Quantum Random Number Generation from Shot Noise and Phase-induced Intensity Noise

Robin Camphausen

1 Introduction

Quantum random number generators (QRNGs) are important for a large number of applications, including for finance, communication and computational modelling [1]. One way to generate quantum random numbers (QRNs) is to measure shot noise, which arises due to the quantised nature of light: when observing a light source over a given time frame a discrete number of photons will arrive at the detector and while the average number of photons stays constant there is a variance in the number of arrivals per time frame [2]. It is also possible to generate QRNs by measuring phase noise, which is due to the fact that a spontaneously emitted photon has a completely random phase, uniformly distributed between 0 and 2π [3, 4]. In this report we describe a hybrid QRNG method, which increases the randomness able to be extracted in the Shot noise method by also taking into account the random optical phases of the light source.

2 Phase-induced Intensity Noise

A single spontaneously emitted photon has random phase, but it is of course not possible to measure the phase of a single photon. In references [4–6] therefore, the single spontaneously emitted photon is generated inside a laser cavity, which subsequently uses stimulated emission to generate many copies of this first photon until the light intensity is large enough for an interferometric measurement of the phase. The laser must subsequently be switched off again to allow all stimulated photons in the cavity to decay, so that upon switching it on again a new spontaneously emitted photon with a new random phase can start the same process again. Another way of exploiting the random phase of a spontaneously emitted photon is to measure many of them at once. If all the photons are emitted such that they have statistically independent amplitudes and phases from each other, the resulting sum can be described as a Random Phasor Sum (RPS) [7]:

$$\mathbf{a} = ae^{i\theta} = \frac{1}{\sqrt{N}} \sum_{k=1}^{N} \alpha_k e^{i\phi_k}. \tag{1}$$

Note that this equation is normalised. $\alpha_k/\sqrt{N}$ and ϕ_k are the amplitudes and phases respectively of the K^{th} photon comprising the RPS. In general α_k can take on any distribution with some mean $\overline{\alpha}$ and second moment $\overline{\alpha^2}$. We let ϕ_k be uniformly distributed over $[0, 2\pi)$. As N gets very large, by the central limit theorem $\mathbf{a}$ becomes a Gaussian random variable. In particular, following Chapter 2.9 from [7], the joint density function of the real(imaginary) components $re(im)$ of $\mathbf{a}$ is

$$P_a(re, im) = \frac{1}{2\pi\sigma^2} e^{-\frac{re^2+im^2}{2\sigma^2}}, \tag{2}$$

where $\sigma^2 = \overline{\alpha^2}/2$. Converting this back to the polar coordinates a and θ we obtain

$$P_a(a,\theta) = \begin{cases} \frac{a}{2\pi\sigma^2} e^{-\frac{a^2}{2\sigma^2}}, & \text{if } 0 \leq \theta < 2\pi,\ a > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

Note that this equation is still uniformly distributed for θ. Now for the case of summing up photons, equation 3 describes the distribution of amplitude a and phase θ of a normalised electric field. At a given moment in time τ the instantaneous amplitude(phase) is $a_\tau(\theta_\tau)$, where the mean and variance respectively of a are $\overline{a} = \sqrt{\pi/2}\sigma$ and $\sigma_a^2 = (2 - \pi/2)\sigma^2$.

However, when detecting light we actually measure the intensity $I = |\mathbf{a}|^2$. To find the distribution as well as the mean and standard deviation of the instantaneous intensity I_τ we make the substitution $I_\tau = a_\tau^2$ and use the relation $P_I(I) = P_A(A = \sqrt{I})\,|dA/dI|$, as well as the statistical properties of the mean and variance (Chapter 4.2 [7]):

$$P_I(I) = \begin{cases} \frac{1}{2\sigma^2} e^{-\frac{I}{2\sigma^2}}, & \text{if } I \geq 0, \\ 0, & \text{otherwise,} \end{cases} \tag{4}$$

$$\sigma_I = \overline{I} = 2\sigma^2 = \overline{\alpha^2}. \tag{5}$$

That is to say, even if the amplitude α of the photons being summed has no variation at all (as long as α is non-zero), the resulting instantaneous intensity of the RPS randomly varies with a standard deviation equal to the mean of the intensity ($\sigma_I = \overline{I}$). This variation is therefore known as phase-induced intensity noise (PIIN). Note that this PIIN superficially appears similar to photon shot noise (in particular eq. 5), however there is an important difference: in equation 1 we summed N phasors each with amplitude $\alpha_k/\sqrt{N}$. While we denoted this as the amplitude of individual photons, there is no reason why each individual phasor cannot be composed of many photons: This would be the case if summing many independent laser modes (out of phase with each other) which each individually contain many in-phase photons. In this case the variance due to PIIN would remain the same, whereas the shot noise would be much smaller due to the large number of photons.

3 Measuring PIIN

The RPS from section 2 in fact accurately describes the majority of light sources available today: incandescent light bulbs, light emitting diodes (LEDs) and amplified spontaneous emission (ASE) all generate light from spontaneously emitted photons; this is also known as thermal light. Moreover, it has already been shown that it is possible to measure PIIN and subsequently extract random numbers from it. This was done by directly measuring the intensity fluctuations of an ASE source [8], interfering an ASE source with itself [9] and by measuring the intensty fluctuations of a superluminescent LED (SLED - essentially a semiconductor laser diode without a cavity) [10, 11]. Now, equation 5 refers to the fluctuations in the *instantaneous* intensity produced by a thermal light source. However, any real device that measures light has a finite bandwidth, and therefore integrates the measured intensity over a non-zero period of time. To see how this affects the measurement we start with an intuitive first-order approximation of thermal light as follows: We model a single mode of incoherent light as an ideal monochromatic sine wave, interrupted by random phase shifts every period τ_c, where τ_c is the coherence time (see fig. 1). When two of these thermal modes are added together (this could represent a spontaneous emission source generating two photons at a time, or a laser with two independent modes) the waves interfere causing a different combined intensity for each τ_c period depending on the phase difference between the two modes (see fig. 2).

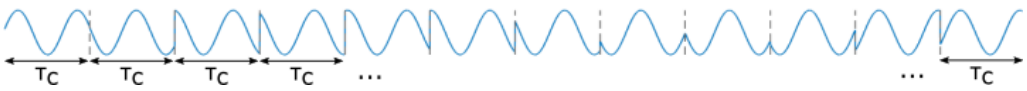

Figure 1: Simple model of a single mode of thermal light: Modelled as a perfect sinusoidal wave interrupted by random phase jumps every coherence time τ_c.

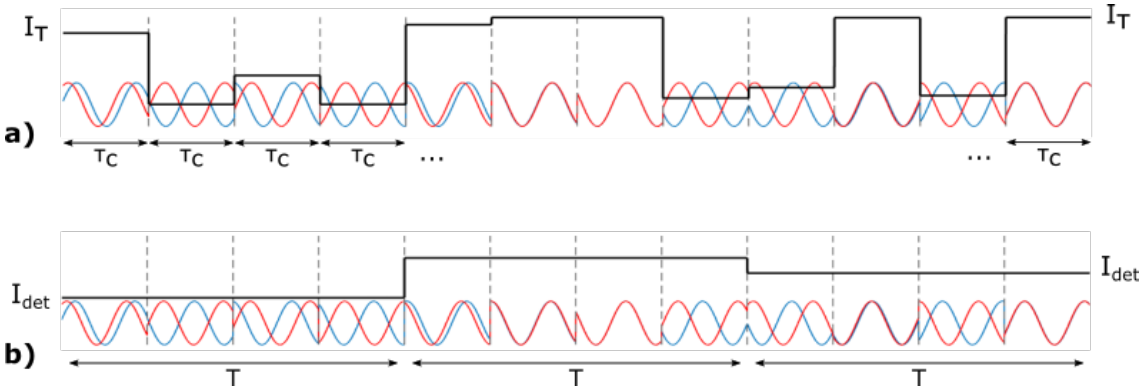

Figure 2: Simple model of the origin and detection of PIIN: when two (or more) modes of thermal light interfere with each other, the random phase jumps will cause a random phase difference between the modes for each period τ_c. **a)** The instantaneous intensity I_τ fluctuates strongly from one coherence period τ_c to the next, due to the modes interfering constructively or destructively depending on the instantaneous phase difference. **b)** When detecting for an integration time T longer than the coherence time (in this case $T = 4\tau_c$) the fluctuations in detected intensity I_{det} weaker, as the integration averages out large fluctuations over multiple coherence times.

The normalised measured instantaneous intensity for each period τ, given some phase difference between the two modes $\Delta\phi$, is $I_\tau = \frac{1+cos(\Delta\phi)}{2}$. Note that $\Delta\phi_k$ is uniformly distributed over $[0, 2\pi)$. However, if the integration time of the detector T is larger than the coherence time τ_c we can define the ratio M as follows:

$$M = T/\tau_c. \tag{6}$$

The normalised detected intensity thus becomes

$$I_{det} = \sum_{m=1}^{M} \frac{1}{M} \frac{1 + cos(\Delta\phi_m)}{2}. \tag{7}$$

Using the statistical properties of the cosine function, and the central limit theorem, we thus obtain the mean and standard deviation of the *measured* intensity:

$$\bar{I}_{det} = \frac{1}{2}, \quad \sigma_{det} = \frac{1}{\sqrt{8M}}. \tag{8}$$

Importantly, what eq. 8 shows is that as the integration time T gets much larger than the coherence time τ_c, the ratio M becomes large and the standard deviation in the detected intensity fluctuation tends to zero. This simple model therefore yields three important conclusions: Firstly, eq. 8 is consistent with our everyday experience, because for thermal light sources commonly encountered (such as incandescent lightbulbs) the coherence time is much shorter than the integration time of the human eye - and thus the PIIN is not readily observed. Secondly it indicates that to extract random numbers from PIIN the light must be measured fast, and indeed the faster it is

measured the more randomness can be extracted. And thirdly, as measured noise is proportional to $1/\sqrt{M} = \sqrt{\tau_c}/\sqrt{T}$, increasing the coherence time of the thermal light source will also increase the measured noise.

Even though we derived eq. 8 for a very simple two-mode light model, the statistical properties of a fully incoherent light source are very similar (see chapter 6 in [7]). In particular, in the limit where $T >> \tau_c$, i.e. of a much longer integration time than coherence time, the measured PIIN is described by

$$\frac{\sigma_{PIIN}}{\overline{I}_{PIIN}} = \frac{1}{\sqrt{M}} = \sqrt{\frac{\tau_c}{T}}. \tag{9}$$

The coherence time τ_c can be approximated in terms of the light source's centre wavelength λ and spectral width $\Delta\lambda$ as follows:

$$\tau_c = \frac{\lambda^2}{c\Delta\lambda}, \tag{10}$$

where c is the speed of light. By substituting λ and $\Delta\lambda$ values for typical incoherent light sources such as LEDs or SLEDs into eq. 10 we can see that τ_c will be on the sub-picosecond timescale. Integration times of photodetectors on the other hand are normally at least two orders of magnitude larger and thus we can apply 9 as we are comfortably in the $T >> \tau_c$ regime. Lastly, note that one will always measure shot noise in addition to PIIN. Further, any real set-up will also measure some technical or system noise, whose origin is not quantum in nature. We can therefore express the total detected noise in terms of PIIN, shot noise and technical noise:

$$\sigma_{total} = \sqrt{\sigma_{PIIN}^2 + \sigma_{shot}^2 + \sigma_{technical}^2}. \tag{11}$$

Now, eqs. 9 and 10 show that for a given integration time a larger PIIN level can be detected for a long coherence time, which in turn requires a narrow source spectral width. The integration time T on the other hand must be kept as low as possible. In past works measuring PIIN in the near-infrared from SLED sources these requirements were met by using a narrowband spectral filter on the source as well as high bandwidth photodiodes and electronics [10, 11].

4 QRNG from PIIN using visible LEDs

While random number generation from PIIN has already been demonstrated for near-infrared wavelengths, this was achieved using bulky, expensive and sensitive components such as a SLED which requires careful optical isolation and precise driving current control. However, to transition to a more affordable and portable solution it would be desirable to use a simple LED light source emitting in the visible, which moreover permits the use of silicon-based photodetection. Unfortunately, as eq. 10 shows, the coherence time of a light source falls quadratically as the wavelength becomes shorter, resulting in more stringent requirements on the integration time and permissible technical noise. At present, single photon avalanche diodes (SPADs) are the only detection technology for the visible wavelength range capable of achieving the low-noise readout and necessary short integration time.

SPADs might at first glance seem a strange choice for measuring intensity fluctuations given that a SPAD is neither particularly cheap nor is it a photon number resolving device - upon detection of light a SPAD emits an electronic pulse that is identical regardless of how many photons initiated the detection event. However the recent rapid advances in SPAD arrays being fabricated using industrial CMOS processes means that both of these objections can be addressed. Firstly regarding cost, while a CMOS-fabricated SPAD array is far more expensive than regular CMOS image sensors available for cameras today, the inherent scalability of optimised CMOS processes coupled with the larger volumes being produced means that costs are already orders of magnitude

lower than a few years ago, and will continue to fall. Secondly, regarding the ability to differentiate between intensities, it is true that one single SPAD only has an effective resolution of one bit. But by evenly spreading the light to be measured across the entire area of a SPAD array the intensity can be measured by the number of SPADs activated by the incoming light. SPAD arrays of size 512×512 pixels have been fabricated thus far, which already gives significant intensity resolution. The method of detecting PIIN that we present in this report therefore needs four main components: a visible wavelength LED source, a narrowband wavelength filter, SPAD array imager, and some optics to distribute the light across the SPAD array. Remembering that according to eq. 11 our set-up will measure the combination of PIIN, shot noise and technical noise, the present scheme can be seen as an extension of the method described in **??**, where random numbers were generated by using a camera to measure the shot noise of an LED. Therefore the proof of principle will be provided by comparing the noise level from only shot noise and technical noise to the noise level when all three types of noise are measured.

References

[1] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, Feb. 2017.

[2] B. Sanguinetti, A. Martin, H. Zbinden, and N. Gisin, "Quantum Random Number Generation on a Mobile Phone," *Physical Review X*, vol. 4, p. 031056, Sept. 2014.

[3] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, "Ultrafast quantum random number generation based on quantum phase fluctuations," *Optics Express*, vol. 20, pp. 12366–12377, May 2012.

[4] C. Abelln, W. Amaya, M. Jofre, M. Curty, A. Acn, J. Capmany, V. Pruneri, and M. W. Mitchell, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," *Optics Express*, vol. 22, p. 1645, Jan. 2014.

[5] M. W. Mitchell, C. Abellan, and W. Amaya, "Strong experimental guarantees in ultrafast quantum random number generation," *Physical Review A*, vol. 91, p. 012314, Jan. 2015.

[6] C. Abelln, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, "Generation of Fresh and Pure Random Numbers for Loophole-Free Bell Tests," *Physical Review Letters*, vol. 115, p. 250403, Dec. 2015.

[7] J. W. Goodman, *Statistical optics*. Wiley classics library, New York: Wiley, wiley classics library ed ed., 2000.

[8] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-Tb/s Physical Random Bit Generators Based on Direct Detection of Amplified Spontaneous Emission Signals," *Journal of Lightwave Technology*, vol. 30, pp. 1329–1334, May 2012.

[9] L. Li, A. Wang, P. Li, H. Xu, L. Wang, and Y. Wang, "Random Bit Generator Using Delayed Self-Difference of Filtered Amplified Spontaneous Emission," *IEEE Photonics Journal*, vol. 6, pp. 1–9, Feb. 2014.

[10] M. Huang, A. Wang, P. Li, H. Xu, and Y. Wang, "Real-time 3gbit/s true random bit generator based on a super-luminescent diode," *Optics Communications*, vol. 325, pp. 165–169, Aug. 2014.

[11] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent LED," *Optics Letters*, vol. 36, p. 1020, Mar. 2011.