Entropy is good

Better Cybersecurity Through Quantum Random Number Generators

What is RANDAEMON?

- Registered in Poland in October 2020 with offices in Warsaw and San Diego, USA
- Develops superior hardware and software technologies for cybersecurity
- In May 2021, the company received $0.5M seed money from Sunfish Partners VC *https://www.sunfish-partners.com*
- The company has 9 US patents issued, several pending, and also patents issued and pending in Korea, Australia, and the EU
- Two types of proof-of-concept (PoC) quantum random number generator (QRNG) devices were built and extensively tested
- A novel stream cipher method based on QRNG was developed and thoroughly tested in the software

Growing pains of cybersecurity today…

- **Mass deployment of IoT devices, especially smartphones:**
  - banking and internet shopping
  - blockchain security
  - health services
  - home automation
  - automotive industry
- **High network traffic leads to increased cybersecurity risks**
  - Algorithmic processing-based security is computationally costly and breakable
  - New technologies are needed (like *cryptographic nonce*)

Quantum computers are around the corner

…and they will bring more significant security problems:

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

  https://www.rand.org

  https://media.nature.com

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

  https://spectrum.ieee.org

QRNGs present new opportunities

- Truly random numbers are an unbreakable toolset for **today's needs**

  and

- for **post-quantum cryptography,** if delivered in billions of binary digits

"*Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.* ***There is no such thing as a random number – there are only methods to produce random numbers****, and a strict arithmetic procedure 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

Existing solutions are not satisfactory

- Cloud RNG https://www.random.org based on atmospheric noise
- HotBits https://www.fourmilab.ch based on Geiger counter
- Protego ST https://www.protegost.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

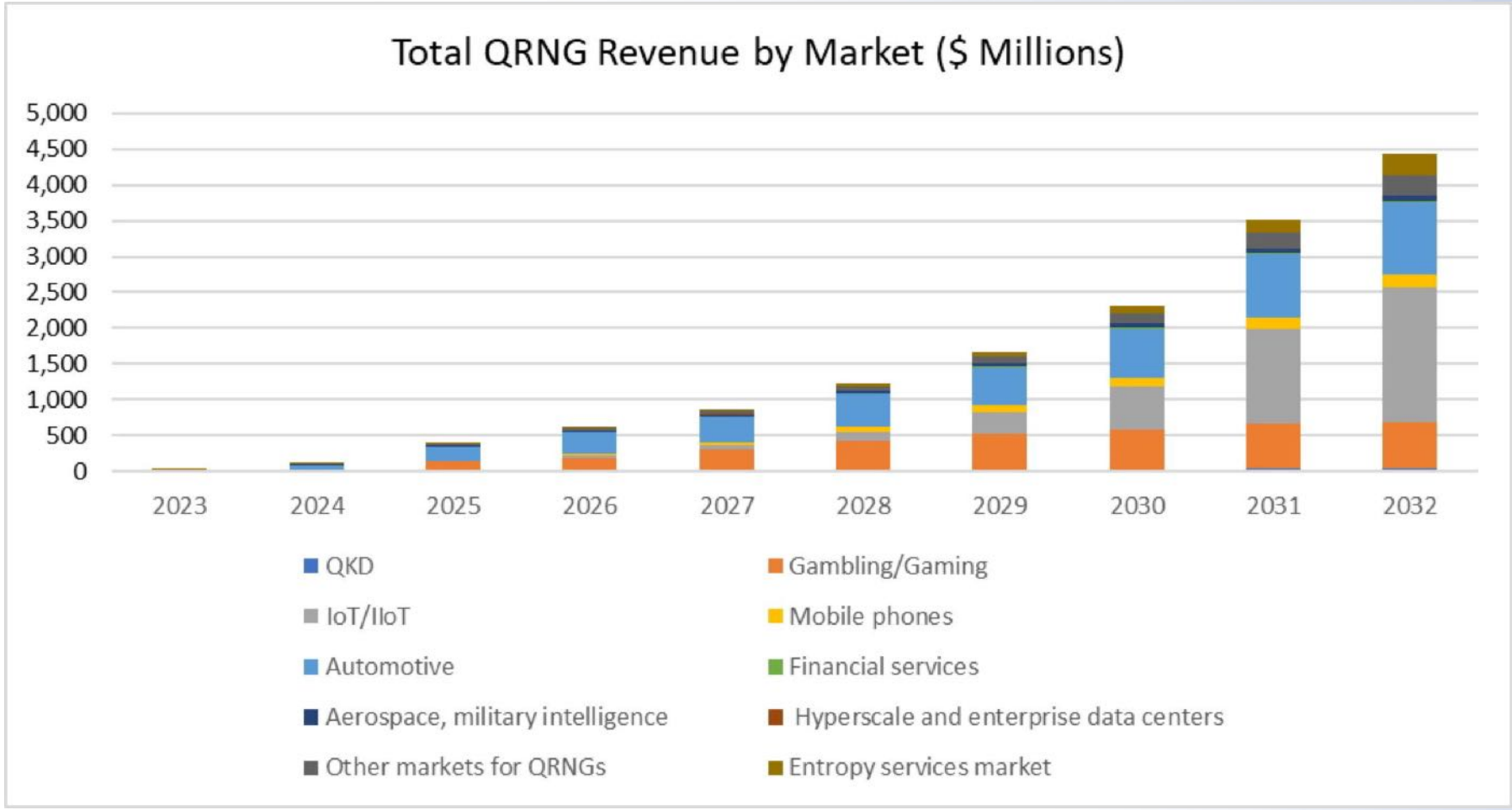
- **Engineering designs are complicated and expensive**
- **Most are not easily incorporated into consumer devices**
- **Suitable devices (*qStream*, *Quantis, QN100*) are not true quantum***
  - **external conditions influence their entropy sources**

☛ *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 is $5B in 10 years

All market segments listed below are relevant to RANDAEMON technology



IQT Research's report *"Quantum Random Number Generators: Market and Technology Assessment 2023-2032"*

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

Our mission

- **RANDAEMON** builds Quantum Random Number Generators:
  - hardware-based, on an integrated circuit
  - integrated into system-on-chip
  - fabricated using standard chip manufacturing technologies
- **RANDAEMON** uses the **ultimate** entropy source:
  - beta decay inside nuclei (conversion of neutron to proton)
  - protected by multiple issued US patents
  - PIN or SPAD diode detectors
- **RANDAEMON** aims at high throughput of perfect random bitstream

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

Why beta decay?

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

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

Pure beta decay - patented and safe entropy source

There are three common isotopes that decay by pure beta emission:

- Tritium (H^3) — possible for use in QRNGs but challenging
  - used in nuclear weapon systems, strictly controlled
  - as a gaseous substance it provides unnecessary challenges for QRNG engineering
- Carbon-14 — not really suitable for QRNGs
  - the half-life time is 5,733 years ☛ very rare decay events
- **Nickel-63 — the ultimate source of entropy for QRNGs**
  - **Low energy beta decay creates no radiation risk during manufacturing, for customers, and recycling**

The issued and pending US and international patents secure RANDAEMON exclusivity for the use of Tritium and Nickel-63 for QRNG technologies

RANDAEMON solutions

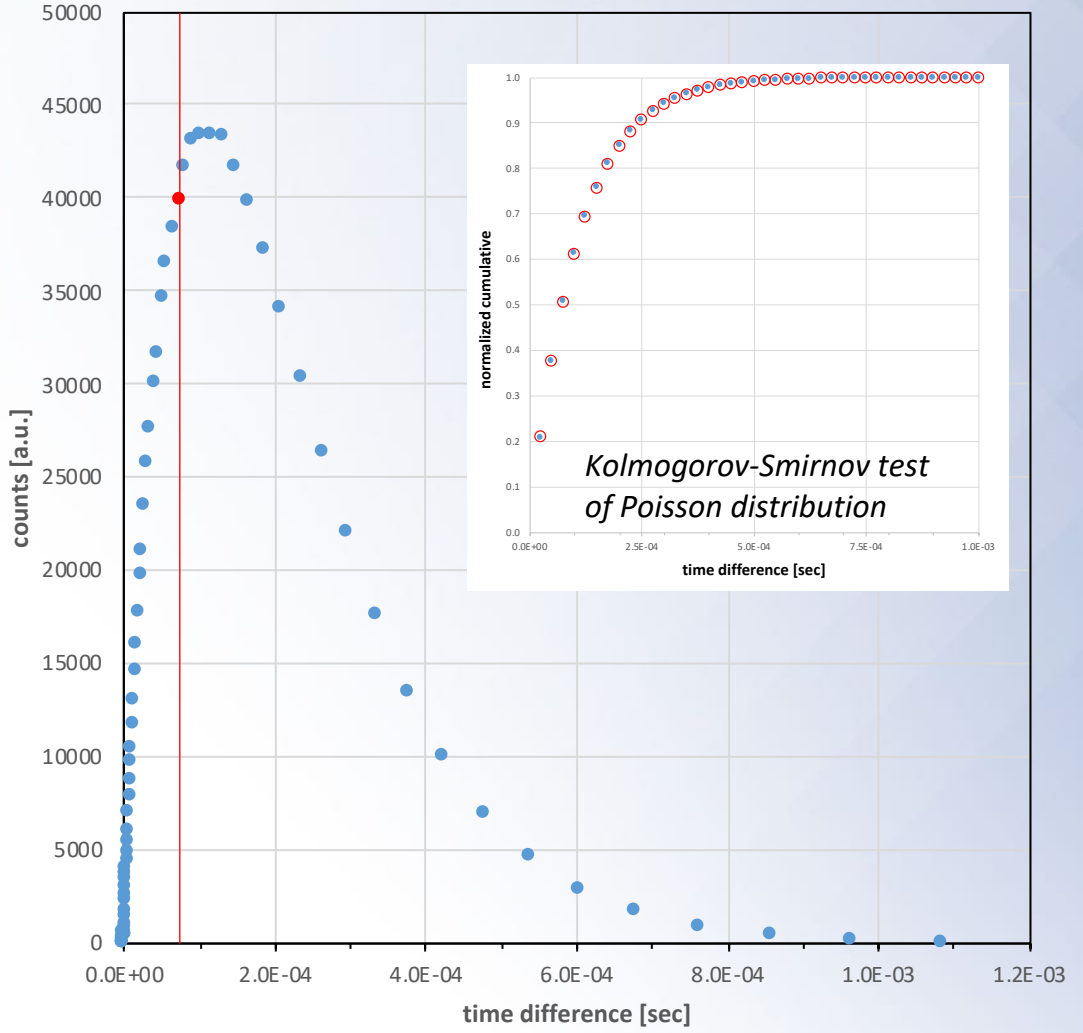
- **Patented QRNGs designs**:
  - set of detectors
    - a small number for simple applications like key fobs
    - a large number (up to 1 million detectors) for demanding applications*
  - easily scalable for any application (e.g. PCI cards for servers)
  - standard manufacturing technologies for integrated circuits
  - **Chip for secure communications** ***(patent pending for novel stream cipher method using QRNG)***

*Quantum networks need huge amounts of random bits for operation

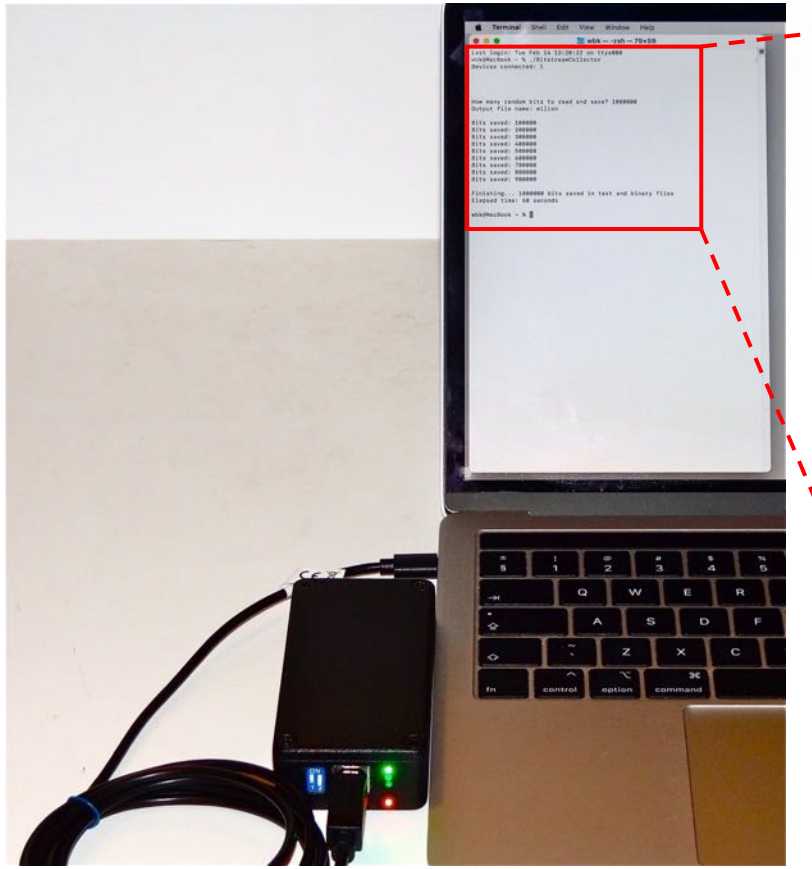
https://www.zdnet.com https://www.energy.gov

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 proves 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
```

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 > 2^{150} possibilities) and no clues 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 17,861,014 *Method and apparatus for steganographical stream cipher encryption using true random number generator*

Investment and deliverables

- **Investment needed $5M**
- **Deliverables:**
  - Short series of IC devices for IoTs, FIDO, servers, quantum networks, etc.
    - 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 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

Business plan (abbreviated)

- **Manufacturing test chips**
- **Testing with potential customers**
- **Licensing of technologies**
  - Three groups of PoCs:
    - Low-efficiency QRNG for IoTs 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
- 1994 – 2012 Technical director of Apple IMC Poland
- 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

- RnDity LLC
- Polish private software and hardware company
- Bartek Świercz Ph.D. owner
- *https://rndity.com*

Chip prototyping

- 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
- Polish fabless semiconductor private company
- Krzysztof Siwiec Ph.D. lead designer
- *http://www.chipcraft-ic.com*

Nickel-63

- 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*

Fab

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

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. 2022 USPTO provisional application 63,430,240 *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 stream cipher encryption using true random number generator*
  - Several of the above-issued US patents were applied for in EU, Canada, Australia, and Korea

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

Thank you for your attention

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