# Practical Semi-Device Independent Randomness Generation Based on Quantum State's Indistinguishability


Hamid Tebyanian[1], Mujtaba Zahidy[1], Marco Avesani[1], Andrea Stanco[1], Paolo Villoresi[1] and Giuseppe Vallone[1,2]

*[1] Dipartimento di Ingegneria dell'Informazione, Universita` degli Studi di Padova, Padova, Italia*

*[2]Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, 35131 Padova, Italy*


## *Random numbers:*

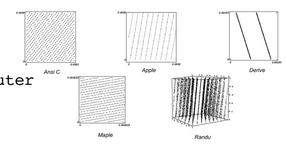
A seed of numbers called random if:
1-Uniformly distributed
2- Unpredictable

**Random number generators (RNG):**

Pseudo RNG → algorithm in a computer — Not secure

True RNG → Based on classical physics(coin tossing) — Not secure

Quantum RNG → Based on Quantum mechanics (intrinsic Randomness) — secure



Experimental complexity

Trusted Device — Semi-Device Independent — Device Independent

Security Level

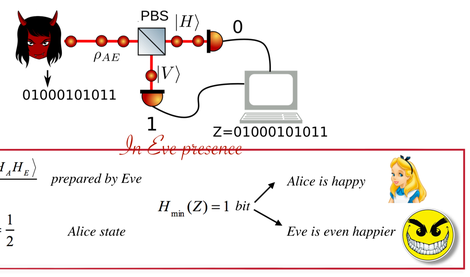
## Quantify randomness:

Min-entropy

$$H_{\min}(Z) = -\log_2 \underbrace{\max_z(P_z)}_{P_{guess}(Z)}$$

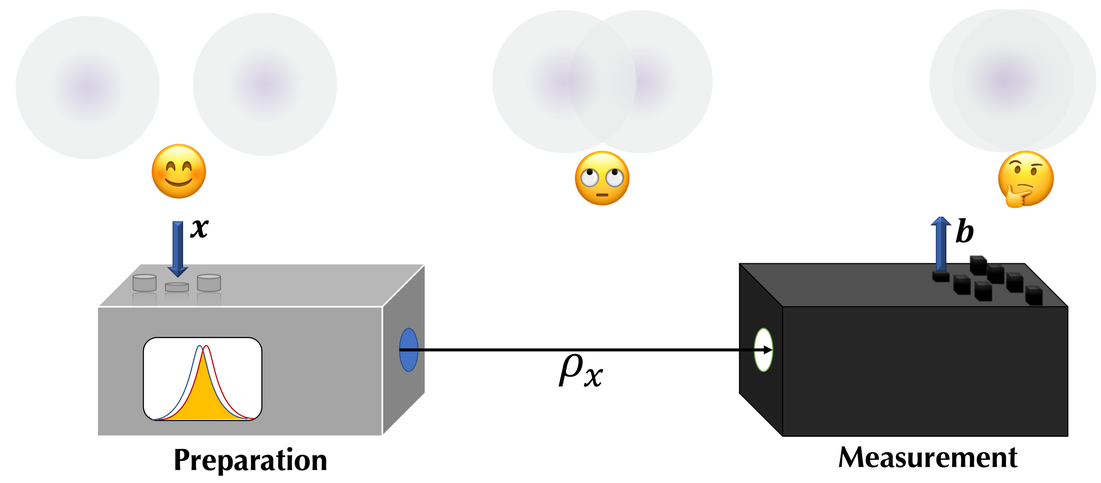
Conditional min-entropy

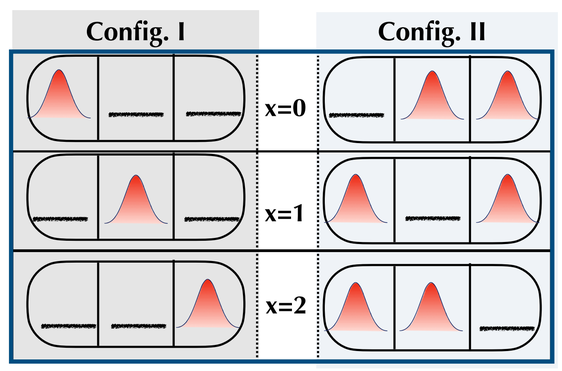
$$H_{\min}(Z \mid E)$$



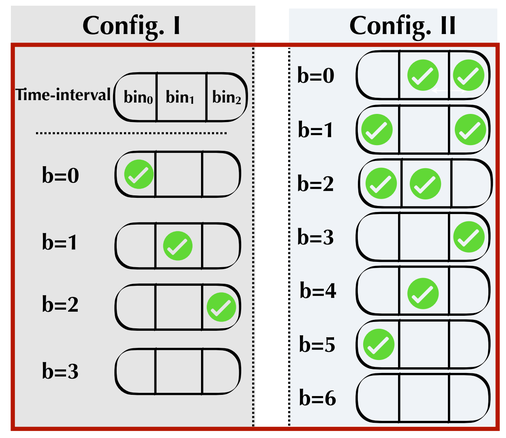

## *Framework:*

Quantum states with overlap cannot be perfectly distinguished in every round



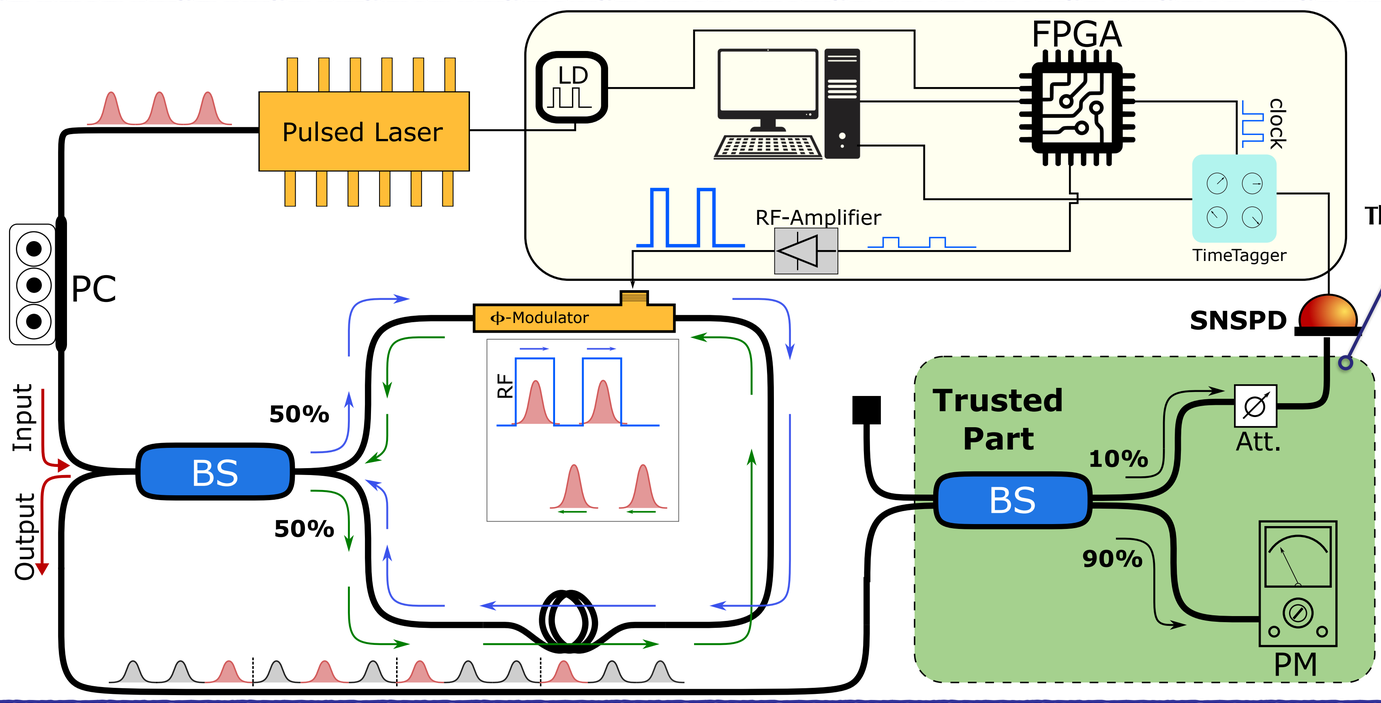

State preparations




Output configurations

## *Experiment:*

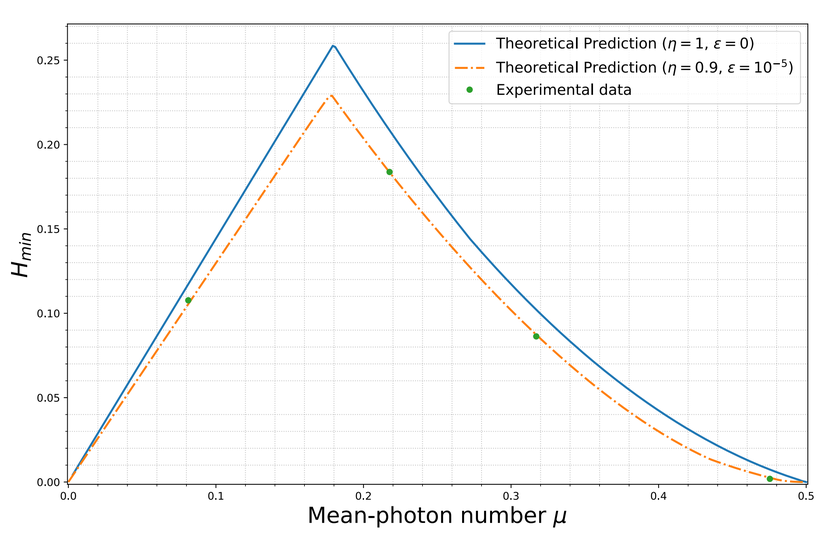
A pulsed laser emits pulses at 1550 nm to a polarization controller and then a Sagnac interferometer (SI). One path in the SI is experiencing either an extra 0 or π-phase shift with respect to the other one. The two parts interfere and recombine at the beam-splitter (BS). Depending on the phase shift, light is redirected to either output or back to the input. Later the single photons are detected with a single-photon detector, in this case, an SNSPD. A time to digital converter (TDC) converts the SNSPD detection event to time-stamps which are analyzed in post-processing. A field-programmable gate array (FPGA) provides the electrical signal to drive the laser driver (LD), phase modulator, and synchronization clock.

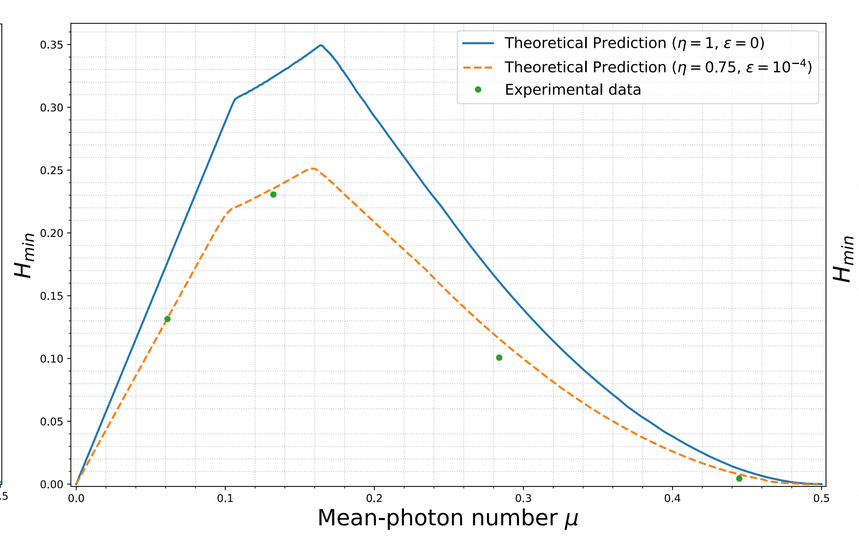


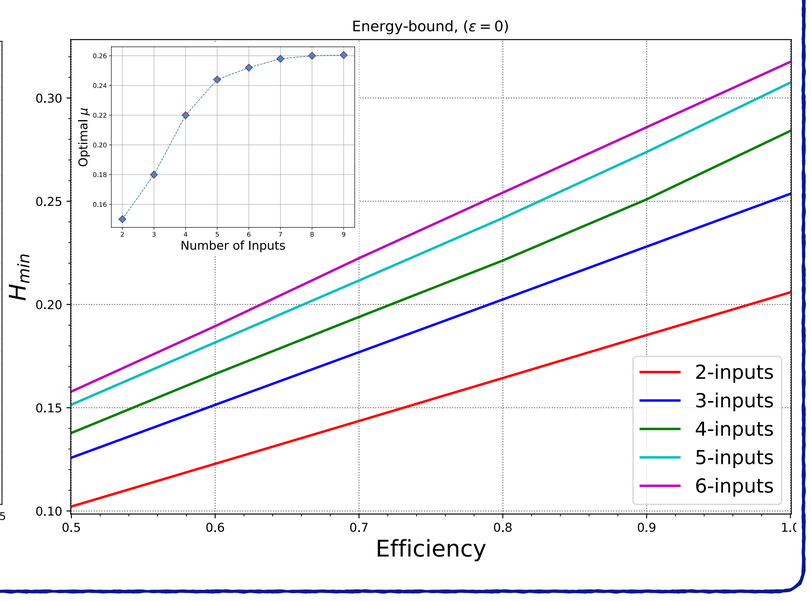

**The only trusted part of the setup:**

The energy (μ) of the transmitted states is bounded in the trusted part. Unlike the rest of the setup this section cannot be under the control of the adversary and should be carefully characterized and monitored in order to avoid information leak, which could compromise the security of the protocol.

## *Results:*




## C*onclusion:*

In conclusion, we presented a semi-DI QRNG protocol with multiple input-output and experimentally test it with an optical setup based on ternary input and measurements with various outcomes. In addition, we compared our results with a binary modulated system and showed that by increasing the number of inputs from two to three, the output **randomness** increases accordingly. The proposed protocol features an **increased security** with respect to common QRNGs, since it only requires two simple assumptions and a measurable condition on the prepared pulses' energy. Simultaneously, the protocol is **practical**, since it can be implemented with a simple all-fiber optical setup at telecom wavelength with only commercial off-the-shelf components. The performances of this proof-of-principle implementation could be further increased using faster repetition rates, faster modulation, or integrated optics.

***References:***


*H. Tebyanian, et.al, Practical Semi-Device Independent Randomness Generation Based on Quantum State's Indistinguishability, arXiv preprint arXiv:2104.11137.*

*M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone,"Semi-device-independent heterodyne-based quantum random number generator," Phys. Rev. Applied 15, 034034.*

*J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Physical Review Applied 7, 054018 (2017).*



hamid.tebyanian@york.ac.uk