optica

Quantum entropy source on an InP photonic integrated circuit for random number generation: supplementary material

CARLOS ABELLAN[1,*], WALDIMAR AMAYA[1], DAVID DOMENECH[2], PASCUAL MUÑOZ[2,3], JOSE CAPMANY[2,3], STEFANO LONGHI[4], MORGAN W. MITCHELL[1,5], AND VALERIO PRUNERI[1,5]

[1]ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
[2]VLC Photonics S.L. Cami de Vera s/n, Edificio 9B, Valencia, Spain
[3]ITEAM Research Institute, Universitat Politecnica de Valencia, Spain
[4]Dipartimento di Fisica and Istituto di Fotonica e Nanotecnologie del CNR, Politecnico di Milano, Milan (Italy)
[5]ICREA - Institucio Catalana de Recerca i Estudis Avancats, 08015 Barcelona, Spain
[*]Corresponding author: carlos.abellan@icfo.eu

Published 8 September 2016

This document provides supplementary information to "Quantum entropy source on an InP photonic integrated circuit for random number generation," http://dx.doi.org/10.1364/optica.3.000989. We demonstrate quantum random number generation from the quantum entropy source presented in the main article using bulk components. Using standard post-processing techniques and a commercial digitization card, we obtain high-quality random numbers that successfully pass industrial randomness tests.

http://dx.doi.org/10.1364/optica.3.000989.s001

1. BEAT SIGNAL BETWEEN TWO LASERS

Let $\mathcal{E}_{\mathrm{gs,cw}}$ be the electromagnetic field of the gain-switched and the continuous wave DFB lasers, with central wavelength $\omega^{(gs)}$ and $\omega^{(cw)}$ respectively. All fields and intensities depend on time. The total field after combining the gain-switched pulses and the cw reference in a combiner is given by $\mathcal{E} \equiv \mathcal{E}_{\mathrm{gs}} + \mathcal{E}_{\mathrm{cw}}$, and the intensity by

$$\begin{aligned} i_T =& |\mathcal{E}|^2 = (\mathcal{E}_{\mathrm{gs}} + \mathcal{E}_{\mathrm{cw}})(\mathcal{E}_{\mathrm{gs}} + \mathcal{E}_{\mathrm{cw}})^* \\ =& |\mathcal{E}_{\mathrm{gs}}|^2 + |\mathcal{E}_{\mathrm{cw}}|^2 + 2\mathrm{Re}\{\mathcal{E}_{\mathrm{cw}}\mathcal{E}_{\mathrm{gs}}^*\}. \end{aligned} \tag{S1}$$

We employ single-frequency and single-spatial mode devices, so we can approximate the laser fields by plane waves. From the experiment, we observe thermal chirp effects during the ON part of the modulation, so we phenomenologically add a linear chirp parameter $\beta_0 t$, as further discussed in the main text. We can rewrite

$$\omega^{(gs)}(t) = \omega_0^{(gs)} + \beta_0 \cdot (t \bmod T), \tag{S2}$$

where $\omega_0^{(gs)}$ is the unchirped frequency of the GS laser, and T is the period of the RF modulation. Defining the frequency detuning between the GS laser and the cw laser as

$$\Omega_c(t) \equiv \omega^{(cw)} - \omega^{(gs)}(t) \tag{S3}$$

$$= \omega^{(cw)} - \omega_0^{(gs)} - \beta_0 \cdot (t \bmod T) \tag{S4}$$

we finally obtain

$$i_T(t) = i^{(cw)} + i^{(gs)} + 2\sqrt{i^{(gs)} i^{(gs)}} \cos\left(\int_0^t d\xi \Omega_c(\xi) + \Delta\phi \right), \tag{S5}$$

where $\Delta\phi \equiv \phi^{(cw)} - \phi^{(gs)}$ is the phase difference between the two laser fields. In gain-switched phase-diffusion random number generators (RNG), the quantum randomness is found in $\phi^{(gs)}$, the phase of the gain-switched laser, which experiences a strong diffusion process during the below-threshold time of the modulation [1–5].

The optical intensity is detected by a finite bandwidth electronic system, introducing several limitations in the operation of the two-laser RNG scheme described in the main text. For

the sake of simplicity, and without loss of generality, we will proceed neglecting the chirp effect in what follows. By doing so, Ω remains constant during the entire GS pulse. The voltage at the output of the detection system can be written as the convolution of the total intensity $i_T(t)$ and the impulse response of the detection system $h_D(t) \sim \exp\{-t^2/2\tau_D^2\}$, which is well represented by a gaussian shape with rms deviation defined by the response time τ_D. The first term in Eq. (S5) describes the intensity of the cw laser, and is nearly constant. Similarly, the second term describes the intensity of the GS laser, which follows the envelope of the modulation signal. Contrary, the last term in Eq. (S5) describes an oscillation within the GS cycle with a frequency Ω and a phase $\Delta\phi = \phi^{(cw)} - \phi^{(gs)}$, which contains the information we want to resolve, $\phi^{(gs)}$. The detected signal for this latter term is therefore given by

$$\begin{aligned}\cos\Big(\Omega t + \Delta\phi\Big) * h_D(t) \\ &= \int_0^\infty d\tau h_D(t-\tau)\cos\left(\Omega\tau + \Delta\phi\right) \\ &\propto \exp\Big\{-\frac{1}{2}\Omega^2\tau_D^2\Big\}\cos\left(\Omega t + \Delta\phi\right), \qquad \textbf{(S6)}\end{aligned}$$

clearly imposing restrictions to the response time of the detection system. If $\Omega\tau_D >> 1$, the term $\exp\{-\frac{1}{2}\Omega^2\tau_D^2\} \to 0$ and therefore we can not recover the beat-note $\cos(\Omega t + \Delta\phi)$. In contrast, if the system responds fast enough $\Omega\tau_D < \sqrt{2}$, the beat-note can be recovered, and thus the random phase $\Delta\phi$.

2. EXPERIMENTAL RESULTS WITH BULK COMPONENTS

The QRNG scheme based on the beating between two semiconductor lasers was also demonstrated with bulk components. An Alcatel A1905LMI DFB laser was used as the gain-switching source, and a tunable laser Photonetics Tunics Plus 3642 HE 10 as the cw reference, as illustrated in Fig. S1. A 2x1 polarization maintaining coupler (PMC) was used to combine the two signals. The interfered signal was detected by a 10 GHz bandwidth photodetector (Nortel PP10G), and digitised by a 2 Gsps digitiser Acquiris U1084A with 1 GHz electrical bandwidth.

In contrast to the integrated version of the system, in which we had access to electrical signals from on-chip photodiodes only, in the bulk scheme we could analyse the optical behaviour

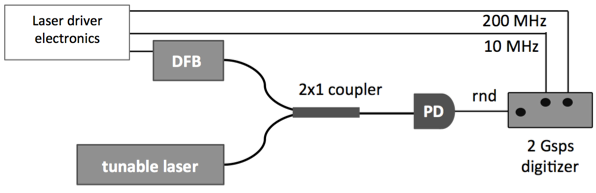

Fig. S1. Bulk setup for the QRNG based on heterodyning two laser diodes. A DFB laser is directly modulated from below to above threshold with a 200 MHz signal. A tunable laser is operated in cw and the central frequency is set very close to the central wavelength of the GS laser. A 2x1 polarisation maintaining coupler combines the two signals and a photodetector (PD) detects the beating field. The random signal (rnd) is sent to a high-speed digitiser. The 200 MHz signal and the internal 2 GHz clock of the digitiser are synchronised with a 10 MHz signal.

too. Using an optical sampling scope and an optical spectrum analyser, we measured the interference visibility (rms deviation of the distribution) as a function of the detuning between the two lasers. In this way, we could set the detuning with high spectral control. As shown in Fig. S2, high interference visibility was observed for detunings up to $\Omega/2\pi \sim 25$ GHz, which corresponded to the detection bandwidth of the sampling scope.

Once the detuning was set, a photodetector was placed at the output of the PMC and the signal digitised with 8-bit resolution. Since the digitiser had 1 GHz electrical bandwidth only, we operated the system with a detuning $\Omega < 1$ GHz to resolve the beating. In contrast to the integrated scheme, in which high-loss PIC and relatively large detunings had to be set to avoid locking mechanisms, the bulk lasers incorporate > 30 dB optical isolators, highly reducing the effect of coupling between the two lasers. No locking mechanism was observed in this configuration for a variety of powers setting in the cw laser.

The system run overnight to acquire, post-process and test 60 sequences of 1 GB (Giga-Bytes). The acquisition, processing and testing of each dataset took ~ 7 minutes. As shown in the histograms depicted in Fig. S3(a), the interference visibility $\mathcal{V}$ was very high over the entire run, indicating that the temperature control of the lasers kept their frequency difference within the detection bandwidth. However, small statistical fluctuations were observed over time. See for instance the difference between the first acquisition (labeled 7 minutes purple color) and the last acquisition (labeled 350 minutes color blue, taken 6 hours after the first one) in Fig. S3. We attribute these differences to slow temperature fluctuations. The digitisation process also introduced some instabilities due to the asynchronous sampling of the signal. However, as shown in Fig. S3(b), the difference between the distributions of two subsequent acquisitions was on average smaller than the difference between the distributions spaced by 70, 140, 210, 280 and 350 minutes, indicating that separation in time led to slightly different distributions. We emphasize this effect is small and is minimised with the integrated QRNG-PICs, since temperature drifts become very similar for the two closely spaced lasers.

To extract randomness from the raw data, we used the two-universal hashing randomness extractor proposed by D.

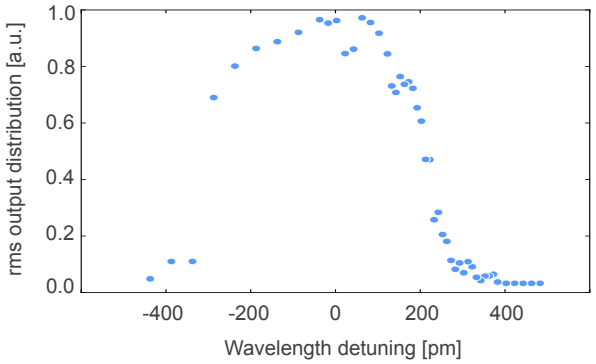

Fig. S2. Interference visibility as a function of the detuning between the gs laser and the cw laser. The interference visibility was measured as the root-mean-square deviation of the observed histogram. The statistics were obtained with a sampling scope Agilent Infiniium DCA-J 86100C and the spectrum with an optical spectrum analyser Yokogawa AQ6370.

Frauchiger et al in ref. [6]. A randomness extractor is an algorithm that takes n-bit corrupted random numbers of min-entropy H_∞ and covert them into m-bit (with $m < n$) uncorrelated and uniformly distributed random numbers, with the same min-entropy. The extractor in ref. [6] uses a constant seed matrix E of random bits, and extracts the randomness doing the operation $y_m = E_{mn}x_n$. This extraction algorithm is proven to be secure even if the matrix E is made public after being hardcoded into the extractor device.

The hardest part of a randomness extraction process remains the estimation of the min-entropy of the raw bits. For a rigourous and conservative estimation, the physical process has to be deeply understood and modelled. Also, memory effects as well as digitisation electronics have to be considered. A detailed description on the estimation for a similar system and components can be found in refs. [3, 7]. In this work, and only for illustration on the simplicity of going from raw data to post-processed data, we generate up to 60 Gb using the extractor in ref. [6] and estimating the min-entropy from the observed frequencies. Even in the case in which we overestimate the min-entropy (i.e. we apply less extraction than we should), the output sequence behaves as a "perfect coin" with respect to the applied tests: correlation output bits and alphabit battery of statistical tests. The autocorrelation for 60 Gb of data is shown in Fig. S4, in which the raw autocorrelation is also shown. In addition, we apply the Alphabit battery in a similar fashion as in [5]. We take 60 sequences of 1 Gb each and measure the failure rate (which is approximately 2% for an ideal random sequence). The generated strings are within 2% range for all the 17 tests of the battery. Another run with $\sim$ 100 Gb of data also passes successfully both the correlation and the Alphabit tests.

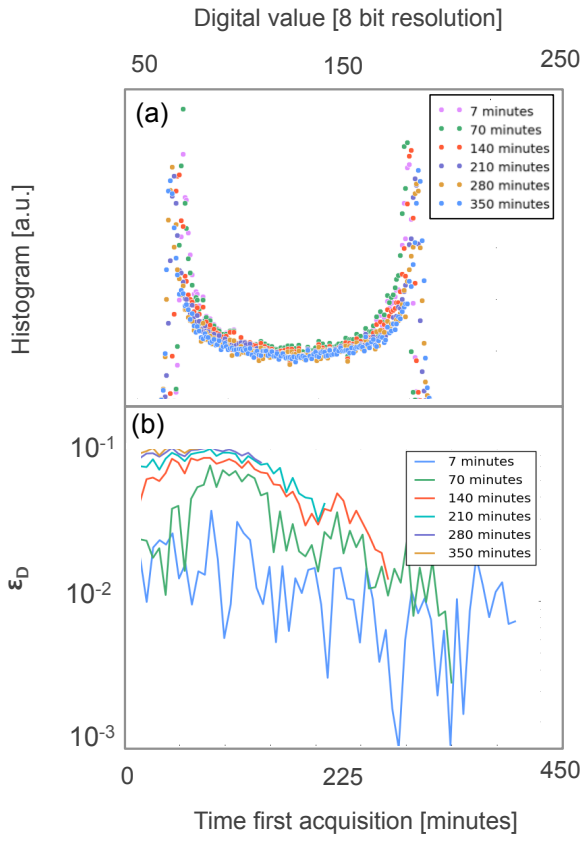

Fig. S3. (a) Histograms for several generated sequences of 1 GB each. Each histogram in this plot is spaced by a 70-minutes temporal window. All histograms show high visibility interference. However, small statistical variations are observed between temporally spaced sequences due to thermal effects. (b) Statistical distance between different histograms taken during the entire run. Let H_i be the histogram of each of the 60 acquisition taken during the experiment. The size of each histogram H_i is $2^8 = 256$ samples. The figure of merit in this plot corresponds to $\epsilon_D \equiv \sqrt{(\sum_j (H_{i+d,j} - H_{i,j})^2)}$, where j iterates over each of the 256 bin. Each value computes the distance between two distributions spaced by $7, 70, 140, 210, 280$, and 350 minutes. In the horizontal axis we indicate when the first distribution involved in the calculation (H_i) was taken.

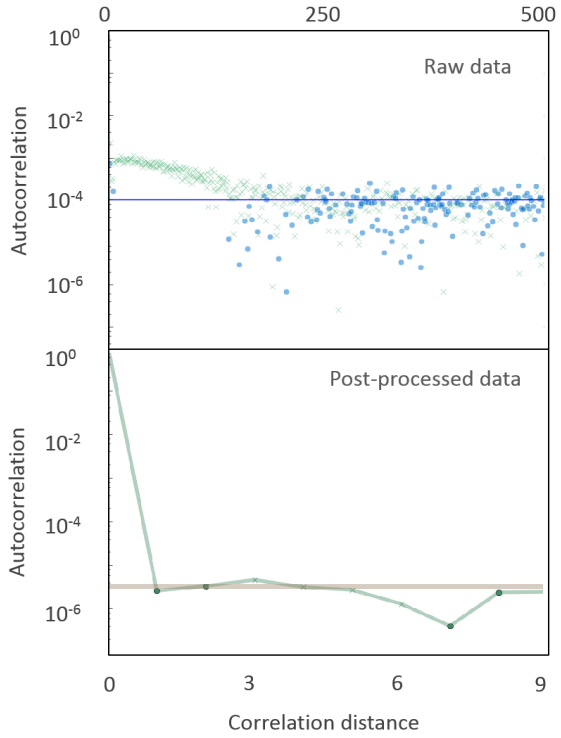

Fig. S4. Autocorrelation bulk experiment. (Upper) Raw autocorrelation. This result is nearly identical to the correlation observed for the delay line case in previous works, both for multiple bit digitisation [3], and for one-bit digitisation [5]. (Lower) Autocorrelation post-processed data.

REFERENCES

1. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Opt. Express **22**, 1645–1654 (2014).
2. Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. Fröhlich, A. Plews, and A. J. Shields, "Robust random number generation using steady-state emission of gain-switched laser diodes," Appl. Phys. Lett. **104**, 261112 (2014).
3. M. W. Mitchell, C. Abellán, and W. Amaya, "Strong experimental guarantees in ultrafast quantum random number generation," Phys. Rev. A **91**, 012314 (2015).
4. Y. Q. Nie, L. Huang, Y. Liu, F. Payne, and J. Zhang, "The gen-

eration of 68 Gbps quantum random number by measuring laser phase fluctuations," Rev. Sci. Instrum. **86**, 063105 (2015).
5. C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, "Generation of fresh and pure random numbers for loophole-free Bell tests," Phys. Rev. Let. **115**, 250403 (2015).
6. D. Frauchiger, R. Renner, and M. Troyer, "True randomness from realistic quantum devices," arXiv (2013).
7. J. Y. Haw, S. M. Assad, A. M. Lance, N. Ng, V. Sharma, P. K. Lam, and T. Symul, "Maximization of Extractable Randomness in a Quantum Random-Number Generator," Phys. Rev. Applied **3**, 054004 (2015).