Progress towards Quantum-based Random Number Generation using Entangled Photons

Joshua C. Bienfang, Peter Bierhorst, Alan Mink and Stephen Jordan, Paulina Kuo, Scott Glancy, S. Nam, K. Shalm, M. Stevens, T. Gerrits, R. Mirin, V. Verma, A. Lita, C. Hodge

National Institute of Standards and Technology
Boulder, CO
and
Gaithersburg, MD
<amink@nist.gov, joshua.bienfang@nist.gov>

Quantum processes are currently the only processes considered truly random. The National Institute of Standards and Technology (NIST) is developing a prototype random number generator system based on a test of local realism (a “Bell test”) that uses detection of entangled photons to create a random bit stream. There are two major technical hurdles. The first is demonstrating that the hardware can perform Bell test measurements with sufficient fidelity and efficiency. We have recently demonstrated that our hardware is suitable by performing a “loophole-free” test of local realism. Our test closed the loopholes present in previous Bell tests by implementing space-like separation of all relevant events, active basis switching, a high fidelity source of entangled photons, and high efficiency photon transmission and detection. It produced data sets with p-values as small as 5.9×10^{-9}, rejecting local realism with high statistical significance. Data sets like these that show violation of local realism are potential secure sources of random numbers. The second major hurdle is to develop and implement appropriate algorithms to convert the measured data into usable random numbers.

We will discuss the overall system configuration and its basic operation. We will also discuss our recent progress at developing the post-processing stages that estimate a bound on the entropy of our measurement string and the Trevisan randomness extraction algorithm used to produce the final uniformly random string. We believe our Bell test system should be capable of high event rates, making it well suited for generating random numbers required by cryptographic applications or as an additional source of real-time randomness into the NIST’s public random number beacon <https://beacon.nist.gov>.