True Random Number Generation based on Interference between Two Independent Lasers

Caleb John, Raju Valivarthi, Qiang Zhou and Wolfgang Tittel

QC2 Lab, Institute for Quantum Science and Technology
Department of Physics and Astronomy, University of Calgary, Canada
June 16, 2015

Outline

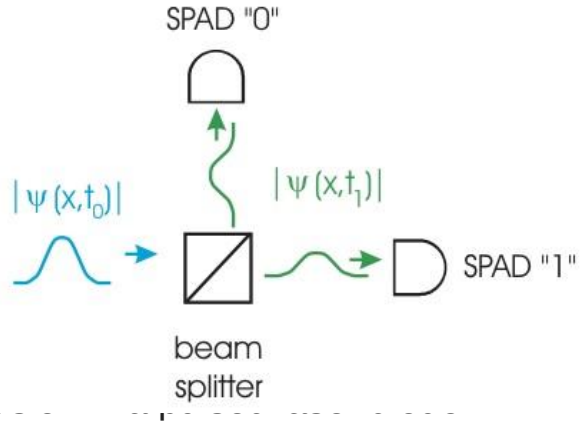
- Motivation
- Principle & implementation
- Analysis & testing
- Conclusions and outlook

Why True Random Numbers?

- True *vs.* Pseudo-Random Number Generator
- Online Casinos
- Statistical Simulations
- Cryptography
- Quantum Cryptography (Quantum Key Distribution, etc.)

Other QRNG Schemes

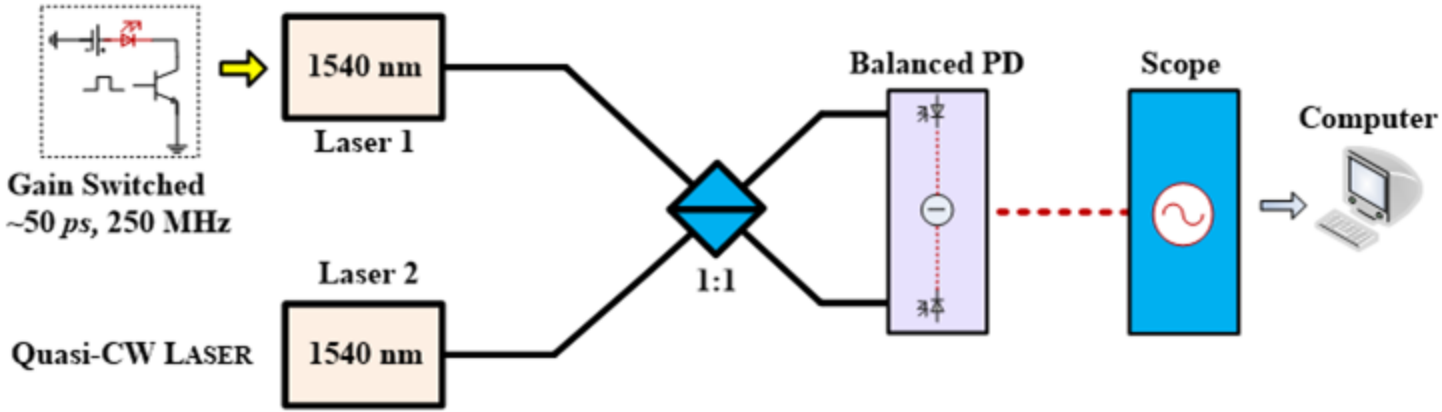
- Commercial QRNG by ID Quantique (~4 MHz)
  ID Quantique - Random Number Generation using single photons
  http://www.idquantique.com/
  - Generation Rate is limited by speed of single photon detectors



- QRNG based on randomness of laser emission (up to
  Ultra-fast quantum randomness generation by accelerated phase diffu
  M. Jofre, et al. Optics express 22.2 (2014): 1645-1654.
  True random numbers from amplified quantum vacuum
  C. Abellan, et al. Optics Express, vol. 19, issue 21, pp. 20665-20672 (2011).

***QRNG: Quantum Random Number Generator**

Our Scheme



$$i_1(t) \propto \frac{1}{2}\left(E_1^{\,2}(t) + E_2^{\,2}(t) - 2E_1(t)E_2(t)\times\sin\left(\Delta\varphi(t)\right)\right)$$

$$i_2(t) \propto \frac{1}{2}\left(E_1^{\,2}(t) + E_2^{\,2}(t) + 2E_1(t)E_2(t)\times\sin\left(\Delta\varphi(t)\right)\right).$$

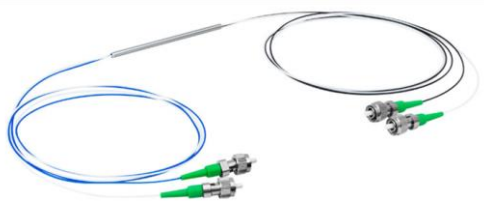
$$\Delta i(t) \propto 4E_1(t)E_2(t)\times\sin\left(\Delta\varphi(t)\right).$$

Random numbers are generated from the phase randomness of laser emissions [1].

[1] C. H. Henry, Quantum Electronics, IEEE Journal of 18, 259-264 (1982).

Implementation

Lasers with drivers and temperature controller

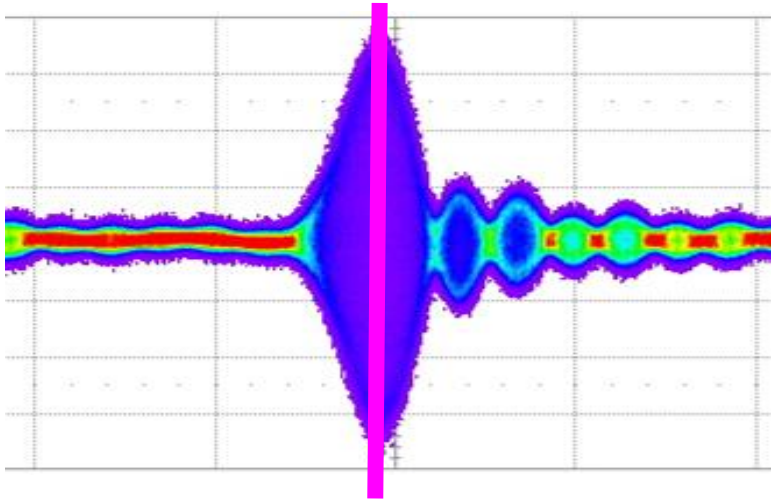


50:50 beam splitter

Balanced photodetector

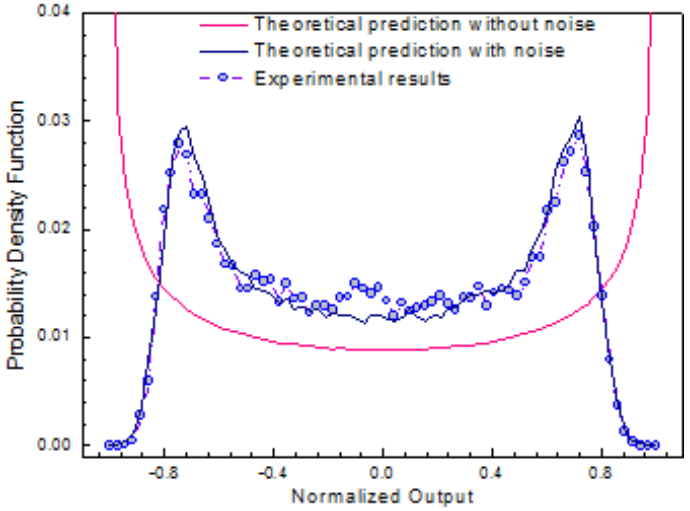
Confirm the randomness of output

Persistence mode oscilloscope trace of 1 pulse



$$\Delta i(t) \propto 4E_1(t)E_2(t)\times\sin\left(\Delta\varphi(t)\right).$$

Histograms of the output

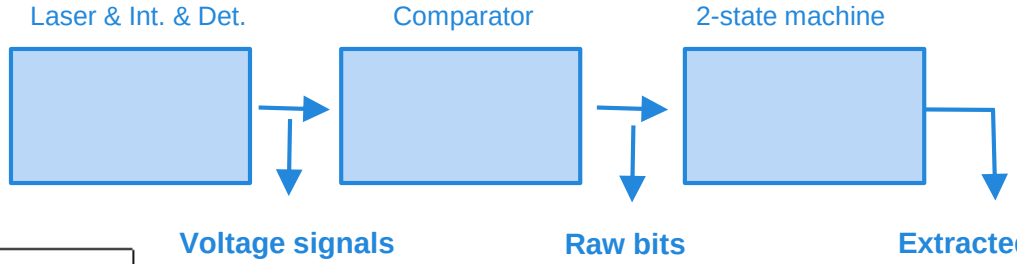


Probability density function of output $1/\left(\pi\times\sqrt{1-x^2}\right)$

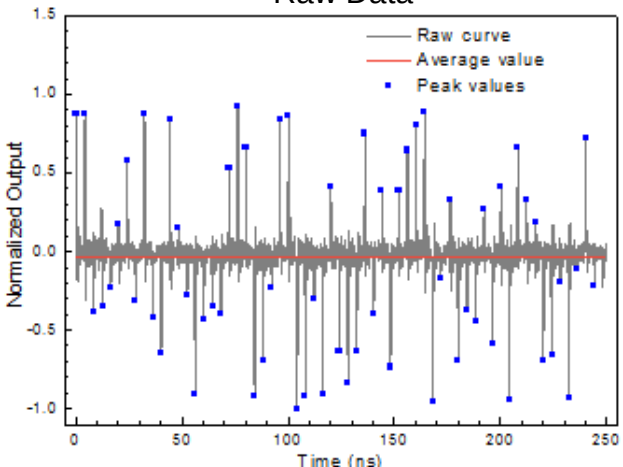
*Assuming phase is uniformly distributed from 0-2π

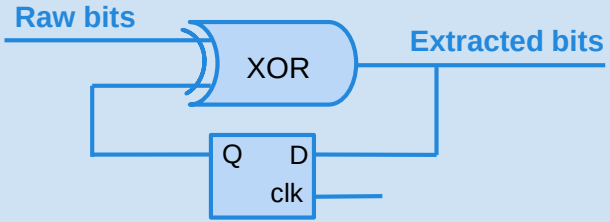
How to get the random bits?

1 bit digitization and extraction



Raw Data



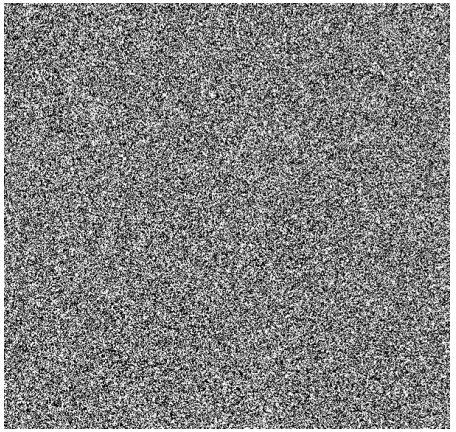


1 bit delayed XOR

How to test the randomness?

- A quick look at the randomness of numbers

Visualization of our bits



- Battery of NIST tests-15 tests for statistical properties of a RNG [1]

[1] A statistical test suite for random and pseudorandom number generators for cryptographic applications, NIST Special Publication 800-22 revision 1a (2010).

Results of the NIST test

*All test were performed with 100 trials, with 1Mbit per trial

	FR.	FB.	RN.	LR.	BR.	FT.	NO.	OT.	US.	LC.	ST.	AE.	CS.	RE.	RV.
Raw bits (1 pulse)	✓	✓	✓	✗	✓	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗
Raw bits (2 pulses)	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓
Extracted bits	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

FR - Frequency
FB - Block Frequency
RN - Runs
LR - Longest Run of Ones
BR - Binary Matrix Rank
FT - Discrete Fourier Transform
NO - Non-Overlapping Templates
OT - Overlapping Template
US - Universal Statistical
LC - Linear Complexity
ST - Serial Test
AE - Approximate Entropy
CS - Cumulative Sums
RE - Random Excursions
RV - Random Excursions Variant

Conclusion & Outlook

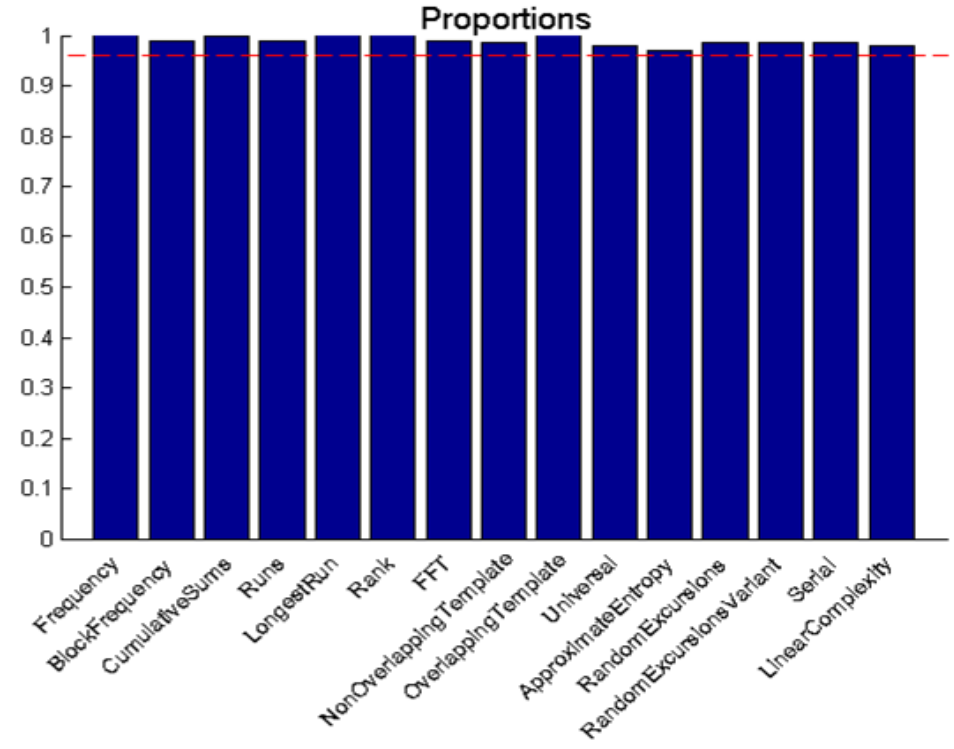
- Proposed and demonstrated a QRNG - Rates up to 250 MHz
- All commercial components

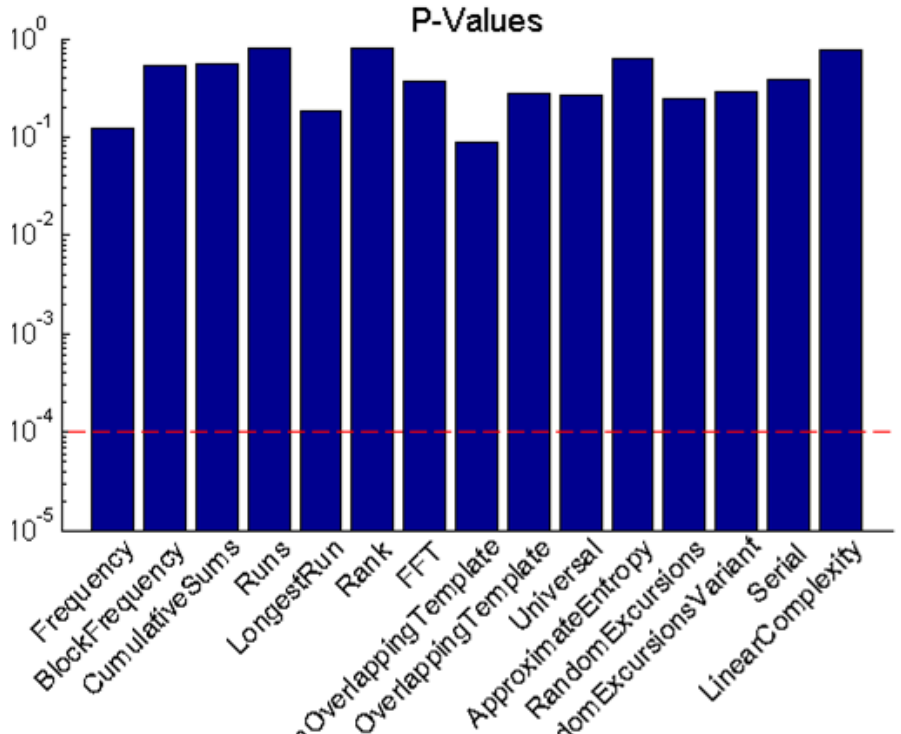
Future Work

- Binning to increase the generation rates ~3 GHz
- Implementing the prototype of a Quantum Random Number Generator

Thanks!

Extended NIST Results





Extra Figures