Supplementary Material of Real-Time Source Independent Quantum Random Number Generator with Squeezed States

Thibault Michel,[1,2,*] Jing Yan Haw,[1] Davide G. Marangon,[3] Oliver Thearle,[1] Giuseppe Vallone,[3,4] Paolo Villoresi,[3,4] Ping Koy Lam,[1,†] and Syed M. Assad[1]

[1] *Center for Quantum Computation and Communication Technology, Department of Quantum Science, The Australian National University, Canberra, ACT 0200, Australia*
[2] *Laboratoire Kastler Brossel, UPMC-Sorbonne Universités, CNRS, ENS-PSL Research University, Collège de France, 4 place Jussieu, 75252 Paris, France*
[3] *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, Via Gradenigo 6B, 35131 Padova, Italy*
[4] *Istituto di Fotonica e Nanotecnologie —CNR, Via Trasea 7, 35131 Padova, Italy*

I. EXPERIMENTAL SET-UP

A detailed scheme of the experimental set-up is shown in Fig. 1.

An **Innolight Diablo** ND:YAG laser provides a continuous wave single mode light beam at 1064 nm used as local oscillator and seed for the Optical Parametric Amplifier (OPA) cavity. It also provides a frequency doubled 532 nm beam used as the OPA pump. A mode cleaner is used on each of the beams to obtain a pure spatial mode (TEM00) as well as a filtering of intensity and frequency noise out of the bandwidth, thus providing shot-noise limited beams above 2MHz.

The pump beam is phase modulated at 30.3125 MHz (signal A) with a **Newport Newfocus 4002** Electro-Optic Modulator (EOM). This modulation is used to lock the OPA cavity length using the Pound Drever Hall method. The seed beam is phase modulated at 20.625 MHz (signal B) with a **Newfocus 4004** EOM. This modulation is used to lock the pump-seed relative phase, as well as to lock the homodyne detection to the $\hat{P}$-quadrature. The seed beam is also amplitude modulated at 11.875 MHz (signal C) with a **Newfocus 4104** EOM. This modulaiton is used to lock the homodyne detection to the $\hat{Q}$-quadrature.

The OPA is a bow-tie doubly resonant cavity with a periodically poled potassium titanium oxide phosphate (KTiOPO4) (PPKTP) crystal. The crystal is 10.5 mm long, it is periodically poled to ensure quasi phase matching around 35°C. Its temperature is controlled with a Peltier cooler and a **Newport Model 3040** temperature controller. The crystal is also AR coated to minimize losses and wedged with a 1° angle to compensate for intracavity dispersion and ensure co-resonance of the 1064 nm and 532 nm beams. The cavity linewidth is around 32 MHz with a finesse of 35 at 1064 nm.

Two **NI PXIe-7856R** FPGA, embedded in a **NI PXIe-1078** chassis with a **NI PXIe-1078** controller, are used to generate all the control and lock signals. This includes the modulation signal A–D, as well as a control signal for the flip-shutters. The various error signals are fed to these FPGA via **AD9460** ADC converters. The FPGA then implements a PID method to generate the feedback lock signals for the piezo-eletric transducers. The flip-shutters are servo-motor controlled with Pulse Width Modulation (PWM) signals.

The QRNG protocol is run in two different configurations. First, using the squeezed source generated from the OPA, with squeezing around 3 dB. Second, using a thermal source. In the latter configuration part of the seed is tapped off before the OPA cavity and sent straight to the homodyne detection. The thermal state was generated by putting additional amplitude and phase white noise signal on the seed beam modulators with a pair of **Agilent 33250A** function generators. This additional noise was varied to span several thermal states.

II. DATA ACQUISITION AND PROCESSING

The subtracted signal from the homodyne detection is mixed down at 15 MHz (signal D) and low pass filtered at 2 MHz to get the sideband signal between 13 and 17 MHz. This frequency band was chosen because it is free from any other modulation and also shows significant squeezing as it is still inside the OPA cavity linewidth. The signal is digitized with a **NI PXIe-5124**. This digitizer converts the analog signal to an effective 12-bits integer. The actual output are 16-bits integers with the 4 least significant bits unused and left at 0, those 4 bits were discarded to obtain an integer in the range $[-2048; 2047]$. The signal was sampled at 200 kHz, well below the Nyquist frequency of the low pass filter, to ensure no time correlation were present. Fig. 2 shows the autocorrelation of a sample of 10^6 points of the raw signal from the thermal run. The low values of autocorrelation between the samples are consistent with our raw data being close to independent and identically distributed random variables. The dashed line shows the theoretical standard deviation of 10^6 truly random points. Note that the computer was performing the data hashing in real time. So we did not oversample to then downsample, as is often done to check that the time-correlation are consistent with the low-pass filter used.

As a sanity check of our hashing process, we tested a collection of random numbers obtained from both the

* thibault.michel@lkb.upmc.fr
† ping.lam@anu.edu.au

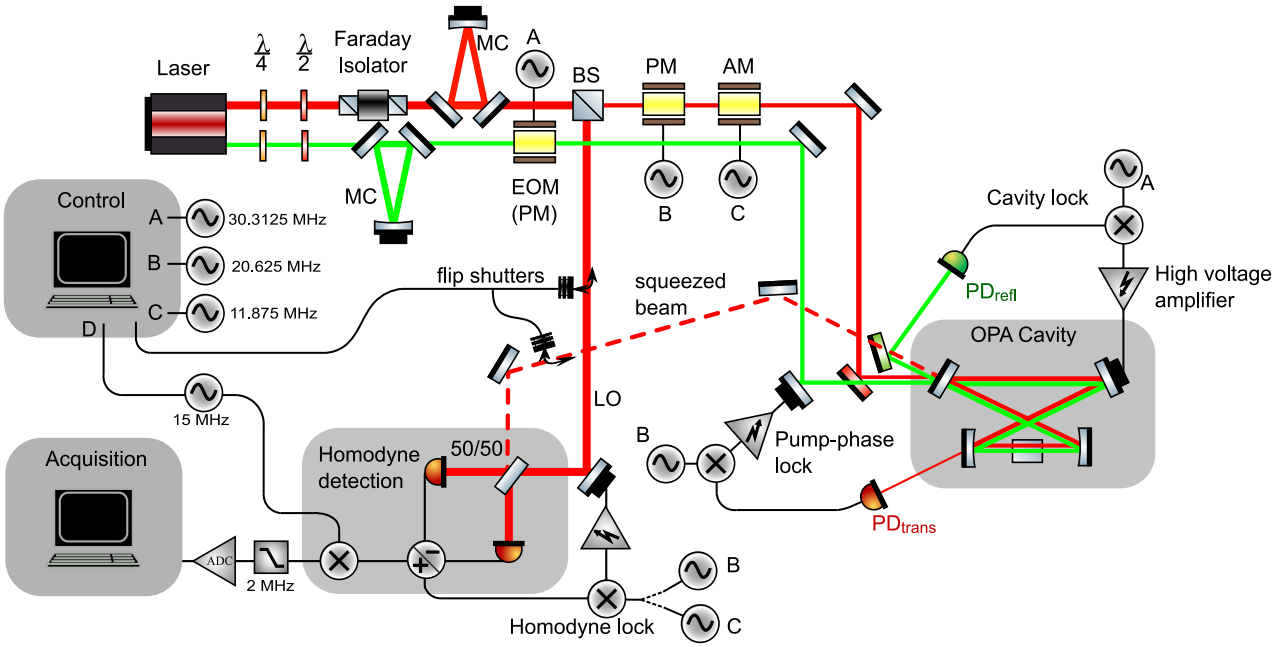

Figure 1: Scheme of the experimental set-up for the squeezed state generation and measurement.

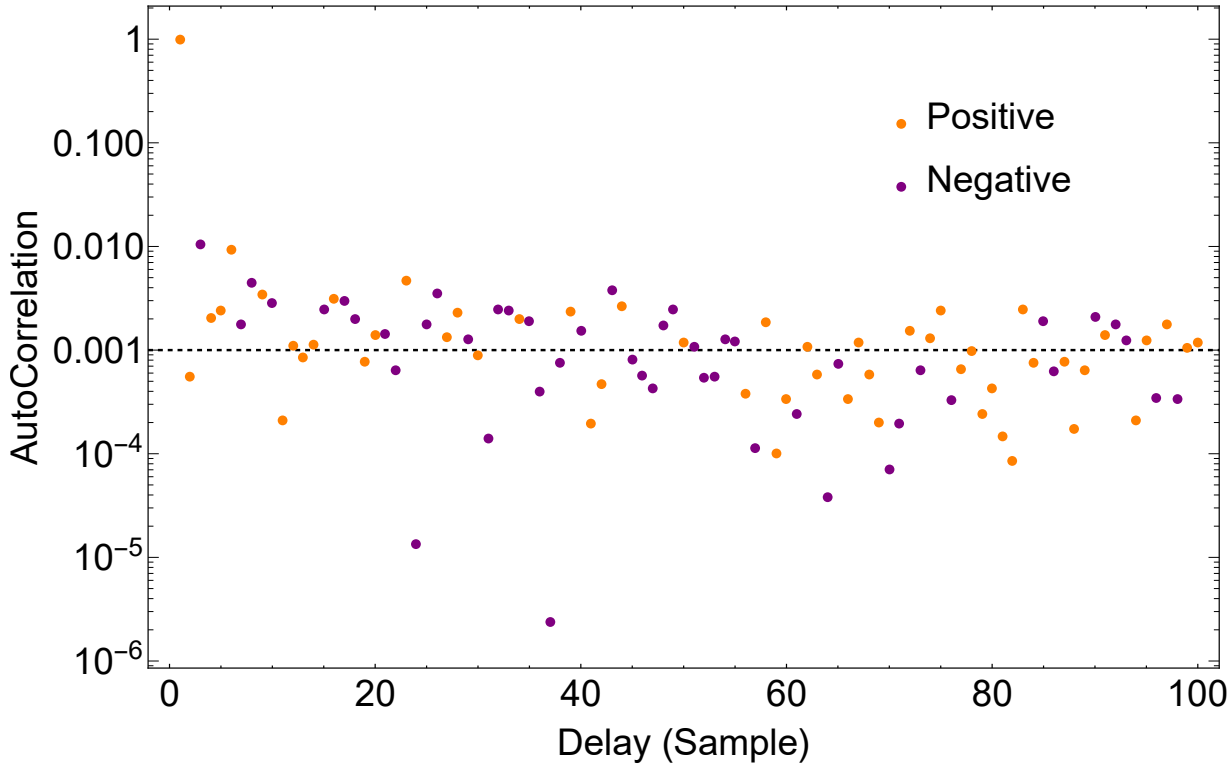

Figure 2: Autocorrelation of a sample of 10^6 points from the raw signal. Dashed line shows the theoretical standard deviation of 10^6 truly random points.

thermal and squeezed states with the NIST statistical test suite. The results are shown in Fig. 3.

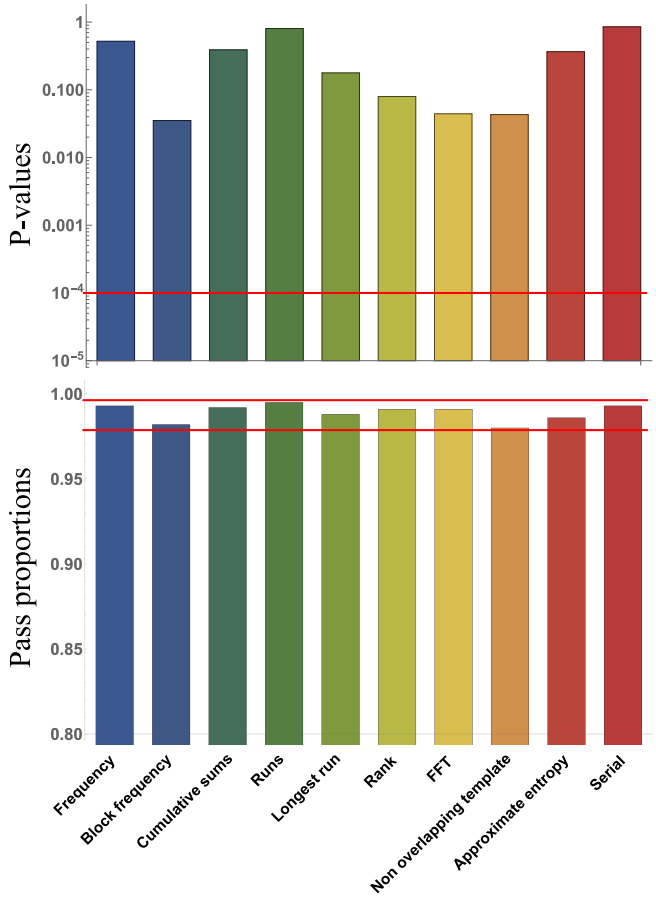

Figure 3: Results of NIST statistical test suites obtained by combining 1000 samples from both the squeezed and thermal state source. Each sample size is 100 kbits and the test significance level is $\alpha = 0.01$. To 'pass', the P-values (uniformity of p-values) should be larger than 0.0001 and the pass proportions should be within the Clopper–Pearson interval of $[0.978724, 0.996273]$.