The UK's European university

University of Kent

Real World Crypto 2018

Quam Bene Non Quantum

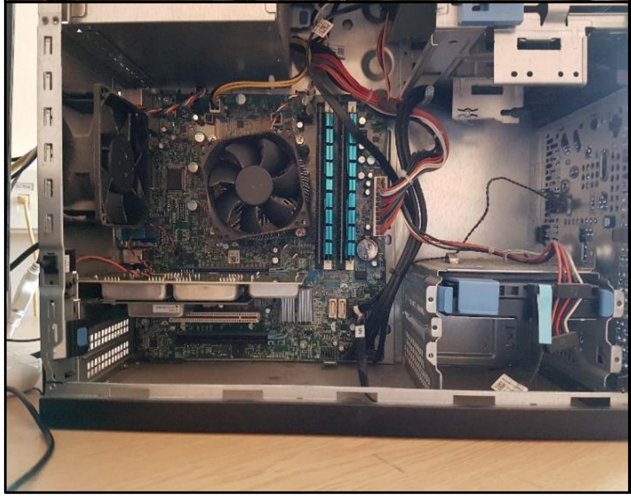
Identifying Bias in a Commercial Quantum Random Number Generator

Darren Hurley-Smith & Julio Hernandez-Castro

University of Kent | Computing

Index

Our targets




University of Kent

Our targets (continued)

Three modules tested:

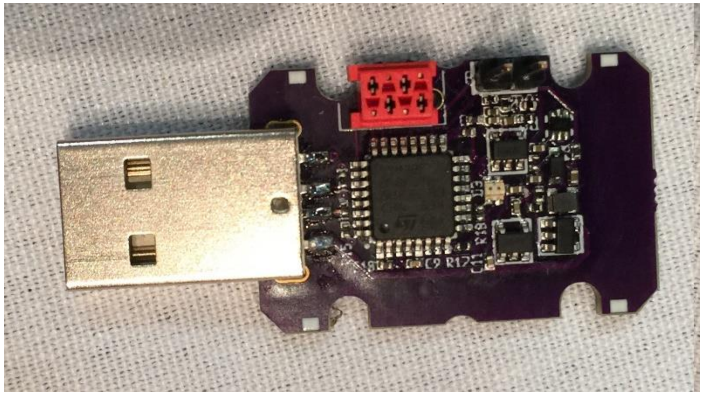
All three use Optical Quantum phenomena as their entropy source (beam splitting)
16M (PCI-E 16Mb/s) @ €2990
4M (PCI-E 4Mb/s) @ €1299
USB (4Mb/s) @ €990

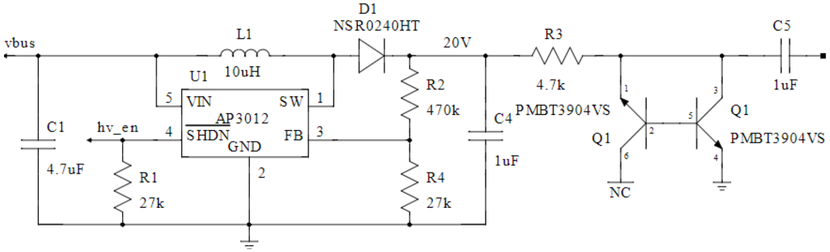
Data Collection:

100 x 2GiB collected from each device
EasyQuantis command-line utility
Raw and post-processed data

Speedtest Results (Raw)

16M (15.87Mb/s), 4M (3.86Mb/s), USB (3.96Mb/s)
ChaosKey TRNG (3.8Mb/s) @ €59





University of Kent

Results (in a nutshell)

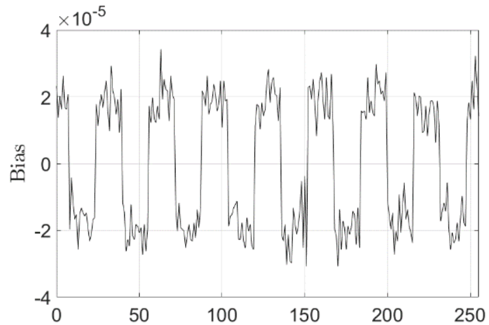
Quantis Claims	Our Results
True random bits	No. Heavily biased and correlated
16Mb/s, 4Mb/s of true random bits	No. Roughly 1/4th of that after post-processing
Post-processing optional	No. Vital & costly
Self-certification is OK	Self-certification is worthless
Third party certification is OK	Certification (below CC EAL5 or AIS 31 PTG.3) is useless
TRNGs with closed hardware design are OK	No. Security by obscurity and all that

Detailed Results (Dieharder/NIST/TestU01)

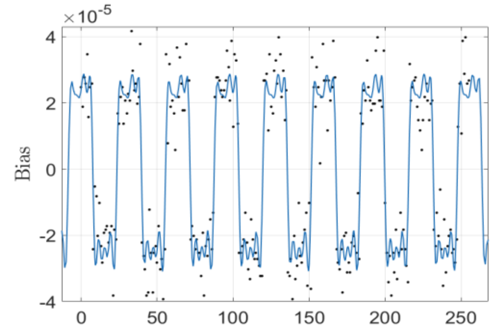
Device	Size	Dieharder	NIST STS 2.1.2	Alphabits	Rabbit
	(GiB)	(Failed/Weak/Passed)	(Passed/Total)	(Passed/Total)	(Passed/Total)
Quantis 16M	2	8 / 11 / 95	182 / 186	7 / 17	26 / 40
	2	6 / 13 / 95	181 / 186	9 / 17	32 / 40
	2	7 / 11 / 96	182 / 186	7 / 17	29 / 40
Quantis 4M	2	0 / 3 / 111	185 / 186	7 / 17	28 / 40
	2	0 / 5 / 109	186 / 186	7 / 17	28 / 40
	2	0 / 6 / 108	186 / 186	7 / 17	27 / 40
Quantis USB	2	0 / 6 / 108	184 / 186	14 / 17	33 / 40
	2	0 / 7 / 107	186 / 186	11 / 17	29 / 40
	2	1 / 6 / 107	184 / 186	10 / 17	30 / 40
ChaosKey	2	0 / 3 / 111	184 / 186	17 / 17	40 / 40
/dev/urandom	2	0 / 3 / 111	186 / 186	17 / 17	40 / 40

- Dieharder and NIST are passed
  - 16M is an exception, but further testing suggests these three initial results are anomalous
- Alphabits and Rabbit fail consistently
  - Devices fail slightly different tests more frequently than others
  - ChaosKey (TRNG USB module) passes all tests providing a TRNG baseline
  - *urandom* also passes all tests providing a PRNG baseline

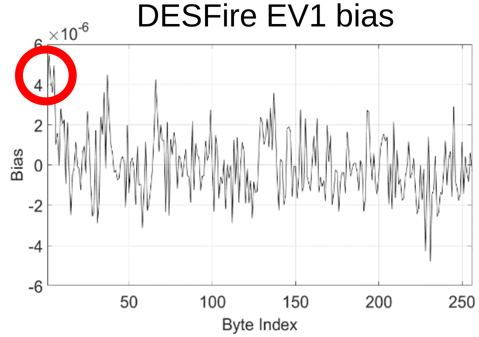
We’ve seen bad X^2 Results before…



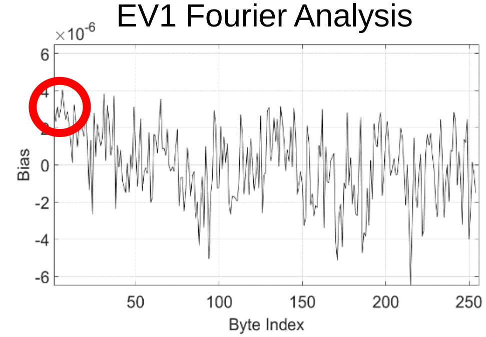
DESFire EV1 bias



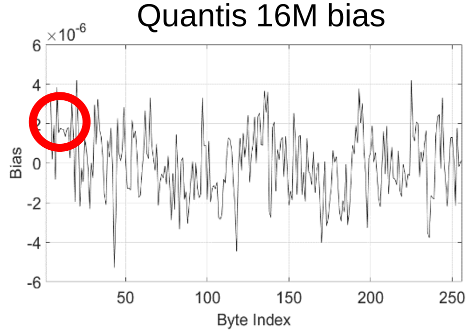
EV1 Fourier Analysis



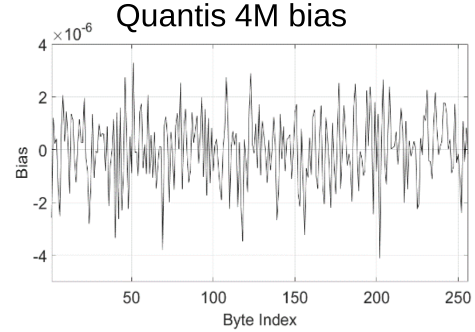
Quantis 16M bias



Quantis 4M bias



Quantis USB bias



/dev/random bias

Conclusion

Many TRNGs seem to barely pass well-known tests, then fail new ones

- Perhaps the classical test are all measuring the same things
- Perhaps an example of lazy engineering
- They are designed-for-testing

Quantum random number generation

- Inherent bias due to thermal noise on optical QRNG is a known phenomenon – physics circles
- Many devices claim random output despite this
- Randomness is achievable, but requires supporting hardware/software

Post-processing should be accounted for

- One shouldn't claim robust randomness at speeds prior to post-processing
- Post-processing is NOT optional
- Potential attack surface increases
  - Manipulation/poor choosing of the input matrix can affect output predictably
  - Unsuitable for IoT devices

Future Works: More Quantum TRNGs

Hotbits @ https://www.fourmilab.ch/hotbits/

- Timed successive pairs of radio-active decay events as entropy source
- Performs poorly in all tests except NIST STS 2.1.2

beta decay of Cæsium-137 and the subsequent rapid gamma emission by the resulting metastable Barium-137 nucleus.

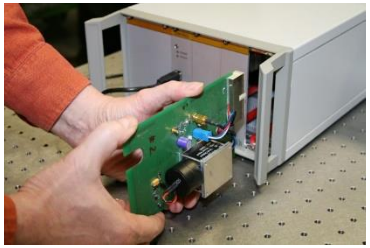
$$^{137}\mathrm{Cs} \xrightarrow{30.17\mathrm{y}} {}^{137\mathrm{m}}\mathrm{Ba} + \beta^- + \overline{\nu_e} \xrightarrow{156\mathrm{s}} {}^{137}\mathrm{Ba} + \gamma$$

Australian National University (ANU) QRNG @ https://qrng.anu.edu.au

- Broadband measurement of a vacuum field contained in the radio frequency sidebands of a single-mode laser
- Performs well in most tests - Some issues with TestU01 Rabbit

Humboldt University Physik Generator @ https://qrng.physik.hu-berlin.de

- Quantum randomness of photon arrival times as entropy source
- Performs very well in all tests so far
  - Dieharder, NIST STS 2.1.2, TestU01, Ent, all report good results



Comscire PQ32MU @ https://comscire.com/product/pq32mu/

- Quantum Entropy provided by shot-noise due to sub-threshold and gate tunnelling leakage in MOS transistors
- Performs well in all tests
- Extremely high rate of number generation (32Mb/s)
- Built-in post-processing
- Bulky!

Acknowledgements

This work received funding from the European Union's Horizon 2020 research and innovation programme, under grant agreement No.700326 (RAMSES project).

We would like to thank ECOST – CRYPTACUS action for their valuable and insightful discussion of this work

We would like to convey our thanks to ID Quantique (IDQ) for their timely and professional response to our responsible disclosure

Thank you for listening

Questions?