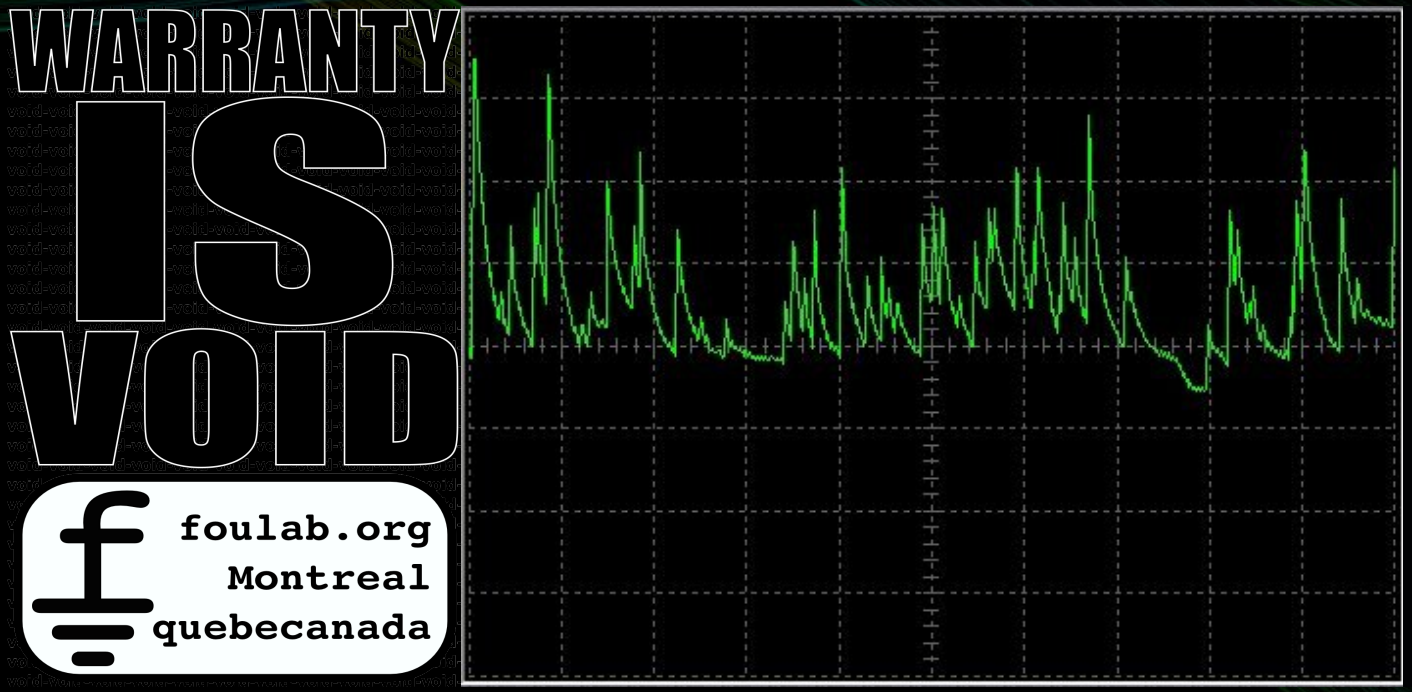
Design and Implementation of a Quantum True Random Number Generator



What is True Randomness?

- Must be unpredictable.
  - For a given set of binary data 'i', the $i+1^{th}$ bit can only be predicted with 50% accuracy.
- Must be unbiased and non-algorithmic. Computers can't do this (and neither can you!).
- Useful for cryptography, science, and games (gambling and drinking).

Types of Random Number Generators

- Pseudorandom (PRNG): Uses an algorithm and a 'secret' initial sequence. This is what your computer does.

- True Random (TRNG): Samples a physical system of high entropy.

- Both are easy to design wrong and they fail silently!

Types of TRNG

- Non Quantum: Samples a complex system of high entropy (lavalamps, time between keypresses).
- Higher bandwidth, easier to construct, numbers are not produced by any obvious algorithm.
- Is complexity as good as randomness?



Types of TRNG

- Quantum TRNG (QTRNG): Samples a simple system of high entropy (behavior of single photons or particles).
- Low bandwidth, difficult to sample quantum level phenomenae.
- However, the output 'should' be truly random!

Mistakes to Avoid

- Do not use more than one entropy source or detector.

- The author of this paper[1] suggests a good method too.

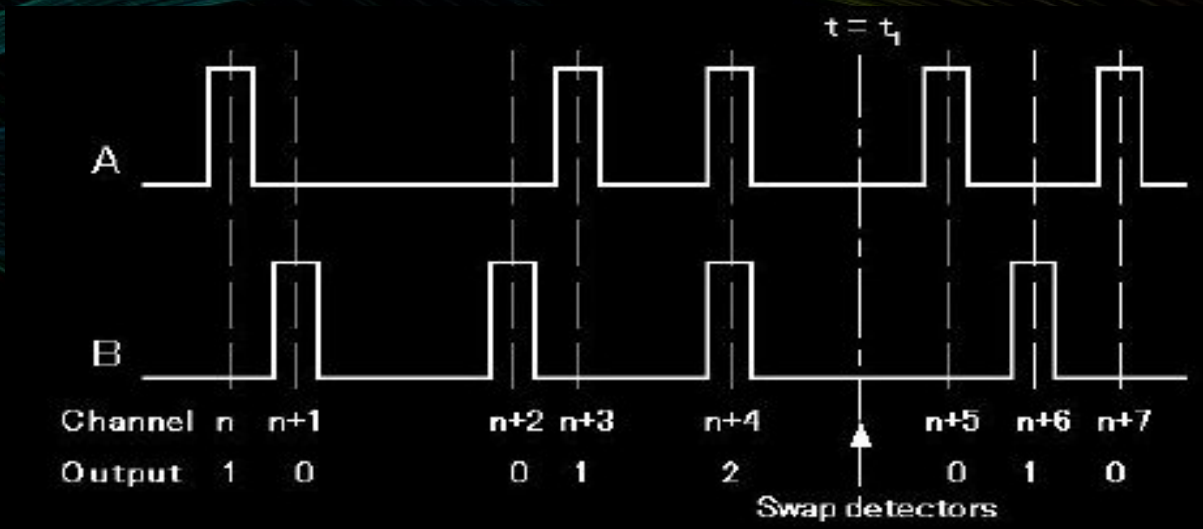


Fig. 2. Pulses recorded in 4096 channel scaler.

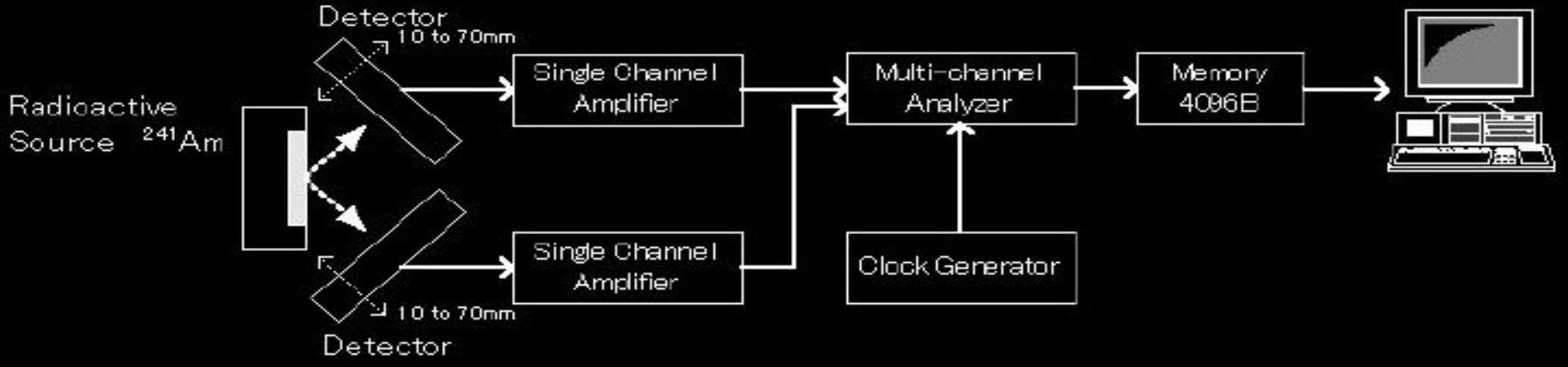
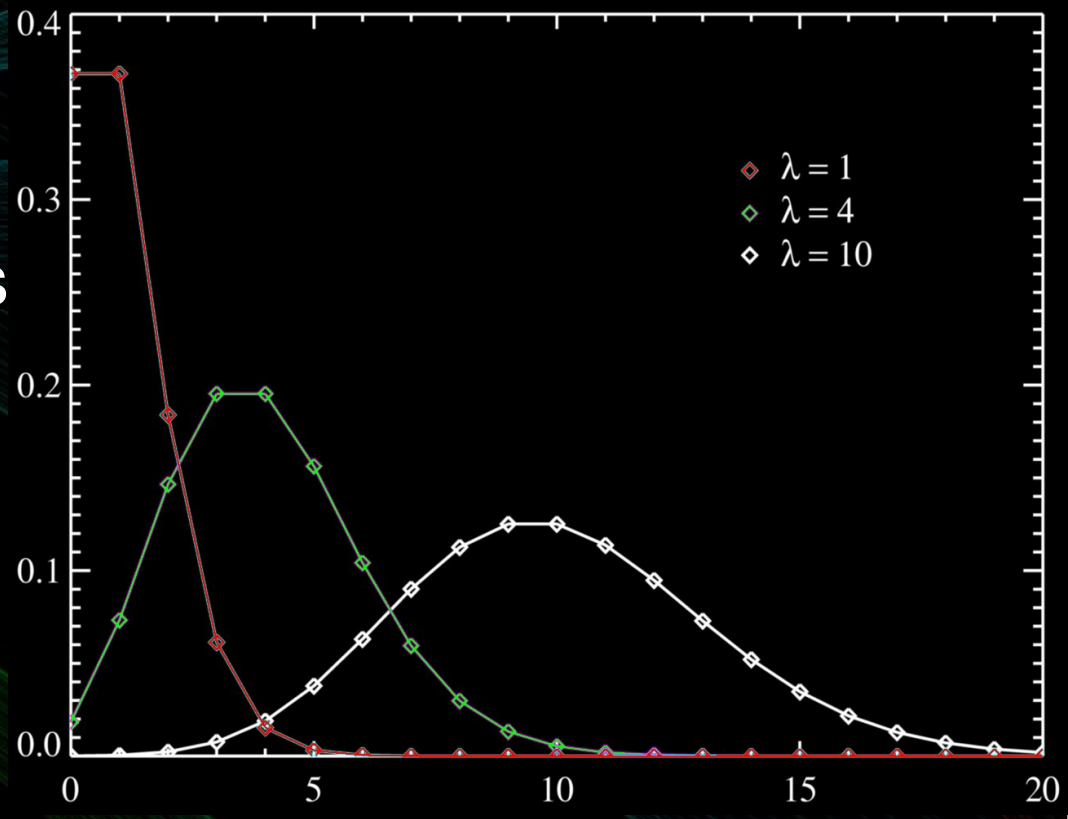


Fig. 1. Schematic diagram of random number generator.

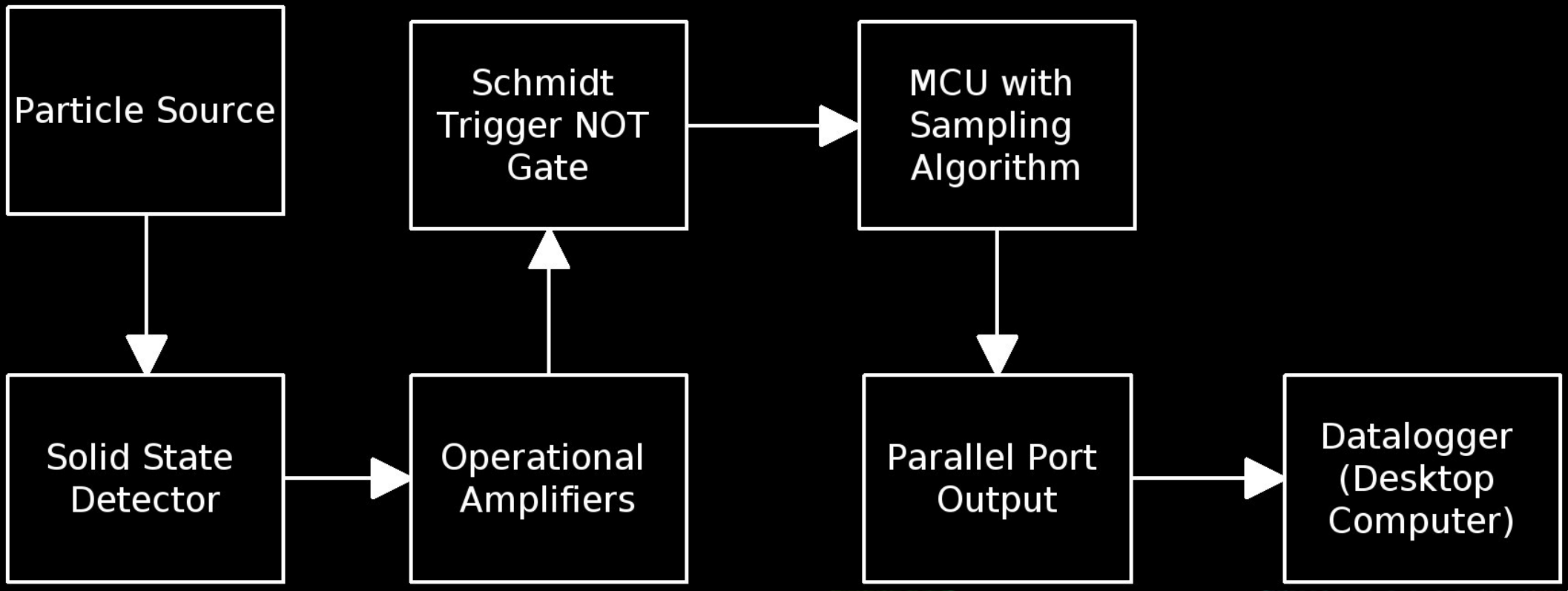
Mistakes to Avoid

- Do not use a counter + CPU interrupts. The number of events within a given time is not a random distribution, it is a Poisson distribution[2].

- Do not try to calculate 'expected' time between events, either.

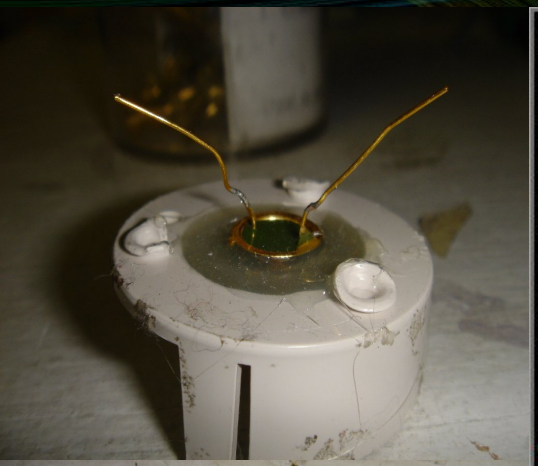


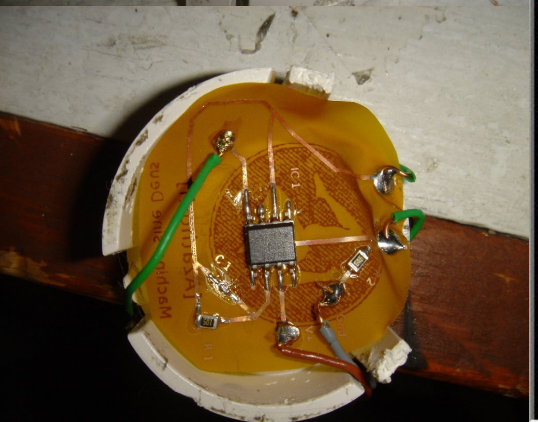
Our Design

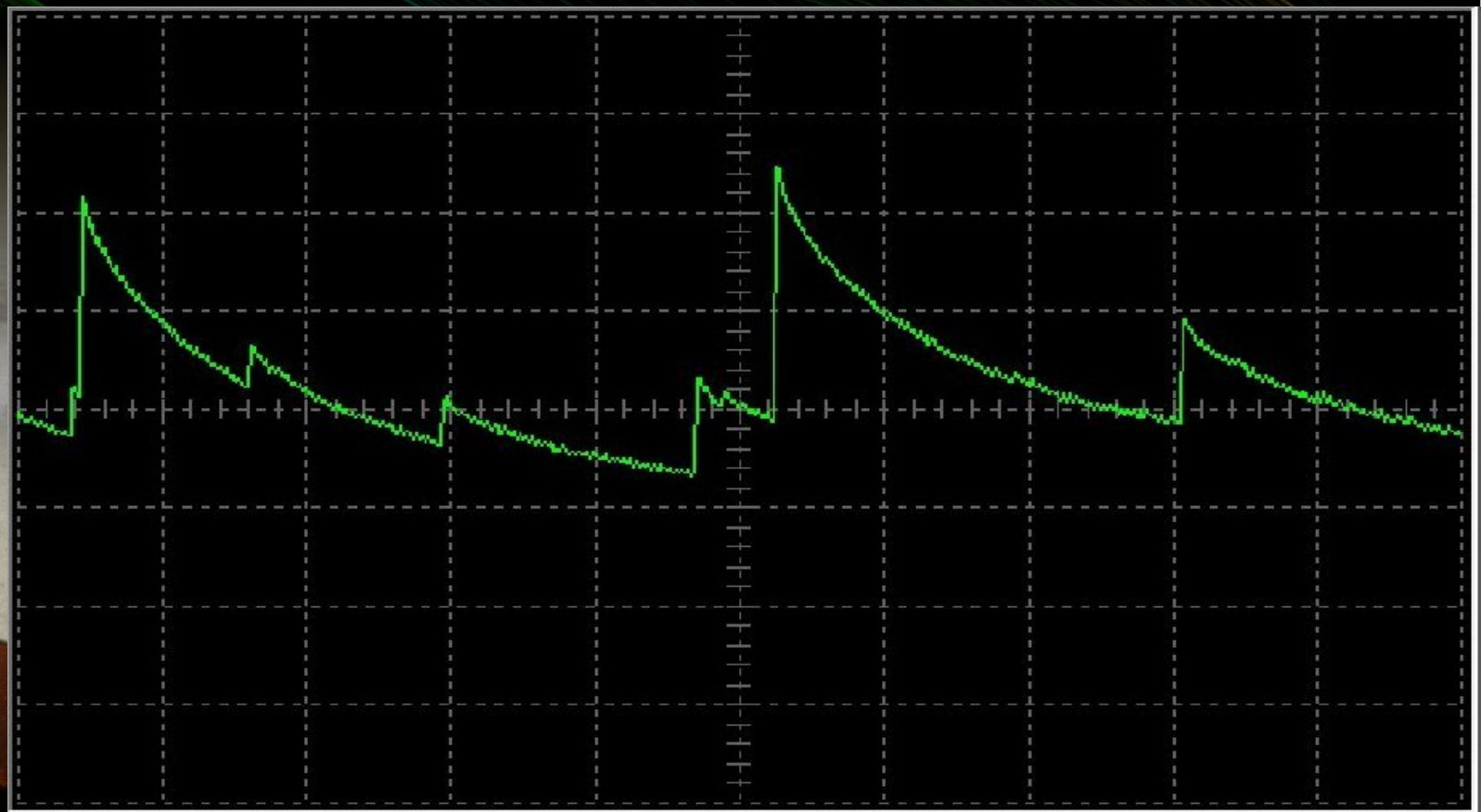

Particle Source
Schmidt Trigger NOT Gate
MCU with Sampling Algorithm
Solid State Detector
Operational Amplifiers
Parallel Port Output
Datalogger (Desktop Computer)

Our Design

- A PIN photodiode and opamps are used as a solid-state particle detector that operates at low voltages. It was enclosed in a Faraday cage.



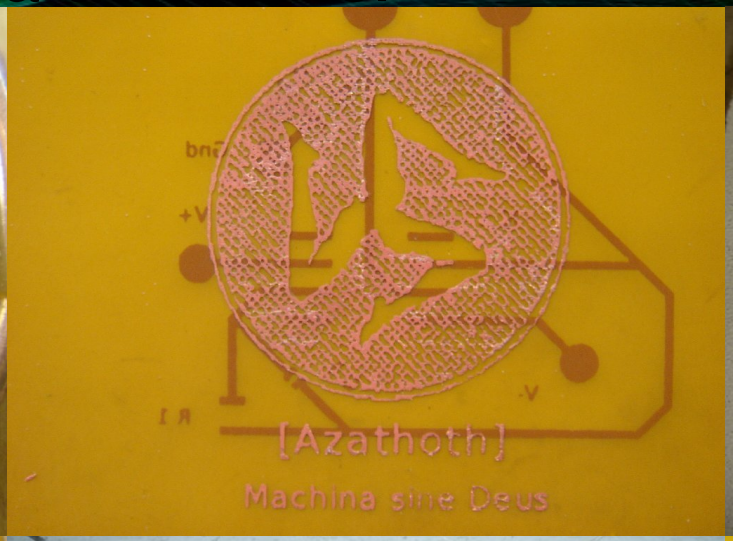


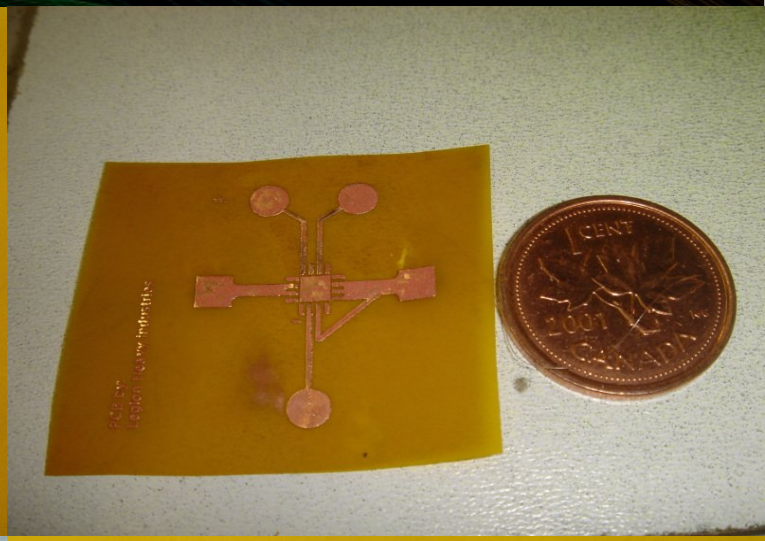


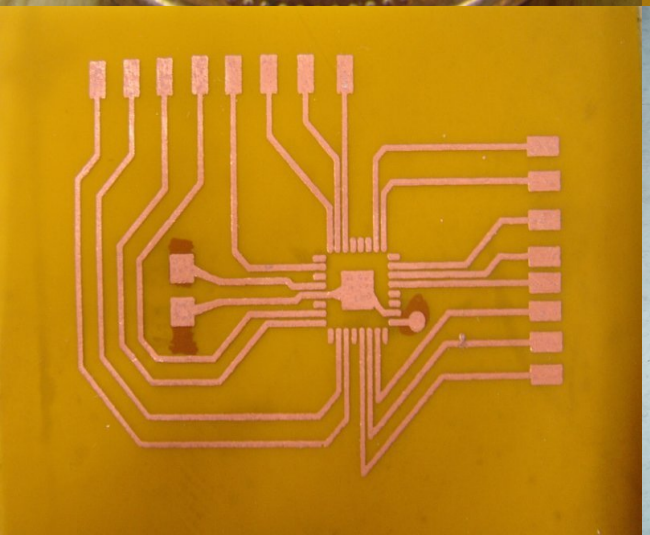
Flex PCB

- Boards were printed on flex PCB for its good rapid prototyping characteristics.

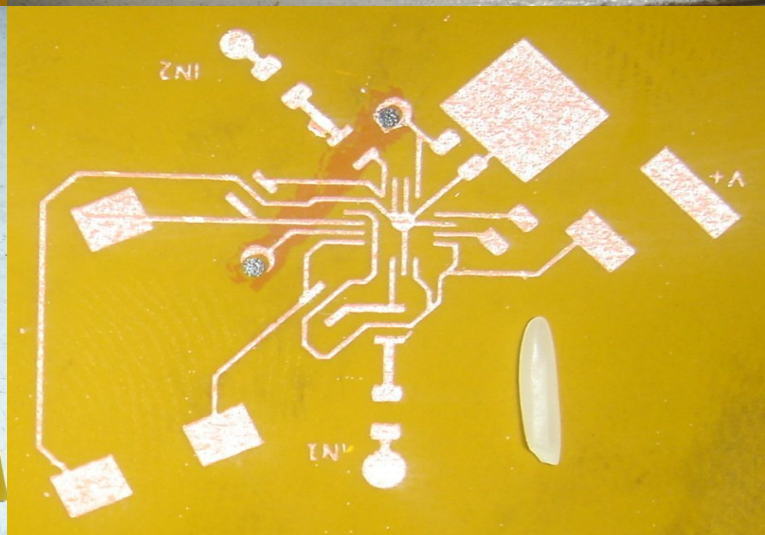






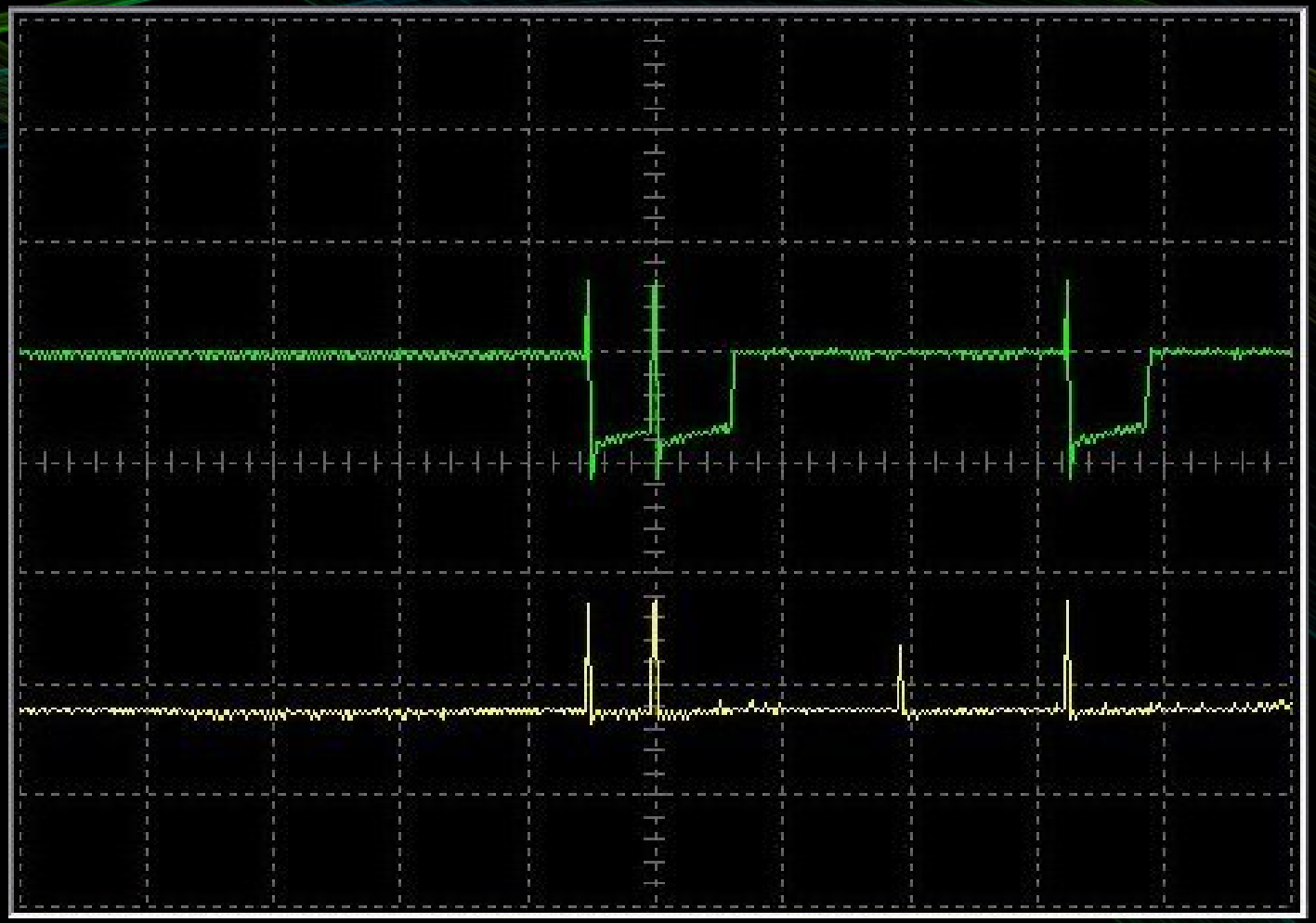


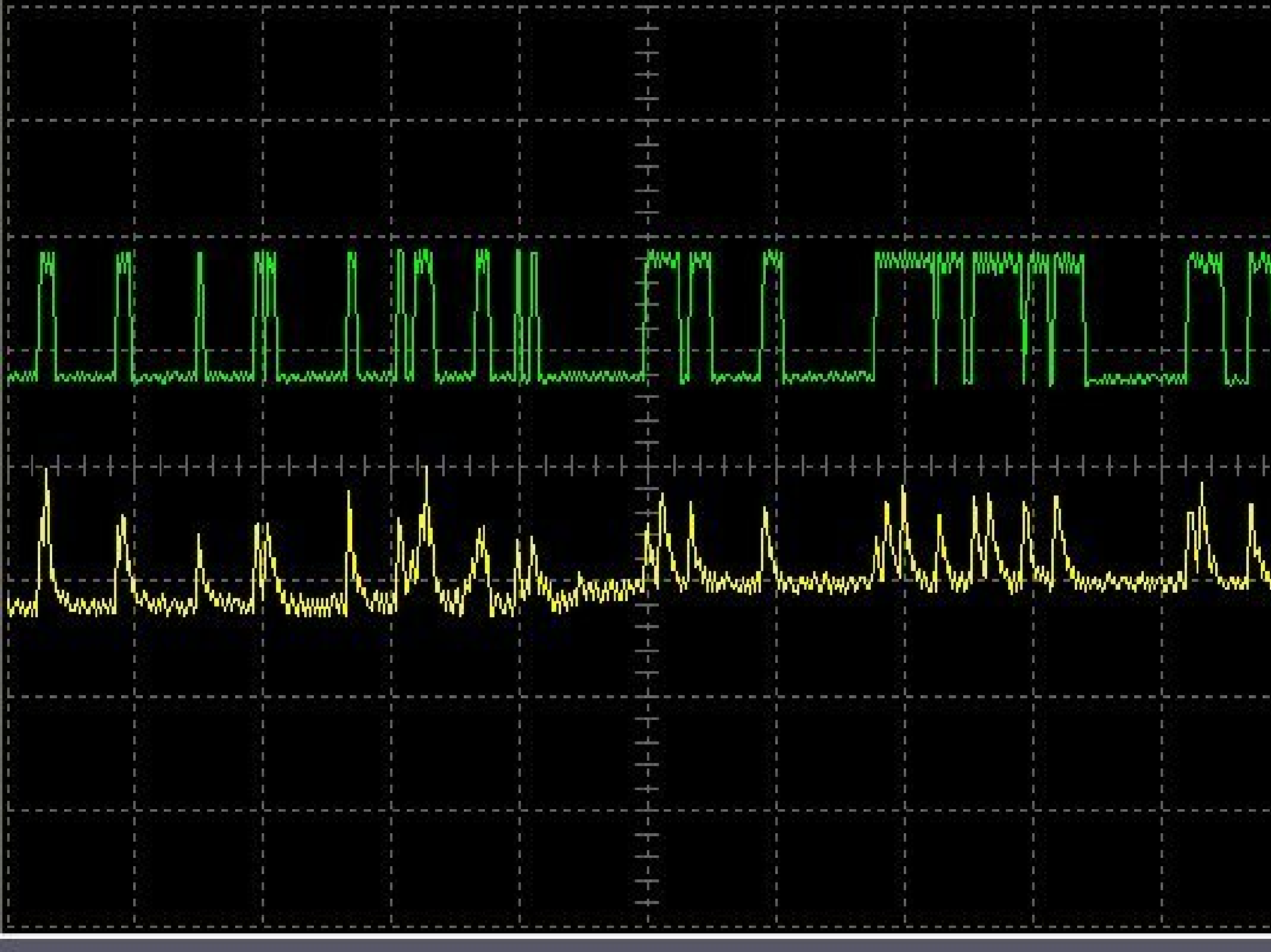




Our Design

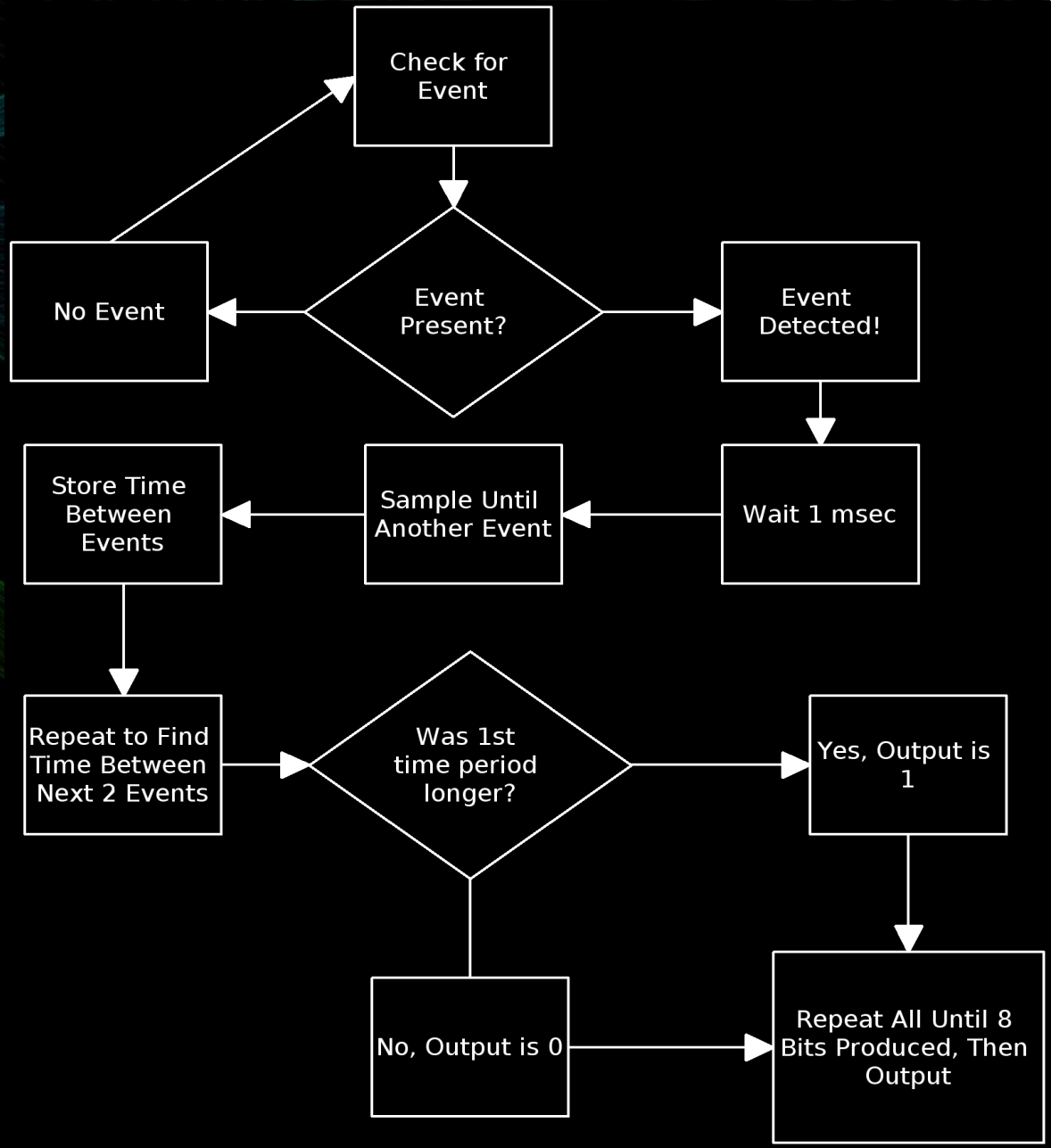
- Pulse shaping is done by a Schmitt-trigger hex inverter.



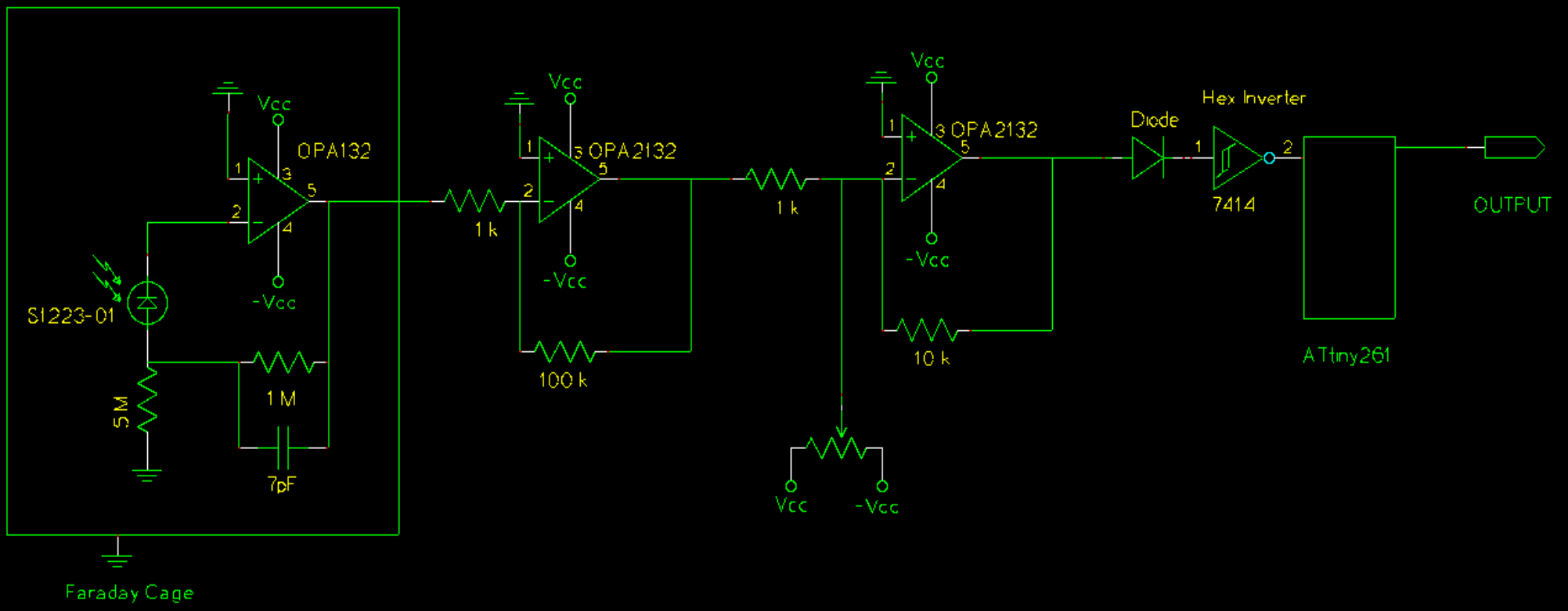


Our Design

- Sampling and parallel output are done by an ATtiny261 MCU @ 8Mhz.



Our Design



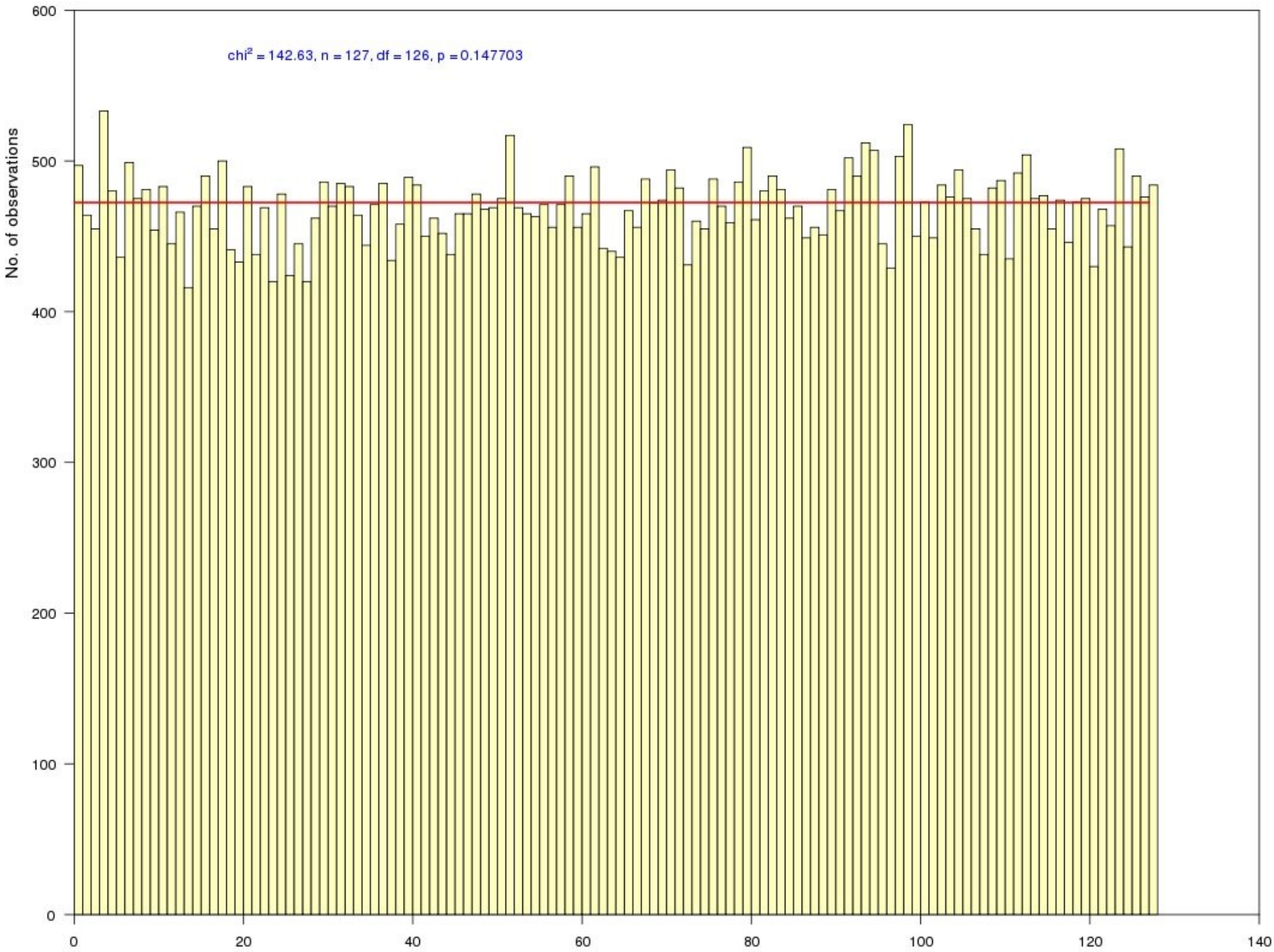
TITLE Quantum Entropy Accumulator	
FILE :	REVISION:
PAGE OF	DRAWN BY: Sean Boyce

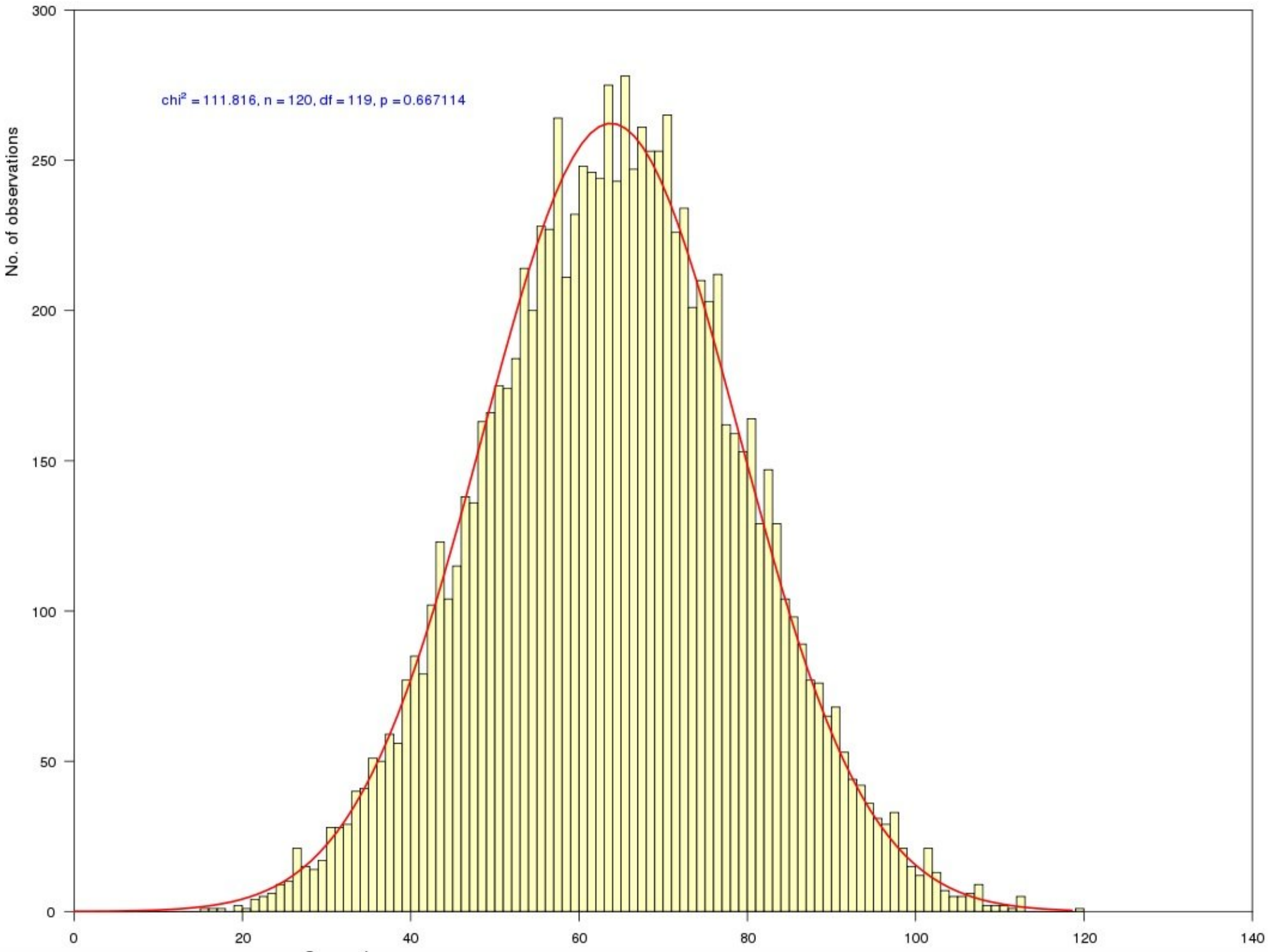
Demonstration

- Hopefully no magic blue smoke

Basic Analysis of Output

- Check for bias by creating simple frequency charts.
- X means of Y random values should approach the binomial distribution for large X and Y^3.
- Keep in mind that 'proving' randomness is impossible through hypothesis testing.


chi² = 142.63, n = 127, df = 126, p = 0.147703
No. of observations
600
500
400
300
200
100
0
0
20
40
60
80
100
120
140


chi² = 111.816, n = 120, df = 119, p = 0.667114
No. of observations
300
250
200
150
100
50
0
0
20
40
60
80
100
120
140

Advanced Analysis

- NIST Random Number Generation Technical Working Group Statistical Test Suite 2.0[4]

- 100 megabits of data were used for these tests, with default options and a=0.01

- The last of 188 tests (linear complexity) did not seem to run correctly.

Advanced Analysis

- Given a block of random data divided into X bitstreams and subjected to Y tests at some threshold alpha value for faliure Z, you expect true random data to fail X*Y*Z tests.
- Minimum 1/alpha bitstreams required (our alpha=0.01)
- We expect 187 faliures, we observe 205.
- Faliures do not cluster on any specific test.

Future Technology!

- Single photon QTRNGs using single-photon emitters and photomultiplier tubes (Ebay!)

- High bandwidth, zero bias! No isotopes! Requires high voltage and vacuum tubes (seriously).



Acknowledgements

- Foulab for a space to work, and friends to work with.
- TRNG driver and data management scripts written by fx

Want to make one yourself?

- If all goes well, boards will be available in one month at www.legionheavyindustries.com

References

1: http://isi.cbs.nl/iamamember/CD2/pdf/545.PDF

2: http://en.wikipedia.org/wiki/Poisson_process

3: http://en.wikipedia.org/wiki/Binomial_distribution

4: http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

For more information:

http://www.national.com/onlineseminar/2004/photodiode/PhotodiodeAmplifers.pdf

http://jp.hamamatsu.com/resources/products/ssd/pdf/s1223_series_kpin1050e01.pdf

http://www.fourmilab.ch/hotbits/how3.html