

FERMIBO

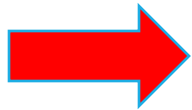
Unbreakable Encryption Technology

The Mission of FERMIBO

- Our mission is to develop and commercialize innovative and unbreakable encryption system based on true physical entropy hardware and sophisticated software:
 - tQRNG hardware (*true Quantum Random Numbers Generators*) creating up to 1 Gbits per second of random digits for encryption needs
 - **HARD** software (*Hidden Among Random Digits*) is a disruptive encryption algorithm that inserts a message into a stream of random bits from tQRNG
 - **QEST** software (*Quantum Entropy Simplified Transcriber*) applied to **HARD** scheme results in a Fully Homomorphic Encryption (FHE) system

Weakness of Current Cryptography

- Common encryption methods are based on numerical algorithms
- Due to AI and quantum computers, existing ciphers require longer keys

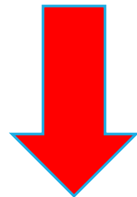


more CPU and time needed for encryption

- Existing methods are not useful for IoT and for encrypting large sets of data

Fewer than 50% of servers and cloud data are protected by secure encryption

Fewer than 2% of data on home devices and IoT is encrypted



- **Innovative solutions are necessary to provide secure, CPU efficient and convenient encryption for Post-Quantum Cryptography (PQC) times**

FERMIBO's Innovative Solutions

- Our encryption method **HARD** uses true random numbers to maximize entropy
- Our cryptographic devices are scalable and can be integrated into IoT, connectable to PCs and networked with servers to support efficient and secure streaming and block encryptions
- **HARD** encryption and decryption processes are CPU-efficient, highly secure and easy to use
- Decrypting messages on any device does not require hardware, just software and a key

Hardware-based Solutions

- Cryptography is all about maximizing the disorder (*entropy*) of ciphers
- **FERMIBO**'s tQRNG use the process of beta decay in ^3H (*tritium*) to generate random numbers continuously
- Advanced, tritium-based PoT (Proof of Technology) tQRNG can generate high-quality random numbers at speeds ranging from 1 Mbps to over 1 Gbps
- tQRNG are being developed in collaboration with MB Microtech, a Swiss company that has over 50 years of experience with and expertise in tritium-based technology
- tQRNG are easy to scale, to build into integrated chips, into USB devices, and blade servers for secure encryption
- The quality of **FERMIBO**'s PoT, which use tQRNG and NVIDIA hardware, have been extensively tested using NIST SP 800-90B and industry tests, such as Dieharder and ENT

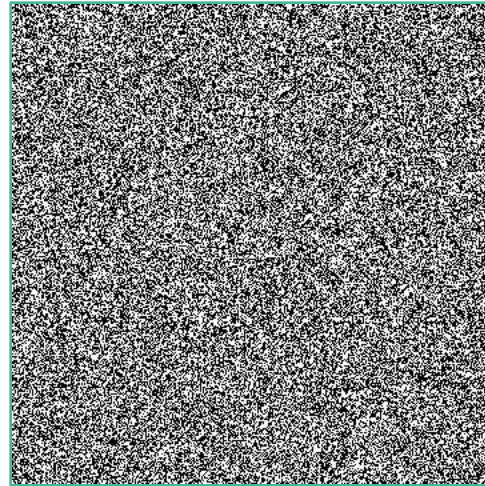
How It Works

- **HARD** is an encryption software that inserts a message into a stream of random bits from built-in tQRNG; it does not use mathematical functions which can be broken by AI
- The resulting cipher resembles random numbers and can be visualized as graphics:



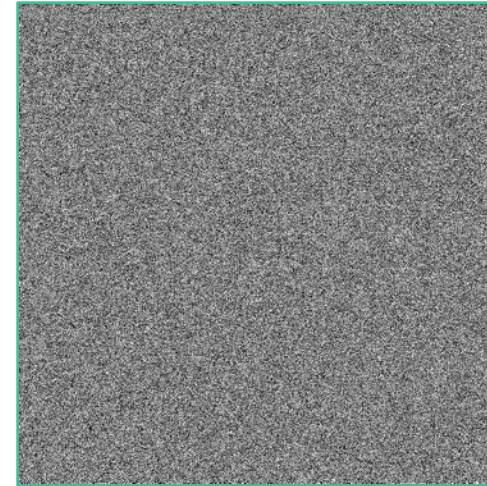
Original medical image
low entropy

+



Random bits
from tQRNG hardware

=



HARD encrypted image
high entropy

Advantages of HARD

- Low-power CPU and IoT devices can support coding and decoding
- High efficiency for streaming and block encoding on servers
- Longer keys do not increase computational complexity
- Decryption requires no hardware, only **HARD** software and the key
- The advantage for PQC era:
 - Future quantum computers will not be able to break **HARD** ciphers
 - 256-bit key creates $3.45 \cdot 10^{62}$ possible permutations to be analyzed
- **HARD** is FHE in combination with **QEST**
- It protects sensitive data, including that of the underserved IoT sector

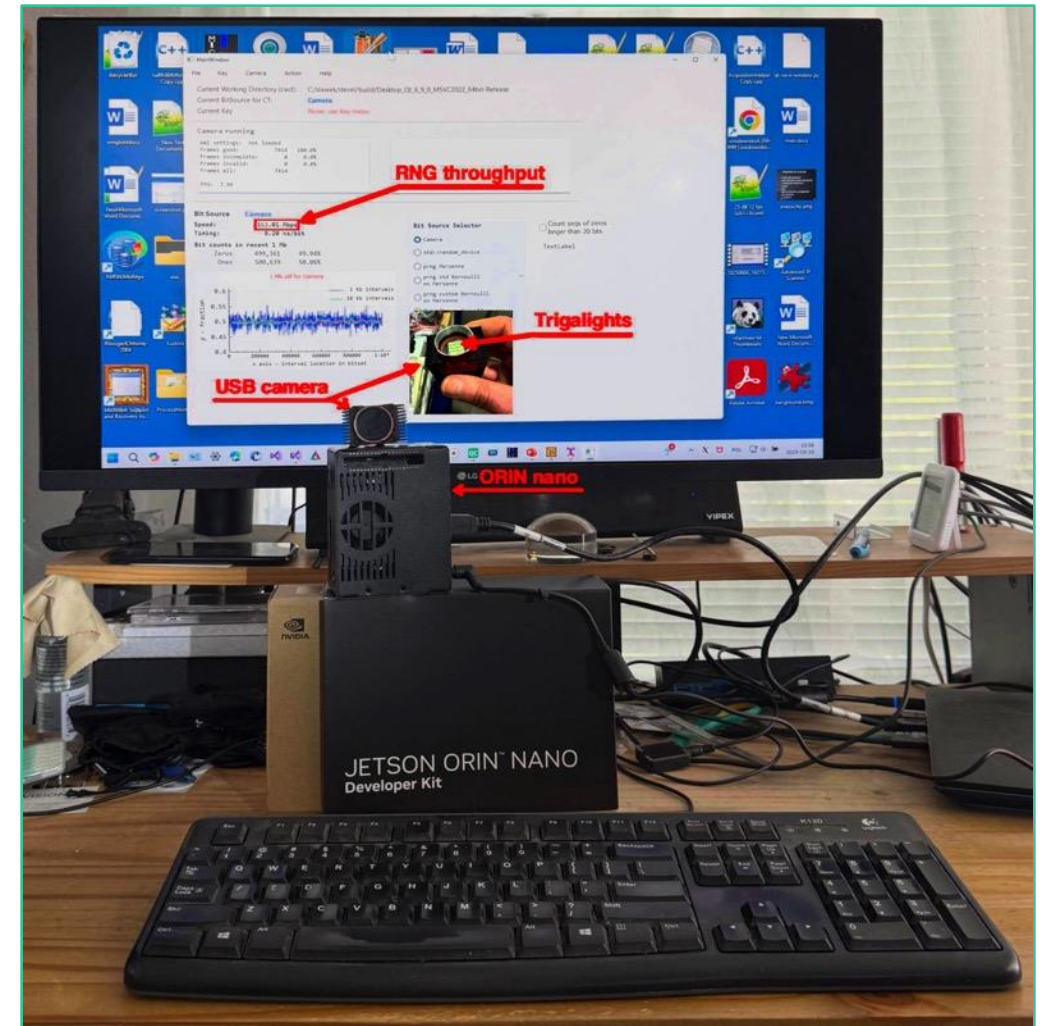
SECURITY

CPU/ENERGY EFFICIENCY

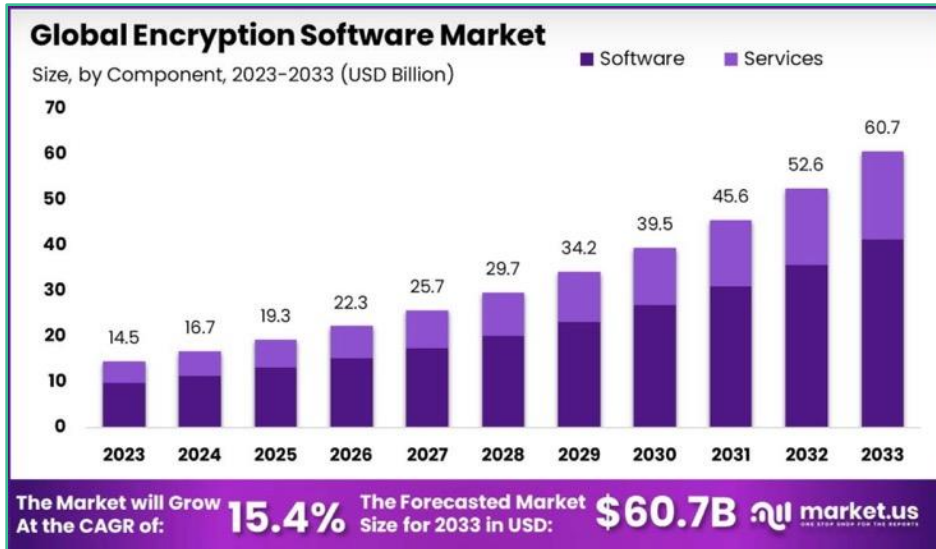
CONVENIENCE

The Current State of Our Technology

- An advanced version of the PoT with optimized software for high-efficiency random bits extraction (up to 1 Gbps) has been built and tested
- **HARD** software, when combined with **QEST**, supports the encryption for FHE on both Linux and Windows platforms
- The Jetson ORIN NANO system is under development



Business Opportunity



Target customers:

- LLM / AI creators and users (data security)
- Cloud service providers (cloud data storage and streaming)
- Banks and financial institutions (records, blockchain)
- Healthcare (protecting patients' clinical data)
- Defense industries (all communication)
- Automotive industry (keyless entry and over-the-air [OTA] updates)



FERMIBO's Business Model

- Our goal is to sell customized cryptographic devices for specific needs:
 - Integrated chips for the IoT, automotive, and home security industries
 - Peripheral USB devices that connect to the PCs used by banking and healthcare clients
 - PCI cards for servers and cloud providers, such as Google, AWS, Microsoft, Oracle, Meta, and more
 - A combination of all these products for the military and defense industries
- In a few months, **FERMIBO** will start building contacts with potential clients and intends to use PoT for demonstrations

Summary

- **HARD** is a superior encryption method based on physical entropy, that has been thoroughly tested
- **QEST** is a software that, when used with hardware, enables fully homomorphic encryption
- **FERMIBO**'s devices are based on tQRNG technology, which produces consistently high-quality random numbers; they also contain embedded software that supports all encryption needs
- The entire solution is based on NVIDIA Jetson technology
- **FERMIBO** will deliver a commercial MVP within 2 years