KB

KeyBITS technology

PROTECTS YOUR COMMUNICATION

WIRELESS,
UNHACKABLE and AFFORDABLE

https://www.keybits.tech
https://www.tkps.eu/

July 2021

Summary

KeyBITS (KB) is a revolutionary key distribution and encryption technologies* combining quantum elements and classical communication signals. It brings perfect secrecy for **all** digital communications. **KB** does not rely on the current encryption algorithmic protocols [inherently breakable] nor on pure quantum protocols (QKD) [slow and expensive].

This innovative technology **generates** truly random encryption keys, securely **distribute** these keys - without using couriers*, **encrypts** and **decrypts** information (default encryption is **bit-by-bit**).
It uses **any** communication channel. It is **fast** **(5G speed)**.
It has **no distance limitations**. It is **affordable** for a large number of users. It guarantees **secrecy** for **in-transit** communication in untrusted networks.

KB delivers the highest degree of protection by mixing **recorded quantum noise** signals with standard digital signals, cloaking the signals from an attacker.

*Contact: Dr. Geraldo A Barbosa, email: GeraldoABarbosa@gmail.com

*Keys can be sent encrypted by algorithm protocols (breakable).
Human carriers (couriers) can be used instead – under high risks.

Salable items

The **KB** technology offers

- fast (GigaBit/sec) optoelectronic KeyBITS key generator (patented) sequences of random bits (known as keys*)
- encryption and decryption performed by software applications for PC, mobile devices and for IoT and IIoT devices
- client support channel
- maintenance for the generator and related services
- Customized software applications for IoT and IIoT

*The market for random keys, unrelated to encryption, include industries, weather prediction, stock markets, epidemiology, and the gambling industry.

Target Markets

- Law enforcement agencies, government and agencies exchanging communications in sensitive areas
- 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
- Precision farming
- IoT (Internet of Things) and IIoT (Industrial IoT)*
- Public safety agencies and services
- Autonomous vehicles (information transferred among vehicles or between support/control centers and vehicles).

*IoT and IIoT devices include:
(1) autonomous vehicles of all kinds and drones; (2) surveillance cameras; (3) electrical grid control points; (4) automated functions of crucial transportation infrastructures such as railway switches, ports, and drawbridges; (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.

The current encryption landscape is insufficient

Today's encryption technologies come in two forms: algorithm and quantum – they don't meet the needs of everyone:

- Encryption using algorithms are ***deterministic*** and ***hackable.*** 🔴

Very soon quantum technologies will be capable of decrypting almost anything classically encrypted (Public key algorithm, for example, has never been proven secure. It may be broken by a mathematical advance or better processing capabilities).
Documents encrypted today with classical encryption technologies will almost certainly be decrypted in the future with quantum technologies.
Post-quantum security (algorithm) protocols are not yet ready. No one knows if they will be proven secure.

- Quantum protocols (**QKD**) are g-r-e-a-t but ***slow & expensive!*** 🟡

These won't be applicable for every need, or for everyone.

What does provide a robust protection?

The digital **KB** technology **does**: 🟢

- **KB** employs truly non-deterministic components to the communication signals, distinguishing it from classical encryption algorithms.
- **KB** is not a pure quantum technology – to avoid slowness and high cost. It is a revolutionary combination of quantum elements and classical technologies. It uses recorded quantum noise to protect the wireless. and fast distribution of *truly random* keys, without using couriers.
- **KB** is fast. There are no distance limitations.
- **KB** seamlessly adapts to any channel, which is particularly important to the varied existing and future flexible communication architectures.

more:

- **KB** solves the widespread insecurity in all networks, including IoT/IIoT.
- **KB** is affordable:

KB can operate station to station with independent connections or in a decentralized mode with one platform connected to N receiving stations. The cost of **KB** is roughly computed as the generator's cost divided by the number N of users. Using a ROM of $US\$25{,}000$ per generator, for a decentralized configuration consisting of one generator and 100 users, the average per user installation cost is $US\$\ 250$.

Contrast it with QKD:

A per station QKD cost is millions per station (US$3 millions), and it grows with the number of stations. A minimum of two stations is required to get started.

KeyBITS background

KB's patent "**Fast Multi-Photon Key Distribution Scheme Secured by Quantum Noise**", **US 7,831,050 B2 (2010),** Inventor and proprietary: **G A Barbosa** (2003), is an **evolution** over the work tested and approved, with support from **DARPA***, started on 2000 and developed at the Center for Photonic Communication and Computing of the Northwestern University, with patent "**Ultra-Secure, Ultra-Efficient Cryptographic System**" (Inventors: H P Yuen, P Kumar and **G A Barbosa** - 2003) **US 7,333,611 B1 (2008)**. **KB** extended the idea for key distribution on optical channels (2003) and, lately (2018), for secure **digital** communications (any channel).

This evolution produced the current wireless version that was positively reviewed on the technology aspect by US agencies including recent **NASA**** (pre-selected project for H9.05 Transformational Communications Technology (SBIR) program-2020), DARPA (Cryptography for Hyper-scale Architectures in a Robust Internet of Things (CHARIOT)-2020, **DoD***/US ARMY** (DoD SBIR 20.2 – Program BAA A20-139), **DHS****** (Secure and Resilient Mobile Network Infrastructure)-2020.

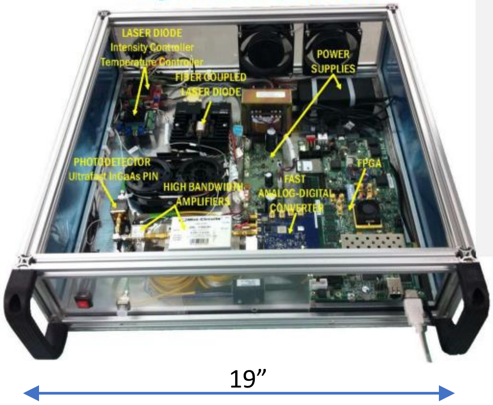
The **KeyBITS generator** prototype had support from the Brazilian Army Command, under the **Renasic** Project ***** (FINEP supported)-2013.

***DARPA**: Defense Advanced Research Projects Agency. Project Cost**: US$(5+5) millions**. Project developed at Center for Photonic Communication and Computing, Northwestern University, Evanston, IL. ****NASA:** National Aeronautics and Space Administration. *****DoD:** US Department of Defense. ******DHS:** U.S. Department of Homeland Security. *******Renasic:** Rede Nacional de Excelência em Segurança da Informação e Criptografia/Brazil. (Renasic Grant 0276/12 – **US$2Million**).

Basic elements of the KB architecture:

- ✓ 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 can also be added to digital standard signals to cloak information from an attacker.
- ✓ Basic universal ***app*** (software) to securely *distribute* encryption keys without couriers, perform the *privacy amplification* (PA) process, and *encryption / decryption* on PCs, mobile devices and for the Internet of Things (IoT).

*KeyBITS GENERATOR



- **Entropy source for bit generation:** Quantum fluctuations of the laser field
- **Stable system** – no interferometry
- **Continuous operation** > 2Gbit/second (just electronics dependent speed – can be increased)
- **Miniaturization possible to increase mobility** (large chip) for large volume marketing
- **Multiple uses:** Secure communications, games, simulations …

✓ **Stand-alone equipment for several applications**

✓ **Built with commercial parts**

KeyBITS Generator comparison with commercial random generators

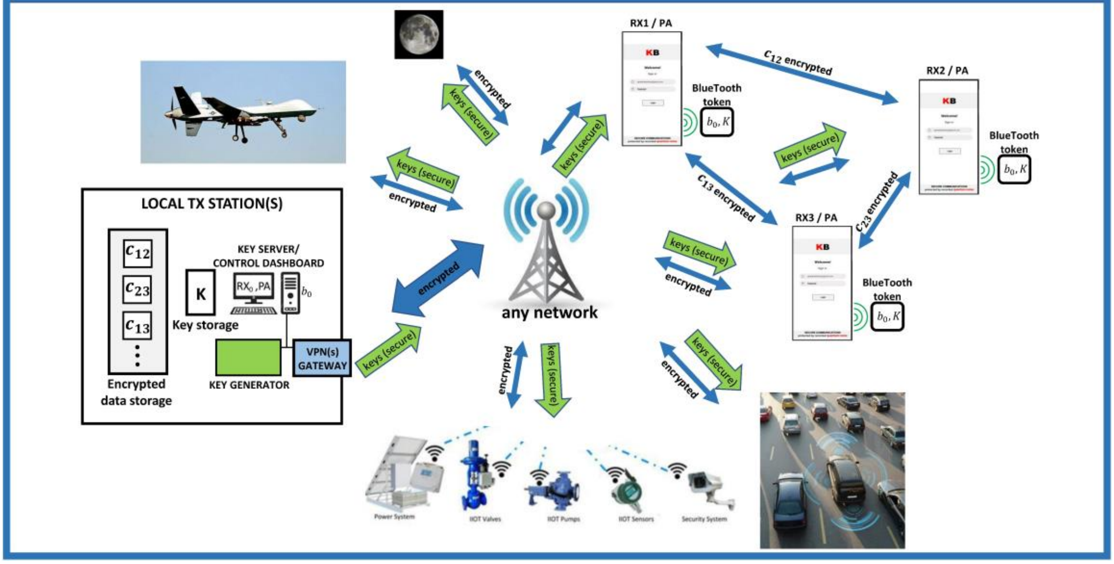
Company or product	NIST tests Short sequences	NIST tests Long sequences	Large Bandwidth (fast speed)	Single detector: Simplicity + no need for balance	No radioactivity
ID Quantique	✓	✗	✗	✗	✓
Photon pairs	✓	✓	✓	✗	✓
EYL	✓	✓	✓	✗	✗
Quintessence	✓	✓	✓	✗	✓
KeyBITS	✓	✓	✓	✓	✓

KeyBITS GENERATOR meets all important criteria

Others don’t

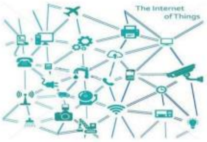
A BROAD RANGE OF APPLICABILITY

Secure VPN networks / KB technology



CONTINUOUS, FAST SECURE REFRESHING OF ENCRYPTION KEYS

Encrypted command/control for **IoT***



Constant fast flow of **encrypted images** and data*

Secure **Tactical** Communications*

Securing *mobile* transmission: **transportation infrastructure** maintenance data from terrorists

Securing transmission of **medical** data

Secure **financial** data transmission

Secure **joint forces** exercises

Be part of making our digital communications more secure with KB

For a main technical reference, 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.

Contact: Dr. Geraldo A Barbosa, GeraldoABarbosa@gmail.com
KeyBITS Encryption Technologies LLC , MD USA / https://www.keybits.tech
SAM designations:
DUNS®: 117035277 Small business // NAICS Codes 341713, 541715, 541513 // CAGE: 8BCU6 (NATO Codification System)