Device-independent Randomness Expansion with Entangled Photons

Yanbao Zhang

NTT Research Center for Theoretical Quantum Physics

NTT Basic Research Lab, Japan

Based on the joint work arXiv:1912.11158 with
Krister Shalm, Joshua Bienfang, Collin Schlager, Martin Stevens,
Michael Mazurek, Carlos Abellan, Waldimar Amaya, Morgan Mitchell,
Mohammad A. Alhejji, Honghao Fu, Joel Ornstein,
Richard P. Mirin, Sae Woo Nam, Manny Knill

Randomness

Random number generator

A random number is:

- Unpredictable
- Uniformly distributed
- Private

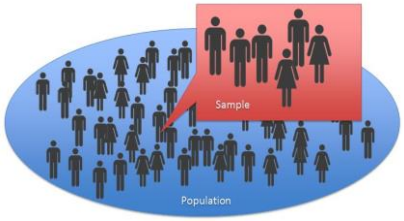
Randomness & its applications

Random number generator

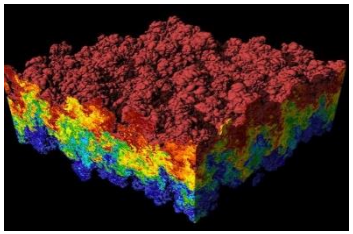
A random number is:

- Unpredictable
- Uniformly distributed
- Private

Gambling



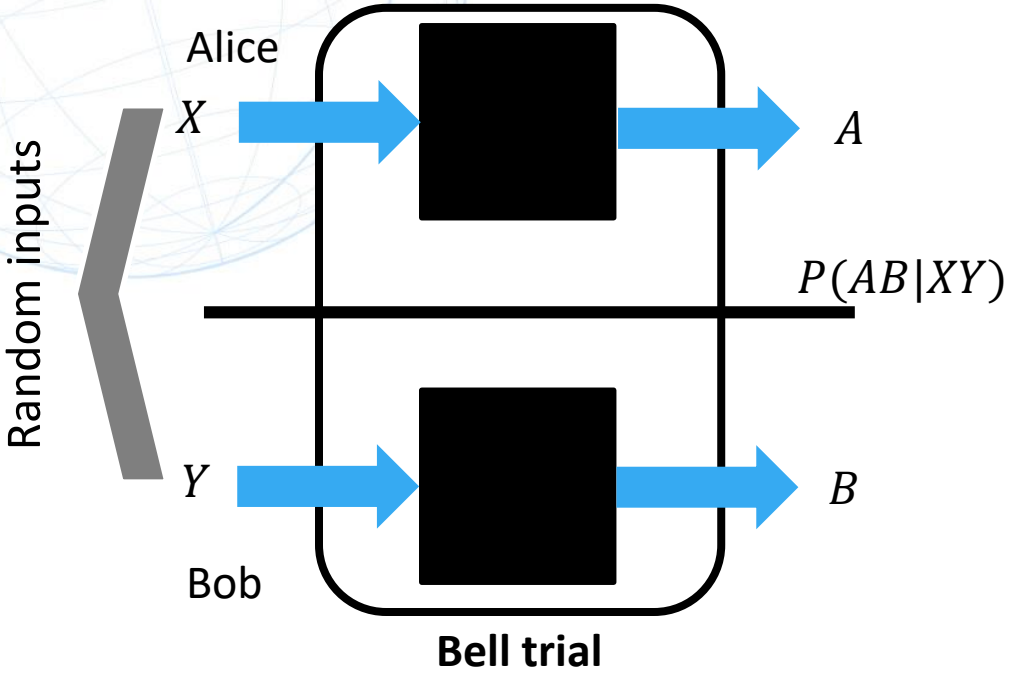
Sampling



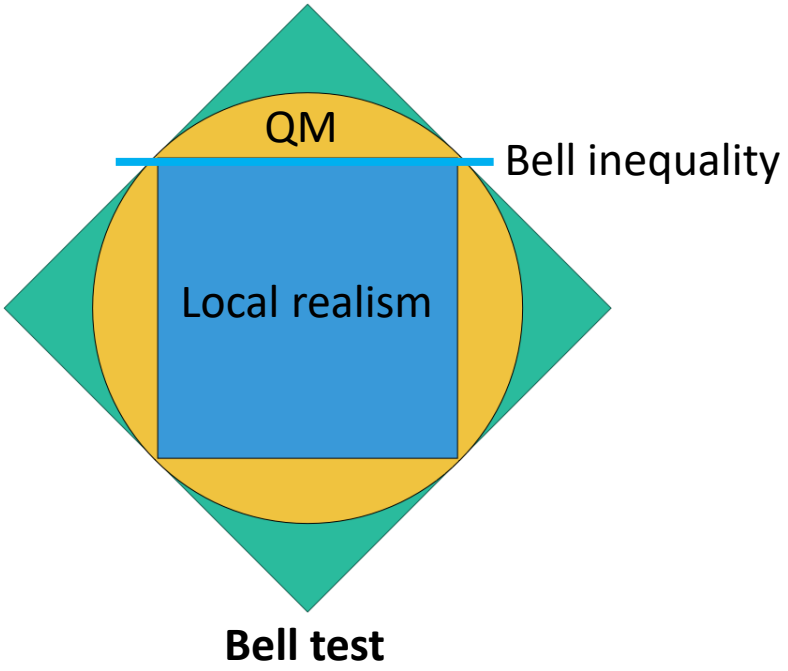
Simulation

Cryptography

Device-independent randomness generation



Bell trial



Bell test

As long as the conditional distributions $P(AB|XY)$ violate local realism, the outputs are not deterministic functions of the inputs and any other side information. Hence, the outputs must contain unpredictable randomness.

R. Colbeck, Ph.D. thesis (2006)

(Loophole-free) demonstrations of DIRG

	Experiment time	# of input bits	# of output bits	Error bound	Adversary
Pironio *et al.*, Nature, 2010	~ 1 month	6032	(unextracted) 42	10^{-2}	Classical
Liu *et al.*, PRL, 2017	111 hours	8×10^{10}	4.6×10^{7}	10^{-5}	Quantum
Bierhorst *et al.*, Nature, 2018	10 mins	1.2×10^{8}	1024	10^{-12}	Classical
Liu *et al.*, Nature, 2018	96 hours	1.4×10^{11}	6.2×10^{7}	10^{-5}	Quantum
Shen *et al.*, PRL, 2018	43 mins	3.5×10^{8}	6.2×10^{5}	10^{-10}	Quantum
Zhang *et al.*, PRL, 2020	~ 5 mins	4.8×10^{7}	512	5.4×10^{-20}	Quantum

*All demonstrations use the CHSH Bell-test configuration, where $A, B, X, Y \in \{0,1\}$.

Device-independent randomness expansion

- Obstacle --- For the CHSH Bell test, each trial consumes exactly 2 random bits and produces at most 2 bits of randomness [A. Acin *et al*., PRL 108, 100402 (2012)].

- Solution --- Spot-checking protocol
  [S. Pironio *et al*., Nature 464, 1021 (2010); C. Miller and Y. Shi, SIAM J. Comput. 46, 1304 (2017)]

A trusted third party determines randomly with a small probability q whether a trial is a spot-checking trial

1. If the trial is a spot-checking trial, Alice and Bob perform the CHSH Bell test.
2. If not, Alice and Bob use the fixed inputs $X = 0$ and $Y = 0$.

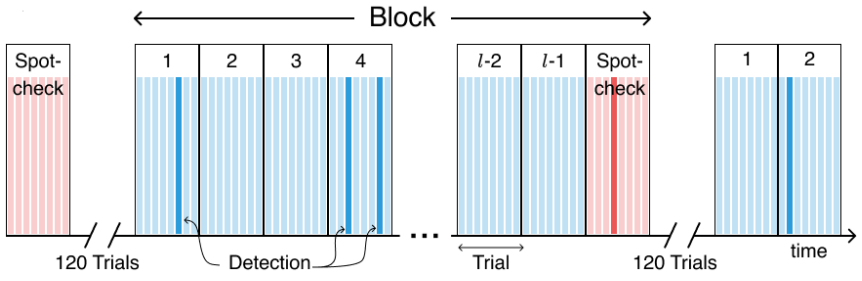
!!! Assumption: The untrusted devices cannot learn in advance whether or not a trial is a spot-checking trial.

Key for expansion: Every trial produces randomness, while only spot-checking trials consume randomness.

Con: It requires random bits with a specific bias.

Block-wise spot-checking protocol

- An experiment consists of a sequence of blocks.
- A trusted third party determines the length of each block (i.e., the number of trials in a block).
  The block length is chosen to be the value l of a uniform random variable L, where $l \in \{1, 2, \dots, 2^k\}$.
- The last trial in a block is the spot-checking trial, while for the other trials in a block, the inputs of Alice and Bob are fixed to $X = 0$ and $Y = 0$.

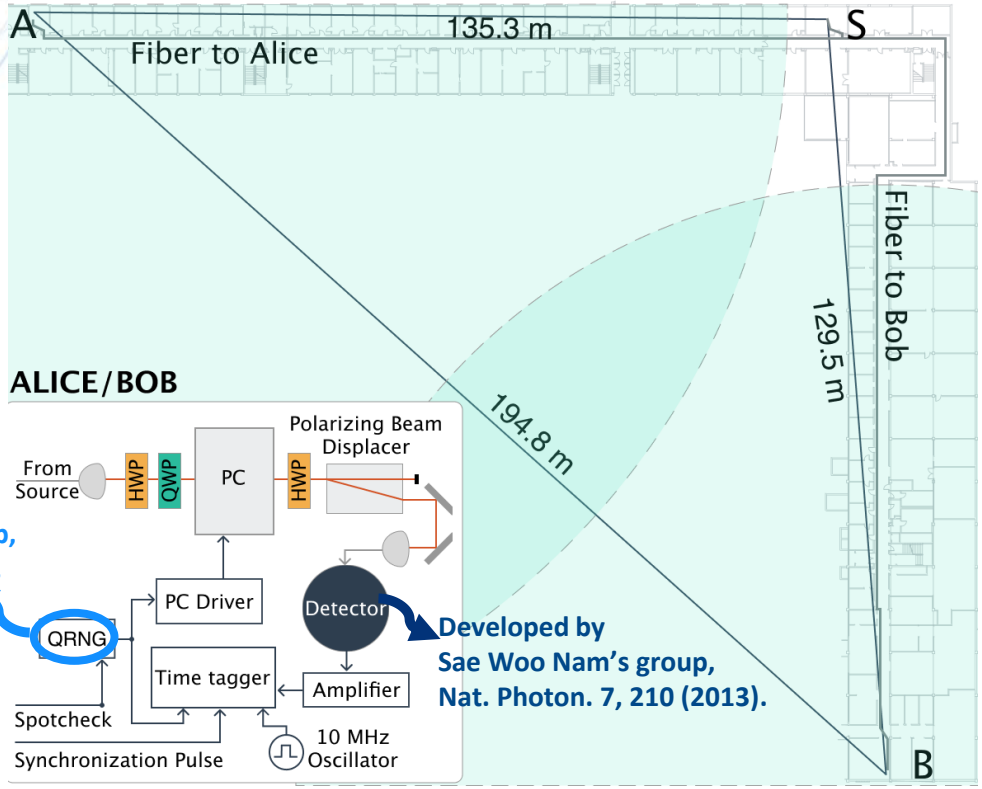


- ☐ Assumption --- The untrusted devices cannot learn in advance when a block ends with a spot-checking trial.
- ✓ Advantage --- consumes only uniform bits!

Key observation for randomness expansion:
Each block consumes only k bits for length determination and 2 bits for input choices (in the CHSH configuration), while each trial in the block contributes to randomness generation.

Experimental implementation (I)

Locations of Alice (**A**) and Bob (**B**), while the source and Spot (the trusted third party) are co-located at the station **S**.



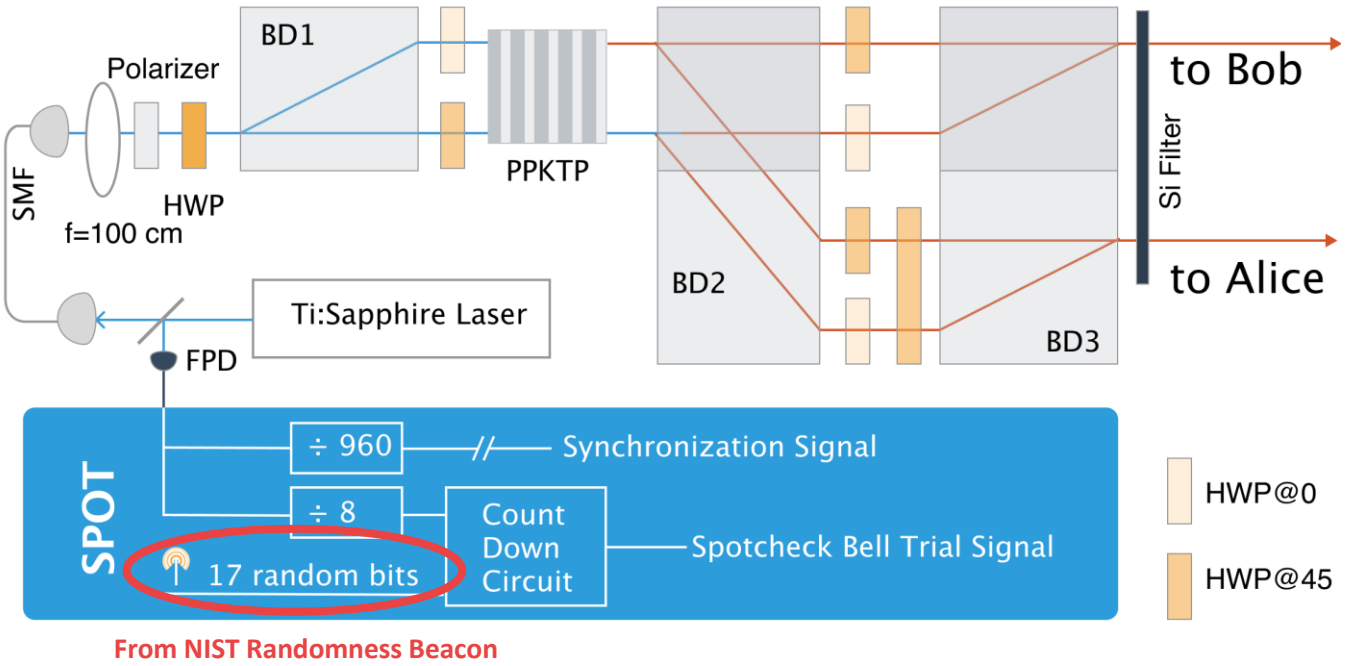
Developed by Morgan Mitchell's group, PRL 115, 250403 (2015).

Developed by Sae Woo Nam's group, Nat. Photon. 7, 210 (2013).

- Detection loophole is closed, as the system detection efficiency is ~76.3%.
- Space-like separation between the measurement processes of Alice and Bob is ensured.

Experimental implementation (II)

Entanglement Source & Spot



From NIST Randomness Beacon

- Trial rate is $\sim 10^7$ trials/second, corresponding to ~153 blocks/second.
- Over two weeks, 110.3 hours worth of block data for expansion was collected.
- We collected data in a series of cycles: After collecting each hour worth of block data or when observing a change of efficiency or visibility, 2 mins of calibration data was collected and a new cycle started.

Certifying randomness by probability estimation

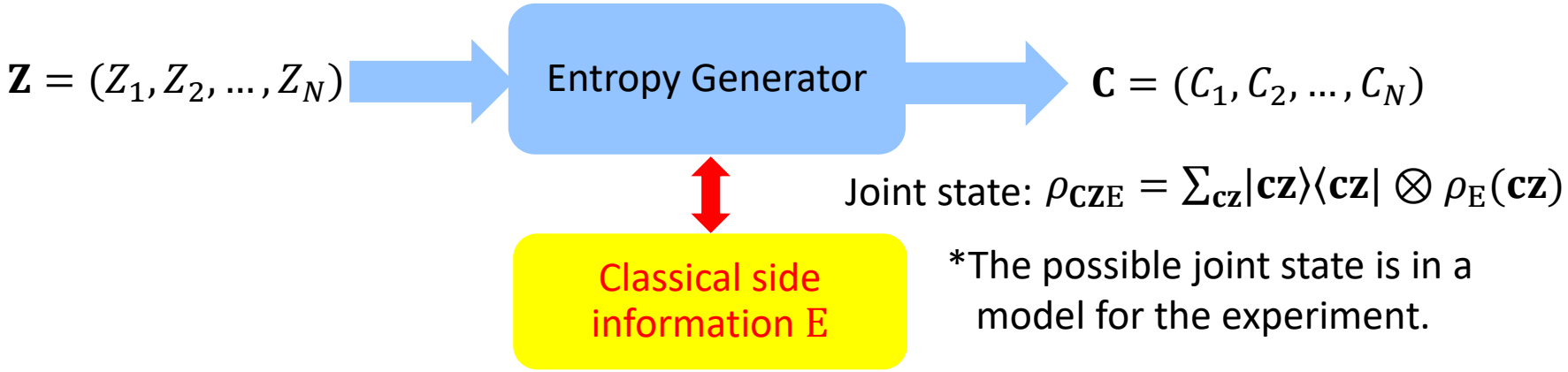
Theorem: For each possible state $\rho_{\mathbf{CZE}}$, *either* the success probability satisfies

$$\mathrm{Prob}_{\rho_{\mathbf{CZE}}}(\Phi) \leq \kappa,$$

or conditional on success

$$H_{\min}^{\varepsilon_{\mathrm{en}}}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho_{\mathbf{CZE}|\Phi}} \geq \frac{1}{\beta}\log(t_{\min}) + \frac{1}{\beta}\log(\varepsilon_{\mathrm{en}}) + \frac{1+\beta}{\beta}\log(\kappa)\,.$$

- An experiment with sequential inputs $\mathbf{Z} = (Z_1, Z_2, \ldots, Z_N)$ and sequential outputs $\mathbf{C} = (C_1, C_2, \ldots, C_N)$. *$C_i = A_i B_i$ and $Z_i = X_i Y_i$.



Joint state: $\rho_{\mathbf{CZE}} = \sum_{\mathbf{cz}} |\mathbf{cz}\rangle\langle\mathbf{cz}| \otimes \rho_{\mathrm{E}}(\mathbf{cz})$

*The possible joint state is in a model for the experiment.

Y Z, E. Knill, and P. Bierhorst, PRA 98, 040304(R), 2018; see also arXiv:1709.06159

Certifying randomness by probability estimation

Theorem: For each possible state $\rho_{\mathbf{CZE}}$, *either* the success probability satisfies

$$\mathrm{Prob}_{\rho_{\mathbf{CZE}}}(\Phi) \leq \kappa,$$

or conditional on success

$$H_{\min}^{\varepsilon_{\mathrm{en}}}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho_{\mathbf{CZE}|\Phi}} \geq \frac{1}{\beta}\log(t_{\min}) + \frac{1}{\beta}\log(\varepsilon_{\mathrm{en}}) + \frac{1+\beta}{\beta}\log(\kappa)\,.$$

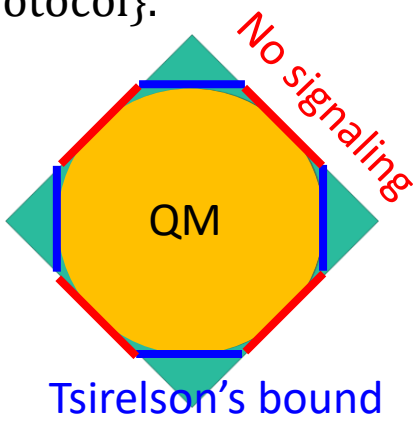
- An experiment with sequential inputs $\mathbf{Z} = (Z_1, Z_2, \ldots, Z_N)$ and sequential outputs $\mathbf{C} = (C_1, C_2, \ldots, C_N)$. *$C_i = A_i B_i$ and $Z_i = X_i Y_i$.
- For each i, Markov-chain condition, $(Z_i \perp \mathrm{C}_{<i})|\mathbf{Z}_{<i}\mathrm{E}$, is satisfied. *IID is not required.
- Model $\boldsymbol{\mathcal{M}}_i$ $(C_i Z_i)$ and probability estimation factor (PEF) $F_i(C_i Z_i) \geq 0$ with power $\beta > 0$ for each trial i. *The models and PEFs for different trials can be different.
- The success event $\Phi \triangleq \{\mathbf{cz}: \prod_{i=1}^{N} F_i(c_i z_i) \geq t_{\min}\}$.
- κ --- a desired lower bound of the success probability.

Y Z, E. Knill, and P. Bierhorst, PRA 98, 040304(R), 2018; see also arXiv:1709.06159

Model for a trial

- The model specifies all possible distributions of trial results CZ.

$$\boldsymbol{\mathcal{M}}(CZ) = \{\rho_{\mathrm{E}}(CZ): 1)\ \rho_{\mathrm{E}}(C|Z) \text{ satisfies no signaling } + \text{Tsirelson's bound};$$
$$2)\ \rho_{\mathrm{E}}(Z) \text{ is as specified according to the protocol}\}.$$



- The input distribution $\rho_{\mathrm{E}}(Z)$ with $Z = XY$ depends on the trial position in a block.

Consider the j'th trial in a block with length L. *The maximum block length is 2^k.

Conditional on $L \geq j$, the j'th trial is a spot-checking trial with prob. $q_j = {}^{1}/_{(2^k - j + 1)}$.

So, the input $Z = XY$ is $\begin{cases} \text{uniformly distributed, with prob. } q_j, \\ (X = 0, Y = 0), \text{with prob. } (1 - q_j). \end{cases}$

PEF for a trial

- A PEF $F(CZ)$ with power is $\beta > 0$ for a trial model $\boldsymbol{\mathcal{M}}(CZ)$ is a non-negative function of CZ satisfying

$$\forall \rho_{\mathrm{E}}(CZ) \in \boldsymbol{\mathcal{M}}(CZ), \left\langle F(CZ)[\rho_{\mathrm{E}}(C|Z)]^{\beta} \right\rangle \leq 1.$$

The larger the PEF, the smaller the conditional probability of C given ZE.

For different trial positions in a block, PEFs are different.

- We can optimize over the trial-wise PEFs and the power β such that the expected lower bound on the smooth min-entropy certified after N_b blocks is as large as possible.

$$\max_{\beta, F_j} \quad \frac{1}{\beta}\left[N_b \left\langle \sum_{j=1}^{L} \log(F_j) \right\rangle + \log(\varepsilon_{\mathrm{en}})\right]$$

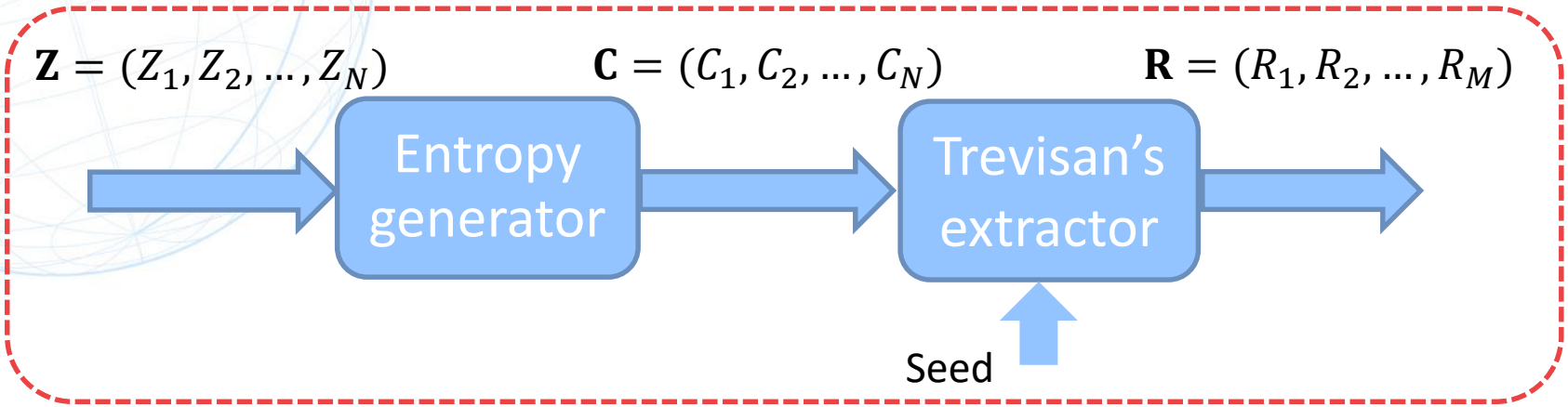
The power β should be optimized and fixed before analyzing the experiment.

The PEF for a trial needs only to be fixed before analyzing the trial.

For details, see our arXiv preprint 1912.11158.

Randomness extraction

(not implemented in our demonstration)



Randomness expansion if # of output bits > # of input bits (including the seed)

1. The amount of extractable random bits is determined by both the smooth min-entropy and the extractor used. For Trevisan's extractor, see arXiv:1212.0520 by W. Mauerer, C. Portmann, and V. B. Scholz.

2. Error is additive:
   If the smoothness error and extractor error are $\varepsilon_{\mathrm{en}}$ and $\varepsilon_{\mathrm{ext}}$, then the final, soundness error of the output bits is $\varepsilon_{\mathrm{en}} + \varepsilon_{\mathrm{ext}}$. The soundness error quantifies the statistical distance between the output bits and the uniformly random bits.

Overview of protocol implementation

- Protocol design and commissioning.

  --- fix the maximum block length (before our experiment)
  --- fix several other parameters involved in our protocol
  --- study how to update PEFs when performing finite-data analysis

  *We use the calibration data before our experiment and the commissioning data for these purposes. The commissioning data is chosen to be the first 7.4% of the recorded data --- the first 16 cycles.

- Analysis run using the remaining 150 cycles. Specifically, we have N_b =56,070,910 blocks for expansion analysis.

  --- perform data analysis using the parameters fixed in the first step
  --- output: success or failure

  *If the analysis succeeds, device-independent randomness expansion is successfully demonstrated (although we didn't actually extract the certified output bits).

Determination of block length

(before our experiment)

- Suppose that the quantum devices used are honest with the distribution $\nu(AB|XY)$ for each trial. The number of trials required for randomness expansion, $N_t(k)$, depends on the maximum block length 2^k.

- There is an optimal choice, $2^{k_{\mathrm{opt}}}$, for the maximum block length such that $N_t(k)$ is minimized.

- By numerical optimization, we observed that the optimal choice k_{opt} depends on the distribution $\nu(AB|XY)$, but not on the soundness error fixed for security analysis.

- To estimate the distribution $\nu(AB|XY)$ in our experiment, we run a standard loophole-free Bell test to obtain about 4.8×10^7 calibration trials.

We fixed the maximum block length to be 2^{17} in our experiment. Accordingly, each block consumes a total of 19 bits, while being estimated to produce on average 32.80 bits of randomness.

Parameter determination

1. Fix the soundness error ε.
2. Fix the smoothness error $\varepsilon_{\mathrm{en}}$ and the PEF power β.
3. Fix the success threshold t_{min}.
4. Determine # of seed bits required and # of random bits extracted.

Parameter determination

1. Fix the soundness error to be $\varepsilon = 5.7 \times 10^{-7}$ (5-sigma criterion).

2. Given ε and N_b, find the optimal values for $\varepsilon_{\mathrm{en}}$ and β such that the expected value of the net number of random bits is maximized.

   *The trial distribution $\nu(AB|XY)$ used in this step is estimated based on the calibration trials in the commissioning data.

3. Fix the threshold $t_{\min}$ such that the probability of success using honest devices with distribution $\nu(AB|XY)$ is at least 0.9938 (one-sided 2.5-sigma criterion).

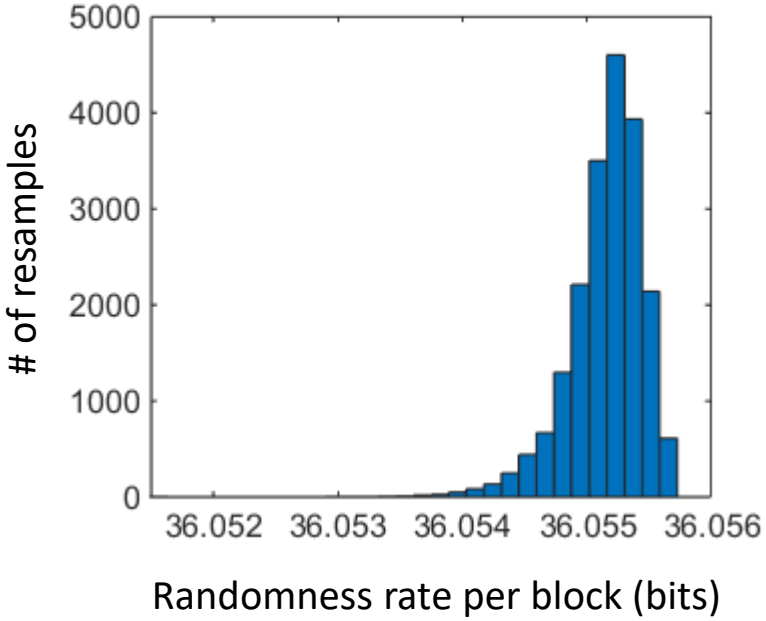
4. Determine # of seed bits required and # of random bits extracted by Trevisan's extractor.

Accordingly, when success we can generate 1,181,264,237 new random bits by consuming 1,065,347,290 random bits for spot checks and input choices as well as 3,725,074 seed bits for randomness extraction. So, we expect that the expansion ratio conditional on success is 1.105.

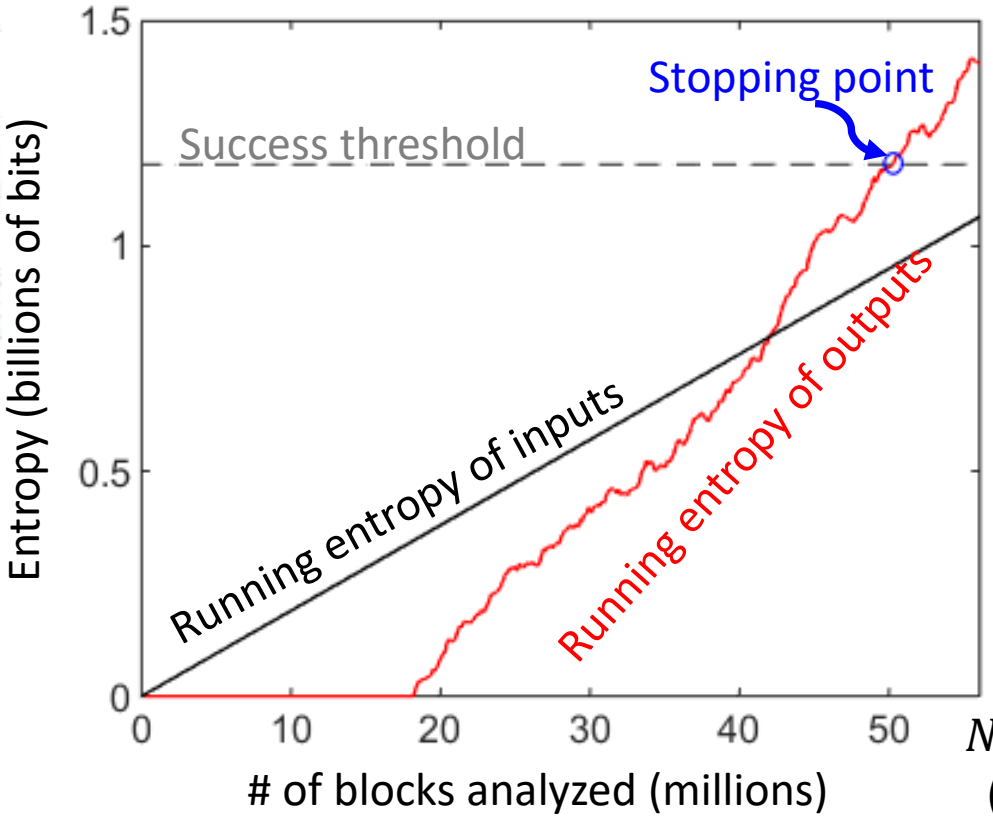
PEF updating

- Before analyzing the results of each cycle, we update the PEFs for each trial position in a block. We perform such updates because the commissioning data suggests that the trial distribution $\nu(AB|XY)$ drifts over cycles.

- The 2-min calibration trials ($\sim 3 \times 10^7$ trials) collected at the beginning of each cycle is sufficient for PEF updating.



Expansion result



$N_b = 56{,}070{,}910$ blocks
(~ 102 hours of data)

- Due to the adaptive construction of PEFs, we can stop early.
- At the stopping point (91 hours), expansion ratio is 1.24, higher than expected.
- The randomness rate is 3606 bits/second. The amount of randomness generated is more than that generated by NIST beacon in last 3 years.
- The latency for certifying any randomness is ~ 33 hours.

Related works

- Device-independent randomness expansion against quantum side information,
  Liu *et al*., arXiv:1912.11159 (see the talk by Wen-Zhao Liu).
  --- the usual spot-checking protocol
  --- 220 hours, 8202 bits/second
  --- soundness error is 3.09×10^{-12}, against quantum side information
  by entropy accumulation [R. Arnon-Friedman *et al*., Nat. commun. 9, 459 (2018); F. Dupuis and O. Fawzi, IEEE Trans. Inf. Theory 65, 7596 (2019)]

- Experimental realization of device-independent quantum randomness expansion,
  Li *et al*., arXiv:1902.07529.
  --- the usual spot-checking protocol
  --- 12.5 hours, 12156 bits/second
  --- soundness error is 4.6×10^{-10}, against quantum side information
  by quantum probability estimation [Y Z, H. Fu, and E. Knill, Phys. Rev. Research 2, 013016 (2020); see also arXiv:1806.04553]

  *The system detection efficiency is $\sim 81.8\%$, higher than ours ($\sim$76.3%).

Summary & Future work

- Devised a block-wise spot-checking protocol for expansion
- Demonstrated device-independent randomness expansion
- Improve our system detection efficiency

  ➡ randomness expansion with less experiment time +
  security analysis against quantum side information +
  running Trevisan's extractor with reasonable time cost

- Spot-checking without a trusted third party, cross-feeding for more efficient randomness expansion, security analysis considering the adversarial biases of input random bits …

Summary & Future work

- Devised a block-wise spot-checking protocol for expansion
- Demonstrated device-independent randomness expansion
- Improve our system detection efficiency

  ➡ randomness expansion with less experiment time +
  security analysis against quantum side information +
  running Trevisan's extractor with reasonable time cost

- Spot-checking without a trusted third party, cross-feeding for more efficient randomness expansion, security analysis considering the adversarial biases of input random bits …

Thank you!

yanbaoz@gmail.com