

Design and Implementation of a Quantum True Random Number Generator

**WARRANTY
IS
VOID**

f foulab.org
Montreal
quebecanada



What is True Randomness?

- For a given set of binary data 'i', the $i+1^{\text{th}}$ bit can only be predicted with 50% accuracy.
- Must be unbiased and non-algorithmic.
- Useful for cryptography, science, and games (gambling and drinking).

Types of Random Number Generators

- Pseudorandom (PRNG): Uses an algorithm and a 'secret' initial sequence.
- 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 an algorithm.
- Is complexity the same 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 phenomena.
- However, the output 'should' be truly random!

Mistakes to Avoid

- Do not use more than one entropy source or detector.
- The author of this paper¹ described a good method too.

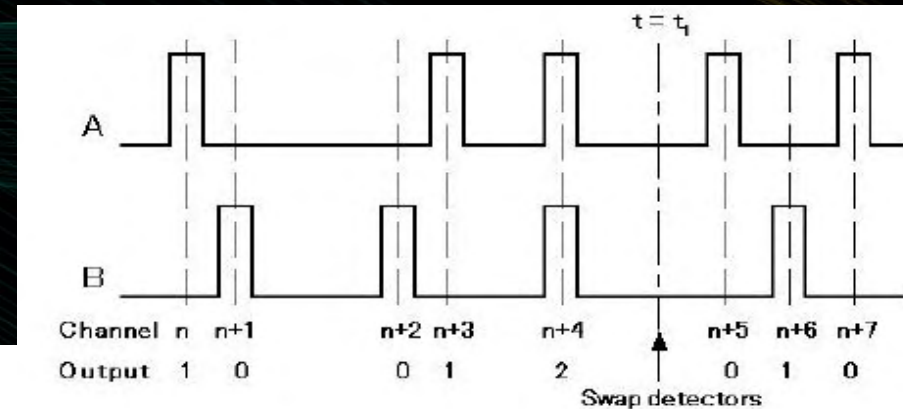


Fig. 2. Pulses recorded in 4096 channel scaler.

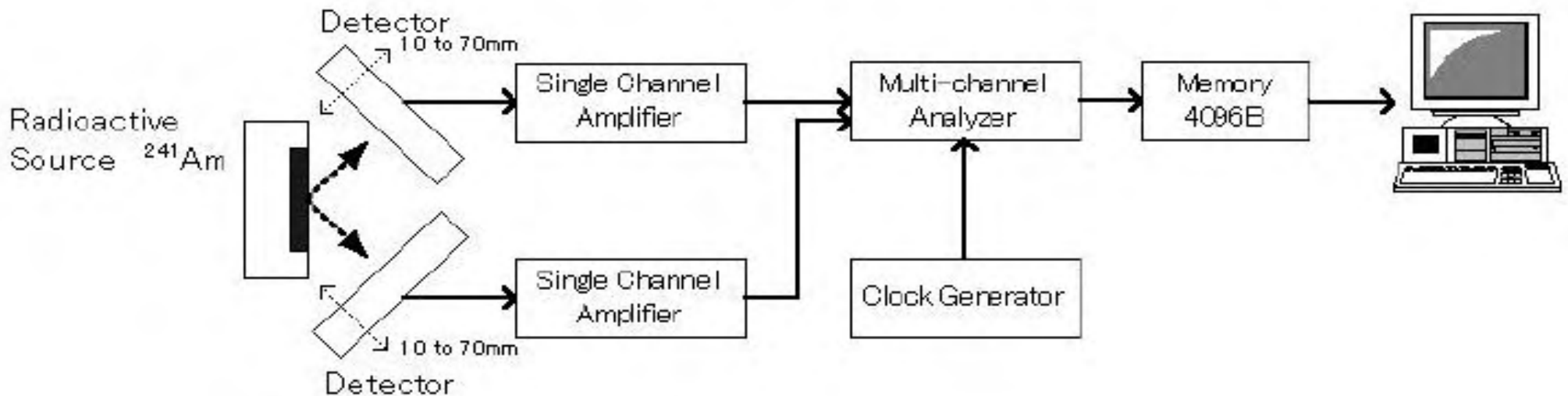
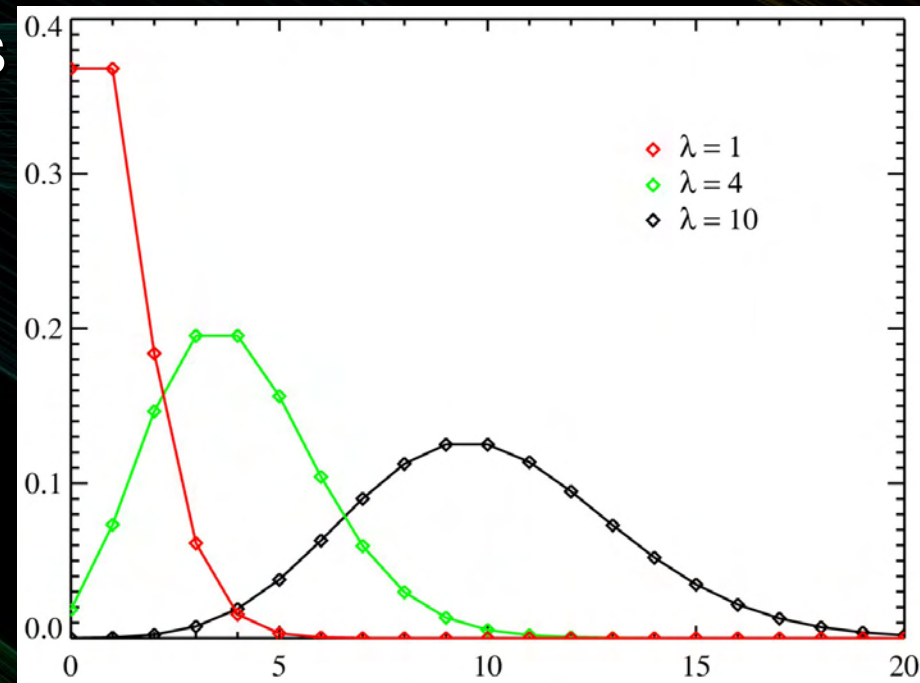


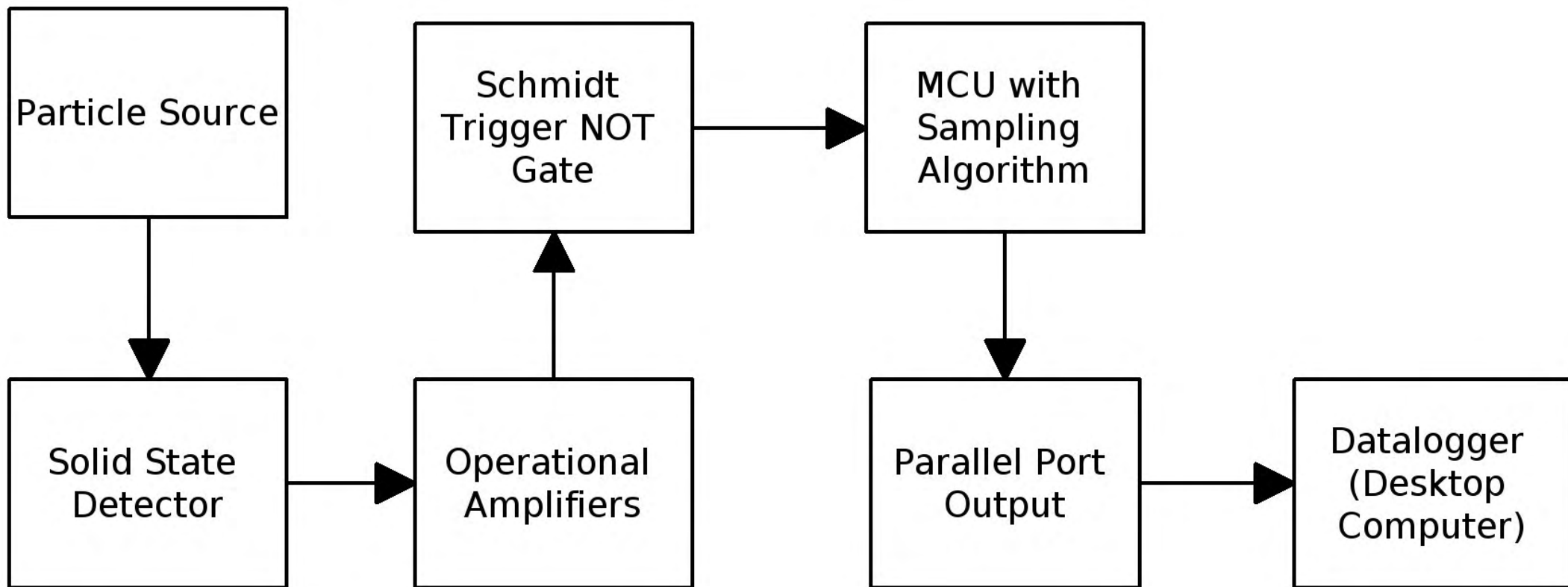
Fig. 1. Schematic diagram of random number generator.

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 distribution².
- Do not try to calculate 'expected' time between events, either.

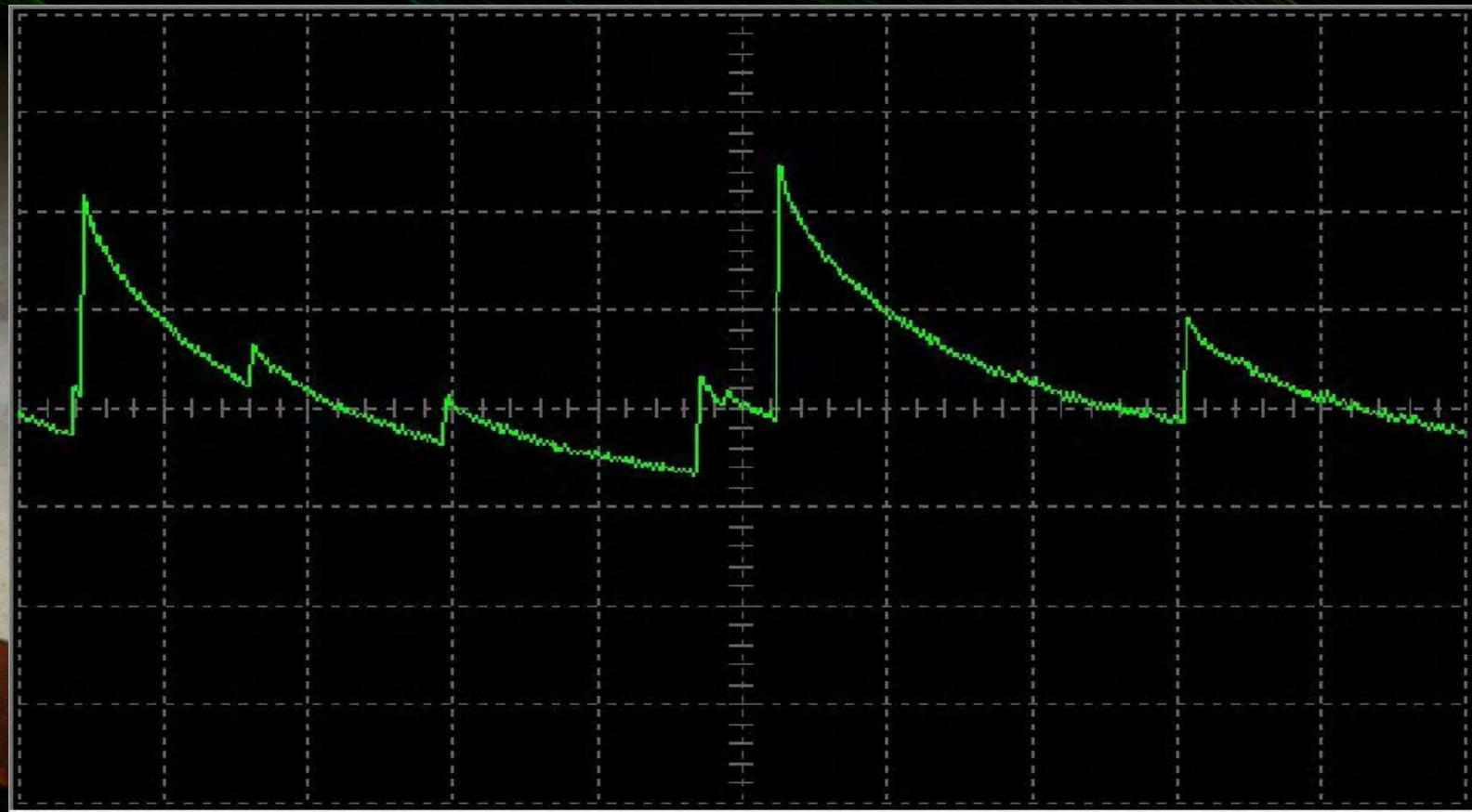
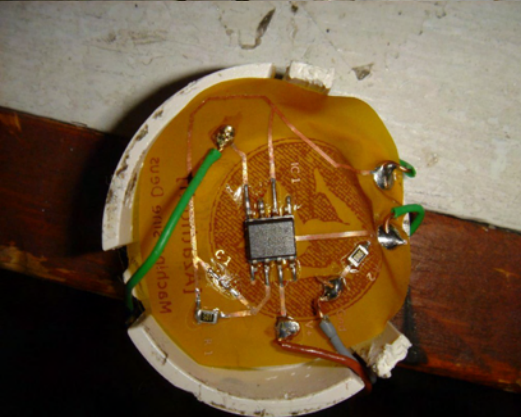
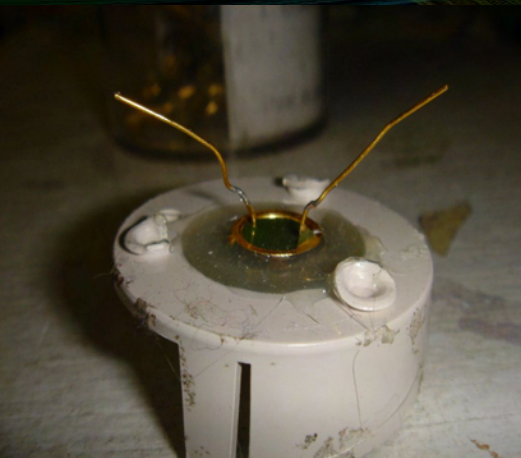


Our Design



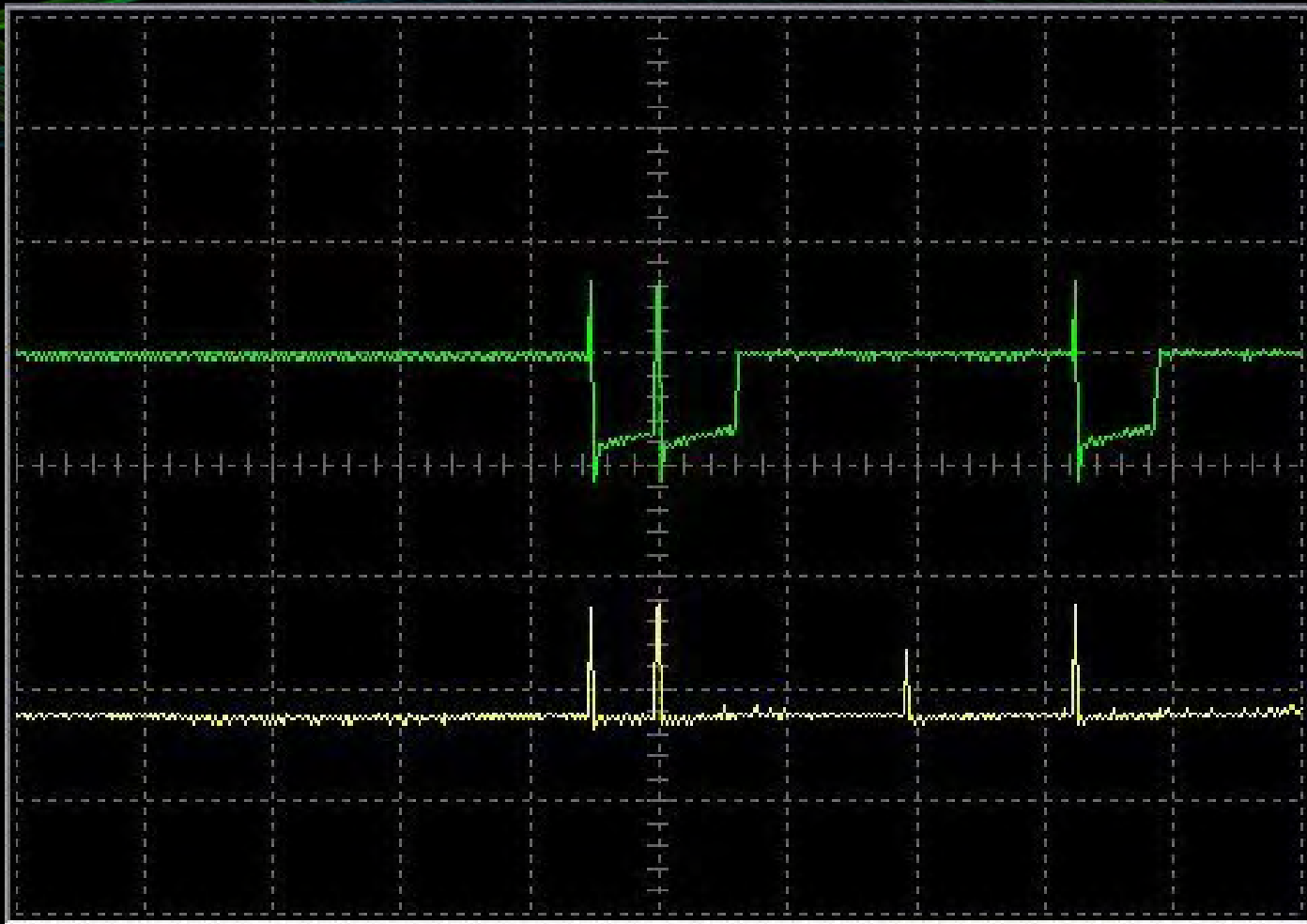
Our Design

- 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.



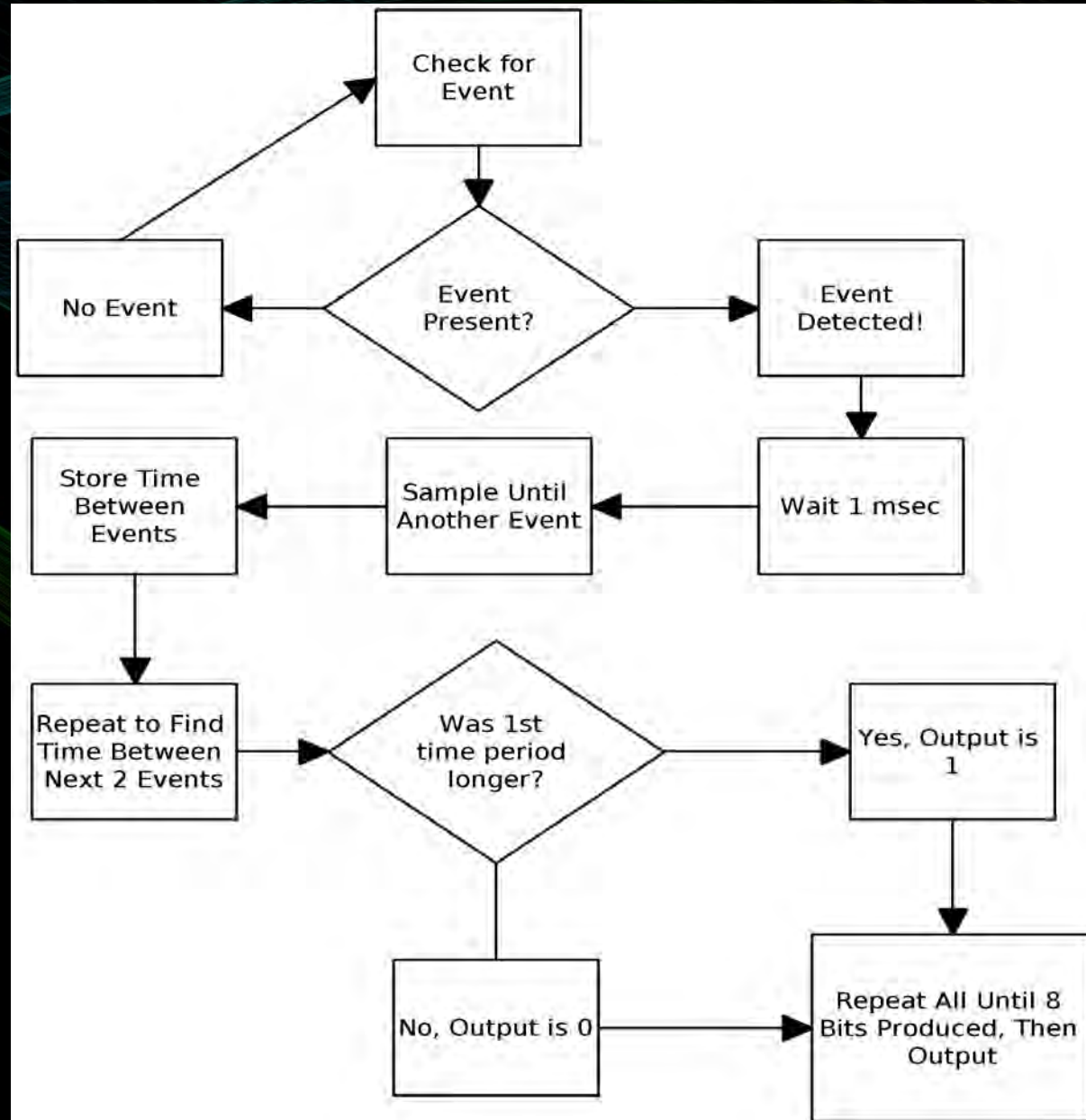
Our Design

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

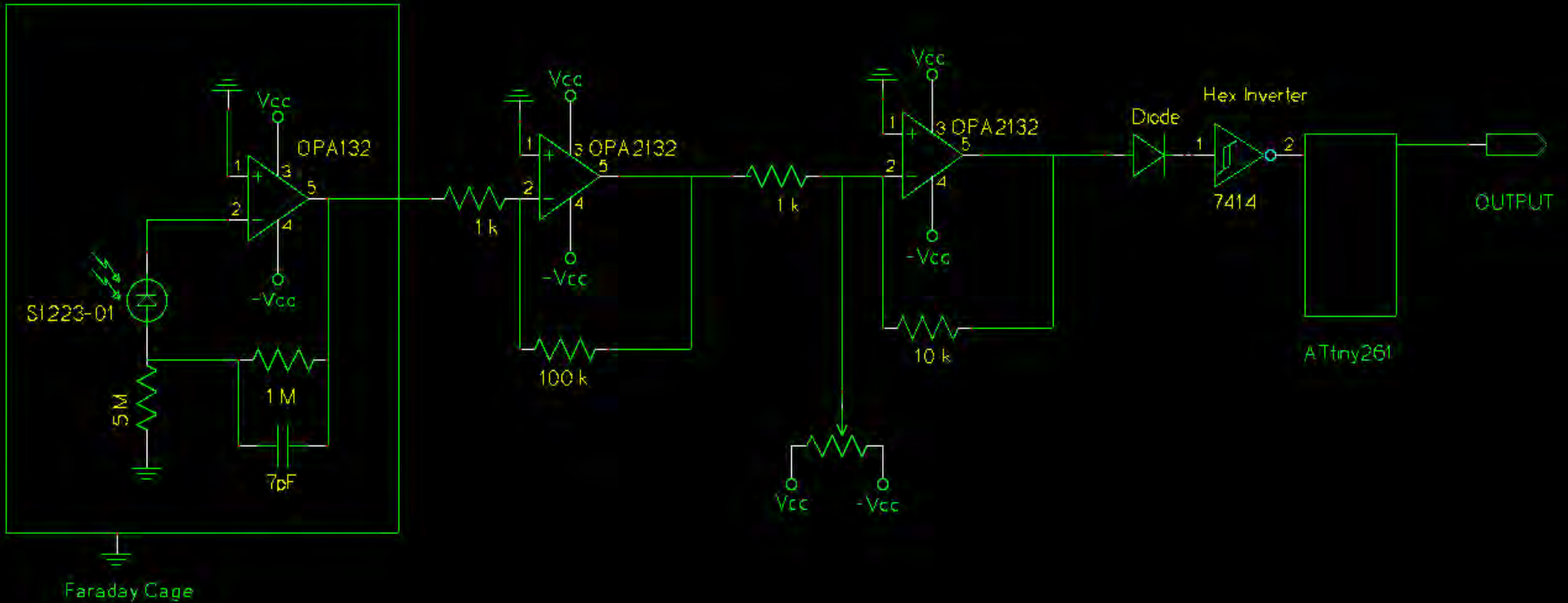


Our Design

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



Our Design



TITLE Quantum Entropy Accumulator

FILE :

REVISION:

PAGE

OF

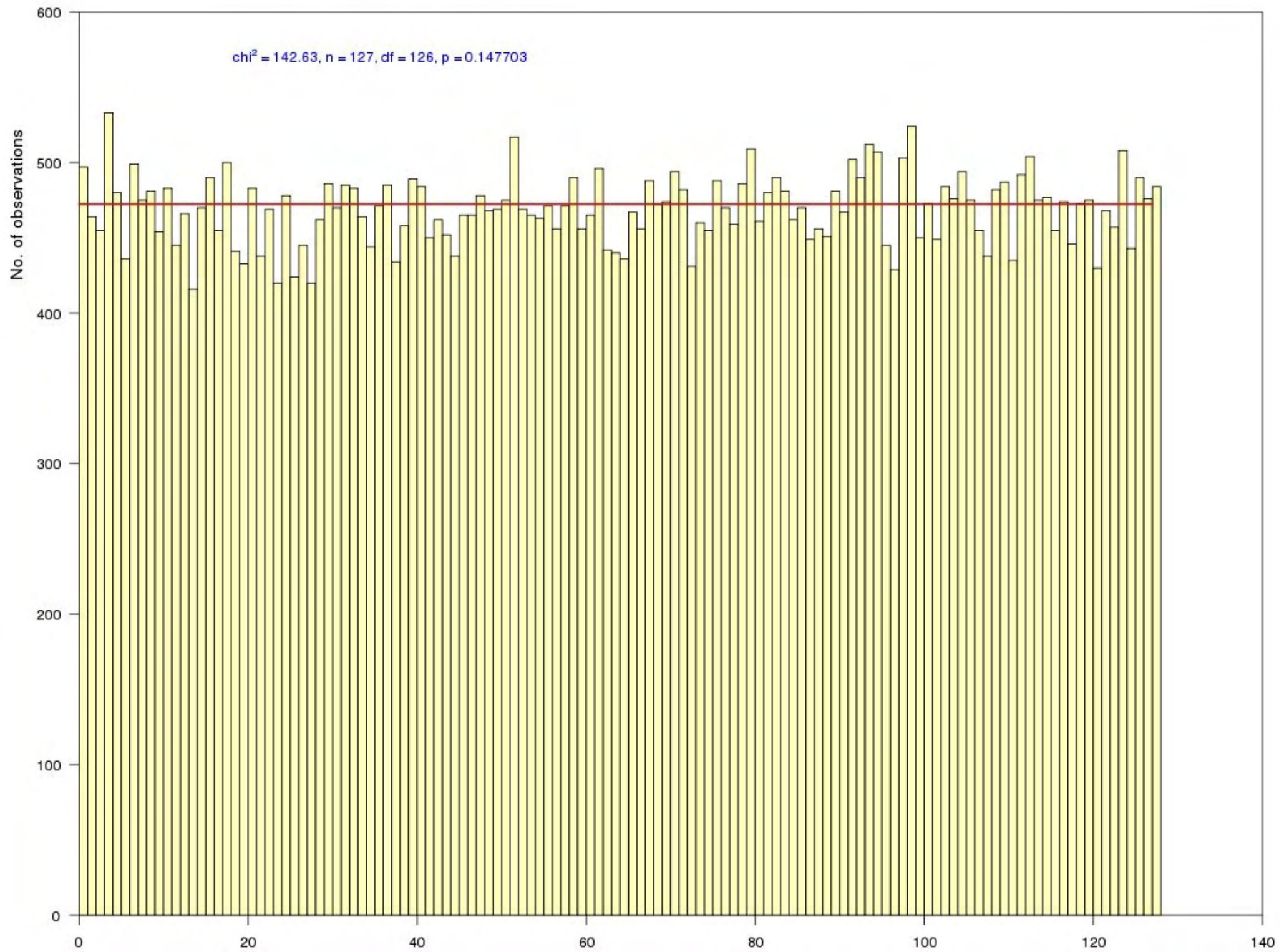
DRAWN BY: Sean Boyce

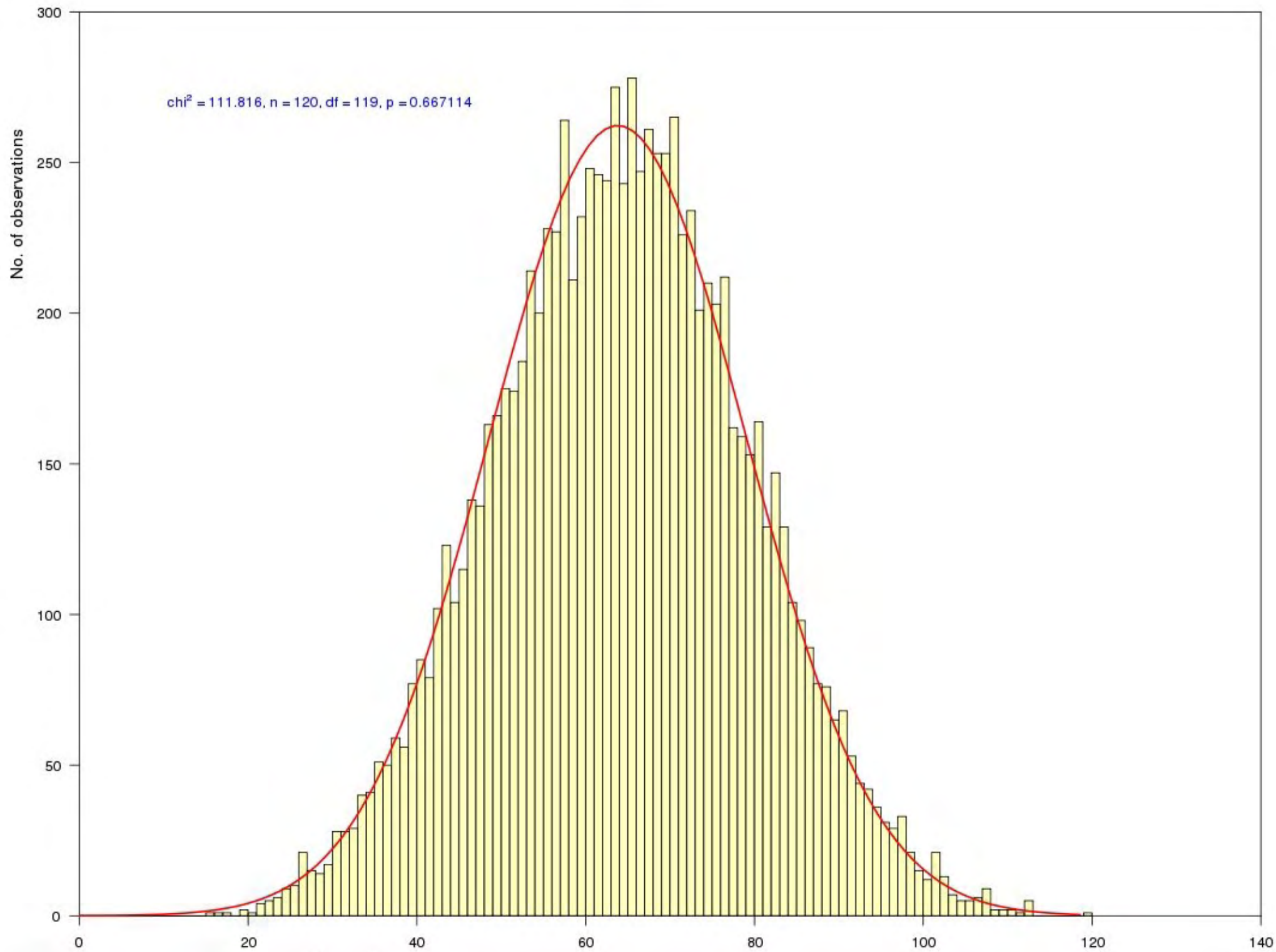
Demonstration

- 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.





Advanced Analysis

- CRSC Random Number Generation Technical Working Group Statistical Test Suite 2.0⁴
- Results here are only with 3 runs of 1 megabit data, and are preliminary only (more data will be collected by DEFCON)

Advanced Analysis

- 1/3 bitstreams fail two of 188 tests at $\alpha=0.01$.
- Given a block of random data divided into X bitstreams and subjected to Y tests at some threshold alpha value for failure Z , you expect even true random data to fail $X*Y*Z$ tests.
- Minimum 100 bitstreams required for a proper analysis.

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 written by fx

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/PhotodiodeAmplifiers.pdf>

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

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