# A High-Speed Secure Quantum Random Number Generator Based on Vacuum States

**Christian Gabriel[1,2,*], Christoffer Wittmann[1,2], Bastian Hacker[1,2], Wolfgang Mauerer[3], Elanor Huntington[4,5], Metin Sabuncu[1,6], Christoph Marquardt[1,2] and Gerd Leuchs[1,2]**

[1] *Max Planck Institute for the Science of Light, Guenther-Scharowsky-Str. 1, D-91058 Erlangen, Germany*
[2] *Institute of Optics, Information and Photonics, University Erlangen-Nuremberg, Staudtstr. 7/B2, D-91058 Erlangen, Germany*
[3] *Siemens AG, Corporate Technology, Otto-Hahn-Ring 6, 81739 München, Germany*
[4] *Centre for Quantum Computation and Communication Technology, Australian Research Council*
[5] *School of Engineering and Information Technology, The University of New South Wales, Canberra, Australian Capital Territory*
[6] *Department of Electrical and Electronics Engineering, Dokuz Eylül University, Tinaztepe, Buca, 35160 Izmir, Turkey*
[*] *Christian.Gabriel@mpl.mpg.de*

**Abstract:** A high-speed continuous-variable quantum random bit generator with an expected effective bit generation rate of up to 10 GBit/s is presented. The obtained bit sequences are truly random and unique, i.e. they cannot be known by an adversary.



**OCIS codes:** 270.5568, 270.5585

Random number generators (RNGs) have become a vital ingredient for a huge variety of fields. These include simulations as well as the important field of cryptography. Especially in the field of quantum cryptography random numbers are essential for an unconditional secure key distribution [1]. The majority of the RNGs used nowadays are based on computer algorithms or classical physical systems. These have the advantage of high speed bit generation and easy implementation. However, although their produced bit sequences might seem random, they still have a purely deterministic nature. Measurements of pure quantum states, on the other hand, yield completely random outcomes as postulated by quantum mechanics. Therefore, it can be assured that the produced bit sequences are truly random. Using quantum mechanical systems for the generation of random bit sequences has even more advantages: It can be guaranteed that the numbers are unique, i.e. that no potential adversary has knowledge over the generated bit string. To assure this the quantum state for the generation of the bit strings itself has to be secure. This can be guaranteed by either utilizing pure states [2], a detection-loophole free Bell test [3] or a tomographical complete measurement [4]. It should be noted that it is also possible for an adversary to perform a side-attack on the classical noise present in any realistic measurement setup. To prevent this, the bit extraction has to be performed in such a way that any classical noise has no significant influence on the obtained random numbers.

In this report, we present a high-speed quantum RNG (QRNG) based on the measurement of pure vacuum states. The principle idea behind such a QRNG was demonstrated in [2]. Our new QRNG has several distinguished properties, making it a device which meets the requirements modern applications set. Firstly, a detector with sub-shot noise resolution over a 1 GHz bandwidth is employed in the measurement of the quantum noise. Furthermore, a novel data processing alongside with a detailed entropy characterization of the system is introduced. These improvements allow a high-speed as well as a secure bit generation.

Our quantum RNG employs a homodyne detection system to measure the quantum fluctuations of a pure vacuum state. In such a scheme a weak signal, which in our case is a vacuum state, and a strong laser beam, often termed as the local oscillator, are interfered on a symmetric beam splitter. Its two output beams impinge on two balanced detectors. In our setup, which is displayed in Fig. 1a, a combination of a half-wave plate and a polarizing beam splitter substitute the actual beam splitter in order to assure an exact splitting ratio of 50%. The signal of the two detectors is subtracted and fed into an oscilloscope with a 4 GHz analog bandwidth and a 20 GS/s sampling rate. By subtracting the two currents, a quadrature amplitude of the vacuum state is measured. The oscilloscope samples the time signal of the vacuum fluctuations which in principle should be random and uncorrelated. However, the electronic noise of the detector and oscilloscope modify the signal with their non-uniform, frequency-dependent spectrum. Therefore, data post-processing steps are required. We perform the data extraction with the quantum fluctuations occurring at each

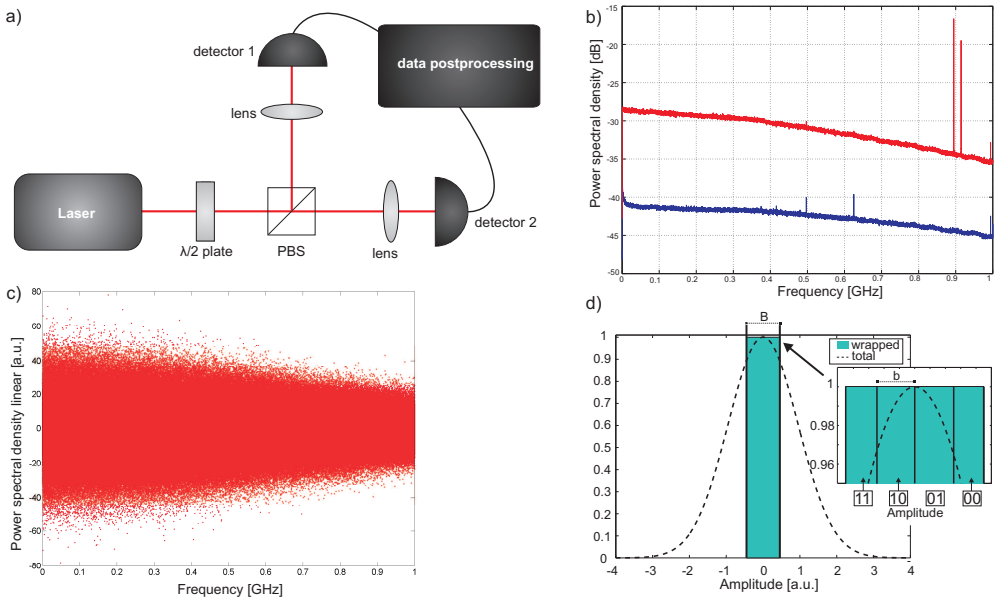


Fig. 1. a) The experimental setup of the QRNG. b) The power spectrum of the vacuum fluctuations (red) and the electronic noise (blue). c) typical real parts after the DFT. d) illustrates the wrapping scheme applied to the Gaussian probability distribution of the total noise at one frequency. Here $n$ bits are assigned to a bin of width $b$. The pattern is repeated after a length of $B = b \cdot 2^n$. This is performed over the whole probability distribution and therefore a uniform distribution is achieved.

single frequency respectively. For this purpose a discrete Fourier transform (DFT) is applied to the measured time signal. The real and imaginary parts of the DFT are independent variables and therefore both can be utilized for the randomness extraction. The DFT is performed with a resolution bandwidth of 0.1 MHz. The amplitude fluctuations at each frequency component are, due to quantum mechanics, absolutely random and follow a Gaussian probability distribution. At certain frequencies the detector has a pick-up signal from an external noise source, for example mobile phone up- and down-links. These frequencies are omitted. The power spectrum as well as the real part of the DFT are displayed in Fig. 1b-c respectively.

To extract bits from the measured signal an equidistant spacing of width $b$ is applied to a length $B = b \cdot 2^n$ of each of the probability distributions. Here $n$ is the number of bits assigned to each measurement value within one bin of width $b$. The pattern is repeated after each length $B$. This scheme has the advantage that if $B$ is chosen small enough a uniform distribution is achieved, i.e. that the numbers are not biased. A detailed entropy model is applied to the system, allowing us to carefully characterize how much information is suited for true random number generation. This includes the determination of the conditional Min-entropy. This gives a value for how much of the total measured noise is not controlled by classical noise. Furthermore, the extractable information of the generated bit string is determined. This examines the information loss if the distributions is not perfectly uniform. A one-way hashing function has to be applied to the raw bit strings to reduce its information content by the appropriate amount. After that the resulting bits only contain information from quantum effects.

The high-speed detector and the new bit extraction method allow an expected random bit extraction speed of up to 10 GBit/s. The produced bits solely arise from quantum noise and are therefore truly random. Furthermore, we have exploited a pure vacuum state as our noise source, i.e. that our random numbers are also unique.

## References

1. N. Gisin *et al.*, "Quantum cryptography," Reviews of Modern Physics **74**, 145–195 (2002).
2. C. Gabriel *et al.*, "A generator for unique quantum random numbers based on vacuum states," Nature Photonics **4**, 711–715 (2010).
3. S. Pironio *et al.*, "Random numbers certified by Bell's theorem." Nature **464**, 1021–4 (2010).
4. M. Fiorentino *et al.*, "Secure self-calibrating quantum random-bit generator," Physical Review A **75** (2007).