

Experimental device-independent certified randomness generation with an instrumental causal structure

Anacapri, 19th of September 2019

I. Agresti, D. Poderini, L. Guerini, M. Mancusi,
G. Carvacho, L. Aolita, D. Cavalcanti, R. Chaves, F. Sciarrino



UNIVERSIDADE FEDERAL
DO RIO DE JANEIRO



DIPARTIMENTO DI FISICA
SAPIENZA
UNIVERSITÀ DI ROMA



ICFO^R
The Institute of Photonic
Sciences



JOHN TEMPLETON FOUNDATION



Random numbers generation



Quantum algorithms can
generate intrinsic randomness

Classical algorithms can only provide
pseudo-random sequences



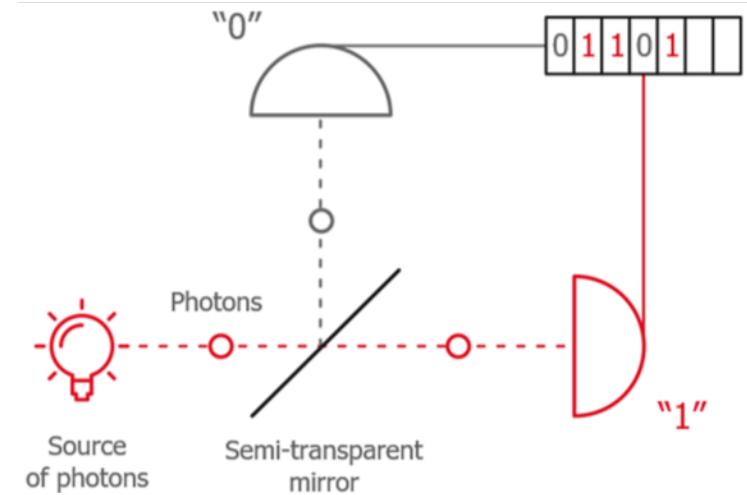
How can we recognize a quantum algorithm?



How can we recognize a quantum algorithm?



```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```



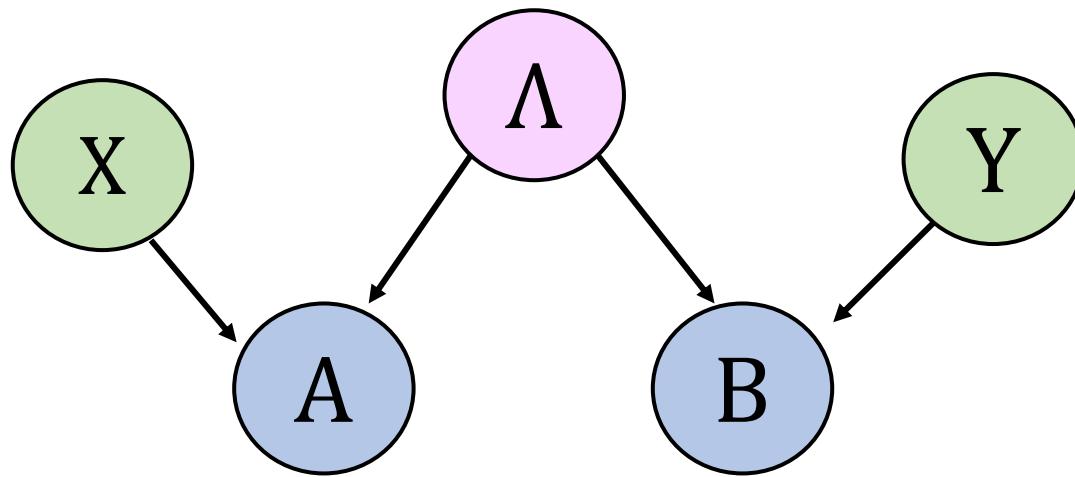
Device Independent Protocols



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

Causal Inference

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



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

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

violation
↓
Different underlying causal structure
↓
non-classical correlations

Conference on Uncertainty in Artificial Intelligence
Tel Aviv, Israel
July 22 - 25, 2019

uai2019

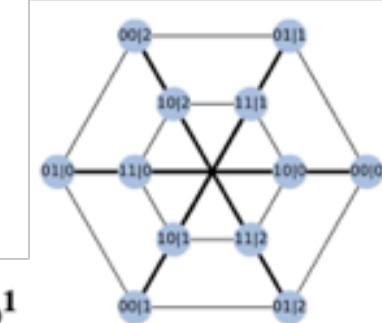
Exclusivity graph approach to Instrumental inequalities

Davide Poderini¹, Rafael Chaves^{2,3}, Iris Agresti¹, Gonzalo Carvacho¹, Fabio Sciarrino¹

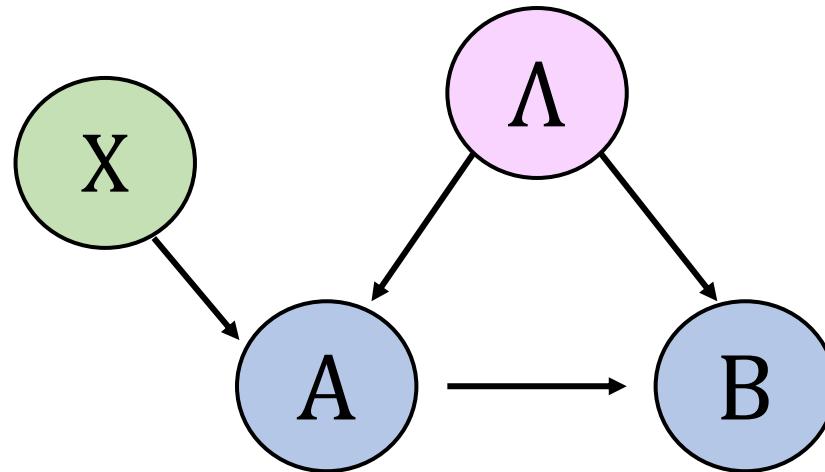
¹*Dipartimento di Fisica, Sapienza Università di Roma, Piazzale Aldo Moro 5, I-00185 Roma, Italy*

²*International Institute of Physics, Federal University of Rio Grande do Norte, 59070-405 Natal, Brazil*

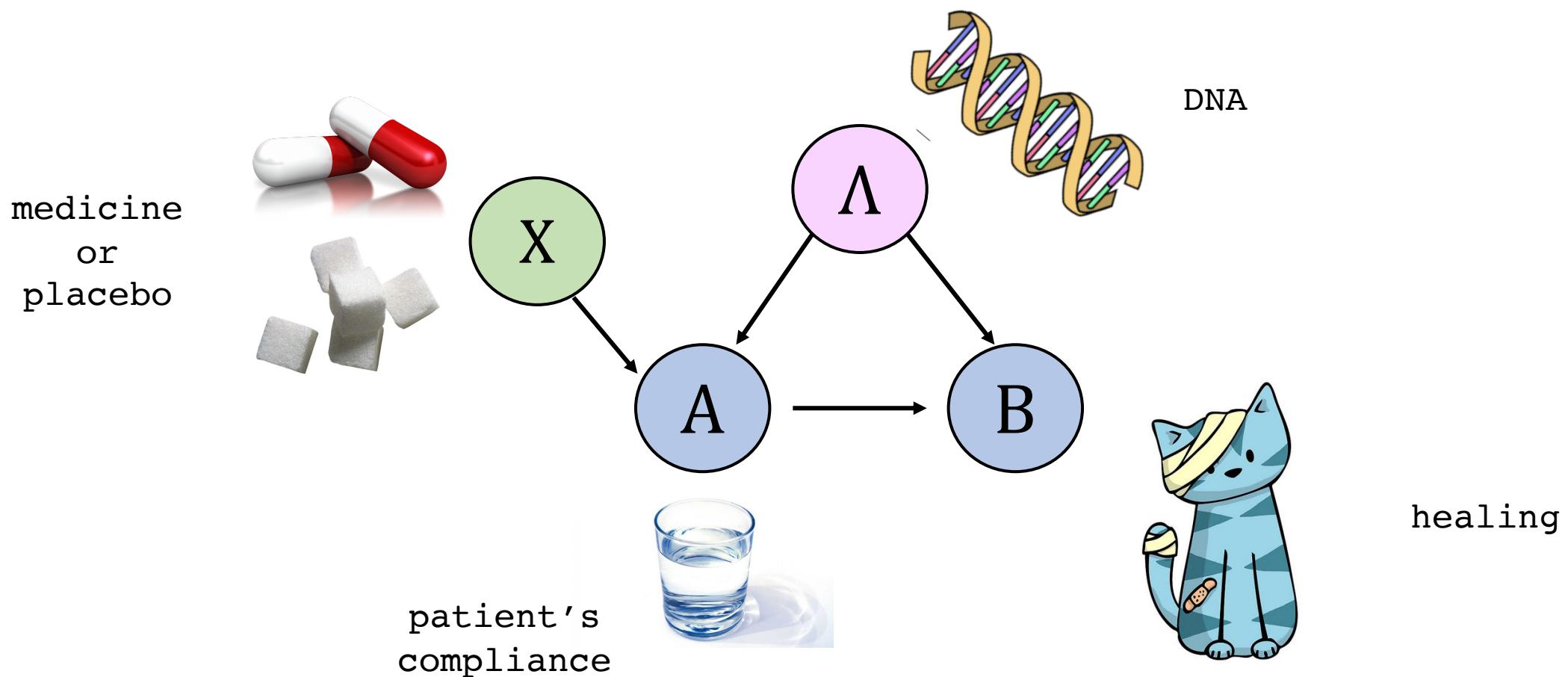
³*School of Science and Technology, Federal University of Rio Grande do Norte, 59078-970 Natal, Brazil*



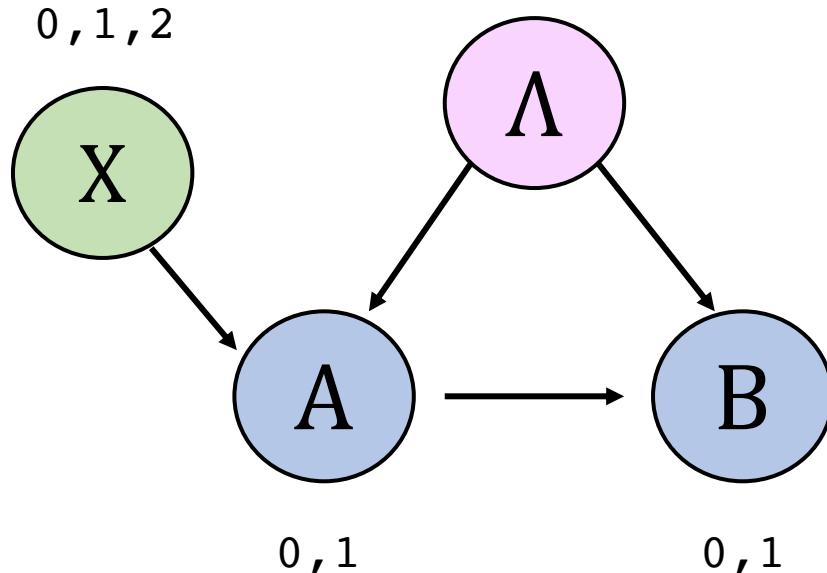
Instrumental scenario



Instrumental scenario



Instrumental scenario

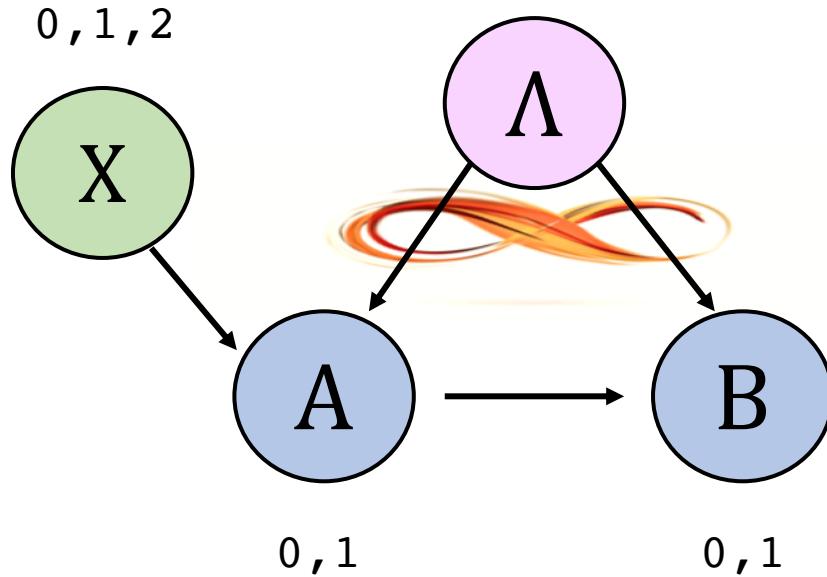


Instrumental Inequality

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

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

Instrumental scenario



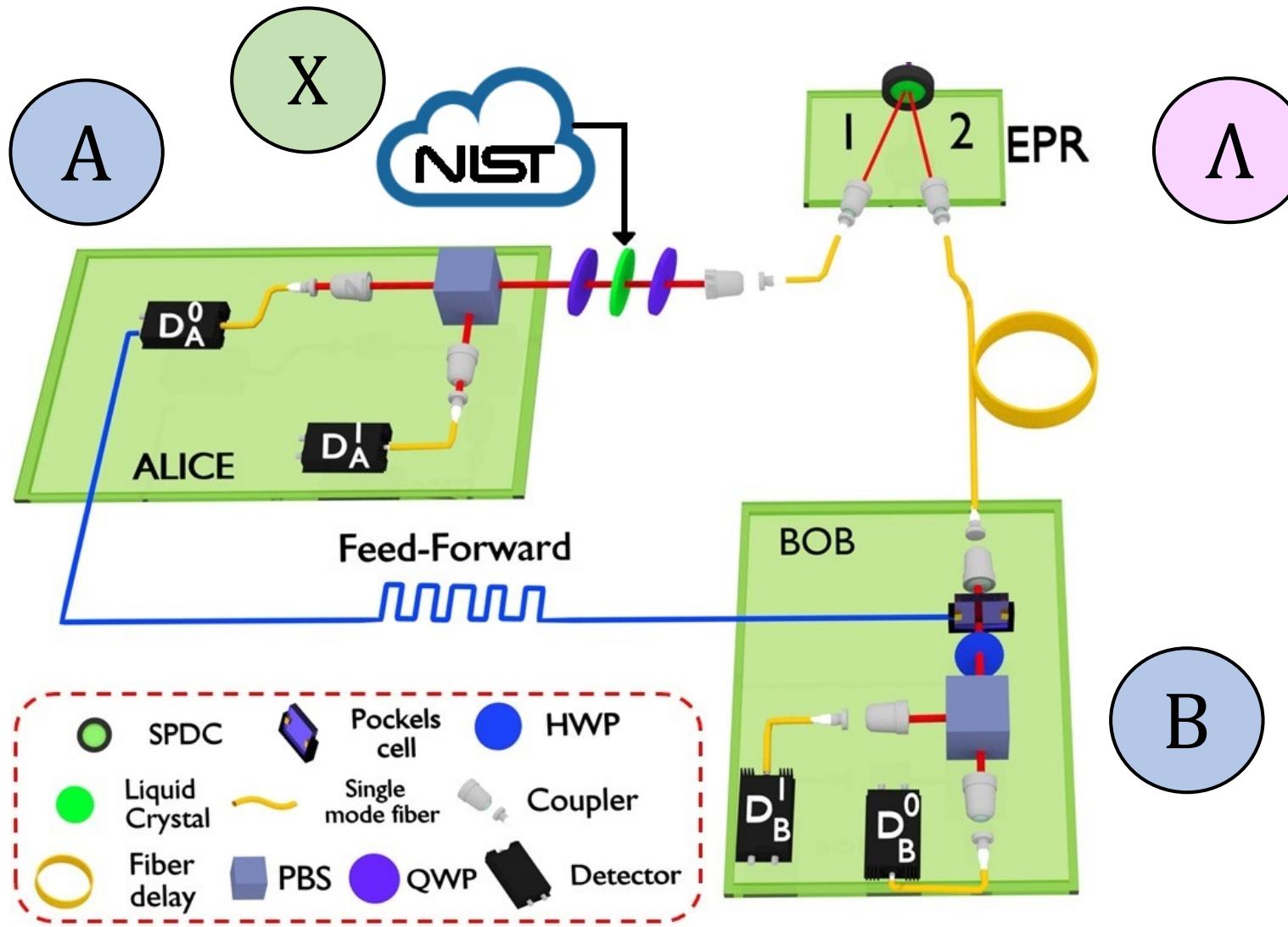
Instrumental Inequality

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

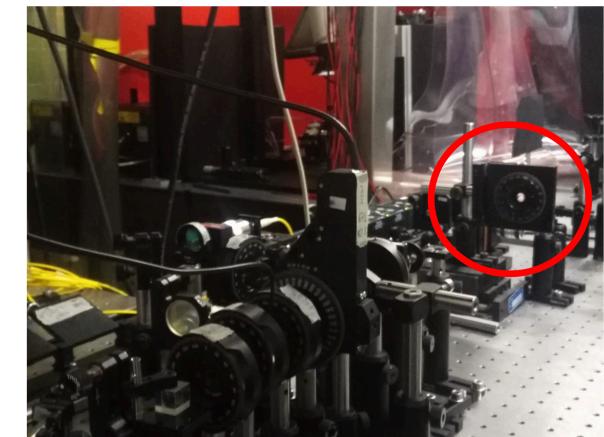
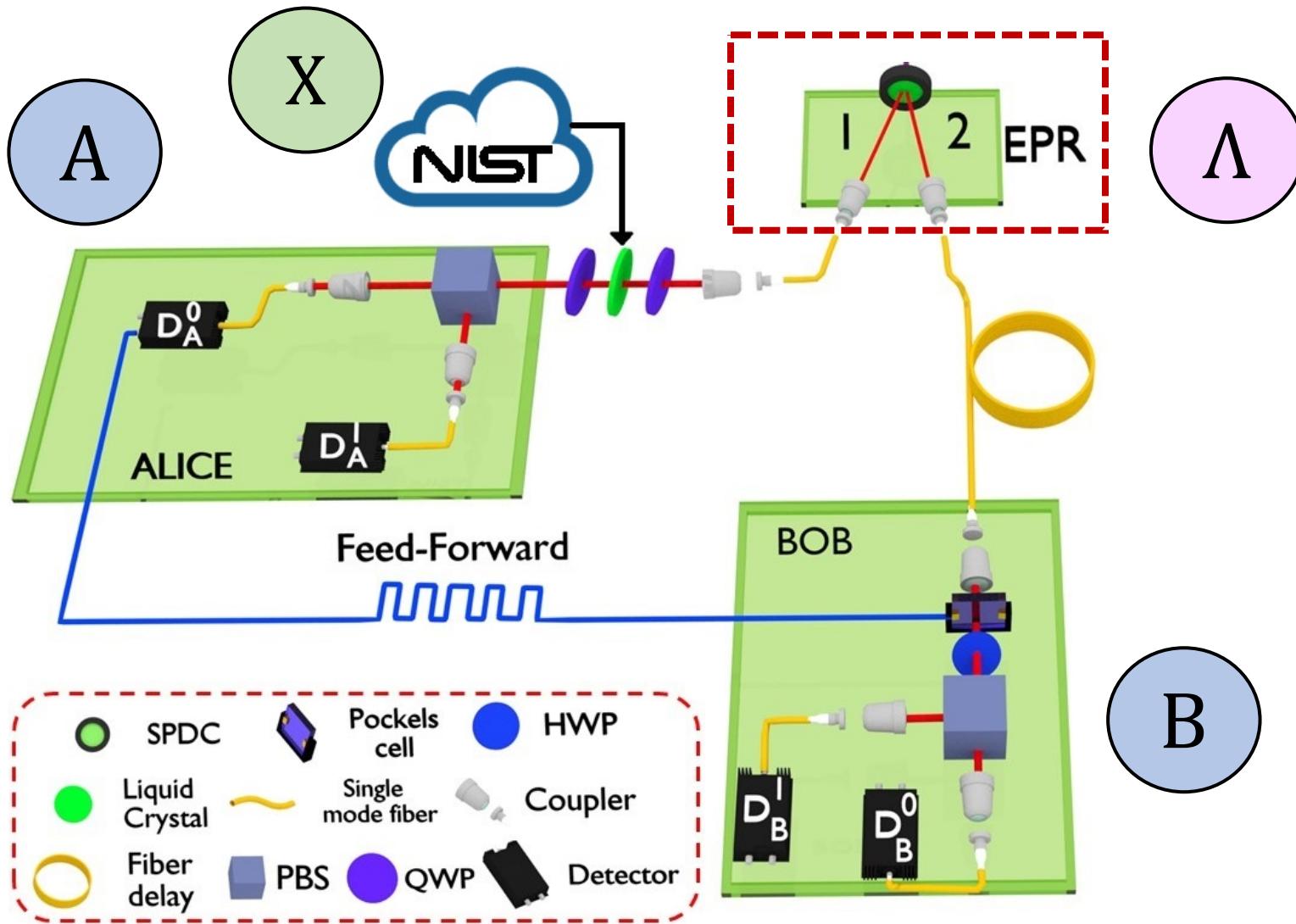
with $\langle AB \rangle_x = \sum_{a,b=0,1} (-1)^{a+b} p(a, b|x)$

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

Experimental Implementation

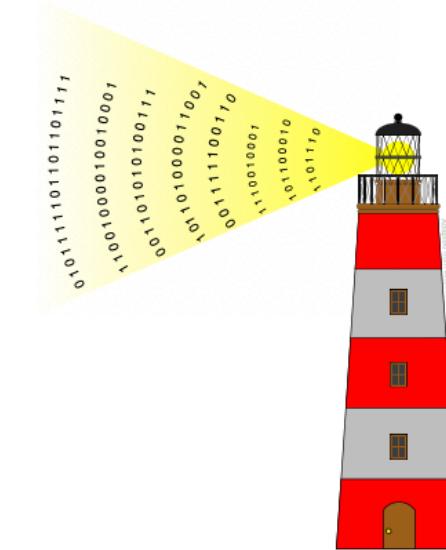
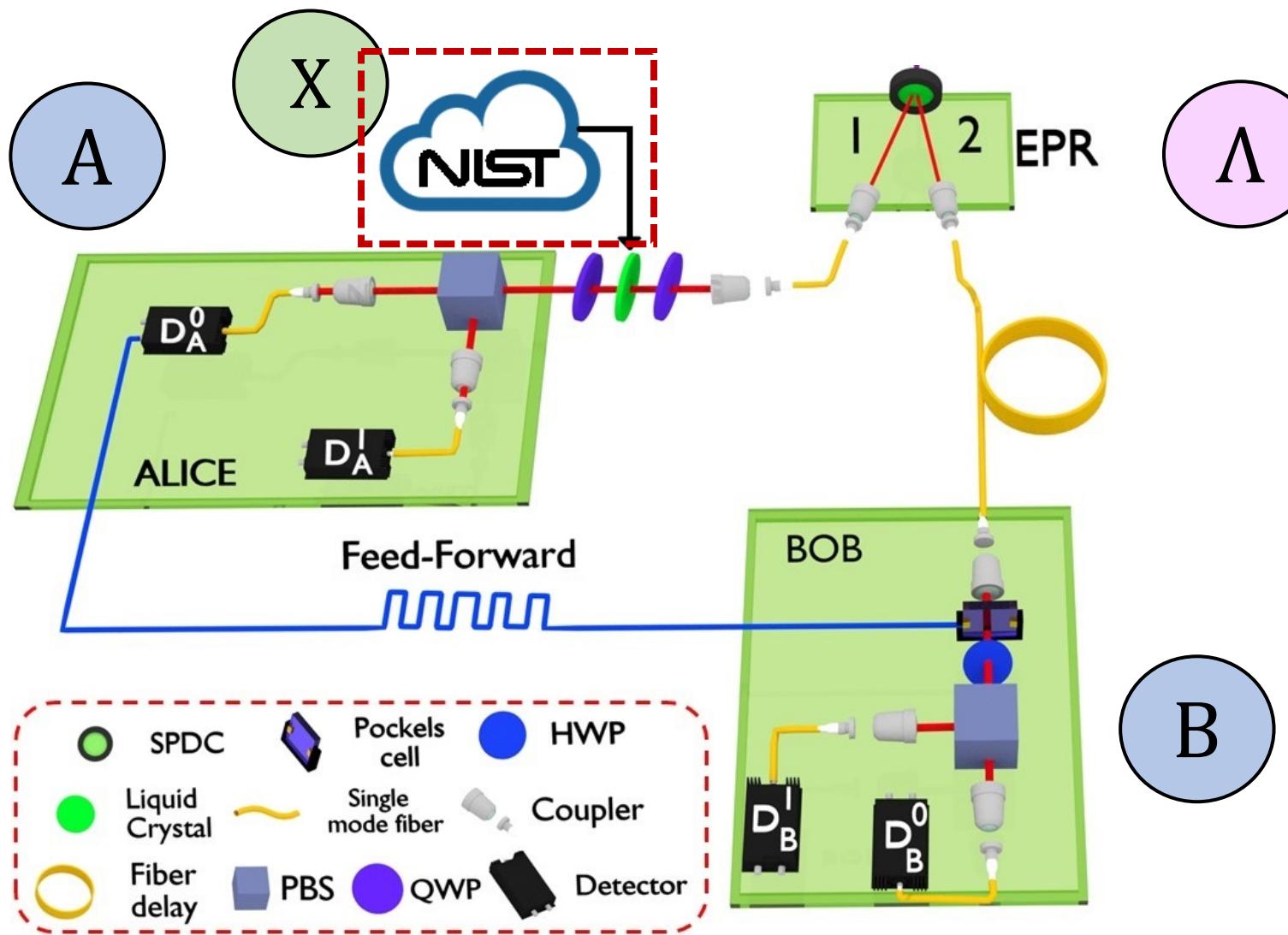


Experimental Implementation



BBO type II crystal

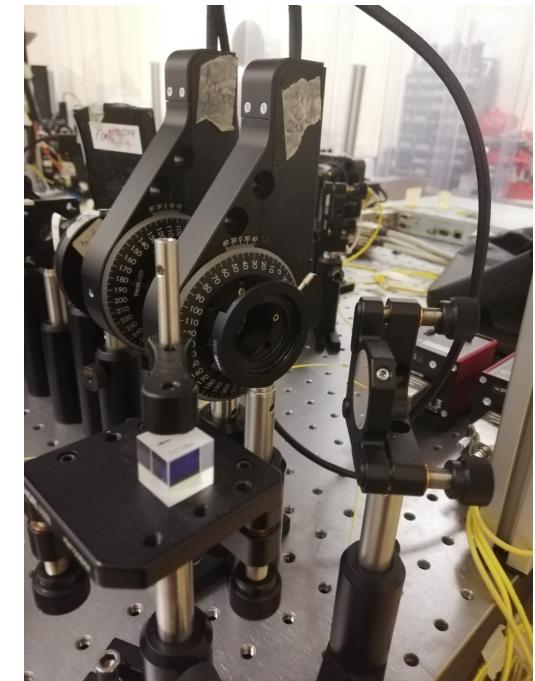
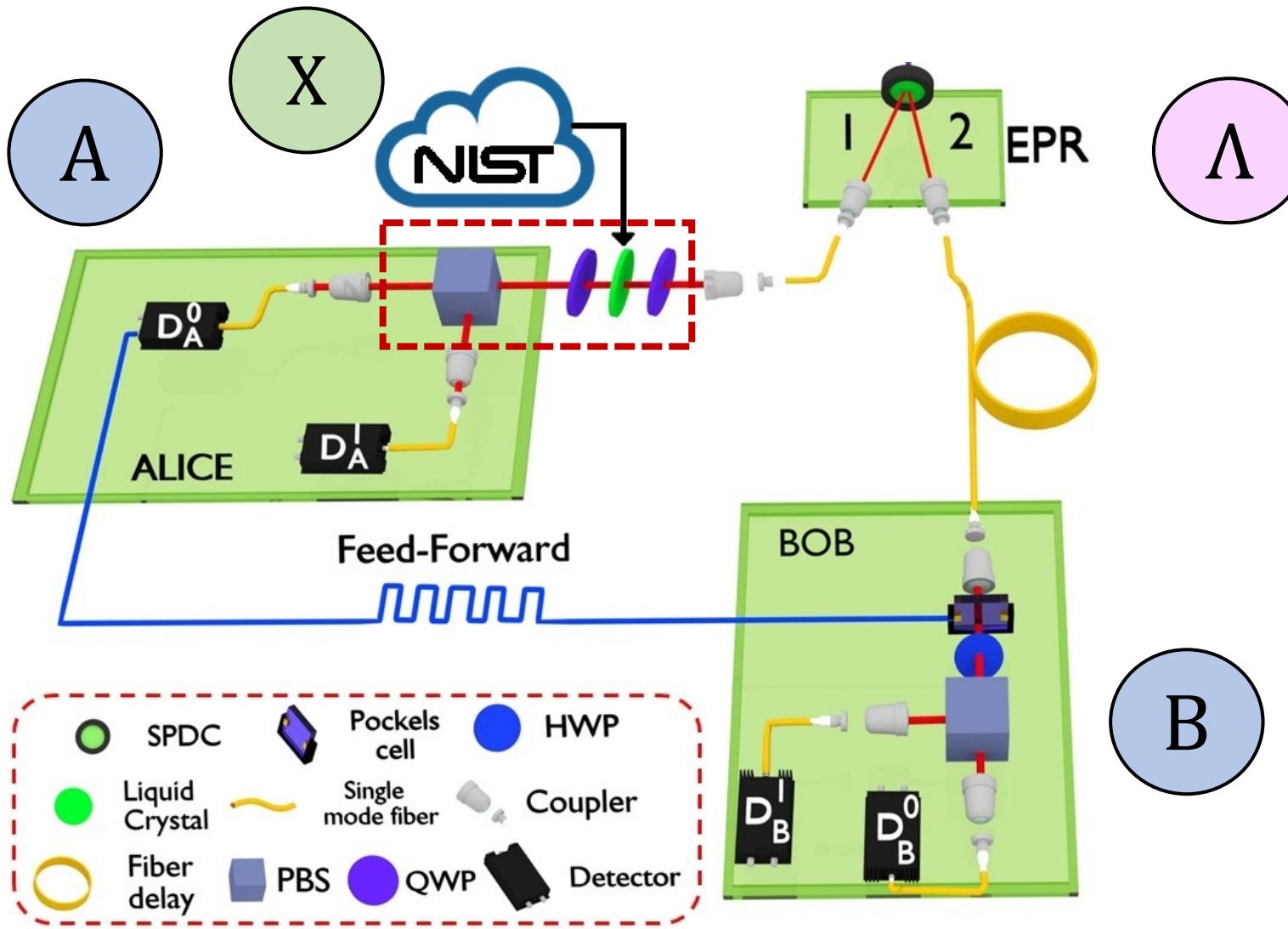
Experimental Implementation



NIST Randomness Beacon
512 bit/minute

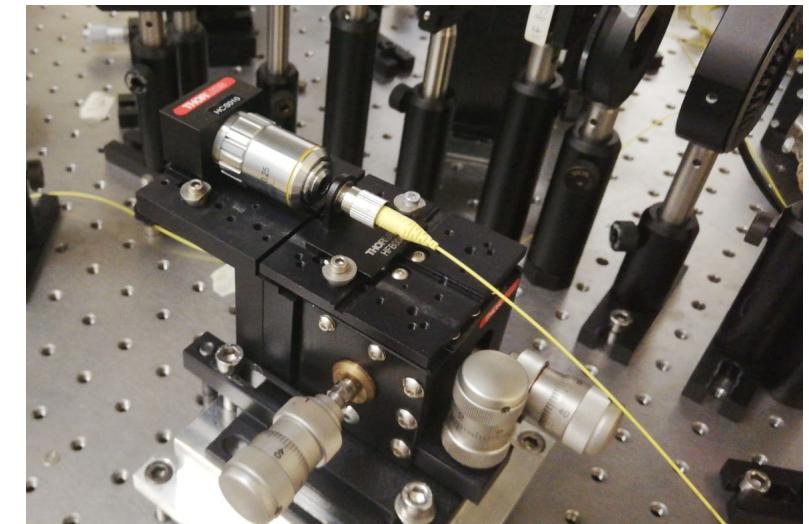
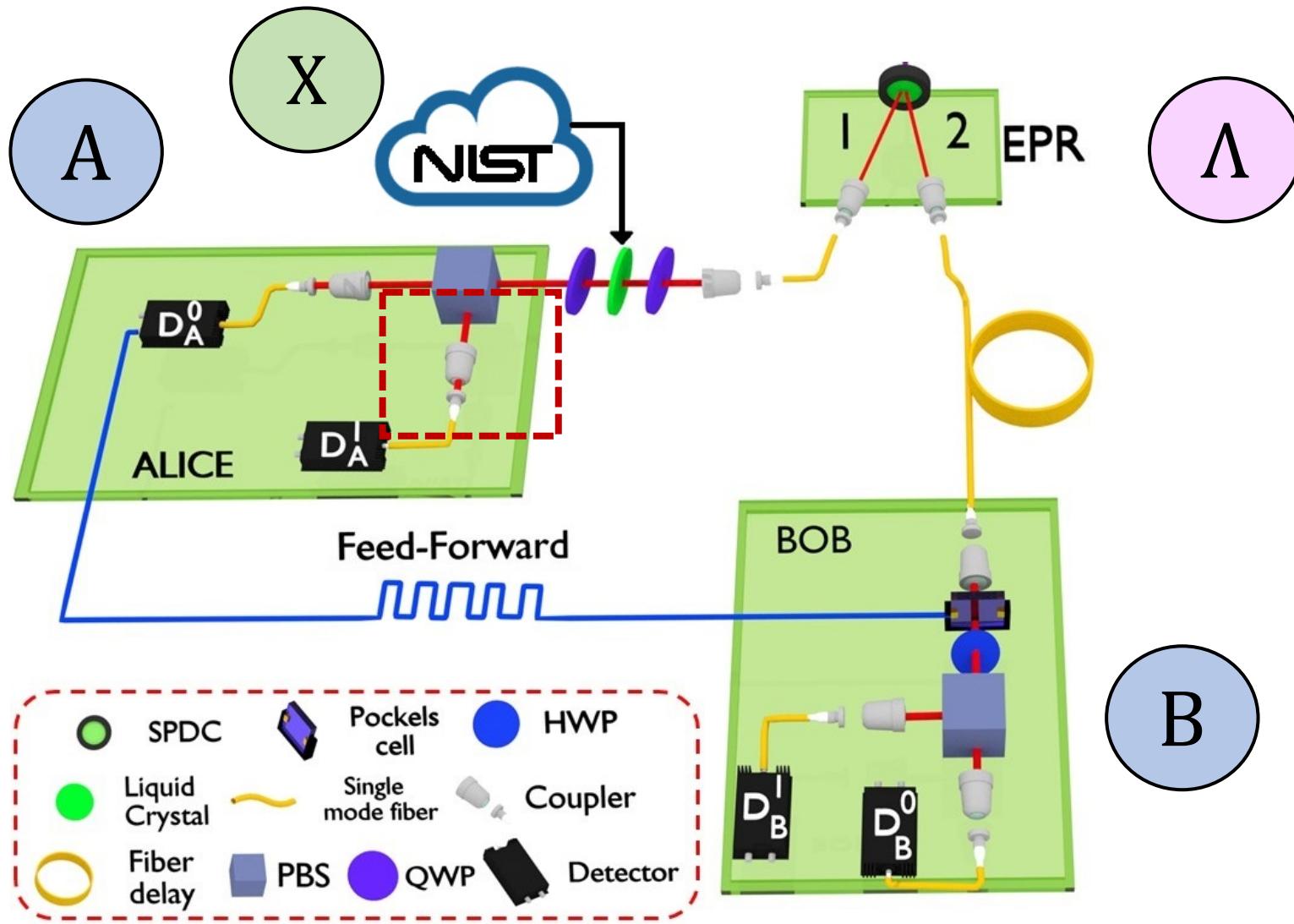
M. J. Fischer et al. Proc. International Conf. on Security and Cryptography 434-438 (2011)

Experimental Implementation



Measurement station

Experimental Implementation



Coupler

Experimental Implementation

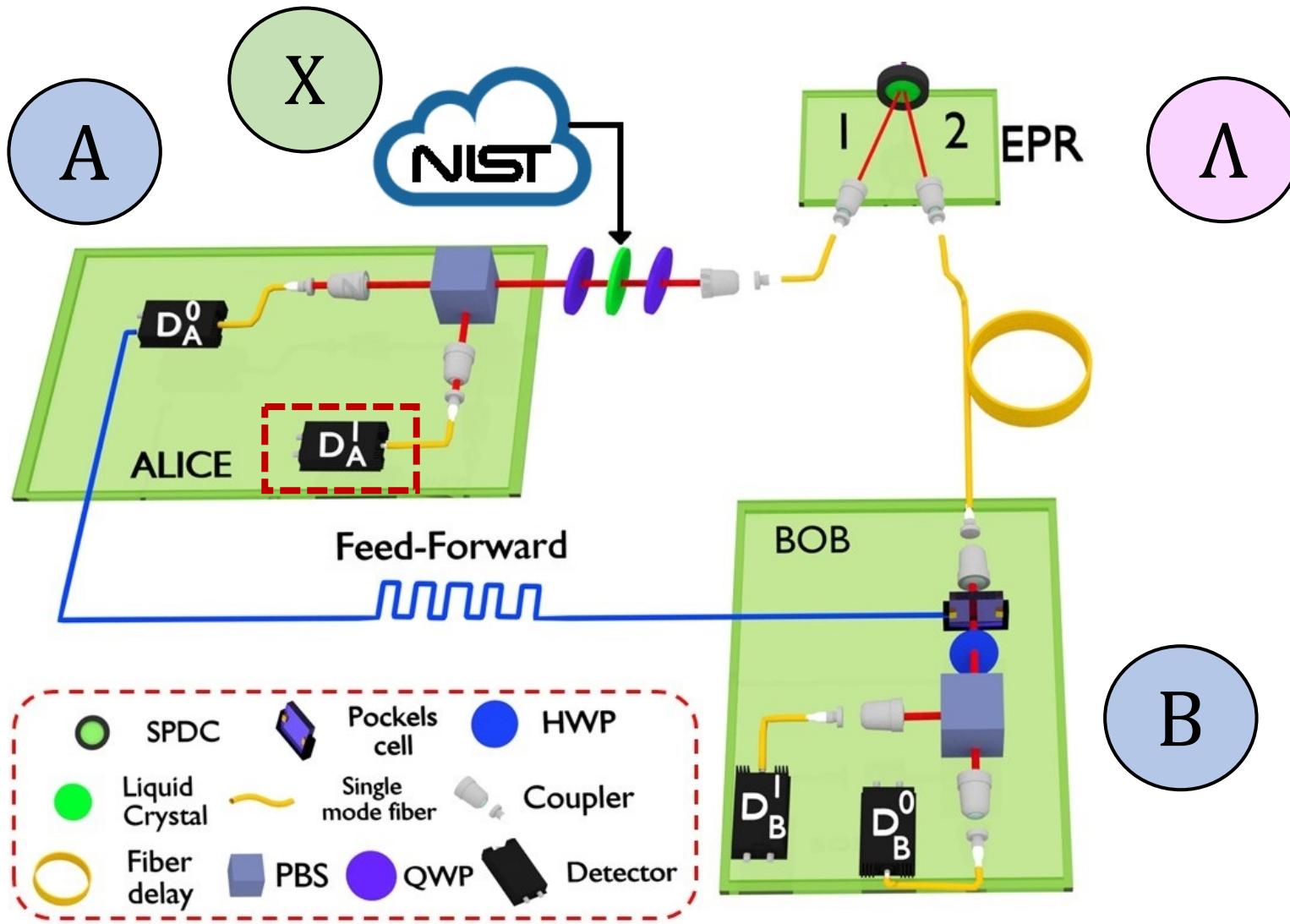
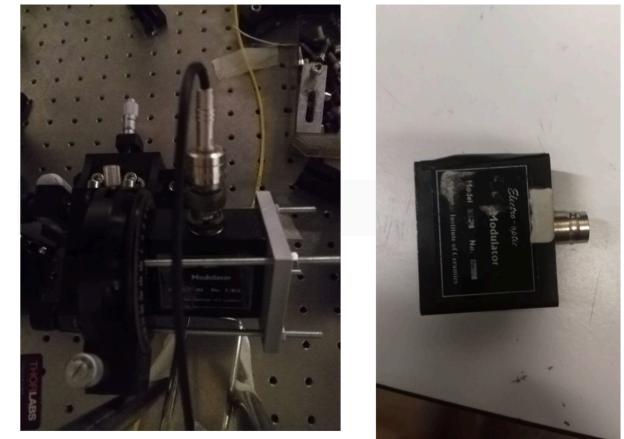
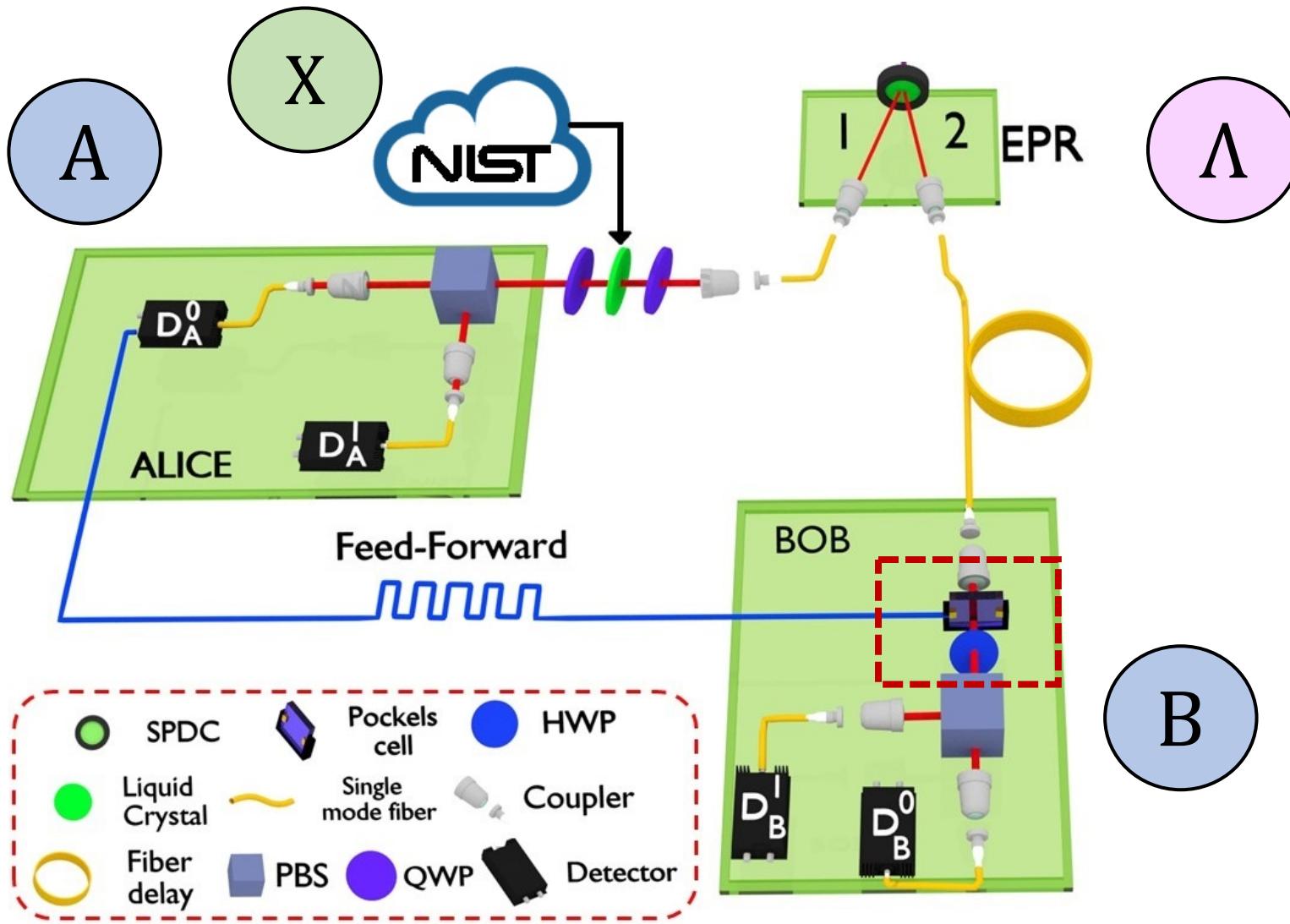


Photo-Detector

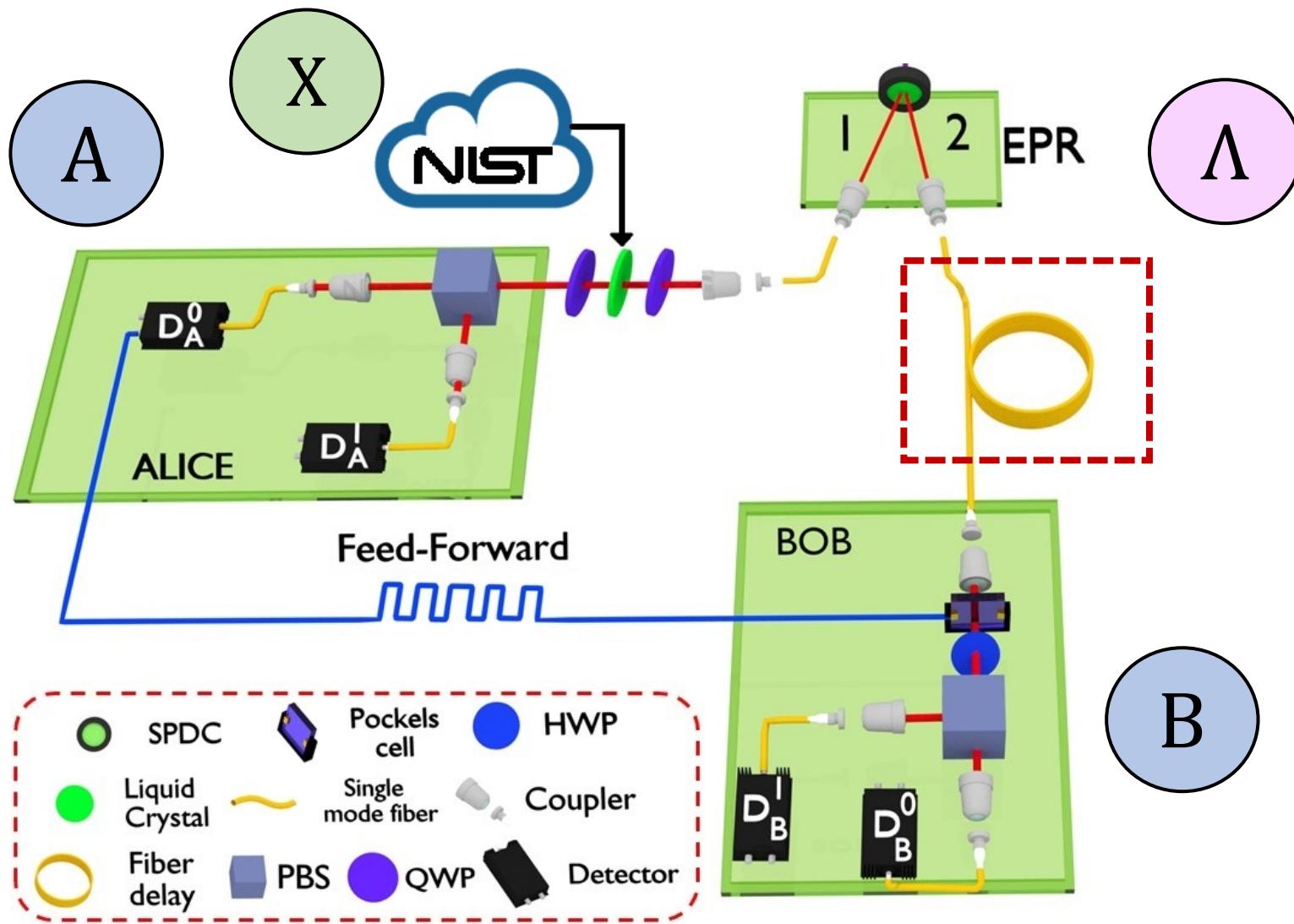
Experimental Implementation



Pockels cell

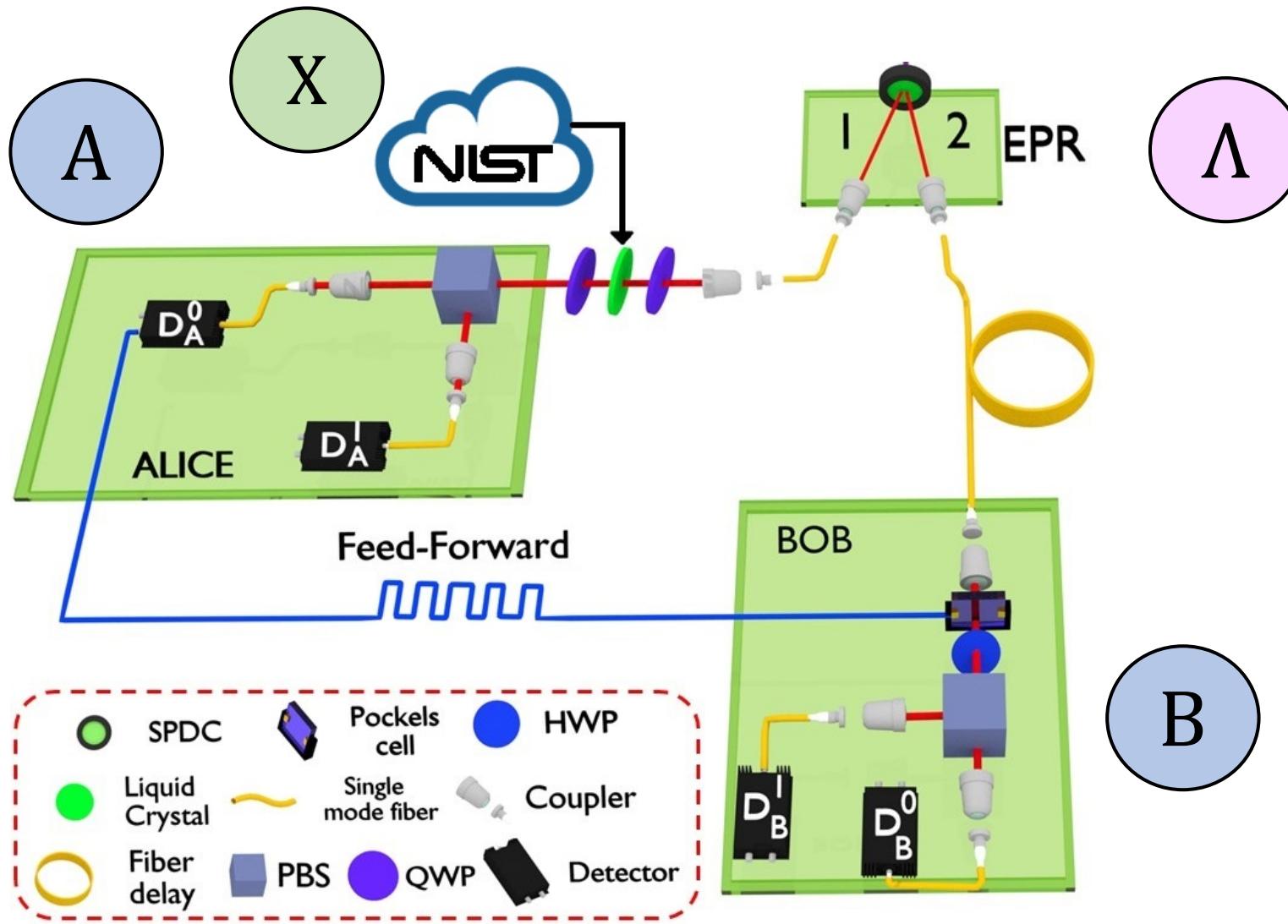
ACTIVE FEED-FORWARD

Experimental Implementation



Single mode fiber 125 m long

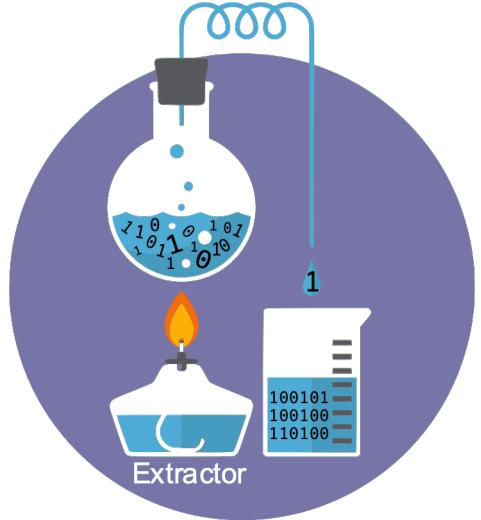
Experimental Implementation



$$\mathcal{I}_{exp} = 3.797 \pm 0.050$$

Randomness extraction

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

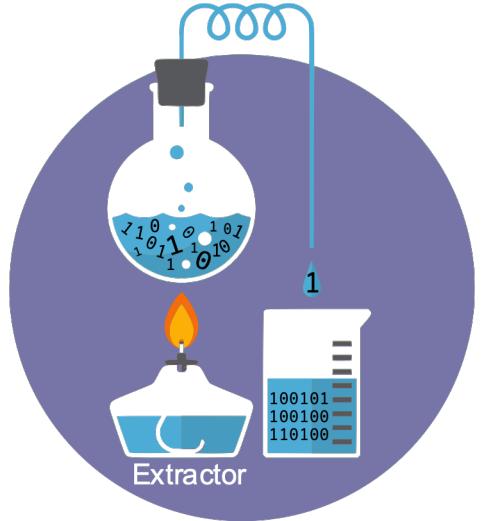
$$P(a,b|x, y=a) = \text{Tr}(\mathcal{M}_a^x \mathcal{M}_b^a \rho_{AB})$$

and

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

Randomness extraction

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



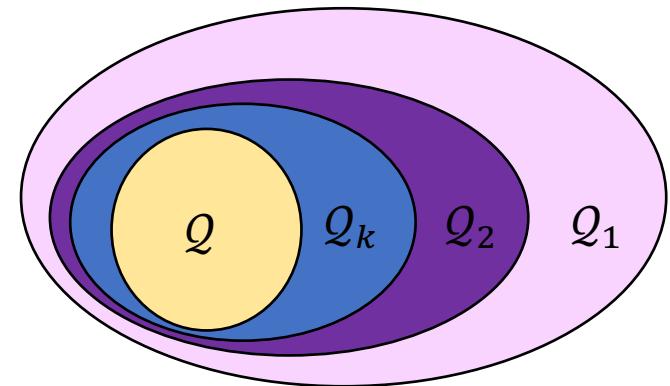
$$\min(\mathcal{H}_{\min}(x)) = f_x(\mathcal{I})$$

NPA hierarchy

We recast the optimization as a SDP problem

$$P(a, b|x, y = a) \in Q_2$$

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



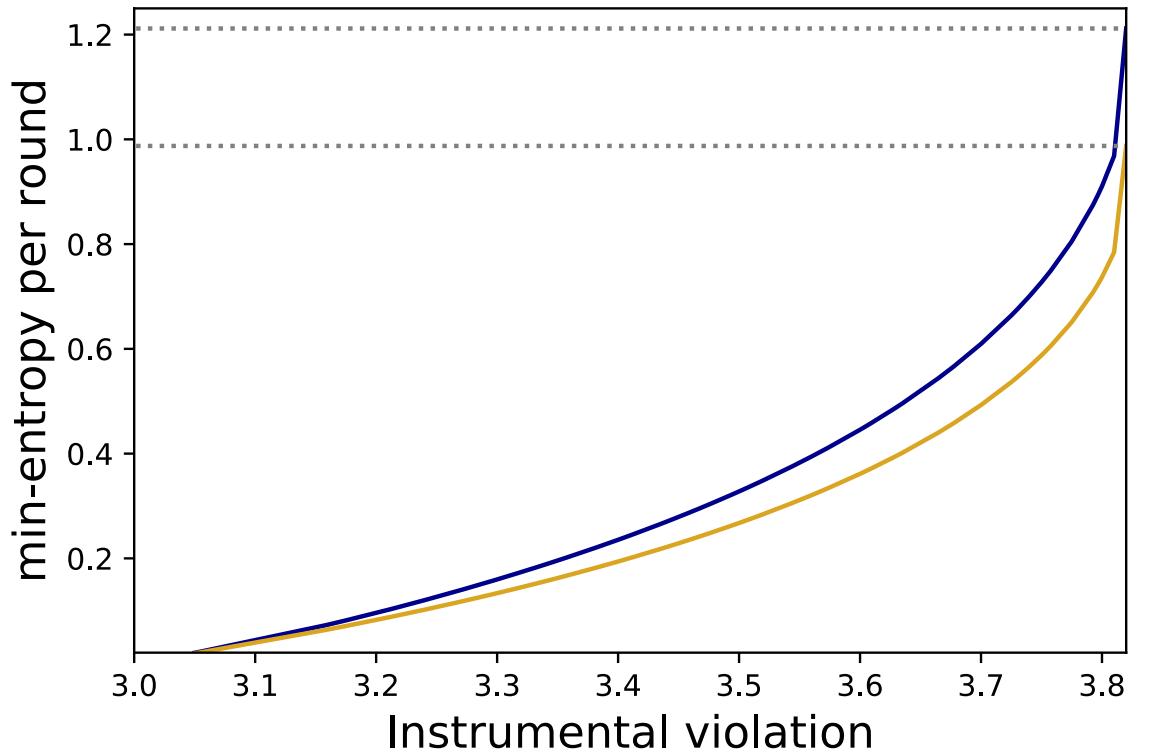
Min-entropy per round

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

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

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

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



How does this min-entropy accumulate throughout the multiple runs?

Entropy accumulation

If the runs are independent and the probability distribution $P(a,b|x)$ is the same (*iid* assumption)

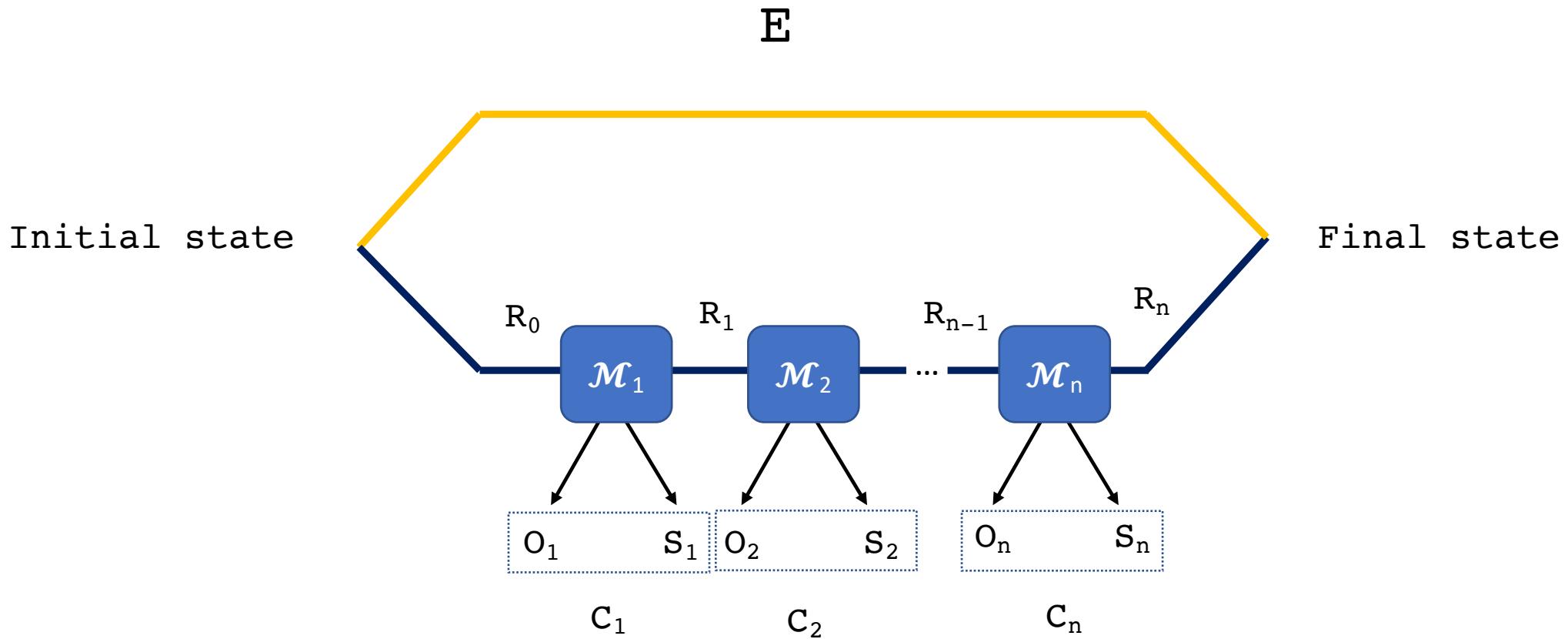
$$\mathcal{H}_{min}^\epsilon(R|S,E) \geq n\mathcal{H}(r|s,e) - c_\epsilon \sqrt{n}$$

$$R = a_1 b_1 a_2 b_2 \dots a_n b_n \quad S = x_1 x_2 \dots x_n \quad r = (a, b) \quad s = x_1$$

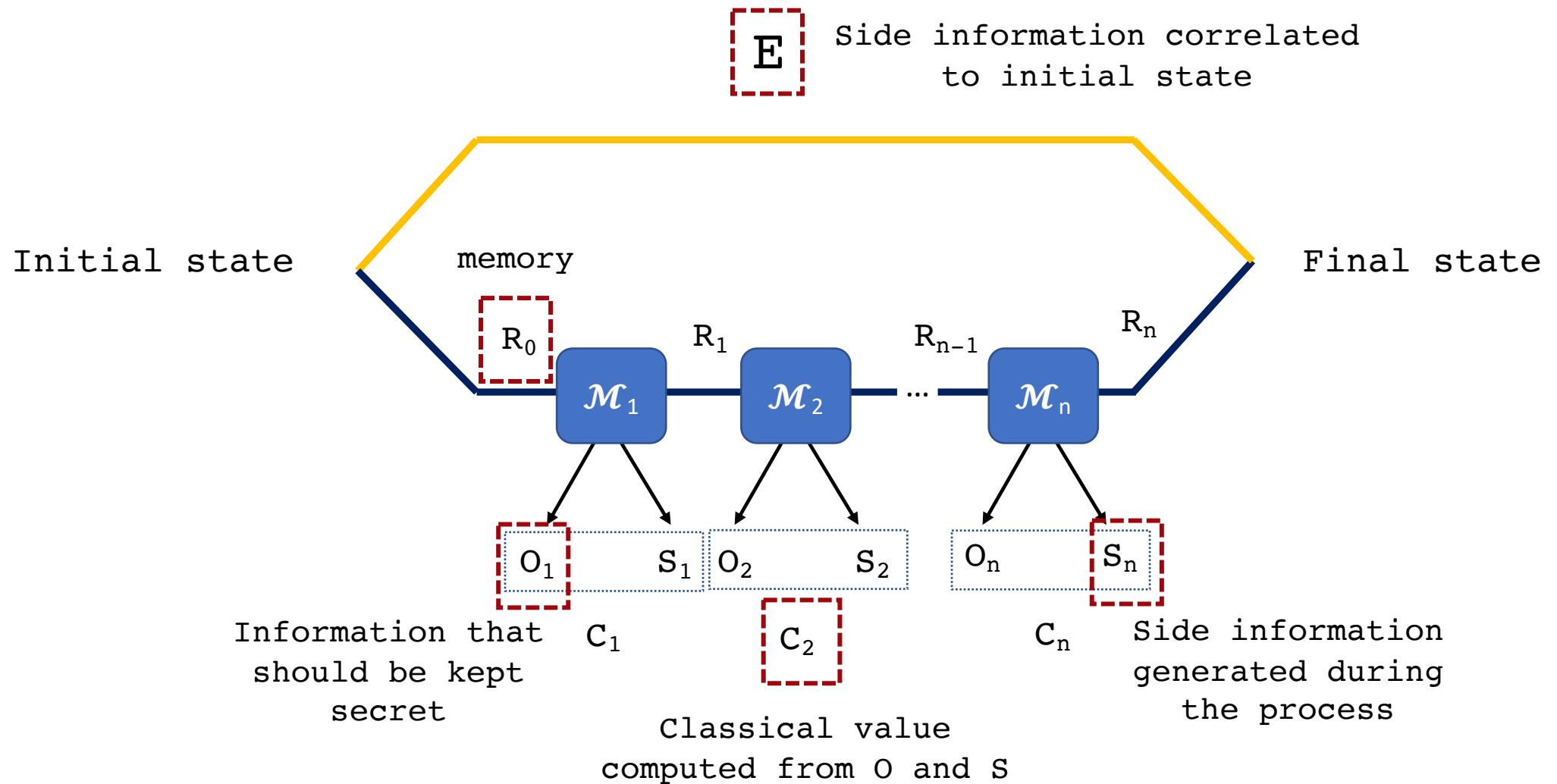
an eavesdropper has side information about the single tuple (a_i, b_i, x_i)

To address the most general case, taking into account that there could be interdependencies among the runs, we need to resort to the **Entropy Accumulation Theorem** (EAT)

EAT channels



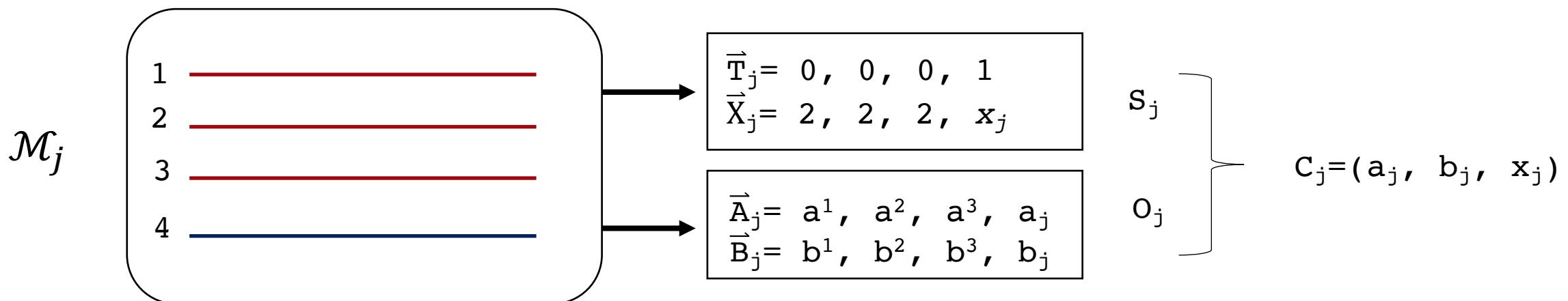
EAT channels



Our Protocol

We define a variable $\mathbf{T} = \text{Bernoulli}(\gamma)$:

- if $T=1$, $x \in (0,1,2)$ (**test** run)
- if $T=0$, $x=2$ (**accumulation** run)



After applying n channels, we evaluate the violation \mathcal{I}_{exp} from the test runs and, if $\mathcal{I}_{exp} < \mathcal{I}_{threshold} + \delta$ the protocol aborts.

Smooth min-entropy bound

We define an event Ω for which our protocol does not abort,

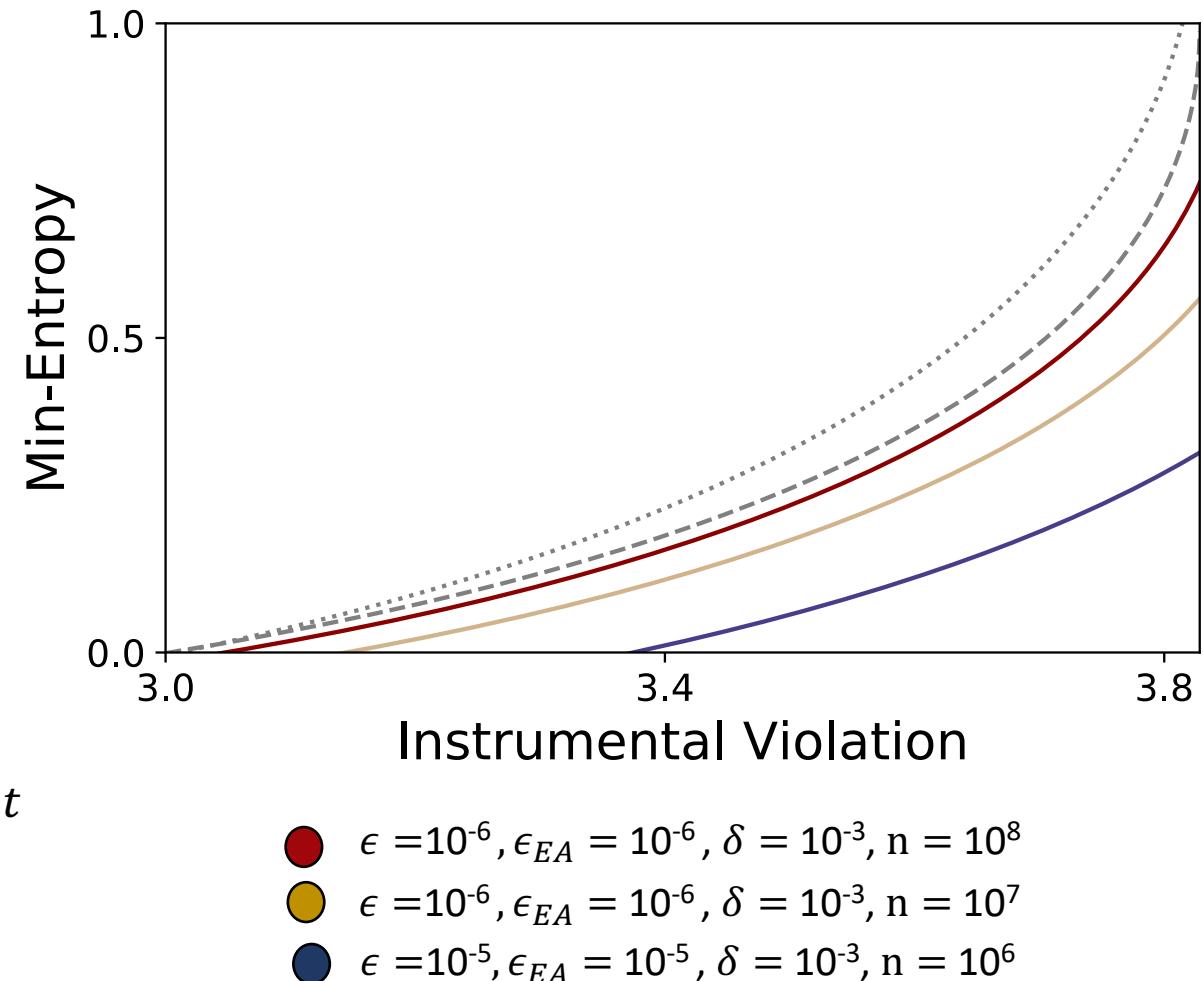
i.e. that we obtain a $\mathcal{I} > \mathcal{I}_{\text{threshold}}$.

Then, the smooth min-entropy, on the state conditioned on Ω is lower bounded by:

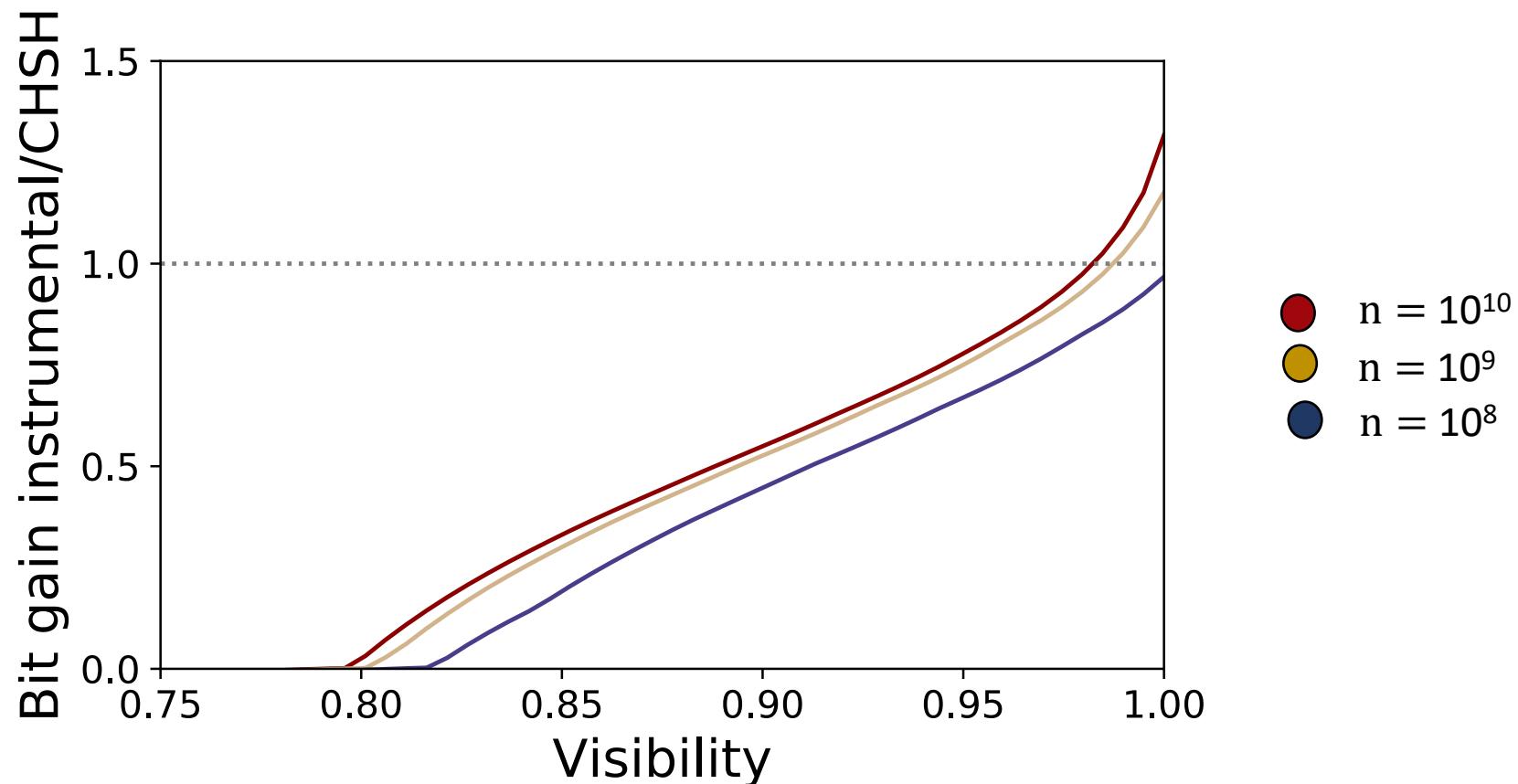
$$\mathcal{H}_{\min}^{\epsilon}(R|S, E) \geq nt - \nu\sqrt{n}$$

ν depends on:

- ϵ (smoothing parameter)
- ϵ_{EA} (error on the EA)
- $\|\nabla f_{\min}\|_{\infty}$ where $f_{\min} \leq \inf_{\Sigma_i(p)} \mathcal{H}(O_i|S_i E)$ and $f_{\min} \geq t$
- d_{O_i} (dimension of O_i)
- δ (statistical uncertainty on \mathcal{I})



Comparison with CHSH



Bit gain = (# obtained bits) / (# invested bits)
Visibility v : $\rho = |\Phi\rangle\langle\Phi| v + I/4(1 - v)$

Results

In our experiment

$n = 172095$

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

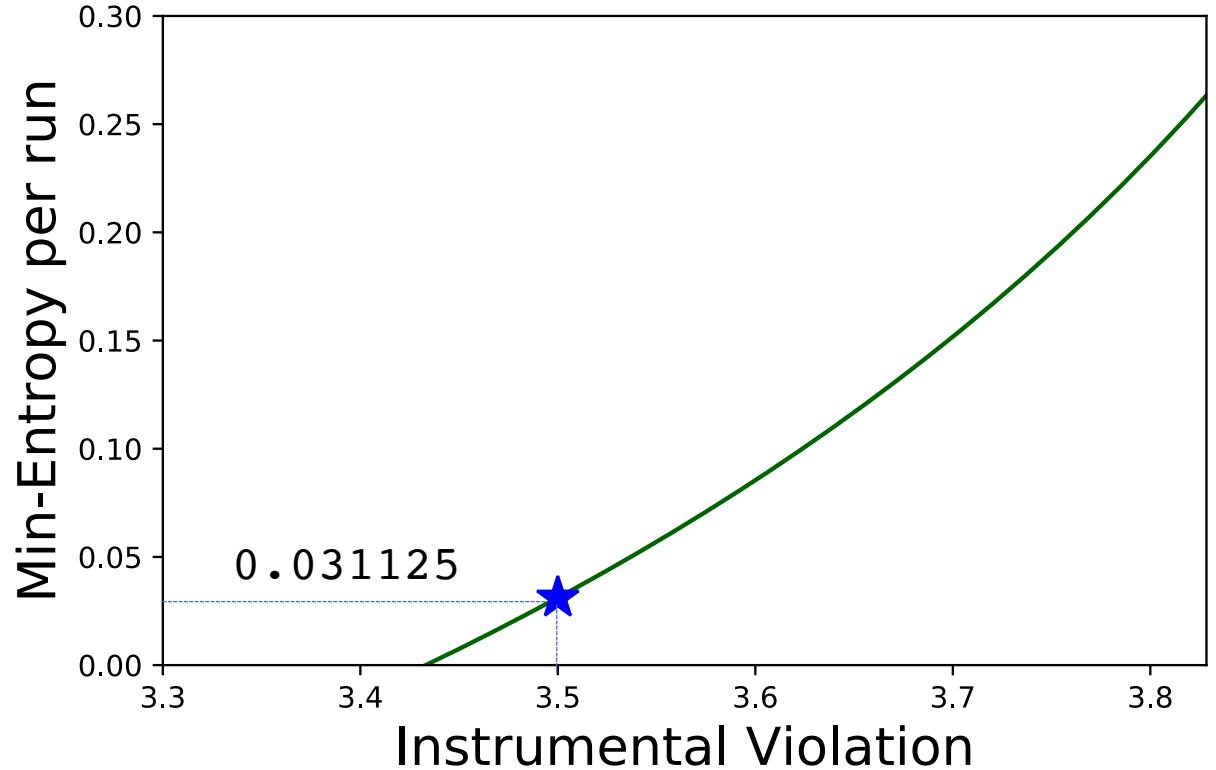
$\mathcal{I}_{threshold} = 3.5$

$\delta = 0.011$

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

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

(classical extractor)



5270 extracted bits

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

I. Agresti et al., arXiv:1905.02027 (2019).

Conclusions

- Design of the first **DI protocol** within the **Instrumental scenario**.
- The protocol guarantees **full security**.
- Experimental **implementation** of the protocol in all of its parts.
- Under given circumstances, the **randomness gain** is **higher** than CHSH based protocols.
- This study opens the path for **future investigation** of the Instrumental scenario for quantum information processing tasks.



UNIVERSIDADE FEDERAL
DO RIO DE JANEIRO



INTERNATIONAL
INSTITUTE OF
PHYSICS
Federal University of Rio Grande do Norte



References

CLASSICAL INSTRUMENTAL SCENARIO

Pearl, Proc. UAI 1995, arXiv:1302.4976

Bonet, Proc. UAI 2001, arXiv:1301.2258

QUANTUM INSTRUMENTAL SCENARIO

Chaves et al., *Nat. Phys.* **14**, 291–296 (2018)

Van Himbeeck et al., arXiv:1804.04119 (2018)

Poderini et al., Proc. UAI 2019

ENTROPY ACCUMULATION THEOREM

Arnon-Friedman et al., *Nat. Comm.* **9**, 459 (2019)

CLASSICAL EXTRACTOR

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



DIPARTIMENTO DI FISICA
SAPIENZA
UNIVERSITÀ DI ROMA



QUANTUM LAB

Quantum Information Lab
Dipartimento di Fisica, Università di Roma La Sapienza



RANDOMNESS DI CERTIFICATION VIA INSTRUMENTAL SCENARIO

arXiv.org > quant-ph > arXiv:1905.02027

Search...
Help | About

Quantum Physics

Experimental device-independent certified randomness generation with an instrumental causal structure

Iris Agresti, Davide Poderini, Leonardo Guerini, Michele Mancusi, Gonzalo Carvacho, Leandro Aolita, Daniel Cavalcanti, Rafael Chaves, Fabio Sciarrino

(Submitted on 3 May 2019 (v1), last revised 8 Sep 2019 (this version, v3))

The intrinsic random nature of quantum physics offers novel tools for the generation of random numbers, a central challenge for a plethora of fields. Bell non-local correlations obtained by measurements on entangled states allow for the generation of bit strings whose randomness is guaranteed in a device-independent manner, i.e. without assumptions on the measurement and state-generation devices. Here, we generate this strong form of certified randomness on a new platform: the so-called instrumental scenario, which is central to the field of causal inference. First, we theoretically show that certified random bits, private against general quantum adversaries, can be extracted exploiting device-independent quantum instrumental-inequality violations. To that end, we adapt techniques previously developed for the Bell scenario. Then, we experimentally implement the corresponding randomness-generation protocol using entangled photons and active feed-forward of information. Moreover, we show that, for low levels of noise, our protocol offers an advantage over the simplest Bell-nonlocality protocol based on the Clauser-Horn-Shimony-Holt inequality.

Agresti et al., arXiv:1905.02027 (2019)

