Comparison of hardware random number generators

In computing, a hardware random number generator is an apparatus that generates random numbers from a physical process. Such devices are often based on microscopic phenomena that generate a low-level, statistically random "noise" signal, such as thermal noise, the photoelectric effect or other quantum phenomena.

Manufacturer	Country	Model	Intro year	Interface	OS	Price	Throughput	Operating principle	Certifications / tests	Open hardware?	Software license
Altus Metrum	USA	ChaosKey 1.0	2016	USB	Linux	$40[1] €45[2]	10 Mbit/s[3]	Reverse biased semiconductor junction[4]	FIPS-140-2[3]	Open	GPLv2
Araneus Information Systems Oy	Finland	Alea II	2014	USB	Windows/Linux /BSD/MacOS X[5]	€109[6]	100 Kbit/s[5]	Reverse biased semiconductor junction	NIST STS / DIE HARD[5]	Closed	Proprietary
BitBabbler	Australia	BitBabbler Black[7]	2015	USB	Linux/BSD /Mac/Windows	AUD$49[8]	650 Kbit/s[9]	Mix of shot noise, Johnson–Nyquist noise, flicker noise, and some electromagnetic interference[10]	ENT test suite / NIST SP800-22 / DIE HARDER / TestU01[11]	Closed	GPLv2
		BitBabbler White[12]	2015	USB	Linux/BSD /Mac/Windows	AUD$199[8]	2.5 Mbit/s[9]	Mix of shot noise, Johnson–Nyquist noise, flicker noise, and some electromagnetic interference[10]	ENT test suite / NIST SP800-22 / DIE HARDER / TestU01[11]	Closed	GPLv2
Comscire	USA	PQ4000KS	2016	USB	Linux/Windows/Mac	$795[13]	4 Mbit/s[14]	Shot noise	NIST SP800-90 B, C,[15] NIST SP800-22 / DIE HARD[16]	Closed	Proprietary
		PQ32MU	2013	USB	Linux/Windows/Mac	$1,495[17]	32 Mbit/s[18]	Shot noise	NIST SP800-90 B, C,[19] NIST SP800-22 / DIE HARD[16]	Closed	Proprietary
Flying Stone Technology	Japan	FST-01 (includes NeuG 1.0)	2013	USB	Windows/Linux /FreeBSD/Mac	$35-$50[20][21]	602 Kbit/s[22]	Analog-to-digital converter noise	NIST SP800-22	Open	GPLv3
Generic	N/A	rtl-sdr dongles	2013	USB	Linux/Mac	$24[23]	2.8 Mbit/s[24]	Atmospheric noise. Requires rtl-entropy[25]	NIST SP800-22	Closed	GPLv3[25]
		STM32 Nucleo Dongles (Running NeuG 1.0)	2015	USB	Windows/Linux /FreeBSD/Mac	$12[26]	560 Kbit/s[22]	Analog-to-digital converter noise	NIST SP800-22	Closed	GPLv3
		Any webcam[27]	2017	USB	Windows/Linux /FreeBSD/Mac	$7[28]	960 Kbit/s[29]	Image noise	NIST SP800-22	Closed	Public domain
ID Quantique SA	Switzerland	Quantis-USB	2006	USB	Windows/Linux	€990[30]	4 Mbit/s[31]	Beam splitter	NIST SP800-22 / DIE HARD by METAS / CTL[31]	Closed	Proprietary
		Quantis-PCIe-4M	2010	PCIe	Windows/Linux	€1,299[30]	4 Mbit/s[31]	Beam splitter	NIST SP800-22 / DIE HARD by METAS / CTL[31]	Closed	Proprietary
		Quantis-PCIe-16M	2010	PCIe	Windows/Linux	€2,990[30]	16 Mbit/s[31]	Beam splitter	NIST SP800-22 / DIE HARD by METAS / CTL[31]	Closed	Proprietary
		Quantis Appliance 4M	2016	Network	Windows/Linux	N/A	4 Mbit/s[31]	Beam splitter	NIST SP800-22 / DIE HARD by METAS / CTL[31]	Closed	Proprietary
		Quantis Appliance 16M	2016	Network	Windows/Linux	N/A	16 Mbit/s[31]	Beam splitter	NIST SP800-22 / DIE HARD by METAS / CTL[31]	Closed	Proprietary
		Quantis AIS31	2015	PCIe / USB	Windows/Linux	N/A	75 Kbit/s[31]	Beam splitter	BSI AIS 31 / NIST SP800-22 / DIE HARD by METAS / CTL[32]	Closed	Proprietary
Intel	USA	Ivy Bridge-EP	2013	CPU	N/A	$323[33]	3 Gbit/s[34]	Johnson–Nyquist noise	N/A	Closed	Mixed
Kidekin	South Korea	TRNG	2015	USB	Linux/Windows/Mac	$79	2 Mbit/s[35]	Registerless linear-feedback shift registers[36]	NIST SP800-22	Closed	Proprietary
LETech	Japan	GRANG (various devices)	2008–2012	USB3/SATA	Linux/Windows	N/A	400 Mbit/s [37]	Johnson–Nyquist noise	NIST SP800-22	Closed	Proprietary
		GRANG Server	2013	Network	Linux	N/A	1.2 Gbit/s [38]	Johnson–Nyquist noise	NIST SP800-22	Closed	Proprietary
Moonbase Otago	N/A	OneRNG	2015	USB	Linux/Windows/Mac	$40[39]	350 Kbit/s[40]	Avalanche diode with optional atmospheric noise	NIST SP800-22	Open	GPLv3/LGPLv3
Protego ST (https://www.protegost.com)	Sweden	SG100 Classic (https://www.protegost.com/product-page/sg100-classic)	1996	USB	Linux/Unix /Windows/Mac	€255[41]	115 Kbit/s	Reverse biased diode	Diehard/FIPS-140-2	Closed	Source code Proprietary
		SG100 EVO-USB (https://www.protegost.com/product-page/sg100-evo)	2013	USB	Linux/Unix /Windows/Mac	€270[41]	115 Kbit/s	Reverse biased diode	Diehard/FIPS-140-2	Closed	Source code Proprietary
		SG100 EVO-USB CERT (https://www.protegost.com/product-page/sg100-evo-cert)	2013	USB	Linux/Unix /Windows/Mac	€530[41]	115 Kbit/s	Reverse biased diode	Diehard/FIPS-140-2	Closed	Source code Proprietary
Quant-Lab	Croatia	QRBG121	2005	USB	Linux/Unix /Windows/Mac	€2,700	12 Mbit/s[42]	Photoelectric effect	NIST SP800-22	Closed	Proprietary
QuintessenceLabs	Australia	qStream, qCrypt-xStream	2012	Network	Linux/Windows	N/A	1 Gbit/s[43]	Beam splitter	NIST SP800-90 A, B, C[43]	Closed	Proprietary
Simtec Electronics	UK	Entropy Key[44]	2009	USB	Linux/BSD /Windows	£36[45]	26.6 Kbit/s[46]	Avalanche noise	NIST SP800-22	Closed	MIT
TectroLabs	USA	SwiftRNG	2016	USB[47]	Windows/Linux /Mac[47]	$249[47]	100 Mbit/s[47]	Reverse biased Zener diodes	NIST SP 800-90B, NIST SP800-22[47]	Closed	Proprietary
		SwiftRNG LE	2016	USB[48]	Windows/Linux /Mac[48]	$149[48]	20 Mbit/s[48]	Reverse biased Zener diodes[48]	NIST SP 800-90B, NIST SP800-22[48]	Closed	Proprietary

Manufacturer	Country	Model	Intro year	Interface	OS	Price	Throughput	Operating principle	Certifications / tests	Open hardware?	Software license
		SwiftRNG Pro	2018	USB[49]	Windows/Linux /Mac[49]	$449[49]	200 Mbit/s[49]	Reverse biased Zener diodes[49]	NIST SP 800-90B, NIST SP800-22[49]	Closed	Proprietary
TRNG98	USA	TRNG9803	2009	Serial	Linux/Windows /Solaris/BSD	€109[50]	72 Kbit/s[51]		NIST SP800-22	Closed	Proprietary
		TRNG9815	2009	USB	Linux/Windows /Solaris/BSD	€620	550 Kbit/s[52]		NIST SP800-22	Closed	Proprietary
ubld.it (http://ubld.it/)	USA	TrueRNG v2 (http://ubld.it/products/truerng-hardware-random-number-generator/)	2014	USB	Linux/Windows/Mac	$49.95[53][54]	350 Kbit/s[55]	Reverse-biased semiconductor junction (avalanche/Zener noise)	DIEHARDER / FIPS-140-2 / NIST STS	Closed	Proprietary
		TrueRNG v3 (http://ubld.it/truerng_v3)	2016	USB	Linux/Windows/Mac	$49.95[56]	400 Kbit/s[57]	Reverse-biased semiconductor junction (avalanche/Zener noise)	DIEHARDER / FIPS-140-2 / NIST STS	Closed	Proprietary
		TrueRNG Pro (http://ubld.it/products/truerngpro)	2015	USB	Linux/Windows/Mac	$99[58][59]	3.2 Mbit/s[60]	Reverse-biased semiconductor junction (avalanche/Zener noise)	DIEHARDER / FIPS-140-2 / NIST STS	Closed	Proprietary
WaywardGeek	USA	Infinite Noise TRNG	2014	USB	Linux/Windows	$35[61]	300 Kbit/s[62]	Johnson–Nyquist noise	NIST SP800-22	Open	Public domain
Whitewood	USA	Entropy Engine	2015	PCIe	Linux	N/A	350 Mbit/s[63]	Photon bunching	NIST SP800-22/ NIST SP800-90 B & C/ DIE HARD/ ENT/ TEST U01	Closed	Proprietary

References

1. "Random Number Generators" (https://shop.gag.com/random.html).
2. "Vikings Shop" (https://store.vikings.net/chaoskey).
3. "Chaoskey - A Hardware Random Number Generator for Everyone" (https://debconf16.debconf.org/talks/94/).
4. "ChaosKey v1.0 Released — USB Attached True Random Number Generator" (https://keithp.com/blogs/chaoskey/).
5. "Araneus Alea II True Random Number Generator" (https://www.araneus.fi/products/alea2/en/). *www.araneus.fi*. Retrieved 2016-04-13.
6. "Araneus Alea II Ordering information" (https://www.araneus.fi/products/alea2/order/en/).
7. "BitBabbler Black - a high quality, single entropy source TRNG" (http://www.bitbabbler.org/what.html).
8. "BitBabbler - Own one yourself" (http://www.bitbabbler.org/buy.html).
9. "BitBabbler - User configurable bitrate" (http://www.bitbabbler.org/how.html#folding).
10. "BitBabbler: How it converts random noise to trusted entropy" (http://www.bitbabbler.org/how.html).
11. "TRNG hardware, software, and testing - BitBabbler" (http://bitbabbler.org/what.html). *bitbabbler.org*. Retrieved 2016-04-13.
12. "BitBabbler White - a high bitrate, high quality, multiple entropy source TRNG" (http://www.bitbabbler.org/what.html).
13. "ComScire QNG Model PQ4000KS" (https://comscire.com/product/pq4000ks/).
14. "PureQuantum™ Model PQ4000KS – ComScire" (https://comscire.com/product/pq4000ks/). *comscire.com*. Retrieved 2016-08-20.
15. "PQ4000KS – ComScire" (https://comscire.com/product/pq4000ks/). *comscire.com*. Retrieved 2016-04-13.
16. "Certifications – ComScire" (https://comscire.com/see-certifications/). *comscire.com*. Retrieved 2016-08-12.
17. "ComScire QNG Model PQ32MU" (https://comscire.com/product/pq32mu/).
18. "PureQuantum™ Model PQ4000KS – ComScire" (https://comscire.com/product/pq4000ks/). *comscire.com*. Retrieved 2016-08-20.
19. "PQ32MU – ComScire" (https://comscire.com/product/pq32mu/). *comscire.com*. Retrieved 2016-04-13.
20. "FST-01 devices" (http://www.seeedstudio.com/depot/s/fst-01.html).
21. "NeuG USB True Random Number Generator, FSF Shop" (https://shop.fsf.org/storage-devices/neug-usb-true-random-number-generator).
22. "NEUG1_0" (http://www.fsij.org/gnuk/neug_version1_0).
23. "NooElec NESDR Mini 2 USB RTL-SDR" (https://www.amazon.com/gp/product/B00P2UOU72/ref=as_li_tl?ie=UTF8&camp=1789&creative=390957&creativeASIN=B00P2UOU72).
24. "HWRNG through an rtl-sdr dongle" (https://pthree.org/2015/06/16/hardware-rng-through-an-rtl-sdr-dongle/).
25. "pwarren/rtl-entropy" (https://github.com/pwarren/rtl-entropy). *GitHub*. Retrieved 2018-05-03.
26. "STM32 Nucleo STM32F103 (sold at Akizuki Denshi)" (http://akizukidenshi.com/catalog/g/gM-07724/).
27. "Random Numbers Generated from Audio and Video Sources" (https://www.hindawi.com/journals/mpe/2013/285373/).
28. "PlayStation 3 Eye" (https://www.amazon.com/dp/B000VTQ3LU/ref=cm_sw_r_cp_ep_dp_htQoAb7W89Y8D).
29. "The Entropy of a Digital Camera CCD/CMOS Sensor" (https://pthree.org/2017/12/22/the-entropy-of-a-digital-camera-ccd-cmos-sensor/). *Aaron Toponce*. Retrieved 2017-12-26.
30. "ID Quantique Online Shop" (https://www.idquantique.com/shop/online-shop/).
31. "Quantis TRNG (True Random Number Generator)" (http://www.idquantique.com/random-number-generation/quantis-random-number-generator/). *IDQ*. Retrieved 2016-04-08.
32. "Quantis AIS 31 certified random number generator (RNG)" (http://www.idquantique.com/random-number-generation/quantis-ais-31/). *IDQ*. Retrieved 2016-04-13.
33. "Intel Core i7-4820K on Newegg" (http://www.newegg.com/Product/Product.aspx?Item=N82E16819116940).
34. "Intel DRNG Implementation Guide" (https://software.intel.com/en-us/articles/intel-digital-random-number-generator-drng-software-implementation-guide).
35. "Kidekin TRNG online user manual" (http://kidekin.nimp.co.uk/trng/kidekin_trng_user_manual.html).
36. "Kidekin TRNG user manual" (http://kidekin.nimp.co.uk/trng/kidekin_trng_user_manual.html). *kidekin.nimp.co.uk*. Retrieved 2015-06-21.
37. "LETech" (http://www.letech.jpn.com/rng/grang_pcic_8ch_e.html).
38. "LETech" (http://www.letech.jpn.com/rng/grang_server_e.html).
39. "OneRNG shop website" (http://moonbase.tictail.com/). Retrieved 20 April 2016.
40. "moonbaseotago.com OneRNG" (http://www.moonbaseotago.com/onerng/).
41. "ProtegoST Store" (https://www.protegost.com/shop/).
42. "QRBG121" (http://qrbg.irb.hr/).
43. "High Speed True Random Numbers for Cyber Security - QuintessenceLabs" (http://www.quintessencelabs.com/products/qstream/). *QuintessenceLabs*. Retrieved 2016-04-13.
44. "Simtec Electronics Entropy Key" (http://www.entropykey.co.uk/). *Simtec Electronics Entropy Key*. Retrieved 2017-10-24.
45. "Simtec Electronics Entropy Key Shop" (http://www.entropykey.co.uk/shop/). *Simtec Electronics Entropy Key*. Retrieved 2017-10-24.
46. "The Entropy Key" (https://pthree.org/2012/10/05/the-entropy-key/). *Aaron Toponce personal blog*. Retrieved 2017-10-24.
47. "SwiftRNG" (https://tectrolabs.com/swiftrng/). *TectroLabs*. Retrieved 20 January 2018.
48. "SwiftRNG LE" (https://tectrolabs.com/swiftrng-le/). *TectroLabs*. Retrieved 20 January 2018.
49. "SwiftRNG Pro" (https://tectrolabs.com/swiftrng-pro/). *TectroLabs*. Retrieved 20 January 2018.
50. "TRNG9803 in the store" (http://www.trng98.se/shop/product_info.php?products_id=33).
51. "TRNG9803 product description" (http://www.trng98.se/serial_trng_9803.html).
52. "TRNG9815" (http://www.trng98.se/usb_trng_9815.html).
53. "TrueRNG - Hardware Random Number Generator" (http://ubld.it/products/truerng-hardware-random-number-generator/). Retrieved 2016-08-20.
54. "TrueRNG V2 by Ubld.It Electronics" (https://www.tindie.com/products/ubldit/truerng-v2/?pt=full_prod_search). *Tindie*. Retrieved 2016-08-20.
55. "ubld.it TrueRNG overview" (http://ubld.it/products/truerng-hardware-random-number-generator/).
56. "TrueRNG - Hardware Random Number Generator v3" (http://ubld.it/truerng_v3). ubld electronics, llc. Retrieved 2016-08-20.
57. "TrueRNG - Hardware Random Number Generator" (http://ubld.it/truerng_v3). Retrieved 2016-08-20.
58. *TrueRNGpro - USB Hardware Random Number Generator* (https://www.amazon.com/TrueRNGpro-Hardware-Random-Number-Generator/dp/B01JTJ6D0S/ref=sr_1_1?ie=UTF8&qid=1471729952&sr=8-1&keywords=truerngpro).
59. "TrueRNGpro by Ubld.It Electronics" (https://www.tindie.com/products/ubldit/truerngpro/?pt=full_prod_search). *Tindie*. Retrieved 2016-08-20.
60. "TrueRNGpro by Ubld.It Electronics" (https://www.tindie.com/products/ubldit/truerngpro/). *Tindie*. Retrieved 2015-09-28.
61. "tindie.com Infinite Noise" (https://www.tindie.com/products/WaywardGeek/infinite-noise-true-random-number-generator/).
62. "github.com Infinite Noise TRNG" (https://github.com/waywardgeek/infnoise/).
63. "Entropy Engine -Quantum true random number generator" (https://www.whitewoodsecurity.com/products/entropy-engine/). Retrieved 2016-07-21.