A Simple Low-latency Real-time Certifiable Quantum Random Number Generator

Yanbao Zhang[1,2], Hsin-Pin Lo[1], Alan Mink[3], Takuya Ikuta[1], Toshimori Honjo[1], Hiroki Takesue[1], and William J. Munro[1,2]

[1]NTT Basic Research Laboratories, NTT Corporation, Atsugi, Kanagawa 243-0198, Japan

[2]NTT Research Center for Theoretical Quantum Physics, NTT Corporation, Atsugi, Kanagawa 243-0198, Japan

[3]National Institute of Standards and Technology, Gaithersburg, Maryland 20899, USA

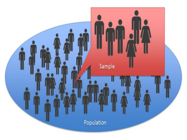
Main Messages

- Quantum mechanics allows to generate and certify genuine randomness.
- Most demonstrations focus on high asymptotic generation rates, resulting in high latency between the initial request and the delivery of the requested random bits.
- We develop methods to efficiently certify randomness taking into account adversarial imperfections in both the state preparation and the measurement apparatus. ➔ no need of the IID assumption & semi-device-independent randomness generation.
- We demonstrate low-latency real-time certifiable quantum randomness generation from measurements on photonic time-bin states.
- Every tenth of a second, we can certify enough entropy with respect to quantum (or classical) adversaries in order to generate a block of 8192 (or 2×8192) random bits with a certified error bounded by 2^{-64} and with an extraction time of 0.02 s (or 0.04 s).
- We quantify the advantage of quantum adversaries vs classical adversaries.

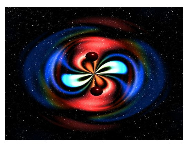
* For details, see Y. Z., H. P. Lo *et al.*, Nat. Commun. 12, 1056 (2021).

Why Is Randomness Important?

Gambling



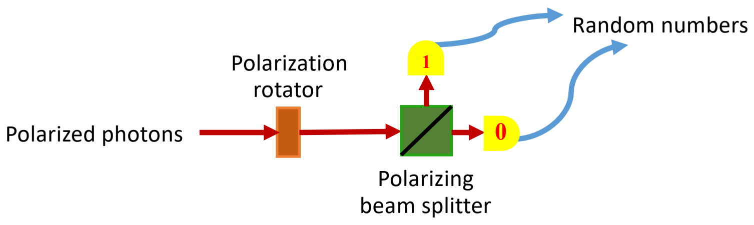
Sampling



Simulation

Cryptography

Device-dependent Quantum Random Number Generator



The generated random numbers are uniformly distributed and unpredictable, *if*

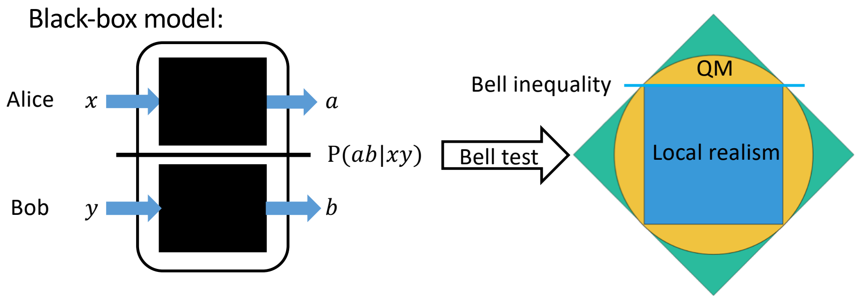
- a particular quantum state, for example $|H\rangle$, is prepared;
- a particular measurement, for example $\{|D\rangle\langle D|, |A\rangle\langle A|\}$, is performed.

Pros: simple and fast generation of quantum random numbers.

Cons: fragile. The security of generated random numbers is easily affected by practical issues (for example, multiphoton events and measurement imprecision).

Device-independent Quantum Random Number Generator

Black-box model:



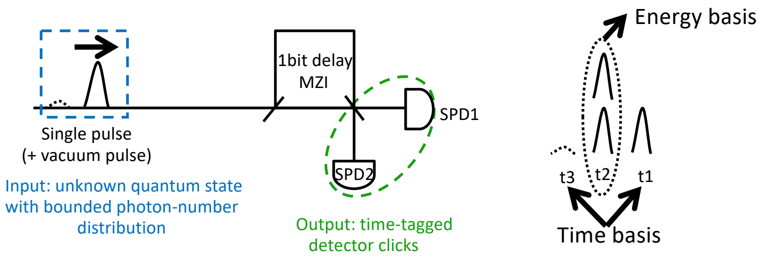
Idea behind randomness generation:
If the distribution $\{\mathrm{P}(ab|xy)\}$ violates local realism, the output ab cannot be a deterministic function of the input xy and any other side information.

Pros: robust and high practical security. Random numbers are certifiable *even if* the inner working of quantum devices is not reliable.

Cons: complicate and low performance. The scheme is difficult to realize and the generation rate is pretty low (~100 bits/second).

A Simple QRNG with Time-bin Measurements

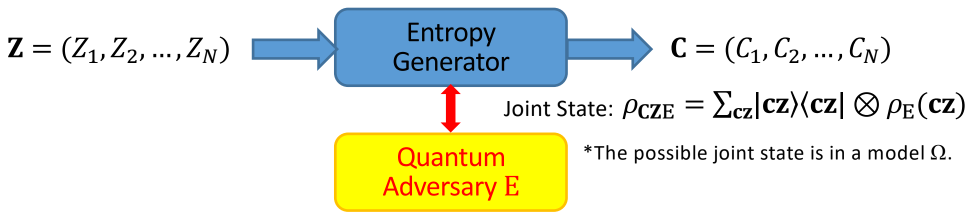
- ➢ An optical pulse in the early time bin is inputted into a MZI, and outputs are detected by two SPDs.
- ➢ Two orthogonal measurement bases: energy-basis and time-basis.
  1. Energy-basis: random (0: click at SPD1, or 1: click at SPD2)
  2. Time-basis: t1 (almost) t3 (rare event)


1bit delay MZI
SPD1
SPD2
Single pulse
(+ vacuum pulse)
Input: unknown quantum state with bounded photon-number distribution
Output: time-tagged detector clicks
Energy basis
t3
t2
t1
Time basis

Practical issues to be addressed:
- Imperfect source
- Imperfect basis choice
- Imperfect measurements

We develop a method to certify quantum randomness in the presence of these practical issues.

Randomness Analysis Theory


$\mathbf{Z} = (Z_1, Z_2, \ldots, Z_N)$
Entropy Generator
$\mathbf{C} = (C_1, C_2, \ldots, C_N)$
Joint State: $\rho_{\mathbf{CZE}} = \sum_{\mathbf{cz}} |\mathbf{cz}\rangle\langle\mathbf{cz}| \otimes \rho_{\mathrm{E}}(\mathbf{cz})$
Quantum Adversary E

*The possible joint state is in a model Ω.

Our goal: Estimate smooth min-entropy $H^{\varepsilon}_{\min}(\mathbf{C}|\mathbf{Z}\mathrm{E};\Phi)$ conditional on $\mathbf{Z}\mathrm{E}$ and success event Φ

Step 1: Construct the "model" Ω of the experiment in the presence of practical issues.

Step 2: Construct non-negative quantum probability estimation factors (QEFs) $F(\mathbf{CZ})$ satisfying that

$$\forall \rho_{\mathbf{CZE}} \in \Omega, \textstyle\sum_{\mathbf{cz}} F(\mathbf{cz}) R_\alpha(\rho_{\mathrm{E}}(\mathbf{cz})|\rho_{\mathrm{E}}(\mathbf{z})) \le 1,$$

where $R_\alpha(\rho_{\mathrm{E}}(\mathbf{cz})|\rho_{\mathrm{E}}(\mathbf{z}))$ are sandwiched Rényi powers of order $\alpha > 1$.

Step 3: When success $\Phi \triangleq \{\mathbf{cz}\colon F(\mathbf{cz}) \ge t_{\min}\}$, lower-bound the ε-smooth min-entropy as

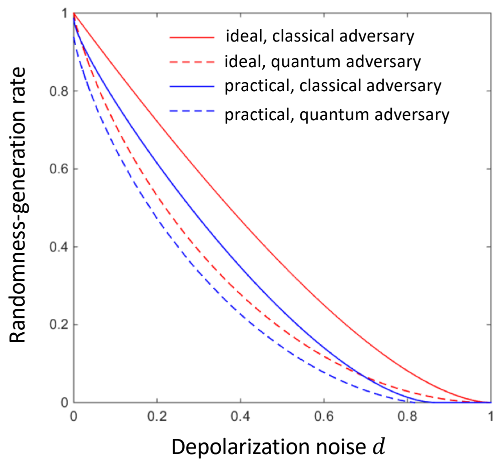
$$\frac{1}{\alpha-1}\log(t_{\min}) - \frac{1}{\alpha-1}\log\frac{1}{1-\sqrt{1-\varepsilon^2}} + \frac{\alpha}{\alpha-1}\log(\kappa),$$

where κ is a lower bound of the success probability.

Step 4: Compose with a quantum-proof strong extractor to generate random bits. The soundness error is determined by the smoothness error ε and the extractor error.

Y. Z., H. Fu, and E. Knill, Phys. Rev. Research 2, 013016 (2020)
Y. Z., H. P. Lo *et al.*, Nat. Commun. 12, 1056 (2021)

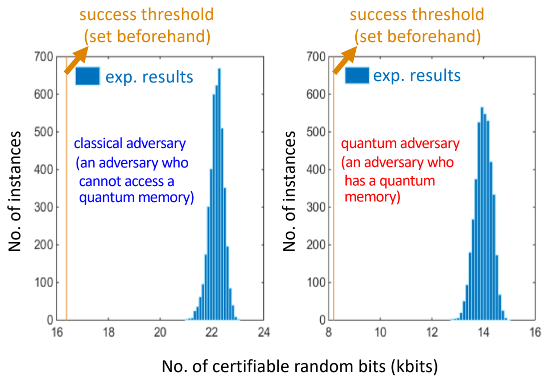
Classical vs Quantum Side Information



Here we simulate the result at a trial according to either the σ_x- or σ_z-basis measurement on the depolarized single-photon state, where the σ_x-basis measurement is chosen with probability 0.9999.

Our method can certify randomness without assuming that the state and measurements are fully characterized. Instead, our method requires only the knowledge of the misalignment angle δ between the two measurement bases and the lower bound $q_{1,\mathrm{lb}}$ on the probability of a single photon in a practical photon source. For the ideal case, we set $q_{1,\mathrm{lb}} = 1$ and $\delta = 0$, while for the practical case, we set $q_{1,\mathrm{lb}} = 0.95$ and $\delta = 5^\circ$.

Low-latency High-security Randomness Generation



Histogram of the numbers of random bits certifiable with soundness error 2^{-64} from 4,200 instances of our QRNG. Each instance of our QRNG uses a data block obtained in 0.1 s runtime.

- ➢ Each instance generates 8192 (or 2×8192) random bits against quantum (or classical) adversaries with soundness error $2^{-64} \approx 5.4\times10^{-20}$ ➔ high security.
- ➢ 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.
- ➢ Clear demonstration of the advantage of quantum adversaries as compared to classical adversaries.

Future Work

- Reduce the size of our QRNG.
- Build a continuously-operating, high-security and high-speed quantum randomness beacon.