

**RAN
DAE
MON**

Entropy is good

**Patented
Quantum
Random
Number
Generator**

The essence of good cryptography

- Three ingredients are required to make hackproof encryption:
 1. a way to produce random numbers - the unique keys to convert a message
 2. an algorithm that converts the message into a string of meaningless characters
 3. a channel to securely deliver the first ingredient to the intended recipient without anyone else gaining insight

The second and third components are well established and widely used by cryptographers, programmers etc.



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](#))



Locality for privacy and secrecy

- To ensure the privacy of any communication, cryptography must be local (e.g., use of the so-called Perfect Forward Secrecy)

<https://www.keycdn.com>

- Cryptographic keys should use a true random number generator *in-situ* (i.e., on the user device)
- Good random number generators must be built into communicating devices (like computers and cell phones)
- The cybersecurity design: QRNGs embedded into a System-on-Chip (SoC)


Technology must be compatible with standard IC manufacturing



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.



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 ultimate entropy source:
 - pure beta decay inside nuclei
 - PIN or SPAD detectors
 - auto-correction and randomization *in situ*
- **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.*

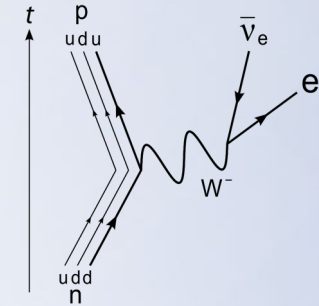
The use of beta decay is perfectly suited for local, *in-situ* QRNGs



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 7.3 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 14 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 0.75 mSv/year
 - [US natural background](#) is about 3 mSv/year; [Annual Limit on Intake](#) is 0.5 Sv

No radiation risk during manufacturing and for customers at all

Two related solutions

- **RANDAEMON** patented QRNGs designs:
 - set of detectors
 - a small number (starting with 1 detector) for simple applications
 - a large number (over 1 million detectors) for demanding applications*
 - easily scalable for any application
 - standard manufacturing technology ➡ up to 0.25 Gbit/(sec·cm²)

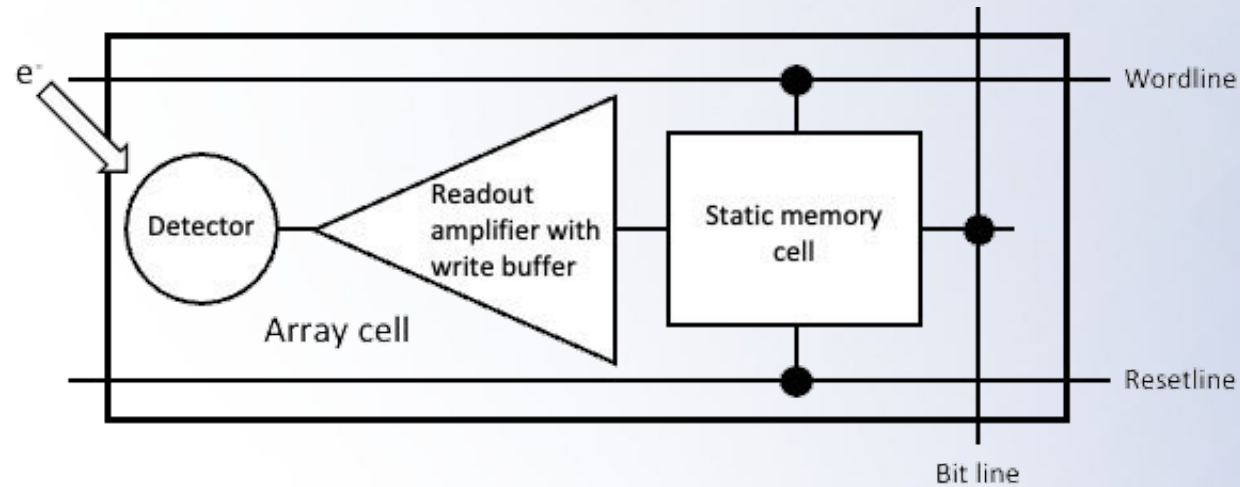
***Quantum networks need huge amounts of random bits for operation**

<https://www.zdnet.com>

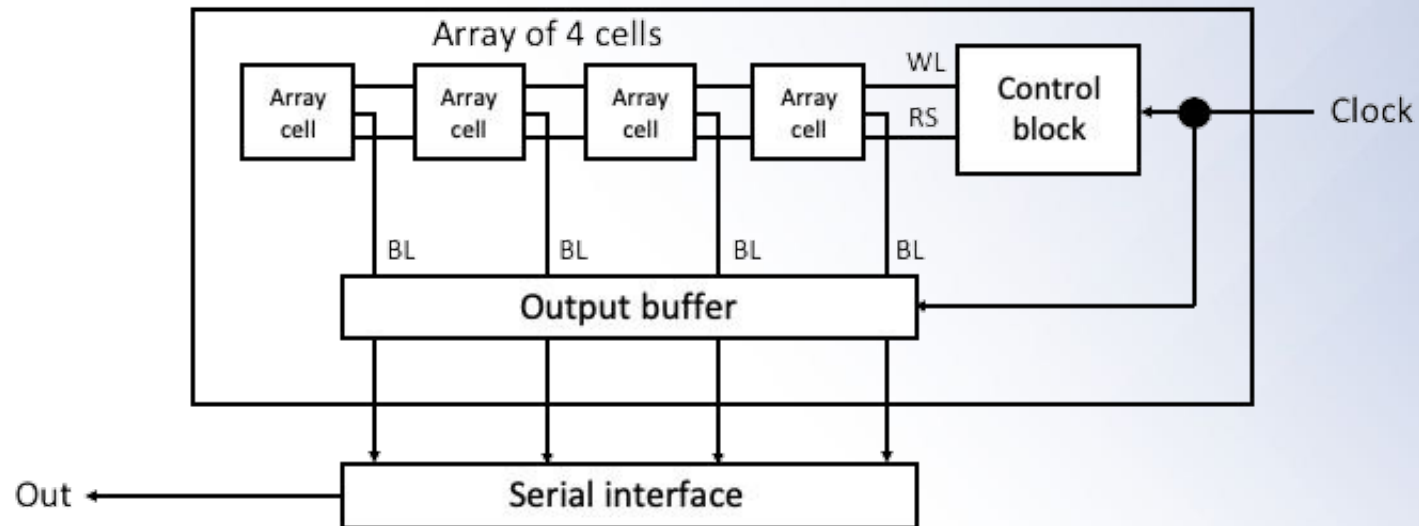
<https://www.energy.gov>



Structure of „small IC” test PoC design



To make testing easy, *NIST set of [statistical tests](#) can be built-in*



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, still employed at 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

- RnDity LLC
- Łódź-based private company
- Spin-off from Łódź University of Technology
- Bartek Świercz Ph.D. owner
- <https://rndity.com>

Chip design

- ChipCraft LLC
- Poland-based fabless semiconductor private company
- Spin-off from Warsaw University of Technology
- Tomasz Borejko 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 patents' portfolio

• 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**
- Kuźmicz 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*
- Kuźmicz 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 2022200920B1 *Method and apparatus for highly effective on-chip true random number generator utilizing beta decay*

• Pending

- Borodziński J.J. et al. 2021 USPTO application 17,687,630 *Method for cost-effective Nickel-63 radiation source for true random number generators*
- Tatarkiewicz J.J. et al. 2022 USPTO application 17,861,014 *Method and apparatus for highly effective on-chip quantum random number generator using beta decay*
- Tatarkiewicz J.J. 2022 USPTO application 17,897,138 *Method and apparatus for highly effective on-chip quantum random number generator*
- several of the above issued US patents were applied for in EU, Canada, Australia, and Korea



Thank you for your attention

RANDAEMON

Ksawerów 21

02-656 Warsaw, Poland

office@randaemon.com