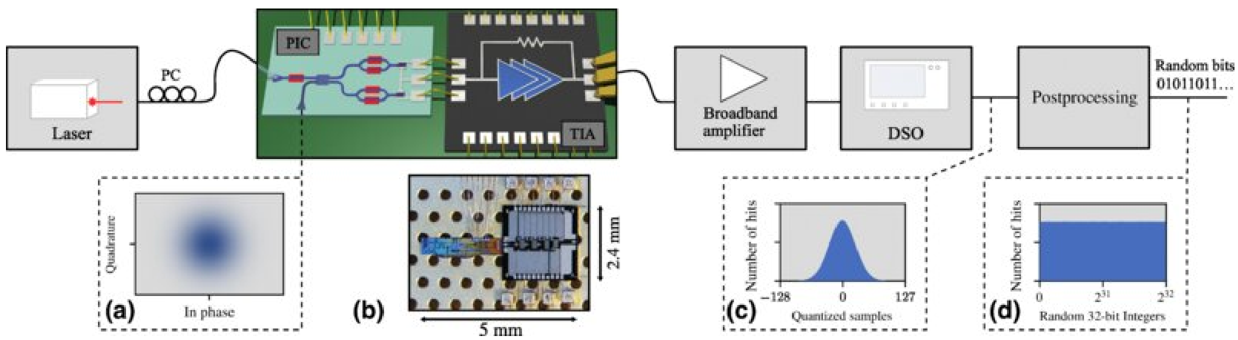
Using quantum fluctuations to generate random numbers faster

April 5 2023, by Bob Yirka



An overview of the QRNG setup. (a) The vacuum noise that is used as a source to generate random numbers. (b) A micrograph of the manufactured PIC and TIA. (c) The Gaussian distribution after digitization. (d) The distribution of the distilled random 32-bit integers, grouped into 256 bins. Credit: *PRX Quantum* (2023). DOI: 10.1103/PRXQuantum.4.010330

A team of physicists from Ghent University—Interuniversity Microelectronics Center, Technical University of Denmark and Politecnico & Università di Bari, reports that it is possible to use quantum fluctuations to generate random numbers faster than standard methods.

In their study, reported in the journal *PRX Quantum,* the group used the behavior of pairs of particles and antiparticles to create a random generator that is up to 200 times faster than conventional systems.

Random number generation is important in computer science. In addition to such applications as generating random backdrops and scenarios in video games, random numbers are used to create encryption keys for a host of sensitive applications. But generating keys that cannot be easily cracked requires computer power and time. For that reason, computer scientists are constantly looking for new ways to generate random numbers.

In this new effort, the research team turned to a new source—quantum fluctuation—which, in its most basic form, is a temporary change in the amount of energy that exists at a unique point in space. Such flickering has been widely studied due to the way it impacts chemical bonding and resulting types of light scattering. In this new effort, the research team took advantage of the randomness of such flickering to create a random number generator. In their approach, they focused on quantum flickering related to instances of particles and antiparticles forming and self-destructing and the fields of energy associated with them. Such flickering has in the past been shown to be random.

To capture the randomness of such flickering, the researchers used an integrated balanced homodyne detector—a device that is capable of measuring the electric field of a quantum state. But noting that such a device is susceptible to also capturing the less-than-random behavior of entangling particles, they added another device designed to identify this noise and ignore it while taking measurements.

The team then shrank the components used by their homodyne detector to a size that would allow incorporation on a chip installed in a computer system. They then used data from the chip to generate random numbers.

More information: Cédric Bruynsteen et al, 100-Gbit/s Integrated Quantum Random Number Generator Based on Vacuum Fluctuations, *PRX Quantum* (2023). DOI: 10.1103/PRXQuantum.4.010330