An ultrafast quantum random number generator based on quantum phase fluctuations

Feihu Xu, Bing Qi, Xiongfeng Ma, He Xu, Haoxuan Zheng, and Hoi-Kwong Lo

Center for Quantum Information and Quantum Control,
Department of ECE and Department of Physics,
University of Toronto

Email: feihu.xu@utoronto.ca

QCRYPT2011, ETH, Zurich,
Sep. 14th, 2011

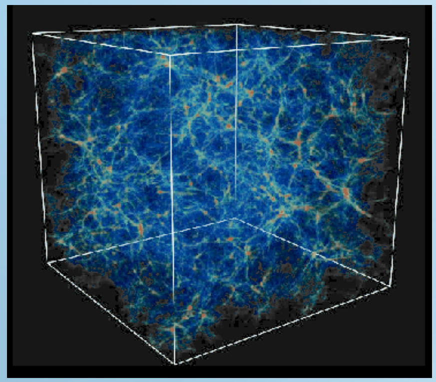
UNIVERSITY OF TORONTO

THE EDWARD S. ROGERS SR. DEPARTMENT OF
ELECTRICAL AND COMPUTER ENGINEERING

Outline

Applications of random numbers

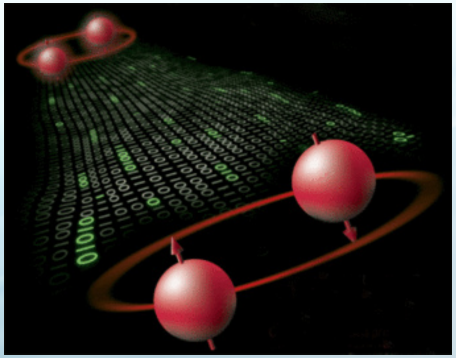
Scientific simulations



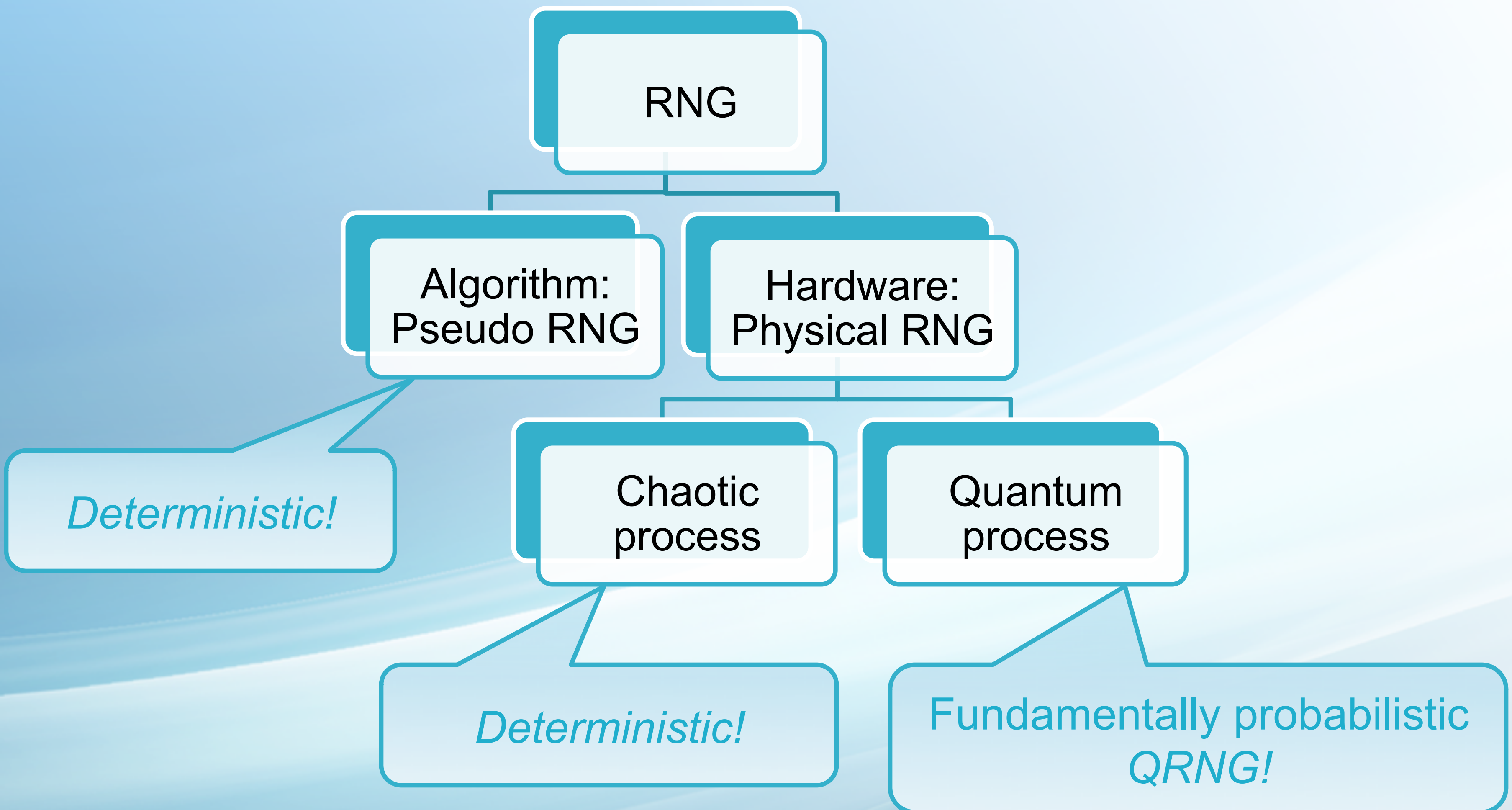
Lottery & Gambling

Market

Cryptography

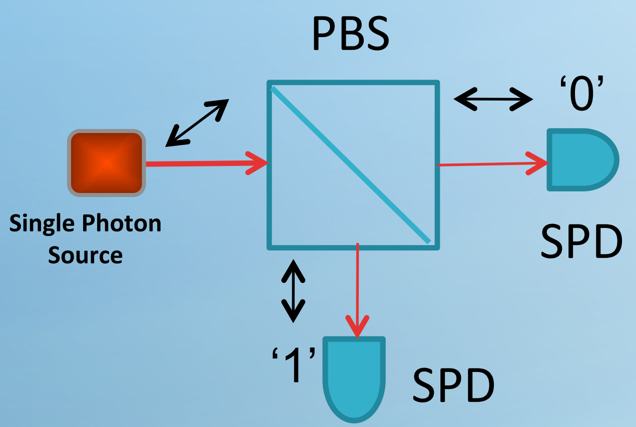


Random number generator (RNG)



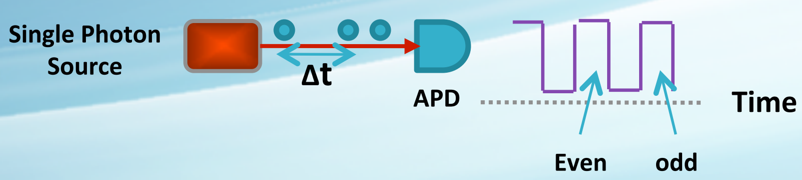
QRNG: single photon detection

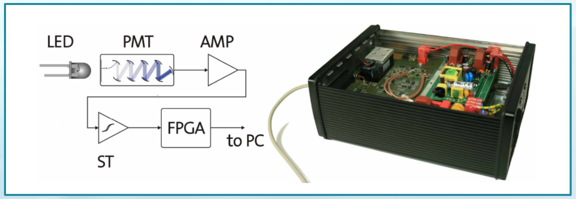
- Polarization measurement [1]



Commercial QRNGs up to 16 Mb/s.
(Figure is from ID Quantique)

- Photon arrival time [2-3] or photon number counting [4]



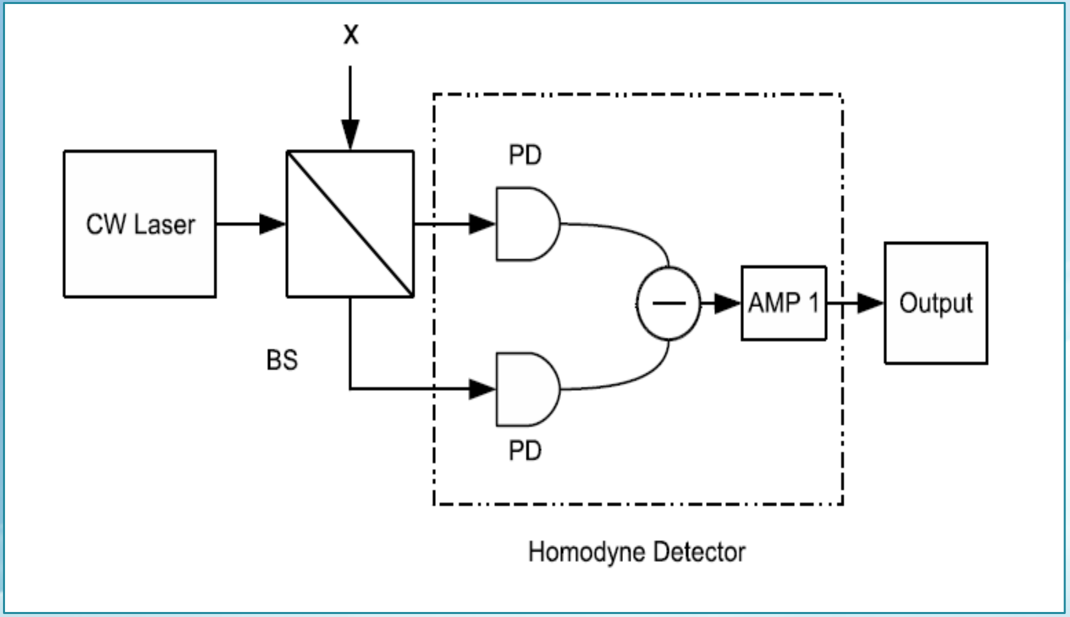


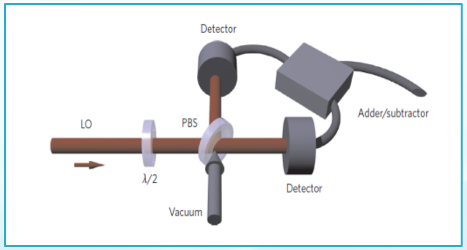
Fully integrated QRNG.
(Figure is from ref [4])

[1] T. Jennewein, et al, Rev. of Sci. Ins., 71:1675-1680, 2000.
[2] P. Kwiat, E. Jeffrey, P. Altepeter, US Patent Appl. 20060010182, 2006.
[3] J. Dynes, et al, App. Phy. Lett., 93, 031109 (2008)
[4] M. Furst, et, al, Opt. Exp. 18, 13029 (2010).

QRNG: vacuum state fluctuations [1-2]

- Homodyne detection measuring the electrical field fluctuations of Vacuum state.



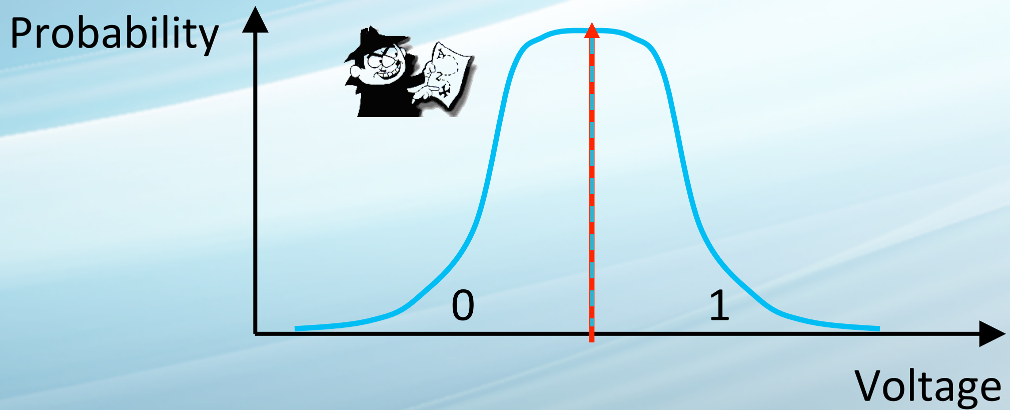


QRNG with 6.5 Mb/s [2].
(Figure is from ref [2])

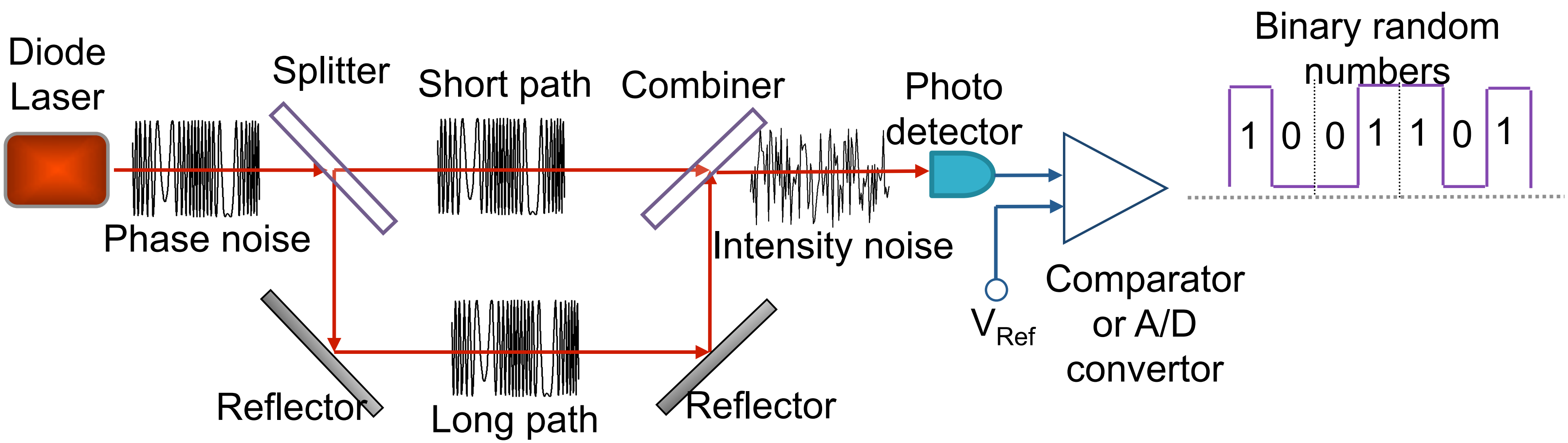
[1] A. Trifonov and H. Vig, US Patent No. 7,284,024, 16 October 2007
[2] C. Gabriel, et al, Nature Photonics, 4, 711–715 (2010)

Motivation: QRNG existing problems

- Low generation rate
  - Typical rates: *6.5 Mb/s* using vacuum state fluctuations, *16 Mb/s* using polarization measurement (commercial QRNG), *152Mb/s* using photon arrival time [M. Wahl, et al, APL, 98, 171105, 2011].
- High cost
  - For example, the IDQ system (Quantis, 16Mb/s) costs 2230 €.
- Eavesdropper (Eve) may have partial information
  - Control side information (detector noise, environmental noise, etc).



Our approach: randomness from laser phase fluctuations

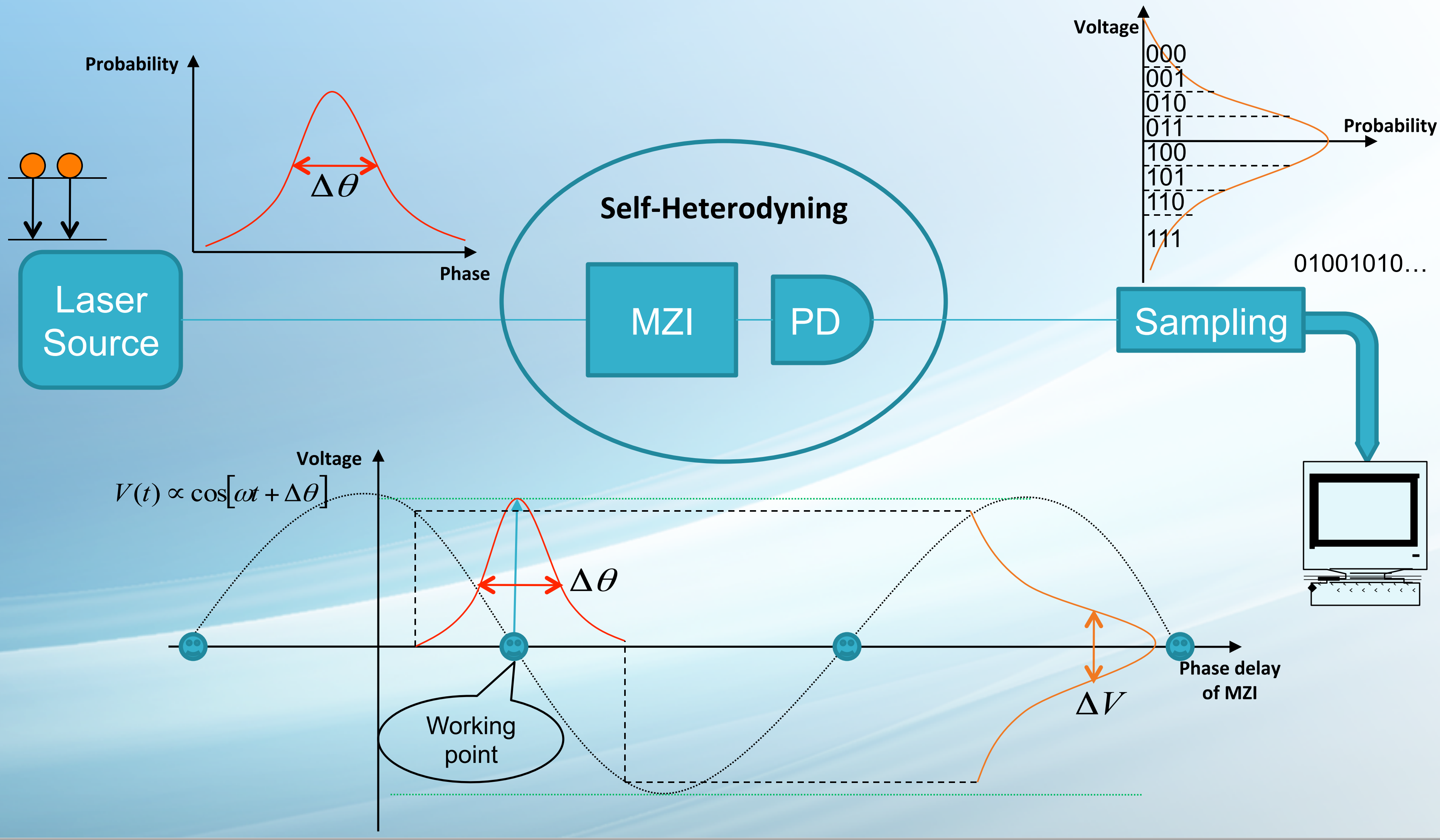


Measure laser phase fluctuations → Sample → Generate digital bits

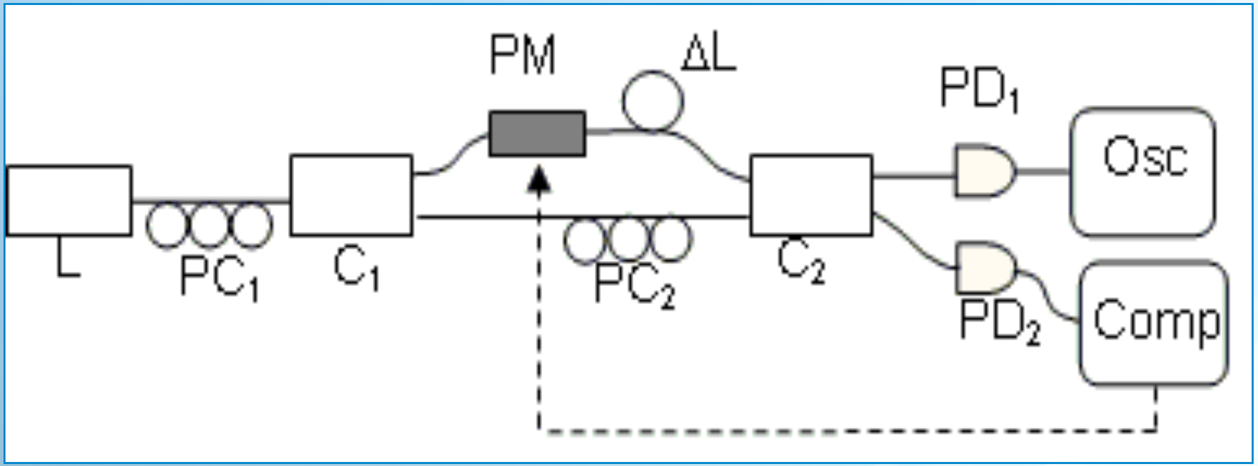
Low cost & high rate!

[1] A. Yariv and P. Yeh, "Photonics: optical electronics in modern communications" (6th edition), Oxford University Press (2007).
[2] K. Petermann, "Laser diode modulation and noise", (Springer, 1988).

How the system works?



Our previous work



L: 1550nm cw DFB laser diode;
PC1,2: polarization controller;
PD2: 1MHz photo-receiver;
OSC: 3GHz oscilloscope;

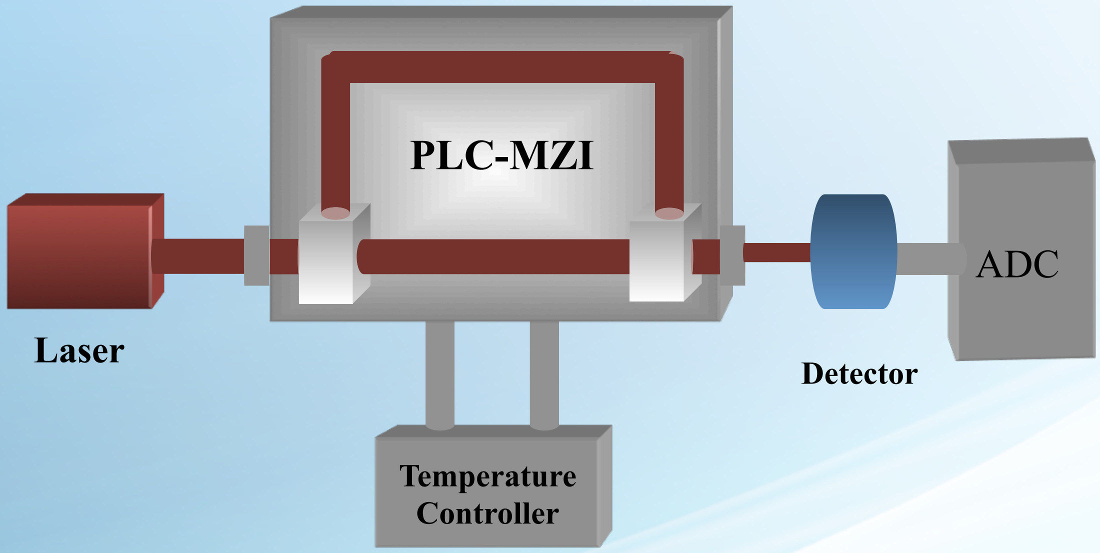
$C_{1,2}$: fiber couplers
PD1: 5GHz photo-detector;
PM: phase modulator;
Comp: computer with DAQ.

- Self-heterodyne system with off-the-shelf components.

- 500 Mb/s

B. Qi, Y.M. Chi, H.-K. Lo, L. Qian, AQIS (2009)
B. Qi, Y.M. Chi, H.-K. Lo, L. Qian, *Optics Letters*, 35, 312 (2010).

Our new setup

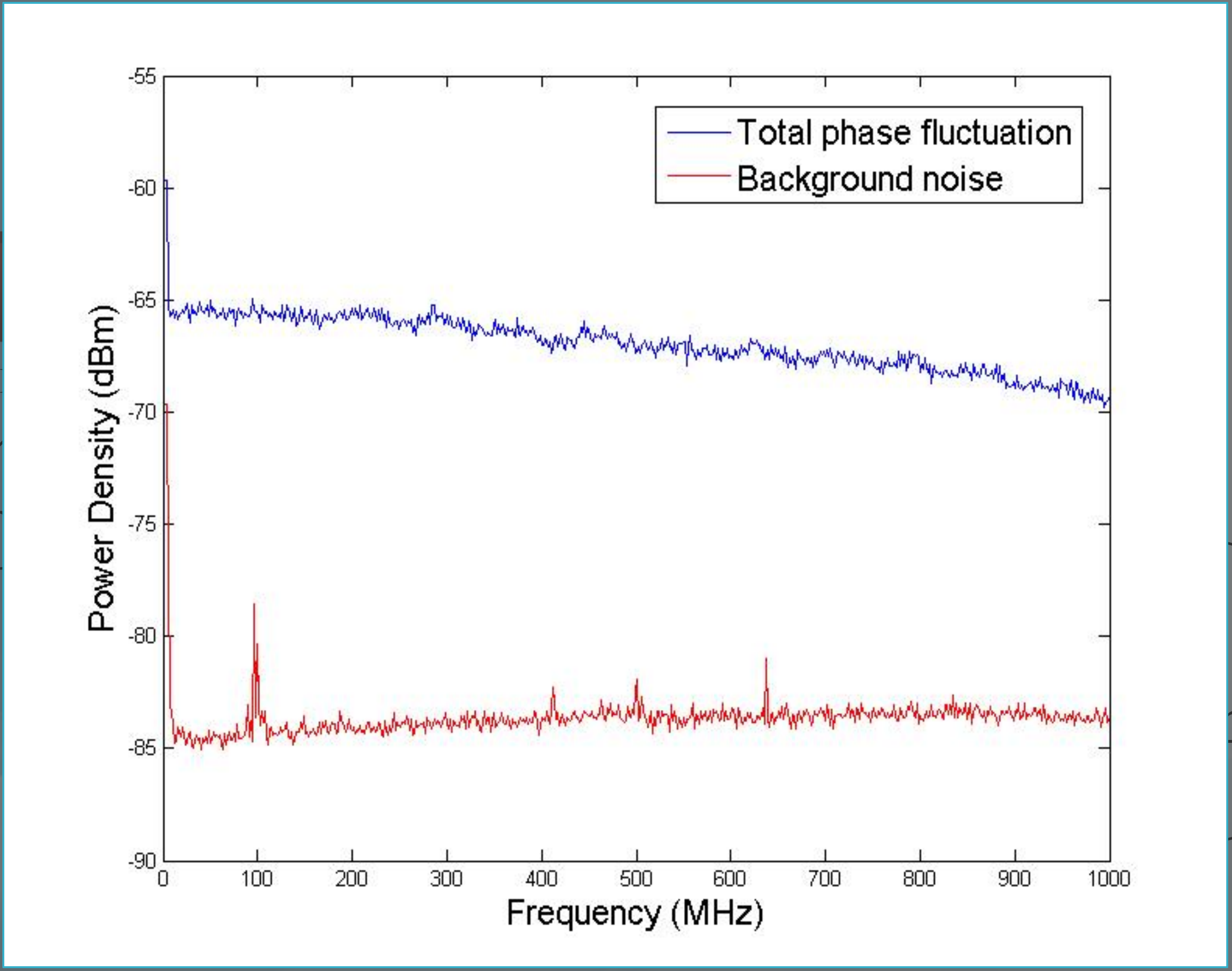


PLC-MZI: planar lightwave circuit Mach-Zehnder interferometer;
ADC: 8-bit analog-to-digital convertor.
Sampling rate: 1G samples per second
Extractable random bits: 6.7 bits/ sample

Generation rate over 6 Gb/s!

F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, H.-K. Lo, *arXiv: 1109.0643* (2011)

Measurement results

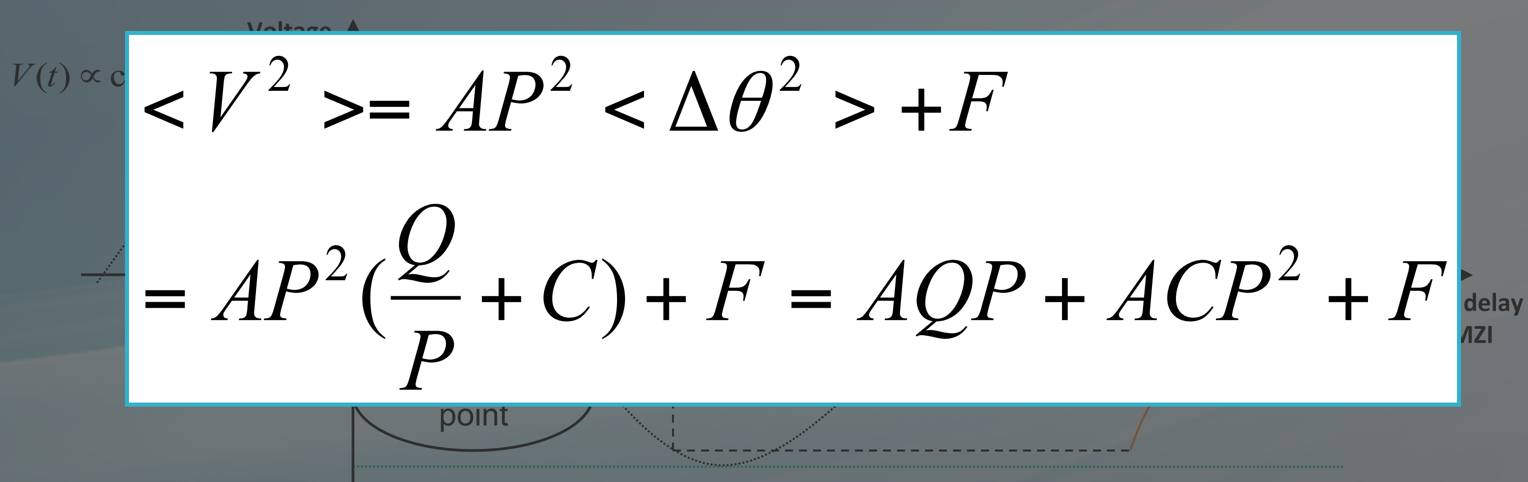


Quantum phase fluctuation is dominant!

F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, H.-K. Lo, *arXiv: 1109.0643* (2011)

Quantum signal and classical noise

- Laser phase fluctuations [1]
  - Quantum: spontaneous emission — Inversely power-dependent (Q/P)
  - Classical: cavity instability, etc. — power-independent (C)
- Electrical noise (detector) and EM noise (environment) — F
- Quantify the parameters:



$$< V^2 > = AP^2 < \Delta\theta^2 > + F$$

$$= AP^2\left(\frac{Q}{P} + C\right) + F = AQP + ACP^2 + F$$

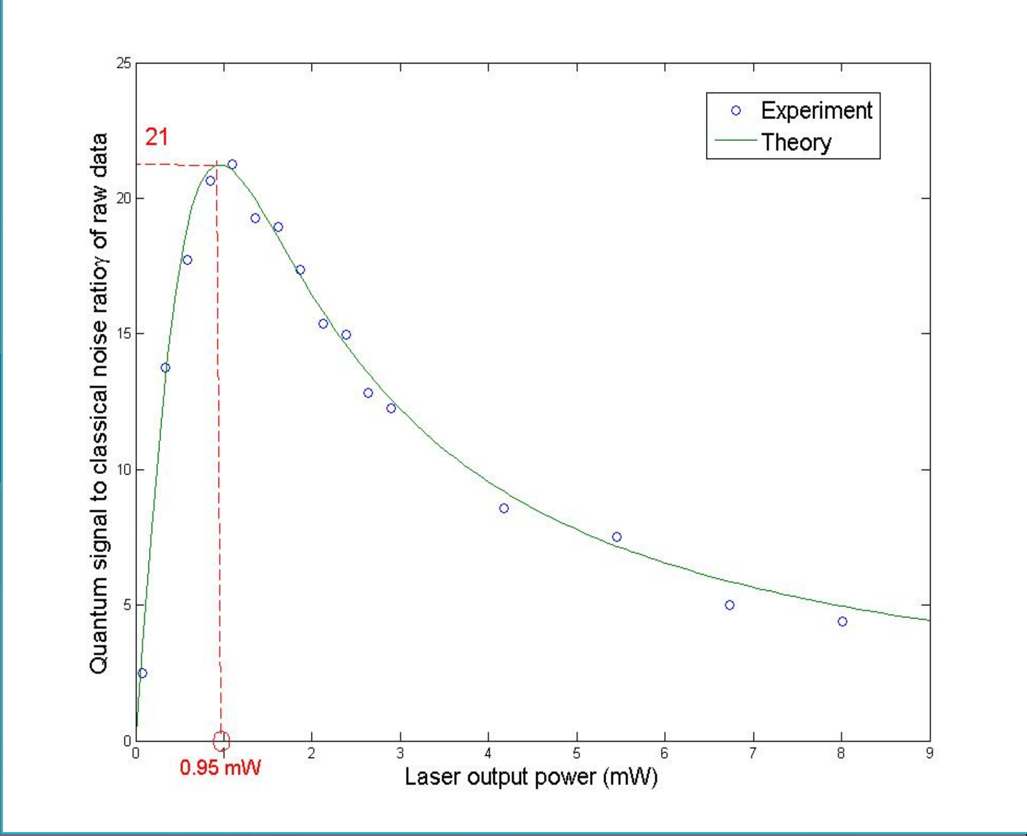
[1] C. H. Henry, IEEE J. Quantum Electron. QE-18, 259 (1982).

Quantum signal and classical noise

$$<V^2> = AQP + ACP^2 + F$$

F (mV²)	AQ (mV²/mW)	AC (mV²/mW²)
0.36±0.06	16.12±0.49	0.40±0.16

$$\gamma = \frac{AQP}{ACP^2 + F}$$



F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, H.-K. Lo, *arXiv: 1109.0643* (2011)

Post-processing

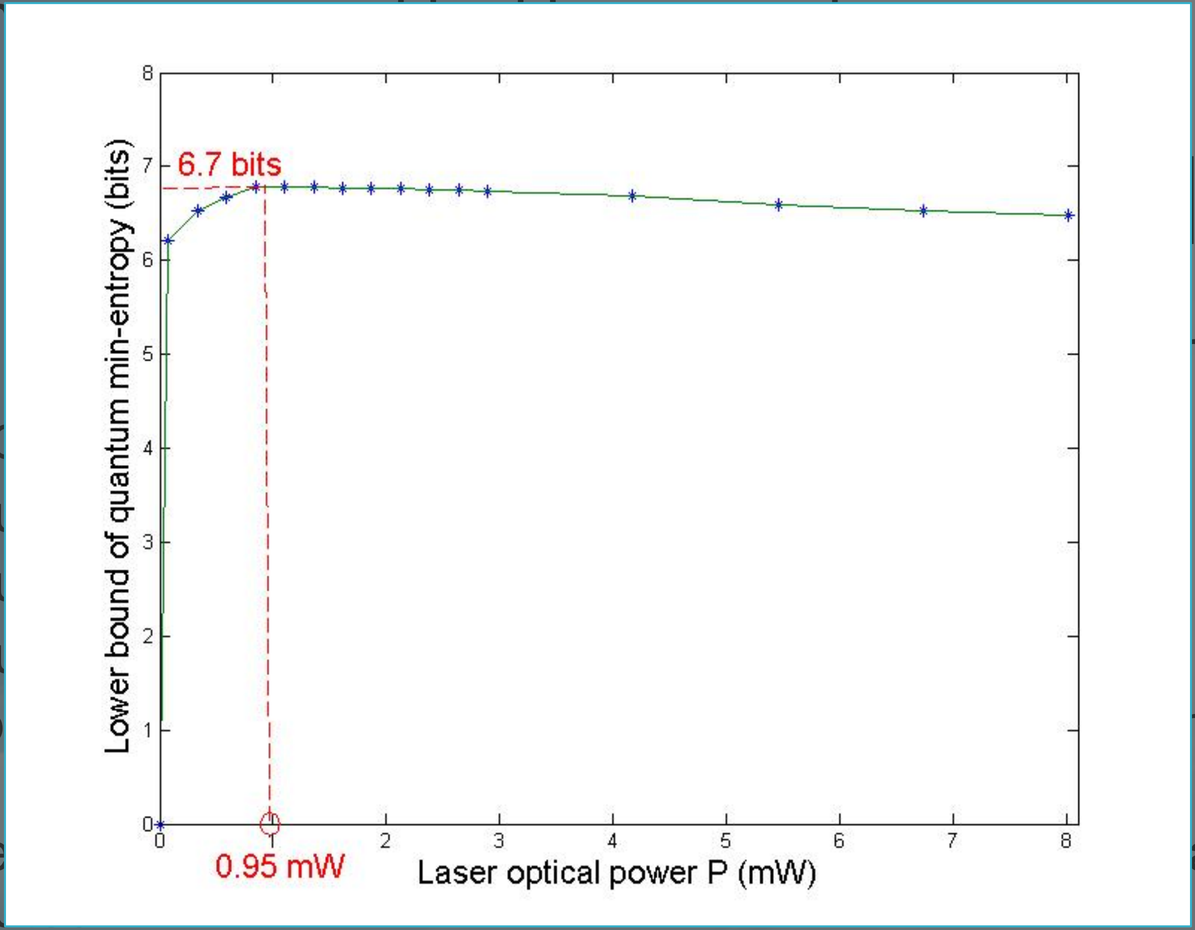
- Why we need post-processing?
  - Eve may have partial information (by controlling classical noise).
  - Quantum fluctuation is a non-uniform distribution (Gaussian).
- Extract out *uniform-quantum* randomness!

Randomness extractor!

- Procedure
  - Min-entropy evaluation
  - Randomness extraction

Min-entropy evaluation

- Randon
- Quantu ... model.
- Assump
  - Quantu
  - Quantu
  - Quantu
  - Total p ... nd classical noise,
  - The se ... ally distribu



F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, H.-K. Lo, *arXiv: 1109.0643* (2011)
X. Ma, et al, *under preparation*, (2011)

Randomness extraction

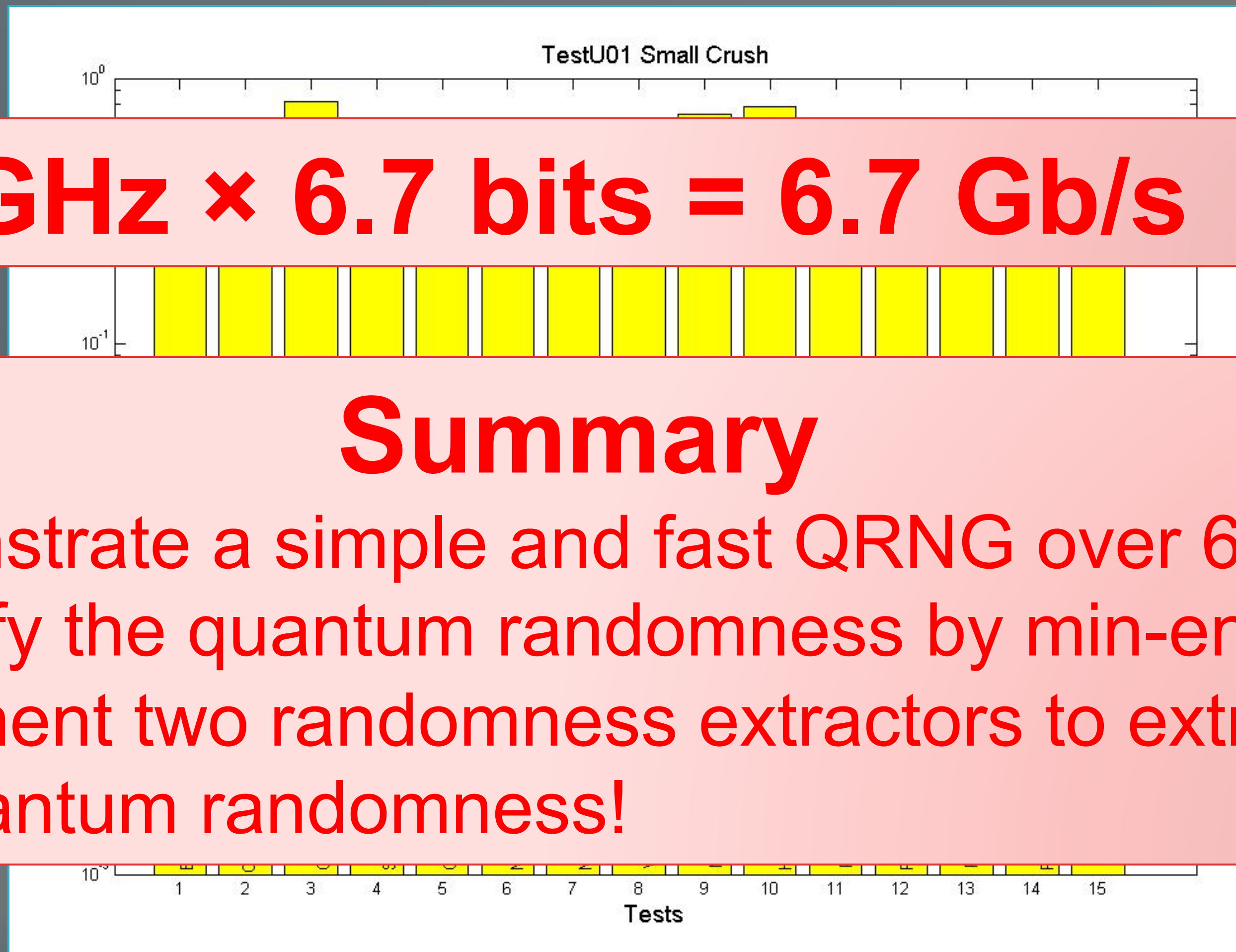
- Implement two extractors
  - Universal Hashing [1]
    - With Toeplitz matrix
  - Trevisan's Extractor [2]

Details of implementations:
Xiongfeng Ma, et al, *under preparation* (2011)

- QRNG with information-theoretically proven randomness!

[1] M. Wegman and J. Carter, Journal of computer and system sciences 22, 265 (1981).
[2] L. Trevisan, Journal of the ACM 48, 2001 (1999).

Extraction results: universal hashing



1 GHz × 6.7 bits = 6.7 Gb/s

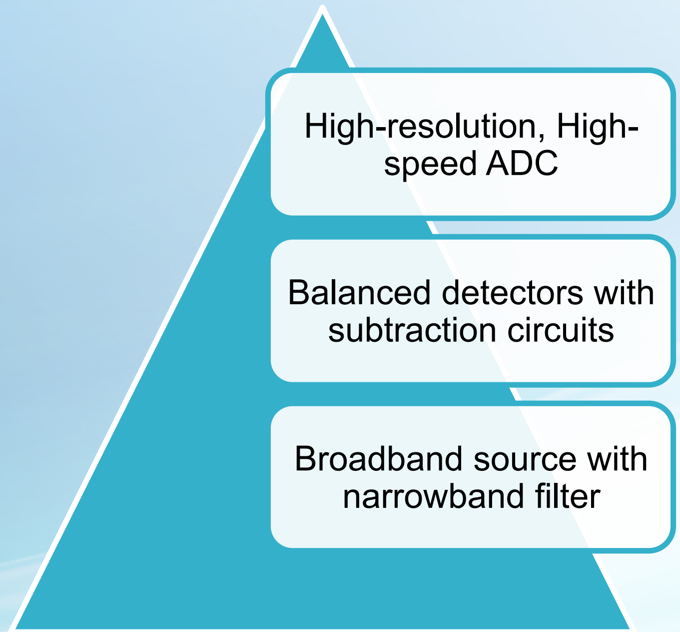
Summary

- Demonstrate a simple and fast QRNG over 6 Gb/s!
- Quantify the quantum randomness by min-entropy!
- Implement two randomness extractors to extract out the quantum randomness!

F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, H.-K. Lo, *arXiv: 1109.0643* (2011)

Future directions

- Optimize system design.



- High-speed electronics for real time randomness extraction.
- Random number storage & transfer.

Acknowledgements

NSERC
CRSNG

Canada Research
Chairs

QuantumWorks
QUANTUM INFORMATION
NETWORK CANADA
RÉSEAU DE L'INFORMATION
QUANTIQUE CANADA

VELUT ARBOR ÆVO

cifar
Canadian Institute for Advanced Research

Previous works:

- B. Qi, et al, *AQIS* (2009)
- B. Qi, et al, *Opt. Lett.* 35, 312 (2010)

Current works:

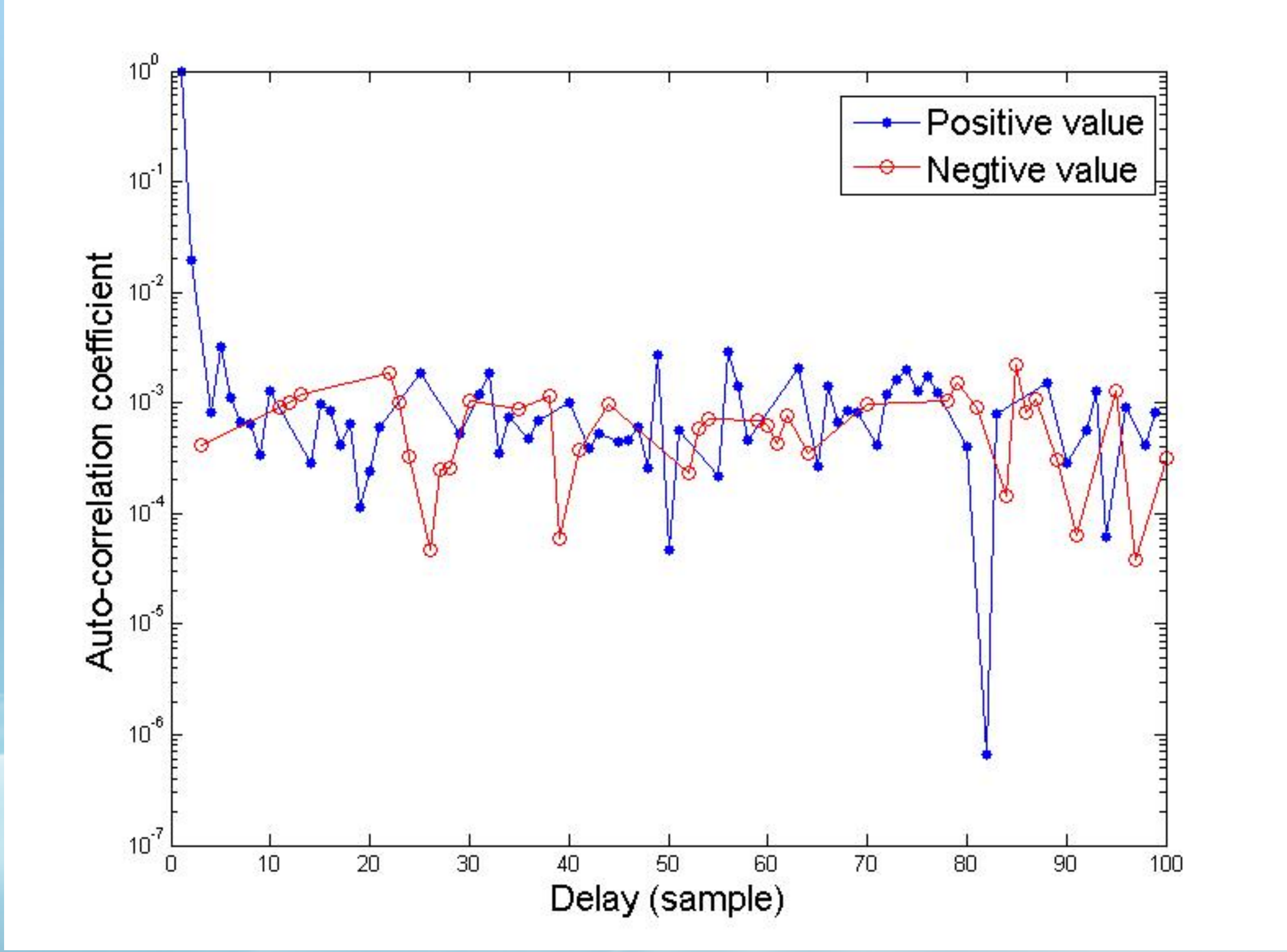
- Feihu Xu, et al, *arXiv: 1109.0643* (2011)
- Xiongfeng Ma, et al, *under preparation* (2011)

Thank You !

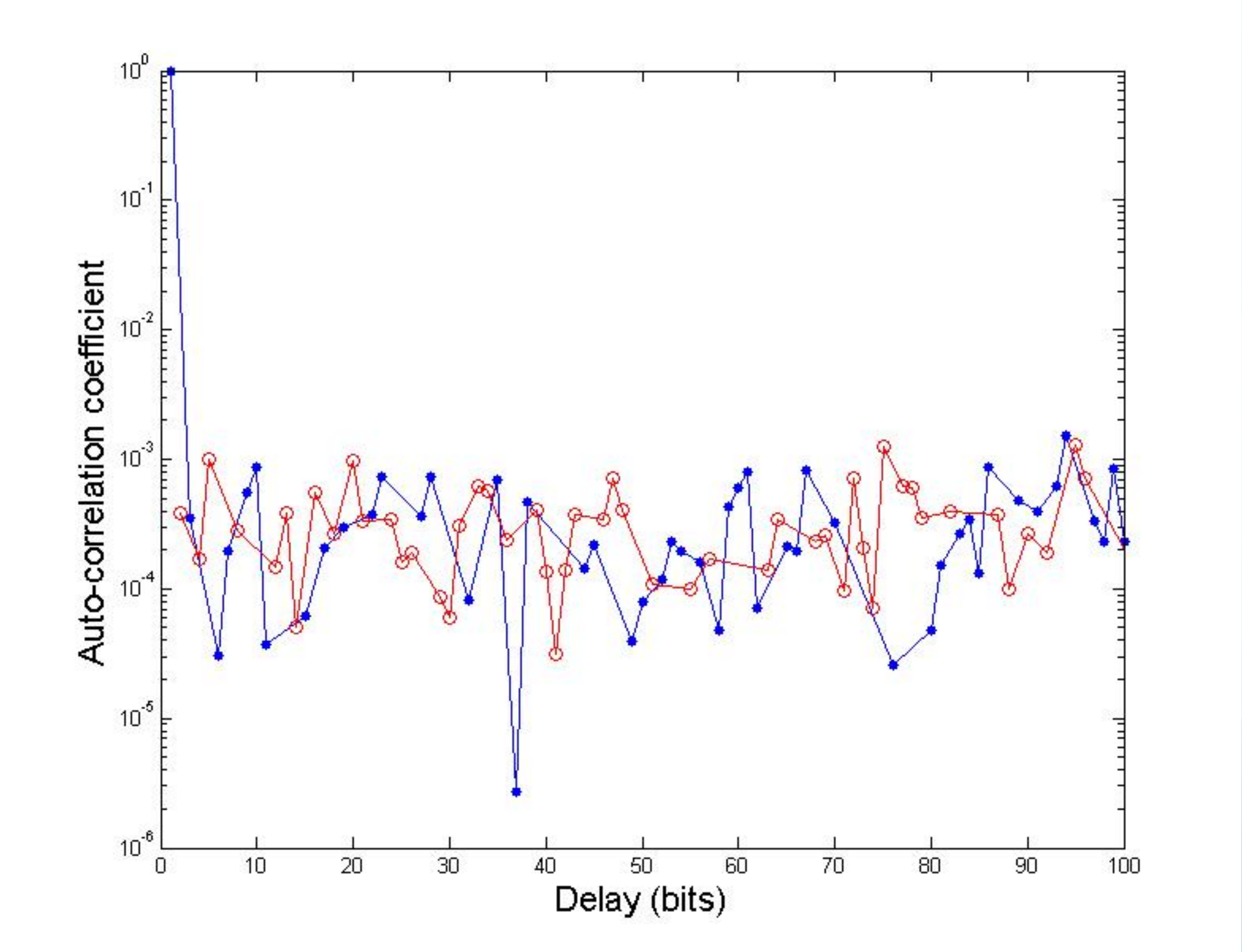
UNIVERSITY OF TORONTO

Backup part

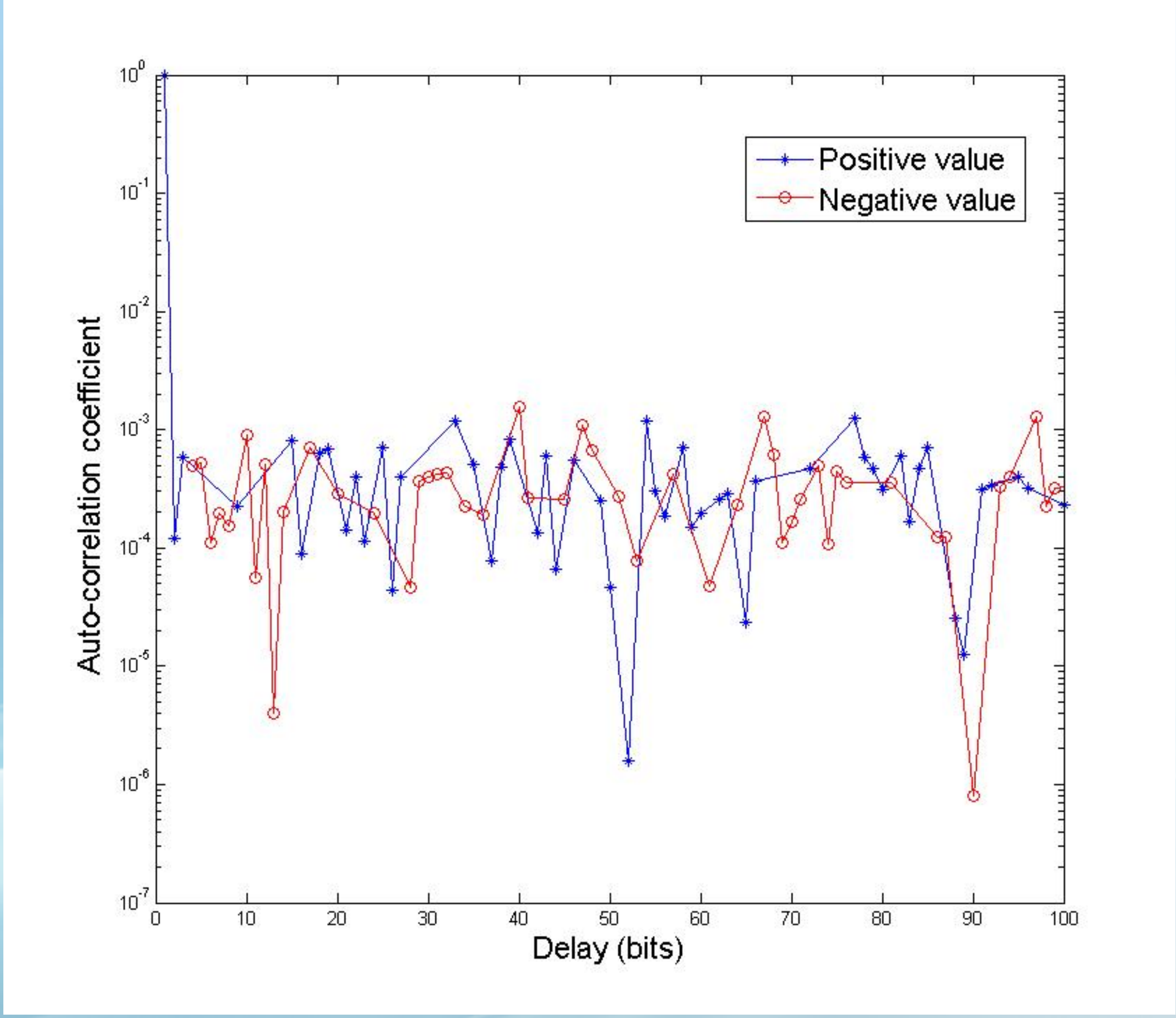
Autocorrelation of raw data



Autocorrelation of Toeplitz-hashing output



Autocorrelation of Trevisan’s extractor output



UNIVERSITY OF TORONTO

Diehard

	Pseudo-RNG	Raw data	Trevisan's		Toeplitz-hashing	
Statistical test	Result	Result	p-value	result	p-value	result
Birthday Spacings [KS]	success	*failure*	0.82263	success	0.340863	success
Overlapping permutations	success	*failure*	0.679927	success	0.403824	success
Ranks of 31x31 matrices	success	*failure*	0.419095	success	0.349441	success
Ranks of 31x32 matrices	success	*failure*	0.715705	success	0.816752	success
Ranks of 6x8 matrices [KS]	success	*failure*	0.195485	success	0.408573	success
Bit stream test	success	*failure*	0.048260	success	0.281680	success
Monkey test OPSO	success	*failure*	0.027300	success	0.892600	success
Monkey test OQSO	success	*failure*	0.023200	success	0.267200	success
Monkey test DNA	*failure*	*failure*	0.038000	success	0.736700	success
Count 1's in stream of bytes	success	*failure*	0.380162	success	0.639691	success
Count 1's in specific bytes	*failure*	*failure*	0.020417	success	0.373149	success
Parking lot test [KS]	*failure*	*failure*	0.629013	success	0.151689	success
Minimum distance test [KS]	success	*failure*	0.019499	success	0.688780	success
Random spheres test [KS]	success	*failure*	0.488703	success	0.939227	success
Squeeze test	success	*failure*	0.238004	success	0.155403	success
Overlapping sums test [KS]	success	*failure*	0.022339	success	0.909675	success
Runs test (up) [KS]	*failure*	*failure*	0.403504	success	0.181024	success
Runs test (down) [KS]	success	*failure*	0.119132	success	0.668512	success
Craps test No. of wins	success	*failure*	0.757521	success	0.826358	success
Craps test throws/game	success	*failure*	0.179705	success	0.862986	success

TABLE V: **Diehard.** Data size is 240MBits. For the cases of multiple P-values, a Kolmogorov-smirnov (KS) test is used to obtain a final P-value, which measures the uniformity of the multiple P-values. The test is successful if all final P-values satisfy $0.01 \leq P \leq 0.99$

NIST

	Pseudo-RNG	Raw data	Toeplitz-hashing		
Statistical test	Result	Result	p-value	Proportion	Result
Frequency	success	*failure*	0.373625	0.9900	success
Block-frequency	success	*failure*	0.310049	0.9960	success
Cumulative sums	success	*failure*	0.422638	0.9980	success
Runs	success	*failure*	0.703417	0.9900	success
LongestRun	success	*failure*	0.013569	0.9880	success
Rank	success	*failure*	0.411840	0.9940	success
FFT	success	*failure*	0.987079	0.9860	success
NonOverlappingTemplate	*failure*	*failure*	0.727851	0.9820	success
overlappingTemplate	success	*failure*	0.110083	0.9780	success
Universal	success	*failure*	0.962688	0.9880	success
ApproximateEntropy	success	*failure*	0.674543	0.9920	success
Random-excursions	success	*failure*	0.409207	0.9900	success
Random-excursions Variant	success	*failure*	0.426358	0.9840	success
Serial	success	*failure*	0.217570	0.9860	success
Linear-complexity	success	*failure*	0.657833	0.9940	success

TABLE VI: **NIST.** Data size is 3.25 Gbits (500 sequences with each sequence around 6.5 Mbits). To pass the test, P-value should be larger than the lowest significant level $\alpha = 0.01$, and the proportion of sequences satisfying $P > \alpha$ should be greater than 0.976. Where the test has multiple P-values, the worst case is selected.

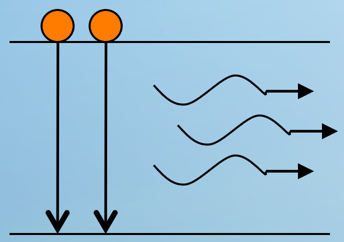
TestU01

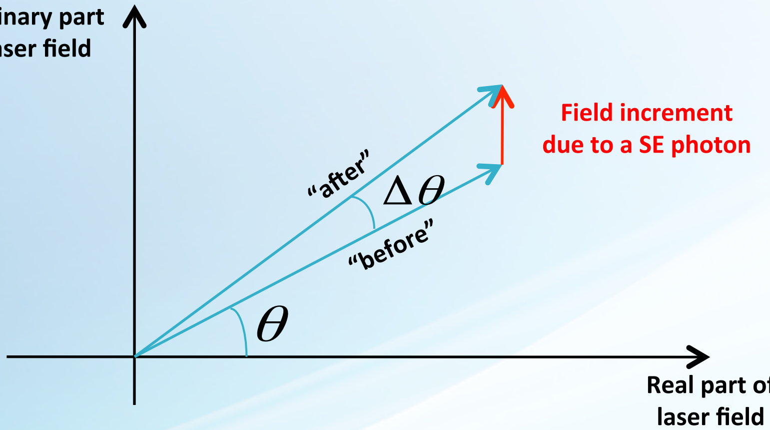
	Pseudo-RNG	Raw data	Toeplitz-hashing	
Statistical Test	Result	Result	p-value	Result
BirthdaySpacings	Success	*failure*	0.5300	success
Collision	Success	*failure*	0.1500	success
Gap Chi-square	success	*failure*	0.8900	success
SimpPoker Chi-square	success	*failure*	0.3500	success
CouponCollector Chi-square	success	*failure*	0.6700	success
MaxOft Chi-square	success	*failure*	0.6900	success
MaxOft Anderson-Darling	success	*failure*	0.9500	success
WeightDistrib Chi-square	success	*failure*	0.5600	success
MatrixRank Chi-square	success	*failure*	0.5100	success
Hammingindep Chi-square	success	*failure*	0.1000	success
RandomWalk1 H Chi-square	success	*failure*	0.9931	success
RandomWalk1 M Chi-square	success	*failure*	0.8300	success
RandomWalk1 J Chi-square	success	*failure*	0.9400	success
RandomWalk1 R Chi-square	success	*failure*	0.7000	success
RandomWalk1 C Chi-square	success	*failure*	0.6600	success

TABLE VII: **TestU01 (Small Crush).** Given the constraint of the data size and computational power of Crush and Big Crush of TestU01, we only perform Small Crush test here. Data size is 8 Gbits. The P-value of falling a test converges to 0 or 1 (eps or 1-eps). Where the test has multiple P-values, the worst case is selected.

Our approach: randomness from laser phase noise

- Physical origin: spontaneous emissions [1, 2]





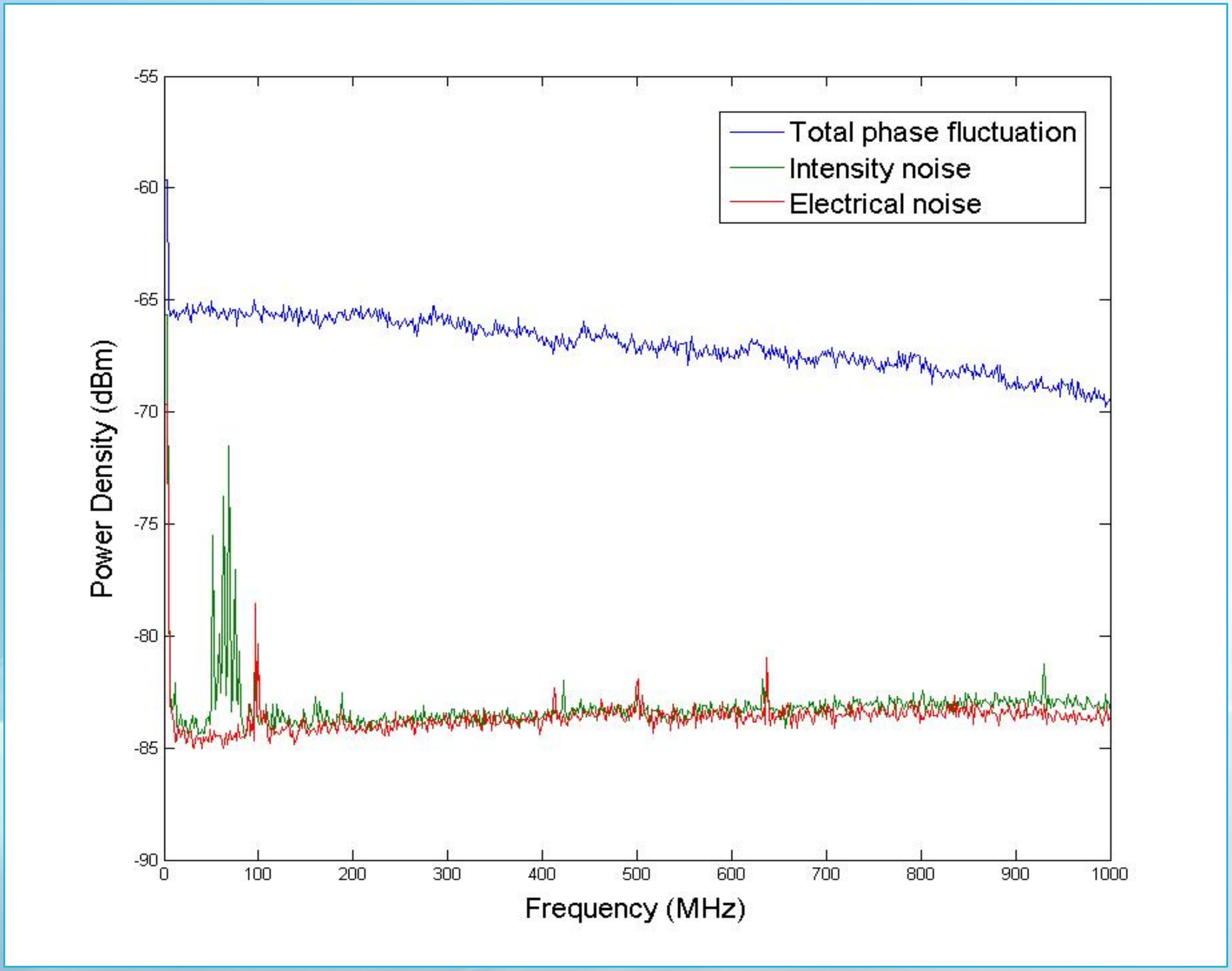
- Quantum phase change within time *t* can be treated as a Gaussian white noise [1,2]

$$\Delta\theta(t) \sim N(0, 2\pi t \Delta f)$$

Laser linewidth

[1] A. Yariv and P. Yeh, "Photonics: optical electronics in modern communications" (6th edition), Oxford University Press (2007).
[2] K. Petermann, "Laser diode modulation and noise", (Springer, 1988).

Laser Intensity Noise



UNIVERSITY OF TORONTO