Entropy is good

RANDAEMON Technology

Random numbers are produced

”Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin. For, as has been pointed out several times, ***there is no such thing as a random number - there are only methods to produce random numbers****, and a strict arithmetic procedure of course is not such a method.”*

J. von Neumann, **Various techniques used in connection with random digits**
vol. **Monte Carlo Method**, eds. A.S. Householder, G.E. Forsythe and H.H. Germond, **1951**

© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

Why entropy is good?

- Large entropy means that there are many possibilities for the states of the system (e.g., the number of atoms to decay)
- Extracting the information about these states leads directly to random numbers
- Practical sources of entropy are based on physical effects:
  - thermal, shot, avalanche, or radio noise
  - computer clock drift
  - polarization of photons
  - *radioactive decays*

Why beta decay?

- The best source of entropy is the one that weakly interacts with the world
- Gravitational, electrical, and magnetic fields are very strong
- Nuclear interactions act only directly upon elementary particles ☞ very short range of interactions

Weak* forces are responsible for beta decay

**stronger than gravitational forces but only over short distances inside nuclei*

© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

Beta decay

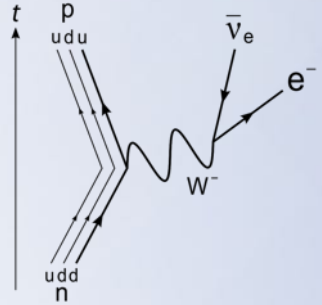
- Most beta-decaying nuclei create multiparticle cascades
  - not suitable for entropy extraction (*complicated Feynman diagrams*)
- There are three common isotopes with pure beta decay:
  - Tritium (^{3}H) $t_{1/2}$ = 12.3 years, average electron energy $\bar{E}$ = 5.7 keV
  - Carbon-14 $t_{1/2}$ = 5,730 years, average electron energy $\bar{E}$ = 49 keV
  - Nickel-63 $t_{1/2}$ = 98.7 years, average electron energy $\bar{E}$ = 17 keV
- **Nickel is the best source of entropy because of $t_{1/2}$ and $\bar{E}$**

© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

Safe entropy source

^{63}Ni as a source of randomness:

- pure beta decay: $^{63}Ni_{28} \rightarrow {}^{63}Cu_{29} + e^- + \bar{\nu}_e$
  - maximum electron energy 67 keV
  - anti-neutrino is practically non-interacting with anything



- range of 70 keV electrons:
  - in the air, about 7 cm ☞ there's no radiation at the distance of 3" from a source
  - In the water, about 78 µm ☞ water layer on the eyes or in the guts is > *100* µm thick
  - in the tissue, about 68 µm ☞ epidermis (dead part of the skin) is > *100* µm thick
  - In the metallic Cu, about 13 µm ☞ no radiation at all outside of the IC enclosure
- activity per simple device ≤ 25 µCi
  - if fully digested (?), the dose absorbed in a human body would be about 0.75 mSv/year
  - for comparison: *US natural background* is about 3 mSv/year; *Annual Limit on Intake* is 0.5 Sv

No radiation risk during manufacturing, for customers, and recycling

© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

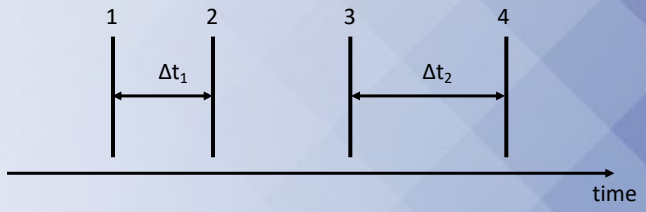
Extraction of entropy from beta decays

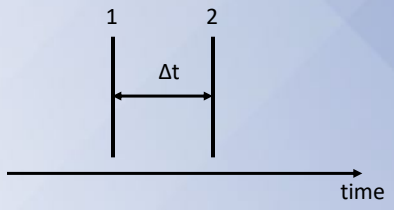
- Decays are random in time (*ticking*) and in space (*place*, *direction*)
- Nickel-63 maximum surface radioactivity of about 15 mCi/cm^2 corresponds to about 10^6 counts/sec on a 0.18 mm^2 detector (240 µm radius)
- Electron's detector can be a PIN or SPAD diode
- Time differences between events detected by such a detector can give about 250 kbit/sec

© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

Temporal entropy extraction

- Comparison of times between four decays:
  - $\Delta t_1 < \Delta t_2$ ☞ generate zero; $\Delta t_1 > \Delta t_2$ ☞ generate one
  - if exactly the same ☞ reject event, use the next four pulses
  - alternating direction of comparisons for better randomness
- Poisson distribution of times between pulses:
  - comparisons with median time between pulses
  - $\Delta t < t_m$ ☞ generate zero; $\Delta t > t_m$ ☞ generate one
  - if exactly the same ☞ reject event, use the next two pulses
- Last three bits of time between two pulses:
  - requires fast clock and good counter
  - the most effective method per number of pulses registered

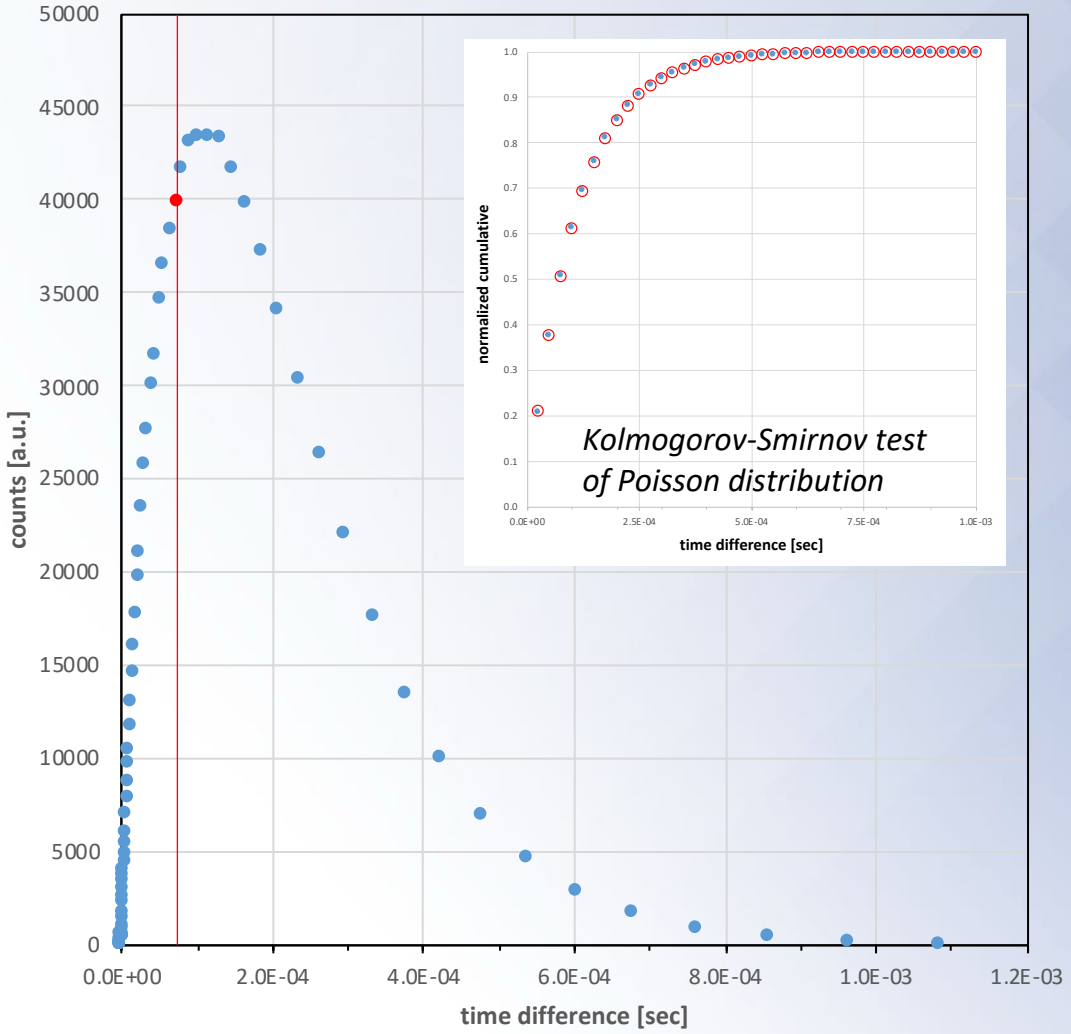




© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

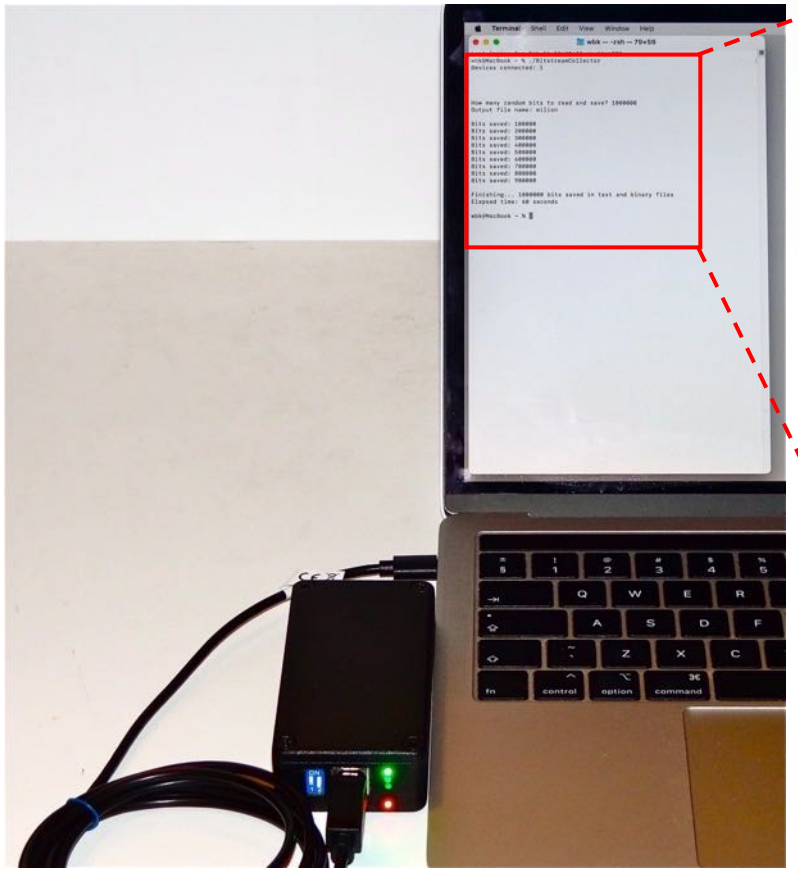
RANDAEMON PoC of QRNG based on PIN diode

Statistically tested theoretical Poisson distribution of time differences between pulses **confirms** the physical model of the device and **proves** its true randomness



© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

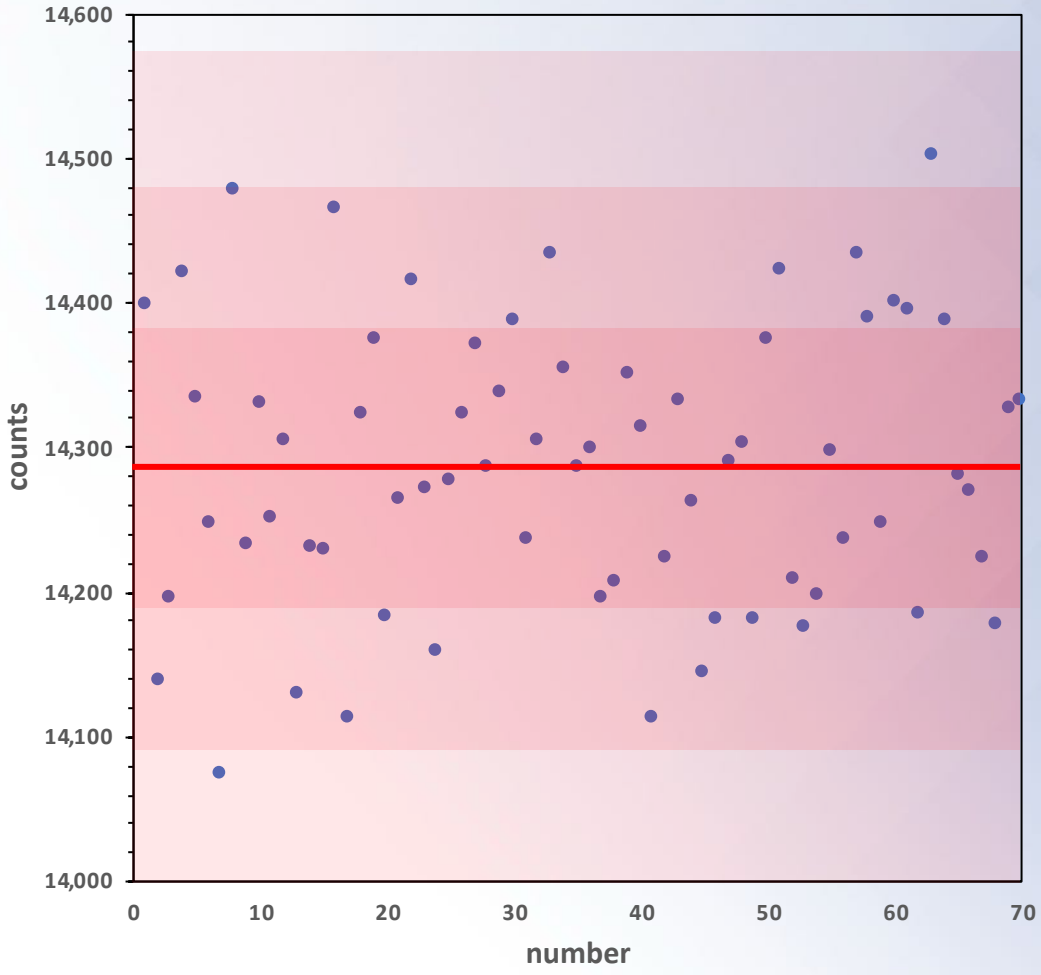
RANDAEMON PoC at work



```
wbk@MacBook ~ % ./BitstreamCollector
Devices connected: 1



How many random bits to read and save? 1000000
Output file name: milion

Bits saved: 100000
Bits saved: 200000
Bits saved: 300000
Bits saved: 400000
Bits saved: 500000
Bits saved: 600000
Bits saved: 700000
Bits saved: 800000
Bits saved: 900000

Finishing... 1000000 bits saved in text and binary files
Elapsed time: 60 seconds
```

Testing, applications

- PoC devices were extensively tested using the NIST battery of tests
  - NIST Publication 800-22
- Application: simulating drawings for a lottery ☞



"20 out of 70"
1,000,000 draws
average = 14,285.7
std. dev. = 96.97

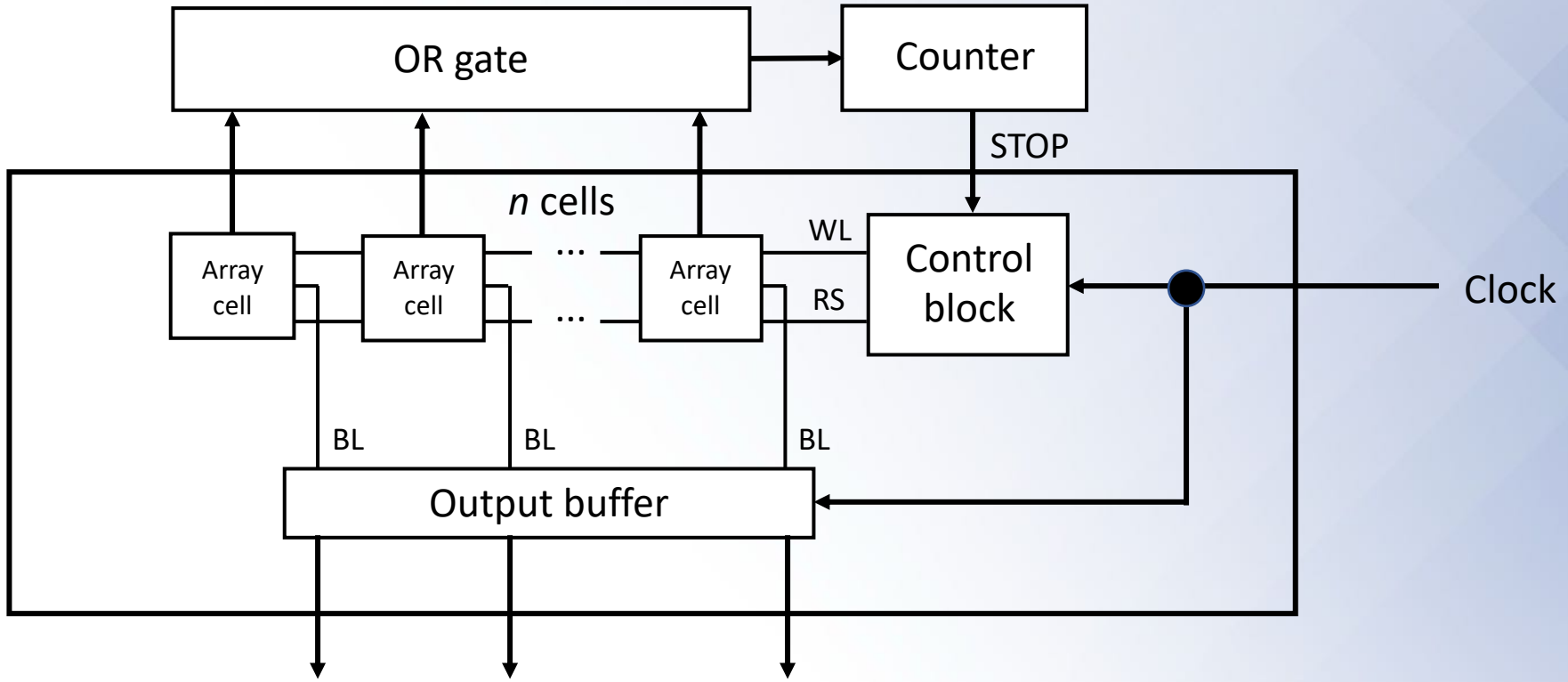
±1 std. dev

±2 std. dev

±3 std. dev

© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

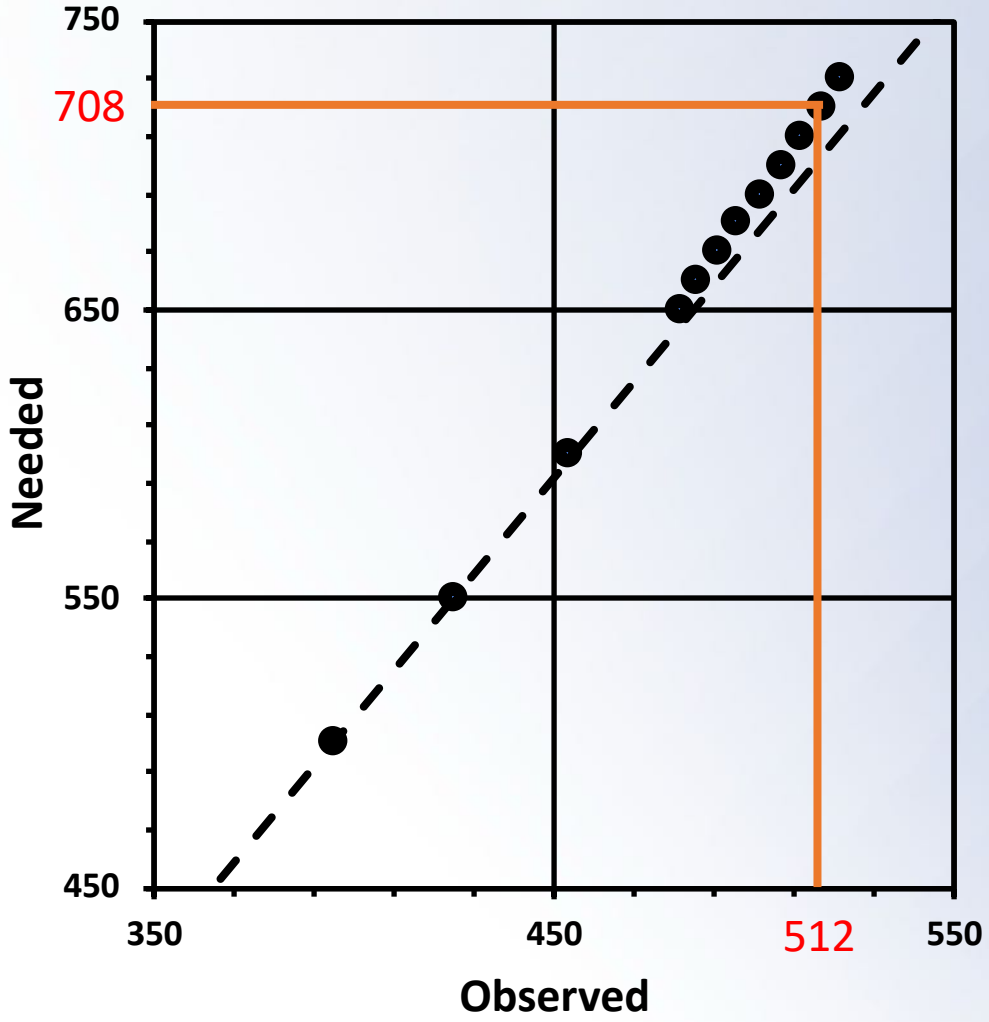
Array of simple detectors (a matrix)



WL: word line
RS: reset line
BL: bit line

Simulation of filling ½ of 1024 detectors

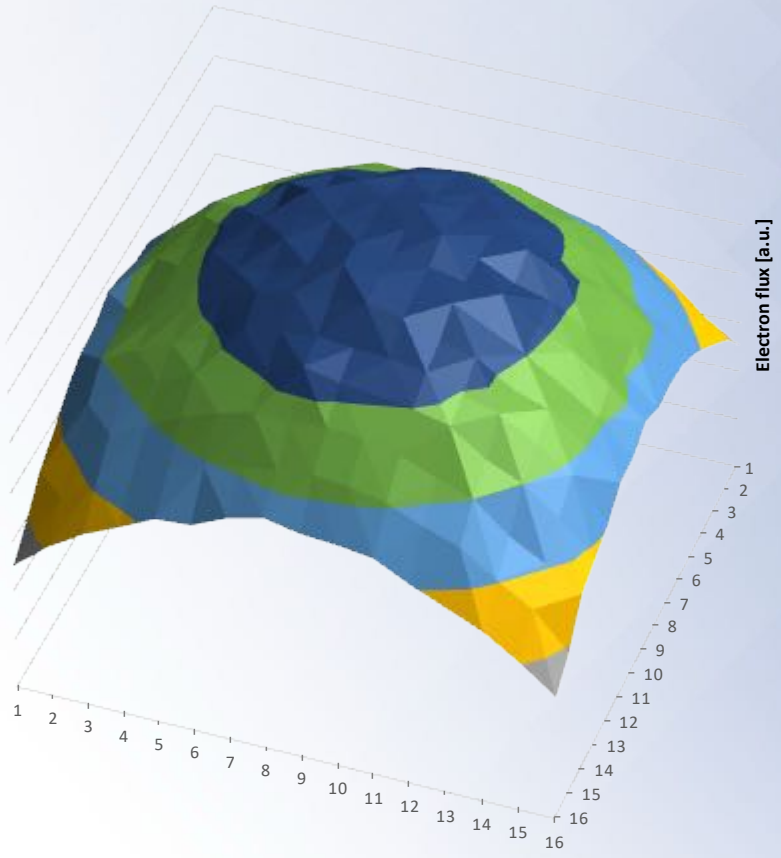
Rain falling or dropping of sand particles on a chess checkerboard ☞ random positions. 708 particles are needed to fill 512 fields with at least one particle.



© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

Large matrix of detectors

N = 256 (matrix 16 x 16)
a = 2 mm (distance between source and detectors)
b = 1.6 mm (side of the square matrix)
c = 1 mm (overhang of the source over matrix)
d = 0.1 mm (single detector diameter)

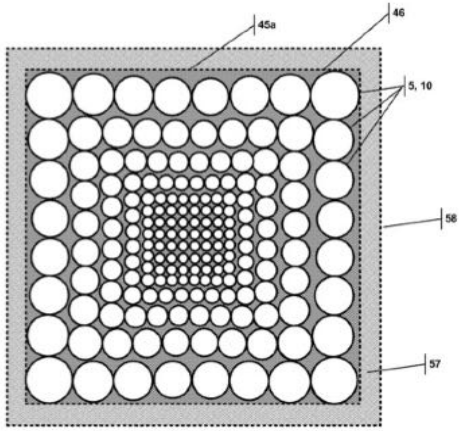


Monte Carlo simulation involved generation of $8 \cdot 10^9$ electrons*
☞ only 1.4 % reached the matrix

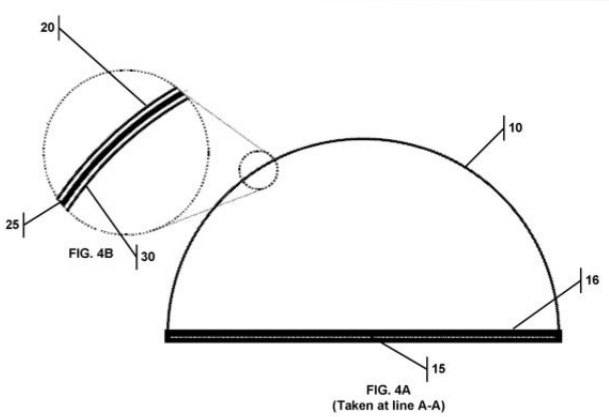
* *VB function Rnd() has a period of about $2 \cdot 10^7$ numbers; we used RndM() based on Wichmann-Hill algorithm with a cycle of about $7 \cdot 10^{12}$ different numbers possible*

Entropy extraction from matrices of detectors

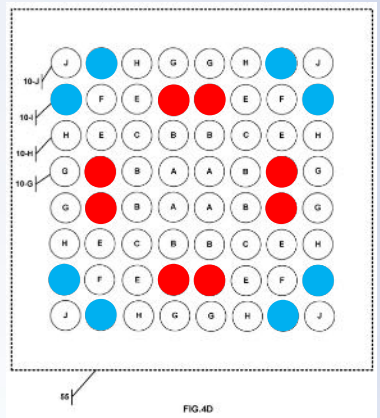
- Separation of the source and a matrix
  - uneven illumination of the center and edges
- Several proposed solutions:



US patent 11,281,432



US patent 11,614,921



US patent 11,567,734

Novel steganographical cryptography*

- The stream of bits from RANDAEMON PoC is truly random
  - no statistical correlations between bits
- RANDAEMON invented the method** called **B**ury **A**mong **R**andom **N**umbers (BARN):
  - every bit of the message is inserted somewhere among random bits using a secret, one-time-key
- Attacking the BARN cipher is similar to finding a needle in a haystack:
  - a vast number of combinations (for a simple key there are more than 2^{150} possibilities) and no clues whatsoever about which bits could contain the message
  - the method is computationally friendly, easy to implement in IoTs, and tough to break
  - it has been extensively tested

* *stegano* (Greek) concealed, covered https://en.wikipedia.org/wiki/Steganography; *crypto* (Greek) hidden, secret https://en.wikipedia.org/wiki/Cryptography

**Tatarkiewicz J.J. et al. 2023 USPTO application 18,201,000 *Method and apparatus for steganographical cipher encryption using true random number generator*

BARN algorithm

bit# →

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	...
0	0	0	1	1	0	1	0	0	0	0	0	1	0	1	1	1	0	1	0	0	...

bits → ☚ stream of random bits

bit# →

1	2	3	4	5	6	7	8	9	10
1	1	1	0	0	0	1	1	0	1

bits → ☚ message

bit# →

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	0	0	**1**	1	**1**	**0**	**0**	0	0	**0**	0	**1**	**1**	**0**	1	1	**1**	1
1			*3*		*2*	*1*	*1*			*3*		*2*	*1*	*1*			*3*	

bits → ☚ message embedded into the random bit stream, key {1, 3, 2, 1}

shift →

bit# →

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	**0**	**0**	1	**1**	**1**	0	**0**	**0**	0	**0**	**0**	1	**1**	**0**	1	**1**	**1**	1
	2	*1*		*2*	*1*		*2*	*1*		*2*	*1*		*2*	*1*		*2*	*1*	

bits → ☚ failed attempt to decode a message, key {2, 1, 2, 1}

shift →

© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

Deliverables to be designed & manufactured

Short series of IC devices for IoT, FIDO, servers, quantum networks, etc.

- low-efficiency QRNGs for simple applications (about 15 kbit/second)
- high throughput QRNGs for servers and quantum networks

  (up to 0.25 Gbit/sec from 1 cm^2 of the chip)
- specialized communications chip for secure data transfer utilizing QRNG and BARN cryptographic approach

- Designed in Poland by experienced chip designers
- Manufactured in the EU by the international fab
- Timeframe – 2 years after closing financing

RANDAEMON portfolio of patents

- **Issued**
  - Tatarkiewicz J.J. 2019 US Patent 10,430,161 *Apparatus, systems, and methods comprising tritium random number generator*
  - Tatarkiewicz J.J. et al. 2021 US patent 10,901,695 *Apparatus, systems, and methods for beta decay based true random number generator*
  - Tatarkiewicz J.J. et al. 2021 US patent 11,036,473 *Apparatus, systems, and methods for beta decay based true random number generator*
  - Tatarkiewicz J.J. et al. 2021 US patent 11,048,478 *Method and apparatus for tritium-based true random number generator*
  - Tatarkiewicz J.J. et al. 2021 Korean patent 10-2289084 베타 붕괴 기반의 진성 난수 생성기를 위한 장치, 시스템, 및 방법
  - Kuzmicz W.B. et al. 2022 US patent 11,249,725 *Method and apparatus for highly effective beta decay based on-chip true random number generator*
  - Tatarkiewicz J.J. 2022 US patent 11,281,432 *Method and apparatus for true random number generator based on nuclear radiation*
  - Tatarkiewicz J.J. 2022 EU patent 3,776,179 *Apparatus, systems, and methods comprising tritium random number generator*
  - Kuzmicz W.B. et al. Korean patent 10-2429142 베타 붕괴를 이용한 고도로 효과적인 온칩 진성 난수 생성기를 위한 방법 및 장치
  - Tatarkiewicz J.J. et al. 2022 AU patent 2022200920 *Method and apparatus for highly effective on-chip true random number generator utilizing beta decay*
  - Tatarkiewicz J.J 2023 US patent 11,567,734 *Method and apparatus for highly effective on-chip quantum random number generator*
  - Borodzinski J.J. et al. 2023 US patent 11,586,421 *Method for cost-effective Nickel-63 radiation source for true random number generators*
  - Tatarkiewicz J.J. et al. 2023 US patent 11,614,921 *Method and apparatus for highly effective on-chip quantum random number generator using beta decay*
- **Pending**
  - Kuzmicz W.B. et al. 2023 USPTO application 18,201,000 *Method and apparatus for implementing on-chip quantum random number generator using beta decay*
  - Tatarkiewicz J.J. et al. 2023 USPTO application 18,113,368 *Method and apparatus for steganographic cipher encryption using true random number generator*
  - Several of the above-issued US patents were applied for in EU, Canada, Australia, and Korea

© RANDAEMON Ltd. Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

Thank you for your attention

Ksawerów 21
02-656 Warsaw, Poland
office@randaemon.com