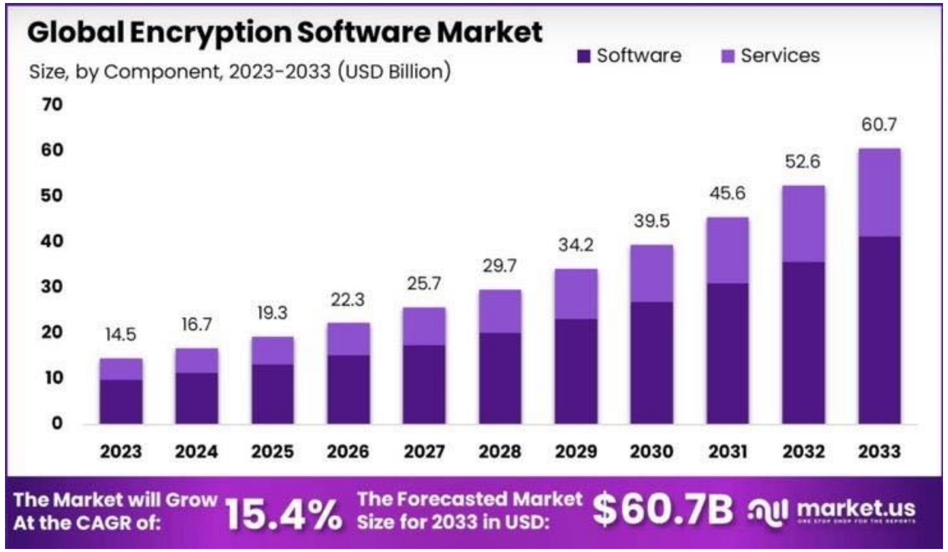
True Entropy Encryptors

Weakness of current cryptography

- Established encryption methods such as *AES* and the new PQC standards *CRYSTALS-Dilithium*, *CRYSTALS-KYBER* or *SPHINCS+* are based on complex numerical algorithms and are becoming more and more CPU-intensive.
- Encryption processes are time-consuming and not practical for IoT and streaming encryption of large amounts of data.
- Encryption is not user friendly.
- Less than 50% of the data on servers and in the cloud is protected by encryption *https://www.statista.com/statistics/1243960/sensitive-data-encrypted-in-cloud-percentage*.
- Less than 2% of data on home devices and IoT is encrypted *https://www.devprojournal.com/technology-trends/internet-of-things/iot-security-avoid-these-5-mistakes/*.
- Unbreakable encryption of all sensitive data in transit and at rest, including the under-served IoT sector, is the most secure solution for the PQC era.

Business opportunity



Target customers:

- Banks and financial institutions
- Healthcare (protecting patients’ clinical data)
- Automotive industry (keyless entry, OTA updates)
- Cloud service providers (cloud data storage and streaming)
- Defense industries

Entropy is good

- The mission of RANDAEMON is to develop an innovative and practical encryption system based on physical entropy.
- Technology protected by 11 issued US patents, several pending and issued in Korea, Australia, and in the EU:

US Patent *10,430,161* US patent *10,901,695* US patent *11,036,473* US patent *11,048,478* US patent *11,249,725*
US patent *11,281,432* US patent *11,567,734* US patent *11,586,421* US patent *11,614,921* US patent *12,014,153*
US patent *12,034,834*

- RANDAEMON's encryption method is unbreakable by quantum computers and AI because it requires brute force search over an enormous number of permutations.

RANDAEMON’s innovative solution

- Encryption method maximizes entropy using true random numbers.
- Cryptographic devices are scalable, integrated into the IoT and connected to PCs via USB or networked with servers, supporting streaming and block encryption.
- Encryption and decryption are fast, easy to use, and very hard to break due to the enormous number of possible permutations available.
- Decrypting messages on computing devices does not require access to the embedded encryption device, only software and the key.

RANDAEMON’s hardware-based solution

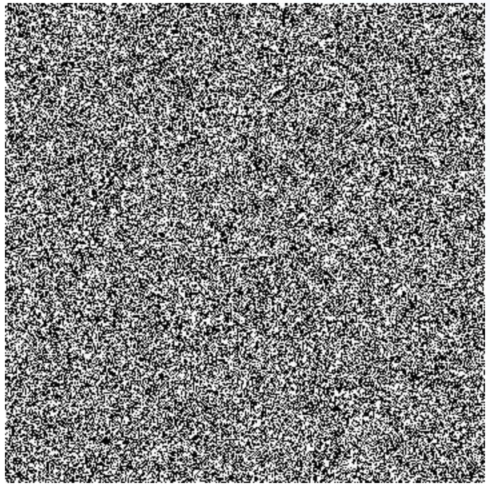
- Cryptography is all about maximizing the state of disorder (entropy) of ciphers.
- Current mainstream cryptography uses pseudo-entropy for encryption
- RANDAEMON’s True Quantum Random Number Generators (tQRNG) are based on a quantum process of beta nuclear decay in nuclei of ^{3}H (tritium) or ^{63}Ni nuclei to continuously generate random numbers.
- The advanced, tritium-based PoC tQRNGs can generate high quality random numbers from 1 Mbps to over 1 Gbps.
- Tritium-based tQRNGs were developed in collaboration with MB Microtech, a Swiss company with over 50 years experience and excellence in tritium-based technology *https://mbmicrotec.com*.
- Easy scaled and manufactured to build integrated chips, USB devices and blade servers for easy to use and safe encryption.
- PoCs have been extensively tested by the *NIST.SP.800-90B* battery of tests and other industry tests such as *Dieharder* or *ENT*.

RANDAEMON’s software solution: AIRBARN™

- AIRBARN™ — *Artificial Intelligence-Resistant Bury Among Random Numbers* encryption software.
- AIRBARN™ inserts a message into a stream of random bits from built-in tQRNGs using a randomly generated key.
- The resulting cipher looks like random numbers (visualized as graphics):

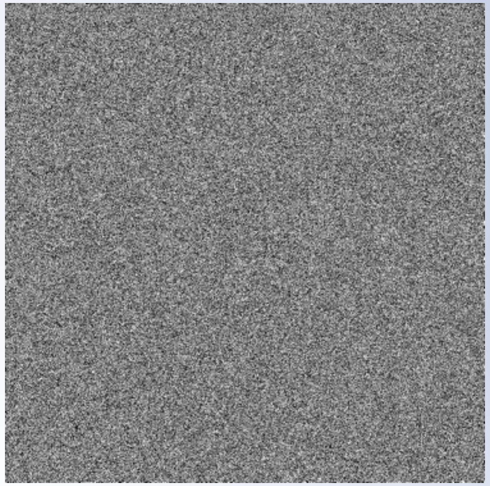
Picture of RANDEAMON’s COO
Low entropy original

+



Random bits
from tQRNG hardware

=



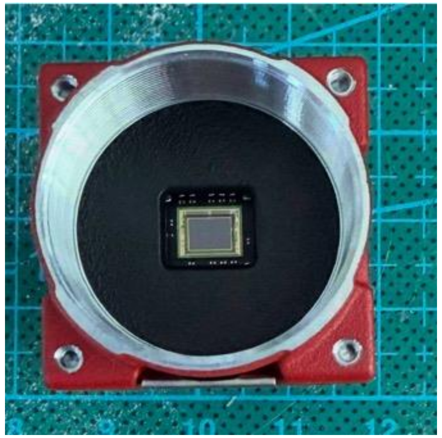
AIRBARN™-encrypted photo
High entropy

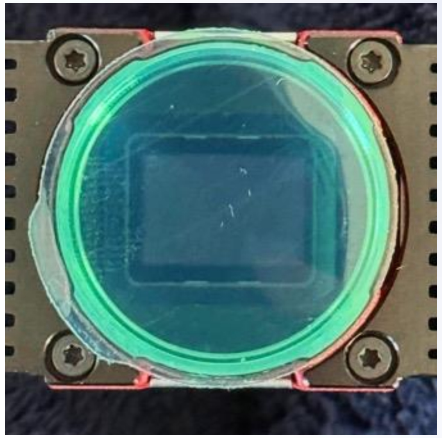
Advantages of AIRBARN™

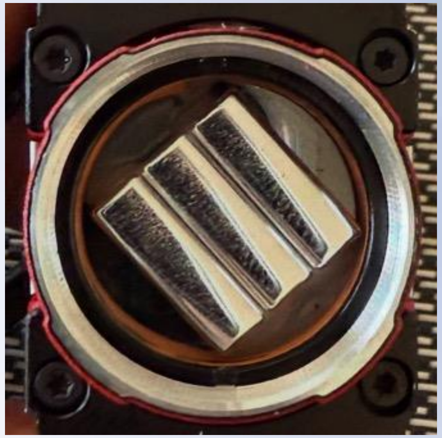
- Coding and decoding can be supported on low-power CPUs (IoT).
- High efficiency for both streaming and block encoding (servers).
- Longer keys do not increase computational complexity but make it harder to break the code.
- Decryption requires NO hardware – only free AIRBARN™ software and the key.
- Great for PQC:
  - Future quantum computers will not be able to break the AIRBARN™ cipher:
    - Simple 256-bit key creates a staggering $3.45 \cdot 10^{62}$ possible permutations.
- Use of AI will not be useful due to the perfect randomness of the encrypted messages.
- Solution for effective encryption methods for both, IoT and servers.

Current state of RANDAEMON technology

- Advanced version of PoC tQRNGs with optimized software for low (1 Mbps) and high (up to 1 Gbps) efficiency random bit extraction have been built and tested.
- AIRBARN™ software supports encryption and decryption on macOS, Linux and Windows, as well as iOS and Android.







Timelines

- Goals:
    - To begin production of V1.0 series,
    - Marketing to reach first enterprise customers.
- Deliverables – products for extensive testing and initial sales:
    - Low efficiency (tQRNG up to 10 Mbps) USB devices with Windows, macOS and Linux user software as well as iOS and Android software for AIRBARN™ encryption,
    - High efficiency (tQRNG ≥ 1 Gbps) blade servers with API to embedded software for AIRBARN™ encryption.
- Timeframe – 18-24 months.
- PoC tQRNG devices and AIRBARN ™ software are available for immediate testing.

RANDAEMON

Designed in California
Made in Europe

https://randaemon.com

krzysztof.appelt@randaemon.com
+1 (760) 840-0572