
*Entropy is good*

# Real Quantum Random Number Generator Based on Beta Decay

# The essence of good cryptography

Three components 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.**

# 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**

# 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*)

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

# 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)
- Real 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**

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

# What is a good RNG?

- Good entropy source
- Resistant to external influences
- Embeddable into any IoT or processor
- A suitable level of bits generated for various applications
- Ease of engineering and manufacturing using typical technologies
- Stable and robust for the lifetime of devices

# Many hardware options are available, but…

Several methods or devices are offered:

- 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
- IDquantique https://www.idquantique.com based on quantum optical randomness
- QN100 https://quside.com based on quantum optical randomness

**None are easily incorporated into consumer devices (IoT)**
**The possible devices (*qStream*, *IDquantique, QN100*) are not pure quantum as claimed: their entropy sources are prone to external influences like temperature, voltage changes, or magnetic field ☞ *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.

# RANDEAMON solution

- **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 *in situ*
- **RANDAEMON** also offers high throughput random bitstream solutions

# Why nuclear beta decay?

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

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

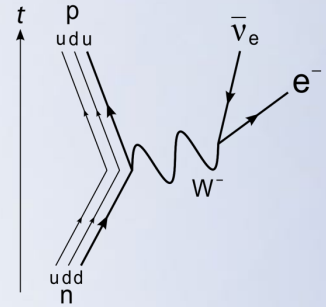
# $^{63}$Ni as an entropy source

- $^{63}$Ni easily produced:
  - $^{62}$Ni isotope is naturally abundant at 3.64%
  - $^{62}$Ni placed in a nuclear reactor converts into $^{63}$Ni by captured neutrons
  - full volume conversion takes about 2 years
- $^{63}$Ni has a half-life time of about 100 years
  - after one year electron flux decreases by about 0.7%
- Only a thin layer of $^{63}$Ni is active
  - the self-absorption of electrons in thick layers
  - max activity of $^{63}$Ni source is about 15 mCi/cm$^2$ (about 550*10$^6$ decays/sec/cm$^2$)
- Controllable deposition of $^{63}$Ni by electroplating (patent pending)
  - IC cover contains the radioactive material (on the inside surface)

# 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
  - 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* µm thick
  - in the tissue about 68 µm ☞ epidermis (dead part of the skin) is typically *>100* µm thick
  - in the metallic Cu about 14 µm ☞ no radiation at all outside of the IC enclosure
- activity per simple device ≤ $3 \cdot 10^{-5}$ 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 line of products

**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·cm$^2$)

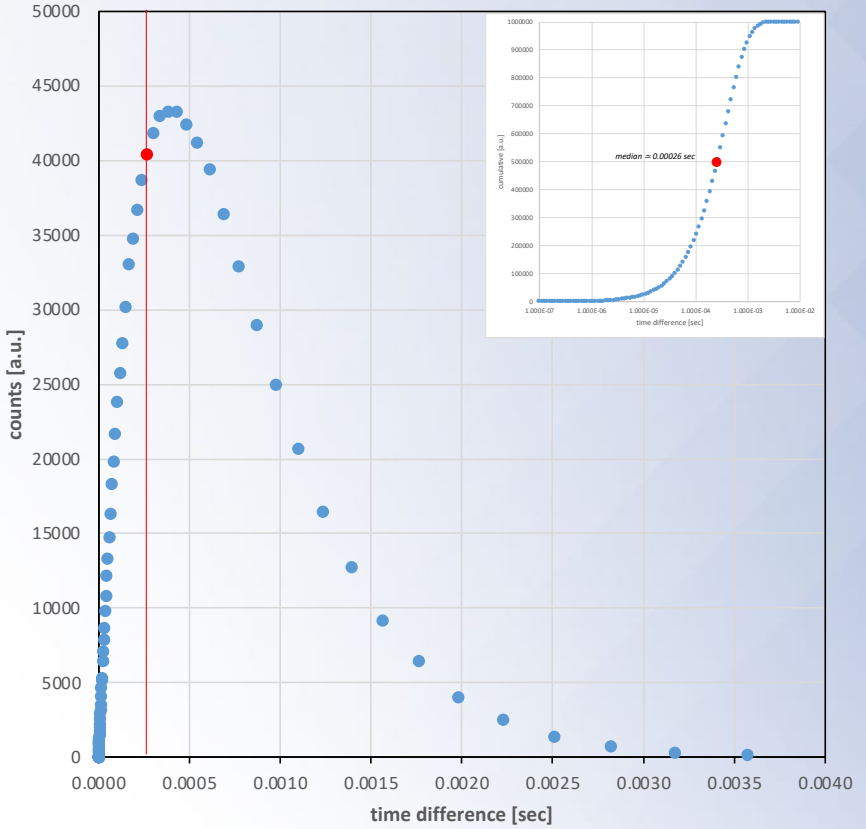
***Quantum networks need huge amounts of random bits for operation**

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

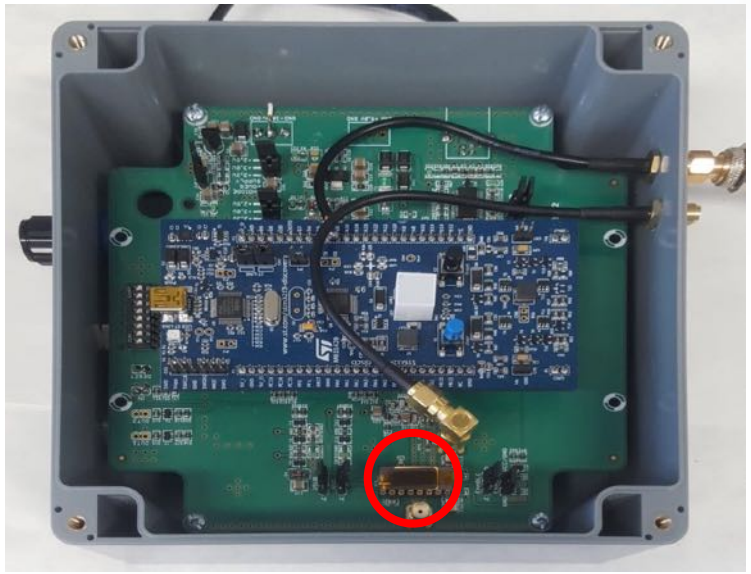
 Ksawerów 21 • 02-656 Warsaw • Poland • office@randaemon.com

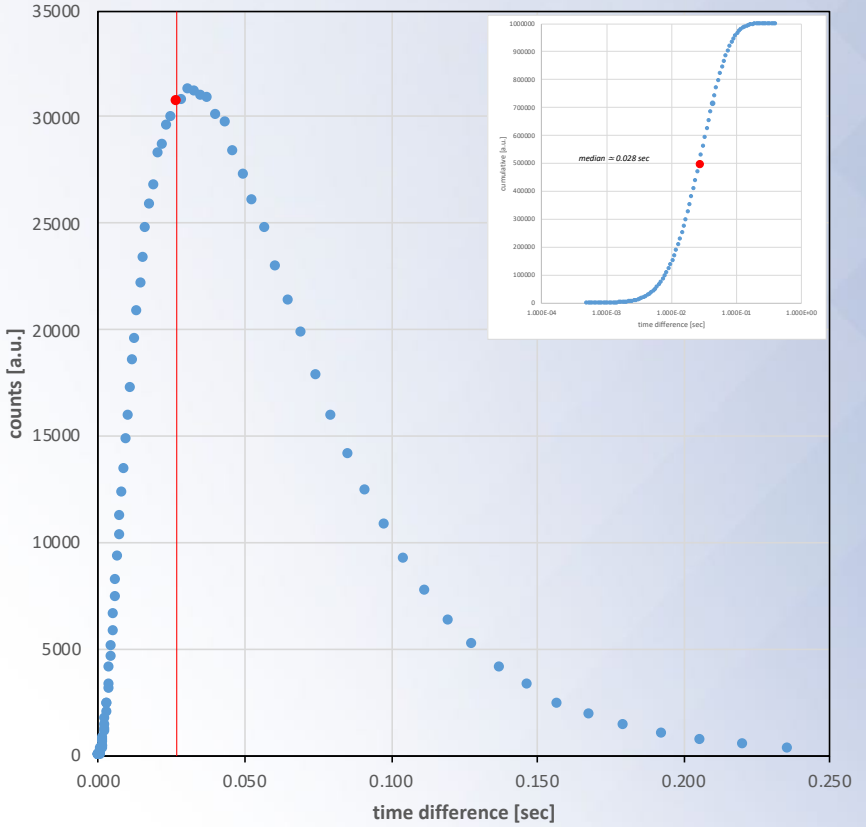
# RANDAEMON PoC #1 based on PIN diode

built at IMiF



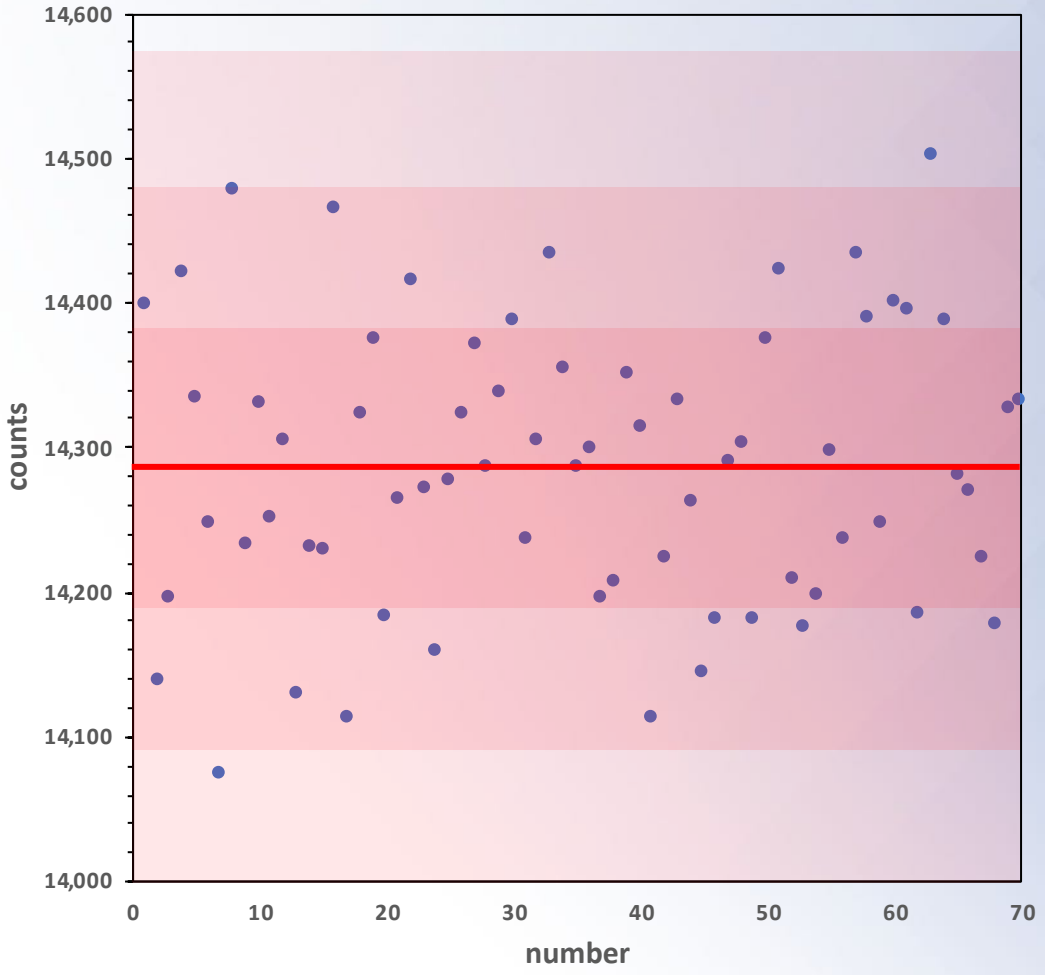
# RANDAEMON PoC #2 based on SPAD diode





# Testing

- Both PoCs 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 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

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

# Thank you for your attention


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