A compact random number generator based on optical homodyne detection

YICHENG SHI,[1] BRENDA CHNG,[1], CHRISTIAN KURTSIEFER,[1,2,*]

[1] *Center for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore, 117543*
[2] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore, 117542*
[*] *christian.kurtsiefer@gmail.com*

References and links

1. N. Metropolis. The beginning of the monte carlo method. *Los Alamos Science*, 15:125–130, 1987.
2. Francis Galton. Dice for statistical experiments. *Nature*, 42(1070):13âĂŞ14, May 1890.
3. Benjamin Jun and Paul Kocher. The intel random number generator. Technical report, Cryptography Research Inc., 1999.
4. Michael Gude. Concept for a high performance random number generator based on physical random phenomena. *Frequenz*, 39:187, 1985.
5. A. Figotin, I. Vitebskiy, V. Popovich, G. Stetsenko, S. Molchanov, A. Gordon, J. Quinn, and N. Stavrakas. Random number generator based on the spontaneous alpha-decay, June 1 2004. US Patent 6,745,217.
6. M. Stipcevic and B. Medved Rogina. Quantum random number generator based on photonic emission in semiconductors. *Rev. Sci. Instrum.*, 78:045104, 2007.
7. Michael A. Wayne, Evan R. Jeffrey, Gleb M. Akselrod, and Paul G. Kwiat. Photon arrival time quantum random number generation. *Journal of Modern Optics*, 56(4):516–522, 2009.
8. Martin Fürst, Henning Weier, Sebastian Nauerth, Davide G. Marangon, Christian Kurtsiefer, and Harald Weinfurter. High speed optical quantum random number generation. *Optics Express*, 18(12):13029, 2010.
9. Michael A. Wayne and Paul G. Kwiat. Low-bias high-speed quantum random number generator via shaped optical pulses. *Opt. Express*, 18(9):9351–9357, Apr 2010.
10. Michael Wahl, Matthias Leifgen, Michael Berlin, Tino RoÌĹhlicke, Hans-JuÌĹrgen Rahn, and Oliver Benson. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters*, 98(17):171105, 2011.
11. You-Qi Nie, Hong-Fei Zhang, Zhen Zhang, Jian Wang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Applied Physics Letters*, 104(5):051110, Feb 2014.
12. Min Ren, E Wu, Yan Liang, Yi Jian, Guang Wu, and Heping Zeng. Quantum random-number generator based on a photon-number-resolving detector. *Physical Review A*, 83(2):023820, Feb 2011.
13. Daniela Frauchiger and Renato Renner. Truly random number generation: an example. *Proc. SPIE*, 8899:88990S–88990S–7, 2013.
14. Caitlin R. S. Williams, Julia C. Salevan, Xiaowen Li, Rajarshi Roy, and Thomas E. Murphy. Fast physical random number generator using amplified spontaneous emission. *Optics Express*, 18(23):23584, Oct 2010.
15. Ido Kanter, Yaara Aviad, Igor Reidler, Elad Cohen, and Michael Rosenbluh. An optical ultrafast random bit generator. *Nature Photon*, 4(1):58âĂŞ61, Dec 2009.
16. Bruno Sanguinetti, Anthony Martin, Hugo Zbinden, and Nicolas Gisin. Quantum random number generation on a mobile phone. *Phys. Rev. X*, 4:031056, Sep 2014.
17. You-Qi Nie, Leilei Huang, Yang Liu, Frank Payne, Jun Zhang, and Jian-Wei Pan. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. *Review of Scientific Instruments*, 86(6):063105, Jun 2015.
18. Bing Qi, Yue-Meng Chi, Hoi-Kwong Lo, and Li Qian. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Opt. Lett.*, 35(3):312, Jan 2010.
19. Feihu Xu, Bing Qi, Xiongfeng Ma, He Xu, Haoxuan Zheng, and Hoi-Kwong Lo. Ultrafast quantum random number generation based on quantum phase fluctuations. *Optics Express*, 20(11):12366, May 2012.
20. C. Abellán, W. Amaya, M. Jofre, M. Curty, A. AcÃŋn, J. Capmany, V. Pruneri, and M. W. Mitchell. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Optics Express*, 22(2):1645, 2014.
21. Carlos Abellán, Waldimar Amaya, Daniel Mitrani, Valerio Pruneri, and Morgan W. Mitchell. Generation of fresh and pure random numbers for loophole-free bell tests. *Phys. Rev. Lett.*, 115:250403, Dec 2015.
22. Z. L. Yuan, M. Lucamarini, J. F. Dynes, B. FrÃűhlich, A. Plews, and A. J. Shields. Robust random number generation using steady-state emission of gain-switched laser diodes. *Applied Physics Letters*, 104(26):261112, Jun 2014.
23. Hongyi Zhou, Xiao Yuan, and Xiongfeng Ma. Randomness generation based on spontaneous emissions of lasers. *Physical Review A*, 91(6):062316, Jun 2015.

24. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri. True random numbers from amplified quantum vacuum. *Optics Express*, 19(21):20665, Oct 2011.
25. Christian Gabriel, Christoffer Wittmann, Denis Sych, Ruifang Dong, Wolfgang Mauerer, Ulrik L. Andersen, Christoph Marquardt, and Gerd Leuchs. A generator for unique quantum random numbers based on vacuum states. *Nature Photon*, 4(10):711âĂŞ715, Aug 2010.
26. T. Symul, S. M. Assad, and P. K. Lam. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters*, 98(23):–, 2011.
27. Yong Shen, Liang Tian, and Hongxin Zou. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Physical Review A*, 81(6):063814, Jun 2010.
28. Yicheng Shi, Brenda Chng, and Christian Kurtsiefer. Random numbers from vacuum fluctuations. *Applied Physics Letters*, 109(4):041101, Jul 2016.
29. Hugo Krawczyk. Lfsr-based hashing and authentication. *Advances in Cryptology âĂŤ CRYPTO âĂŹ94*, page 129âĂŞ139, 1994.
30. Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. National Institute of Standards and Technology, April 2010.
31. David Bauer Robert G. Brown, Dirk Eddelbuettel. Dieharder: A random number test suite, 2004.

Abstract: We implement a quantum random number generator based on a balanced homodyne measurement of vacuum fluctuations of the electromagnetic field. We used wave front splitting of the local oscillator instead of amplitude splitting in order to simplify the optical setup. The digitized noise signal is processed with a fast randomness extraction scheme based on a linear feedback shift register. The random bit stream is continuously read in a computer at a rate of about 480 Mbit/s and passes an extended test suite for random numbers.

1. Introduction

Generating high quality and trusted random numbers is an essential task in various cryptographic schemes and many other fields such as Monte Carlo simulations [1] and various randomized algorithms. Algorithmically generated pseudo-random numbers are available at very high rates and can be easily implemented in software, but they are deterministic in nature and therefore are not suitable for cryptographic purposes. As an alternative, hardware random number generators have been used [2,3]. They measure noisy physical processes and convert the outcome into random numbers. Since it is impossible to predict the outcome of such measurements, these physically generated random numbers are more trusted compared to pseudo-random numbers.

Quantum random number generators (QRNG) is a class of hardware random number generators whose source of randomness is the outcome of quantum measurements. Early implementations of QRNGs made use of decay statistics of radioactive nuclei [4, 5]. A number of more recent implementations using quantum optical measurements have been reported. These include measuring photon number statistics [6–12], scattering events of single photons by a beam splitter [13], amplified spontaneous emission of a fiber amplifier [14]. QRNGs based on measuring the intensity [15, 16] and phase noise [17–24] of different light sources have also been reported.

In this paper we report on a QRNG implementation based on measuring the vacuum fluctuations of the electromagnetic field, which has been reported in [25–28]. Such measurements are known for their high bandwidth and simple optical setup. In this paper, we simplify the optical setup of the homodyne detector down to only a laser diode and two photodiodes without using light splitting components. Combined with an efficient randomness extractor, we are able to generate unbiased and uncorrelated stream of random bits at a high rate, but now with a much simpler optical setup.

2. Optical homodyne measurement by wavefront splitting

The QRNG based on measuring vacuum fluctuations of the electromagnetic field uses an balanced homodyne detector. A conventional setup consists of a laser diode (LD) as a local oscillator, a 50:50 beam splitter (BS), and two photodiodes (PD_1, PD_2). A collimation lens and a mirror is also used to steer and guide the laser beam.

Fig. 1 (b) shows the schematic of a conventional balanced homodyne detector. The local oscillator (LO) in mode a enters the BS and is directed onto two photodiodes and the photocurrent difference is measured. This setup maps fluctuations of electrical field in mode b to the photocurrent difference $i_1 - i_2$. When probing the vacuum fluctuations of EM fields, the input mode b of the BS is kept empty (i.e. mode b is at $|0\rangle$).

A core requirement for a balanced homodyne detection is the mixing of mode a and b at the beam splitter, which is governed by the following matrix

$$\begin{pmatrix} \tilde{E}_c \\ \tilde{E}_d \end{pmatrix} = M \begin{pmatrix} \tilde{E}_a \\ \tilde{E}_b \end{pmatrix} \quad \text{where} \quad \mathrm{M} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \tag{1}$$

Where $\tilde{E}_{a,\,b,\,c,\,d}$ represents the oscillating electrical fields at modes a, b, c, d. This matrix relation is ensured by the boundary conditions of the electromagnetic fields between the dielectric media of the beam splitter. The mixing of mode a and b also requires good overlap of their spatial profile as well as their frequency. Although measuring the vacuum state does not need to go through this non-trivial process, careful placement and tuning of optical components are still needed.

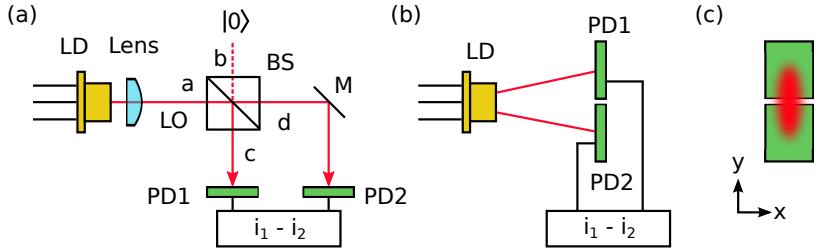

Fig. 1. Splitting mechanisms of the two different implementations. A conventional balanced homodyne detection scheme (a) relies on the beam splitter matrix relation between the input modes a, b and the output modes c, d. In the wavefront-splitting implementation (b), this is replaced by spatially splitting the elliptical transverse mode of a laser beam.

We can simplify the setup of the balanced homodyne detector by using a different mode decompositon of the local oscillator, thus replacing the beam splitter matrix in (1). Fig.1 (b) shows the simplified setup that we propose. A pair of square shaped photodiodes are placed adjacent to each other are directly exposed to the laser beam, each receiving approximately half of the laser beam spot. The optical mode from the laser diode is typically of elliptical transverse profile and for simplicity, the electrical field amplitude at the photodiode surface can be approximated by

$$\tilde{E}_l(x,y,t) = \hat{E}_0 \cdot g(x,y,t) = \hat{\epsilon} E_0 (e^{-i\omega t} \cdot e^{-x^2/{w_x}^2} \cdot e^{-y^2/{w_y}^2}) \tag{2}$$

where ϵ is the polarization vector, and E_0 is the global field amplitude. The term $e^{-x^2/{w_x}^2} \cdot e^{-y^2/{w_y}^2}$ describes a transverse beam profile of a 2D gaussian distribution with different parameters ω_x, ω_y along x, y directions. The function $g(x,y,t) = e^{-i\omega t} \cdot e^{-x^2/{w_x}^2} \cdot e^{-y^2/{w_y}^2}$ describes the optical mode of the local oscillator.

We now introduce a somewhat similar mode function $h(x,y,t)$ which is manually defined as

$$h(x,y,t) = g(x,y,t) \cdot \begin{cases} +1 & for \quad y > 0 \\ -1 & for \quad y < 0 \end{cases} \tag{3}$$

It is clear that $h(x,y,t)$ is orthogonal to $g(x,y,t)$ since $\int g(x,y,t) \cdot h(x,y,t) \mathrm{d}x^3 = 0$, thus the two modes can be considered as independent harmonic oscillators. Consider a second field in mode h, $\tilde{E}_v = \hat{\epsilon} E_1 \cdot h(x,y,t)$ is being mixed with the local oscillator at mode g. The electrical field on the "upper half" ($y > 0$) and "down half" ($y < 0$) can be written as

$$\begin{aligned} \tilde{E}_{up} &= \hat{\epsilon}(E_0 + E_1) \cdot \begin{cases} g(x,y,t) & for \quad y > 0 \\ 0 & for \quad y < 0 \end{cases} \\ \tilde{E}_{down} &= \hat{\epsilon}(E_0 - E_1) \cdot \begin{cases} 0 & for \quad y > 0 \\ g(x,y,t) & for \quad y < 0 \end{cases} \end{aligned} \tag{4}$$

It it easy to see that Equation (4) reproduce the beam splitter matrix in (1). The photocurrent difference $i_1 - i_2$ shown in Fig.1 (b) now maps to the vacuum fluctuations of an electromagnetic field with a mode function $h(x,y,t)$, which is kept at vacuum state. The mixing of the two modes is automatically ensured since the vacuum field is present everywhere.

In contrast to a conventional homodyne detector based on amplitude splitting of fields through beam splitter, we use the splitting of wave front of the laser beam and thus eliminated the usage of beam splitting components. The setup is now much simplified compared to those in [25–28] and the non-trivial alignment procedures can be avoided.

3. Implementation

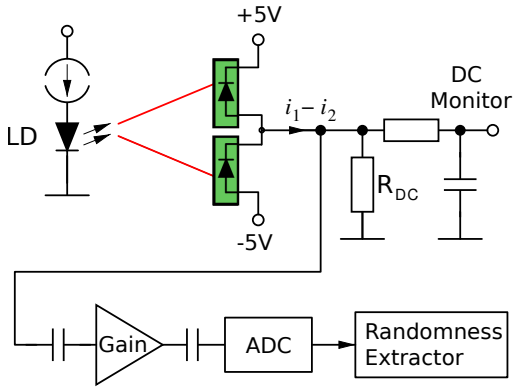

Fig. 2. Amplified noise levels measured into a resolution bandwidth $B = 60$ kHz. The red trace is the amplified photocurrent difference $i_1 - i_2$, with equal optical power impinging on both photodiodes. The blue trace corresponds to the electronic noise which is measured without any optical input.

Figure 2 schematically shows the balanced homodyne detection setup of our QRNG. A continuous wave laser (wavelength 780 nm) is used as the local oscillator for the vacuum fluctuations. The beam from the laser diode impinges directly onto a pair of photodiodes (OSRAM SFH2701). The sensitive area of the two photodiodes are two 0.6×0.6 mm squares and are placed next to each other with a 1 mm gap in between.

The laser diode casts an elliptical beam spot of about 2.5 mm long and 0.7 mm wide, which covers the two photodiodes. A fraction of the optical power is received by the two photodiodes. By carefully adjusting the position of the beam spot, we are able to balance the optical power

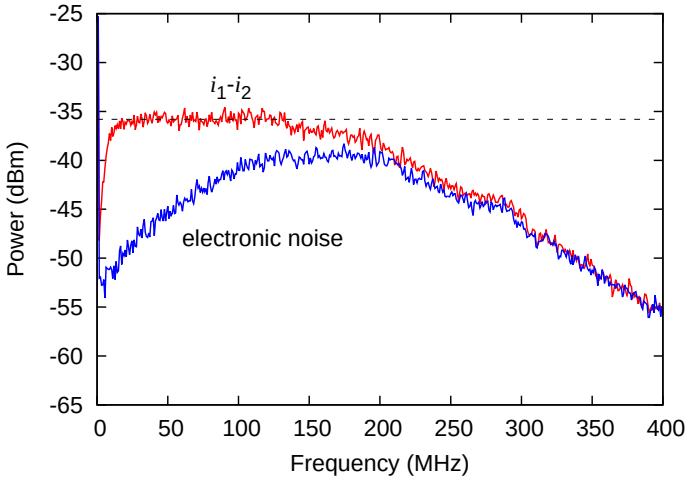

Fig. 3. Amplified noise levels measured into a resolution bandwidth $B = 100$ kHz. The red trace is the amplified photocurrent difference $i_1 - i_2$, with equal optical power impinging on both photodiodes. The blue trace corresponds to the electronic noise which is measured without any optical input.

received by the two diodes. The fluctuations of photocurrent difference $\Delta(i_1 - i_2)$ is amplified by a transimpedance amplifier (Analog Devices AD8015) followed by two wideband RF differential amplifiers (Analog Devices AD8351). The entire amplifier chain has a calculated effective transimpedance of $R_{\text{eff}} \approx 1\,\text{M}\Omega$.

Fig 3 shows the measured total noise output (red trace) which has a relative flat power density range from about 10 MHz to 150 MHz. The lower end of the band is set by the AC coupling capacitors in the gain block while the high end is determined by the cut-off frequency of the amplifiers. As a comparison, the electronic noise (blue trace) is measured with the laser diode switched off. The signal to noise ration is found to be over 10 dB at lower frequencies (0-50 MHz) and around 5 dB at higher frequencies (50-100 MHz) and we conclude that the total noise is dominated by quantum fluctuations.

The amplified noise signal is digitized into signed 12 bit words at a sampling rate of 200 MHz with an analog to digital converter (ADC, Analog Devices AD9634). The normalized autocorrelation evaluated over 10^7 samples is shown in Fig 4. The autocorrelation measured up to a delay of $d = 100$ is on the order of 10^{-4} which is below the 2σ confidence level. Residual correlation is observed for $d < 10$ and is a consequence of the finite bandwidth of the noise signal (150 MHz) and the high sampling rate of the ADC (200 MHz).

4. Entropy estimation and randomness extraction

We estimate the entropy in the raw data to help determine the amount of extractable randomness from our QRNG. Two different definitions of entropy are used here. An upper bound of randomness is given by the Shannon entropy, and the min-entropy is computed to set an lower bound.

For this setup, we followed the same assumptions made in our previous work [28] which assumes that the measured total noise signal $X_t = X_q + X_e$ is the sum of independent random variables X_q for the quantum noise, and X_e for the electronic noise. The three variables X_q, X_e and X_t are assumed to follow Gaussian distributions and take discrete values between -2^{11} and $2^{11} - 1$. Considering the worst case scenario that an adversary has full knowledge of the

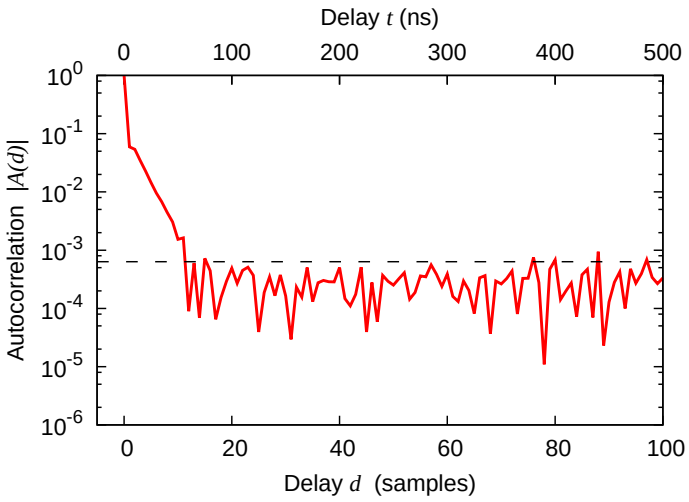

Fig. 4. Autocorrelation of the total noise signal sampled at 200 MHz, computed over 10^7 samples (solid line), compared with the 2σ confidence level (dashed line).

electronic noise, the conditional Shannon entropy in this case is

$$H(X_t|X_e) = H(X_q + X_e|X_e) = H(X_q|X_e) = H(X_q) \tag{5}$$

A variance of $\sigma_q^2 = \sigma_t^2 - \sigma_e^2 \approx 531.6^2$ is calculated for X_q. For such a Gaussian distribution with $\sigma_q \gg 1$, the Shannon entropy can be computed as

$$\begin{aligned} H_S(X_q) &= \sum_{x=-2^{11}}^{2^{11}-1} -p_q(x)\log_2 p_q(x) \\ &\approx \int_{-\infty}^{+\infty} -f(x)\log_2 f(x)\,\mathrm{d}x = \log_2(\sqrt{2\pi e}\,\sigma_q) \\ &\approx 11.1\text{bits} \end{aligned} \tag{6}$$

The min-entropy of the quantum noise X_q is computed as

$$\begin{aligned} H_\infty(X_q) &= -\log_2(\max[p_q(x)]) \\ &\approx \log_2(\sqrt{2\pi}\sigma_q) \\ &\approx 10.38\text{bits} \end{aligned} \tag{7}$$

The Shannon entropy $H_S(X_q)$ and min-entropy $H_\infty(X_q)$ set up the upper and lower bound of extractable randomness. We use a randomness extractor based on a Linear Feedback Shift Register (LFSR) which has been reported in our previous work [28]. The extractor is equivalent to multiplying an input stream of 63 bits to a 63×63 Toeplitz matrix generated from a LFSR and is shown to be a valid hashing function [29]. The low complexity of this extractor allows it to be easily implemented either in high speed or low power technology. This scheme can be par- allelized using 126 register cells, capable of receiving up to 63 injected raw bits per clock cycle to even further speed up the process.

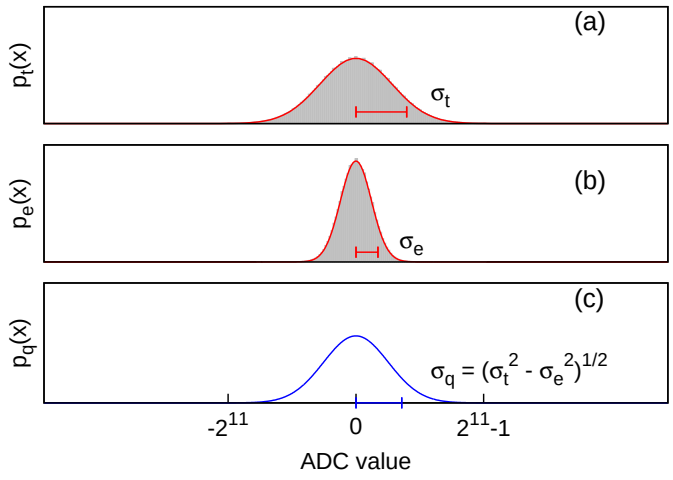

Fig. 5. Probability distribution of the measured total noise with variance $\sigma_t{}^2$ (a), electronic noise with variance $\sigma_e{}^2$ (b), and the estimated quantum noise with variance $\sigma_q{}^2$ (c). The filled areas in (a), (b) show the actual measurements over 10^7 samples, the solid lines fit to Gaussian distributions.

5. Performance

We apply the statistical test suite from NIST [30], and the "Die-harder" randomness test battery [31] to evaluate the quality of the extracted random numbers. Our RNG output passed both tests consistently when evaluated over a sample of 400 Gigabit in the sense that occasional weak outcomes of some tests do not repeat.

Our implementation has an output rate of about 480 Mbit/s of uniformly distributed random bits, with the digitizer unit sampling at 200 MHz and randomness extraction ratio of 66%; this is limited by the speed of the data transmission protocol (USB2.0). Although significantly higher generation rates have been reported recently [14, 17, 19], our design is by far the most compact and with moderate effort, our random number generation rate can be greatly increased by extending the bandwidth of the photodi- odes, amplifiers, and digitizer devices.

6. Conclusion

In summary, we demonstrated a random number generation scheme by measuring the vacuum fluctuations of the electromagnetic field. By using wave front splitting instead of amplitude splitting, we eliminated the usage of any beam splitting optics in our setup. By estimating the amount of usable entropy from quantum noise and using an efficient randomness extractor based on a linear feedback shift register, we can generate uniformly distributed random numbers at a high rate from a fundamentally unpredictable quantum measurement.