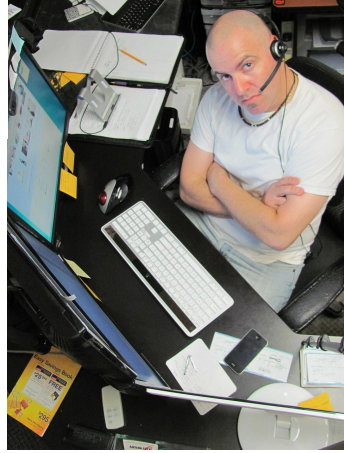
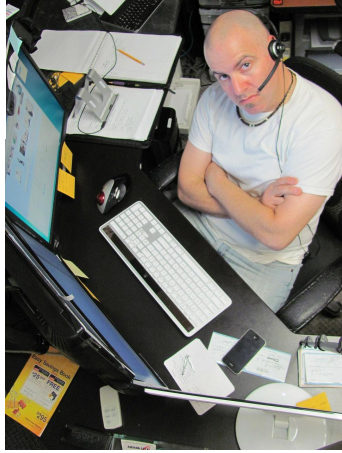
Extremely Secure Communication

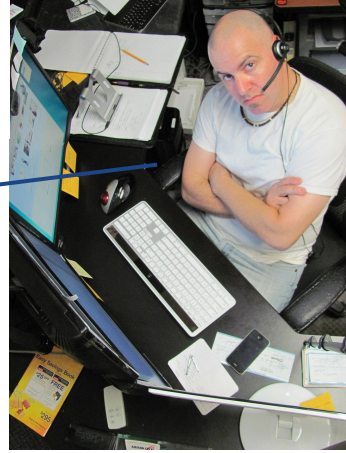
Daniel Romão - daniel.romao@os3.nl

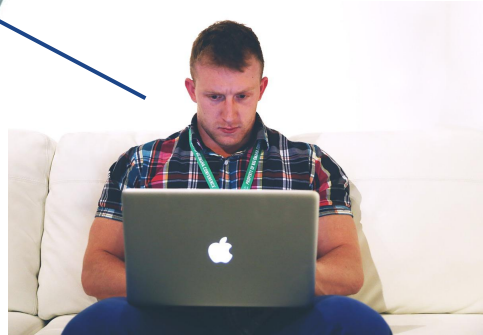


Oil Company



Oil Company





What (almost) everyone knows:

NSA collects traffic

Confidential data can be compromised

Backdoors in encryption-related software and hardware make it easier

Research Question

How can an extremely secure communication on the Internet be deployed for work teams and individuals around the globe?

What can we do?

1 - Avoid possible backdoors on RNGs

2 - Avoid having all data going over a single link

What can we do?

1 - Avoid possible backdoors on RNGs

- ➢ Use a verifiable HRNG to improve the kernel entropy pool

2 - Avoid having all data going over a single link

What can we do?

1 - Avoid possible backdoors on RNGs

- ➢ Use a verifiable HRNG to improve the kernel entropy pool

2 - Avoid having all data going over a single link

- ➢ Use a multipoint VPN!

Hardware Random Number Generator

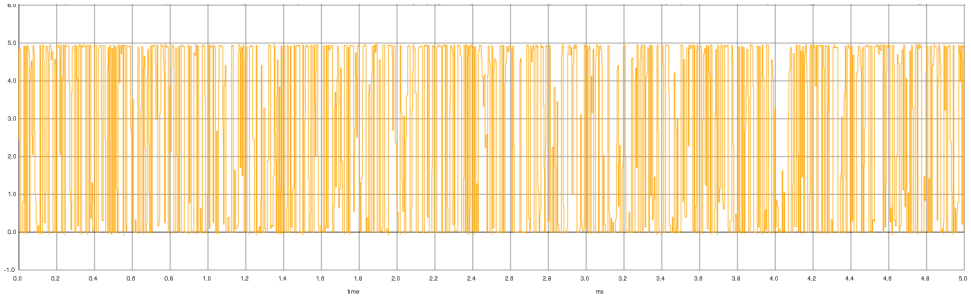
- Multiple devices exist, mostly closed source
  - Big price differences

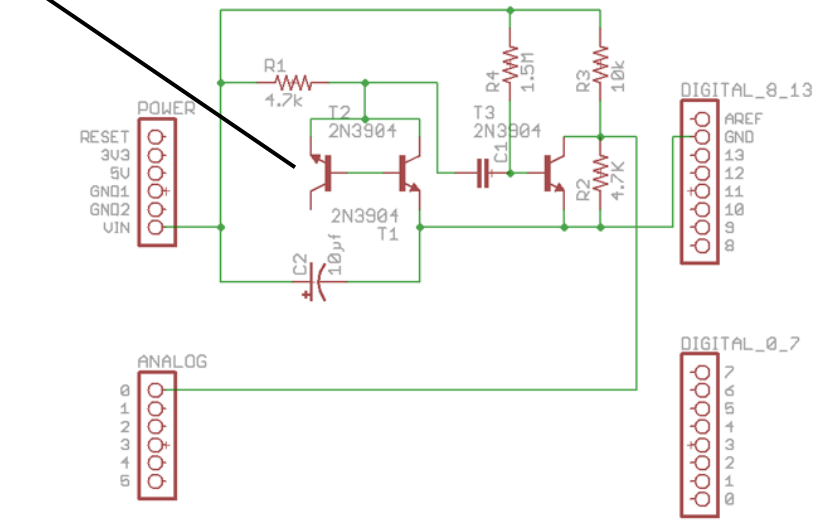
- Ongoing discussion on noise sources
  - PN junctions, RF noise, clock drift, thermal noise...

What if we implement a HRNG that is verifiable and has multiple noise sources?

HRNG - Related Work

- Rob Seward implemented a basic HRNG on Arduino using a single PN junction
  - Calibration on startup
  - XOR and Von Neumann filtering
  - Serial interface for output



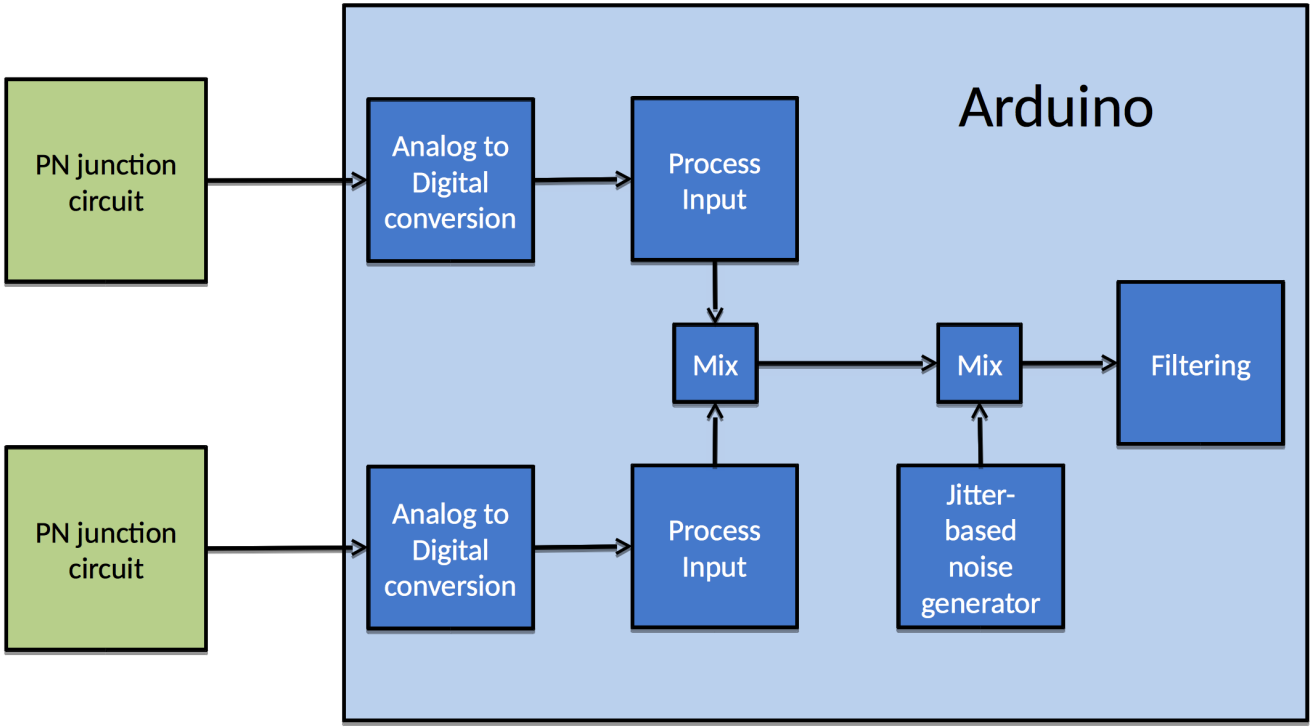


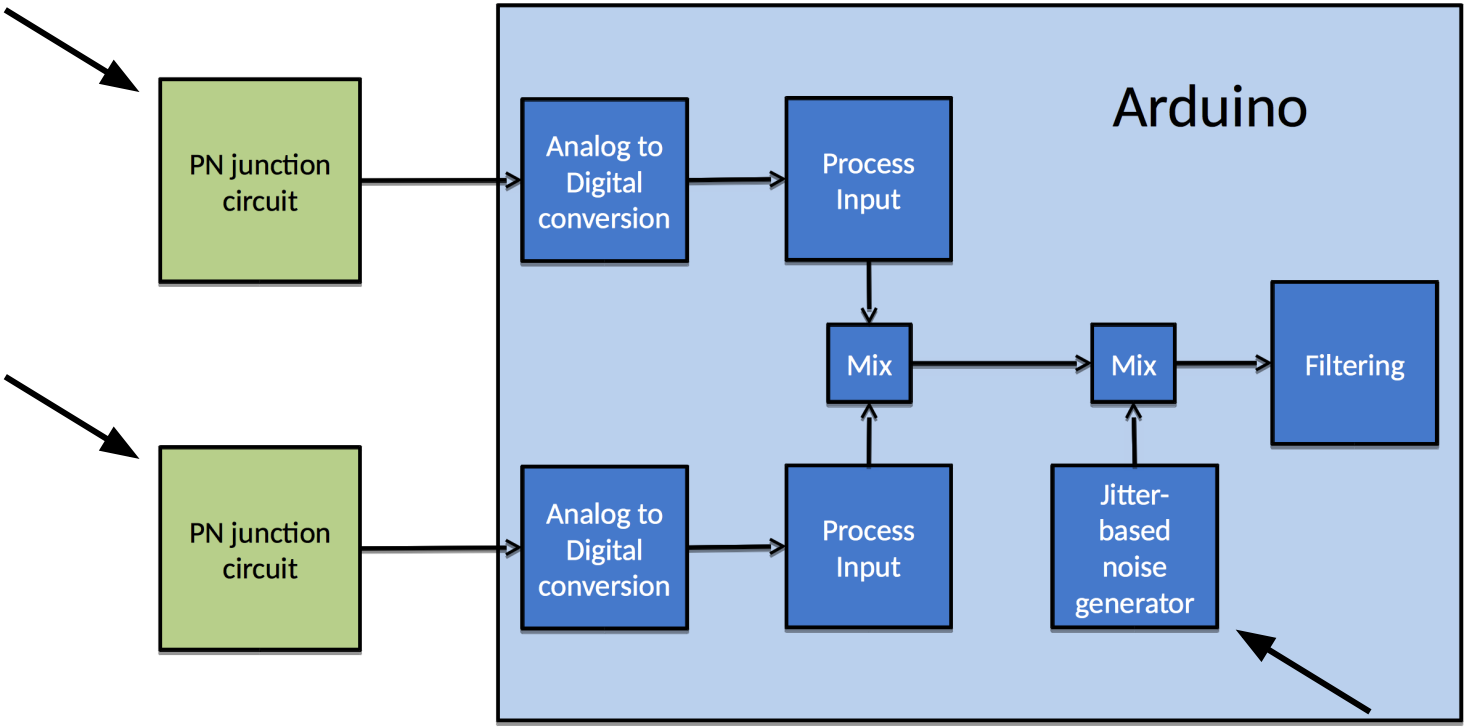
http://holdenc.altervista.org/avalanche/images/noise.png

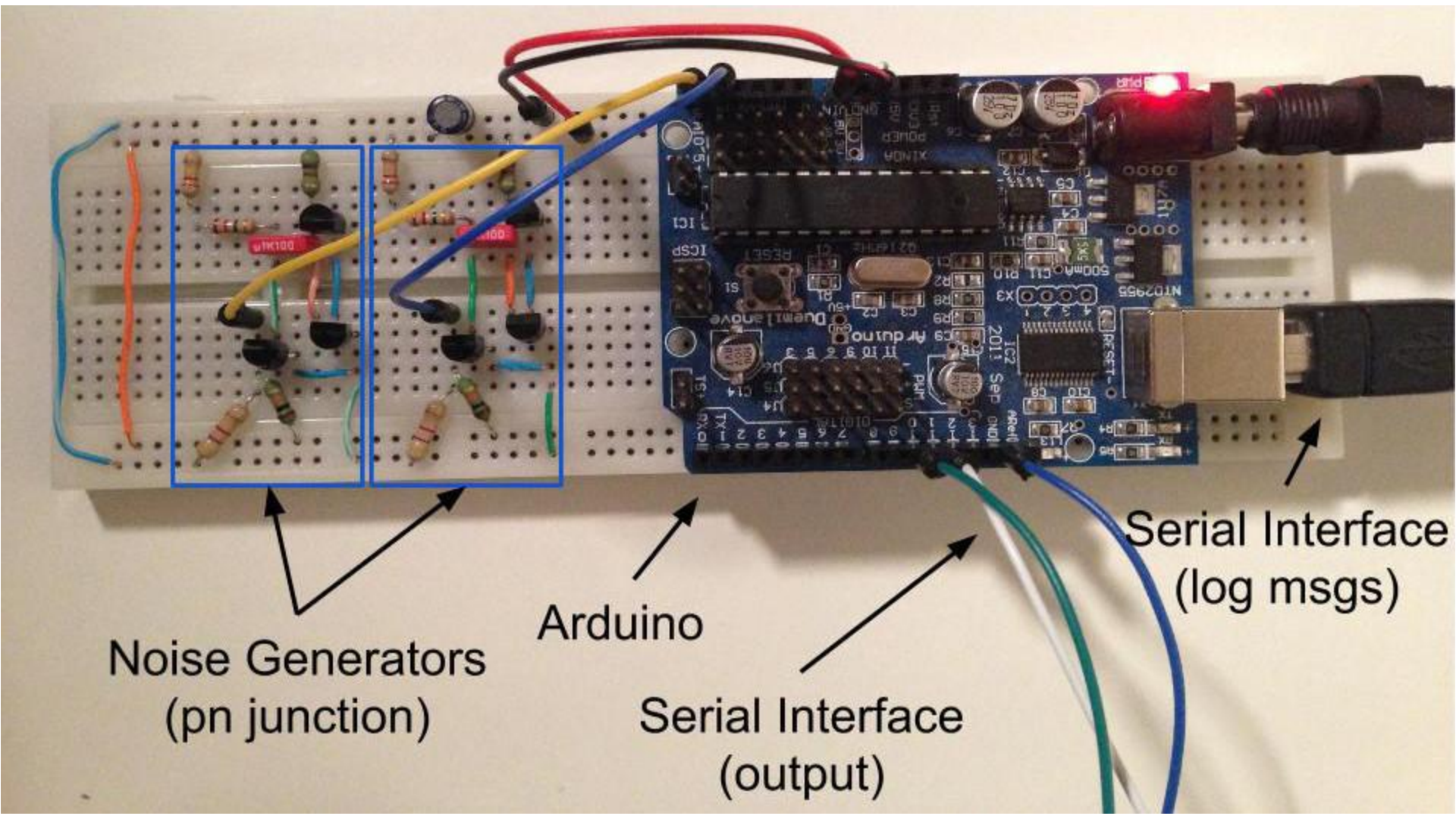
http://robseward.com/misc/RNG2/RNG_Version_2_images/rng2_circuit_small.png

HRNG Implemented

- Extension of the previous work
  - Multiple noise sources
  - Continuous calibration
  - Second serial interface for logging
  - Raw byte output mode for rng-tools


Arduino
PN junction circuit
PN junction circuit
Analog to Digital conversion
Analog to Digital conversion
Process Input
Process Input
Mix
Mix
Filtering
Jitter-based noise generator


PN junction circuit
PN junction circuit
Arduino
Analog to Digital conversion
Analog to Digital conversion
Process Input
Process Input
Mix
Mix
Filtering
Jitter-based noise generator


Noise Generators
(pn junction)
Arduino
Serial Interface
(output)
Serial Interface
(log msgs)

HRNG Testing

- Ent
  - Entropy, Optimum compression, Chi square, Arithmetic mean, Monte Carlo Pi, Serial correlation

- RNGtest
  - FIPS-140-2 test
  - To test cryptographic modules for use by the United States federal government

RNG	Filtering	Throughput (byte/sec)
Single oscillator	None	586.59
Single oscillator	XOR	587.12
Single oscillator	Von Neumann	208.24
Dual oscillator	None	383.39
Dual oscillator	XOR	375.59
Dual oscillator	Von Neumann	115.46
Jitter	None	0.85
Jitter	XOR	0.85
Jitter	Von Neumann	0.21
Single oscillator + jitter	None	0.85
Single oscillator + jitter	XOR	0.85
Single oscillator + jitter	Von Neumann	0.21
Dual oscillator + jitter	None	0.85
Dual oscillator + jitter	XOR	0.85
Dual oscillator + jitter	Von Neumann	0.22
/dev/urandom	n.a.	2730666.67

Ent results

Sample size: 2504 bytes

RNG	Filtering	Entropy	Optimum compression	Chi Square (2504 samples)	Arithmetic mean	Monte Carlo Pi	Serial correlation
Single oscillator	None	7.920038	0%	252.70 (50.00%)	129.5843	3.069544365 (2.29%)	-0.016443
Single oscillator	XOR	7.902325	1%	322.84 (0.50%)	130.6138	3.050359712 (2.90%)	-0.012846
Single oscillator	Von Neumann	7.903012	1%	305.25 (2.50%)	129.4093	3.059952038 (2.60%)	-0.004145
Dual oscillator	None	7.909748	1%	290.12 (10.00%)	126.6058	3.155875300 (0.45%)	-0.034352
Dual oscillator	XOR	7.905288	1%	306.07 (2.50%)	128.8694	3.098321343 (1.38%)	0.010862
Dual oscillator	Von Neumann	7.920281	0%	257.20 (50.00%)	129.9812	3.223021583 (2.59%)	-0.013156
Jitter	None	7.907869	1%	290.73 (10.00%)	130.472	3.031175060 (3.51%)	0.007691
Jitter	XOR	7.919676	1%	260.68 (50.00%)	128.6118	3.031175060 (3.51%)	0.02388
Jitter	Von Neumann	7.919558	1%	255.36 (50.00%)	129.3962	3.194244604 (1.68%)	0.02403
Single oscillator + jitter	None	7.908752	1%	288.69 (10.00%)	128.5555	3.117505995 (0.77%)	0.008573
Single oscillator + jitter	XOR	7.923098	0%	240.23 (50.00%)	127.3027	3.165467626 (0.76%)	-0.00664
Single oscillator + jitter	Von Neumann	7.90949	1%	299.73 (5.00%)	131.0276	3.184652278 (1.37%)	-0.020073
Dual oscillator + jitter	None	7.920467	0%	250.25 (50.00%)	125.5395	3.165467626 (0.76%)	-0.008814
Dual oscillator + jitter	XOR	7.924311	0%	242.68 (50.00%)	128.7999	3.107913669 (1.07%)	0.027533
Dual oscillator + jitter	Von Neumann	7.9119	1%	282.35 (25.00%)	130.8427	3.194244604 (1.68%)	0.000254
/dev/urandom	n.a.	7.932694	0%	228.37 (75.00%)	126.3586	3.050359712 (2.90%)	0.002745

Ent results

Sample size: 512Kb

RNG	Filtering	Entropy	Optimum compression	Chi Square (524288 samples)	Arithmetic mean	Monte Carlo Pi	Serial correlation
Single oscillator	None	7.987673	0%	4868.18 (0.01%)	128.0038	3.145489294 (0.12%)	0.000724
Single oscillator	XOR	7.987554	0%	4957.42 (0.01%)	128.1143	3.123058789 (0.59%)	-0.001192
Single oscillator	Von Neumann	7.9883	0%	4410.29 (0.01%)	128.8105	3.119213559 (0.71%)	0.000148
Dual oscillator	None	7.988324	0%	4392.78 (0.01%)	128.2537	3.137615729 (0.13%)	0.000895
Dual oscillator	XOR	7.988355	0%	4370.00 (0.01%)	128.2837	3.131390119 (0.32%)	0.000916
Dual oscillator	Von Neumann	7.988333	0%	4386.37 (0.01%)	128.3335	3.129467504 (0.39%)	-0.00196
/dev/urandom	n.a.	7.999602	0%	288.92 (10.00%)	127.3549	3.140408098 (0.04%)	-0.000704

RNGtest results

Sample size: 512Kb

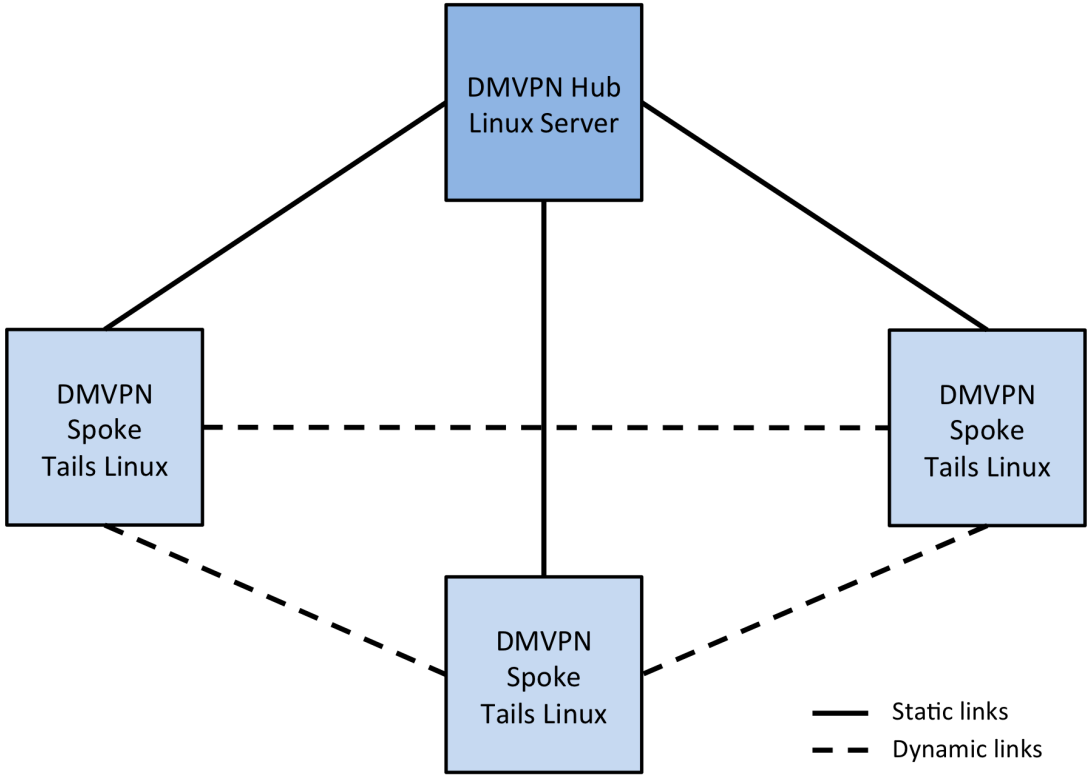
RNG	Filtering	Number of Successes	Number of Failures	Percentage of Success
Single oscillator	None	199	10	95.22%
Single oscillator	XOR	206	3	98.56%
Single oscillator	Von Neumann	209	0	100.00%
Dual oscillator	None	209	0	100.00%
Dual oscillator	XOR	209	0	100.00%
Dual oscillator	Von Neumann	209	0	100.00%
/dev/urandom	n.a.	209	0	100.00%

Multipoint VPN

- DMVPN
  - Cisco technology
  - Open source implementation exists: OpenNHRP
  - IPSec
  - Hub (server), Spokes (clients)

Operating System

- Tails Linux
  - Open source operating system
  - Aimed at privacy and anonymity on the Internet
  - Only traffic over Tor and I2P networks can go
  - Always boots from a clean install state


DMVPN Hub
Linux Server
DMVPN
Spoke
Tails Linux
DMVPN
Spoke
Tails Linux
DMVPN
Spoke
Tails Linux
Static links
Dynamic links

How to deploy the DMVPN spoke software on Tails?

Conclusion

- HRNG and a Tails DMVPN spoke integrate well with each other
- Jitter-based noise generator has very low throughput
- Dual oscillator without filtering was overall the setting with best performance

Future Work

- More experiments with the HRNG
  - Other noise sources and filtering
  - Faster microcontroller

- Optimization of the configuration

KPMG

UNIVERSITY OF AMSTERDAM

Thank you!

Go get it: https://github.com/dromao/arduino-rng

https://github.com/dromao/dmvpn-spoke