

**RAN
DAE
MON**

Entropy is good

**Better Cybersecurity
Through Quantum
Random Number
Generators**

Tomorrow's technology today

- **Quantum Computers Will Break the Internet, but Only If We Let Them**

<https://www.rand.org>
<https://media.nature.com>

- **The Future of Cybersecurity are the Quantum Random Number Generators (QRNGs)**

<https://spectrum.ieee.org>


- Truly random numbers (delivered in billions of binary digits) provide an unbreakable toolset for cryptography
- QRNGs are essential for providing quantum-unbreakable encryption:
 - for internet banking
 - for health-care privacy
 - for internet shopping
 - for internet devices
- QRNGs are crucial for blockchain security ([cryptographic nonce](#))



Many hardware options are available, but...

Several methods or devices are offered, e.g.,

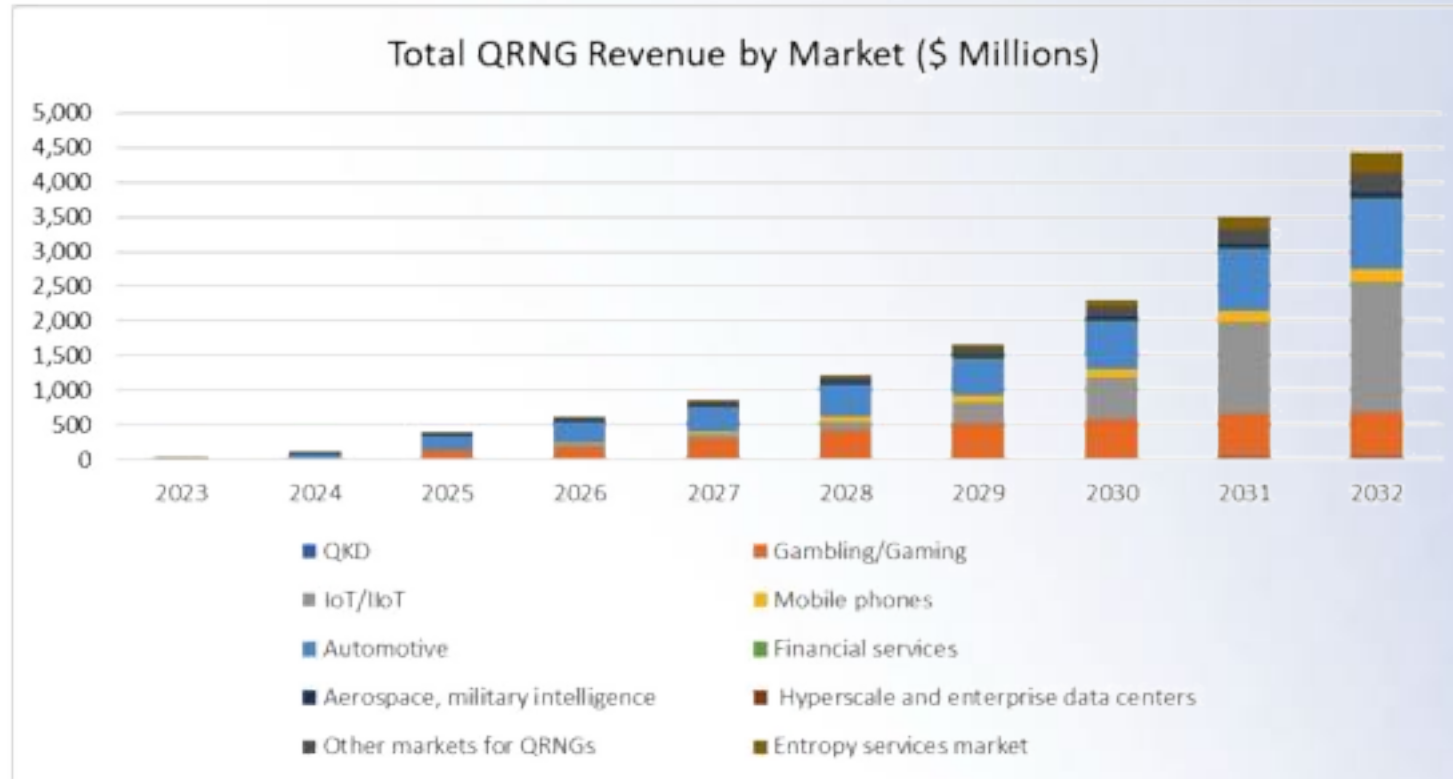
- Cloud RNG <https://www.random.org> based on atmospheric noise
- HotBits <https://www.fourmilab.ch> based on Geiger counter
- Protego ST <https://www.proteghost.com> noise-based key fobs or chips
- ComScire <https://comscire.com> tunneling leakage in MOS transistors
- qStream <https://www.quintessencelabs.com> based on quantum tunneling
- Quantis <https://www.idquantique.com> based on quantum optical randomness
- QN100 <https://quside.com> based on quantum optical randomness

Most are not easily incorporated into consumer devices
The suitable devices (*qStream*, *Quantis*, *QN100*) are not pure quantum as claimed: their entropy sources are prone to external influences like temperature or voltage changes  *breakable**

* cf. e.g., Abbott A.A. et al. 2014 *Non-uniformity in the Quantis Random Number Generator*, Centre for Discrete Mathematics and Theoretical Computer Science CDMTCS-472 November 2014 or Hurley-Smith D. and Hernandez-Castro J. 2020 *Quantum Leap and Crash: Searching and Finding Bias in Quantum Random Number Generators*. Security, 23 (3). pp. 1-25. ISSN 2471-2566.



Projected market size for QRNGs



[IQT Research's report](#) "Quantum Random Number Generators: Market and Technology Assessment 2023-2032"



Our mission

- **RANDAEMON** builds Quantum Random Number Generators:
 - hardware-based, on an integrated circuit (IC)
 - integrated into SoC
 - fabricated using standard chip manufacturing technology
- **RANDAEMON** uses the **ultimate** entropy source:
 - protected by multiple issued US patents
 - pure beta decay inside nuclei
 - PIN or SPAD detectors
- **RANDAEMON** aims at high throughput for random bitstream



Why nuclear beta decay?

- The pure quantum process inside nuclei
- Decays are random in time (*ticking*) and in space (*direction*)
- Beta radiation (*electrons*) is easily detectable
- The emission of electrons is not affected by normal conditions:
 - *acceleration*
 - *pressure*
 - *temperature*
 - *magnetic and electric fields*
 - *etc. etc.*

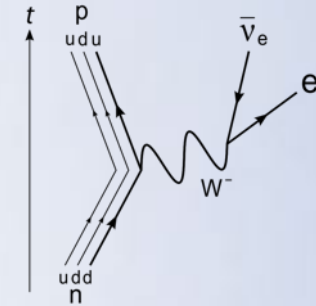
The use of beta decay is perfectly suited for local, *in-situ* QRNGs



Safe entropy source

^{63}Ni as a source of randomness:

- pure beta decay: $^{63}\text{Ni}_{28} \rightarrow ^{63}\text{Cu}_{29} + e^{-} + \bar{\nu}_e$
 - maximum electron energy 67 keV
 - average electron energy 17 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 eyes or in guts is $> 100 \mu\text{m}$ thick
 - in the tissue about 68 μm ☞ epidermis (dead part of the skin) is typically $> 100 \mu\text{m}$ thick
 - in the metallic Cu about 13 μm ☞ no radiation at all outside of the IC enclosure
- activity per simple device $\leq 3 \cdot 10^{-5}$ Ci
 - if fully digested (?), the dose absorbed 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 solutions

- **Patented QRNGs designs:**
 - set of detectors
 - a small number (starting with 1 detector) for simple applications
 - a large number (up to 1 million detectors) for demanding applications*
 - easily scalable for any application
 - standard manufacturing technology
 - **Chip for secure communications** (*patent pending for novel stream cipher method using QRNG*)

***Quantum networks need huge amounts of random bits for operation**

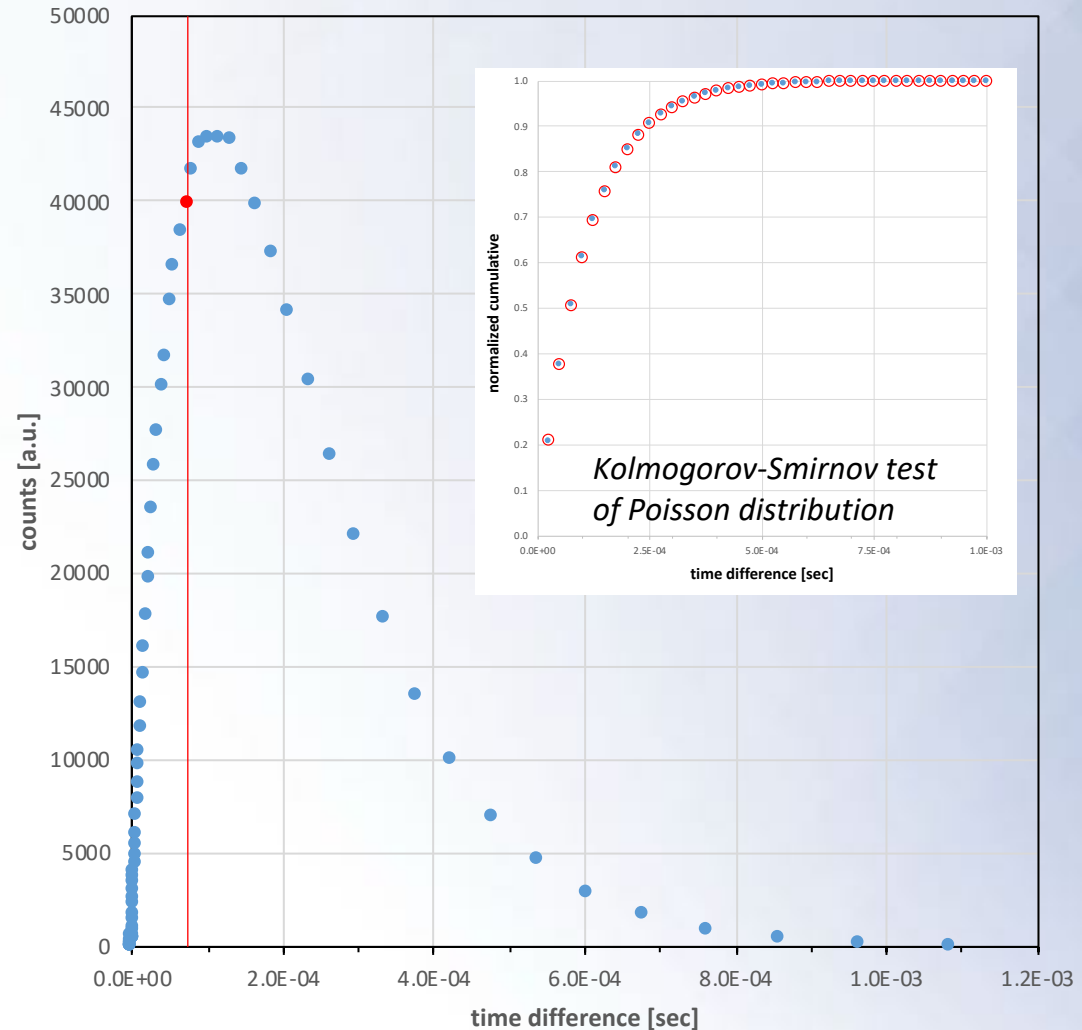
<https://www.zdnet.com>

<https://www.energy.gov>



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 its perfect randomness



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
```

RAN
DAE
MON

Novel steganographical cryptography*

- The stream of bits from RANDAEMON PoC is truly random
 - this means that there are no statistical correlations between bits
- The method of encryption is called **Bury Among Random Numbers (BARN)**
 - every bit of the message is inserted somewhere among random bits using some (secret) key
 - technically this is called *symmetrical stream cipher* because a stream of bits is inserted into a random stream of bits and there is one secret key
- Attacking the BARN cipher is similar to finding a needle in a haystack
 - a huge number of combinations (typically for a simple key $>2^{100}$) and no clues about which bits could contain the message → the method is very hard to crack but is very simple to be implemented in IoTs

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 provisional application 63,441,979 *Method and apparatus for steganographical stream cipher encryption using true random number generator*



Investment and deliverables

- **Investment in resources and financial support needed**
- **RANDAEMON delivers:**
 - Limited series of IC devices for IoTs, servers, and quantum networks:
 - low-efficiency QRNGs for simple applications (15 kbit/second)
 - high throughput QRNGs for servers and quantum networks (up to 0.25 Gbit/sec from 1 cm² of the chip)
 - specialized communications chip for secure data transfer utilizing QRNG and novel cryptographic approach (patent pending)
- Designed in Poland by experienced chip designers
- Manufactured in Germany by the international fab



Business plan (abbreviated)

- **Manufacturing test chips**
- **Testing with potential customers**
- **Licensing of technologies**
 - Three groups of PoCs:
 - Low-efficiency QRNG for IoT applications
 - High throughput QRNG for servers and quantum networks
 - Communications chip for secure data transfer via USB key
- **Shareholders will financially benefit from license royalties**
- **Eventually, licensing will lead to the sale of the Company**



RANDAEMON team

CEO:
Janusz Borodziński

- Ph.D. in electro-chemistry, Warsaw University
- 1987-1988 University College, Cork, Ireland – research associate
- 1991-1993 Université de Sherbrooke, Canada – visiting professor
- Technical director of Apple IMC Poland 1994-2012
- Experienced entrepreneur, consultant, teacher

CFO:
Krzysztof Appelt

- Ph.D. in biophysics, Max Planck Institute, West Berlin
- 1984 – 1985 Assistant Professor UCSD, Dept. of Physics and Chemistry
- 1986 – 2004 R&D executive positions in the pharma and biotech industry
- 2005 – 2015 Founder, CEO & President of Great Lakes Pharmaceuticals, Inc.
- 2018 – 2020 Founder and CEO of Visthera, Inc.
- 2015 – now Director, Airspeed Equity

CTO:
Jan „Kuba” Tatarkiewicz

- Ph.D., D.Sc. in nuclear methods in solid-state physics, Warsaw University
- Physicist (post-doc at MPI FKF Stuttgart), programmer (Monte Carlo code in ORNL library, localization of Mac OS for Poland), IT director (MIT Lab for Nuclear Science, UCSD)
- Author of 50+ papers published in refereed journals
- Several invited lectures at international conferences
- 20+ patents issued
- The entrepreneur started 10 companies; recently MANTA Instruments sold to HORIBA Scientific

Technical advisor:
Wiesław Kuźmicz

- Ph.D., D.Sc. in solid-state electronics, Warsaw University of Technology
- Since 1970 worked at Warsaw University of Technology
- From 1984 to 1985 and in 1989 visiting professor at Carnegie Mellon University
- Professor emeritus, Warsaw University of Technology
- Research interests include the physics of semiconductor devices, development of simulation and EDA tools, and design of VLSI circuits for demanding nontrivial applications
- Author of over 100 research papers and two textbooks



RANDAEMON cooperation

PCI Express card / USB

- Łukasiewicz Research Network – Institute of Microelectronics and Photonics
- Research Group of Integrated Circuits and System Design
- Grzegorz Janczyk Ph.D. Research Group Leader
- <https://imif.lukasiewicz.gov.pl>

Chip design

- ChipCraft LLC
- Poland-based fabless semiconductor private company
- Spin-off from Warsaw University of Technology
- Krzysztof Siwiec Ph.D. lead designer, vast experience with digital security
- <http://www.chipcraft-ic.com>

Fab

- X-FAB Silicon Foundries
- German company that does prototyping in suitable technologies
- <https://www.xfab.com>

⁶³Nickel

- Institute of Nuclear Chemistry and Technology
- Aleksander Bilewicz Ph.D., D.Sc. head of the Laboratory of Chemistry of Radioelements
- <http://www.ichtj.waw.pl>



RANDAEMON's portfolio of patents

1. Tatarkiewicz J.J. 2019 US Patent 10,430,161 *Apparatus, systems, and methods comprising tritium random number generator*
2. Tatarkiewicz J.J. et al. 2021 US patent 10,901,695 *Apparatus, systems, and methods for beta decay based true random number generator*
3. Tatarkiewicz J.J. et al. 2021 US patent 11,036,473 *Apparatus, systems, and methods for beta decay based true random number generator*
4. Tatarkiewicz J.J. et al. 2021 US patent 11,048,478 *Method and apparatus for tritium-based true random number generator*
5. [Tatarkiewicz J.J. et al. 2021 Korean patent 10-2289084](#) 베타 붕괴 기반의 진성 난수 생성기를 위한 장치, 시스템, 및 방법
6. 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*
7. Tatarkiewicz J.J. 2022 US patent 11,281,432 *Method and apparatus for true random number generator based on nuclear radiation*
8. [Tatarkiewicz J.J. 2022 EU patent 3,776,179](#) *Apparatus, systems, and methods comprising tritium random number generator*
9. [Kuzmicz W.B. et al. Korean patent 10-2429142](#) 베타 붕괴를 이용한 고도로 효과적인 온칩 진성 난수 생성기를 위한 방법 및 장치
10. [Tatarkiewicz J.J. et al. 2022 AU patent 2022200920](#) *Method and apparatus for highly effective on-chip true random number generator utilizing beta decay*
11. Tatarkiewicz J.J. 2023 US patent 11,567,734 *Method and apparatus for highly effective on-chip quantum random number generator*
12. Borodzinski J.J. et al. 2023 US patent 11,586,421 *Method for cost-effective Nickel-63 radiation source for true random number generators*
13. 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*
14. Kuzmicz W.B. et al. 2024 US patent granted, to be published *Method and apparatus for implementing on-chip quantum random number generator using beta decay*
15. Tatarkiewicz J.J. et al. 2024 US patent granted, to be published *Method and apparatus for steganographic cipher encryption using true random number generator*



Thank you for your attention

RANDAEMON

Ksawerów 21

02-656 Warsaw, Poland

office@randaemon.com