Pros
The generated random numbers are uniformly distributed and unpredictable.
Idea behind randomness generation:
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 teeth of a second, we can certify enough entropy with respect to quantum (or classical) adversaries in order to generate a block of \( \text{II}_192 \) or \( 2 \times 9192 \) random bits with a certified error bounded by \( 2^{-30} \) 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
Polarization rotator
Polarized photons
Polarizing beam splitter
Random numbers

The generated random numbers are uniformly distributed and unpredictable, if:
- a particular quantum state, for example \( |\psi\rangle \), is prepared;
- a particular measurement, for example \( \langle D(y)|A(x)|A(A)\rangle \), 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:
Alice x
Bell test
Bob y
P(ab|xy)

Idea behind randomness generation:
if the distribution \( P(ab|xy) \) 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: complicated and low performance. The scheme is difficult to realize and the generation rate is pretty low (\( \sim 100 \) bits/second).

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 teeth of a second, we can certify enough entropy with respect to quantum (or classical) adversaries in order to generate a block of \( \text{II}_192 \) or \( 2 \times 9192 \) random bits with a certified error bounded by \( 2^{-30} \) 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).

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: \( t_1 \) (almost) \( t_3 \) (rare event)

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

Randomness Analysis Theory

Experimental REAL
Output time-lagged adjacent clicks
 entropy

Classical vs Quantum Side Information

Low-latency High-security Randomness Generation

Histogram of the numbers of random bits certifiable with soundness error \( 2^{-30} \) 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 \( \text{II}_192 \) or \( 2 \times 9192 \) random bits against quantum (or classical) adversaries with soundness error \( 2^{-30} \) \( \times \) \( 0.04 \) \( \times \) \( 0.04 \) high security.

Each instance takes 0.1 s runtime (which includes the latency 0.04 s) + 0.02 s (or 0.04 s) extraction time \( \rightarrow \) 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.

A Simple Low-latency Real-time Certifiable Quantum Random Number Generator
Yanbao Zhang1,2, Hsin-Pin Lo1, Alan Mink3, Takuya Ikuta3, Toshimori Honjo1, Hiroki Takesue1, and William J. Munro1,2
1NTT Basic Research Laboratories, NTT Corporation, Atsugi, Kanagawa 243-0198, Japan
2NTT Research Center for Theoretical Quantum Physics, NTT Corporation, Atsugi, Kanagawa 243-0198, Japan
3National Institute of Standards and Technology, Gaithersburg, Maryland 20899, USA

Why Is Randomness Important?
Gambling
Sampling
Simulation
Cryptography

Device-dependent Quantum Random Number Generator
Polarization rotator
Polarized photons
Polarizing beam splitter
Random numbers

The generated random numbers are uniformly distributed and unpredictable, if:
- a particular quantum state, for example \( |\psi\rangle \), is prepared;
- a particular measurement, for example \( \langle D(y)|A(x)|A(A)\rangle \), 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 Number Random Number Generator

Black-box model:
Alice x
Bell test
Bob y
P(ab|xy)

Idea behind randomness generation:
if the distribution \( P(ab|xy) \) 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: complicated and low performance. The scheme is difficult to realize and the generation rate is pretty low (\( \sim 100 \) bits/second).