Society for Electronic Transactions and Security (SETS)

QUANTUM RANDOM NUMBER GENERATOR AND SERVICES

Quantum Random Number Generator (QRNG) offers high-quality random sequences using the unique properties of quantum physics. QRNG exploits nature's inherent randomness. SETS is developing a portable QRNG technology for cryptographic applications.
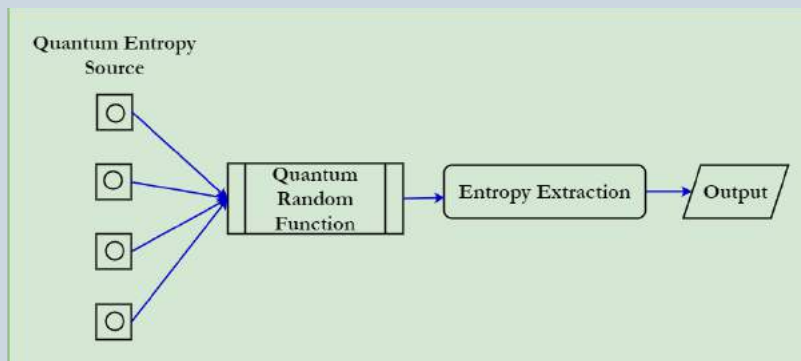
High-level description:

- A Light-source (LED) emits a photon shot noise onto an image sensor
- Sensors capture the photon noises and generate raw data
- The raw data from multiple independent quantum random sources is processed by Quantum Random Function (QRF)
- The output of the system is a sequence of binary bits with verifiable entropies
- The numerically transformed binary bits can be used in a wide range of applications, including seeding of Quantum Key Generation protocols

Salient Features:

- Co-operative quantum randomness at high generation rates
- Reliable and verifiable source of randomness
- Ability to extract entropy from un-trusted random sources
- Post-quantum cryptographic solution
- The AI-assisted entropy monitoring module
- USB/Web interfaces and cloud services
- Compliant with common standards.
- Affordable cost and easy to use
- Randomness Tests: NIST, Dieharder , Alphabit, Rabbit