Semi-Device-Independent Heterodyne-based QRNG

Hamid Tebyanian¹, Marco Avesani², Paolo Villoresi² and Giuseppe Vallone¹,²

¹Dipartimento di Ingegneria dell’Informazione, Università degli Studi di Padova, Padova, Italia
²Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, 35131 Padova, Italy

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

Random number generators (RNG):
- Pseudo RNG
- True RNG
- Quantum RNG

Quantify randomness:
- Min-entropy
- Conditional min-entropy

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

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.

Preparation
- 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.

Measurement:
- Signal and LO are split into two branches (one with 1% of the light, the other one with 99% of the light). The two branches are dependent on a 90° optical hybrid. In each branch, 10% of light is transmitted to PM for monitoring the power and 90% is sent to balanced detectors.
- The balanced detectors produce a DC signal, which is amplified by a amplifier and fed to an oscilloscope.
- The phase shifter, which is controlled by an FPGA, is used to vary the phase between the signal and the LO.

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.
- Relative phase $\phi$ 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.

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.

References: