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 [**?**]. 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 [**?**]. 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 π [**?**, **?**]. 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 Noise - Random Phasor Sums

A single spontaneously emitted photon has random phase, but it is of course not possible to measure the phase of a single photon.