Semi-Device-Independent Heterodyne-based QRNG

Hamid Tebyanian[1], Marco Avesani[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

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

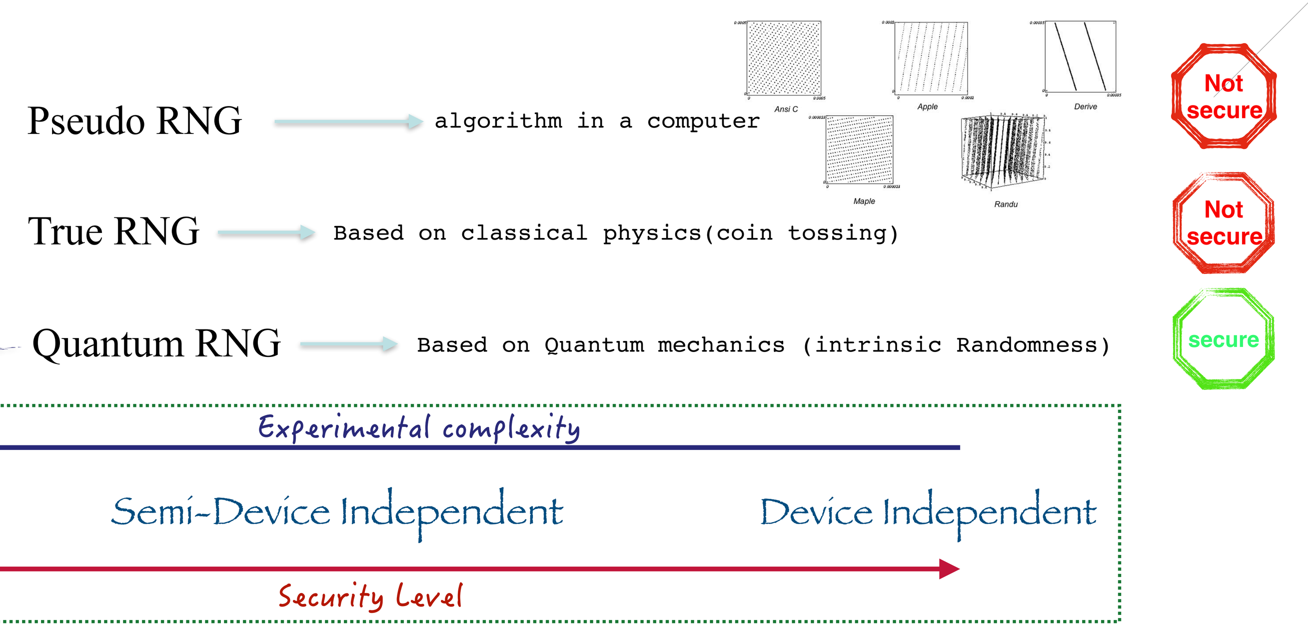
QCALL

Quantum Future

Random numbers:

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

Random number generators (RNG):



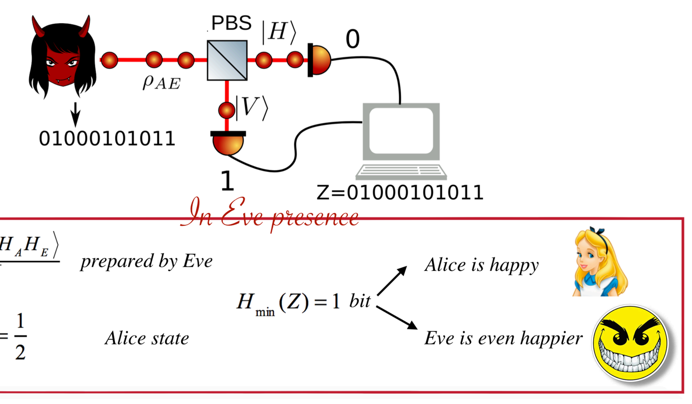
Quantify randomness:

Min-entropy

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

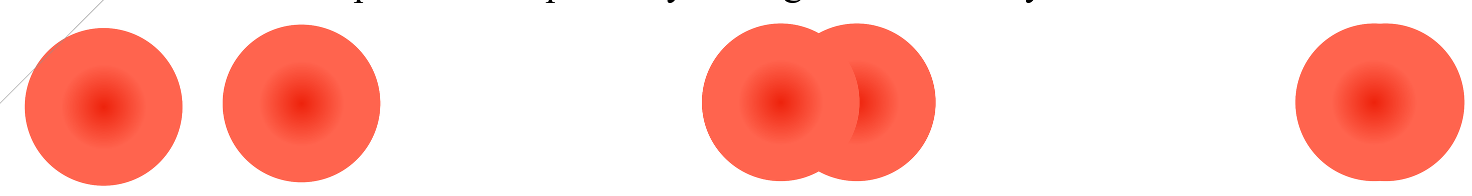
Conditional min-entropy

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



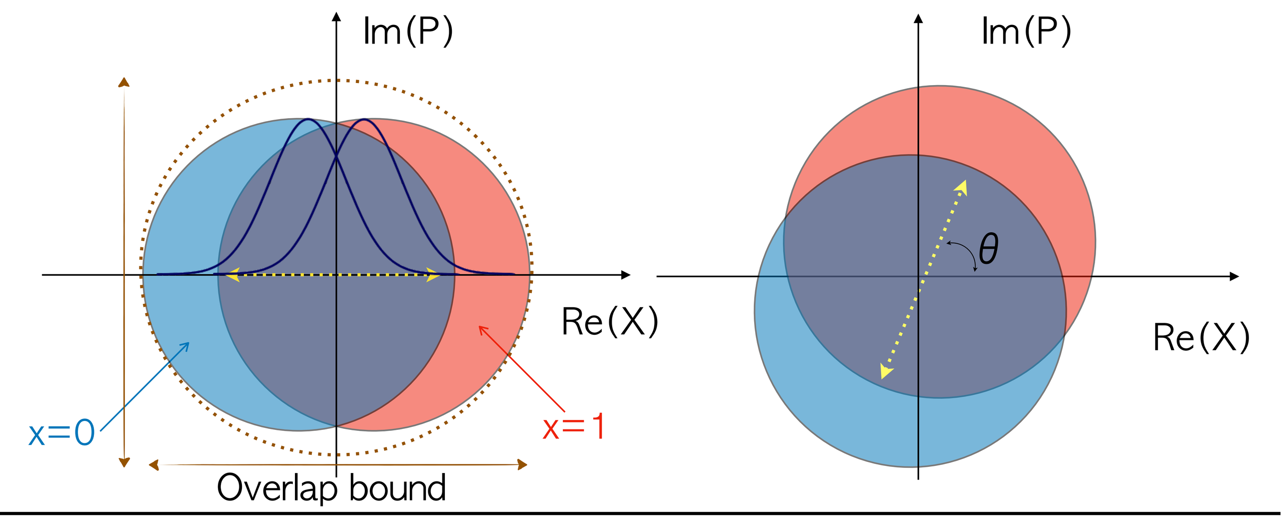
Framework:

Quantum states with overlap cannot be perfectly distinguished in every round

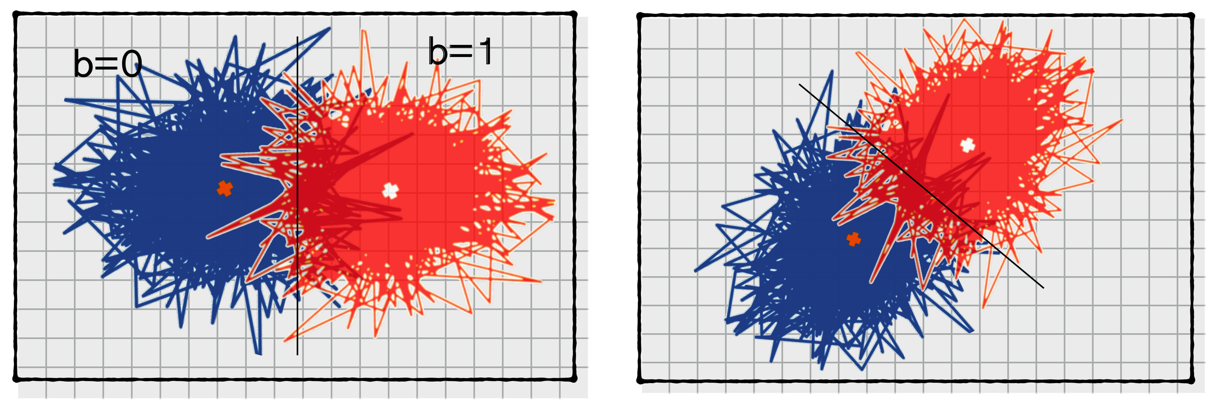


Main assumption: a bound on the energy of the prepared states fixes a bound on the overlap

$$\langle \hat{n} \rangle_{\rho_x} \le \mu \longrightarrow |\langle \psi_0^{\lambda} | \psi_1^{\lambda'} \rangle| \ge 1 - 2\mu$$

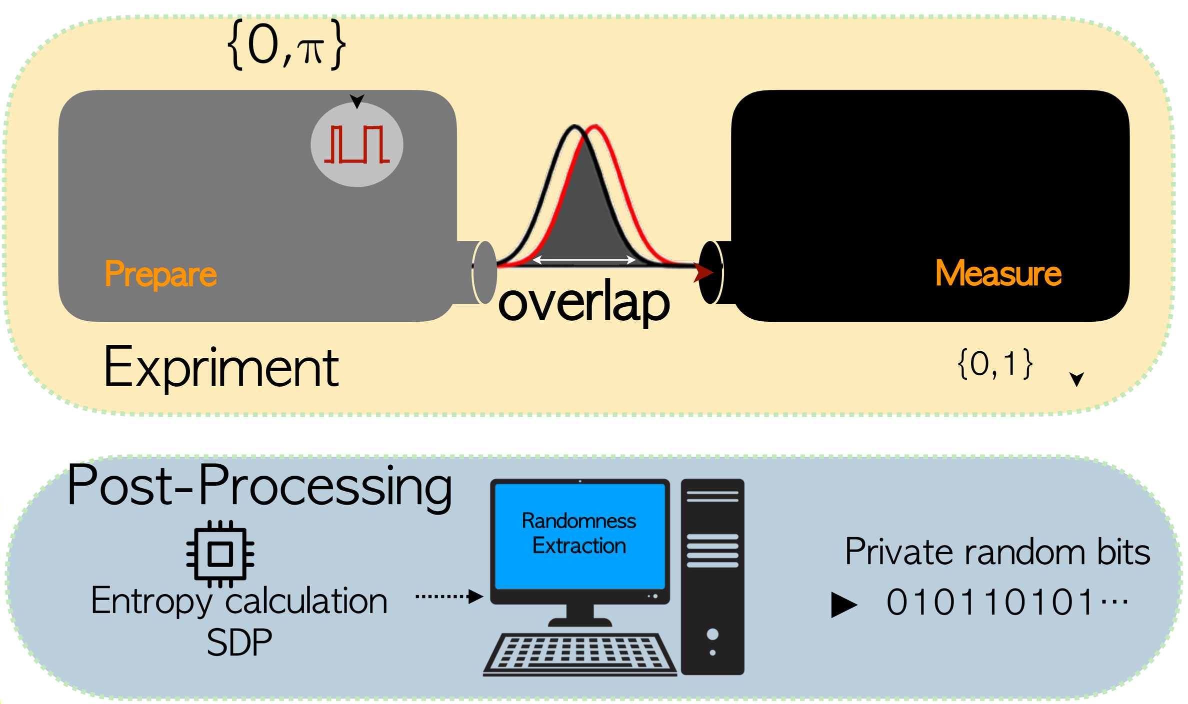


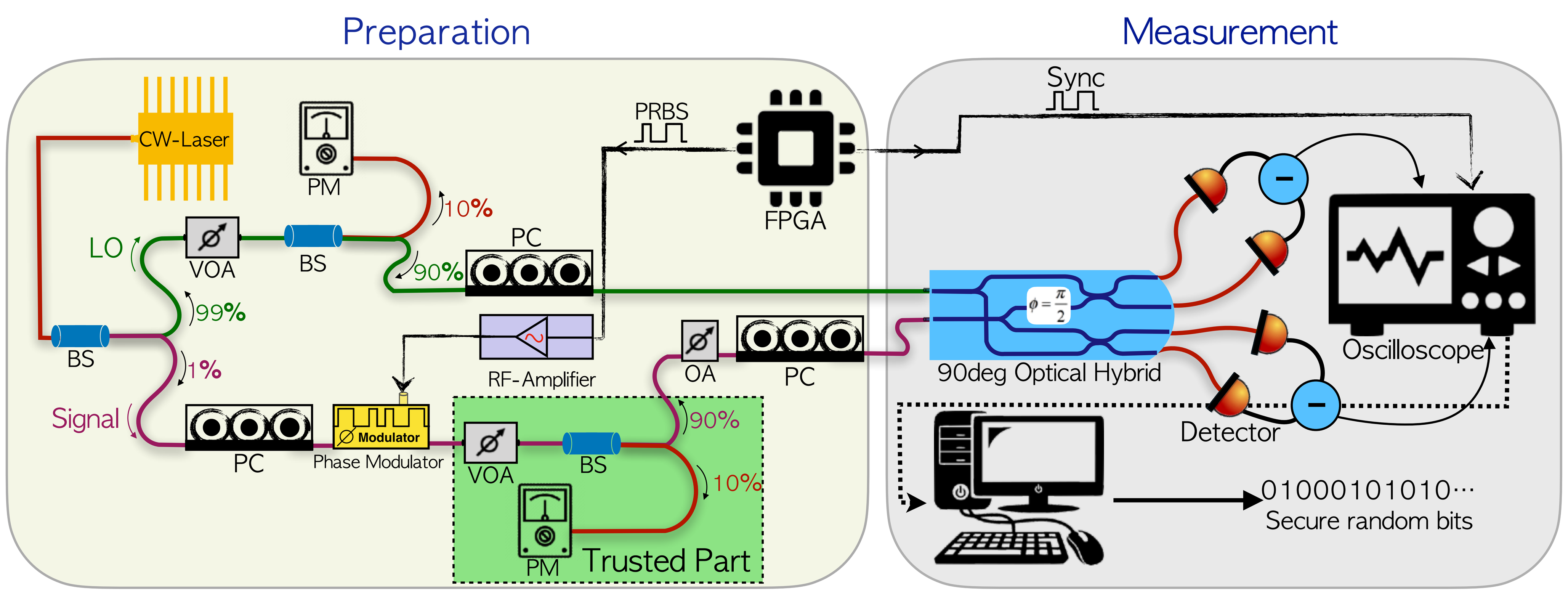
Heterodyne measurement: due to the tomographic properties of heterodyne measurement is not affected by phase fluctuations



Experiment:

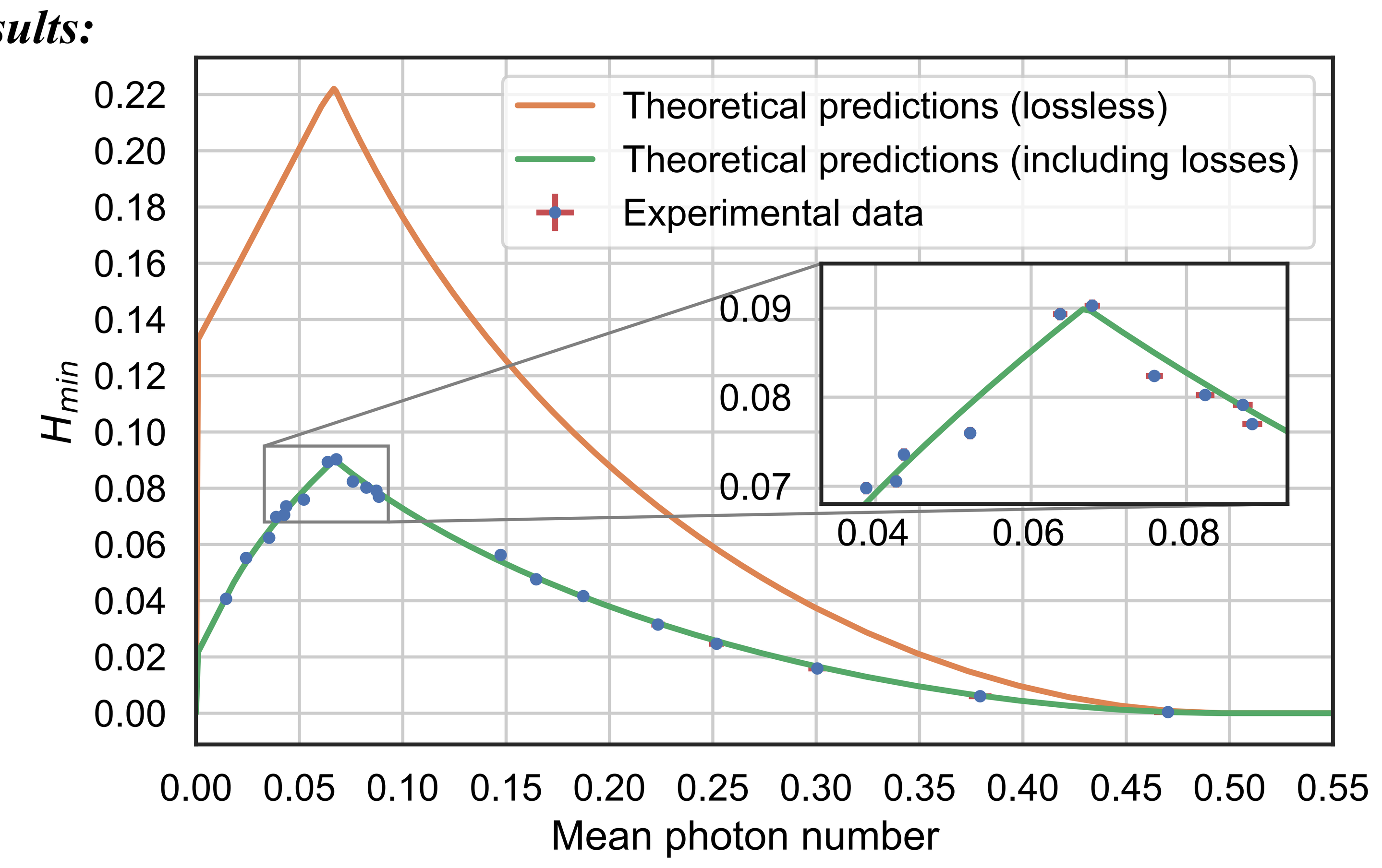
The experiment works in a prepare and measure scenario where measurement and source are untrusted, but a bound on the energy of the prepared states is assumed.



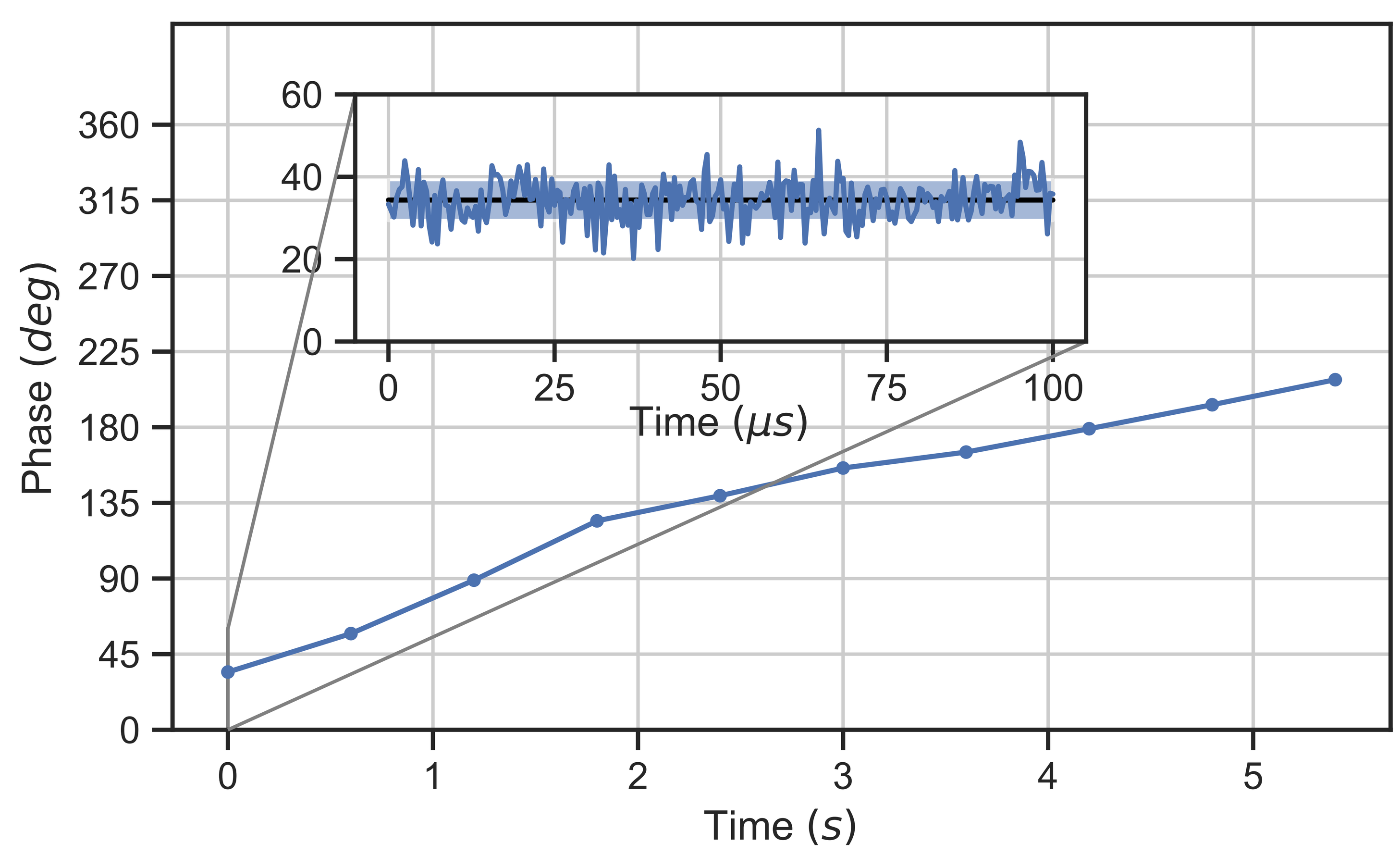


A coherent state is generated by a CW-laser and sent to the interferometer. One arm, with 1% of the light (purple path), is employed to prepare the signal, and the other one with 99% of the light (green route), is the local oscillator. In each path, 10% of light is transmitted to PM for monitoring the power. The two paths are combined on the 90 optical hybrid, which is followed by a pair of balanced detectors implementing the heterodyne measurement. An FPGA controls the phase modulator and the synchronization with the oscilloscope at 1.25 GHz repetition rate.

Results:



Conditional min-entropy as a function of the mean photon number. The orange curve is the numerical predictions obtained by SDP. The green one shows the numerical results of SDP when inefficiencies are considered and shows good agreement with experimental data (blue points).



Relative phase ϕ between signal and LO as a function of time. The system shows a drift of about 32 deg /s, while for time scales comparable with the chunk size no drift is observed (see inset).

In conclusion, we realized a simple Semi-DI QRNG solution, based on heterodyne detection and a single assumption on the maximal energy of the prepared quantum states. From the experimental point of view, our realization is based on the prepare-and-measure scenario implemented in a simple all-in-fiber optical setup with only COTS components. Our setup exploits heterodyne detection, as it provides several key advantages respect to other measurement strategies. First, it allows us to use commercial high-speed balanced detectors instead of slow and expensive single photon detectors, greatly increasing the performances while reducing the experimental complexity of the system. Secondly, by sampling the entire phase space, it allows us to track the unavoidable phase drift between the signals and the LO. In this way, fast drifts can be compensated via software during the post- processing, avoiding the need of a complex active phase stabilization system. With this scheme, we are able to generate and certify private random bits at a rate higher than 113Mbps.

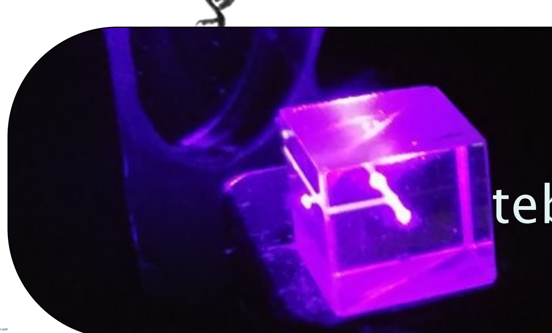
QRNG COMING

References:

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

M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Semi-device-independent heterodyne-based quantum random number generator," (2020), arXiv:2004.08344 [quant-ph].

QRNG COMING



tebyanian@dei.unipd.it