RAN
DAE
MON

Entropy is good

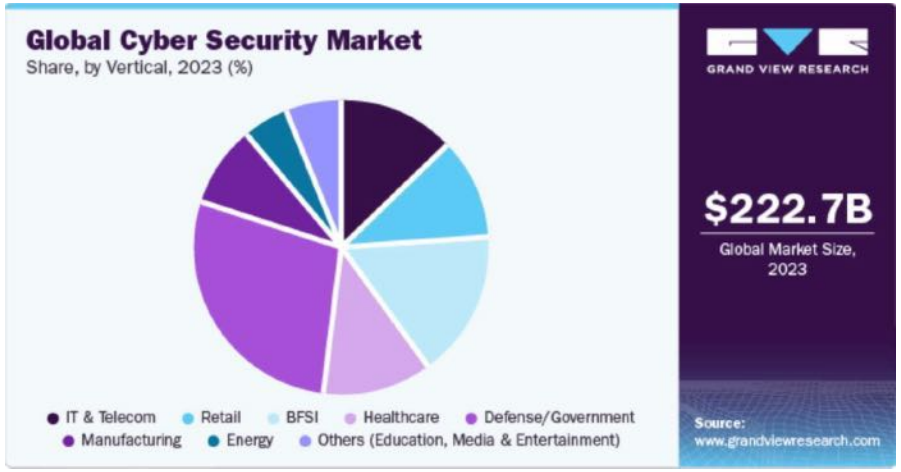
Innovative Quantum-Resistant Cryptography

Who We Are

- Polish deep tech company established by four founders with exceptional records, achievements, and excellence in technology, science, and entrepreneurial history https://www.randaemon.com
- RANDAEMON's mission is to develop superior hardware and software for entropy-based novel quantum-resistant cryptography
- In May 2021, the company received €1M seed money from Sunfish Partners https://www.sunfish-partners.com
- The company has 9 US patents issued and several pending:
  - All US patents have been submitted in the EU (PCT); one is issued, and the other pending
  - Patents issued and pending in Korea, Australia, Canada
- Two types of proof-of-concept (PoC) true Quantum Random Number Generator (tQRNG) devices were built and analysed by independent experts
- A novel type of encryption algorithm called BARN was developed and extensively tested using PoC QRNGs

Cryptography Is an Essential Part of Cybersecurity

- 2023 global cybersecurity market was valued at $222,7B and it is projected to grow at an annual growth rate of 12,3% https://www.grandviewresearch.com/industry-analysis/cyber-security-market



- Daily reports of successful hacking attacks and loss of critical confidential data call for changes and novel approaches to improve current inadequate cybersecurity

Today’s Cryptography Is Imperfect

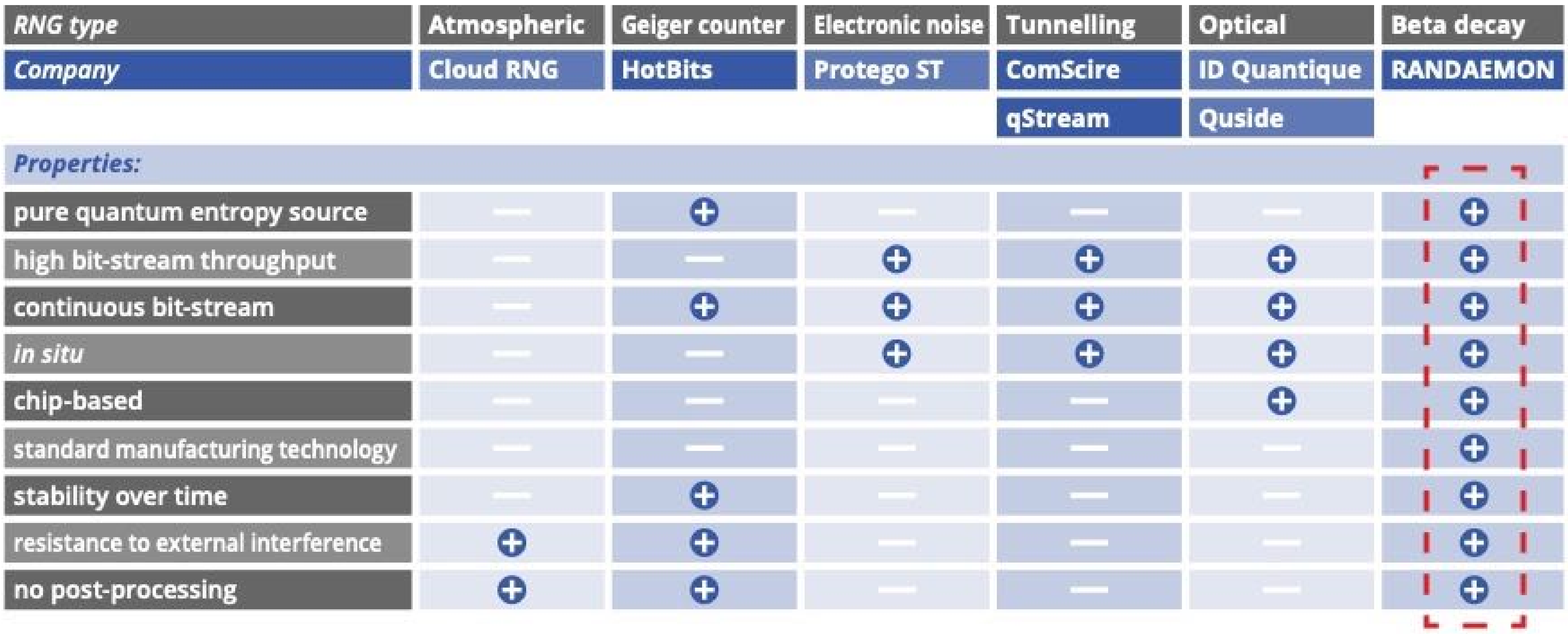
- All common encryption methods, like RSA and AES, use numerical algorithms for both encoding and decoding
  - Inverse functions and quantum algorithms, augmented by AI, are already impacting the safety of existing encryption
  - Some versions with shorter keys had been cracked already
  - Longer keys are now being required in anticipation of quantum computing to facilitate future security; in anticipation of new tools, hackers’ model is “*steal now, decrypt later*”
- On top of the safety issues, RSA and AES ciphers have additional substantial problems
  - The use of numerical algorithms requires high computing power for encryption
  - Longer keys are already used and further increase computing needs
  - High computing needs prevent their use in devices such as IoTs and hand-held devices, cloud computing, and encryptions of large volumes of digital data
  - RSA and AES are block ciphers, not suitable for encoding voice and video in streaming mode

RANDAEMON Has Disruptive, Innovative, and Efficient Solutions

- **B**ury **A**mong **R**andom **N**umbers (BARN) encryption software
  - Pure entropy-based cryptography using tQRNG as the source of random numbers
  - BARN is a method of random insertion of message's bits into the stream of truly random bits by using a randomly generated key
  - BARN is working with only minimal computing resources
  - BARN can be used either as a finite block cipher or stream cipher
  - BARN can be cracked only by the brute force search through all possible keys
    - 256-bit key creates $3{,}45 \cdot 10^{62}$ possible permutations

- **tQRNG** based on a quantum process of beta nuclear decay in nuclei of ^{63}Ni
  - Producing high-quality random numbers from 15 Kbits to ≥1 Gbits per second
  - Manufactured PoC was extensively tested by the recognized expert, Dr Hurley-Smith from London College
    - Statistical tests performed on billions of generated bits confirmed high quality and superiority to other supposedly QRNGs currently available
  - RANDAEMON's tQRNGs:
    - Easy to manufacture
    - Can be miniaturized
    - Embedded in chips and PCI/USB devices with BARN software

High-quality Random Numbers Are Essential for Cryptography



RNG type	Atmospheric	Geiger counter	Electronic noise	Tunnelling	Optical	Beta decay
Company	Cloud RNG	HotBits	Protego ST	ComScire qStream	ID Quantique Quside	RANDAEMON
Properties:						
pure quantum entropy source	—	⊕	—	—	—	⊕
high bit-stream throughput	—	—	⊕	⊕	⊕	⊕
continuous bit-stream	—	⊕	⊕	⊕	⊕	⊕
in situ	—	—	⊕	⊕	⊕	⊕
chip-based	—	—	—	—	⊕	⊕
standard manufacturing technology	—	—	—	—	—	⊕
stability over time	—	⊕	—	—	—	⊕
resistance to external interference	⊕	⊕	—	—	—	⊕
no post-processing	⊕	⊕	—	—	—	⊕

“Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin.”

J. von Neumann, Various techniques used in connection with random digits, 1951

Two Classes of Products for All Encryption Needs

- Products constitute integrated solutions:
  - BARN software
  - tQRNG as the source of a continuous stream of random bits
- Differentiation by how tQRNG is used:
  - Chip-based 15 Kbits per second
    - IoTs, IIoTs
    - Automotive industry
    - Data and voice encryption for hand-held devices
  - PCI/USB high-throughput devices ≥1 Gbits per second
    - Servers for cloud storage
    - Mass distribution of confidential information to individuals
    - Confidential video meetings and VOD streaming

- Future goals:
  - Continue testing BARN's Mac OS X and iOS versions
  - Development of Windows, Android, and Unix versions
  - Chip-based products
    - The initial design of masks and testing is completed
    - Manufacturing of prototypes requires 18 months, depending on the fabs' manufacturing cycles and corrections
  - PCI/USB high throughput devices
    - Development and manufacturing of prototypes require 12 months
  - Chips and devices will be developed concurrently

Markets and Clients

- Comparable products do not exist
- Increased criminal activity by organizations supported by rogue states is clearly evident
- Demand for modern cryptography is growing

- Markets:
  - Data security
  - Financial data and transactions
  - Healthcare, personal DNA data
  - Secure communications:
    - Law enforcement
    - Public aviation
    - Military
    - Home and vehicle safety

- Clients:
  - Governments
  - Military and Defence industry
  - Financial institutions
  - Stock exchange
  - Hospitals
  - Insurance companies
  - Automotive industry
  - Video streaming providers

Importance for the EU community

- Current encryption methods were developed and are maintained by the USA agencies NSA and NIST
- The methods are old and becoming inadequate for today’s needs and certainly not for post-quantum cryptography (PQC)
- Political uncertainty in the world is growing
- It is vitally essential for the EU to develop an independent, superior, and efficient encryption method to provide better cybersecurity for the EU and its citizens
- Shared with NATO partners, RANDAEMON’s products will enhance defence capabilities and strengthen the alliance
- RANDAEMON’s technology is based on EU resources only