Quantum random number generation using an on-chip linear plasmonic beamsplitter

C Strydom and M S Tame

Department of Physics, SU, Matieland 7602, RSA

E-mail: `conradstryd@gmail.com`

Abstract. True random numbers are essential in cryptography, simulation and many other information processing tasks. Here we experimentally demonstrate quantum random number generation with an on-chip linear plasmonic beamsplitter to generate true random numbers. The beamsplitter has a footprint of $2\,\mu\text{m}\times 25\,\mu\text{m}$ and is more compact than a previous demonstration, with a reduction in size by a factor of 2, thereby reducing the impact of loss. At the input grating of the beamsplitter, free-space single photons are converted into single surface plasmon polaritons which propagate along one of two gold stripe waveguides to one of two output gratings where they are converted back into photons. The value of each random bit is determined by the output at which each photon is detected. In our experiment, we achieved a random number generation rate of 2.86 Mbits/s, despite the presence of loss. By applying randomness extraction in the form of a deterministic shuffle followed by the recursive von Neumann algorithm to our raw bits, we obtained a sample of bits which passed the ENT and NIST Statistical Test Suites.

1. Introduction

Random numbers are ubiquitous in cryptography, simulation and coordination in computer networks, to name but a few [1]. However, they are very difficult to generate reliably using classical hardware, as the unpredictability relies on incomplete knowledge, which can introduce ordered features and compromise their utility. In contrast, the inherent randomness of quantum mechanics makes quantum hardware ideal for generating random numbers [1]. Studies have confirmed that in many important applications, such as molecular Monte Carlo simulations [2], results obtained with poor quality classical pseudorandom number generators can deviate significantly from those obtained with true quantum random number generators. While high quality pseudorandom number generators exist, they are extremely resource intensive [3]. This has led to an increasing interest in the development of dedicated quantum hardware for random number generation. In particular, quantum random number generation has been successfully realised experimentally in a great variety of physical settings, ranging from cloud-based superconducting quantum computers [4] to photonic integrated circuits [5].

It was also recently shown that a truly random sample of bits can be generated using an on-chip plasmonic beamsplitter [6]. The main advantage of plasmonic hardware [7] is that it allows light to be confined below the diffraction limit, which enables a significant reduction in device footprints compared to the dielectric hardware conventionally used in photonic integrated circuits. In this work, we investigate quantum random number generation with an on-chip linear plasmonic beamsplitter. Our linear plasmonic beamsplitter is more compact than the cross-shaped plasmonic beamsplitter used in Ref. [6], with a reduction in size by a factor of 2. In our experiment, free-space single photons focused onto the input grating of the on-chip linear plasmonic beamsplitter randomly couple into one of its two gold stripe waveguides, allowing us to obtain random bits. By applying standard randomness extraction protocols to raw bits generated at a rate of 2.86 Mbits/s, we obtained a sample of processed bits with a marginally reduced effective generation rate of 2.85 Mbits/s which passed industry standard tests. Our work successfully demonstrates the use of a highly compact on-chip plasmonic component for quantum random number generation and will be of interest to researchers developing plasmonic components for this and other important quantum information processing tasks [7].

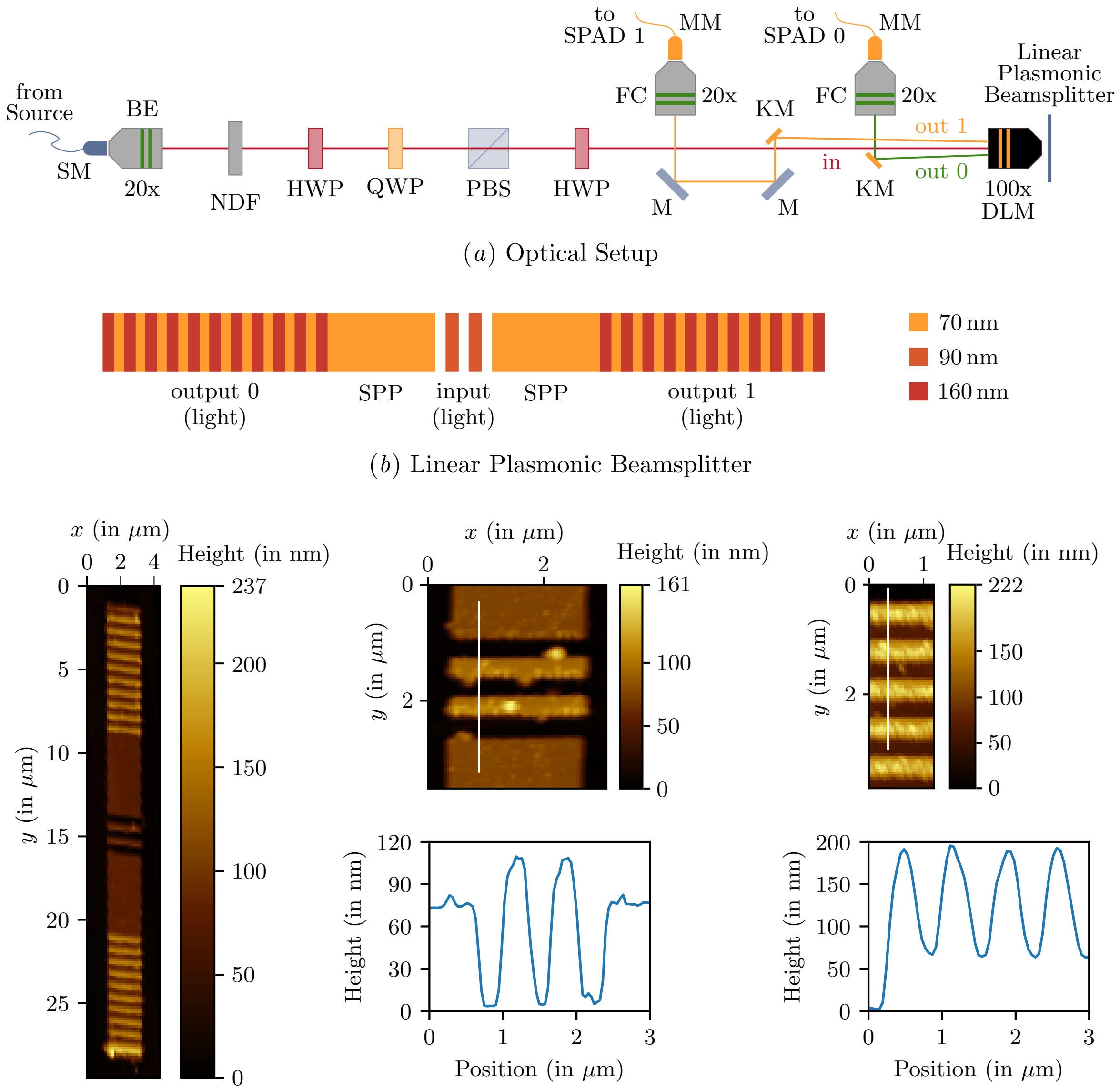
2. Experimental setup

The optical experimental setup for generating random numbers with an on-chip linear plasmonic beamsplitter is shown in figure 1(a) and a diagram of the beamsplitter used in our experiment is shown in figure 1(b). Our on-chip linear plasmonic beamsplitter has a footprint of just $2\,\mu$m × $25\,\mu$m, making it a highly compact device. It comprises a central 2-step input grating, with a $2\,\mu$m wide gold stripe waveguide and an 11-step output grating on either end. Each output grating has a period of 740 nm. The gold linear plasmonic beamsplitter is fabricated on a 0.17 mm thick silica glass substrate with a refractive index of $n = 1.5255$ using a combination of electron beam lithography and electron beam evaporation, as described in Ref. [6]. Figure 1(c) shows atomic force microscope (NT-MDT Smena) images of the final fabricated structure.

The light source used in our experiment is a continuous-wave laser (Thorlabs LPS-785-FC), with a vacuum wavelength of $\lambda_0 = 785\,$nm and a frequency bandwidth of $\delta\nu = 5.36\,$THz, operating above the lasing threshold. Polarised coherent laser light is injected into the optical setup in figure 1(a) via a beam expander (BE), which is connected to the continuous-wave laser by a polarisation-preserving single-mode optical fibre (SM). In our setup, the beam is first sent through a neutral density filter (NDF), which attenuates the coherent laser light down to the single-photon level, as will be explained later. The photons then pass through a half-wave plate (HWP), a quarter-wave plate (QWP), a polarising beamsplitter (PBS) and another HWP, which are used to refine and control their polarisation. A 100x diffraction limited microscope (DLM) objective is used to focus these free-space single photons onto the input grating of the on-chip linear plasmonic beamsplitter (a diffraction-limited spot of approximately $2\,\mu$m) where they are converted into single surface plasmon polaritons (SPPs). The single SPPs propagate along one of the two gold stripe waveguides of the linear beamsplitter to one of its two output gratings, where they are converted back into photons.

Out-coupled photons from the two output gratings of the beamsplitter are collected by the same DLM objective that was used to focus input photons onto its input grating, and are then reflected into fibre couplers (FCs) by knife-edge mirrors (KMs). Each FC is connected to a single-photon avalanche diode (SPAD) detector (Excelitas SPCM-AQRH-15), with a dead time of $T_d = 24\,$ns, by a multi-mode optical fibre (MM). Each SPAD detector is in turn connected to a channel of a Picoquant TimeHarp 260, which can measure the arrival time of a photon at a detector to a precision of 25 ps. The arrival of a photon at one detector or the other results in the generation of a bit (either 0 or 1). Hence it is the process by which a free-space single photon, focused onto the input grating of the linear plasmonic beamsplitter, randomly couples into one of its two gold stripe waveguides which ultimately allows us to obtain a random bit.

The attenuation of the coherent laser source by the NDF ensures that the linear plasmonic beamsplitter is operating in the single-excitation regime so that single-photon splitting is realised at its input grating. We can model the attenuated light entering the linear plasmonic beamsplitter as a weak coherent state $|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle$, with mean excitation number $\langle\hat{n}\rangle = |\alpha|^2 \ll 1$ [6]. The photon number distribution is given by $p_n = e^{-|\alpha|^2}\frac{|\alpha|^{2n}}{n!}$, where p_0 and p_1 are the dominant components since $|\alpha|^2 \ll 1$. The use of a SPAD detector at each output of the



(a) Optical Setup

(b) Linear Plasmonic Beamsplitter

(c) Atomic Force Microscope Images

Figure 1. Quantum random number generation using an on-chip linear plasmonic beamsplitter. (a) Optical Setup shows the optical experimental setup for generating random numbers with an on-chip linear plasmonic beamsplitter. Legend for labels: single-mode optical fibre (SM), beam expander (BE), neutral density filter (NDF), half-wave plate (HWP), quarter-wave plate (QWP), polarising beamsplitter (PBS), diffraction-limited microscope (DLM), knife-edge mirror (KM), mirror (M), fibre coupler (FC), multi-mode optical fibre (MM), single-photon avalanche diode detector (SPAD). (b) Linear Plasmonic Beamsplitter shows a diagram of the on-chip linear plasmonic beamsplitter used in our experiment. (c) Atomic Force Microscope Images shows atomic force microscope images of the linear plasmonic beamsplitter (left), its input grating (top centre) and its top output grating (top right), as well as height profiles of its input grating (bottom centre) and its top output grating (bottom right).

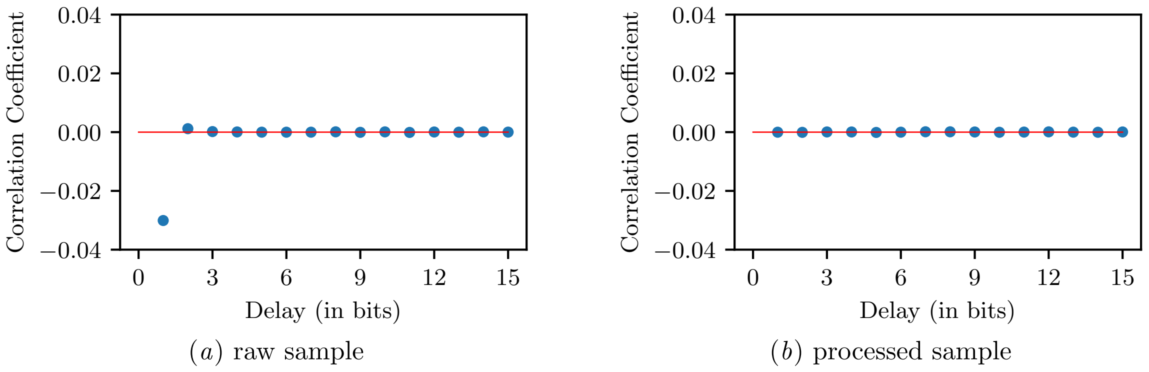
beamsplitter removes the vacuum component p_0 by post-selection so that only the single-photon component p_1 remains (with $p_i \approx 0$ for $i \geq 2$).

The random number generation rate is determined by the light intensity at which the setup is operated. While increasing the light intensity increases the generation rate, there are two important considerations which limit the light intensity [6]. Firstly, to ensure that the mean photon number $\langle \hat{n} \rangle \ll 1$ for light entering the linear plasmonic beamsplitter, the rate at which photons enter the beamsplitter, r, must be much less than the reciprocal of the coherence time, τ, of the source. For our continuous-wave laser, $\tau = \sqrt{2 \ln 2}/\pi\delta\nu = 7.00 \times 10^{-14}\,\mathrm{s}$, and using the method proposed in Ref. [6], we determined that $r = 1.20 \times 10^{9}\,\mathrm{s}^{-1}$ for our chosen light intensity. Hence $r \ll \frac{1}{\tau} = 1.43 \times 10^{13}\,\mathrm{s}^{-1}$, as required. Secondly, to ensure that the majority of photons arriving at each SPAD detector are detected, the photon detection rate, R, for each detector must be much less than the reciprocal of T_d. For our chosen light intensity, $R = 1.4 \times 10^{6}\,\mathrm{s}^{-1}$ for both detectors, so that $R \ll \frac{1}{T_d} = 4.2 \times 10^{7}\,\mathrm{s}^{-1}$. We were able to acquire 171,543,801 bits in 60 s, giving a random number generation rate of about 2.86 Mbits/s. In what follows, we will refer to the first 170 Mbits as the raw sample.

3. Results

The Pearson correlation coefficient [8] of the raw sample with 1-bit to 15-bit delays of itself is plotted in figure 2(a). The Pearson correlation coefficient ranges from -1 to 1, where a positive value indicates a positive correlation and a negative value indicates a negative correlation, while a value close to 0 suggests that no correlation is present. Hence we find that small negative correlations exist between adjacent bits in the raw sample, while short-ranged correlations between non-adjacent bits are negligible. The correlations between adjacent bits can likely be attributed to SPAD detector imperfections [6]. In the raw sample, the relative frequency of zeros is 0.49527 and the relative frequency of ones is 0.50473. Hence the raw sample shows a small bias towards one. This is likely a result of asymmetry in the linear plasmonic beamsplitter and collection optics [6].

We first deterministically rearranged or shuffled the 171,543,801 raw bits generated using our on-chip linear plasmonic beamsplitter in an attempt to remove the correlations between adjacent bits, and then applied the recursive von Neumann algorithm [9] to the shuffled bits in an attempt to remove the bias. In what follows, we will refer to the first 170 Mbits of the resulting sample of 170,925,124 processed bits as the processed sample. The von Neumann scheme constructs an unbiased sample of bits from a biased sample by mapping the bit-pairs 01 and 10, which occur with equal probability in a biased sample in which adjacent bits are uncorrelated, to



(a) raw sample

(b) processed sample

Figure 2. Pearson correlation coefficient of the (a) raw sample and (b) processed sample with 1-bit to 15-bit delays of itself.

Table 1. ENT Statistical Test Suite results for the processed sample and expected results for a true random sample.

Statistical Test	Processed Sample	True Random Sample
Entropy	7.999992	8.000000
χ^2 Distribution	73.15%	10–90%
Arithmetic Mean	127.467	127.500
Monte Carlo value for π	3.14273000	3.14159265
Serial Correlation Coefficient	0.000114	0.000000

Table 2. NIST Statistical Test Suite results for the processed sample. 'Tested' shows the number of equal-length sequences into which the 170 Mbit processed sample was divided for a test. 'Threshold' shows the minimum number of sequences which must pass a test for the processed sample to pass. 'Passed' shows the number of sequences which passed a test. The p-value for a test quantifies the uniformity of the distribution of the test results obtained for the different sequences and must be greater than 0.0001 for the processed sample to pass. Medians of test results are given for tests which comprise more than five subtests (marked with *).

Statistical Test	Tested	Threshold	Passed	p-value
Frequency	1700	1670	1683	0.126572
Block Frequency	1700	1670	1686	0.955304
Cumulative Sums 1	1700	1670	1681	0.685984
Cumulative Sums 2	1700	1670	1683	0.969205
Runs	1700	1670	1678	0.873253
Longest Run of Ones	1700	1670	1682	0.334538
Binary Matrix Rank	340	331	340	0.594330
Discrete Fourier Transform	1700	1670	1677	0.366918
Non-overlapping Template*	1700	1670	1681.5	0.555022
Overlapping Template	170	164	169	0.149743
Universal Statistical	170	164	169	0.144842
Approximate Entropy	340	331	339	0.594330
Random Excursions*	170	104	109	0.709445
Random Excursions Variant*	170	104	109	0.367453
Serial 1	170	164	169	0.839406
Serial 2	170	164	168	0.849412
Linear Complexity	170	164	166	0.751633

the bits 0 and 1 respectively. In the standard von Neumann algorithm [10], the bit-pairs 00 and 11 are simply discarded, resulting in a substantial reduction in sample size and effective generation rate. In the recursive von Neumann algorithm [9] employed here however, these bit-pairs are used to construct additional biased samples to which the von Neumann scheme is recursively applied, and the reduction in effective generation rate is kept to a minimum. We indeed find that randomness extraction only marginally reduced the effective generation rate to about 2.85 Mbits/s. Figure 2(b) confirms that our deterministic shuffle successfully removed the correlations between adjacent bits. The relative frequency of zeros and ones in the processed sample is 0.50006 and 0.49994 respectively, which confirms that the von Neumann scheme successfully removed the bias.

The quality of the processed sample was analysed further using the ENT [11] and NIST [12] Statistical Test Suites. In the ENT Statistical Test Suite, five key statistical quantities are determined for the sample in question, and the values obtained are compared to the expected values for a true random sample. As can be seen in table 1, the values obtained for the processed sample show excellent agreement with the expected values for a true random sample. The NIST Statistical Test Suite comprises fifteen rigorous industry standard tests, which are mainly aimed at assessing a random number generator's suitability for use in cryptographic applications. Detailed NIST test results for the processed sample are presented in table 2. The processed sample passed the NIST Statistical Test Suite, which confirms that, with standard post-processing, our linear plasmonic beamsplitter can be used to generate random numbers of sufficient quality to meet the stringent requirements of cryptographic applications.

4. Conclusion

We successfully demonstrated quantum random number generation using an on-chip linear plasmonic beamsplitter. The linear plasmonic beamsplitter used in our experiment is more compact than the plasmonic beamsplitter used in previous work [6], with a reduction in size by a factor of 2, thereby reducing the impact of loss. In our setup, the value of each random bit is determined by the waveguide into which each free-space single photon couples at the input grating of the linear plasmonic beamsplitter. Raw bits, generated at a rate of 2.86 Mbits/s, initially showed small correlations between adjacent bits and a small bias towards one, due to detector imperfections and asymmetry in the beamsplitter and collection optics. However, by employing standard randomness extraction protocols, we obtained a sample of high quality processed bits, with a marginally reduced effective generation rate of 2.85 Mbits/s, which passed the ENT and NIST Statistical Test Suites. Future work could involve integrating an on-chip source and on-chip detectors into our linear plasmonic beamsplitter to produce a highly compact, fully self-contained plasmonic quantum random number generator chip.

Acknowledgments

We acknowledge the use of the services of NTT-AT Japan for the fabrication of the on-chip linear plasmonic beamsplitter. This research was supported by the Harry Crossley Foundation, the University of Stellenbosch and the South African Quantum Technology Initiative (SAQuTI) through the Department of Science and Innovation of South Africa.

References

[1] Herrero-Collantes M and Garcia-Escartin J C 2017 *Rev. Mod. Phys.* **89** 015004

[2] Ghersi D, Parakh A and Mezei M 2017 *J. Comput. Chem.* **38** 2713–20

[3] Tian X and Benkrid K 2009 *Proc. of the 2009 NASA/ESA Conf. on Adaptive Hardware and Systems* (Washington, DC: IEEE Computer Society) pp 460–4

[4] Strydom C and Tame M S 2021 *The Proc. of SAIP2021, the 65th Annual Conf. of the South African Institute of Physics* (Pretoria: SAIP) pp 630–5

[5] Bai B, Huang J, Qiao G R, Nie Y Q, Tang W, Chu T, Zhang J and Pan J W 2021 *Appl. Phys. Lett.* **118** 264001

[6] Francis J T, Zhang X, Özdemir Ş K and Tame M S 2017 *Quantum Sci. Technol.* **2** 035004

[7] Tame M S, McEnery K R, Özdemir Ş K, Lee J, Maier S A and Kim M S 2013 *Nat. Phys.* **9** 329–40

[8] Edwards A L 1976 *An Introduction to Linear Regression and Correlation* (San Francisco, CA: Freeman) chapter 4 pp 33–46

[9] Peres Y 1992 *Ann. Stat.* **20** 590–7

[10] von Neumann J 1951 *Natl Bur. Stand. Appl. Math. Ser.* **12** 36–8

[11] Walker J 2008 https://www.fourmilab.ch/random/

[12] Rukhin A *et al.* 2010 https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-22r1a.pdf