Using the unpredictable nature of quantum mechanics to generate truly random numbers

January 22 2021, by Bob Yirka

Credit: CC0 Public Domain

A team of researchers from the U.K., Germany and Russia has used the unpredictable nature of quantum mechanics to create a device capable of generating truly random numbers. In their paper published in the journal

Physical Review Letters, the group describes using aspects of quantum theory to develop a framework for building a truly random number generator.

For many years, computer scientists have been looking for a way to generate truly random numbers—the random number generator found on most home and business computers is far from random due to hardware limitations. Random number generation is important because it forms the basis of cryptography. Messages that are encoded using numbers that are not truly random can be hacked given enough computing power. In this new effort, the researchers looked to the quantum world to create a truly random number generator.

Unlike the natural world around us, the quantum world has instances of true randomness—the unpredictable nature of photon behavior, for example. In this new effort, the researchers found a way to harness this unpredictability to build a truly random number generator.

The device built by the team consisted of a laser fired directed into one of the inputs of a generic beam splitter. The other input was kept void. This resulted in a zero signal. The outgoing beam was then measured using two independent detectors. In their setup, each of the photons arriving at the beam splitter had an even chance of being either transmitted or reflected, which meant that the difference between measurements taken by the detectors could not be predicted. Because of that, the numbers generated were truly random.

The researchers then took their work another step by measuring the states of the photons before they were split. That verified that the numbers generated by their device truly were random. The end result was a device capable of generating random numbers at a pace of 8.05 gigabits per second, each of which were certifiably random—all in real time. Remarkably, the device they built was made using off-the-shelf

equipment.

More information: David Drahi et al. Certified Quantum Random Numbers from Untrusted Light, *Physical Review X* (2020). DOI: 10.1103/PhysRevX.10.041048