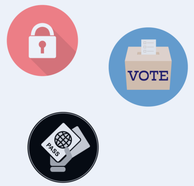
The World's Fastest Coin Flip: Randomness for Everyone!

Michael A. Wayne, Alan L. Migdall, and Joshua C. Bienfang
National Institute of Standards and Technology / Joint quantum Institute, Gaithersburg, MD 20899, USA
michael.wayne@nist.gov

Randomness as a Public Service



The world often requires trusted randomness.

A randomness beacon provides a public source of entropy.

NIST Beacon (USA)
beacon.nist.gov/home

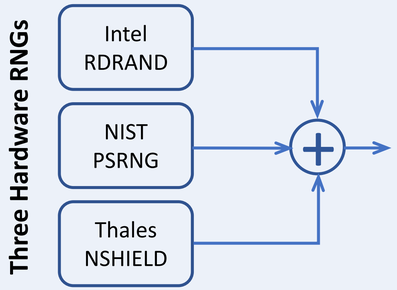
CLCERT Beacon (Chile)
beacon.clcert.cl

Inmetro Beacon (Brazil)
beacon.inmetro.gov.br

The NIST Beacon is one of several beacons in the world.

Multiple ***independent*** beacons can be combined to increase trust.

The NIST Randomness Beacon



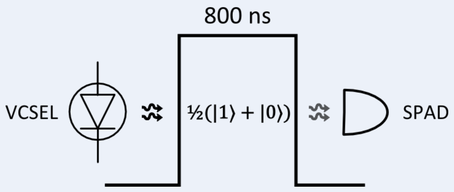
At NIST, three physical RNG systems are combined to generate a high-quality random stream at a rate of 512 bits / minute.

Two (Intel, Thales) are commercially-available hardware RNGs, while the other [1] is a NIST-designed quantum random number generator.

The output of a loophole-free Bell test[2], will eventually be used to add ***certifiable*** randomness to the beacon.

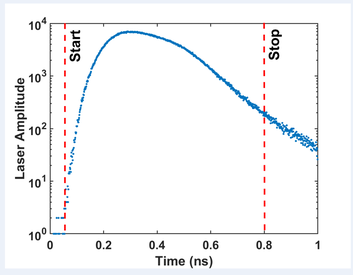
Photon Sampling Random Number Generator (PSRNG)

The Random Process



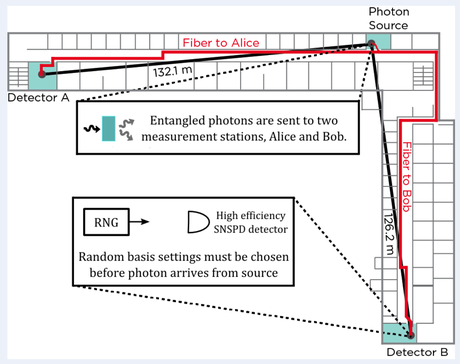
The arrival time of single photon from a coherent source is a random process. Bit values are determined by whether a photon is detected during an 800 ps window.

PSRNG Timing Window



- Detection during window = "1" value
- No Detection during window = "0" value
- Ideally, P(1) = P(0) = 0.5
- Absence of post-processing leaves system vulnerable to long-term drift.

Loophole-Free Bell Test



The PSRNG was used in one of the first experimental demonstrations of a loophole-free Bell test [2].

In this application, the random process must not begin until a bit is requested, and then the bit must be generated and made available as fast as possible.

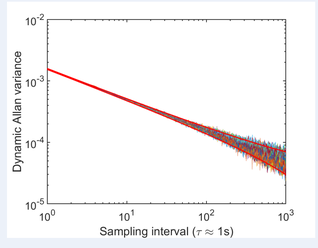
This excludes the use of post-processing to eliminate drift or unwanted bias, and requires a very prompt random process.

The Allan Variance

The Allan variance [3] is a clock analysis measure used to identify types and strengths of noise.

The Allan variance indicates that the PSRNG output is the sum of a random white-noise process and a weak random-walk type process.

Allan variance over several days



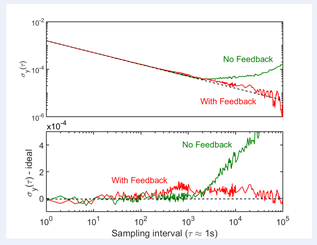
Consecutive measurements over a many days reveal no short-term instabilities in the additional noise type [4].

On average, the per second drift is very small.

- $\Delta P(1) \approx 5.2(1) \times 10^{-7}$

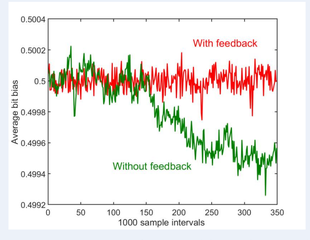
PSRNG Results

Allan variance after feedback



After feedback, output is statistically indistinguishable from white noise (dashed black line) for sample sizes of up to one day.

Bit-bias after feedback



Output rate of 100 kbit /s, and time from bit request to output is 2.4(3) ns.

Worlds fastest coin flip!

It's Actually a Black Box!

The PSRNG is housed in an insulated box to reduce temperature-induced drift. It has real-time monitoring and communicates with the beacon through a microcontroller-based USB interface.

References

[1]. Wayne, M. A., Migdall, A. L., Levine, Z. H., and Bienfang, J. C., "*A post-processing-free single-photon random number generator with ultra-low latency*," Optics Express **26**, 32788-32801 (2018).

[2]. Shalm, L. K., et al. "*Strong loophole-free test of local realism,*" Phys. Rev. Lett. **115**(25), 250402 (2015).

[3]. Riley, W. J., *Handbook of frequency stability analysis.* NIST Special Publication No. 1065 (2008).

[4]. Galleani, L. and Tavella, P. "*The dynamic Allan variance*," IEEE Trans. Ultrason. Ferroelectr. Freq. Control **56**(3), 450-464 (2009).