Certifying quantum randomness with low latency

Yanbao Zhang

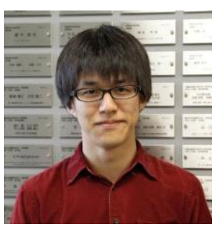
NTT Research Center for Theoretical Quantum Physics

NTT Basic Research Lab, Japan

Feb. 19, 2021

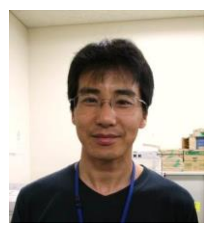
Experimental realization

Hsin-Pin Lo



Takuya Ikuta

Toshimori Honjo



Hiroki Takesue

Theoretical model, security analysis & randomness extraction

Alan Mink

William J. Munro

Outline of the talk

- Introduction to randomness
- Our scheme for quantum randomness generation
- Our method for certifying quantum randomness
- Experimental realization & results

Background: Why randomness is important?

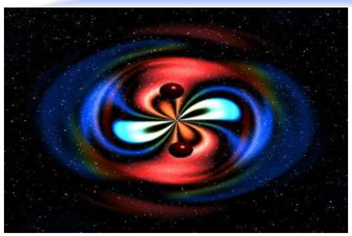
- Random numbers are generated through a process or device called the random number generator (RNG).

RNG → random numbers { unpredictable / uniformly distributed / private

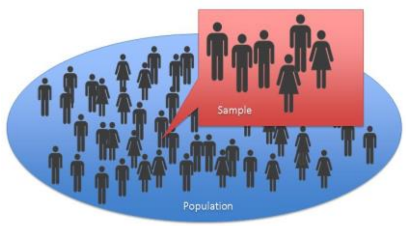
---

Huge amount of uniform randomness

High-quality, certified, private randomness



Simulation



Sampling

Gambling

Cryptography

Background: Why randomness is important?

NTT

- Random numbers are generated through a process or device called the random number generator (RNG).

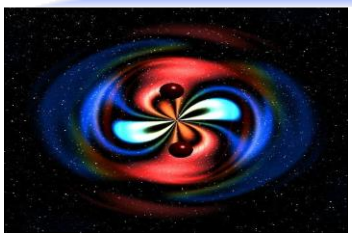
RNG → random numbers { unpredictable / uniformly distributed / private

E.g.

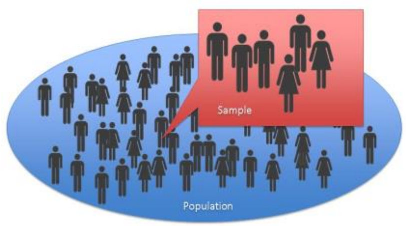
A classical random number generator

Huge amount of uniform randomness

High-quality, certified, private randomness



Simulation



Sampling

Gambling

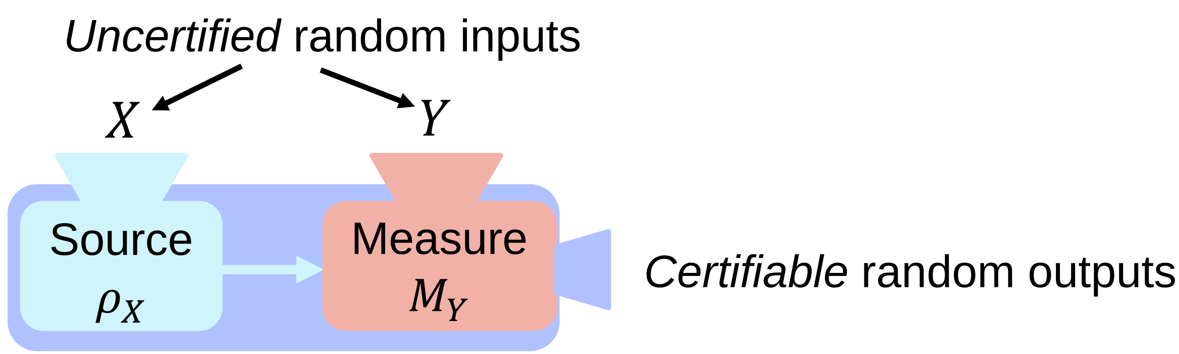
Cryptography

Classical process is deterministic → ***No perfect random numbers***

Quantum measure is probabilistic → ***Ideal random numbers as needed***

Background: Quantum random number generators

❖ Main idea: exploits the probabilistic nature of quantum measurements to generate genuine random numbers.

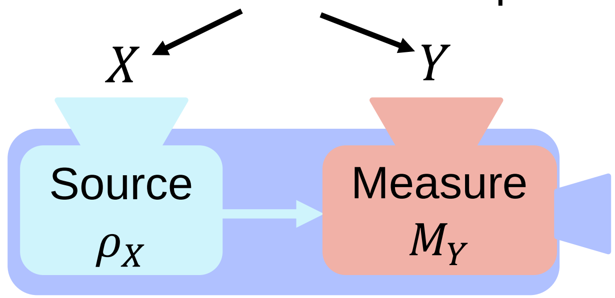


A general QRNG

Background: Quantum random number generators

❖ Main idea: exploits the probabilistic nature of quantum measurements to generate genuine random numbers.

Uncertified random inputs



Certifiable random outputs

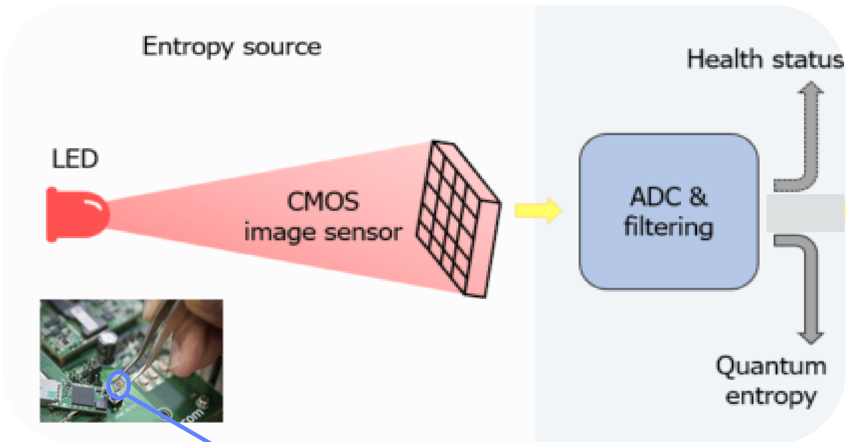
A general QRNG

Depending on the amount of characterization on the quantum devices:

- ➢ Device-dependent QRNG
- ➢ Semi-device-(in)dependent QRNG
- ➢ Device-independent QRNG

Background: Quantum random number generators

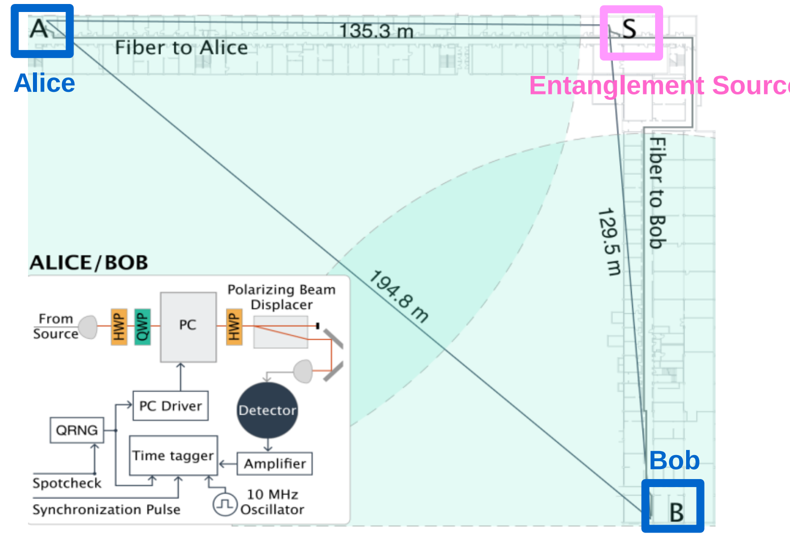
Device-dependent QRNG



QRNG chip @ ID Quantique

- ✓ simple --- a small device
- ✓ high performance --- randomness rate ~250 Kbps (embedded in a smartphone)
- × require **fully characterized** device --- impossible to achieve in practice, so **security is problematic**

Device-independent QRNG



Loophole-free Bell-test setup @ NIST-Boulder

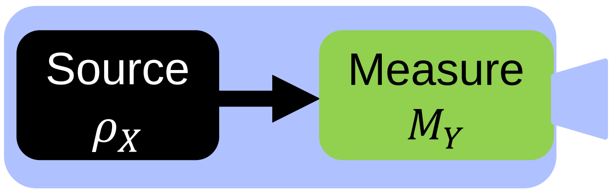
- ✓ high security --- no need to characterize the device
- × complicated --- a large-scale device
- × high latency (time consuming) --- a few minutes or hours delay before generating randomness
- × low performance --- randomness rate ~100 bps

Background: Semi-device-independent QRNG

- Semi-device-independent --- the device is partially characterized.
- Advantage --- can achieve a balance between **performance** and **security**.

Previous works

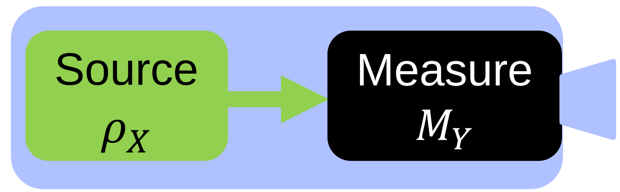
Source-independent QRNG



Uncharacterized *Characterized*

Cao *et al*., PRX 6, 011020 (2016)
Marangon *et al*., PRL118, 060503 (2017)

Measurement-device-independent QRNG



Characterized *Uncharacterized*

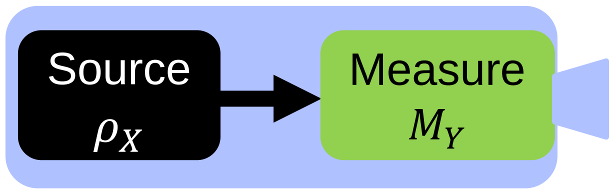
Chaturvedi *et al*., EPL 112, 30003 (2015)
Cao *et al*., NJP 17, 125011 (2015)

Background: Semi-device-independent QRNG

- Semi-device-independent --- the device is partially characterized.
- Advantage --- can achieve a balance between **performance** and **security**.

Previous works

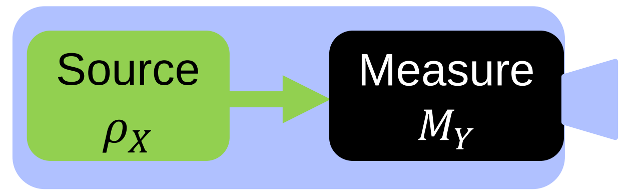
Source-independent QRNG



Uncharacterized *Characterized*

Cao *et al*., PRX 6, 011020 (2016)
Marangon *et al*., PRL118, 060503 (2017)

Measurement-device-independent QRNG



Characterized *Uncharacterized*

Chaturvedi *et al*., EPL 112, 30003 (2015)
Cao *et al*., NJP 17, 125011 (2015)

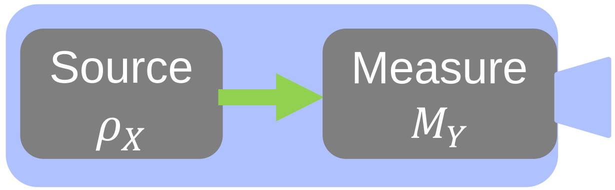
❖ Current problems: reliability and latency

Questions:

- ❑ Increase reliability: can we address imperfections in both source & measure?
- ❑ Reduce latency: can we achieve low-latency randomness generation?

Overview of our achievements

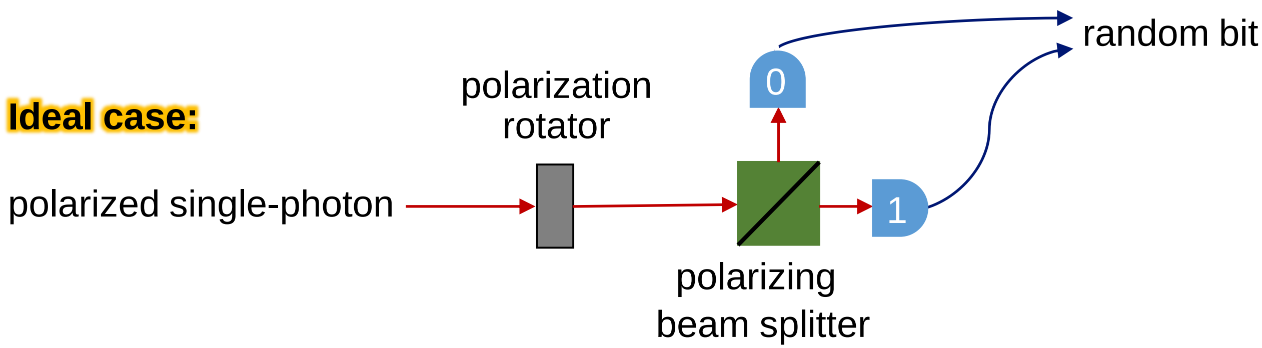
- Studied a new semi-device-independent QRNG scheme



Both Source and Measure *are* *partially characterized.*

An example

Ideal case:

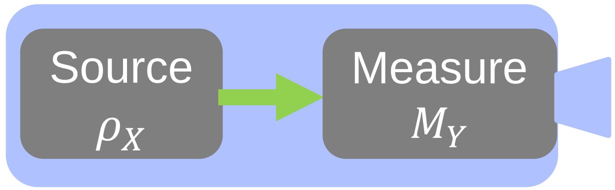


In practice,

- a single-photon source is not easily accessible.
- a particular quantum state is hard to prepare.
- a particular measurement is hard to perform.

Overview of our achievements

- Studied a new semi-device-independent QRNG scheme

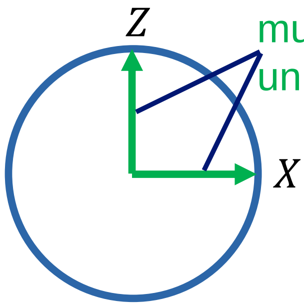


Both Source and Measure *are partially characterized.*

- Developed *efficient* methods for randomness certification in the above scenario

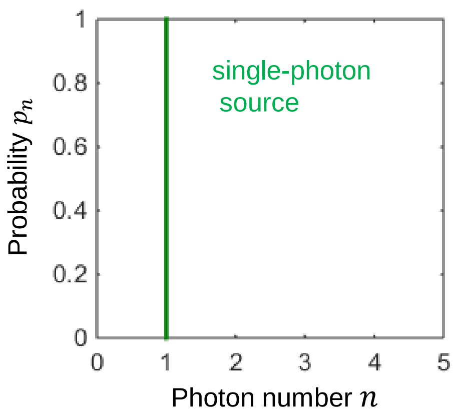
- *Realized* a simple low-latency real-time high-security QRNG

A simple QRNG scheme



Imbalance
$\tau = (P_X - P_Z)/2$
is exactly known

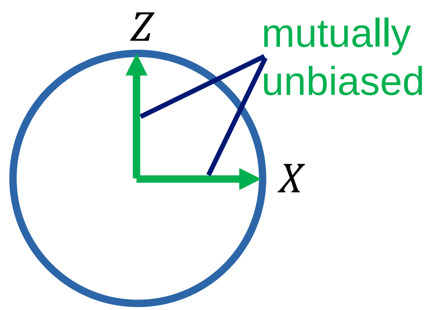
Ideal measure
in the single-photon space



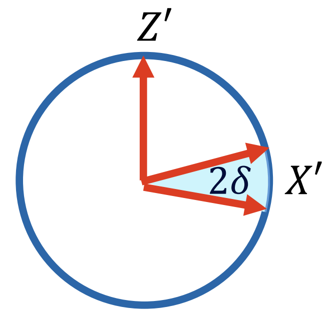
Ideal source

A simple QRNG scheme with imperfections

Imbalance
$\tau = (P_X - P_Z)/2$
is exactly known



Ideal measure
in the single-photon space

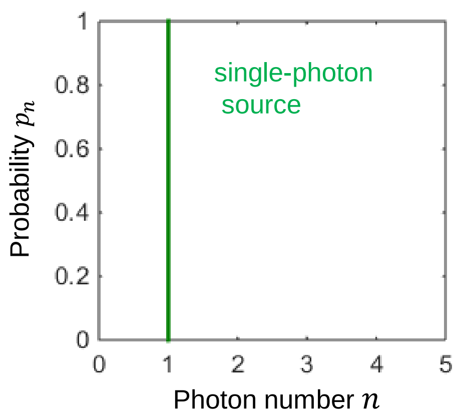


Practical measure
in the single-photon space

1) Misalignment angle
δ is bounded
such that $|\delta| \leq \Delta$!

2) Imbalance is bounded
$\tau_{\mathrm{lb}} \leq \tau \leq \tau_{\mathrm{ub}}$.

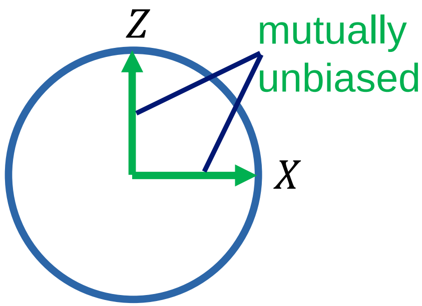
*Adversarial manipulations
are allowed.



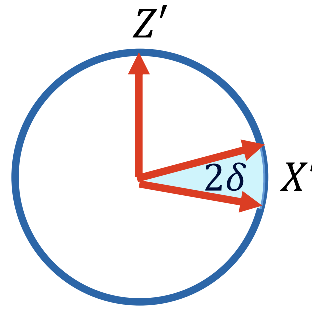
Ideal source

A simple QRNG scheme with imperfections

Imbalance
$\tau = (P_X - P_Z)/2$
is exactly known



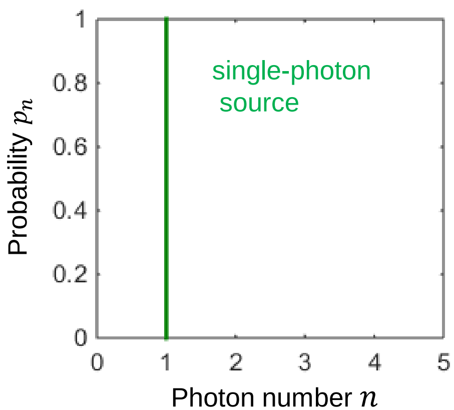
Ideal measure
in the single-photon space



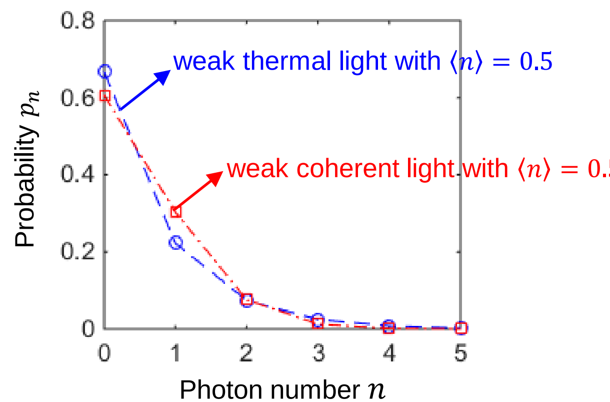
Practical measure
in the single-photon space

1) Misalignment angle δ is bounded such that $|\delta| \leq \Delta$!
2) Imbalance is bounded $\tau_{\rm lb} \leq \tau \leq \tau_{\rm ub}$.

*Adversarial manipulations are allowed.



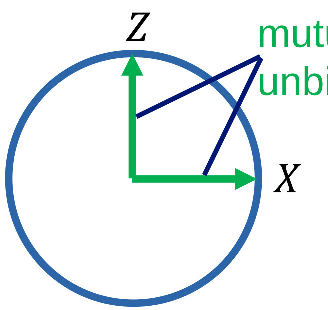
Ideal source



Practical
source

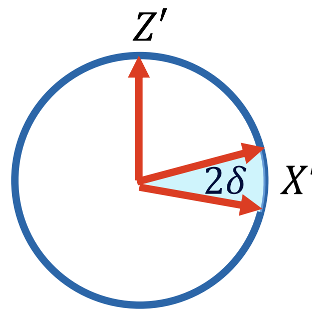
A simple QRNG scheme with imperfections

Imbalance
$\tau = (P_X - P_Z)/2$
is exactly known



mutually
unbiased

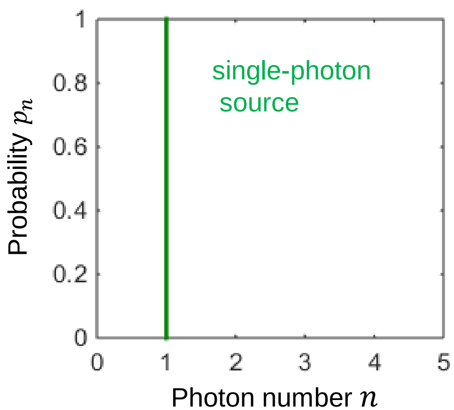
Ideal measure
in the single-photon space



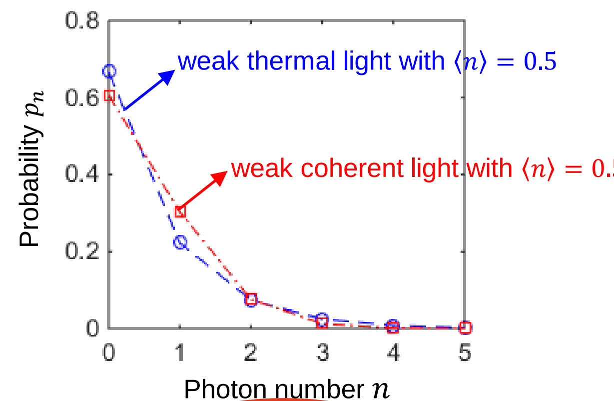
1) Misalignment angle δ is bounded such that $|\delta| \leq \Delta$!
2) Imbalance is bounded $\tau_{\mathrm{lb}} \leq \tau \leq \tau_{\mathrm{ub}}$.

*Adversarial manipulations are allowed.

Practical measure
in the single-photon space



Ideal source



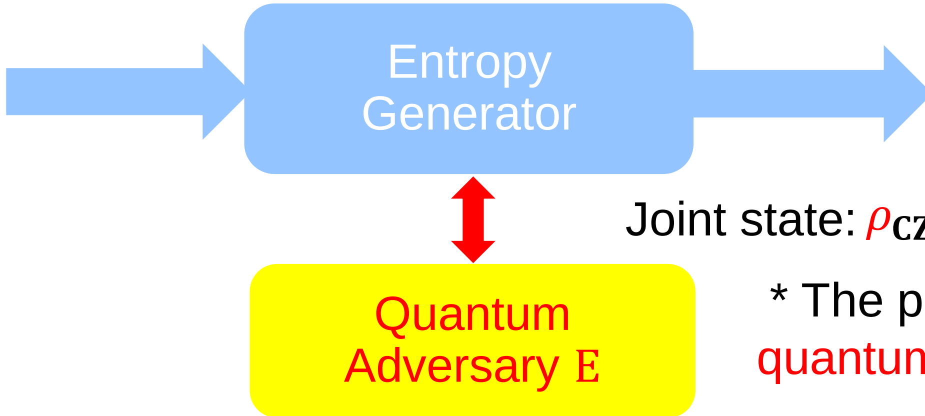
Practical source

1) Photon-number dist. is bounded such that $p_{n=1} \geq p_{1,\mathrm{lb}}$ or $p_{n=1}/p_{n\geq 1} \geq p_{1,\mathrm{lb}}$.
2) Measurements are block-diagonal $\boldsymbol{M} = \boldsymbol{M}_{n=1} \oplus \boldsymbol{M}_{n\neq 1}$.

Our method: Quantification of randomness

NTT

$\mathbf{Z} = (Z_1, Z_2, \ldots, Z_N)$



$\mathbf{C} = (C_1, C_2, \ldots, C_N)$

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

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

- Guessing probability: $P_{\mathrm{guess}}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho}$
- Easily accessible measure of uniform randomness:

$$H_{\min}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho} = -\log_2[P_{\mathrm{guess}}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho}]$$

- Flexible measure of uniform randomness:

$$H_{\min}^{\varepsilon}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho} = \sup_{\rho'}\{H_{\min}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho'}, P(\rho, \rho') \leq \varepsilon\}$$

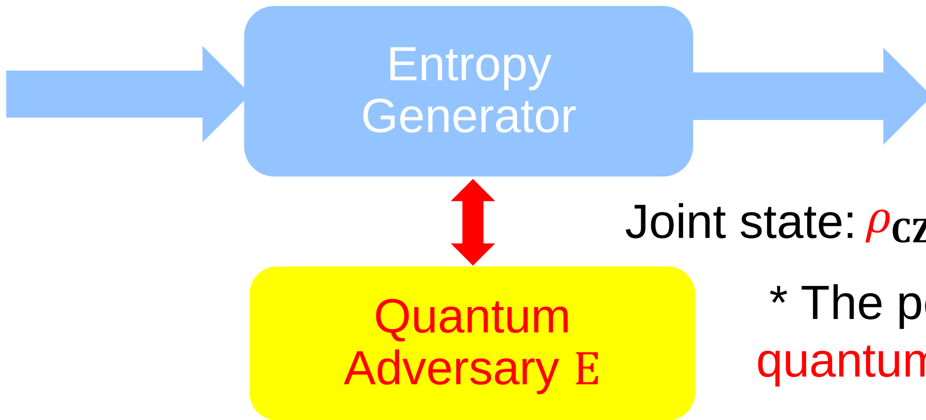
R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory 55, 4337 (2009)

M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory 56, 4674 (2010)

Our method: Quantification of randomness

NTT

$\mathbf{Z} = (Z_1, Z_2, \dots, Z_N)$



$\mathbf{C} = (C_1, C_2, \dots, C_N)$

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

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

- Guessing probability: $P_{\mathrm{guess}}(\mathbf{C}|\mathbf{Z}\mathrm{E})_\rho$
- Easily accessible measure of uniform randomness:

$$H_{\min}(\mathbf{C}|\mathbf{Z}\mathrm{E})_\rho = -\log_2[P_{\mathrm{guess}}(\mathbf{C}|\mathbf{Z}\mathrm{E})_\rho]$$

- Flexible measure of uniform randomness:

$$H_{\min}^{\varepsilon}(\mathbf{C}|\mathbf{Z}\mathrm{E})_\rho = \sup_{\rho'}\{H_{\min}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho'}, P(\rho, \rho') \le \varepsilon\}$$

Goal: Lower-bound smooth conditional min-entropy $H_{\min}^{\varepsilon}(\mathbf{C}|\mathbf{Z}\mathrm{E})$

Our method: Quantification of randomness

(in the presence of classical side information)

$\mathbf{Z} = (Z_1, Z_2, \dots, Z_N)$ → Entropy Generator → $\mathbf{C} = (C_1, C_2, \dots, C_N)$

Entropy Generator ↕ Classical Adversary E

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

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

- Guessing probability: $P_{\mathrm{guess}}(\mathbf{C}|\mathbf{Z}\mathrm{E})_\mu$
- Easily accessible measure of uniform randomness:

$$H_{\min}(\mathbf{C}|\mathbf{Z}\mathrm{E})_\mu = -\log_2[P_{\mathrm{guess}}(\mathbf{C}|\mathbf{Z}\mathrm{E})_\mu]$$

- Flexible measure of uniform randomness:

$$H_{\min}^{\varepsilon}(\mathbf{C}|\mathbf{Z}\mathrm{E})_\mu = \sup_{\mu'}\{H_{\min}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\mu'}, TV(\mu, \mu') \leq \varepsilon\}$$

Goal: Lower-bound smooth conditional min-entropy $H_{\min}^{\varepsilon}(\mathbf{C}|\mathbf{Z}\mathrm{E})$

Our method: Concepts involved

(in the *general* approach of quantum probability estimation)

- Quantum model $\mathcal{Q}(\mathbf{CZ})$ --- the set of all possible joint states $\rho_{\mathbf{CZE}}$ at the end of the experiment.
- Quantum estimation factor (QEF) --- a function $F_{\mathrm{q}}(\mathbf{CZ})$ satisfying a set of constraints imposed by each possible $\rho_{\mathbf{CZE}} \in \mathcal{Q}(\mathbf{CZ})$.

Y. Z., H. Fu, and E. Knill, Phys. Rev. Research 2, 013016 (2020)

Y. Z., L. K. Shalm *et al*., Phys. Rev. Lett. 124, 010505 (2020)

Our method: Concepts involved

(in the *general* approach of quantum probability estimation)

- Quantum model $\mathcal{Q}(\mathbf{CZ})$ --- the set of all possible joint states $\rho_{\mathbf{CZ}\mathrm{E}}$ at the end of the experiment.

- Quantum estimation factor (QEF) --- a function $F_{\mathrm{q}}(\mathbf{CZ})$ satisfying a set of constraints imposed by each possible $\rho_{\mathbf{CZ}\mathrm{E}} \in \mathcal{Q}(\mathbf{CZ})$.

Under the quantum Markov-chain conditions (natural for time-ordered trials)

$$\mathbf{C}_{<i} \leftrightarrow (\mathbf{Z}_{<i}, \mathrm{E}) \leftrightarrow Z_i, \forall\, i,$$ [IID assumption is not required]

we need only to construct

- Model $\mathcal{Q}(CZ)$ --- the set of all possible joint states $\rho_{CZ\mathrm{E}}$ at the end of a trial.

- Corresponding QEF --- a function $F_{\mathrm{q}}(CZ)$ satisfying a set of constraints imposed by each possible $\rho_{CZ\mathrm{E}} \in \mathcal{Q}(CZ)$.

Y. Z., H. Fu, and E. Knill, Phys. Rev. Research 2, 013016 (2020)

Y. Z., L. K. Shalm *et al*., Phys. Rev. Lett. 124, 010505 (2020)

Our method: Concepts involved

(in the *general* approach of probability estimation)

- Classical model $\boldsymbol{\mathcal{C}}(\mathbf{CZ})$ --- the set of all possible joint states $\mu_{\mathbf{CZ}\mathrm{E}}$ at the end of the experiment.
- Probability estimation factor (PEF) --- a function $F_{\mathrm{c}}(\mathbf{CZ})$ satisfying a set of constraints imposed by each possible $\mu_{\mathbf{CZ}\mathrm{E}} \in \boldsymbol{\mathcal{C}}(\mathbf{CZ})$.

Under the Markov-chain conditions (natural for time-ordered trials)

$$\mathbf{C}_{<i} \leftrightarrow (\mathbf{Z}_{<i}, \mathrm{E}) \leftrightarrow Z_i, \forall\, i,$$ [IID assumption is not required]

we need only to construct

- Model $\boldsymbol{\mathcal{C}}(CZ)$ --- the set of all possible joint states $\mu_{CZ\mathrm{E}}$ at the end of a trial.
- Corresponding PEF --- a function $F_{\mathrm{c}}(CZ)$ satisfying a set of constraints imposed by each possible $\mu_{CZ\mathrm{E}} \in \boldsymbol{\mathcal{C}}(CZ)$.

Y. Z., E. Knill, and P. Bierhorst, Phys. Rev. A 98, 040304(R) (2018)

E. Knill, Y. Z., and P. Bierhorst, Phys. Rev. Research 2, 033465 (2020)

Our method: Main theorem

(of quantum probability estimation)

- Quantum model $\mathcal{Q}_i\ (C_iZ_i)$ and QEF $F_{\mathrm{q},i}(C_iZ_i) \geq 0$ with power $\beta_{\mathrm{q}} > 0$ for each trial i.

QEF Def. $\forall \rho_{C_iZ_i\mathrm{E}} \in \mathcal{Q}_i\ (C_iZ_i), \left\langle F_{\mathrm{q},i}(C_iZ_i)\hat{R}_{1+\beta_{\mathrm{q}}}(\rho_{\mathrm{E}}(C_iZ_i)|\rho_{\mathrm{E}}(Z_i))\right\rangle \leq 1.$

* Models and QEFs for different trials can be different.

* $\hat{R}_{1+\beta_{\mathrm{q}}}(\rho_{\mathrm{E}}(C_iZ_i)|\rho_{\mathrm{E}}(Z_i))$ is the sandwiched Rényi power of order $(1+\beta_{\mathrm{q}})$.

Our method: Main theorem

(of quantum probability estimation)

- Quantum model $\mathcal{Q}_i\ (C_iZ_i)$ and QEF $F_{\mathrm{q},i}(C_iZ_i) \geq 0$ with power $\beta_{\mathrm{q}} > 0$ for each trial i.

QEF Def. $\forall \rho_{C_iZ_i\mathrm{E}} \in \mathcal{Q}_i\ (C_iZ_i), \left\langle F_{\mathrm{q},i}(C_iZ_i)\hat{R}_{1+\beta_{\mathrm{q}}}(\rho_{\mathrm{E}}(C_iZ_i)|\rho_{\mathrm{E}}(Z_i))\right\rangle \leq 1.$

* Models and QEFs for different trials can be different.

* $\hat{R}_{1+\beta_{\mathrm{q}}}(\rho_{\mathrm{E}}(C_iZ_i)|\rho_{\mathrm{E}}(Z_i))$ is the sandwiched Rényi power of order $(1+\beta_{\mathrm{q}})$.

- The success event $\Phi \triangleq \left\{\mathbf{cz}: \prod_{i=1}^{N} F_{\mathrm{q},i}(c_iz_i) \geq t_{\min}\right\}$.

- κ --- a desired lower bound of the success probability.

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

$$H_{\min}^{\varepsilon}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\rho_{\mathbf{CZE}|\Phi}} \geq \frac{1}{\beta_{\mathrm{q}}}\log(t_{\min}) + \frac{1}{\beta_{\mathrm{q}}}\log\left(\frac{\varepsilon^2}{2}\right) + \frac{1+\beta_{\mathrm{q}}}{\beta_{\mathrm{q}}}\log(\kappa).$$

Our method: Main theorem

(of probability estimation)

- Classical model $\mathcal{C}_i\ (C_iZ_i)$ and PEF $F_{\mathrm{c},i}(C_iZ_i) \geq 0$ with power $\beta_\mathrm{c} > 0$ for each trial i.

  PEF Def. $\forall \mu_{C_iZ_i\mathrm{E}} \in \mathcal{C}_i\ (C_iZ_i),\ \left\langle F_{\mathrm{c},i}(C_iZ_i)[\mu_\mathrm{E}(C_i|Z_i)]^{\beta_\mathrm{c}} \right\rangle \leq 1.$

  * Models and PEFs for different trials can be different.

- The success event $\Phi \triangleq \left\{\mathbf{cz}\colon \prod_{i=1}^{N} F_{\mathrm{c},i}(c_iz_i) \geq t_{\min}\right\}$.

- κ --- a desired lower bound of the success probability.

Theorem: For each possible state $\mu_{\mathbf{CZ}\mathrm{E}}$, *either* the success probability satisfies

$$\mathrm{Prob}_{\mu_{\mathbf{CZ}\mathrm{E}}}(\Phi) \leq \kappa,$$

or conditional on success

$$H_{\min}^{\varepsilon}(\mathbf{C}|\mathbf{Z}\mathrm{E})_{\mu_{\mathbf{CZ}\mathrm{E}|\Phi}} \geq \frac{1}{\beta_\mathrm{c}}\log(t_{\min}) + \frac{1}{\beta_\mathrm{c}}\log(\varepsilon) + \frac{1+\beta_\mathrm{c}}{\beta_\mathrm{c}}\log(\kappa).$$

Our method: for the scenario considered

Measurements considered :

$M_X = \begin{pmatrix} M_{X,\,n=1} & 0 \\ 0 & M_{X,\,n\neq 1} \end{pmatrix}$, $M_z = \begin{pmatrix} M_{z,\,n=1} & 0 \\ 0 & M_{z,\,n\neq 1} \end{pmatrix}$,

1. $M_{X,\,n\neq 1}$ and $M_{z,\,n\neq 1}$ are arbitrary
2. $M_{X,\,n=1}$ and $M_{z,\,n=1}$ are qubit measurements with $|\delta| \leq \Delta$.
3. M_X and M_Z are randomly selected with bounded probabilities.

States considered : $\rho = \begin{pmatrix} \rho_{n=1} & 0 \\ 0 & \rho_{n\neq 1} \end{pmatrix}$, where $\mathrm{Tr}(\rho_{n=1}) \geq p_{1,\mathrm{lb}}$.

Physical model

Our method: for the scenario considered

Measurements considered:

$$M_X = \begin{pmatrix} M_{X,n=1} & 0 \\ 0 & M_{X,n\neq1} \end{pmatrix}, \quad M_Z = \begin{pmatrix} M_{Z,n=1} & 0 \\ 0 & M_{Z,n\neq1} \end{pmatrix},$$

1. $M_{X,n\neq1}$ and $M_{Z,n\neq1}$ are arbitrary
2. $M_{X,n=1}$ and $M_{Z,n=1}$ are qubit measurements with $|\delta| \leq \Delta$.
3. M_X and M_Z are randomly selected with bounded probabilities.

States considered: $\rho = \begin{pmatrix} \rho_{n=1} & 0 \\ 0 & \rho_{n\neq1} \end{pmatrix}$, where $\mathrm{Tr}(\rho_{n=1}) \geq p_{1,\mathrm{lb}}$.

Physical model

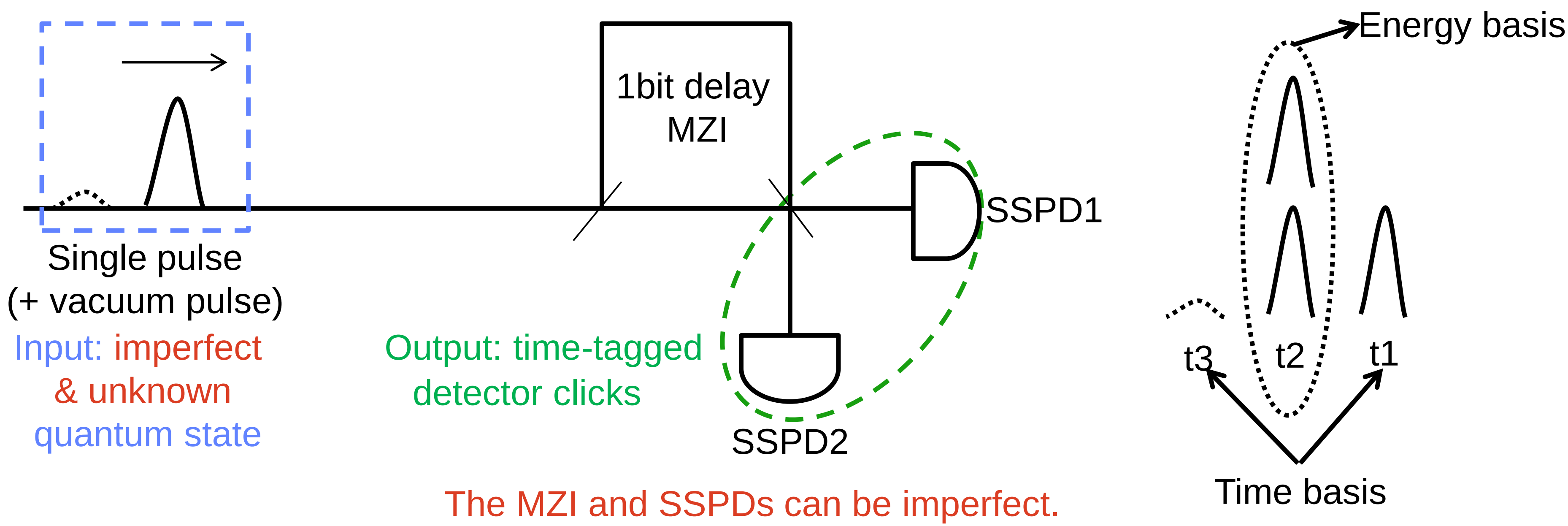
Quantum model $\mathcal{Q}$
& classical model $\mathcal{C}$

Convex polytope $\mathcal{P}_{\mathrm{Q}} \supseteq \mathcal{Q}$
& convex polytope $\mathcal{P}_{\mathrm{C}} \supseteq \mathcal{C}$

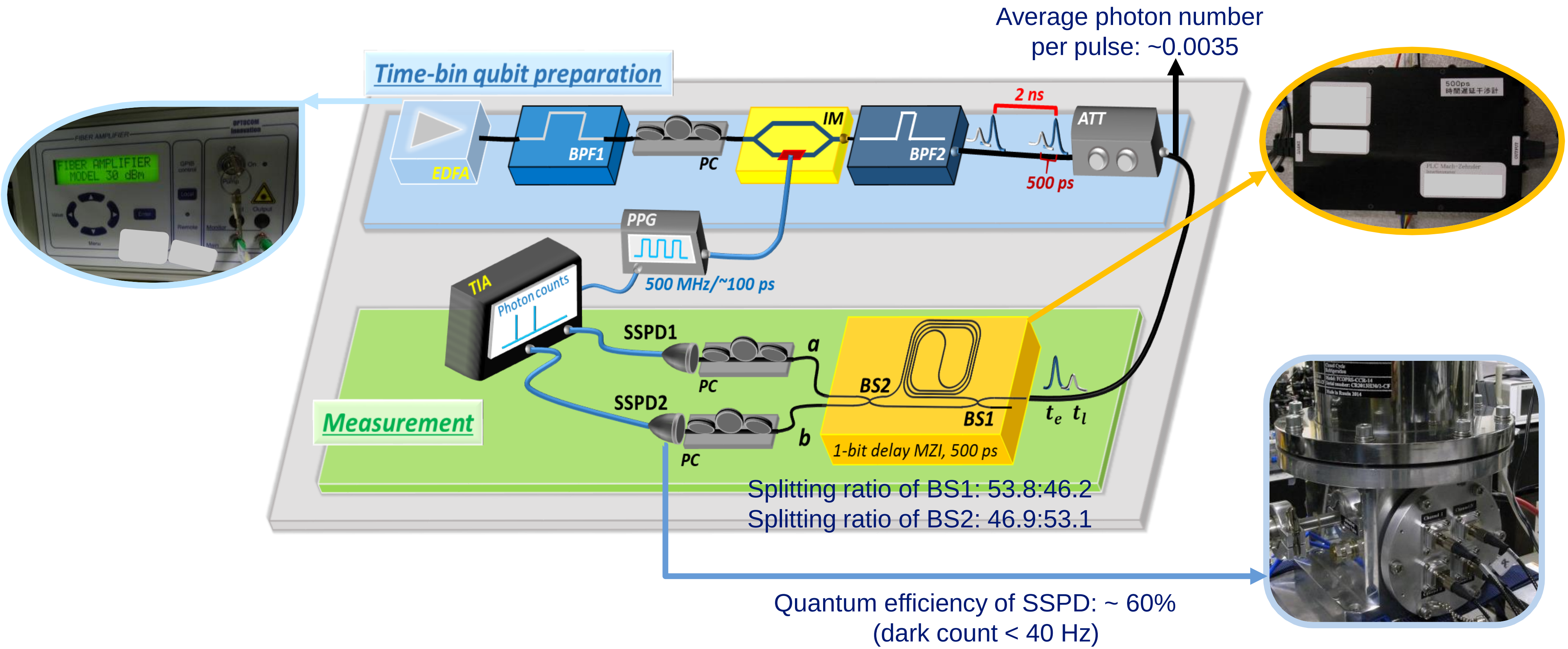
Construct the best QEF and PEF
by convex optimization

Our QRNG: Experimental realization

- A laser pulse is inputted into a Mach–Zehnder interferometer (MZI), and outputs are detected by two superconducting single-photon detectors (SSPDs).
- Two orthogonal measurement bases: energy basis & time basis.
  1. Energy basis: random (0: click at SSPD1, or 1: click at SSPD2)
  2. Time basis: t1 (almost) t3 (rare event)
- Advantage --- easily integrated onto a chip.
- Our QRNG is semi-device-independent --- **allows imperfections in both source & measure**.



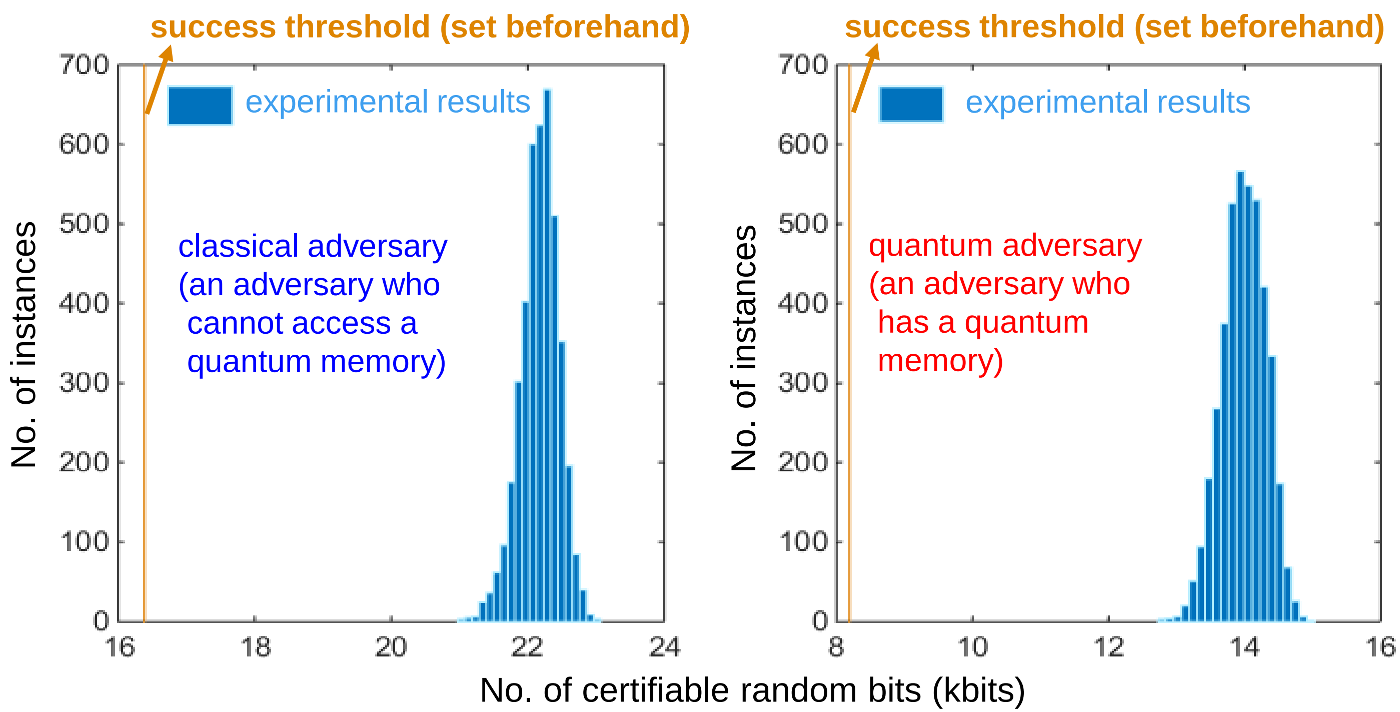
Our QRNG: Experimental realization



Our QRNG allows:

- Imperfect source --- weak optical pulse *rather than* single-photon source.
- Imperfect basis choice --- a basis is selected with an inexact probability.
- Imperfect measure --- measurements are misaligned.

Result 1: Low-latency real-time high-security QRNG



- Each instance generates 8192 (or 2×8192) random bits against quantum (or classical) adversary with insecurity $2^{-64} \approx 5.4 \times 10^{-20}$ ➔ high security.

  Insecurity --- Adversary's ability to distinguish the generated random bits (real case) from the perfectly random bits (ideal case).

- Each instance takes 0.1 s runtime (which includes the latency 0.047 s) + 0.02 s (or 0.04 s) extraction time ➔ real time & low latency.

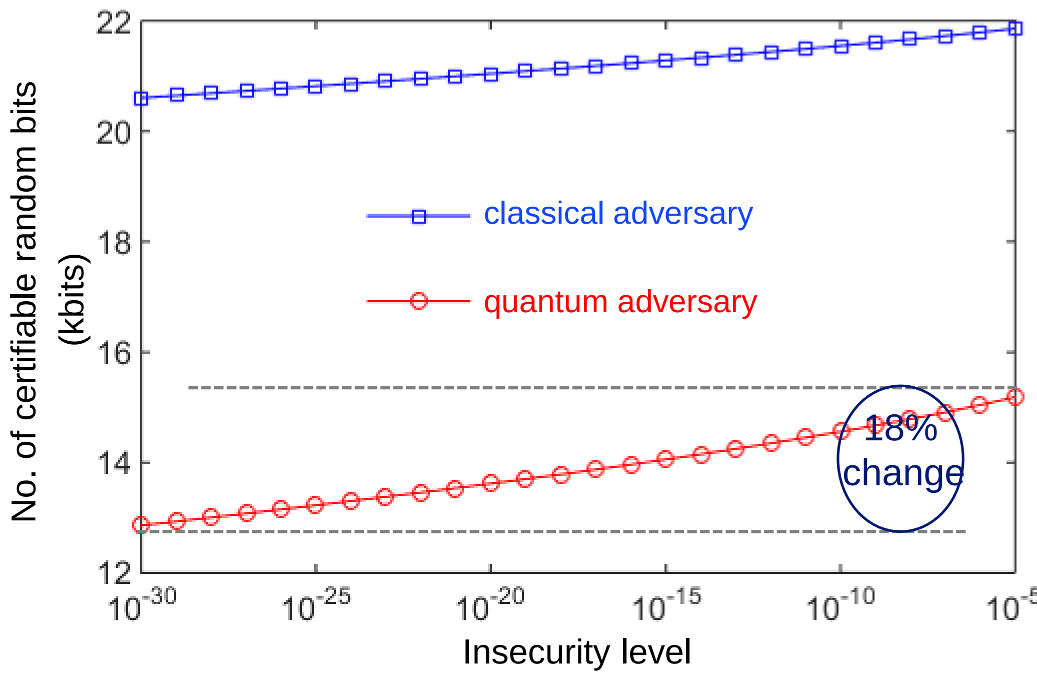
Result 2: Trade-off between quantity & quality

NTT

- Depending on the specific application, we choose the insecurity level beforehand. E.g.,

  Simulation requires low security --- recommended insecurity level 10^{-5}.

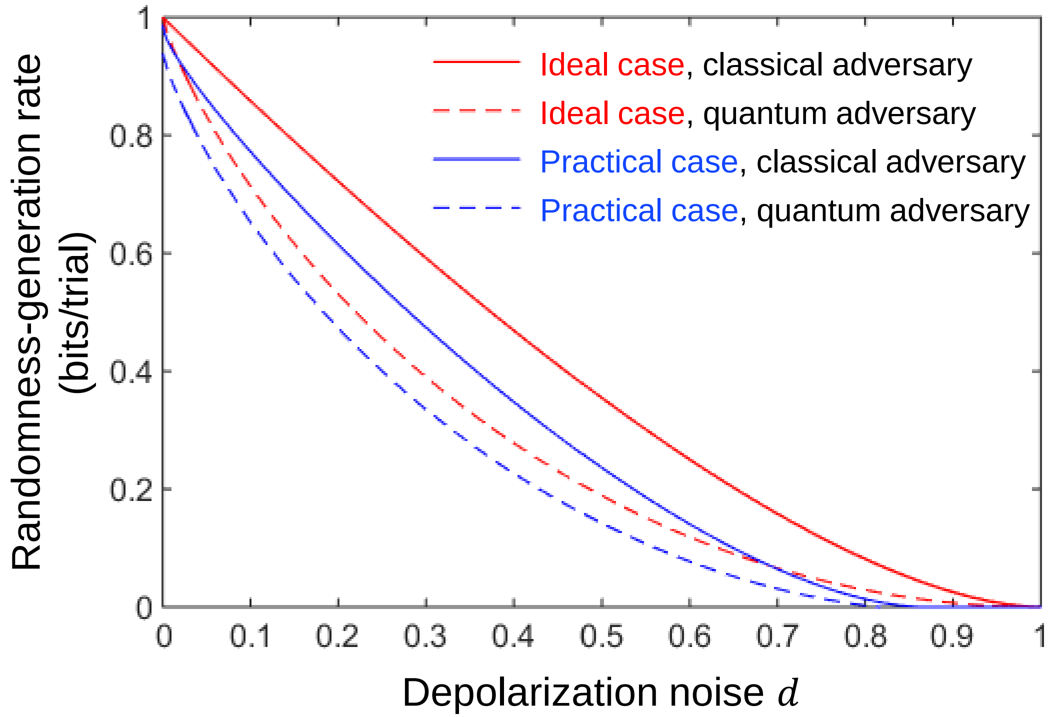
  Cryptography requires high security --- recommended insecurity level 10^{-20}.



Our method is efficient
➔ the amount of certifiable randomness doesn't change much with the insecurity level.

Expected number of random bits certifiable from the measurement outcomes observed in every 0.1 s runtime.

Result 3: Classical vs Quantum adversary



Simulation:
Binary-outcome measurements such that $\langle M_1 \rangle$=0 and $\langle M_2 \rangle$=1 − d.

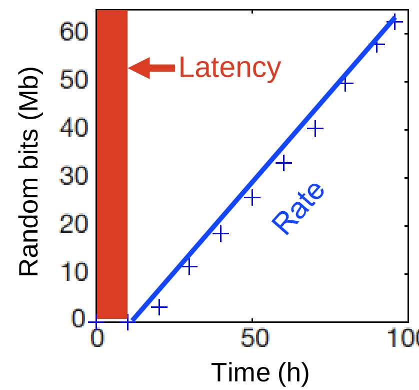
Ideal case: 1-qubit + two mutually unbiased measurements
Practical case: 95% 1-qubit + two misaligned measurements (misalignment angle is 5°)

Clear demonstration of the reduction of the rate w.r.t. quantum adversaries as compared to that w.r.t. classical adversaries.

Comparison with other start-of-art works

	QRNG Type	Latency	Rate (over a long run)	Insecurity
ID Quantique PRX, 2014 arXiv:2011.14129	device dependent	*unreported*	4.90 Mbps** (the best QRNG chip)	*uncertified*
USTC Nature, 2018	device independent	13 hours	181 bps	10^{-5} quantum adversary
NIST PRL, 2020	device independent	5 min	55 bps	5.4×10^{-20} quantum adversary
Tsinghua Uvi. PRX 2016	semi device independent	*unreported*	5 Kbps	1.8×10^{-15} quantum adversary
Our work	semi device independent	47 ms	153 Kbps	5.4×10^{-20} quantum adversary

Fig. 3 of USTC, Nature 2018



* Latency and Rate are two *different* measures of QRNG performance.

* Previous works focus on the study of the rate of a QRNG; however, the latency is more relevant for practical applications.

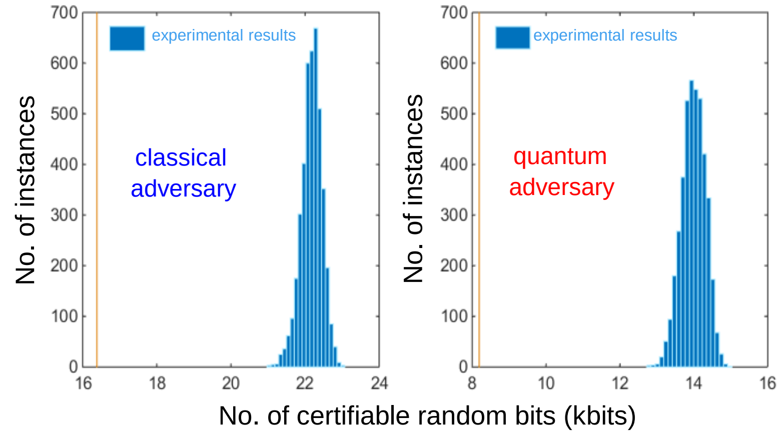
** The rate 250 Kbps in the video presentation is the typical entropy rate of the smallest QRNG chip embedded in a smartphone.

Significance of this work and future developments

NTT

Summary

- Simple & reliable QRNG scheme even with imperfections in both source and measure.
- New & efficient method for randomness certification, which is extendable to QKD.
- Low-latency real-time high-security QRNG.
- Advantage of quantum adversary.



Outlook

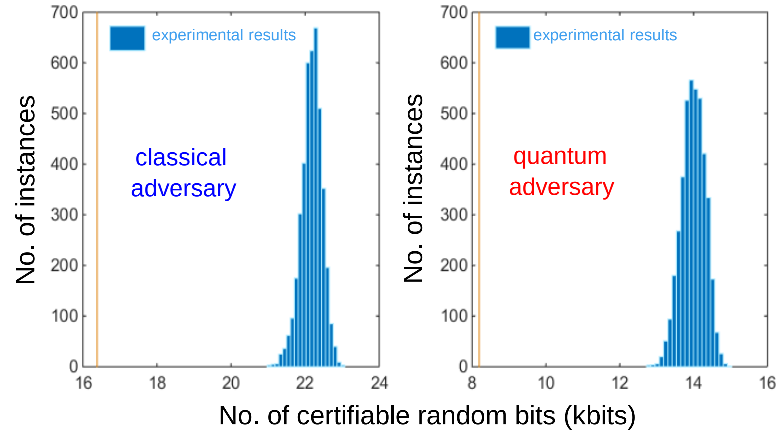
- Reduce the size of our QRNG ➔ Integration into mobile phones.
- Build a continuously-operating, high-security and high-speed quantum randomness beacon [ongoing efforts at NIST@USA and USTC@China].

Significance of this work and future developments

NTT

Summary

- Simple & reliable QRNG scheme even with imperfections in both source and measure.
- New & efficient method for randomness certification, which is extendable to QKD.
- Low-latency real-time high-security QRNG.
- Advantage of quantum adversary.



Outlook

- Reduce the size of our QRNG ➔ Integration into mobile phones.
- Build a continuously-operating, high-security and high-speed quantum randomness beacon [ongoing efforts at NIST@USA and USTC@China].

Thank you for your attention!