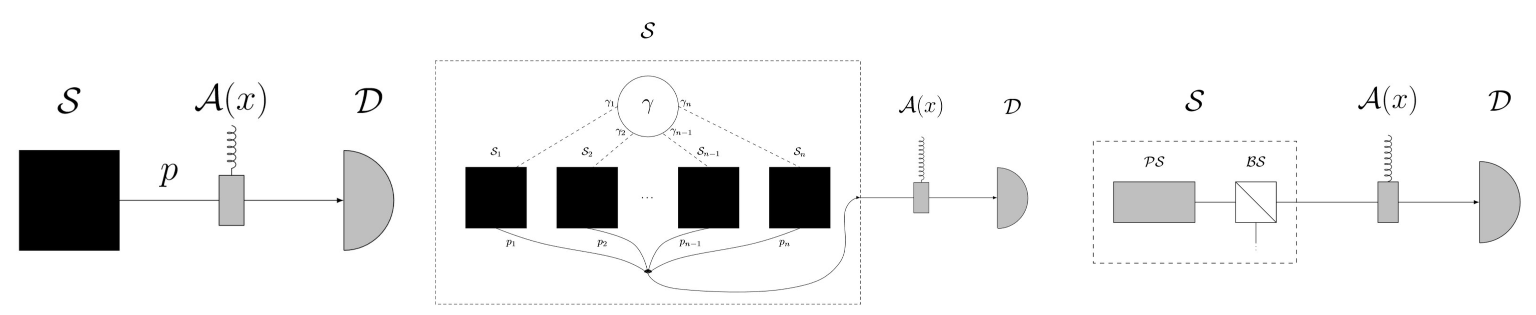
SEMI-DEVICE-INDEPENDENT RNG WITH FLEXIBLE ASSUMPTIONS

Edgar A. Aguilar — ÖAW Austrian Academy of Sciences, IQOQI Vienna
Máté Farkas — KCIK
Matej Pivoluska — Masaryk University
Martin Plesch — Masaryk University
Natália Ružičková — IST Austria, Institute of Science and Technology
Will McCutcheon — Heriot-Watt University
Clara Flegel — Heriot-Watt University
Natalia Herrera V. — Heriot-Watt University
Mehul Malik — Heriot-Watt University

Here we propose and experimentally test a new framework for semi-device-independent randomness certification that employs a flexible set of assumptions, allowing it to be applied in a range of physical scenarios involving both quantum and classical entropy sources. At the heart of our method lies a source of trusted vacuum in the form of a signal shutter, which enables the honesty of partially trusted measurement devices to be tested and provides lower bounds on the guessing probability of their measurement outcomes. We experimentally verify our protocol with a photonic setup and generate secure random bits under three different source assumptions with varying degrees of security and resulting data rates.

General Idea



- Simple source emits a signal with probability p. The signal can be blocked by a shutter $A(x)$.
- Mixed source is a mixture of simple sources governed by probability distribution γ known to the adversary, which can be fully characterized, or characterized only partially
- Photonic example is depicted on the right. Three possible assumptions on the photon source (1) single photon source, (2) known photon number distribution, (3) only mean number of photons μ known

Protocol

Below we describe our randomness generation protocol, consisting of two parts: *data collection* and *post-processing*. For practical purposes, the protocol is run in large batches of N rounds.

1. Data Collection
   I. From a private biased distribution, pick out $Q_i \in \{\text{TEST}, \text{GEN}\}$ at random with probability $(q, 1-q)$.
   II. If $Q_i = \text{TEST}$: Pick out $x_i \in \{0,1\}$ at random with probability $\left(\frac{1}{2}, \frac{1}{2}\right)$, which will determine whether to leave the shutter *open* ($x = 0$) or *closed* ($x = 1$). The outcome frequencies are used to update S_{exp}.
   III. If $Q_i = \text{GEN}$: Use $x_i = 0$ for the round, record the output y_i.
2. Post-Processing
   I. Estimate the min-entropy $H_{\min}(Y)$ of Y based on the test statistics S_e and desired assumptions.
   II. Use a universal hash-function to obtain a string Z of length $H_{\min}(Y)$ up to ϵ error.

Optimization problems

The main goal is to upper bound the guessing probability g^* of an adversary correlated with untrusted the measurement devices.

Extremal Deterministic strategies of detectors

- In simple source scenario strategies are: "Never Click", "Always Click", "Click if it detects signal".
- Correspondingly , they would produce the following statistics:

$S_N = (0,0); S_Y = (1,1); S_H = (p, 0);$ where $S := (p(\text{Click}|x=0), p(\text{Click}|x=1))$.

- Observed statistics are then $S_e = \lambda_N S_N + \lambda_Y S_Y + \lambda_H S_H$.
- Optimization can be phrased:

$$\begin{aligned} g^* = \max_{\{\lambda\}} \quad & \lambda_N + \lambda_Y + \lambda_H \cdot g \\ \text{s.t.} \quad & \lambda_Y + \lambda_H \cdot p = \alpha \\ & \lambda_Y = \beta \\ & \lambda_N + \lambda_Y + \lambda_H = 1 \\ & \lambda_{N,Y,H} \geq 0 \end{aligned}$$

- Generalization for mixed sources (adversary knows γ_i in each round):

Fully characterized

$$\begin{aligned} \max_{\{\lambda\}} \quad & \sum_i \gamma_i(\lambda_{i,N} + \lambda_{i,Y} + \lambda_{i,H} \cdot g_i) \\ \text{s.t.} \quad & \sum_i \gamma_i (\lambda_{i,Y} + \lambda_{i,H} \cdot p_i) = \alpha \\ & \sum_i \gamma_i \cdot \lambda_{i,Y} = \beta \\ & \lambda_{i,N} + \lambda_{i,Y} + \lambda_{i,H} = 1 \ \forall i \\ & \lambda_{i,\{N,Y,H\}} \geq 0. \end{aligned}$$

Partially characterized

$$\begin{aligned} \max_{\{\lambda\},\{\gamma\}} \quad & \sum_i \gamma_i (\lambda_{i,N} + \lambda_{i,Y} + \lambda_{i,H} \cdot g_i) \\ \text{s.t.} \quad & f_j(\gamma) = c_j \quad \forall j \\ & \sum_i \gamma_i = 1 \\ & \sum_i \gamma_i (\lambda_{i,Y} + \lambda_{i,H} \cdot p_i) = \alpha \\ & \sum_i \gamma_i (\lambda_{i,Y} + \lambda_{i,H}) = \beta \\ & \lambda_{i,N} + \lambda_{i,Y} + \lambda_{i,H} = 1 \quad \forall i \\ & \lambda_{i,\{N,Y,H\}} \geq 0 \\ & \gamma_i \geq 0. \end{aligned}$$

- Simple source and fully characterized mixed source are solvable analytically. Partially characterized mixed source is solvable analytically in special case

Entropy estimates for photonic setup

Let us consider photonic setup given in the first box, using a beam-splitter with reflection probability π. Solutions to the optimization problems are:

Single Photon:

$$g^s = 1 - (\alpha - \beta)\left(\frac{\pi}{1-\pi}\right)$$

Known Photon Number Distribution:

Define N implicitly

$$\sum_{i=N+1}^{\infty} \gamma_i(1-\pi^i) < (\alpha - \beta); \sum_{i=N}^{\infty} \gamma_i(1-\pi^i) \geq (\alpha - \beta)$$

Then the guessing probability becomes

$$g^{kd} = 1 - \frac{\pi^N}{1-\pi^N}(\alpha - \beta) + \sum_{i=N+1}^{\infty} \gamma_i \left(\frac{1-\pi^i}{1-\pi^N} - 1\right)$$

Mean Photon Number Known:

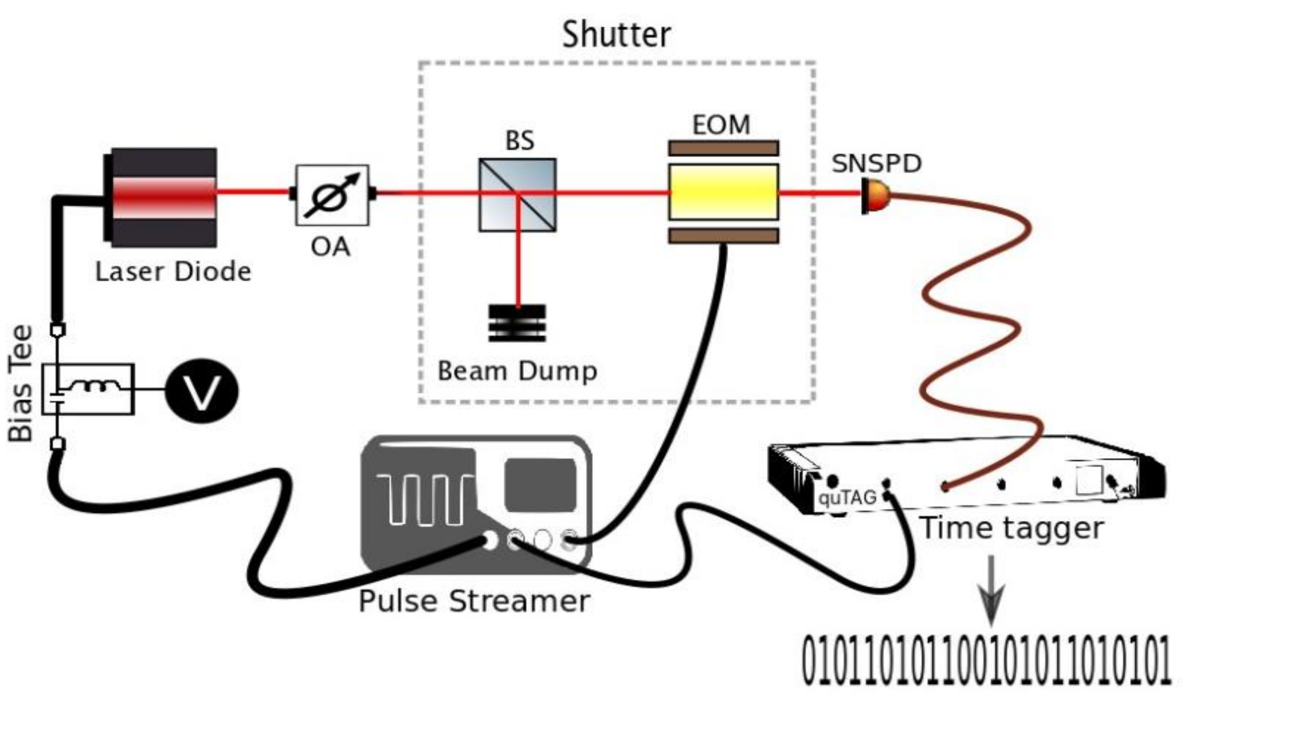
Leads to a solution with only three non-zero frequencies for *0*, *N* and *N+1* photons

$$g^{\mu} = 1 + (\alpha - \beta) - \left(\frac{(\alpha-\beta) + \mu(\pi^{N+1} - \pi^N)}{(N+1)(1-\pi^N) - N(1-\pi^{N+1})}\right)$$

Experiment and results

The source is composed of a Laser and an Optical Attenuator (OA), used to reduce the power of the input light to the order of a few photons. The shutter is composed of two Polarization Controllers (POL Control), an Electro-Optical Modulator (EOM), and a Polarizer filter. If no voltage is applied to the EOM, no light passes the filter, and when a voltage is applied there is a pi-phase shift allowing light to pass the polarizer. Finally, there is a balanced beam splitter and the detector. The expected rate is 100 kbs of raw data with telecomm frequencies.

The setup



Entropy estimates of 1000 batches of 100000 rounds