Quantum random number generation on a photonic chip using single photons from hexagonal boron nitride

Simon J. U. White,[1*] Friederike Klauck,[2] Toan Trong Tran,[1] Nora Schmitt,[2] Mehran Kianinia,[1] Andrea Steinfurth,[2] Matthias Heinrich,[2] Milos Toth,[1] Alexander Szameit,[2] Igor Aharonovich,[1] and Alexander S. Solntsev[1*]

1. School of Mathematical and Physical Sciences, Faculty of Science, University of Technology Sydney, Ultimo, NSW, 2007, Australia
2. Institut für Physik, Universität Rostock, Albert-Einstein-Straße 23, 18059 Rostock, Germany)
Author e-mail address: simon.white@uts.edu.au, alexander.solntsev@uts.edu.au

Abstract: Quantum random number generation (QRNG) harnesses the intrinsic randomness of quantum mechanical phenomena. Here, we couple bright room-temperature single-photon emission from a hexagonal boron nitride atomic defect into a laser-written photonic chip and demonstrate QRNG.

Introduction

The fundamental unpredictability inherent in genuine random numbers is vital for truly secure encryption, data science, and fundamental research [1-3]. Yet obtaining true randomness turns out to be a highly nontrivial task: Many conventional RNGs are actually pseudo-random, and, at their core, require a trusted source of randomness to expand with deterministic algorithms [4]. While such pseudo-random sequences can be obtained with great speed and efficiency, they tend to be subject to long term correlations. Beyond being a mere nuisance in data science and fundamental research, low-quality random number generators introduce critical points of failure in cryptographic applications. A particularly elegant approach to the generation of sequences of fundamentally random numbers are measurements of multipartite quantum states [5]. In this vein, a wide range of platforms for quantum random number generation (QRNG) have been implemented measuring, radioactive decay, vacuum fluctuations, laser phase fluctuations, and single photons in superposition modes [6]. 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 [7]. 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 [8, 9]. 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 [10]. We couple this SPE to a laser-written photonic chip and demonstrate on-chip single photon multiplexing to generate binary sequences and verify quantum random number generation (QRNG).

Implementation and Quantum Random Number Generation

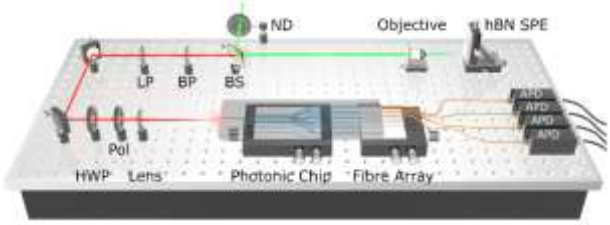

Fig. 1. Schematic of experimental setup

A hexagonal boron nitride single photon source is excited to emit a stream of discrete photons with a 300 uw 532 nm continuous wave laser, as illustrated in Fig. 1. The emission is collected using a 0.9 NA objective, the laser is excluded using a 568 nm long pass filter (LP) and the zero phonon 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. The device is designed to efficiently evolve a single photon in one single spatial mode to a multipath superposition state via a simultaneous radial coupling. Photons at the end of the chip are collected using a butt coupled fibre array. The functional region of this chip is invariant in propagation direction and therefore free of radiation losses associated with repeated S-bends. Once the desired multipartite spatial superposition state has evolved, a fan-out section serves to separate the individual channels to ensure compatibility with commercially available fibre arrays. Photons are finally detected using avalanche photodiodes and arrival times are recorded using a Swabian Instruments time tagger.

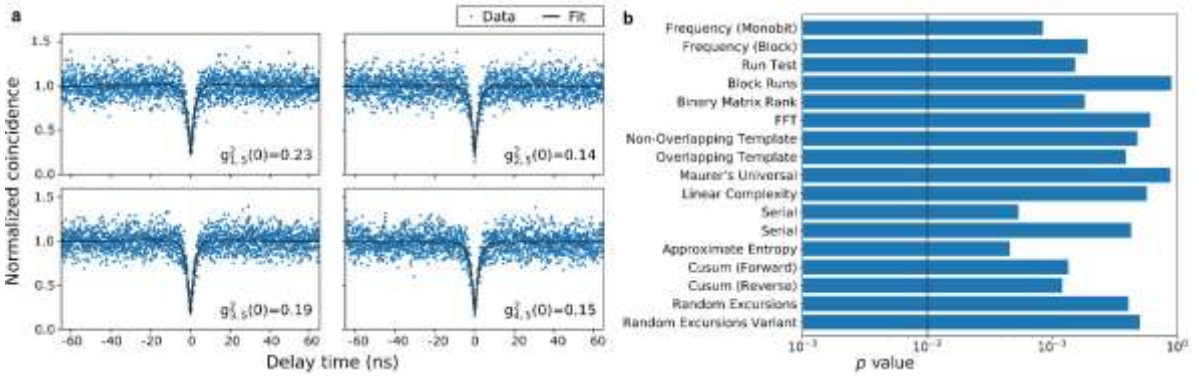

Fig. 2. Single photon purity and random number statistics. **a** Second order correlation data recorded showing arrival correlations between channel 5 and channels 1-4. Single photon purity is confirmed with fit $g^2(\tau=0)$ well below the required 0.5. **b** National Institute of Standards and Technology (NIST) randomness suite test results. The tests were performed on 1 M bits and pass the required p value > 0.01 (black vertical line) to indicate randomness.

The emitter is excited, as above, and produces single photons at a rate of ~1 MHz before the chip. Due to in- and outcoupling losses as well as bending losses within the fan-out section of the waveguides we measure a count rate around 350 kHz after the chip (total from nine waveguides). To verify that the single-photon emissions of the hBN source were efficiently coupled to the chip and additional background counts were negligible, we recorded second-order correlations between pairs of output channels ($g^2_{1,5}(0)$ for channels 1 and 5). With minimal losses, the single-photon purity is maintained and is unequivocally demonstrated with fitted $g^2(0) < 0.24$, as seen in Fig. 2a. Fig. 2b shows NIST randomness test results for a sequence of 1 M bits, generated using the arrival position of a single photon from four spatial modes. In this measurement scheme each photon represents 2 bits (i.e. channel 1 ➔ 0,0. Channel 4 ➔ 1,1). For larger arrays of coupled modes this regime scales well, as a single photon can represent *n* bits, i.e. 2^n numbers in 2^n waveguides. As seen in Fig. 2b, all of tests pass the required p value > 0.01, at a significance level of $\alpha = 0.01$, thus the sequence is considered random.

In conclusion, this work demonstrates the first on-chip state manipulation using a room temperature single photon source. We generate a spatial superposition state that maintains high single photon purity which can be used for quantum random number generation. We test the quality of our generated random numbers using the benchmark NIST test suite and pass all tests. Combining the brightness and robustness of hexagonal boron nitride single photon emitters with a photonic chip that can readily be integrated with standard optical fibers and other photonic platforms we present a platform for use toward photonic quantum information processing.

[1] Gisin, Nicolas, et al. "Quantum cryptography." Rev. Mod. Phys. **74**(1), 145–195 (2002).

[2] Metropolis, Nicholas, and Stanislaw Ulam. "The monte carlo method." J. Am. Stat. Assoc. **44**(247), 335-341 (1949).

[3] Acín, Antonio, Serge Massar, and Stefano Pironio. "Randomness versus nonlocality and entanglement." Phys. Rev. Lett. **108**(10) 100402 (2012).

[4] Knuth, Donald E. *Art of computer programming, volume 2: Seminumerical algorithms.* (Addison-Wesley Professional, 2014).

[5] Ma, Xiongfeng, et al. "Quantum random number generation." npj Quantum Inf. **2**(1), 1-9 (2016).

[6] Herrero-Collantes, Miguel, and Juan Carlos Garcia-Escartin. "Quantum random number generators." Rev. Mod. Phys. **89**(1), 015004 (2017).

[7] O'brien, Jeremy L., Akira Furusawa, and Jelena Vučković. "Photonic quantum technologies." Nat. Photonics **3**(12), 687 (2009).

[8] Gräfe, Markus, et al. "On-chip generation of high-order single-photon W-states." Nat. Photonics **8**(10), 791. (2014).

[9] Shadbolt, Peter J., et al. "Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit." Nat. Photonics **6**(1), 45 (2012).

[10] Tran, Toan Trong, et al. "Robust multicolor single photon emission from point defects in hexagonal boron nitride." ACS Nano **10**(8), 7331-7338 (2016).