KeyBITS TECHNOLOGY:
PERFECT SECURITY FOR DIGITAL COMMUNICATIONS

UNHACKABLE and AFFORDABLE

KeyBITS (**KB**) *unique* technology protects the secure transmission of keys using classical digital communication signals fast mixed with recorded quantum signals. **KB** does not rely on algorithmic protocols [which are inherently breakable] nor on pure quantum protocols (QKD) [which are slow and expensive] for its security. It guarantees perfect **secrecy** for **in-transit** communication in untrusted networks. It is secure against quantum processors. **KB** signals run in any network, with no distance limitation. Keys (random bits) are generated by quantum fluctuations in a laser beam.

The **KB** technology is used by the **Quantum Communicator – QC**.
QC is an app that easily installs on *any* platform, including PCs, mobile devices, and for the Internet of Things (IoT/IIoT).
The technology allows the secure *distribution of* encryption keys *without couriers*, performs the privacy amplification (PA) process, and *encrypts / decrypts* on any platform.
QC can be customized to distinct needs for IoT/IIoT. The basic architecture to secure communications for IIoT networks was also developed.

Both the Key Generator and the QC prototypes are ready for industrialization.

What the core KeyBITS technology does

- It **generates** truly random encryption keys, securely **distribute** these keys - without using couriers, using recorded quantum noise to cloak signals.
- It **encrypts** and **decrypts** information (default encryption is **bit-by-bit**): One-Time-Pad encryption is unbreakable.
- It uses **any** communication channel.
- It is **fast** (5G speeds).
- It has **no distance limitations**.
- It is **affordable** for multiple users.

Commercialization products

- **Key generator** (patented) – continuous generation of random keys at high speed
- Encryption **keys** according to the user need (generic use for multiple applications)
- **Encryption and decryption** performed by software applications and usable on and between PCs, mobile devices and IoT and IIoT devices
- **Customized software** applications for IoT and IIoT
- Multiple **services**, including customer support

Markets

- Companies and private sector with sensitive information to be transmitted
- Law enforcement, government, embassies, and agencies
- Utility companies and smart grids
- Military
- Health care secure data exchange among enterprises and medical services offering on-line patient monitoring and intervention (e.g., vital signals, pacemaker signals)
- Finance enterprises, banking
- Precision farming
- Public safety agencies and services
- IoT (Internet of Things) and IIoT (Industrial IoT) *****
- Game industries (random numbers), weather simulations, finance predictors

***IoT and IIoT devices include:**

(1) autonomous vehicles of all kinds and drones; (2) surveillance cameras; (3) electrical and water grid control points; (4) automated functions of crucial transportation infrastructures such as railway switches, ports, drawbridges, and oil pipelines; (5) property management and perimeter security devices such as motion sensors and intrusion alarms; (6) “smart home” hubs that control appliances and home security features; and (7) all military equipment for which effectiveness requires either confidentiality in digital transmissions or remote monitoring or operation.

Basic elements of the secure communications architecture

1. A unique ***random number physical generator****, based on *quantum fluctuations* of a light field. It generates noisy quantum signals that, in recorded form, give random bits. These bits are used for encryption. Random bits are also added to digital standard signals to cloak information from an attacker: a physical protection layer for digital signals.

KeyBITS Generator comparison with commercial random generators

Company or product	NIST tests Short sequences	NIST tests Long sequences	Large Bandwidth (fast speed)	Single detector: Simplicity + no need for balance	No radioactivity
ID Quantique	✓	✗	✗	✗	✓
Photon pairs	✓	✓	✓	✗	✓
EYL	✓	✓	✓	✗	✗
Quintessence	✓	✓	✓	✗	✓
KeyBITS	✓	✓	✓	✓	✓

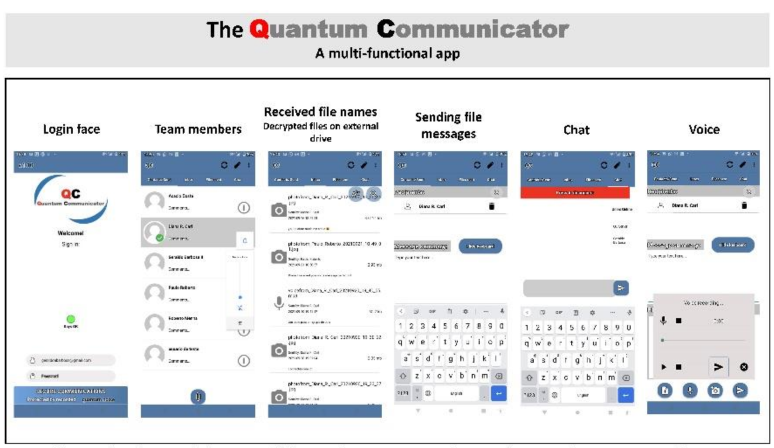
The KB generator meets all important NIST criteria and has other good qualities, that others don't!

2. The **Quantum Communicator**™
   (Version **Messenger** and **IoT/IIoT**)

It is a universal ***app*** (software for all platforms) to securely *distribute* encryption keys *without* couriers, perform the *privacy amplification* (PA) process, and *encryption / decryption* on **PC**s, **mobile devices**. It allows customizations for the Internet of Things (IoT/IIoT).

Functions:

- One-Time-Pad (OTP) Encrypt/decrypt all files
- Send / Receive
- Camera (OTP encrypted)
- Voice (OTP encrypted)
- Chat (OTP encrypted)
- OTP Encrypted Command/Control of IoT/IIoT devices
- Keys are kept on external device with password (USB, Bluetooth memory)
- Decrypted information is **not** kept on the **QC**: provides added security



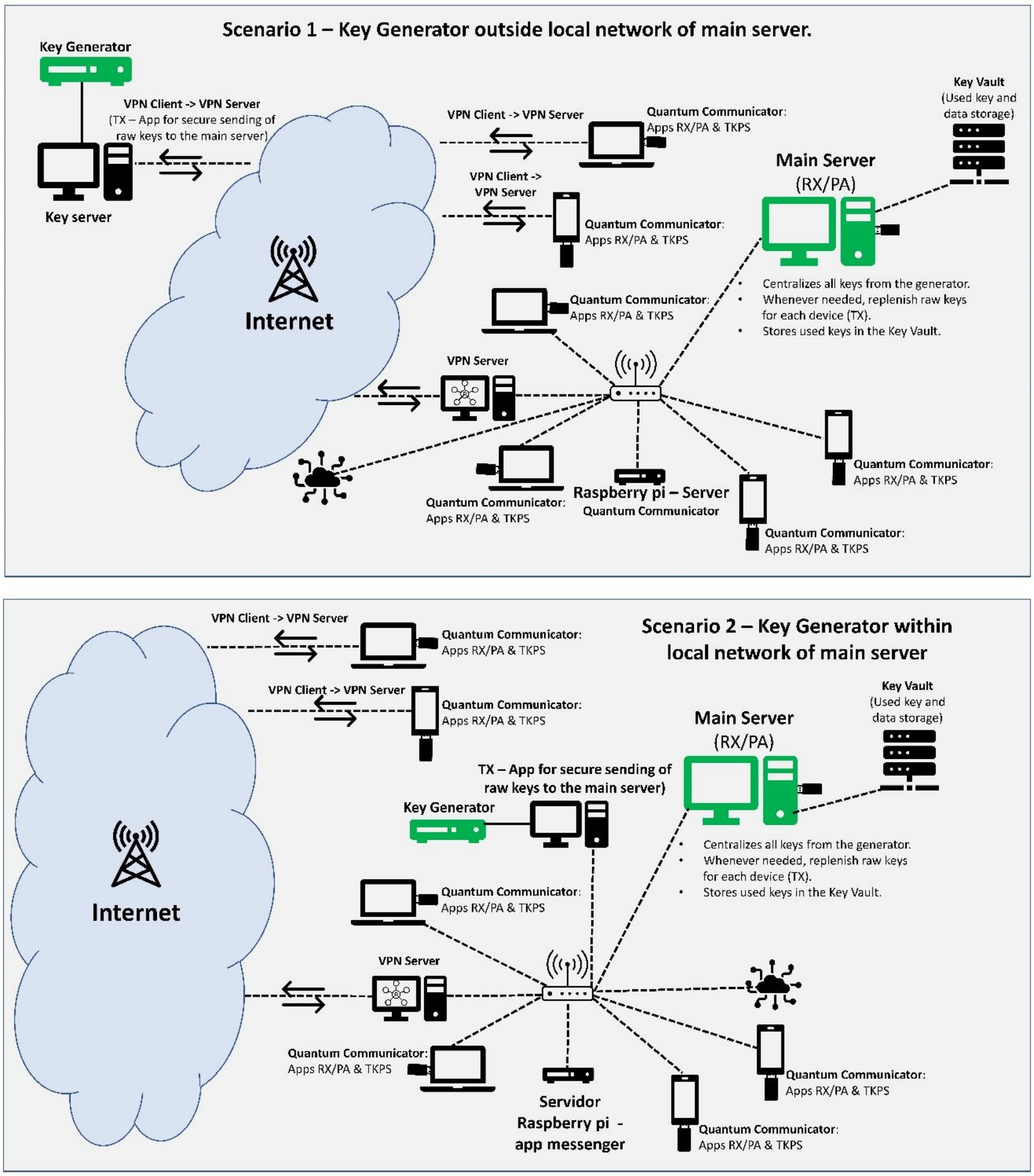
Encryption **keys** and **decrypted** files are kept on **external** memories – **under your control!**

References: see arXiv1901.05324v3: "*A wireless secure key distribution system with no couriers a One-Time-Pad Revival*", and references therein. See also the original *key distribution* idea presented in patent US 7,333,611 B1 (2008), that utilizes optical noise intrinsic to the *optical* channels.

IoT and IIoT utilizes the same basic protection for secure communication built in the Quantum Communicator. Due to distinct needs of the industrial, or even a home environment, customizations can be done at the normal software level, to adapt it to specific conditions demanded.

Adaptive scenarios exemplify servers to be used, mobile devices, hubs, and controlled equipment at the edge level:

IIoT scenarios (KeyBITS/TKPS architecture)



INFO and CONTACTS

KeyBITS Encryption Technologies LCC, MD - USA
https://www.keybits.tech

- DUNS®: 117035277
- Small business
- NAICS Codes 341713, 541715, 541513
- CAGE: 8BCU6

Dr. **Geraldo A. Barbosa**
E-mail: GeraldoABarbosa@gmail.com
Cell: +1 443 891 7138

09November2021