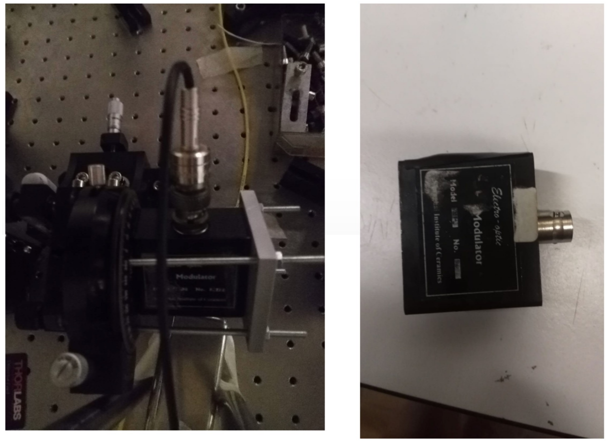


Photo-Detector

Experimental Implementation

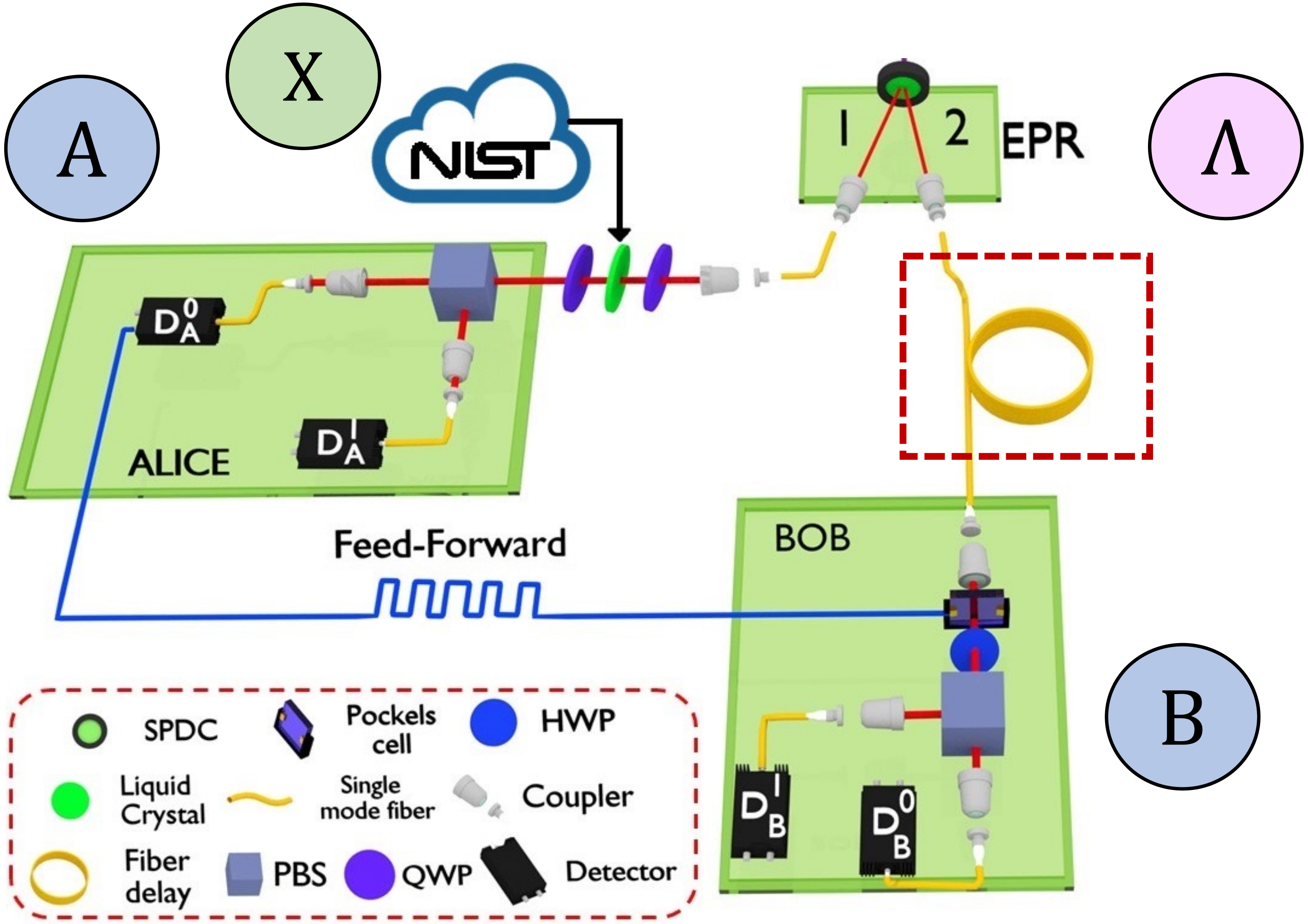




Pockels cell

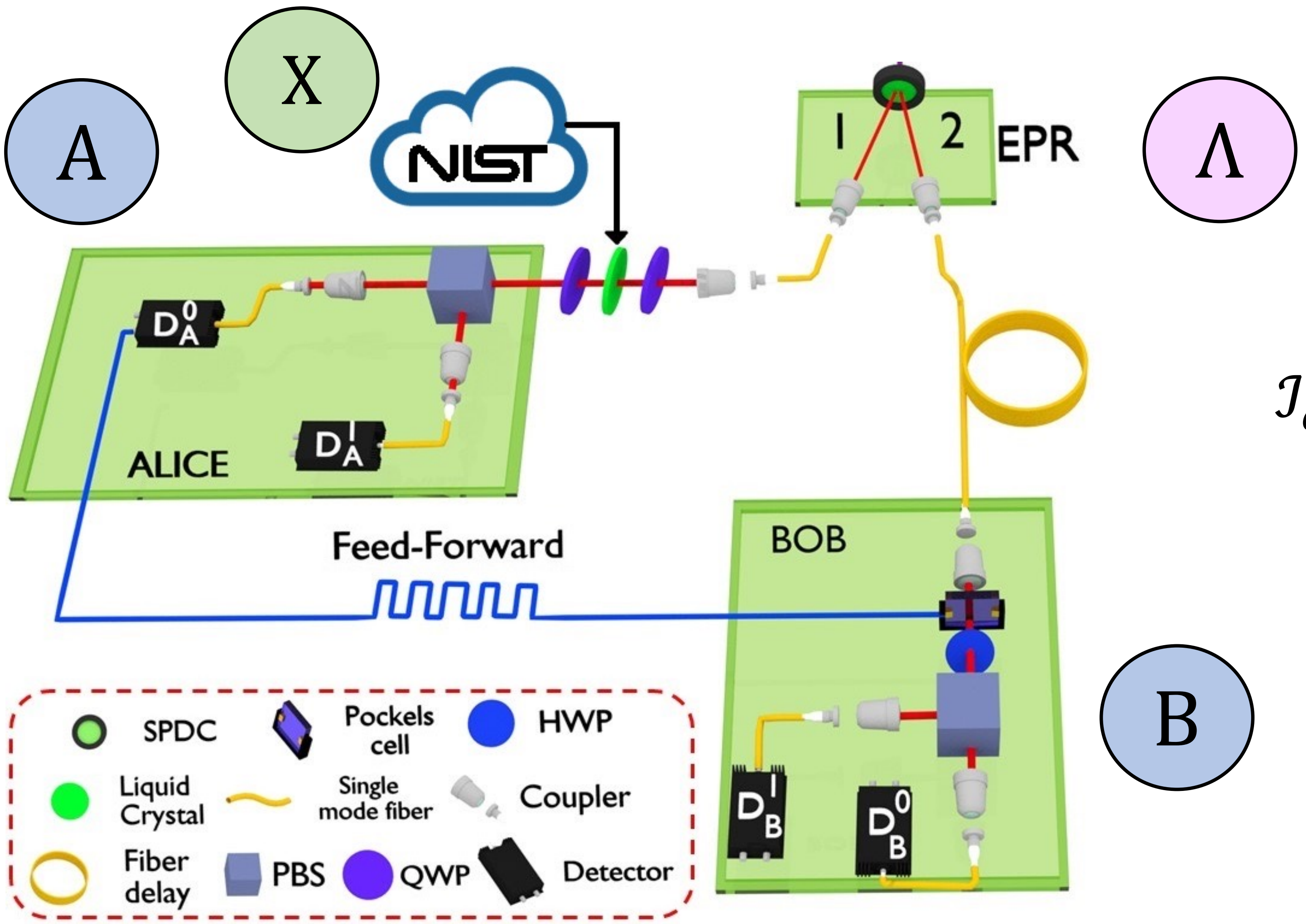
ACTIVE FEED-FORWARD

Experimental Implementation



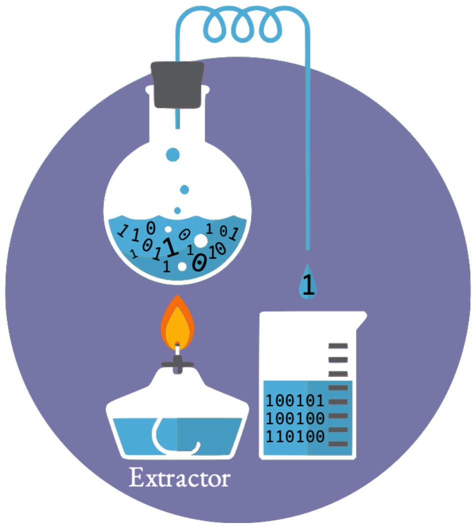
Single mode fiber 125 m long

Experimental Implementation



$$\mathcal{J}_{exp} = 3.797 \pm 0.050 > 3$$

What can we do with it?



We can exploit the instrumental inequalities to detect non-classical correlations and **certify intrinsic randomness**

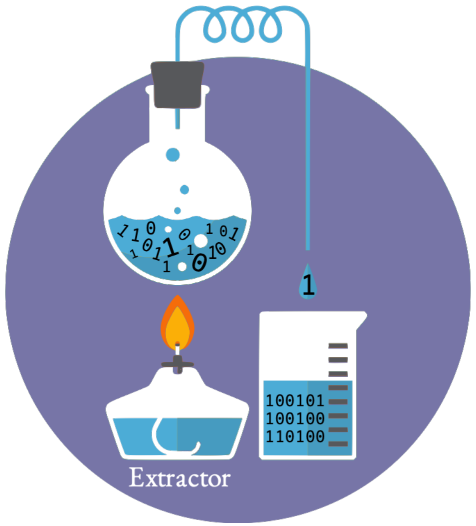
Randomness Quantifier

$$\mathcal{H}_{min}(x) = -\log_2\left(\sum_e P(e)\, max_{a,b} P(a,b|e,x)\right)$$

We want to obtain a lower bound **min($\mathcal{H}_{min}(x)$)=$f_x(\mathcal{I})$** for the min-entropy, performing the optimization over all quantum probabilities, such that

$$P(a,b|x,y=a) = Tr(\mathcal{M}_a^x \mathcal{M}_b^a\, \rho_{AB}) \quad \text{and} \quad \sum_{a,b,x} c_{abx} P(a,b|x) = \mathcal{I}$$

What can we do with it?



We can exploit the instrumental inequalities to detect non-classical correlations and **certify intrinsic randomness**

Randomness Quantifier

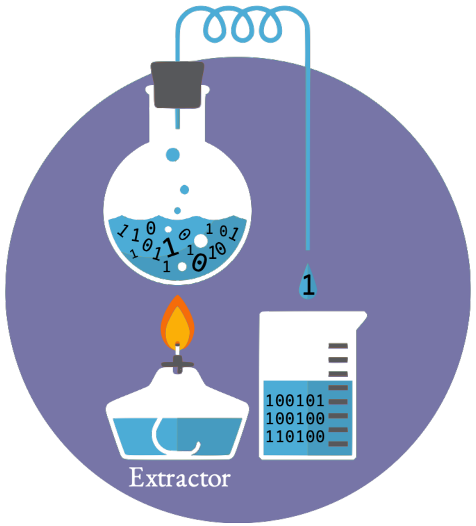
$$\mathcal{H}_{min}(x) = -\log_2\left(\sum_e P(e)\, max_{a,b} P(a,b|e,x)\right)$$

We want to obtain a lower bound **min($\mathcal{H}_{min}(x)$)=$f_x(\mathcal{I})$** for the min-entropy, performing the optimization over all quantum probabilities, such that

NOT FEASIBLE

~~$P(a,b|x,y=a) = Tr(\mathcal{M}_a^x \mathcal{M}_b^a\, \rho_{AB})$~~ and $\sum_{a,b,x} c_{abx} P(a,b|x) = \mathcal{I}$

Randomness lower bound



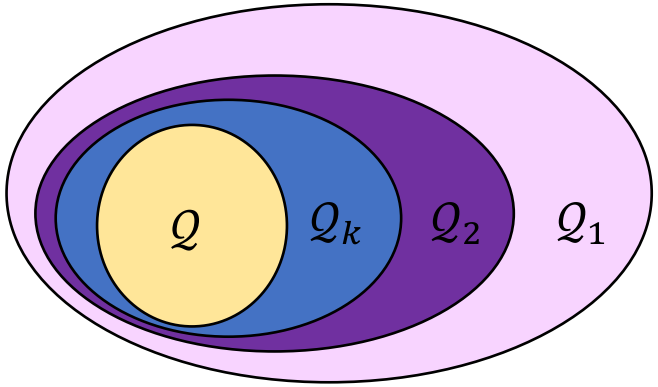
$$\min(\mathcal{H}_{min}(x)) = f_x(\mathcal{J})$$

NPA hierarchy

We recast the optimization as a SDP problem

$$P(a,b|x,y=a) \in \mathcal{Q}_2$$

$$\sum_{a,b,x} c_{abx} P(a,b|x) = \mathcal{J}$$



M. Navascués, S. Pironio, A. Acín, *Phys. Rev. Lett.* **98, 010401** (2007)

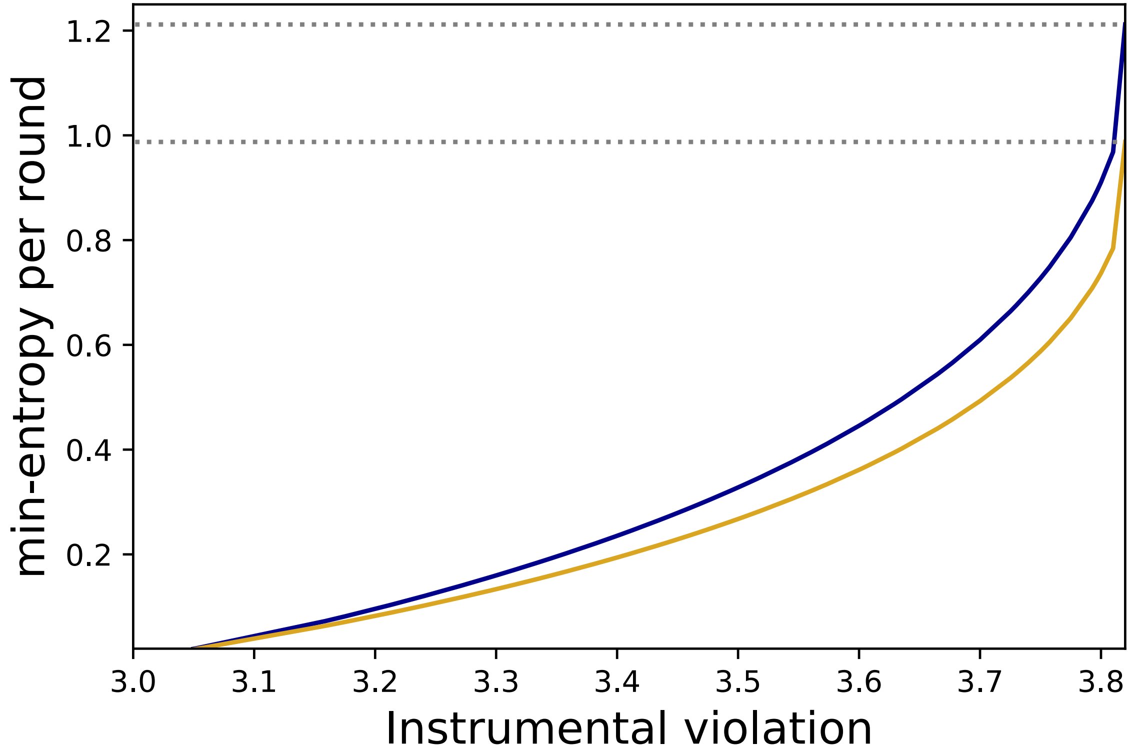
Min-entropy per round

$$\min(\mathcal{H}_{min}(x)) = f_x(\mathcal{I})$$

$$P(a,b|x,y=a) \in \mathcal{Q}_2$$

$$\sum_{a,b,x} c_{abx} P(a,b|x) = \mathcal{I}$$

$$\mathcal{H}_{min}(x) = -\log_2\left(\sum_e P(e)\, max_{a,b} P(a,b|e,x)\right)$$



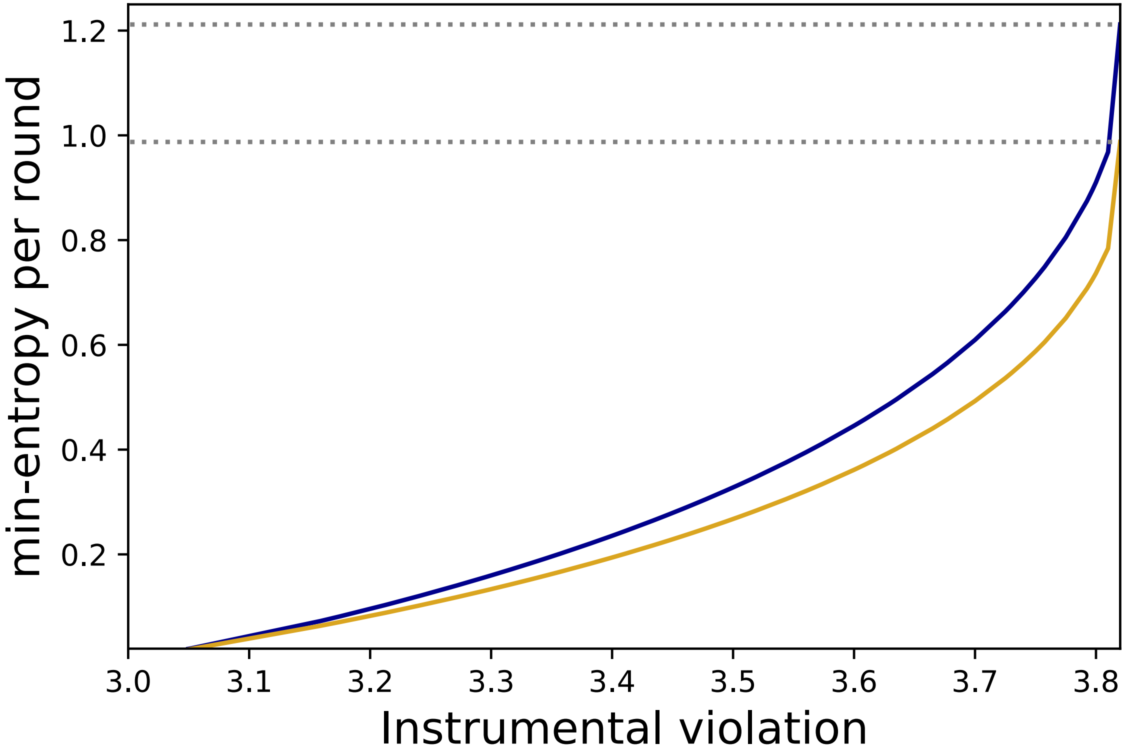
Min-entropy per round

$$\min(\mathcal{H}_{min}(x)) = f_x(\mathcal{I})$$

$$P(a,b|x,y=a) \in \mathcal{Q}_2$$

$$\sum_{a,b,x} c_{abx} P(a,b|x) = \mathcal{I}$$

$$\mathcal{H}_{min}(x) = -\log_2\left(\sum_e P(e)\, max_{a,b} P(a,b|e,x)\right)$$



We resort to the **Entropy Accumulation theorem** to evaluate how the min-entropy accumulates over the runs.

Results

In our experiment

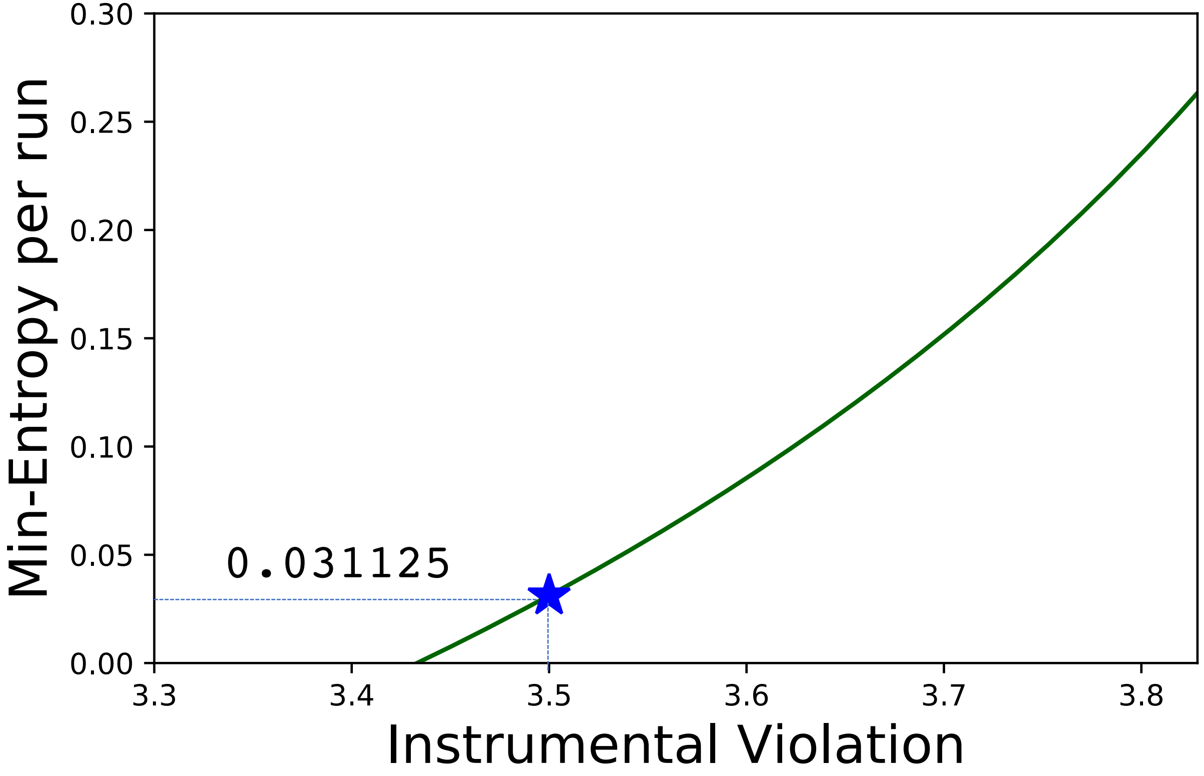
n= 172095

$\gamma = 1$ only **test runs**

$\mathcal{J}_{threshold}$= 3.5

$\delta = 0.011$

$\epsilon = \epsilon_{EA} = 0.1$



Results

In our experiment

n= 172095

$\gamma = 1$ only **test runs**

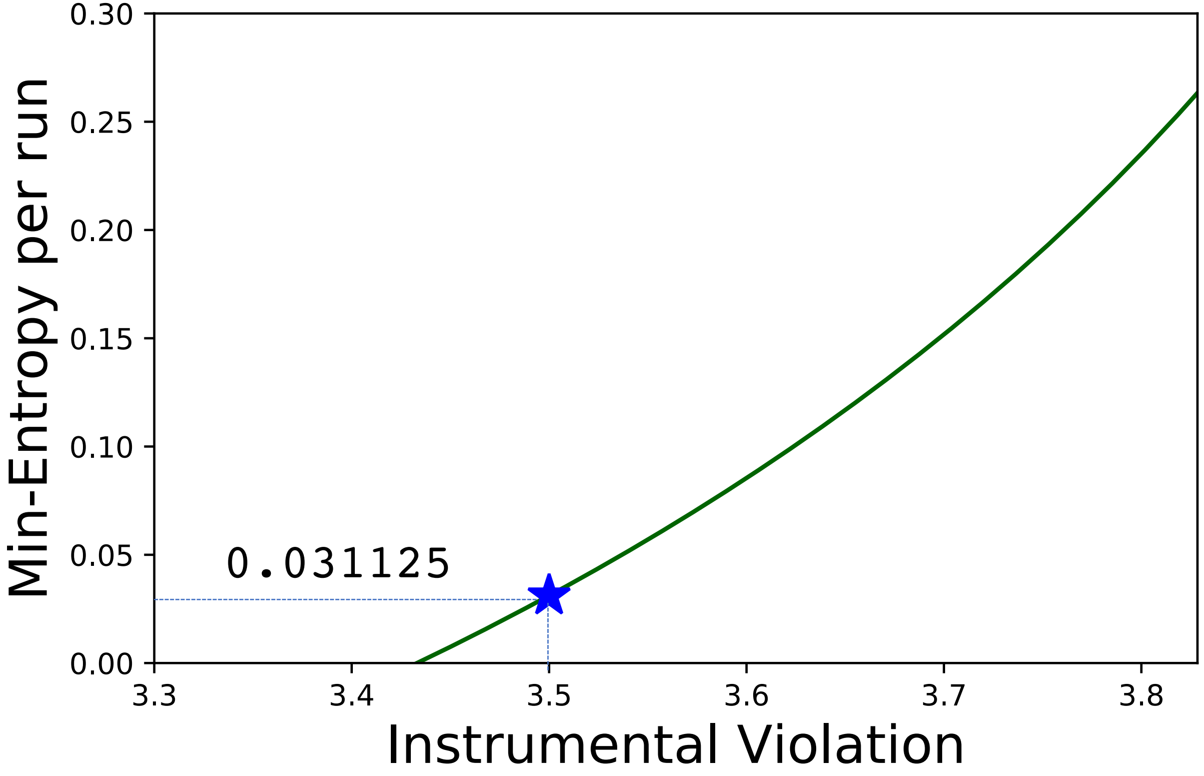
$\mathcal{I}_{threshold}$= 3.5

$\delta = 0.011$

$\epsilon = \epsilon_{EA} = 0.1$

$\epsilon_{ext} = 10^{-6}$

(classical extractor)



L. Trevisan, *J. ACM* **48, 860-879,** (2001).

I. Agresti et al., Communications Physics, **3, 110** (2020).

Results

In our experiment

n= 172095

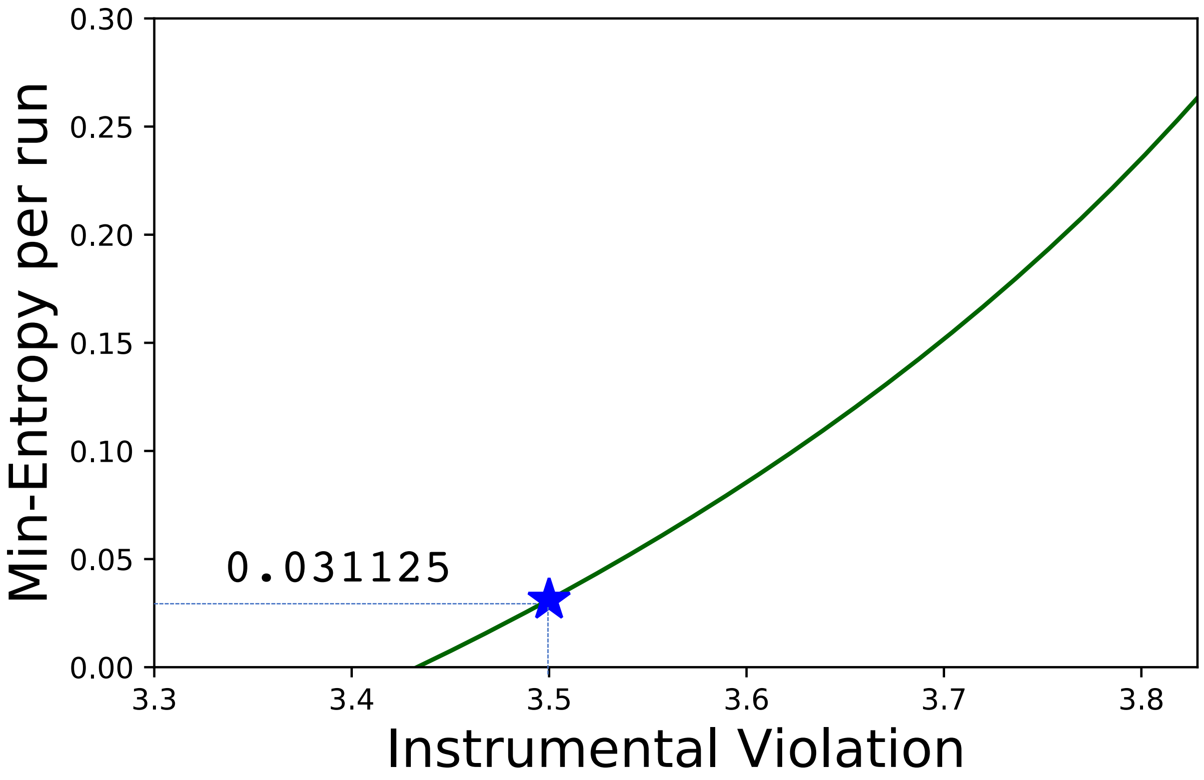
$\gamma = 1$ only **test runs**

$\mathcal{J}_{threshold}$= 3.5

$\delta = 0.011$

$\epsilon = \epsilon_{EA} = 0.1$

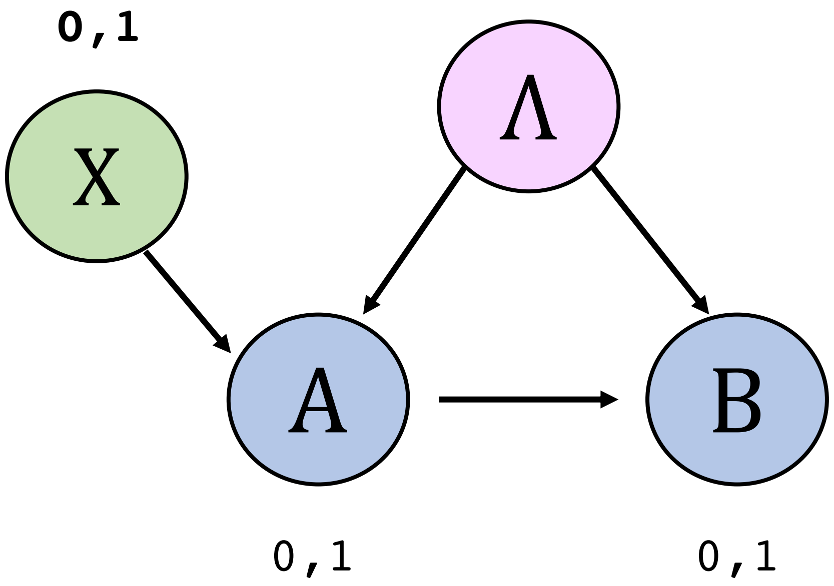
$\epsilon_{ext} = 10^{-6}$
(classical extractor)



5270 extracted bits

L. Trevisan, *J. ACM* **48, 860-879,** (2001).
I. Agresti et al., Communications Physics, **3, 110** (2020).

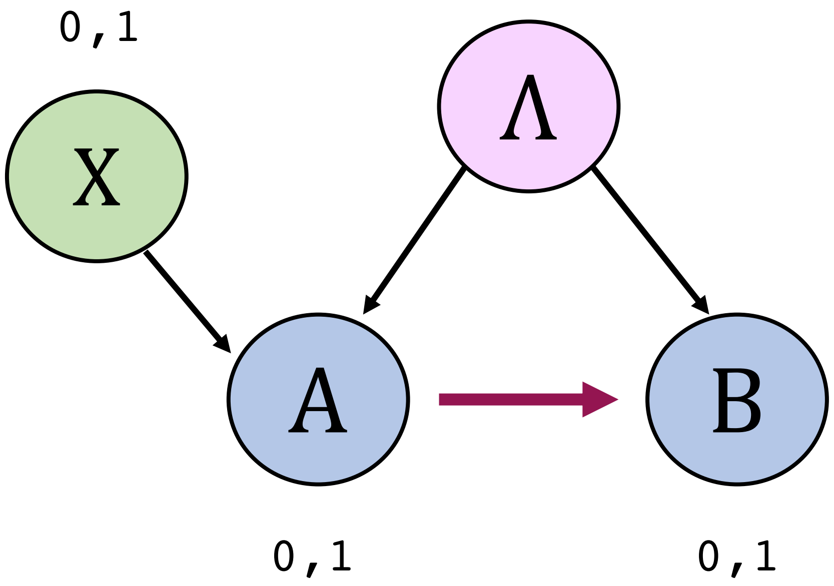
Instrumental process



In this case the quantum and classical causal predictions coincide

NO QUANTUM VIOLATION IS POSSIBLE

Instrumental process



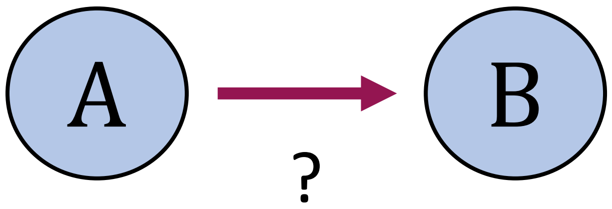
In this case the quantum and classical causal predictions coincide

NO QUANTUM VIOLATION IS POSSIBLE

BUT

We can still certify the presence of non-classical correlations through the **amount of influence between A and B**

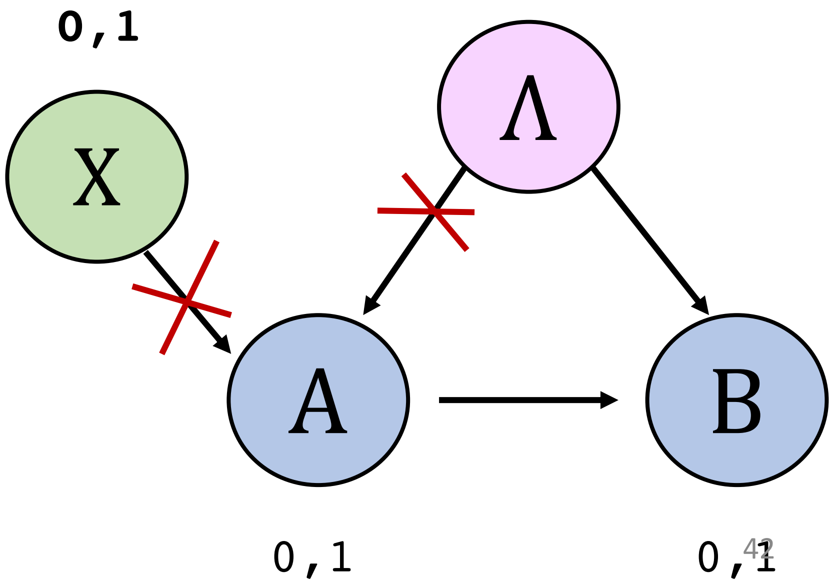
Average Causal effect



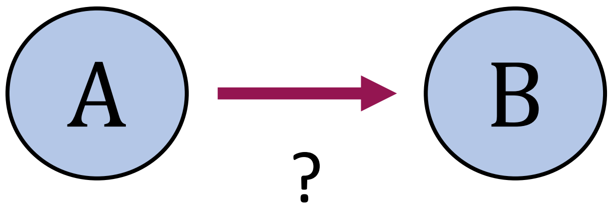
We can quantify the amount of causal influence between A and B, in this way:

$$\mathrm{ACE} = \max_{a,a',b} |p(b|do(a)) - p(b|do(a'))|$$

INTERVENTION



Average Causal effect



We can quantify the amount of causal influence between A and B, in this way:

$$\mathrm{ACE} = \max_{a,a',b} |p(b|do(a)) - p(b|do(a'))|$$

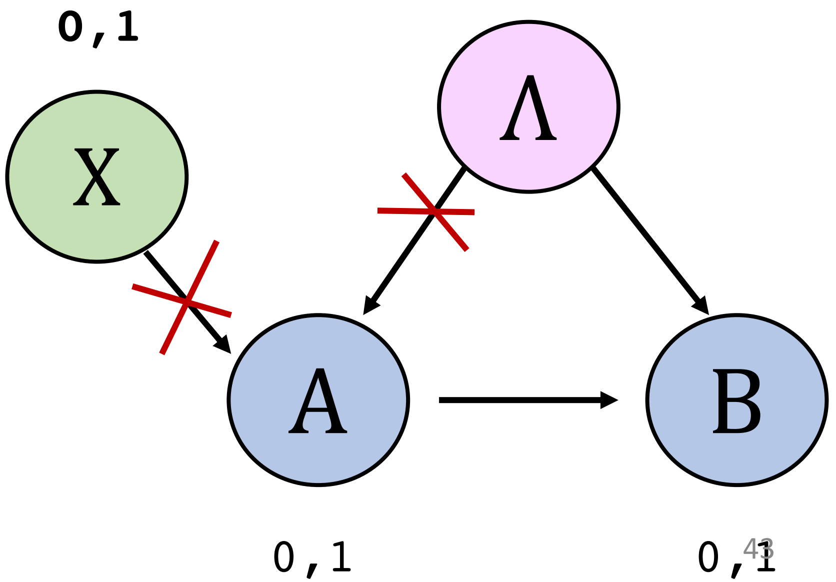
INTERVENTION

LOWER BOUNDS on the ACE

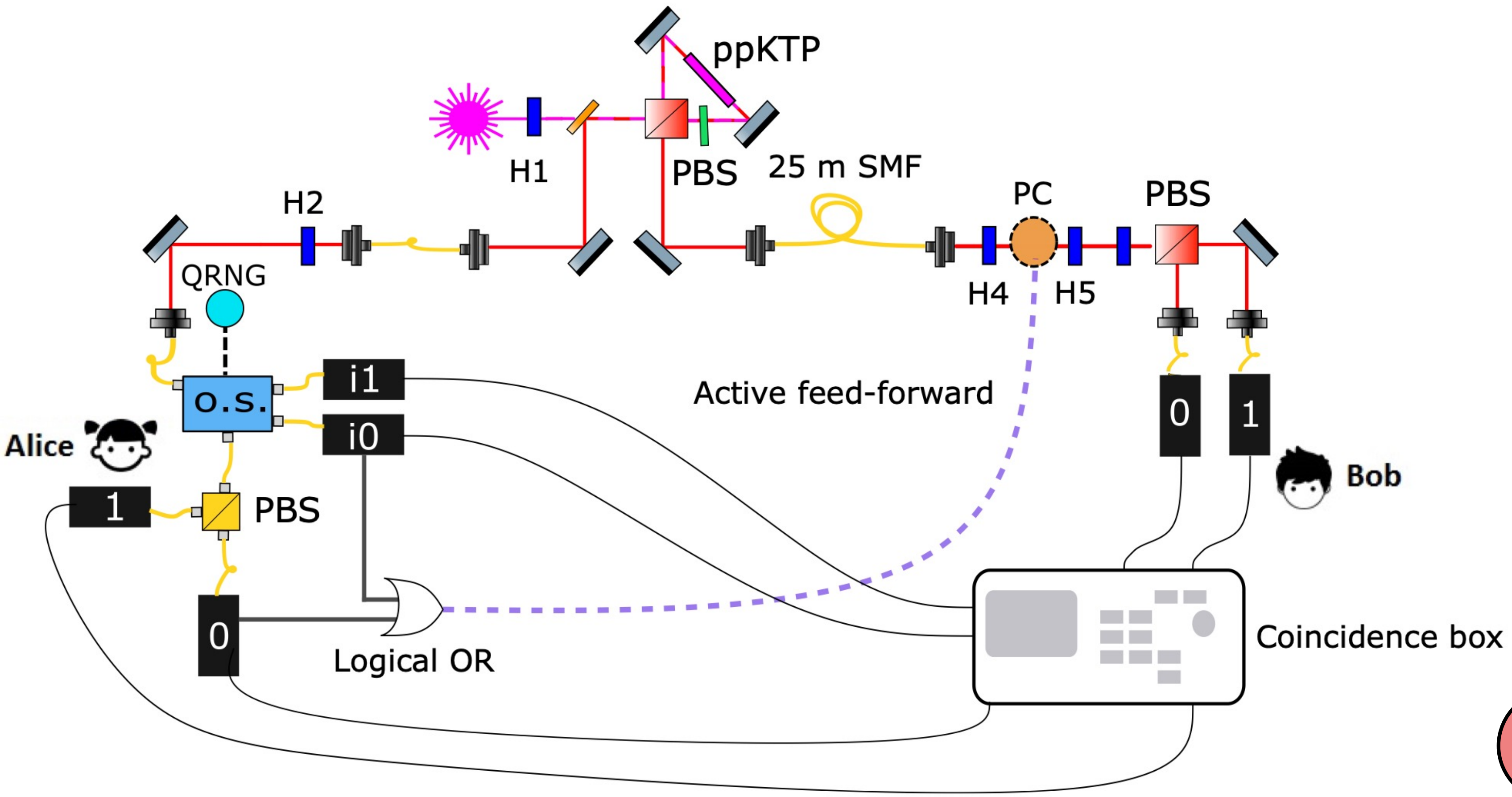
$$ACE \geq 2\,p(0{,}0|0) + p(1{,}1|0) + p(0{,}1|1) + p(1{,}1|1) - 2$$

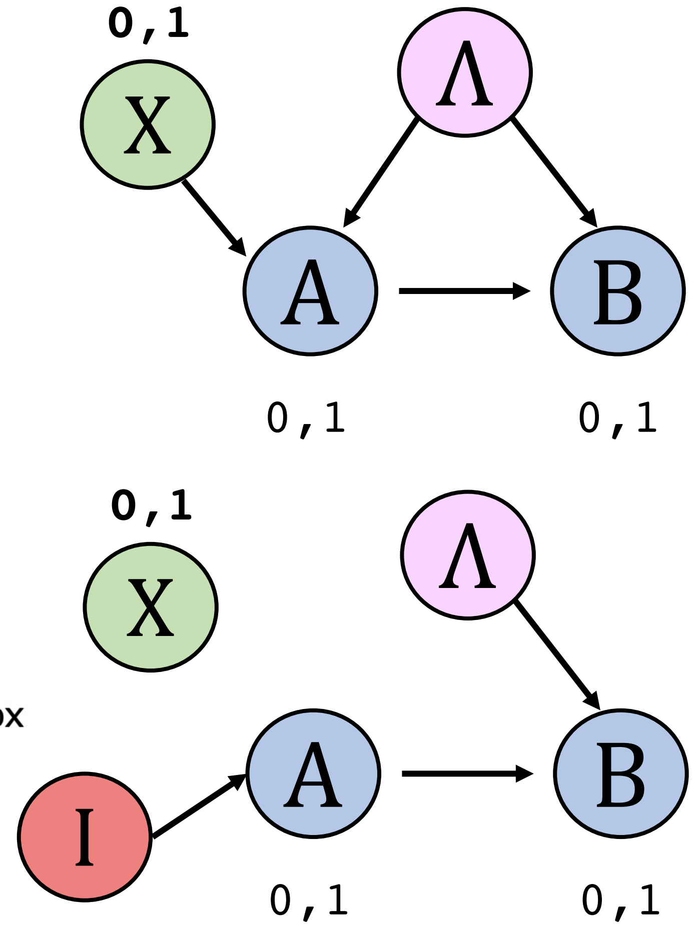
$$qACE \geq \sum_{0,1} \big(p(0{,}0|x) + p(1{,}1|x)\big) - \zeta - 1$$

If qACE < ACE, we have a quantum violation!

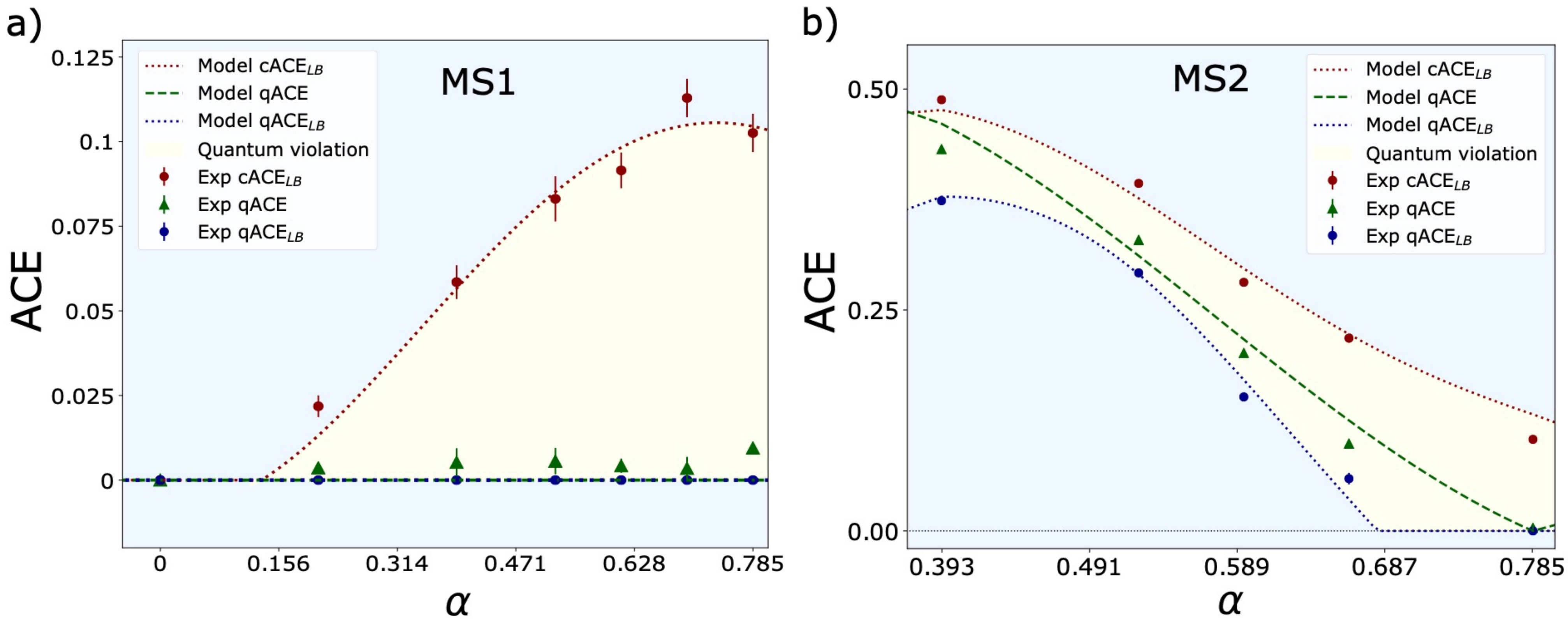


Experimental apparatus



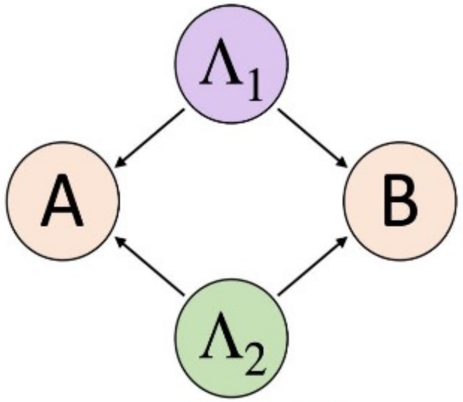


Results

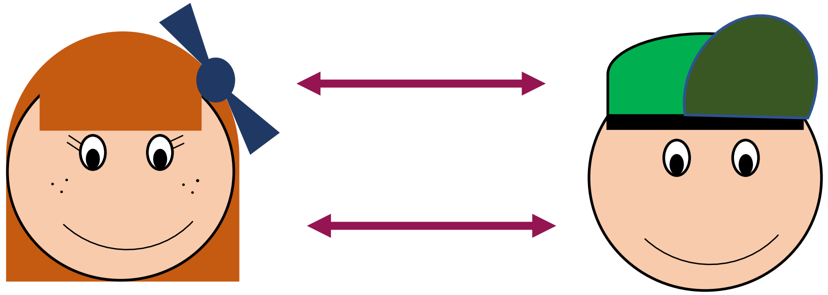


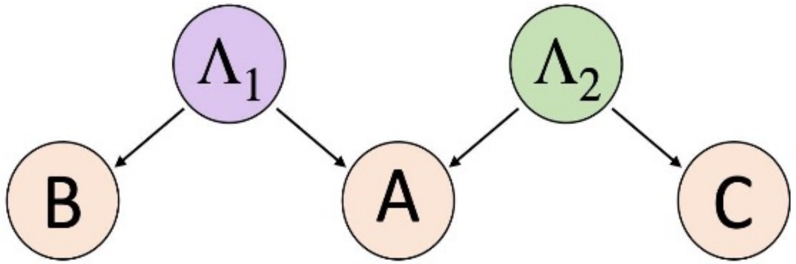
I. Agresti et al., arXiv:2108.08926 (2021).

Quantum network prototypes

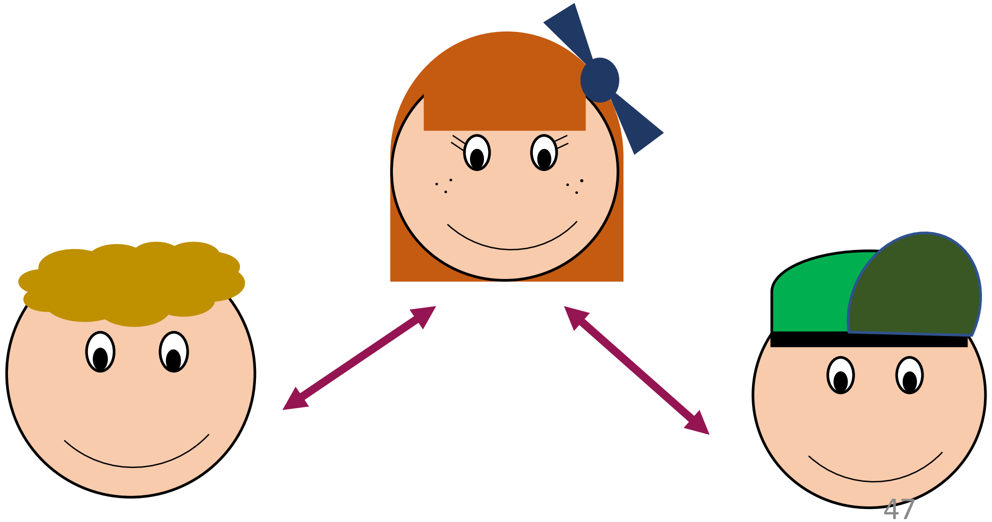


Parallel scenario





Three-parties scenario



I. Agresti et al., PRX Quantum 2, 020346 (2021).

Self-testing protocol

It allows to evaluate the a lower bound on the fidelity of the generated state with respect to a target state (in our case the tensor product of 2-qubit maximally entangled ones)

target state $|\psi\rangle \otimes |\psi\rangle$

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Self-testing protocol

It allows to evaluate the a lower bound on the fidelity of the generated state with respect to a target state (in our case the tensor product of 2-qubit maximally entangled ones)

target state $$|\psi\rangle \otimes |\psi\rangle$$

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$F(\rho, |\psi\rangle\langle\psi|) = \sqrt{\langle\psi|\rho|\psi\rangle}$$

Self-testing protocol

It allows to evaluate the a lower bound on the fidelity of the generated state with respect to a target state (in our case the tensor product of 2-qubit maximally entangled ones)

target state $$|\psi\rangle \otimes |\psi\rangle$$

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

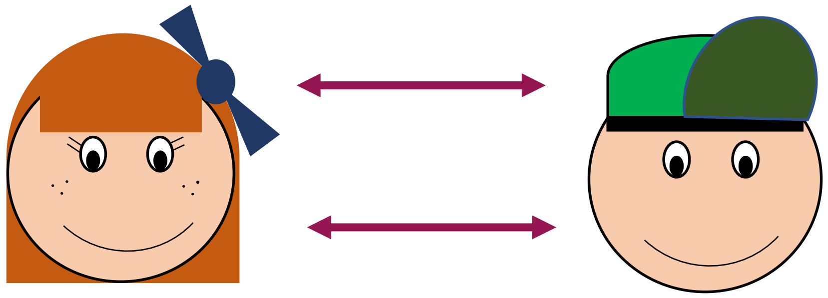
$$F(\rho, |\psi\rangle\langle\psi|) = \sqrt{\langle\psi|\rho|\psi\rangle}$$

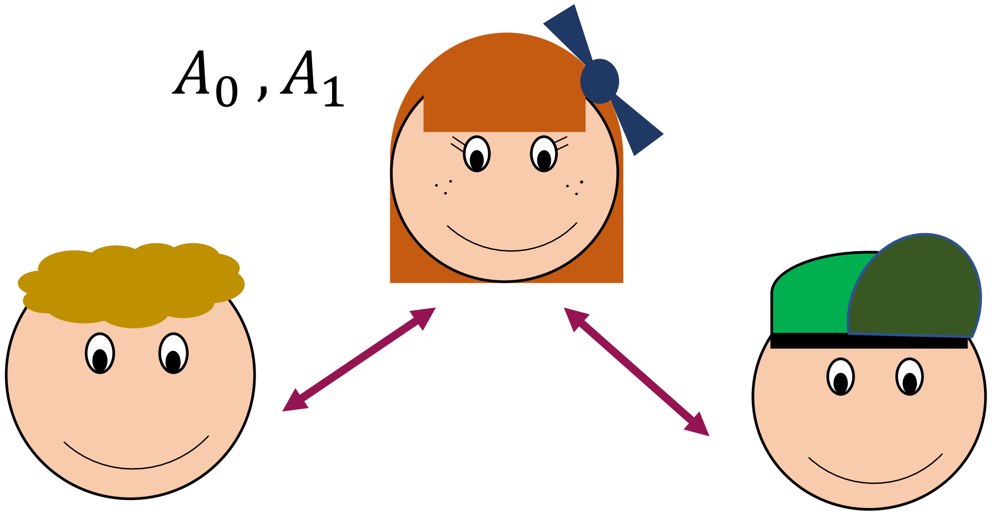
In order to properly define the fidelity, we would have to assume the dimension of the state. To avoid this assumption, we resort to the so-called SWAP operator.

Swap operator

The swap operator allows to express the fidelity in terms of correlations obtained by the parties, performing measurements in two bases.

$$F(\rho, |\psi\rangle\langle\psi|) = \sum c_{xx'x''yy'y''} tr(\rho_{AB} A_x A_{x'} A_{x''} B_y B_{y'} B_{y''})$$





Lower bound on the fidelity

At this point we want to minimize the square fidelity with ρ_{swap} over the set of quantum correlations:

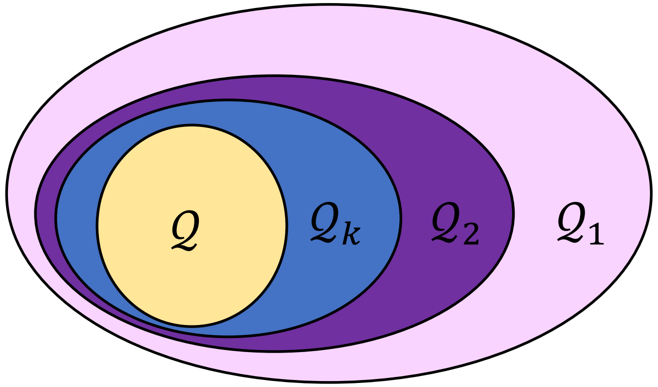
$$F(\rho, |\psi\rangle\langle\psi|) = \langle\psi|\rho|\psi\rangle \qquad \text{s.t.} \qquad p(a,b|x,y) \in \mathcal{Q}$$

Since this problem is not feasible, we relax this assumption to a superset of the quantum correlations one.

NPA hierarchy

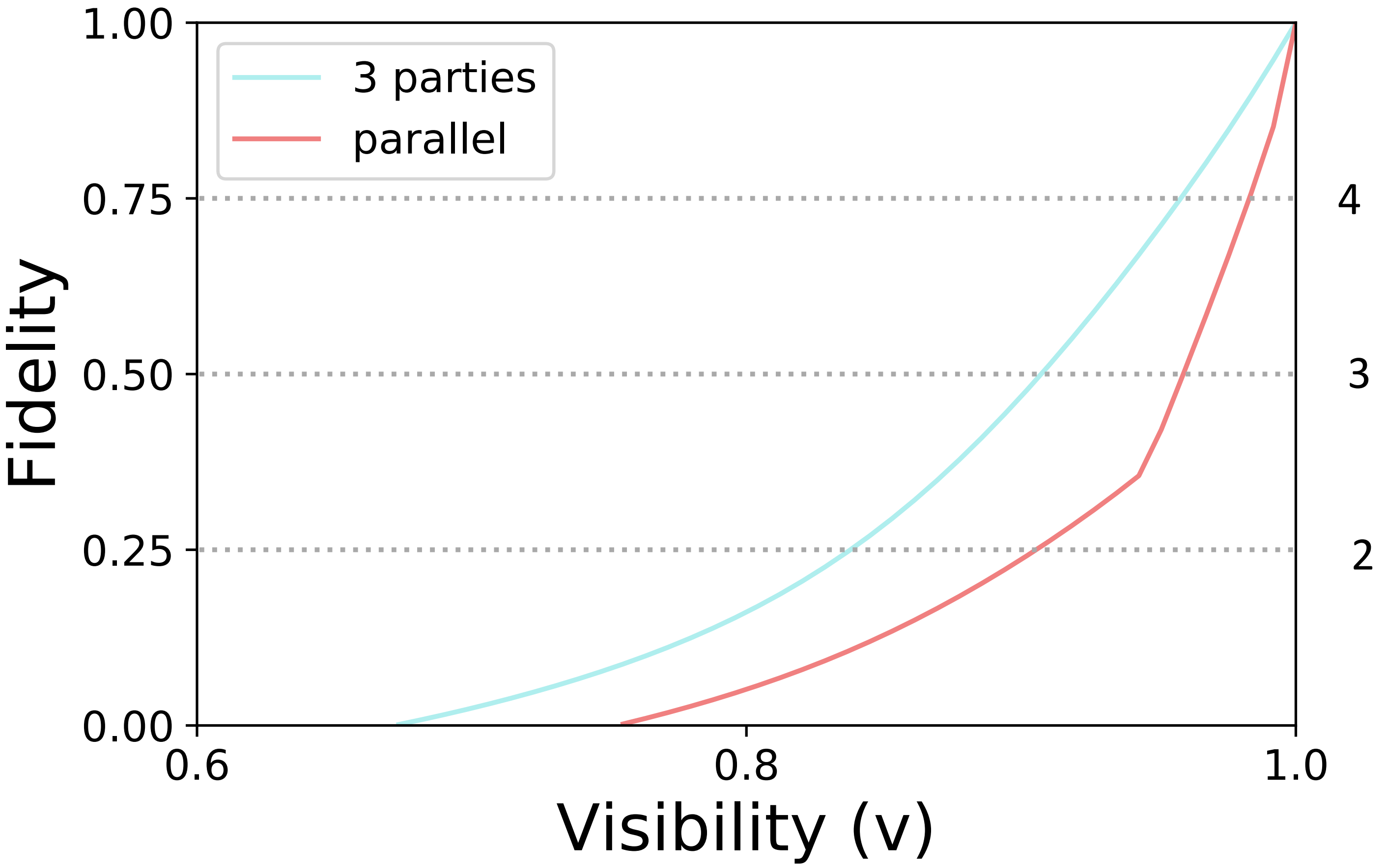
We recast the optimization as a SDP problem

$$P(a,b|x,y) \in \mathcal{Q}_3$$

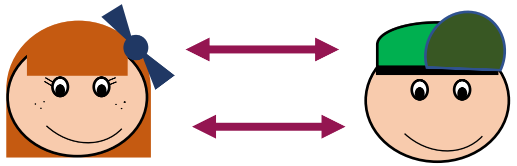


M. Navascués, S. Pironio, A. Acín, *Phys. Rev. Lett.* **98, 010401** (2007)

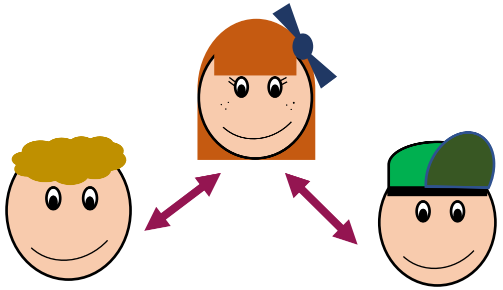
Numerical results



$$v_1 = v_2 = v$$



$$\rho_{AB} = \rho_1^{v_1} \otimes \rho_2^{v_2}$$

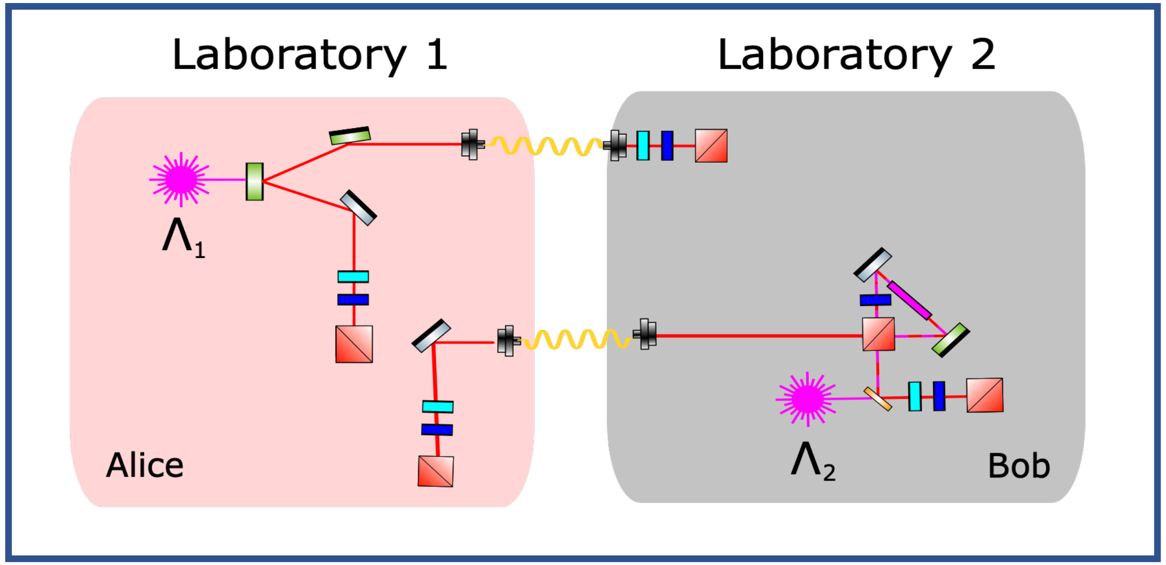


$$\rho_{ABC} = \rho_{AB}^{v_1} \otimes \rho_{AC}^{v_2}$$

$$\rho^v = v|\psi\rangle\langle\psi| + (1-v)\frac{\mathbb{1}}{4}$$

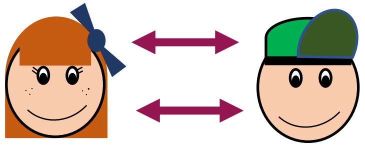
Experimental implementation

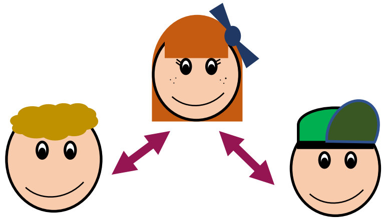
Our **goal** is to self-test a state of 4 qubits generated by two quantum networks



$|\psi\rangle_{A_1B_1} \otimes |\psi\rangle_{A_2B_2}$

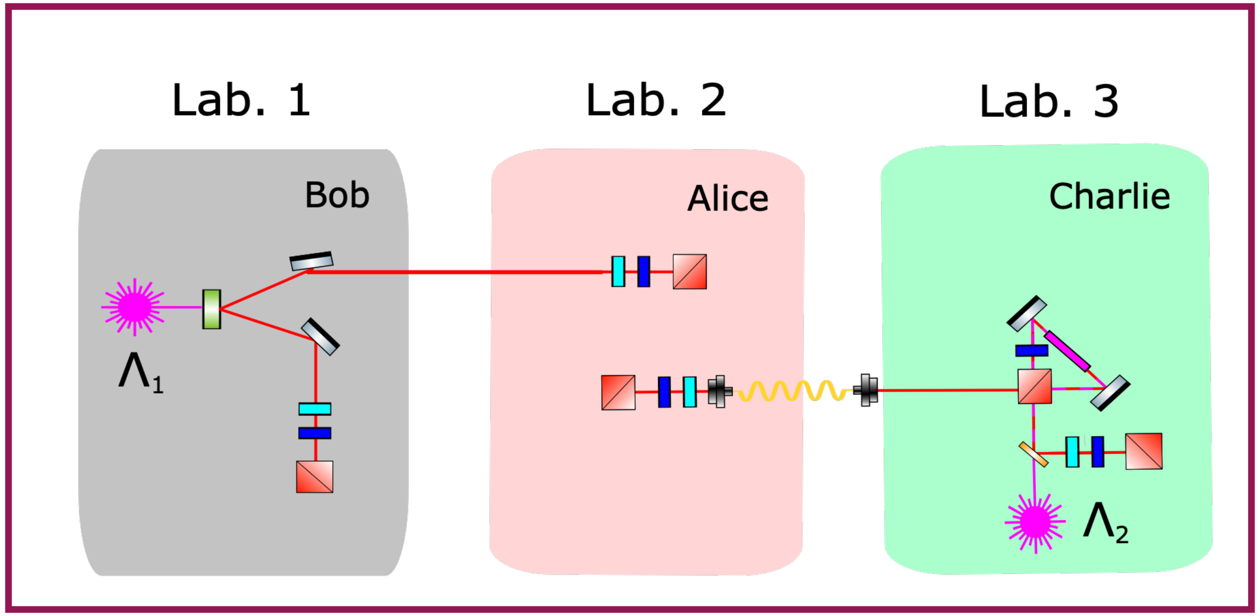
Parallel case



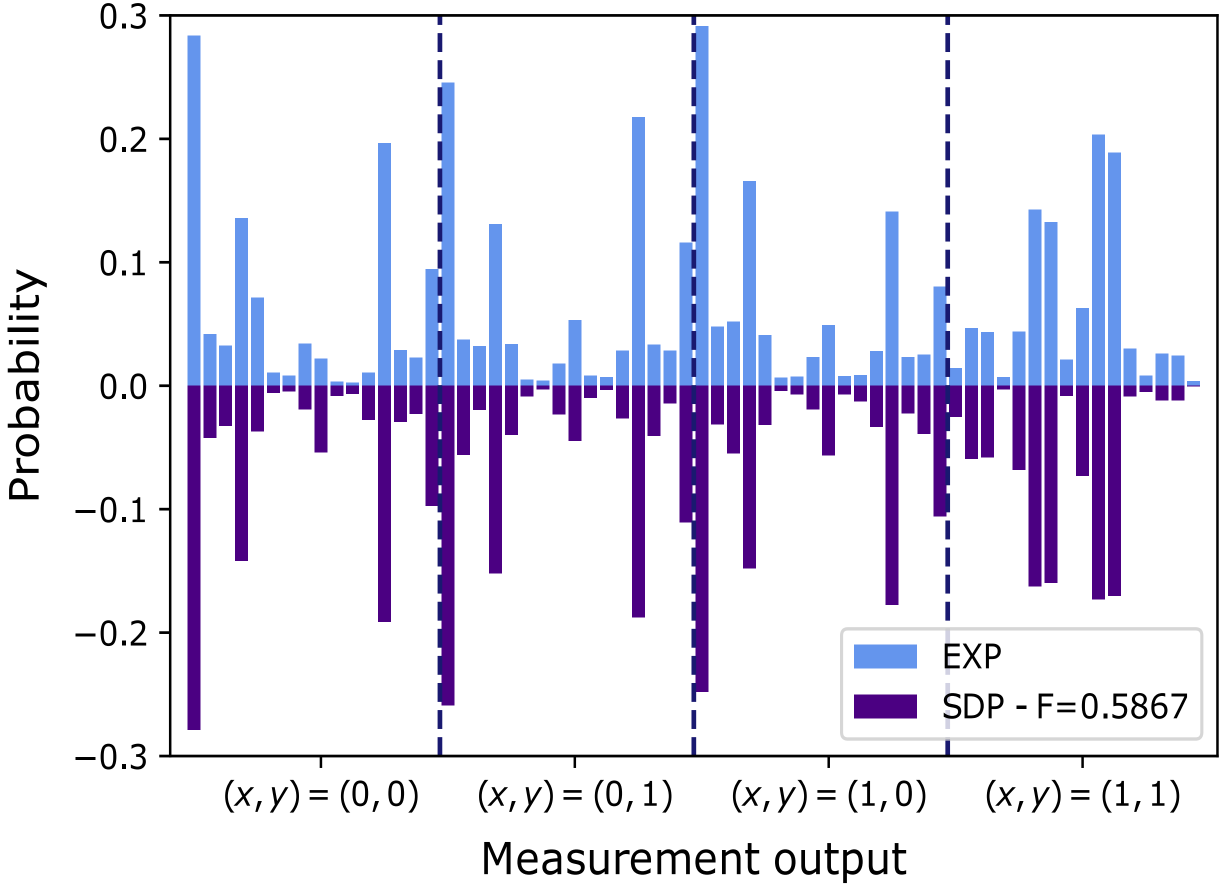


$|\psi\rangle_{A_1B} \otimes |\psi\rangle_{A_2C}$

Three parties case

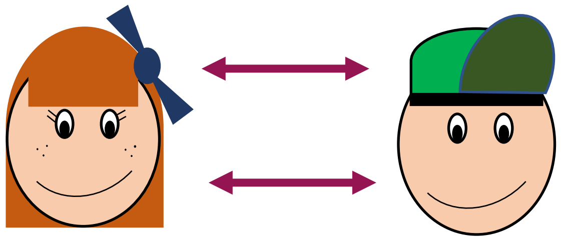


Results



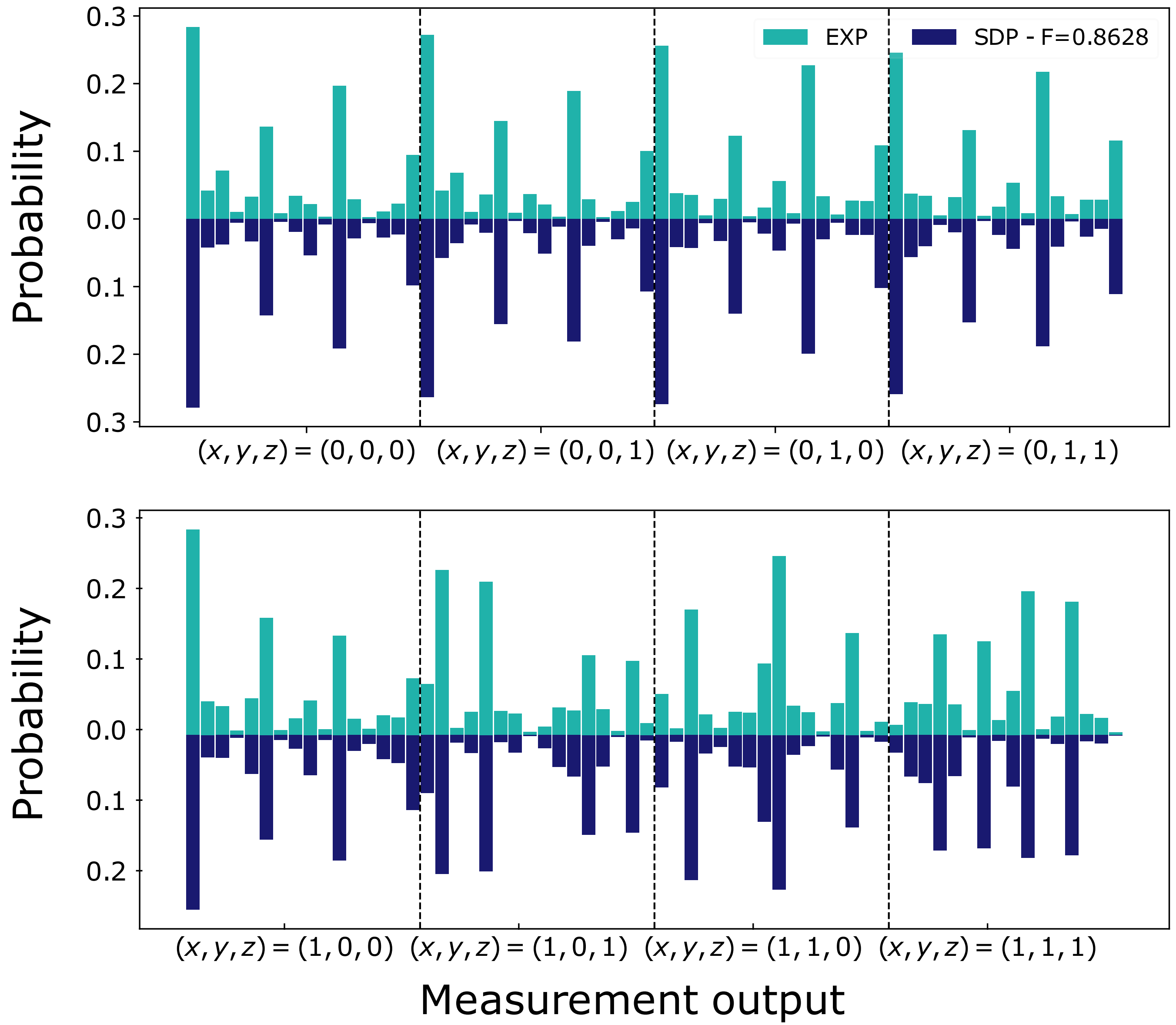
Parallel self-testing case

$$\langle\psi|\rho|\psi\rangle = 0.587 \pm 0.053 > 0.50$$



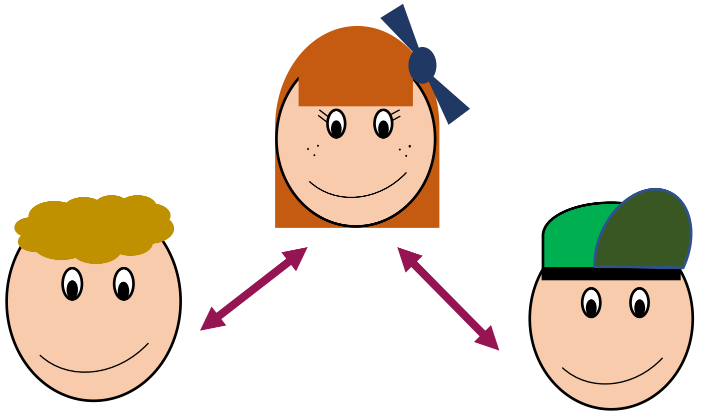
Schmidt number ≥ 3

Results



Three parties case

$$\langle\psi|\rho|\psi\rangle = 0.863 \pm 0.032 > 0.75$$



Schmidt number ≥ 4

Conclusions

- It is possible to design **device-independent protocols** exploiting different causal structures than the standard Bell-like scenario.

Conclusions

- It is possible to design **device-independent protocols** exploiting different causal structures than the standard Bell-like scenario.

- We presented three device-independent protocols, exploiting the **instrumental causal structure** and causal structures involving **two quantum state sources**.

Conclusions

- It is possible to design **device-independent protocols** exploiting different causal structures than the standard Bell-like scenario.
- We presented three device-independent protocols, exploiting the **instrumental causal structure** and causal structures involving **two quantum state sources**.
- Exploiting the quantum violation of the instrumental inequality we **designed and implemented a generator of certified random bits**, secure against any adversarial attack (EAT theorem).

Conclusions

- It is possible to design **device-independent protocols** exploiting different causal structures than the standard Bell-like scenario.

- We presented three device-independent protocols, exploiting the **instrumental causal structure** and causal structures involving **two quantum state sources**.

- Exploiting the quantum violation of the instrumental inequality we **designed and implemented a generator of certified random bits**, secure against any adversarial attack (EAT theorem).

- When **no quantum inequality violation is possible**, non-classical correlations are still certifiable, through the average causal effect.

Conclusions

- It is possible to design **device-independent protocols** exploiting different causal structures than the standard Bell-like scenario.
- We presented three device-independent protocols, exploiting the **instrumental causal structure** and causal structures involving **two quantum state sources**.
- Exploiting the quantum violation of the instrumental inequality we **designed and implemented a generator of certified random bits**, secure against any adversarial attack (EAT theorem).
- When **no quantum inequality violation is possible**, non-classical correlations are still certifiable, through the average causal effect.
- We developed and implemented a **self-testing protocol**, based on the swap operator, to certify a lower bound on the fidelity between an unknown state generated by a quantum network and a target state. We obtained **non trivial lower bounds on the fidelity and entanglement dimension** of the generated states with the targets, with no assumptions on the experimental apparatus.