Title:	Quantum Random Number Generator (QRNG)
Author(s):	Everhart - Erickson, Michael Charles
Intended for:	Report
Issued:	2021-01-29

Disclaimer:
Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by Triad National Security, LLC for the National Nuclear Security Administration of U.S. Department of Energy under contract 89233218CNA000001. By approving this article, the publisher recognizes that the U.S. Government retains nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy. Los Alamos National Laboratory strongly supports academic freedom and a researcher's right to publish; as an institution, however, the Laboratory does not endorse the viewpoint of a publication or guarantee its technical correctness.

Quantum Random Number Generator (QRNG)

Lost Alamos National Laboratory and Qrypt, Inc.

Innovation

The Los Alamos QRNG is a hardware-based high-performance Random Number Generator capable of generating 200 Mbit/s or more of true random numbers. The device harvests entropy from fluctuations in an optical source that arise from quantum mechanical properties of light. These quantum effects are irreducibly random; the resulting numbers are unpredictable and beyond the influence of any adversary.

Qrypt, Inc., launched in 2017, has amassed multiple quantum entropy sources to create high-quality random keys at scale. The company is engaging with Los Alamos through license and a Cooperative Research and Development Agreement to facilitate the transition of QRNG technology and deploy the technology into the marketplace.

Technology Advancement

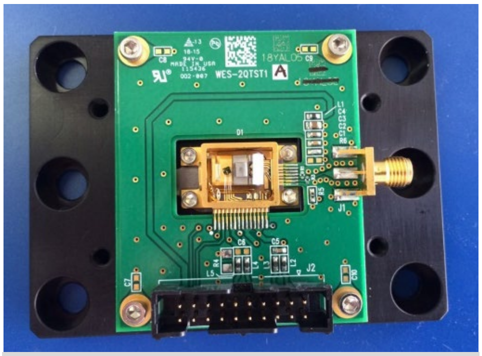
Los Alamos' QRNG uses the unique properties of quantum mechanics to generate true entropy in a way that is immune from external influence. Using a phenomenon of light known as photon bunching the entropy source generates an almost perfectly random signal that is digitized and provided as a stream of random numbers. Other random number generators capture entropy from a variety of natural and man-made sources but few have the fundamental randomness and true unpredictability provided by quantum mechanics.

The LANL QRNG can satisfy the demands of even the highest-performance crypto-systems. This device can used as a dedicated random number generator or deployed as the core component of an entropy-as-a-service network device.

Impact

Poor random number generation becomes a single point of failure, an issue that is compounded by the fact that measuring the quality of random number generators is notoriously difficult. Proving that keys are truly random and unpredictable and attesting to crypto system security becomes almost impossible if a solid foundation of random number generation is not present.

Qrypt is making strategic investments in cutting-edge quantum hardware companies and partnerships with premier global research institutes and U.S. national labs to amass multiple quantum entropy sources and create high-quality random keys at scale.



Quantum Random Number generator optical engine: integrated light source, lens and photodetector

Timeline

February, 2020: Los Alamos signed an agreement with Qrypt, Inc. to license specific LANL QRNG intellectual property.

November, 2020: Los Alamos entered into a Cooperative Research and Development Agreement with Qrypt to further develop and transition the QRNG technology to the company.