Quantum Random Number Generation
Using a Solid State Single Photon Source

Simon J. U. Whitea, Friederike Klaucka, Nora Schmittb, Toan Trong Tranb, Mehran Kianiniaa, Andrea Steinfurthb, Igor Aharonovichb, Alexander Szameitb, and Alexander S. Solntsev*.

aSchool of Mathematical and Physical Sciences,
University of Technology Sydney, Ultimo, New South Wales, 2007, Australia

bInstitut für Physik, Universität Rostock, Albert-Einstein-Straße 23, 18059 Rostock, Germany

*Alexander.Solntsev@uts.edu.au

ABSTRACT

In this work we couple bright room-temperature single-photon emission from a hexagonal boron nitride atomic defect into a laser-written photonic chip. We perform single photon state manipulation with evanescently coupled waveguides acting as a multiple beam splitter, and generate a superposition state maintaining single photon purity. We demonstrate that such states can be utilized for quantum random number generation.

Keywords: single photon source, hexagonal boron nitride, quantum random number generation

1. INTRODUCTION

Random numbers are integral for cryptography, data science and fundamental research [1]. There are a number of implementations used for random number generators, but low quality generators can be points of failure for cryptographic applications and research [2]. Random numbers derived from the processes of quantum mechanics ensure fundamental randomness, and a number of demonstrations have been implemented measuring, radioactive decay, vacuum fluctuations, laser phase fluctuations, and single photons in superposition modes [1]. In quantum photonics, single photons are used as the fundamental storage unit for information. The advantage of photons for quantum information include high transmission speed, ease of maintaining coherence and a variety of tasks that can be solved by photons, including the generation of random numbers [3]. Advancements in on-chip photon coupling, state manipulation and detection are bridging the gap towards quantum optical circuits, but typically require the use of probabilistic photon sources or cooling to cryogenic temperatures [4, 5]. In this work, we utilize a true deterministic quantum light source operating at room temperature — a single photon emitter (SPE) based on solid state defects in hexagonal boron nitride [6]. We couple this SPE to a laser-written photonic chip [4] and demonstrate on-chip single photon multiplexing to generate binary sequences and verify quantum random number generation (QRNG).

2. EXPERIMENTAL SETUP AND QUANTUM RANDOM NUMBER GENERATION

In the experiment shown in Figure 1, a hexagonal boron nitride single photon source is excited with a 300 uw 532 nm continuous wave laser, and photons are collected through a 0.9 NA objective. The laser excitation is excluded using a 568 nm long pass filter (LP) and the zero photon line selected using a 630 ± 20 nm band-pass filter (BP). The photons polarisation is then controlled using a half wave plate (HWP) and a linear polariser (Pol) and are directly coupled to the chip using a lens and collected using a butt coupled fibre array. Photons are detected using avalanche photodiode and arrival times are recorded using a Swabian Instruments time tagger.
In Figure 2(a), antibunching curves show that single photon purity is retained throughout the chip, after splitting into multiple outputs. The second order correlation dip between two chip outputs is always below 0.5. Each output is correlated with output 5, i.e. blue = 1 vs. 5, orange = 2 vs. 5, green = 3 vs. 5 and red = 4 vs. 5. Figure 2(b) shows time traces of single photons arriving from four outputs of the chip exhibiting no intensity correlation. The solid line represents the sum of 100 × 1 ms bins of each output, normalized to channel 1 (blue), and the shaded region is the standard deviation. The total count rate (kHz) of each channel is also shown with negligible deviation on the s⁻¹ time scale. Figure 2(c) shows NIST randomness test results for a sequence of 300 000 bits, generated using single photons position in four spatial modes. The majority of tests pass the required p value > 0.01 to indicate randomness, but failures are seen in tests for bias. Figure 2(d) shows NIST test results for a sequence of 74440 bits generated using the position of a photon in two spatial modes. All the tests produce a p value > 0.01 indicating true randomness.

3. CONCLUSION

We have demonstrated QRNG based on a solid state SPE operating deterministically at room temperature. Although competing QRNG methods currently provide higher data rates, the exceptional brightness and stability of hBN-based single photon sources promises significant improvements in the future with better coupling and detection optimization.

REFERENCES

[1] M. H.-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. 89, 015004 (2017)
[2] T. H. Click, A. Liu, and G. A. Kaminski, J. Computational Chemistry 32, 513 (2011).
[3] J. L. O’Brien, A. Furusawa, and J. Vuckovic, Nat. Photonics 3, 687 (2009).
[4] M. Gräfe, R. Heilmann, A. Perez-Leija, R. Keil, F. Dreisow, M. Heinrich, H. Moya-Cessa, S. Nolte, D. N Christodoulides, and A. Szameit, Nat. Photonics 8, 791 (2014).
[5] P. J. Shadbolt, M. R. Verde, A. Peruzzo, A. Politi, A. Laing, M. Lobino, J. C. F. Matthews, M. G. Thompson, and J. L. O’Brien, Nat. Photonics 6, 45 (2012).
[6] T. T. Tran, K. Bray, M. J. Ford, M. Toth, and I. Aharonovich, Nat. Nanotechnol. 11, 37 (2016).