1.4. Hardware Random Number Generator

Preston Maness

Motivation

Why?

- Familiarize myself with an important aspect of modern cryptographic systems.
- Gain experience with signal shaping.
- Explore the interface between hardware and software and how it can be both exploited and hardened.

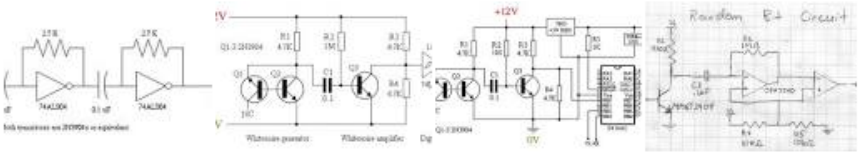
On the Shoulders of Giants

Google hardware random number generator schematic

Web Images Maps Shopping More Search tools

About 1,310,000 results (0.36 seconds)

Images for **hardware random number generator schematic** - Report images



Rob Seward :: True **Random Number Generator**
robseward.com/itp/adv_tech/**random_generator**/
I've included **circuit diagrams** as well as links to instructions for fabricating **...** True **random number generators** create sequences that are impossible to predict.

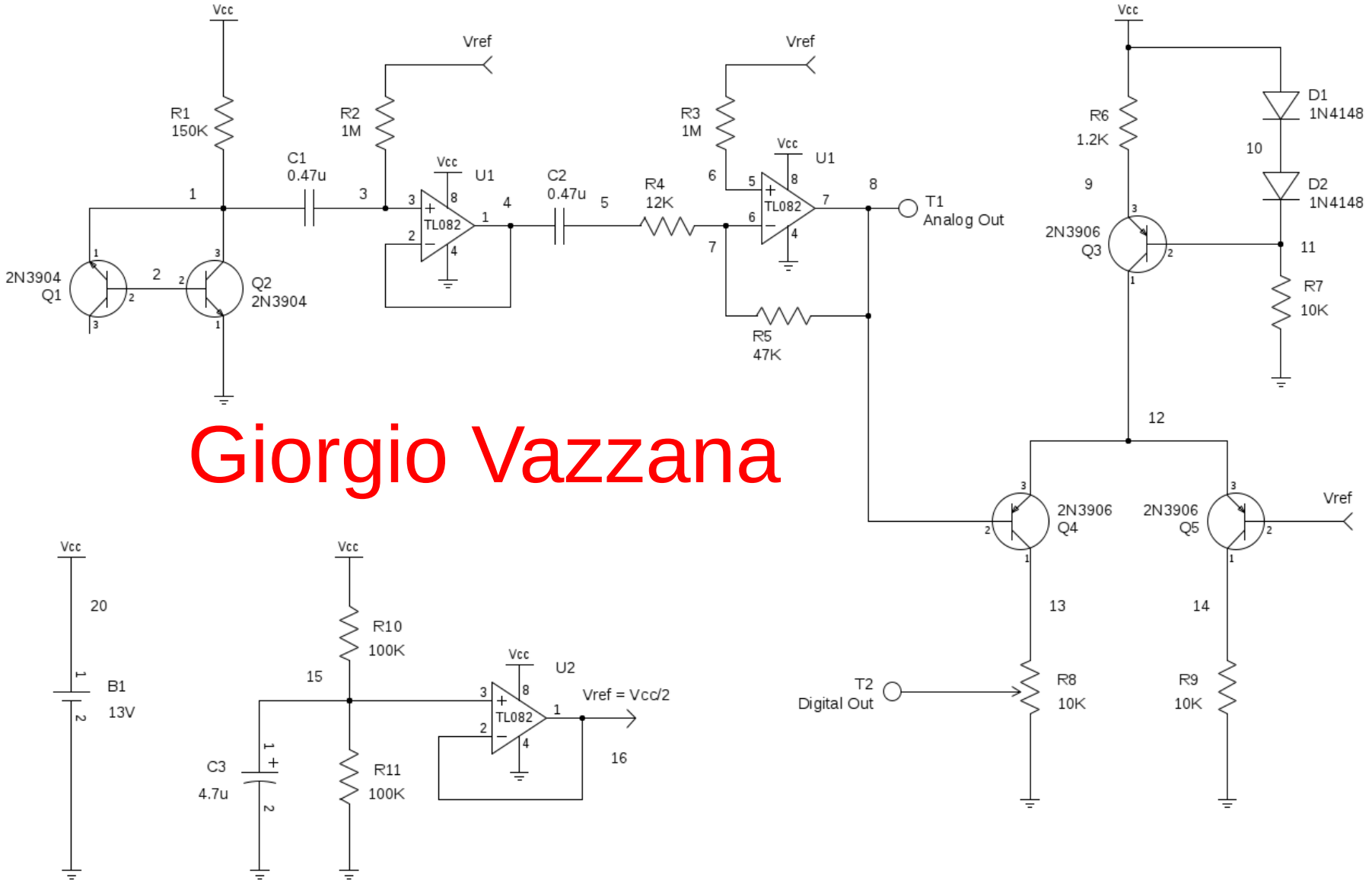
Hardware Random Bit **Generator** - Jfet.org
web.jfet.org/hw-rng.html
These are some notes about building a **hardware** random bit **generator**. **...** who contemplates arithmetic methods for the generation of **random numbers** is in a state of sin. **...** This **circuit** uses avalanche noise in a reverse-biased PN junction, the **...**

HOW TO – Build your own "True **Random Number Generator**" | MAKE

makezine.com/2006/10/06/how-to-build-your-own-tru/
by Phillip Torrone
Oct 6, 2006 - I've included **circuit diagrams** as well as links to instructions for fabricating your **...** True **random number generators** create sequences that are **...**

Building a **Hardware Random** Bit **Generator** for EVPmaker
www.tonbandstimmen.de › Start › Software › EVPmaker
I have built the **circuit** on a piece of perforated **circuit** board. **...** To get a 32-bit **random number**, the port has to be queried 32 times, while each retrieved bit is **...**

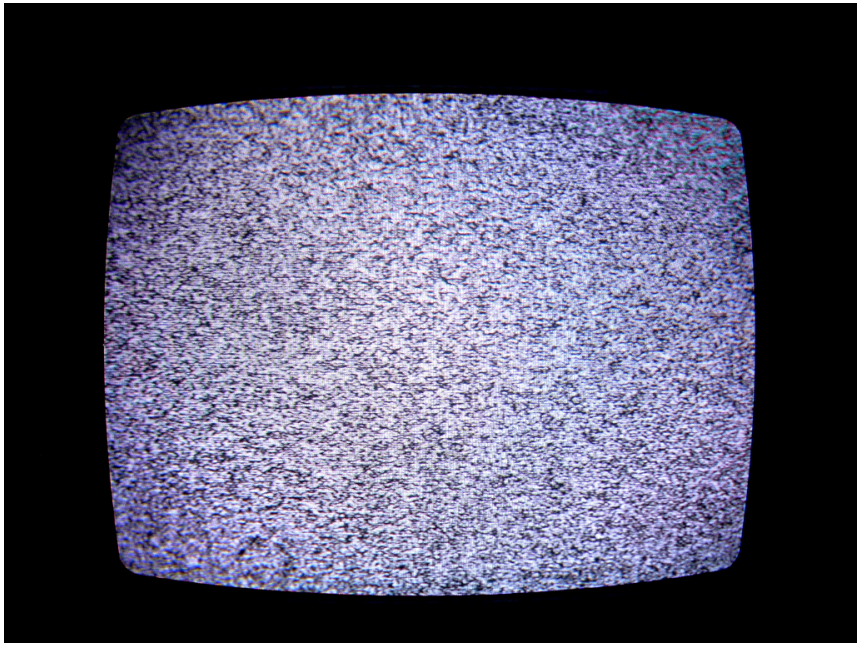
Random Sequence **Generator** based on Avalanche Noise
holdenc.altervista.org/avalanche/
After my experiments with a random sequence **generator** based on Chua **Circuit**, I started investigating other methods for building **hardware random number ...**



Giorgio Vazzana

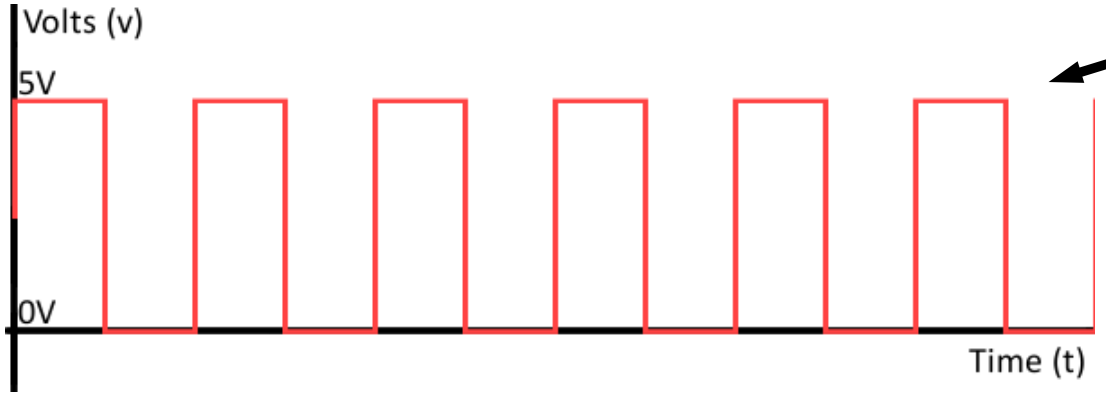
TITLE	Random Bit Generator based on Avalanche Noise		
FILE:		REVISION:	1.0
PAGE	1 OF 1	DRAWN BY:	Giorgio Vazzana

General Principle

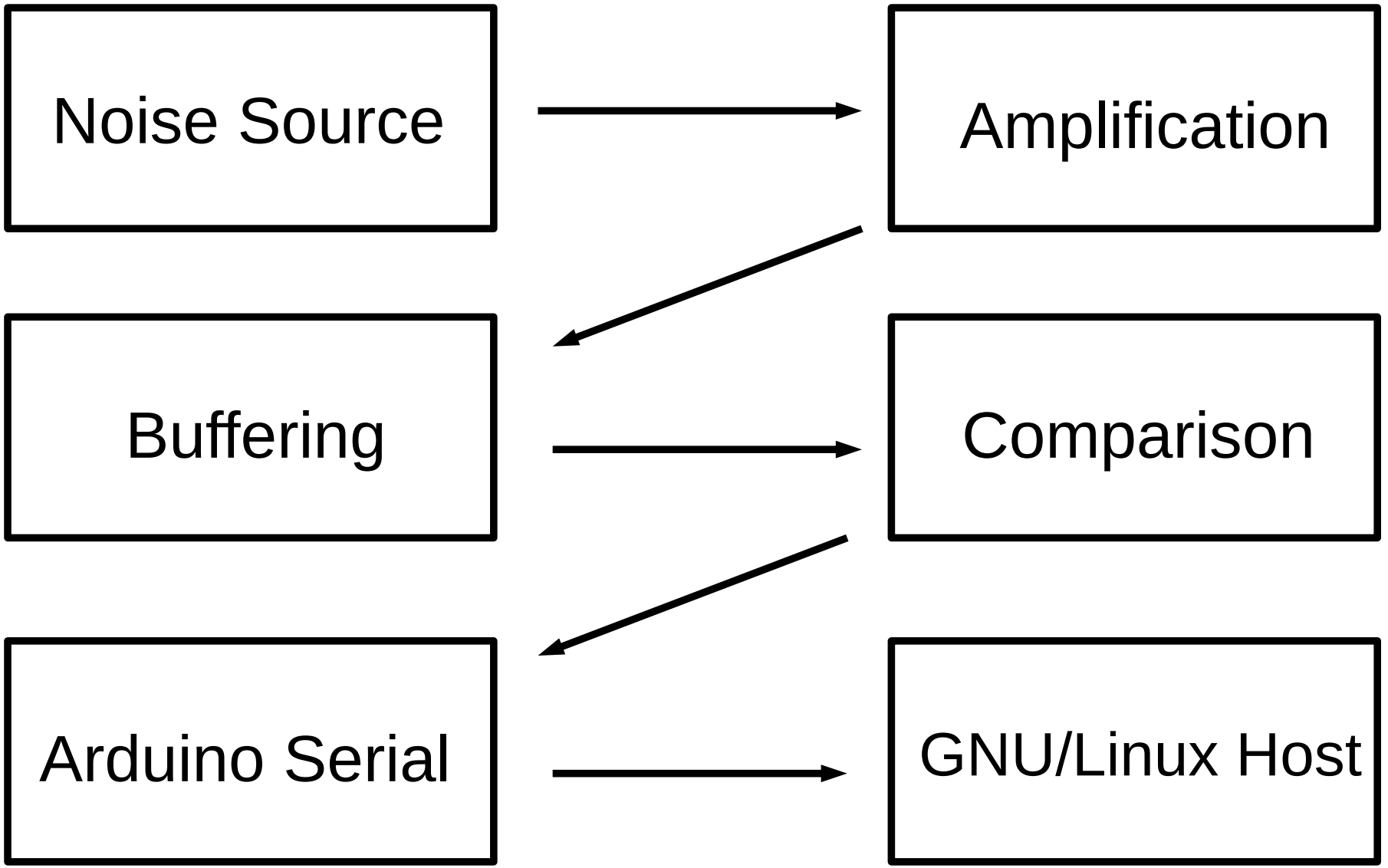


Amplify

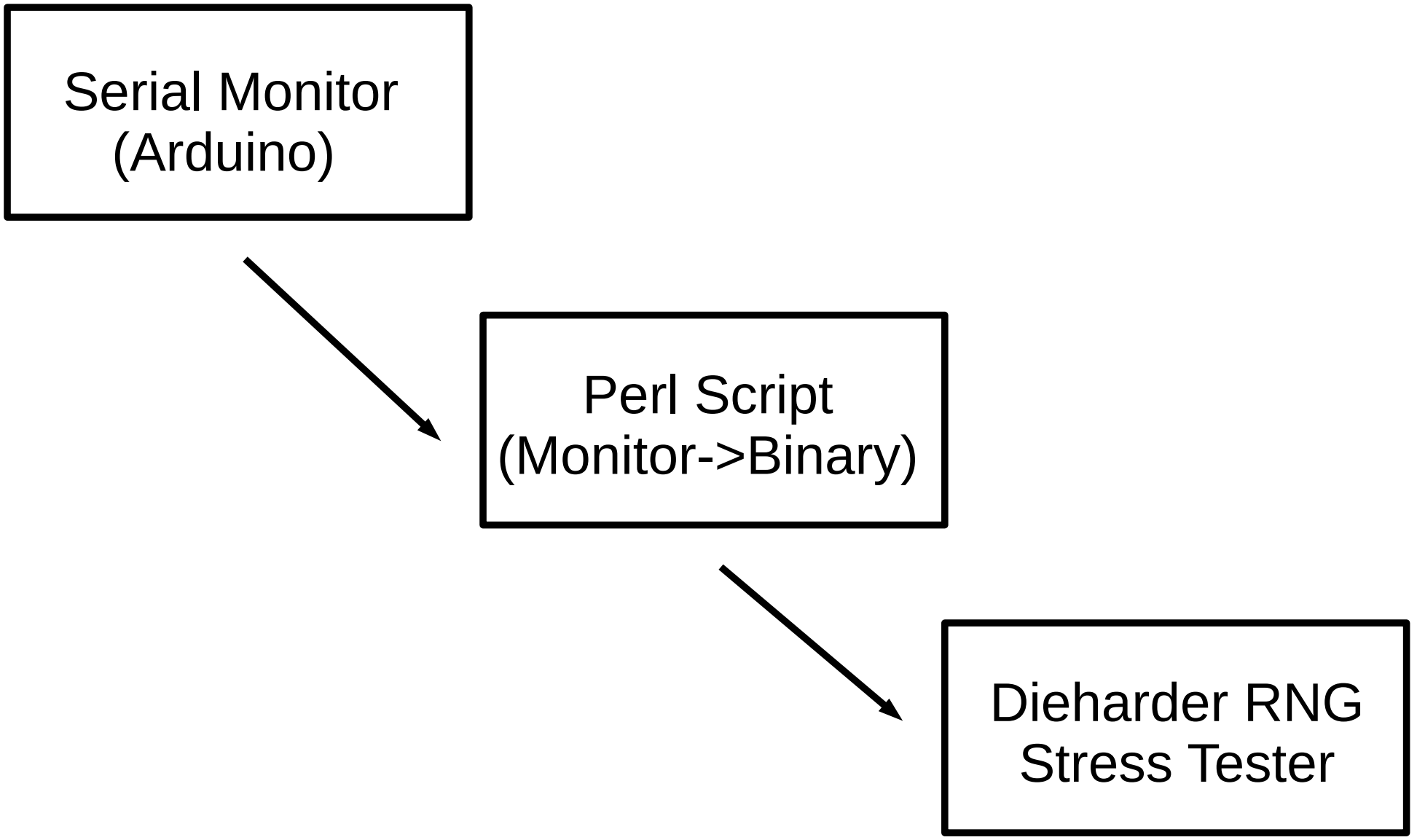
Digitize



Hardware Block Diagram



Software Stack



Deliverables

- Functioning prototype that outputs bits to the host.
- Host is able to read this bitstream.
- Host tests the randomness of bitstream.
- Inclusion of verified bitstream into entropy pool.
- Hardware-side verification.
- Automated testing.

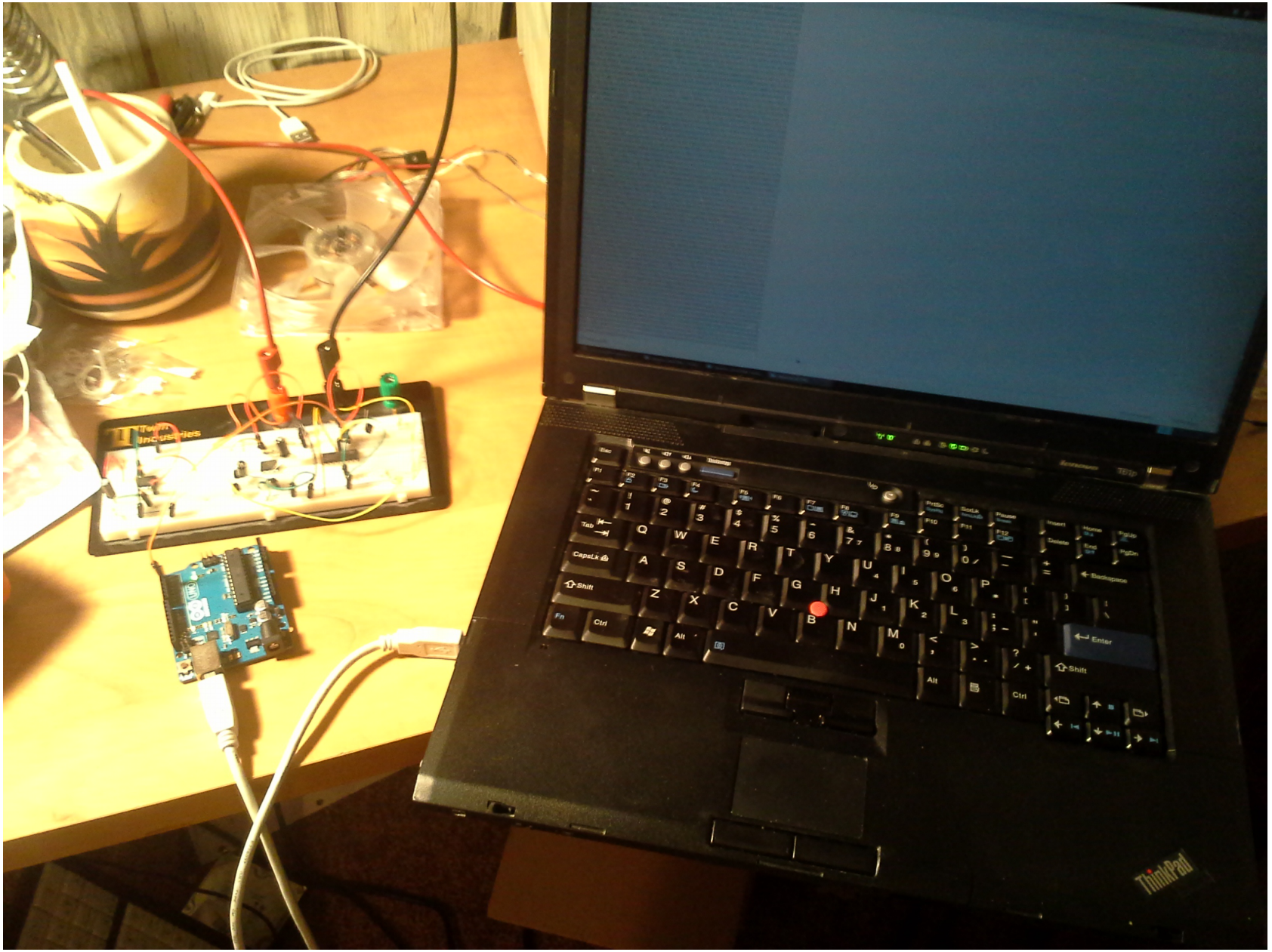
Timeline

Timeframe	Goals
Continuous	• Research, Verify, Research, and Research some more.
By end of September	• Verification pipeline determined (dieharder). • Hardware to host communication.
By end of October	• Verification pipeline functional and providing results of its tests.
By end of semester	• Verified bitstream. • Automated testing.

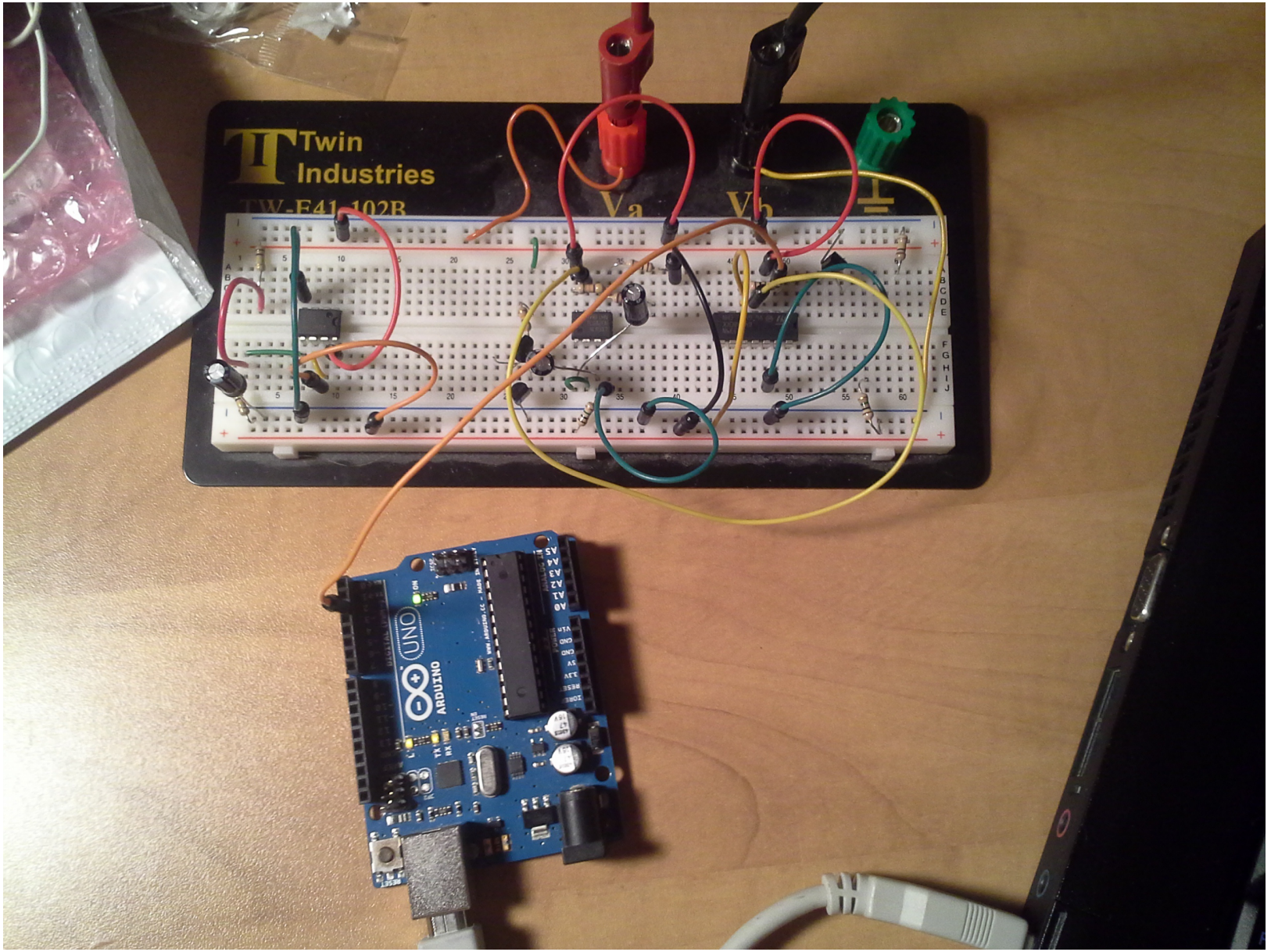
Expense Report

Item	Quantity	Cost
Op-Amp (TL082)	50	$9.99
BJT (2N3904)	50	$4.98
Comparator (LM339N)	10	$3.50
Arduino Uno	1	$25 (Already Owned)
Resistors	100	~$5 (Already Owned)
Capacitors	20	~$5 (Already Owned)
Wiring	Varied	$2.98
	TOTAL: **OUT OF POCKET:**	$56.45 **$21.45**

Messy Lab Benches!



Messy Breadboards!

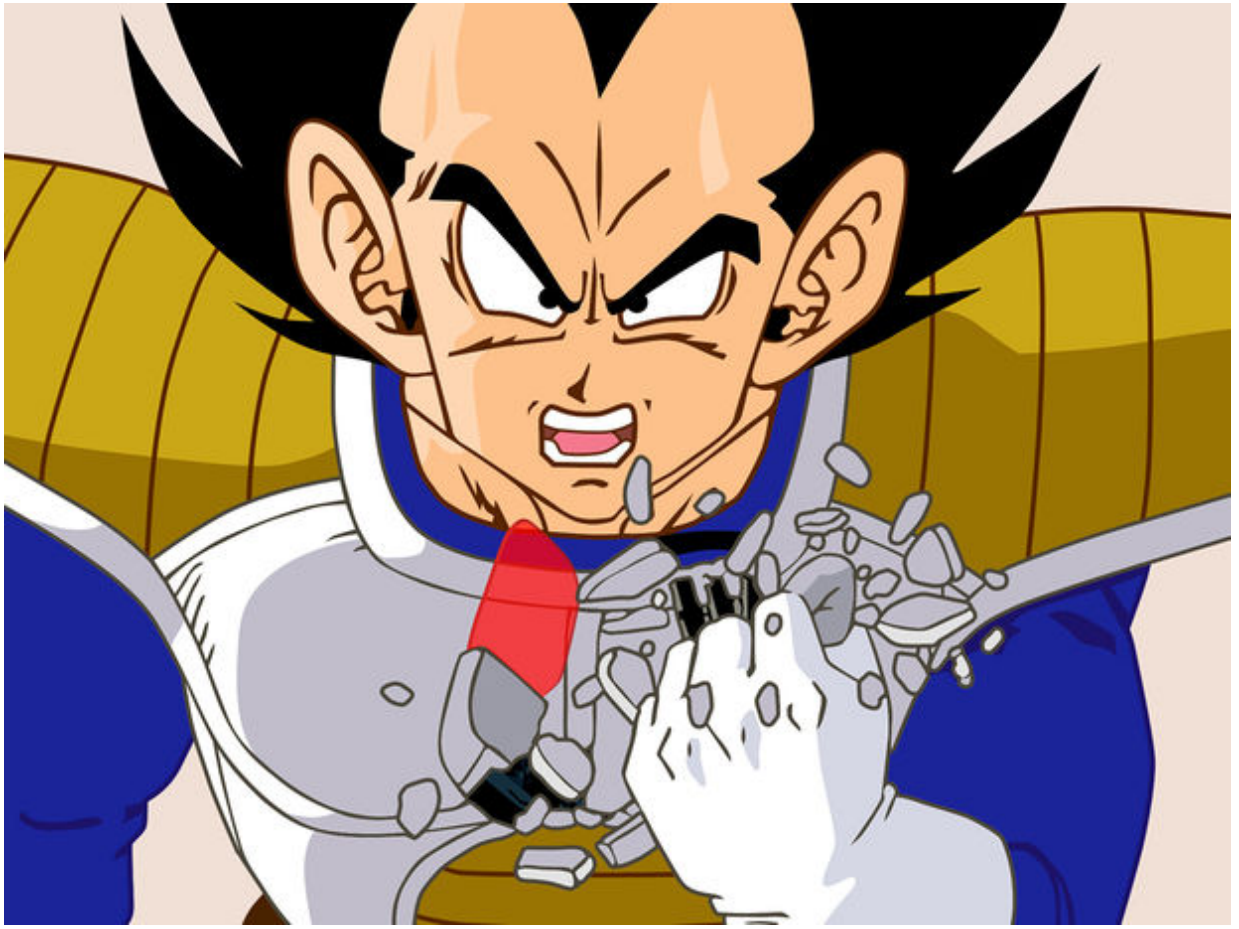


Messy Progress!

D'OH!

```
preston@neo:~/ee4390-senior-design-1/src/dieharder-3.31.1/dieharder$ ./dieharder
 -g 201 -a -f ../../rand-stream.bin
#=============================================================================#
#            dieharder version 3.31.1 Copyright 2003 Robert G. Brown          #
#=============================================================================#
   rng_name    |           filename             |rands/second|
 file_input_raw|           ../../rand-stream.bin|  3.55e+07  |
#=============================================================================#
        test_name   |ntup| tsamples |psamples|  p-value |Assessment
#=============================================================================#
# The file file_input_raw was rewound 288 times
   diehard_birthdays|   0|       100|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 2373 times
      diehard_operm5|   0|   1000000|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 5042 times
  diehard_rank_32x32|   0|     40000|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 6293 times
    diehard_rank_6x8|   0|    100000|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 6840 times
   diehard_bitstream|   0|   2097152|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 11213 times
        diehard_opso|   0|   2097152|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 14128 times
        diehard_oqso|   0|   2097152|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 15495 times
         diehard_dna|   0|   2097152|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 15628 times
diehard_count_1s_str|   0|    256000|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 18297 times
diehard_count_1s_byt|   0|    256000|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 18347 times
 diehard_parking_lot|   0|     12000|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 18381 times
    diehard_2dsphere|   2|      8000|     100|0.00000000|  FAILED
# The file file_input_raw was rewound 18406 times
    diehard_3dsphere|   3|      4000|     100|0.00000000|  FAILED
```

The file was rewound...



OVER 9000 TIMES!

Speed Issues

MY SAMPLING RATE IS BAD

AND I SHOULD FEEL BAD

Looking Forward

- Successful verification via faster sampling.
- Inclusion into kernel entropy pool.
- Automate testing harness.

- Verify with hardware.
- Parallelized implementation with rapid sampling of each stream to increase throughput.

Stalk The Project Manager!

https://github.com/aggroskater?tab=repositories

Preston Maness
aggroskater

aggroskater@gmail.com
http://aspensmonster.com
Joined on Jul 27, 2011

1	9	0
follower	starred	following

Contributions | Repositories | Public Activity | Edit Your Profile

Find a repository… Search

All Public Private Sources Forks Mirrors New

ee4323-digital-image-processing — Matlab ★0 ⑂0
Digital Image Processing with MATLAB
Last updated 6 days ago

cs4328-operating-systems — C ★0 ⑂0
Repo for CS4328 OS class with Dr. Ziliang during Fall 2013 at Texas State University.
Last updated 6 days ago

ee4352-cmos-vlsi — Verilog ★0 ⑂0
CMOS VLSI Design with Dr. Aslan Fall 2013 ; Final project 4-bit ALU.
Last updated 6 days ago

cs3339-computer-architecture — C ★0 ⑂0
Work for Dr. Burtscher's CS3339 Computer Architecture class at Texas State University
Last updated 25 days ago

ee4390-senior-design-i — Perl ★0 ⑂0
The project is a hardware RNG. The repo holds code, documentation, schematics/netlists/models, and other work for EE4390 Senior Design I with Dr. Stapleton, Fall 2013.