The impact of digitization on the entropy generation rates of physical sources of randomness

Joseph D. Hart[1,2,*], Thomas E. Murphy[2,3], Rajarshi Roy[2,3,4], Gerry Baumgartner[5]

[1] Dept. of Physics

[2] Institute for Research in Electronics & Applied Physics

[3] Dept. of Electrical & Computer Engineering

[4] Institute for Physical Science and Technology

[5] Laboratory for Telecommunication Science

UNIVERSITY OF MARYLAND

[*] jhart12@umd.edu

Why Physical RNG?

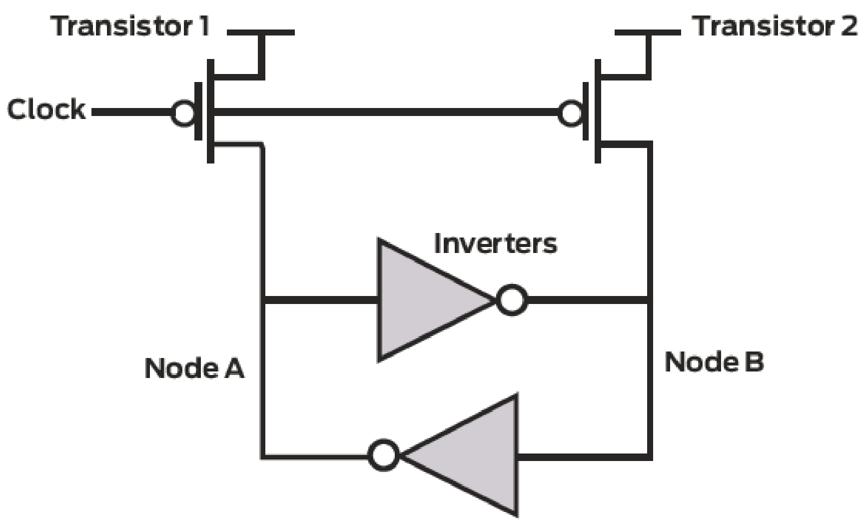
Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin.

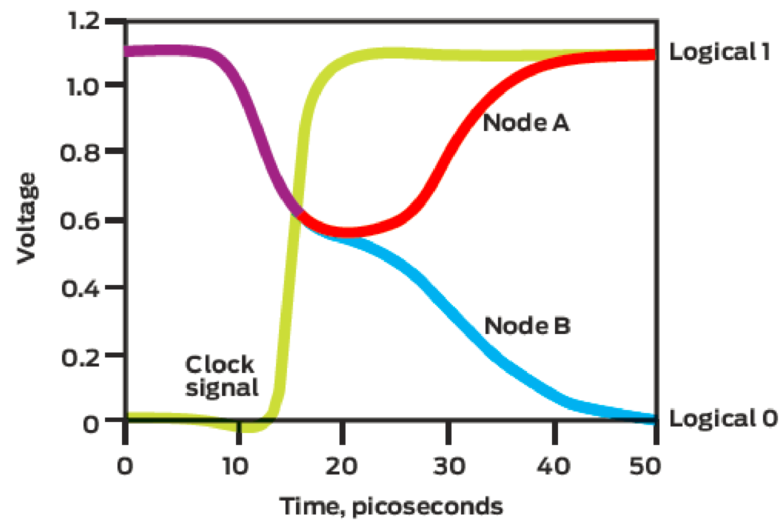
--John von Neumann

Physical RNG

- Algorithms can only produce pseudo-random numbers
- For true random numbers, we turn to physical systems
- Can be FASTER because not limited by CPU clock
- Need to be post-processed to remove bias, etc.
- Important differences between pseudo-RNG and physical RNG should be reflected in evaluation metrics

Electronic Physical RNG Today (Intel Ivy Bridge Processors)



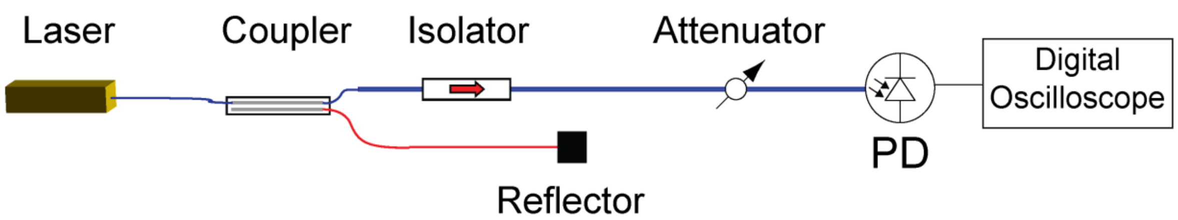


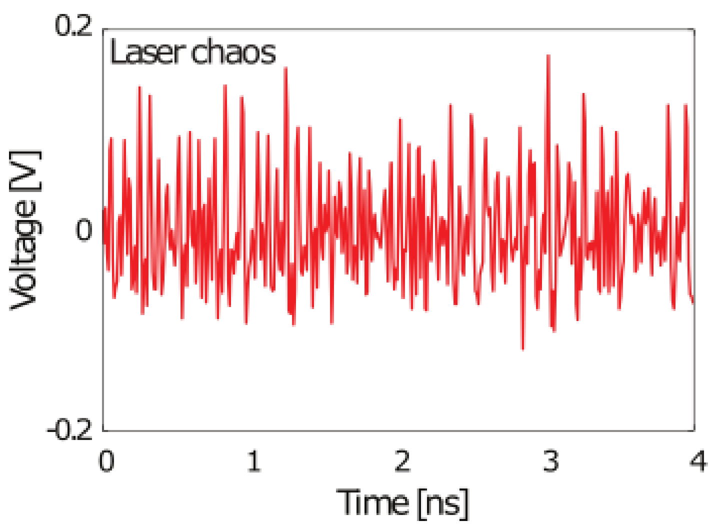
- 3 Gb/s raw RNG rate
- Raw bits are not directly used (nor accessible)
- Continuously re-seeds a pseudo-random generator
- Instruction: RDRND

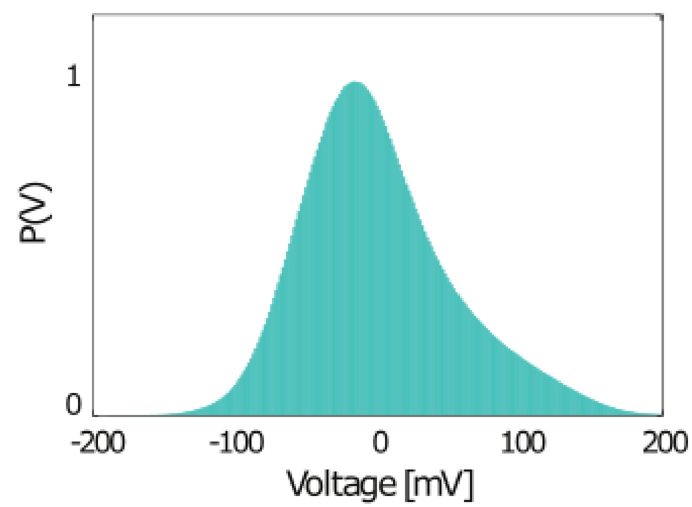
Chaotic Semiconductor Laser

- Fluctuations are fast and chaotic

(sensitive dependence on initial conditions)



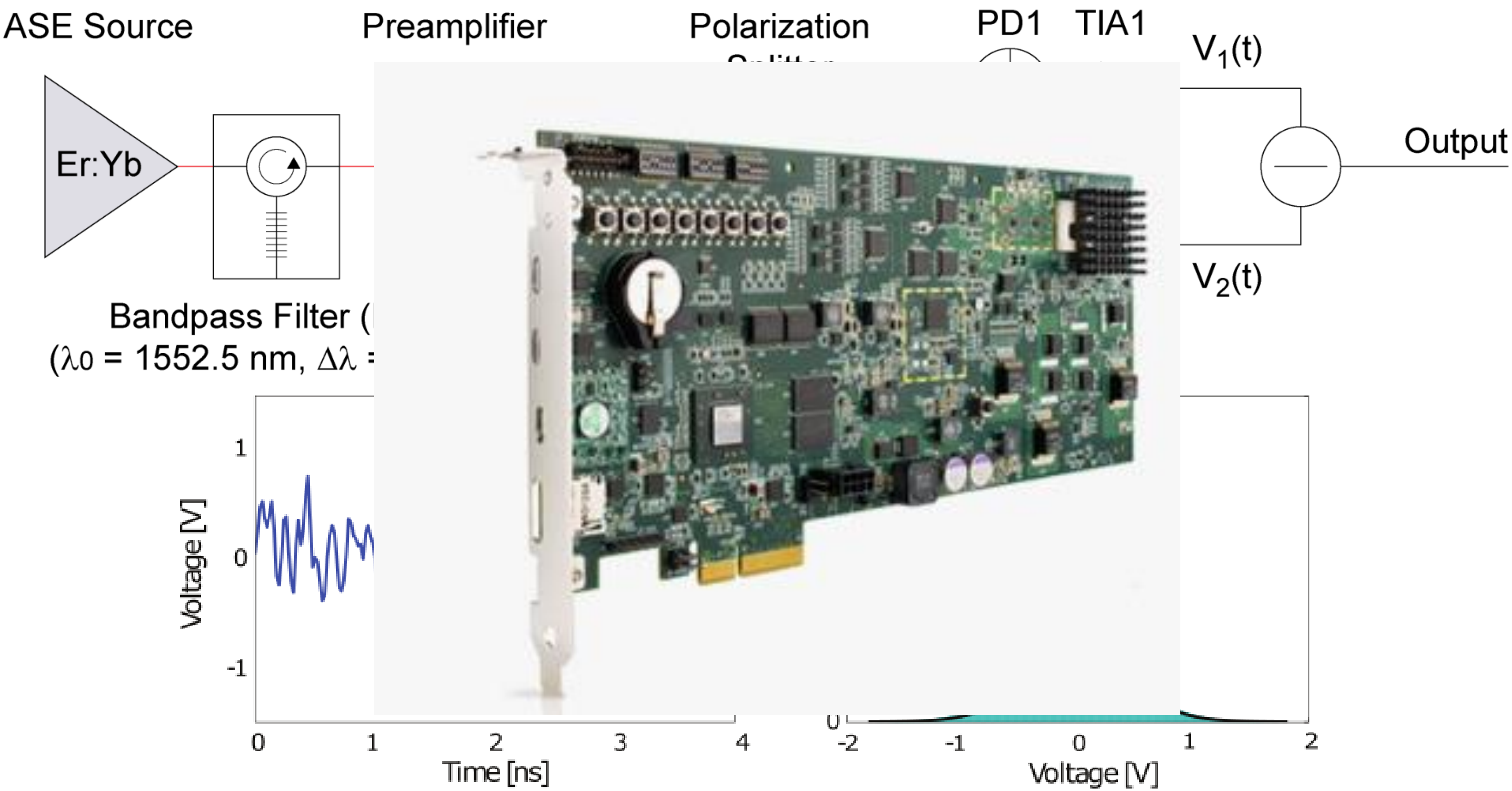




Sakuraba, Ryohsuke, et al. *Optics express* 23.2 (2015): 1470-1490.

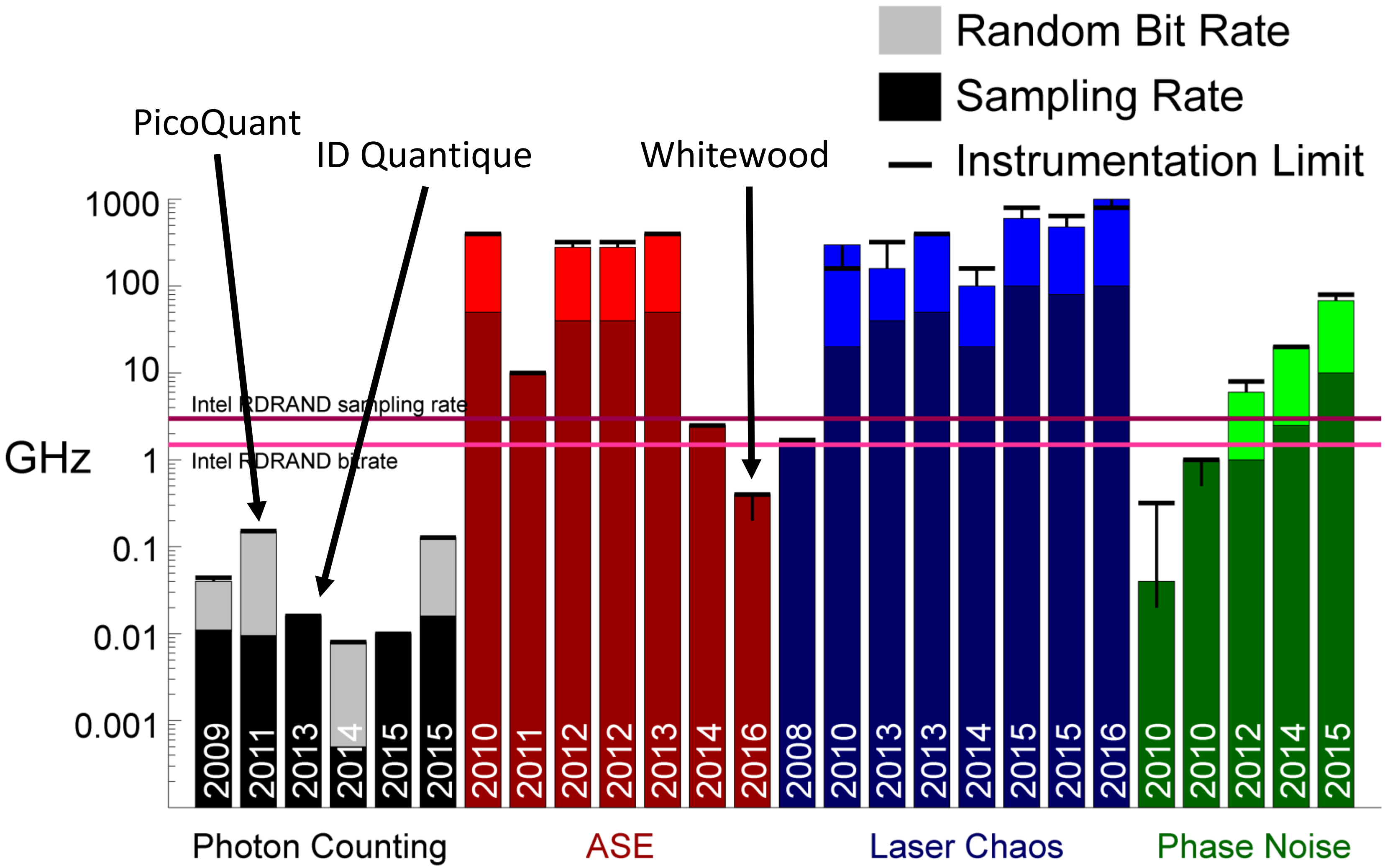
WHITEWOOD

Amplifie ... ission



C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Optics Express **18**, 23584–23597 (2010).

Comparison of Optical RNG Methods – Recent Research

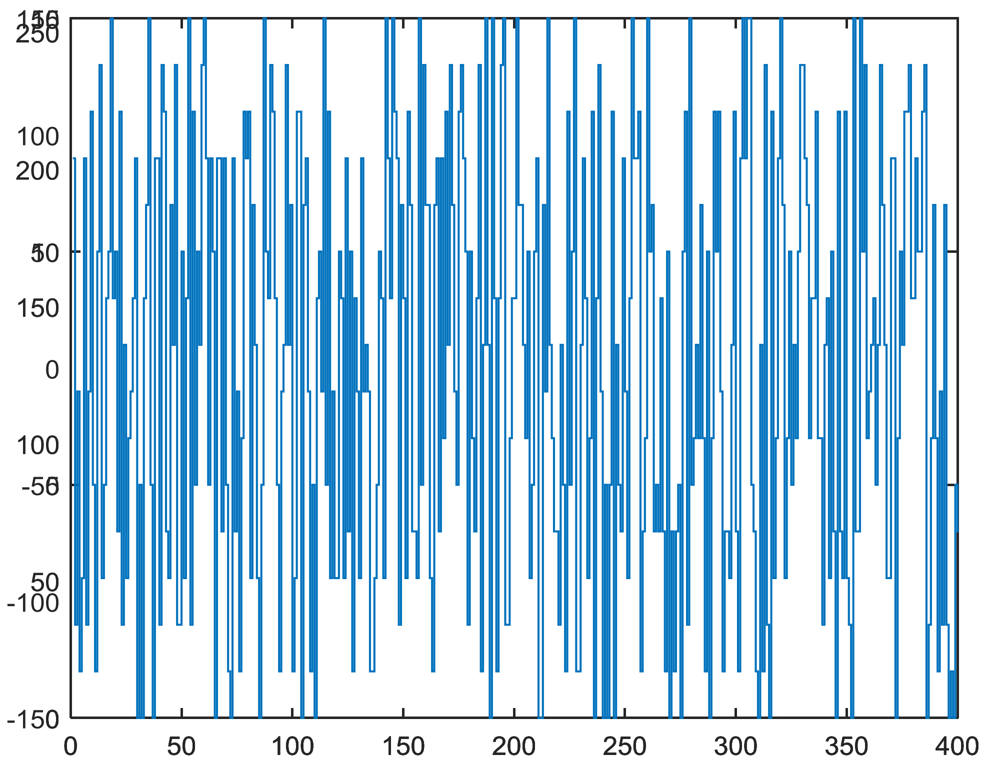


NIST SP 800-22rev1a

- Easy to implement
- Publicly accessible standard
- Even non-cryptographically secure Pseudo-RNG methods (e.g., Mersenne Twister) will pass all tests
- Only works on binary data (1s and 0s), not analog data or waveforms
- Most physical RNG methods require post-processing to pass tests

Post-Processing of Digitized Waveforms

- Least Significant Bit Extraction:



What is the source of entropy?
(waveform, digitizer, thermal noise?)

Entropy estimates

- Try to quantify the number of random bits allowed to be harvested from a physical system
- Works on raw data, not post-processed data
- Can help reveal *where* the entropy is coming from
- Can be slower, require more data than NIST SP 800-22rev1a

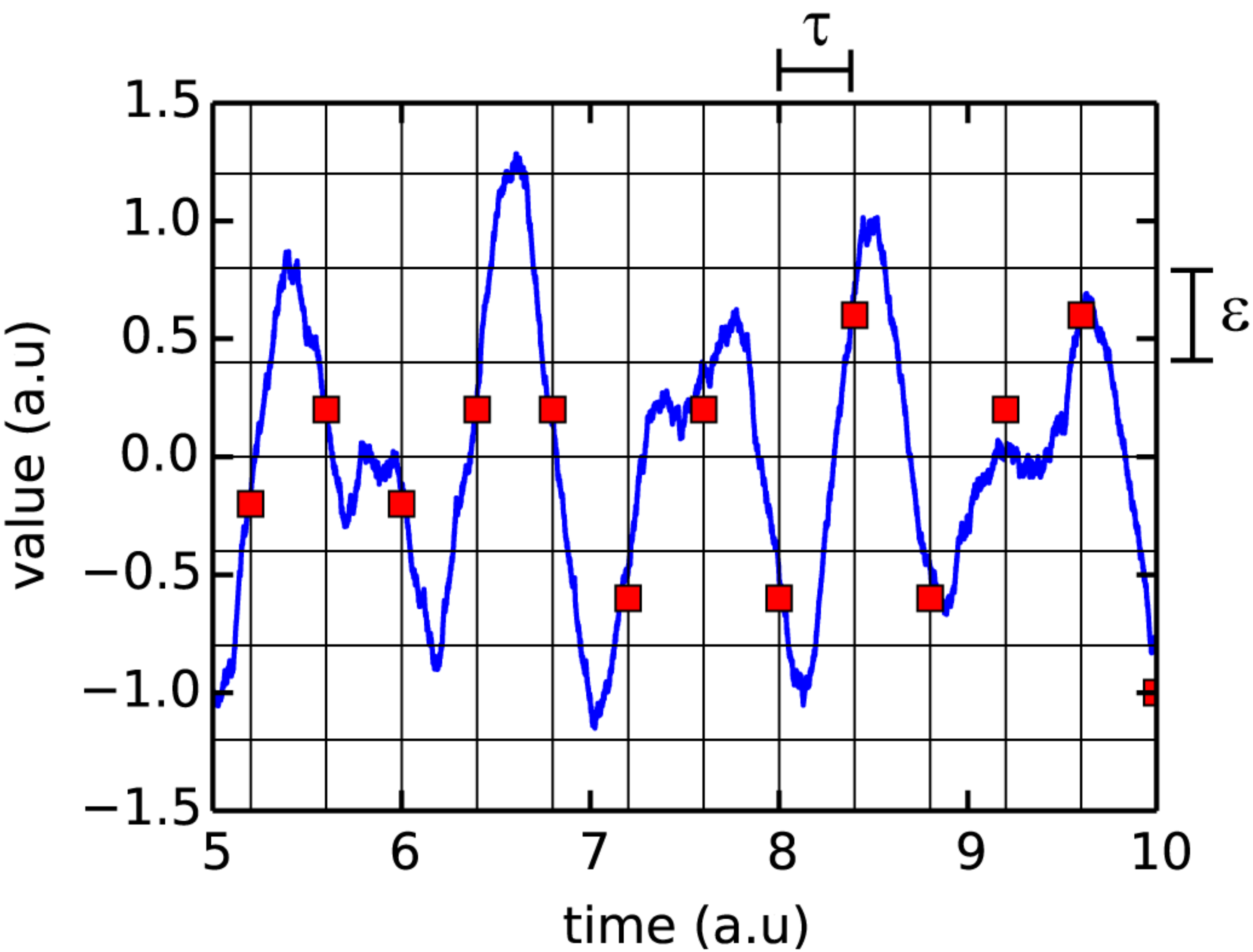
Dynamical systems approach to entropy generation

- Kolmogorov-Sinai (or metric) entropy

$$H = -\frac{1}{d\tau}\sum p(i_1, \ldots, i_d) \log_2 p(i_1, \ldots, i_d)$$

- Analog of Shannon entropy for dynamical system
- Allows for direct comparison of dynamical processes, stochastic processes, and mixed processes

Discretization of analog signals

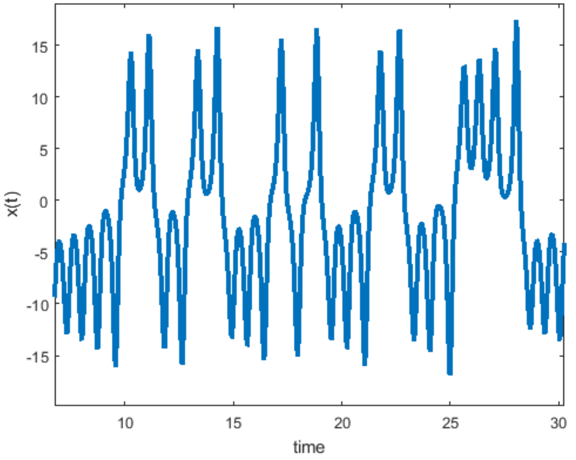


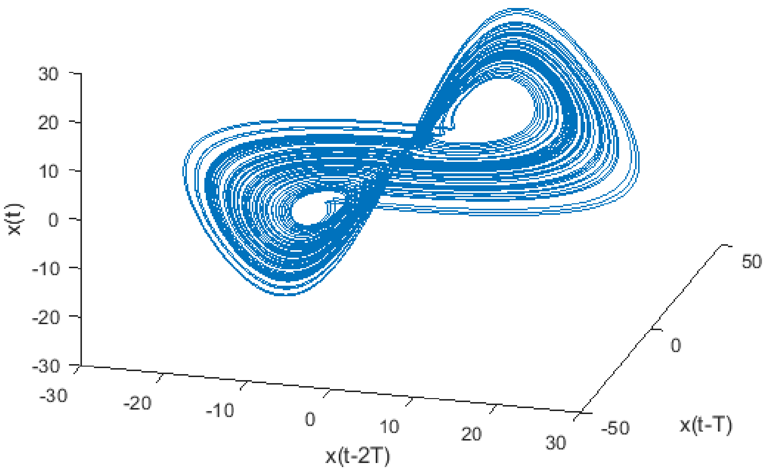
Time-delay embedding

- Reconstruct phase-space of dynamical system from measurement of one variable

$$\vec{\mathbf{x}}(t) = (x(t), x(t-T), \ldots, x(t-(d-1)T))$$

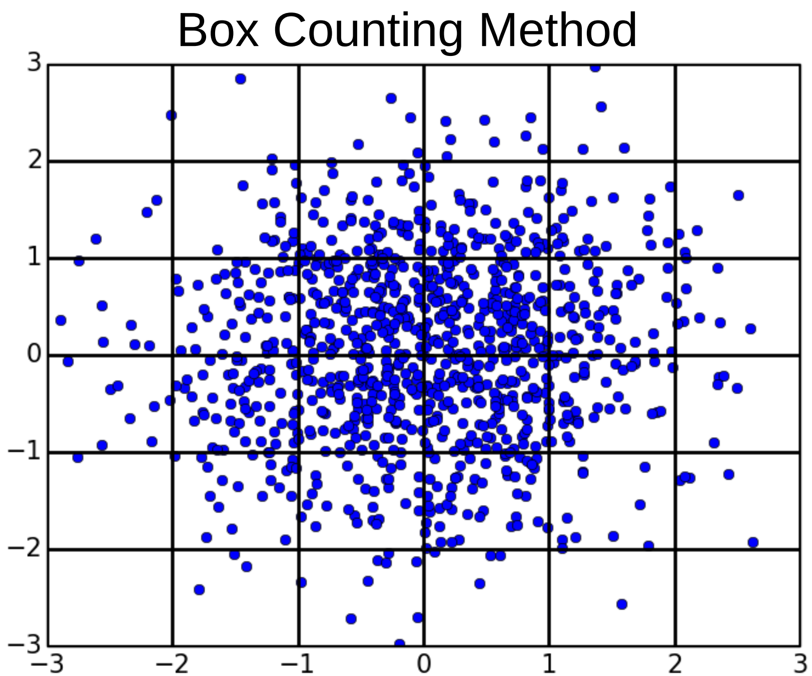
Lorenz attractor

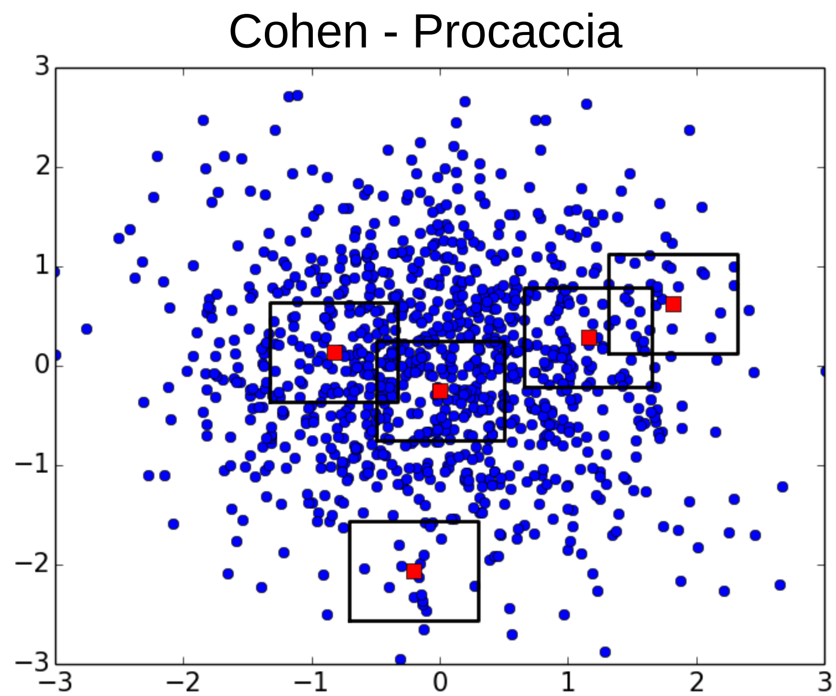




Takens, Floris. *Detecting strange attractors in turbulence*. Springer Berlin Heidelberg, 1981.

Numerically Estimating Entropy





$$H = -\sum_i \frac{N_i}{N} \log_2 \frac{N_i}{N}$$

$$H = -\frac{1}{N_r} \sum_i \log_2 \frac{N_i}{N}$$

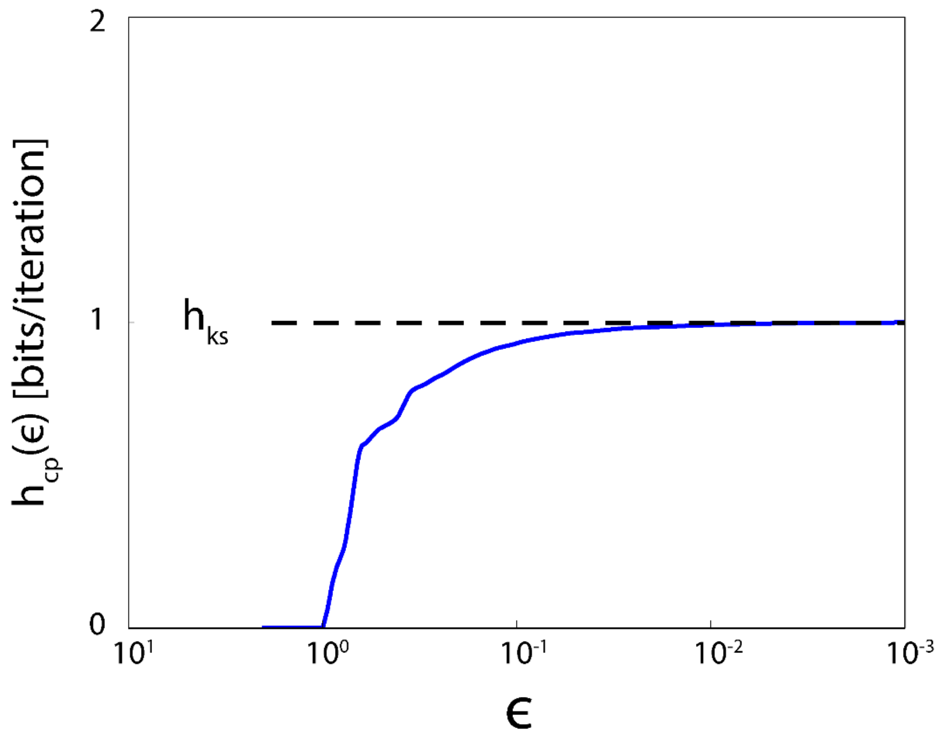
Cohen and Procaccia, “Computing the Kolmogorov entropy from time signals of dissipative and conservative dynamical systems”, Phys. Rev. A **31**, 1872 (1985)

Entropy of chaotic systems

For small ε

$$h(\varepsilon) = h_{KS} = \frac{1}{\ln(2)} \sum_{\lambda_i > 0} \lambda_i$$

$$X_{t+1} = 4X_t(1 - X_t)$$

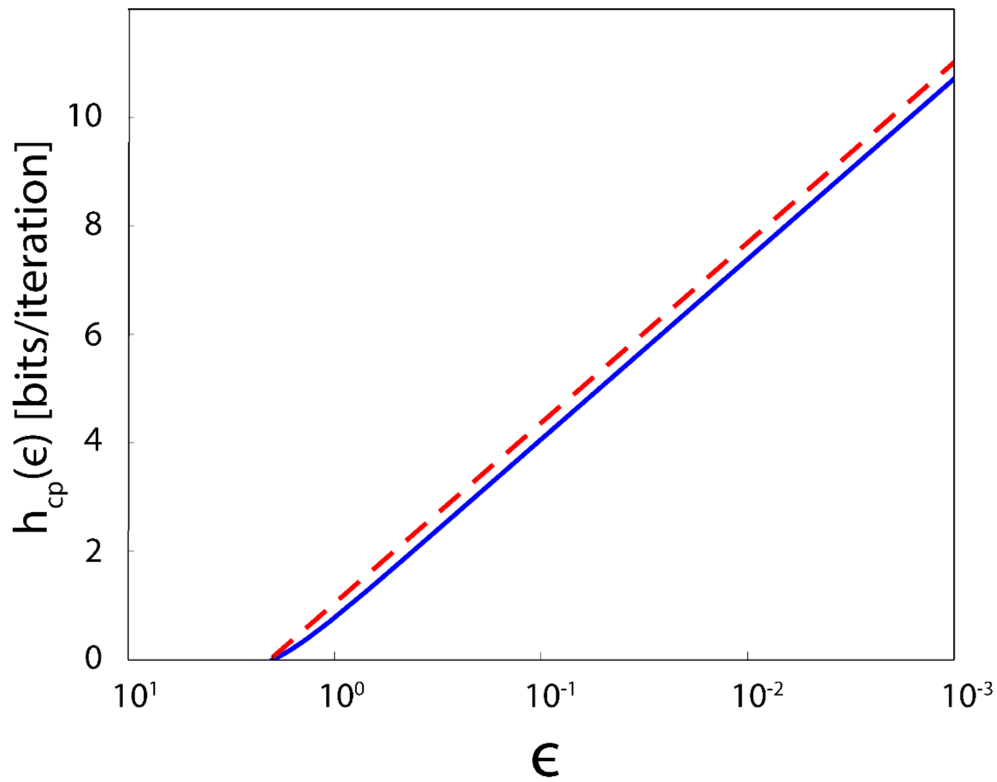


P. Gaspard and X. Wang,
Physics Reports,
Volume 235, 1993

(ε-τ) entropy of noise

$$h(\varepsilon) \sim -\log_2(\varepsilon)$$

Gaussian random variable



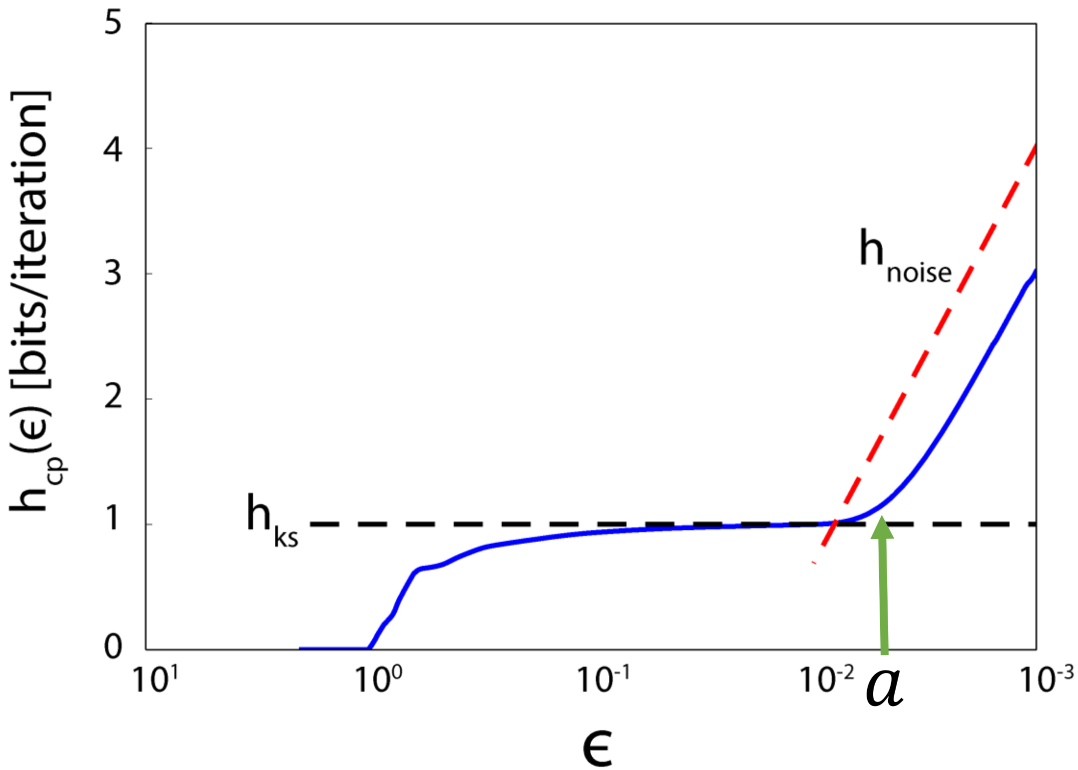
P. Gaspard and X. Wang,
Physics Reports,
Volume 235, 1993

Noisy chaotic systems

$$Z_{t+1} = X_t + aR_t$$

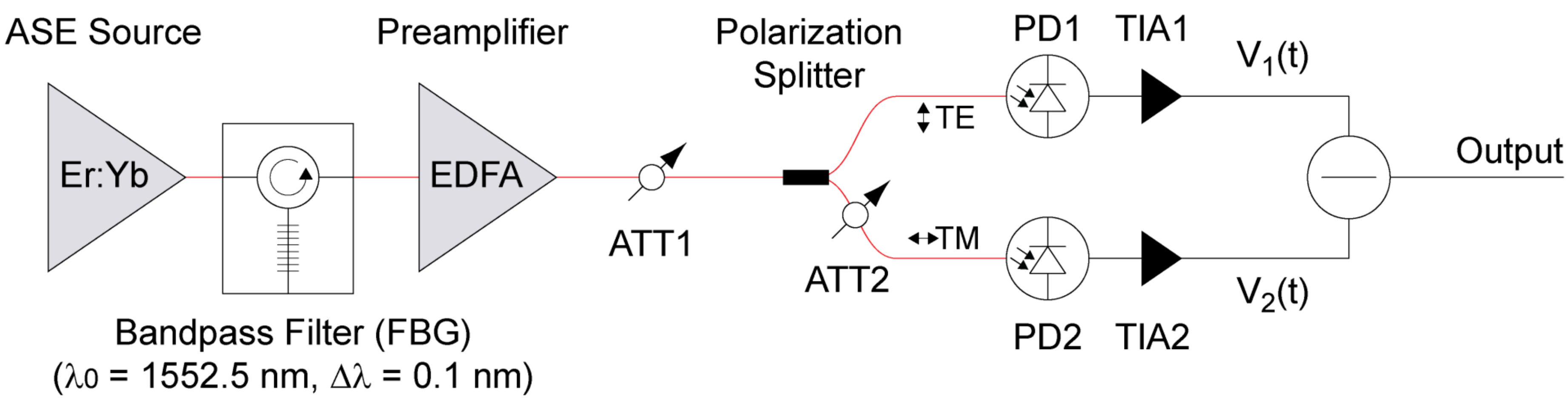
$$X_{t+1} = 4X_t(1 - X_t)$$

R is random Gaussian variable



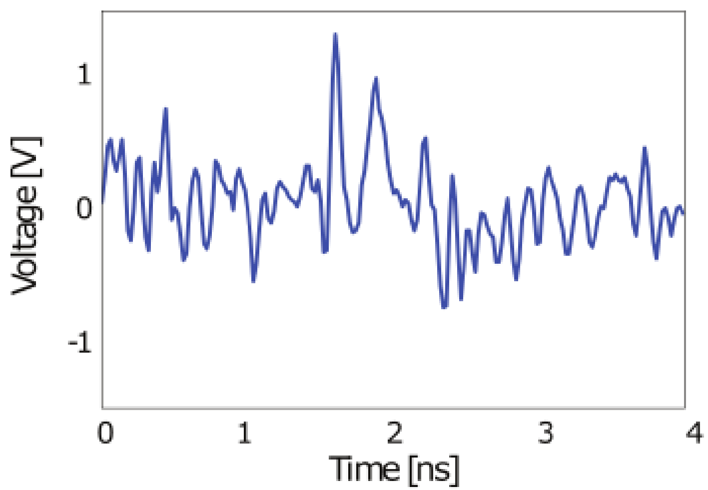
P. Gaspard and X. Wang,
Physics Reports,
Volume 235, 1993

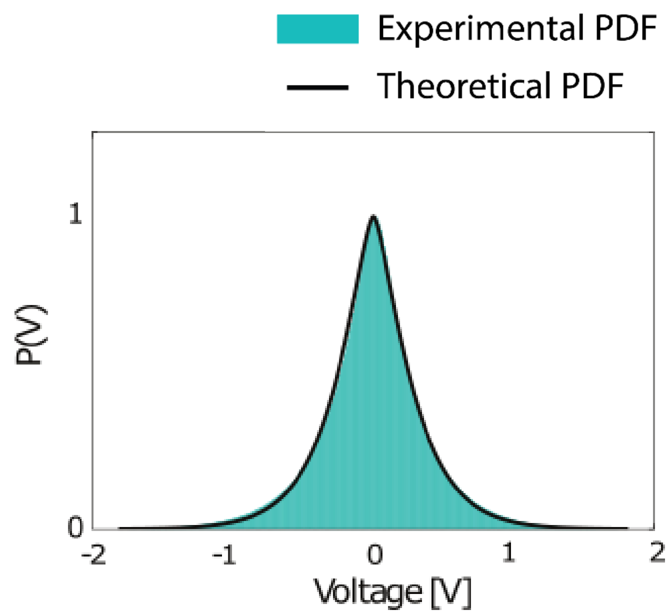
Case study:
Amplified Spontaneous Emission (ASE)

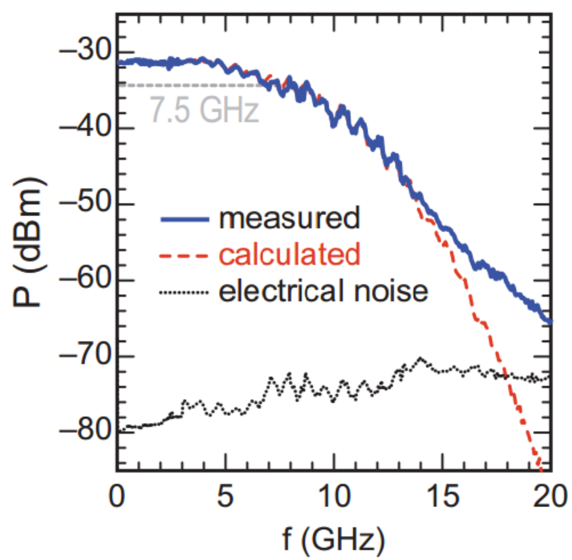


C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Optics Express **18**, 23584–23597 (2010).

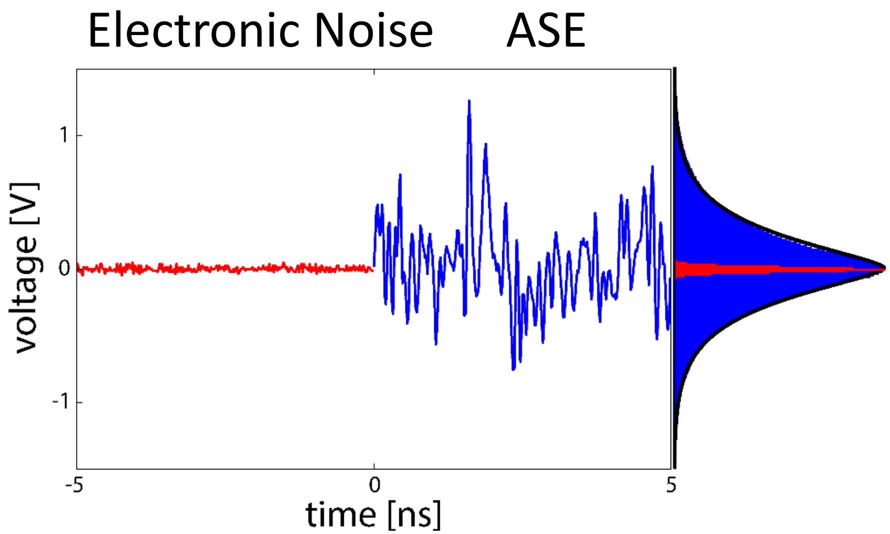
ASE

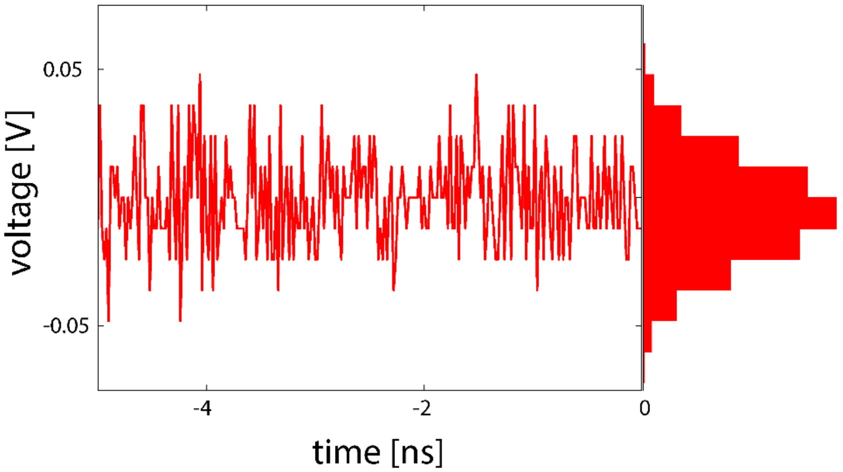

Voltage [V]
1
0
-1
0
1
2
3
4
Time [ns]


Experimental PDF
Theoretical PDF
P(V)
1
0
-2
-1
0
1
2
Voltage [V]


P (dBm)
–30
–40
–50
–60
–70
–80
7.5 GHz
measured
calculated
electrical noise
0
5
10
15
20
f (GHz)

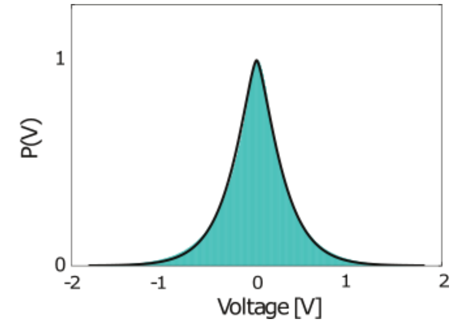
Signal and Noise

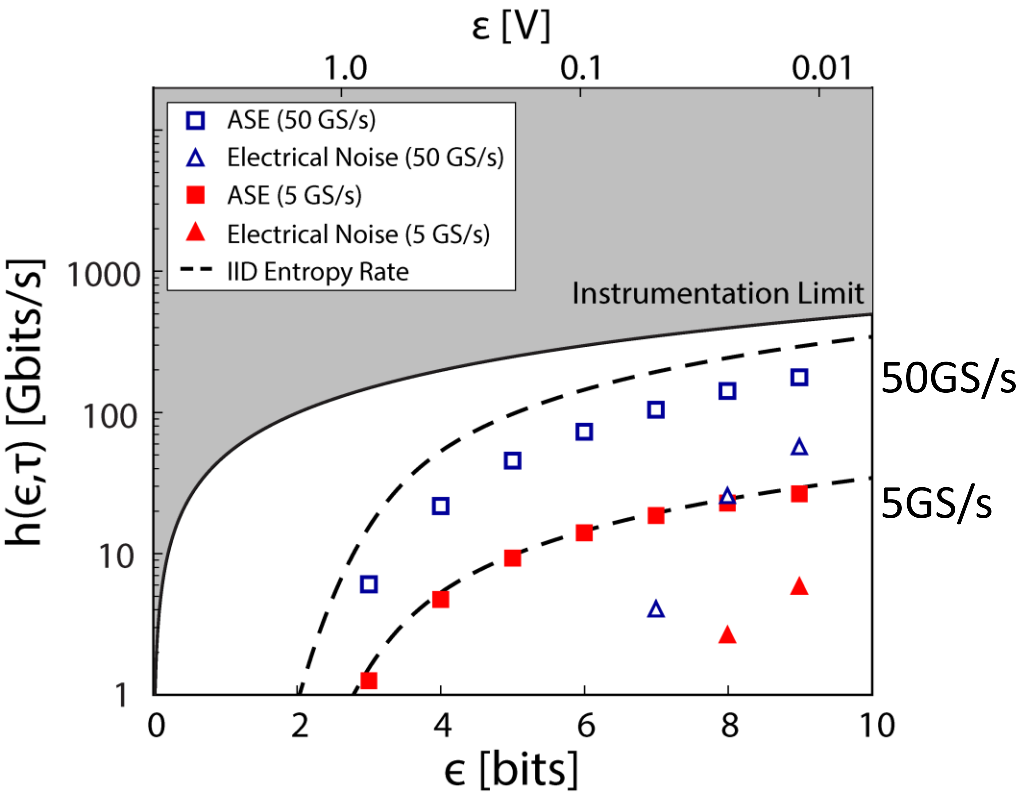




- Least-significant bits contribute considerable entropy (not optical!)

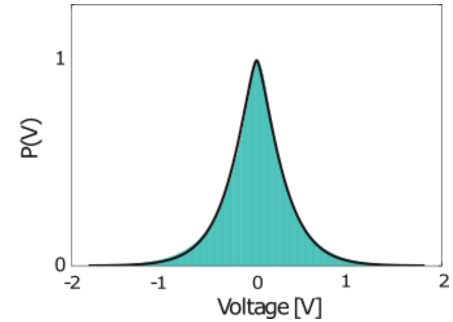
Entropy Rate - ASE

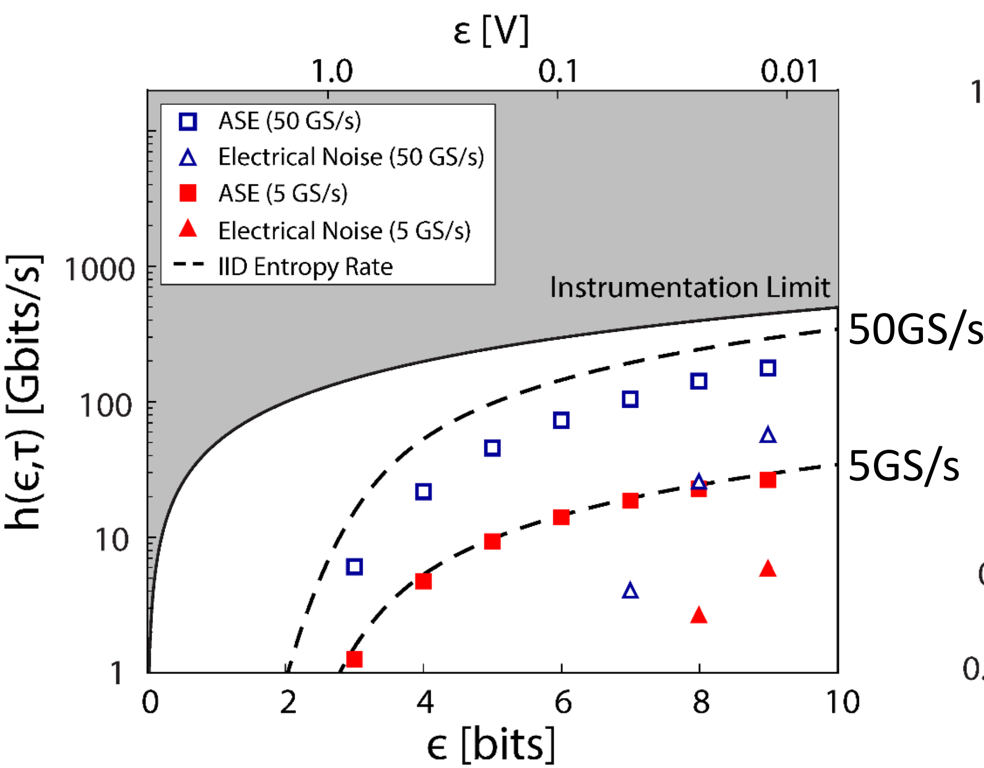


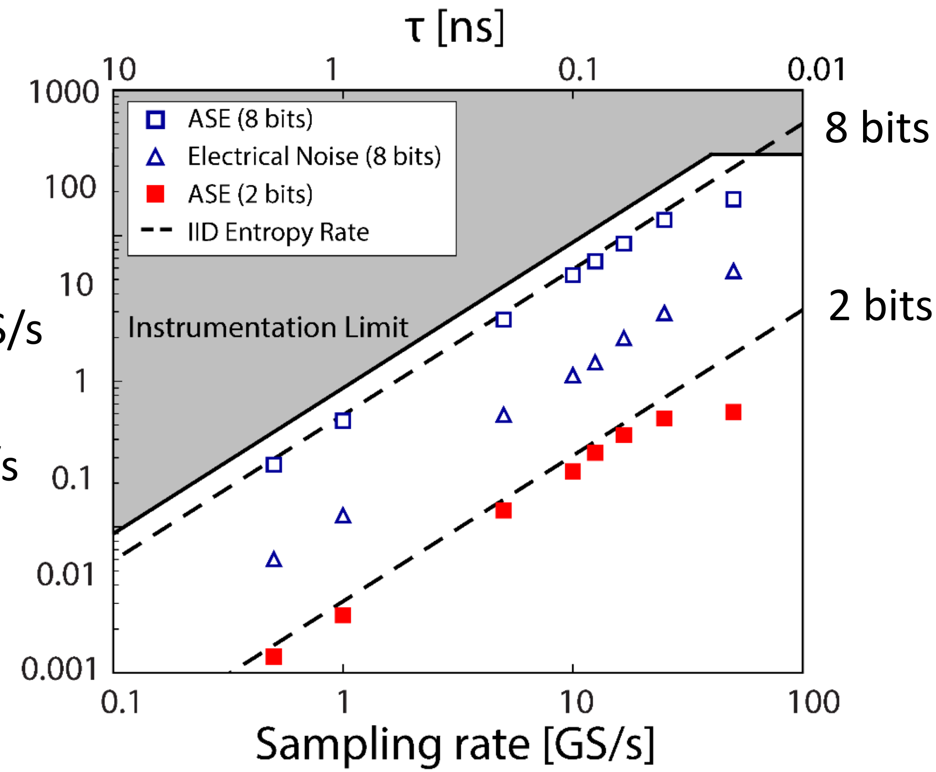


- Entropy rolls off with sample rate

Entropy Rate - ASE







- Entropy rolls off with sample rate

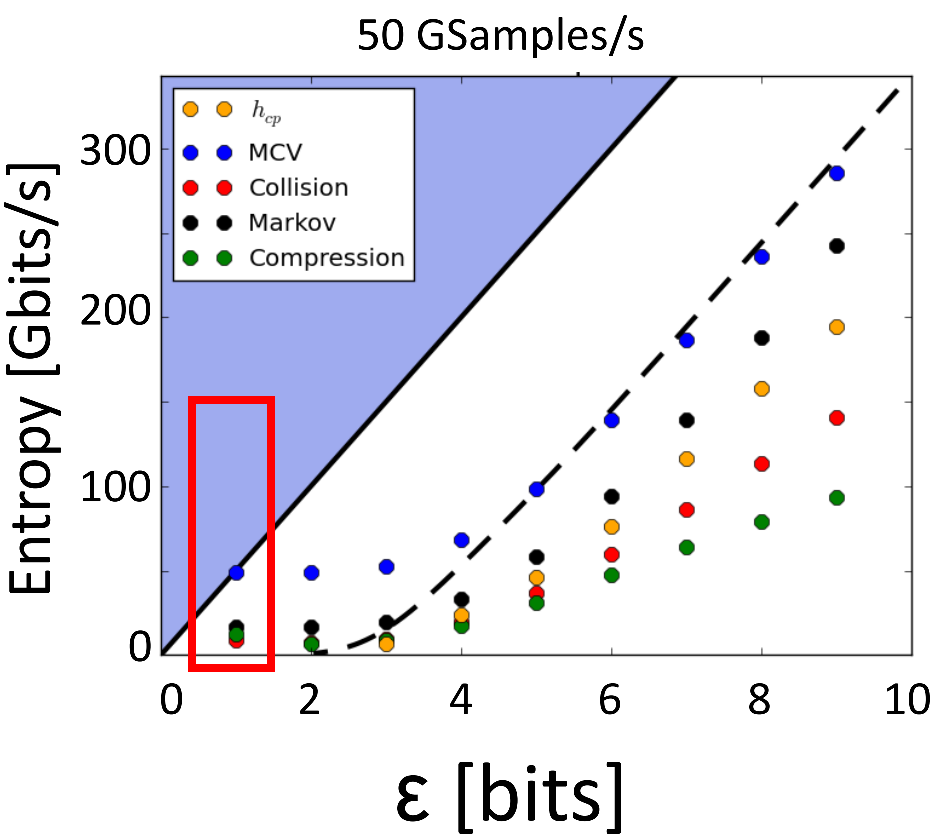
NIST SP 800-90B Entropy Estimates

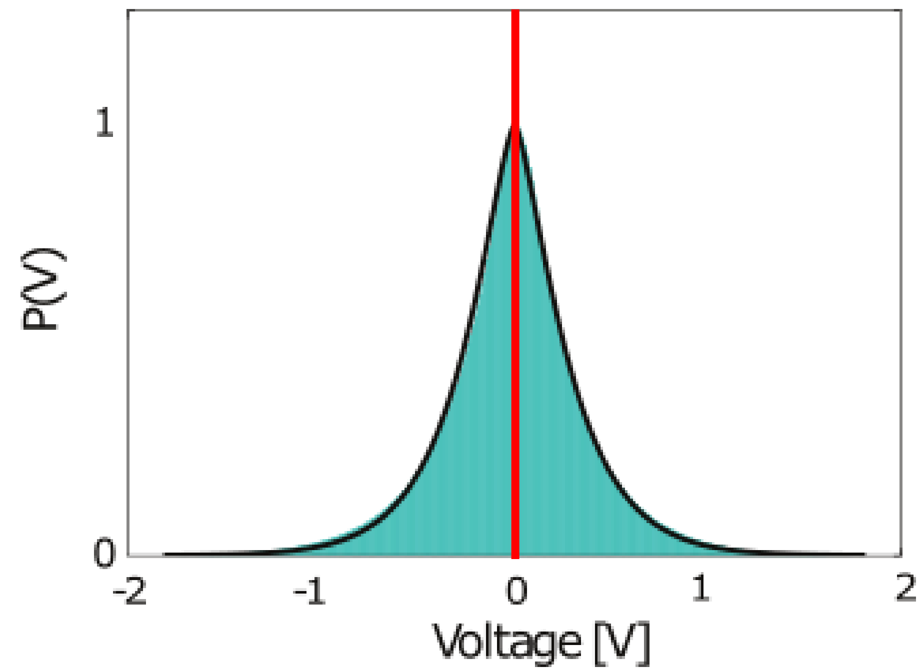
- Most Common Value Estimate
- Collision Estimate—based on mean time until first repeated value
- Markov Estimate—measures dependencies between consecutive values
- Compression Estimate—estimates how much the dataset can be compressed
- Other more complicated tests…

Entropy rate as a function of measurement resolution (ε)

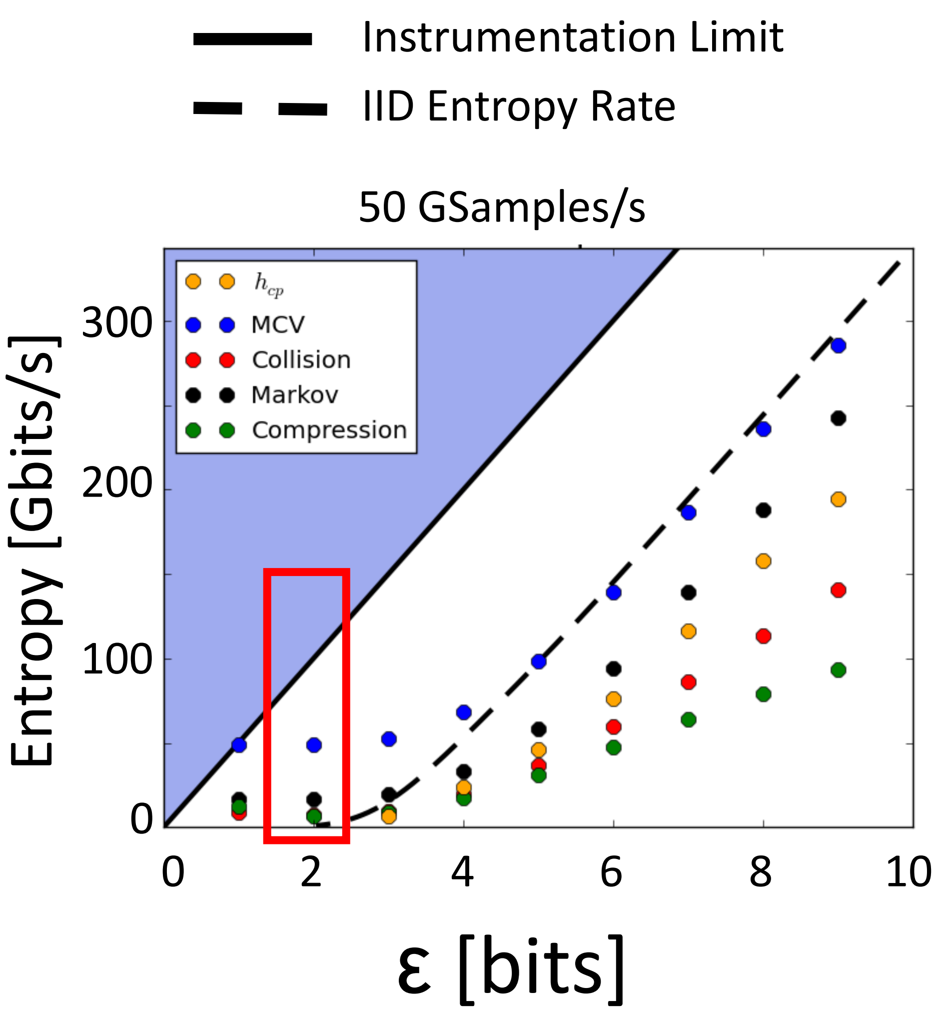
Instrumentation Limit

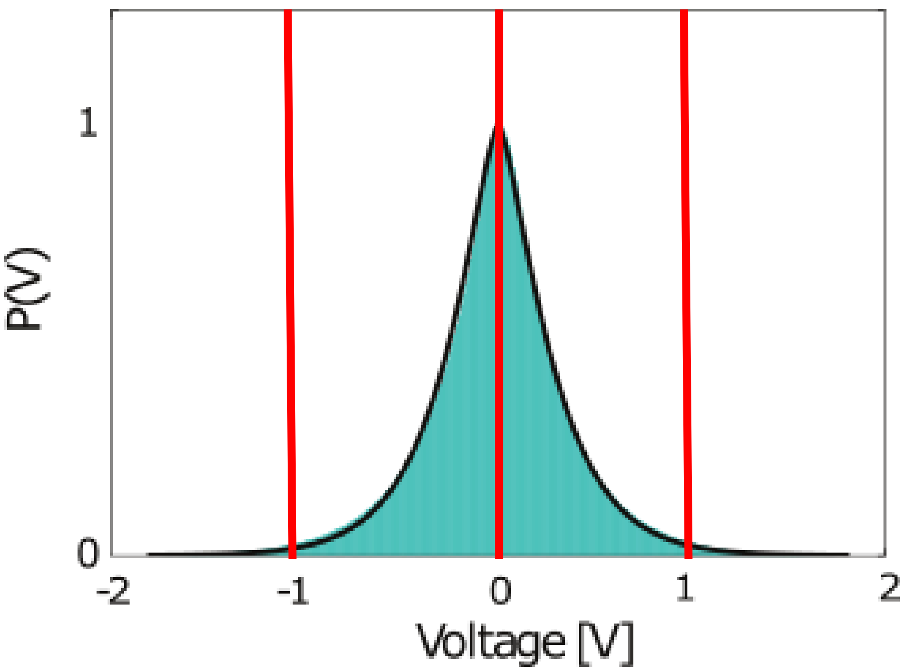
IID Entropy Rate



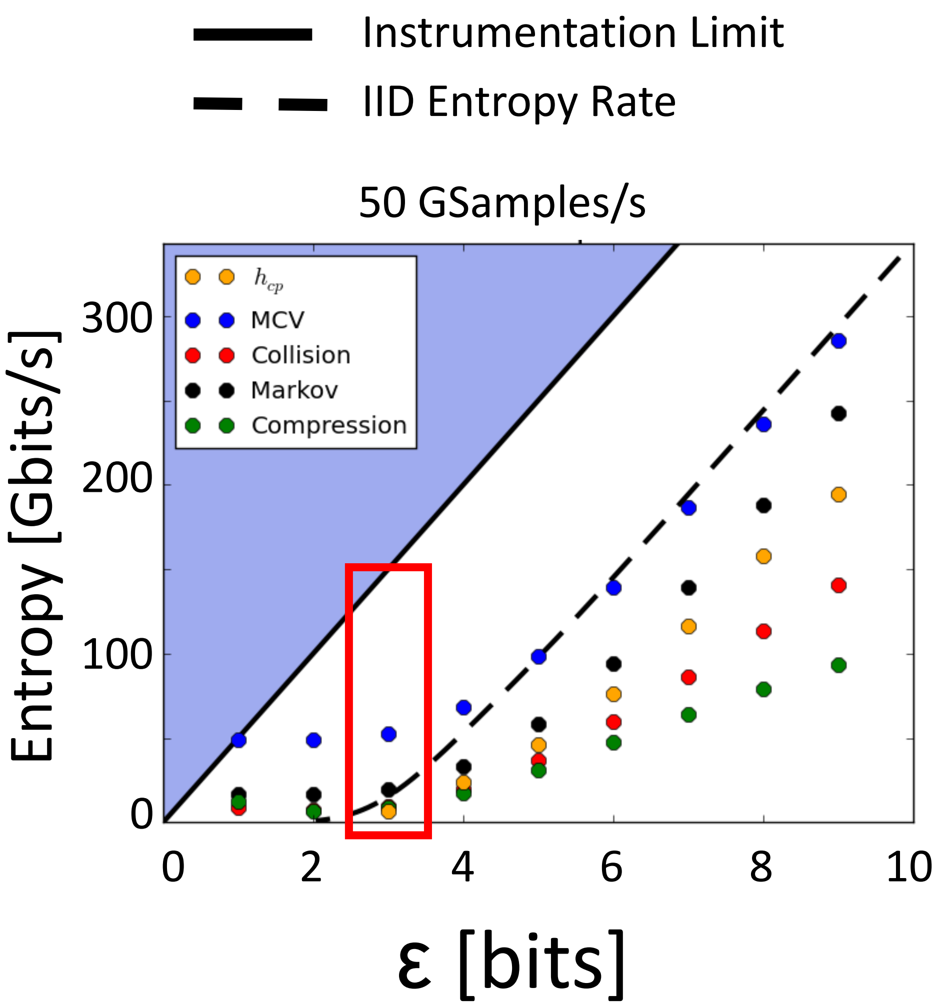


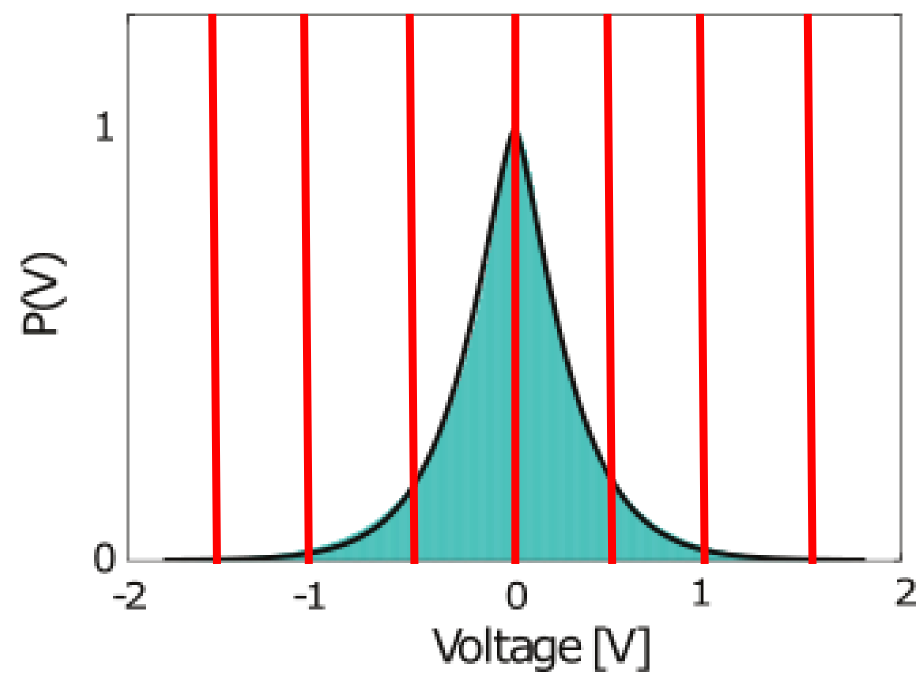
Entropy rate as a function of measurement resolution (ε)



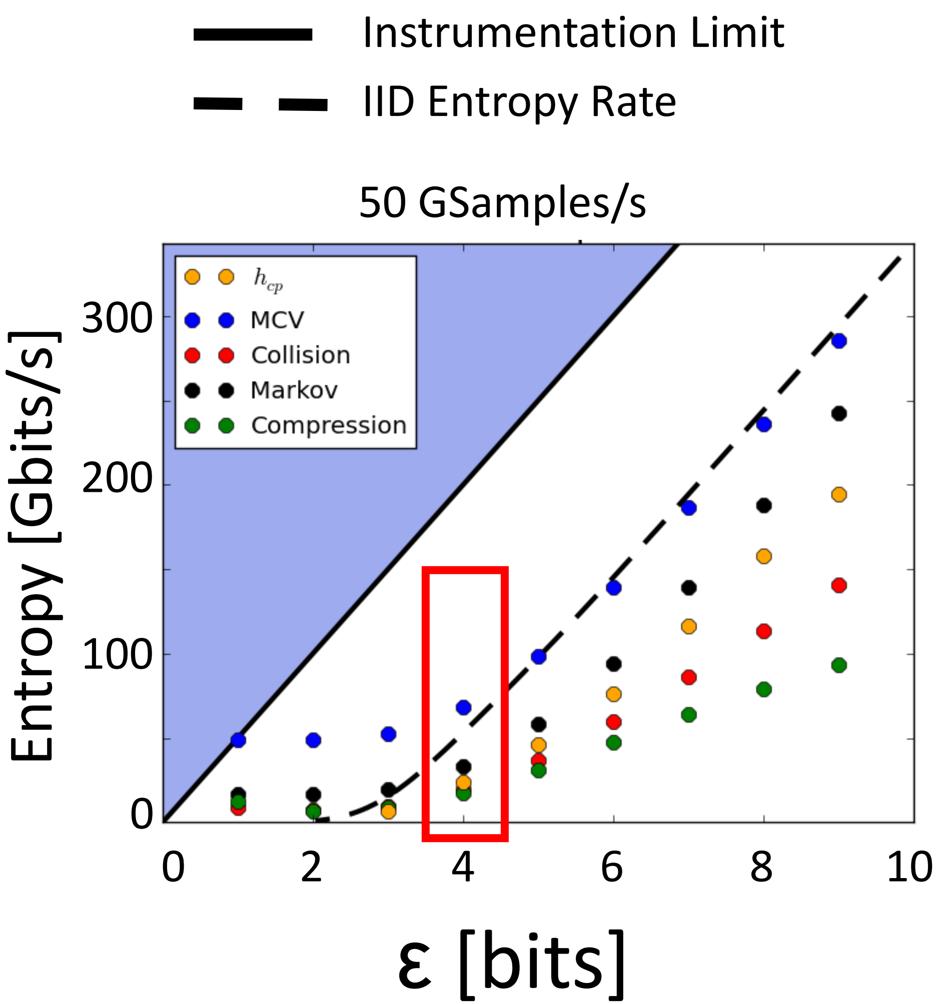


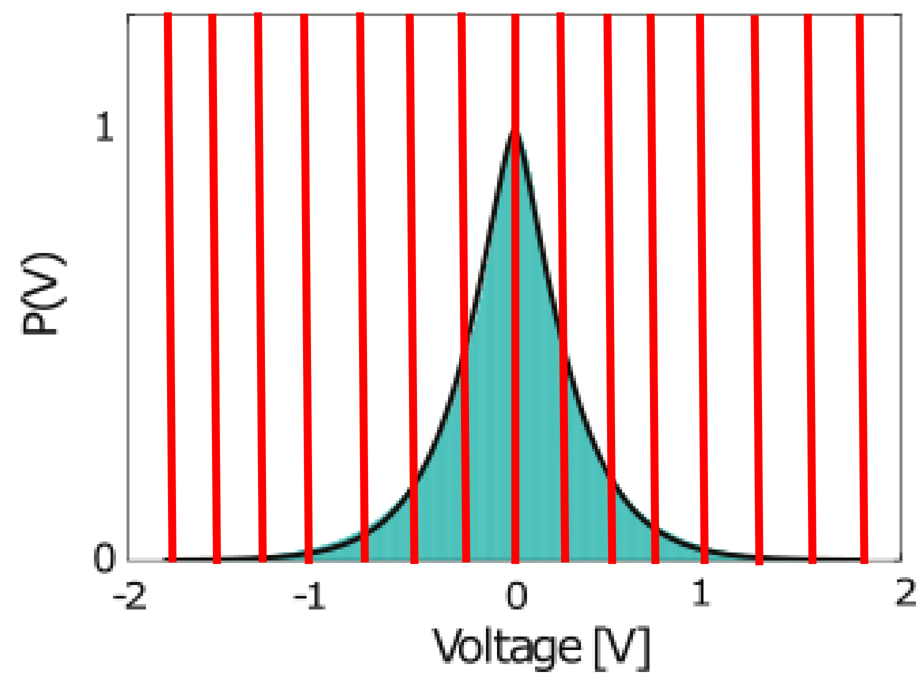
Entropy rate as a function of measurement resolution (ε)



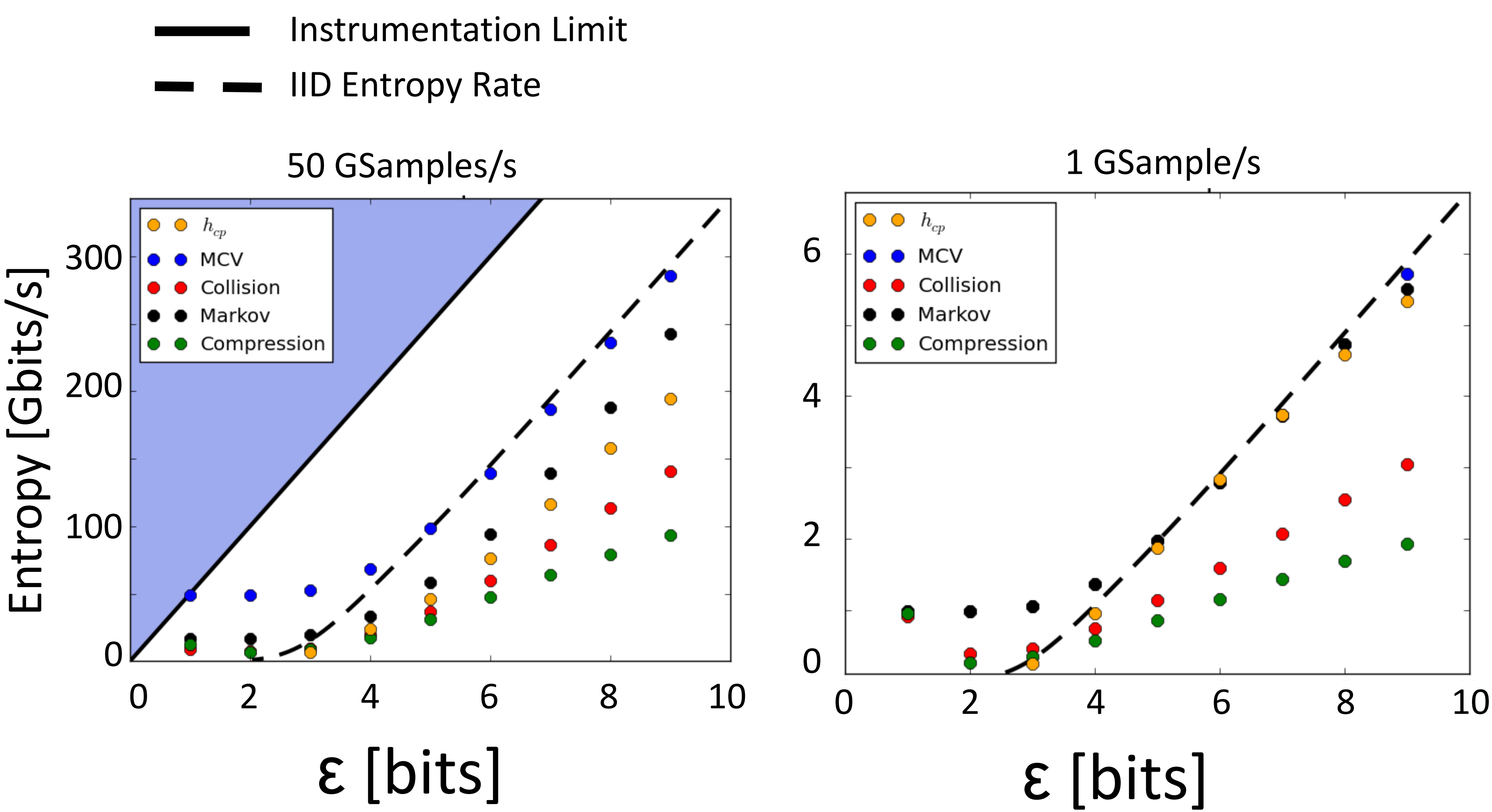


Entropy rate as a function of measurement resolution (ε)

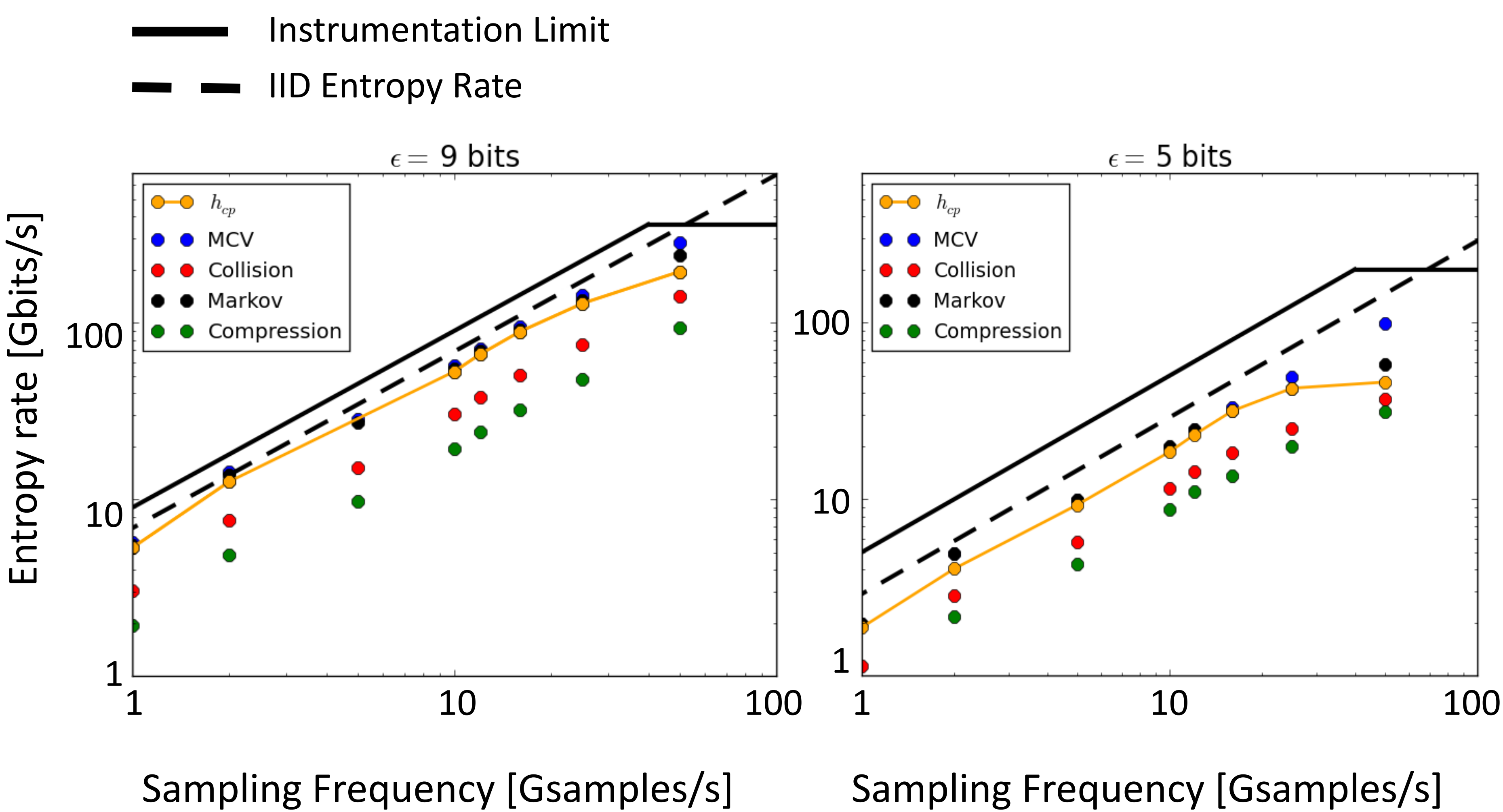




Entropy rate as a function of measurement resolution (ε)

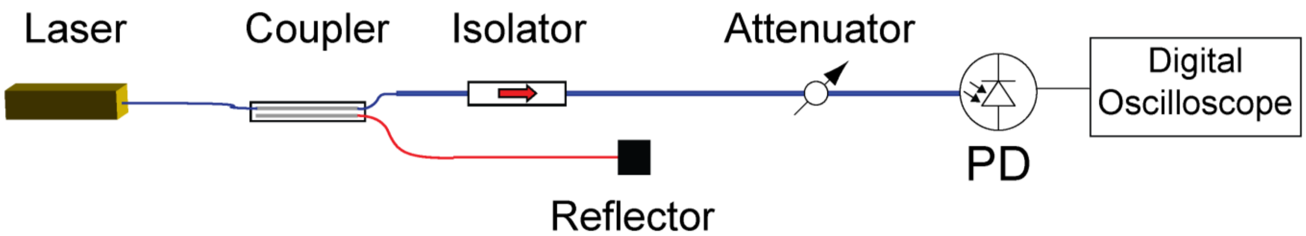


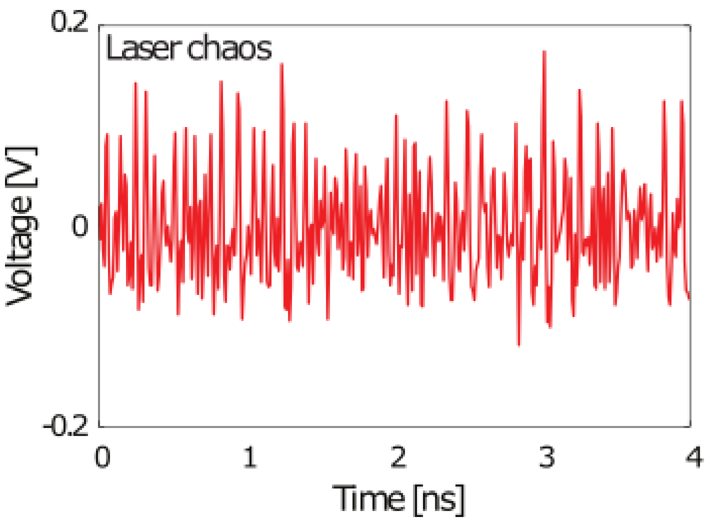
Capturing Temporal Correlations

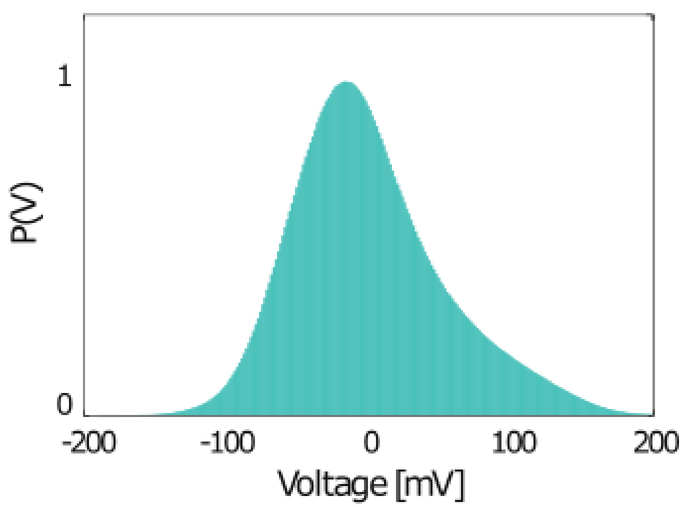


Chaotic Laser

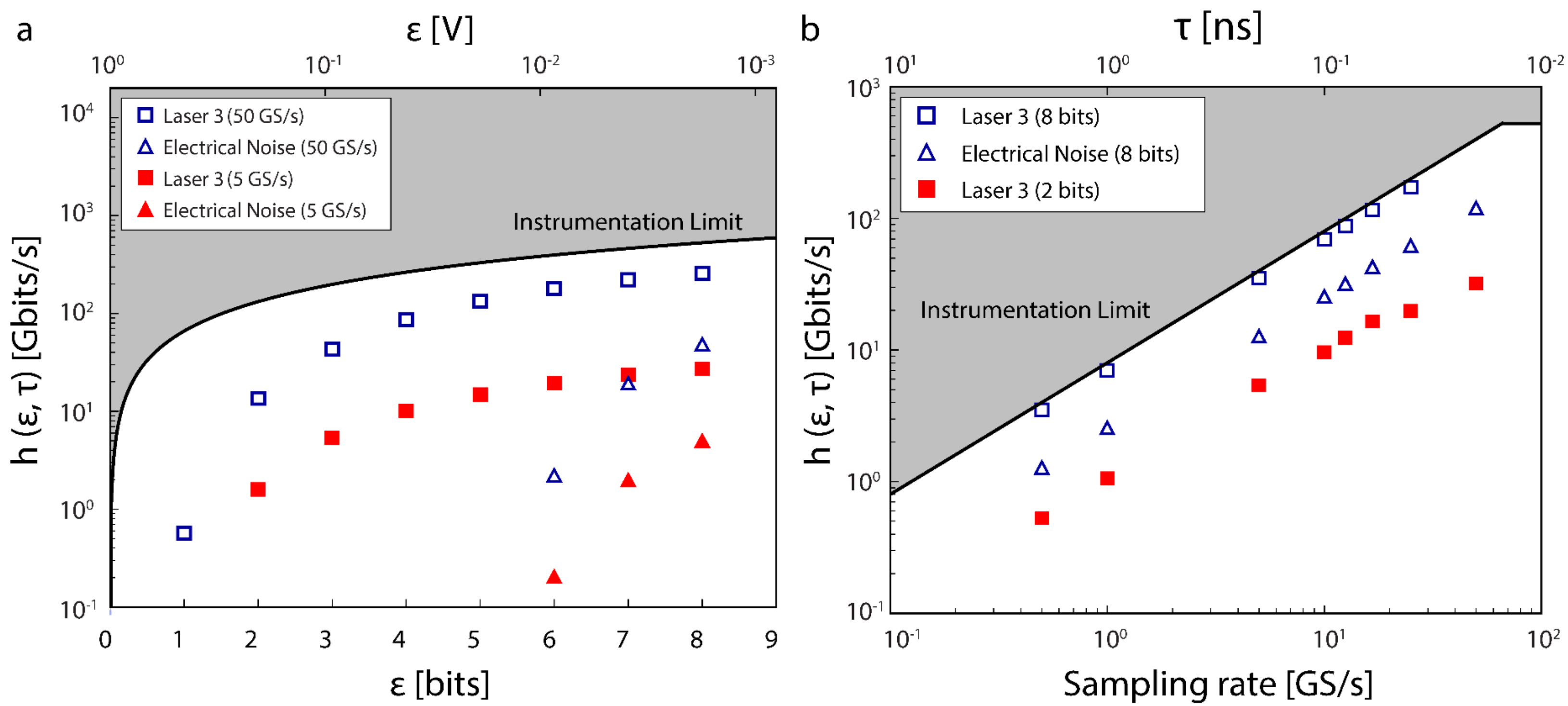
- Fluctuations are fast and chaotic (sensitive dependence on initial conditions)







Entropy rate—laser chaos



- Significant portion of entropy comes from background noise (especially at high resolution)

Conclusions:

- Important to look at entropy as a function of measurement resolution and sampling frequency
- Different physical processes can generate entropy, *even within the same experiment*
- Measurement determines which physical entropy generation processes you observe
- Entropy estimates should consider analog data, not post-processed bit stream

To learn more about:

Entropy generation in noisy chaotic systems:

Aaron M. Hagerstrom, Thomas E. Murphy, and Rajarshi Roy. "Harvesting entropy and quantifying the transition from noise to chaos in a photon-counting feedback loop." *Proceedings of the National Academy of Sciences* 112.30 (2015): 9258-9263.

Amplified spontaneous emission:

Williams, Caitlin RS, et al. "Fast physical random number generator using amplified spontaneous emission." *Optics express* 18.23 (2010): 23584-23597.

Li, Xiaowen, et al. "Scalable parallel physical random number generator based on a superluminescent LED." *Optics letters* 36.6 (2011): 1020-1022.