



Post-quantum and (quantum-enabled) quantum-immune cryptosystems

Dr. Roberto Gallo
KRYPTUS CEO/Chief Scientist

gallo@kryptus.com

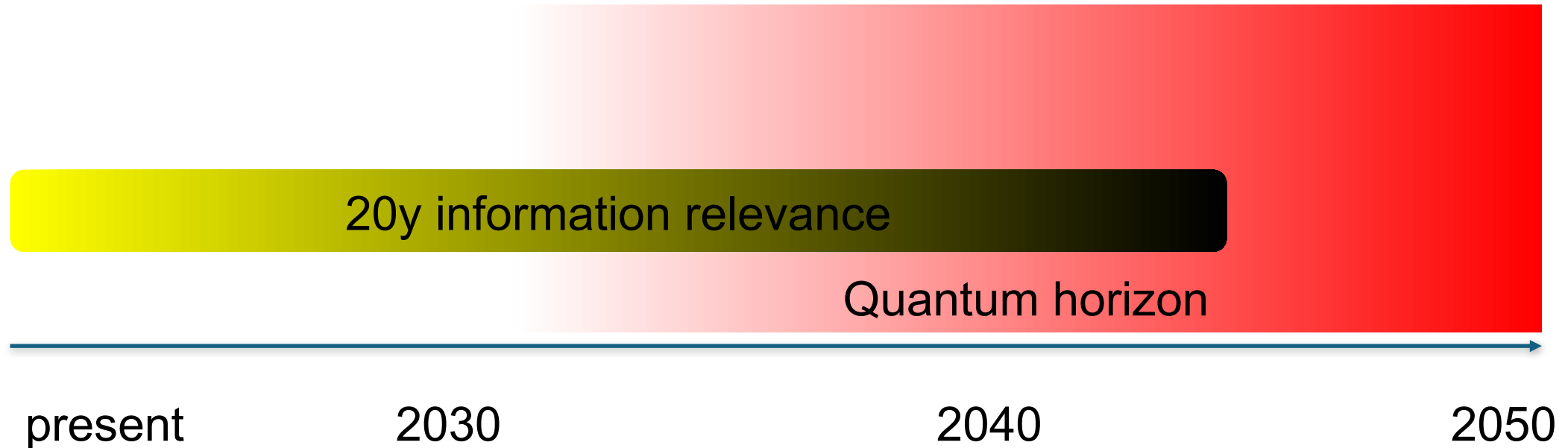


The challenge

- Quantum computers will (eventually) crack the encryption algorithms used in over 99% of the global IT and TELCO systems!
 - Shor [95,97], Grover [96] – *strangely nothing new in 30 years...*
- A piece of information sensitive today tends to remain sensitive... medical data records, State affairs, critical intellectual property may need decades of protection.
 - Digital signatures may live for decades in Real Estate (such as in Elektronisches Grundbuch)
- (Encrypted) data leakages remain in the wild for many years and three-letter agencies uses the “store-now-decrypt-latter” approach.



The quantum time-window is already clashing with the information relevance window.





What can be done?

Post-Quantum Crypto (PQC)

- [+] Least challenging, covers most use cases
- [-] Missing full Trust on PQC algs., unsuitable for very critical applications

Quantum Key Distribution (QKD)

- [+] (Quasi) perfect security throughout entanglement, Heisenberg principle
- [-] Depends on the media, not E2E, and depends on ... classical crypto (!)

Unconditionally secure One Time Pad (OTP)

- [+] Perfect security, covers data at rest, and communications use cases
- [-] More complex than PQC and less than QKD to deployment, requires a very good (physics-based) source of real entropy



But implementing crypto the right ways is a very hard task

- Side-channels analysis can recover crypto keys from almost any physical phenomena as noise, electromagnetic emanations, timing, power consumptions... Anti SCA is a must.
- A cryptosystem must not disclose the keys even with advanced physical attacks such as semiconductor slicing, fault injection, etc.
- ... and there must be a true source of entropy for key generation
 - However computers are not good at being non deterministic :-)



BRUITBLANC

ONE TIME PAD, PQC ENCRYPTION

CRYPTO ALGORITHMS EXPIRE. BRUITBLANC DOESN'T.

Physical random sequence
generators, based on
thermal noise and quantum
effect



ASI-HSM OTP for secure
sequence storage,
management



KeyGuardian OTP for user
portable encryption

Fully verifiable, free from
encryption or surveillance
laws

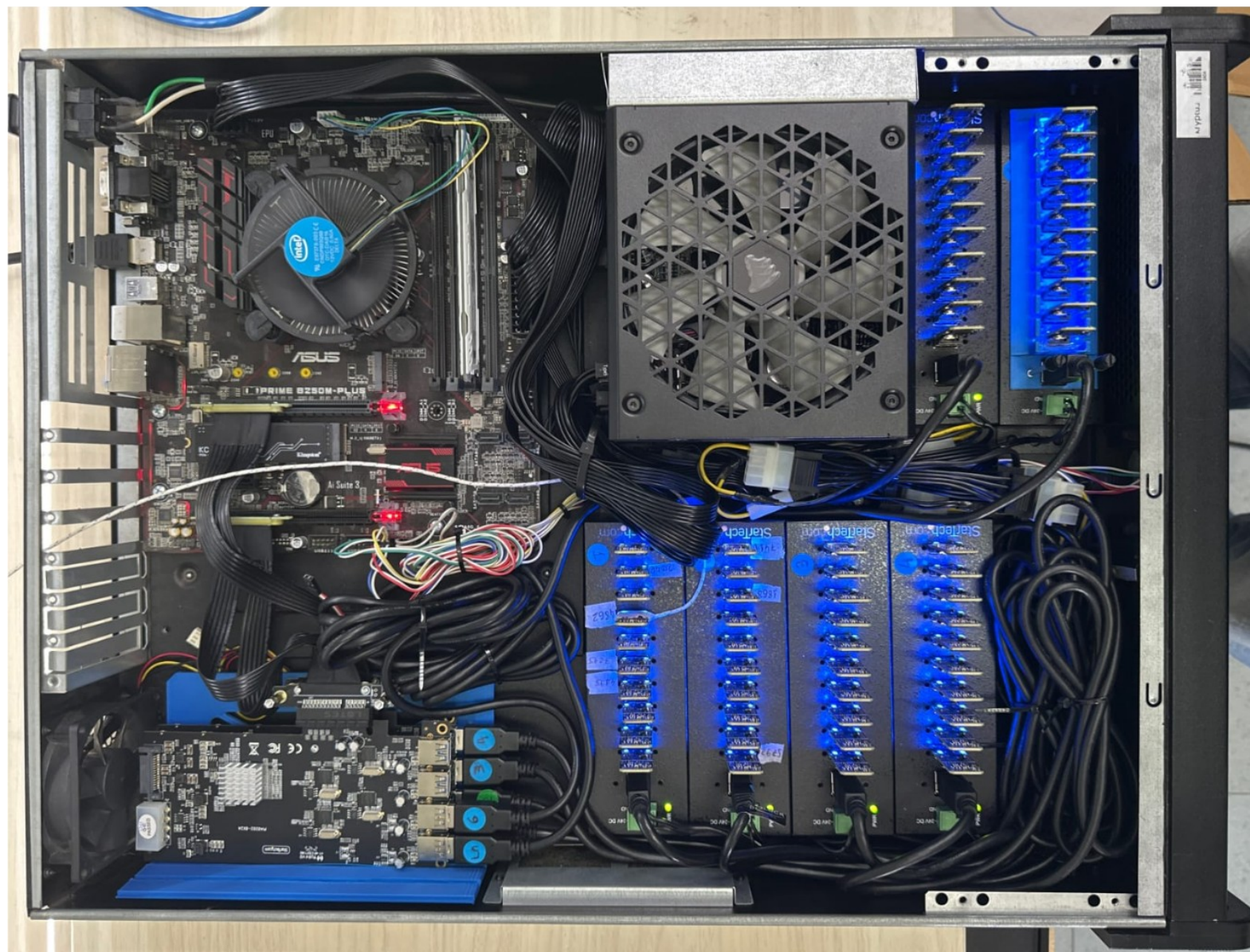


**Unbreakable Miller-Vernan's
One-Time Pad Encryption**

**Hassle-free system
management and operation**

**Convenient for office or on-the-
go usage**

**Trustworthy platform, respects
sovereign needs**



Collaboration
opportunity
around TRNG and
QKD

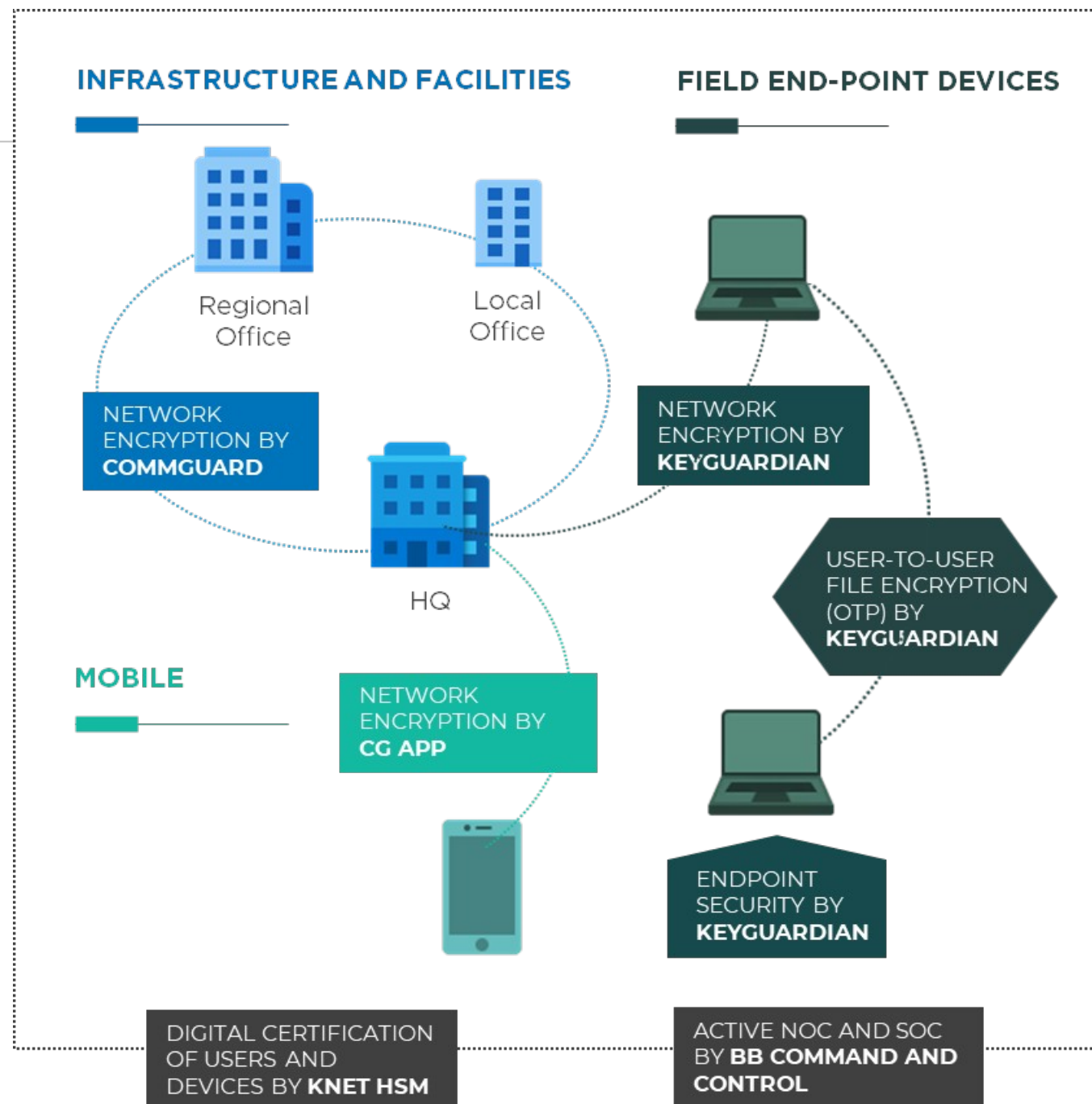


BRUITBLANC

ONE TIME PAD, PQC ENCRYPTION

USE CASES

- IP Network encryption 1Mbps to 10Gbps (ethernet, fiber, satellite, etc.);
 - Supports any service, including videoconferencing
- Mobile network encryption (iOS, Android, MacOS, Linux, Windows)
- Per application and/or network domain/IP
- File and folder encryption (MacOS, Linux, Windows)
 - OTP unbreakable encryption





This technology is being used

- By various customers in over 20 countries
- Serving over 130 million users
- In Brazil we are about to the deploy the largest PQC e-Gov service on earth (2025H1)
- Only made possible by the continuous support of FAPESP in Brazil



FAPESP
WEEK
GERMANY

March 25-26th, 2025

Continuous support from FAPESP

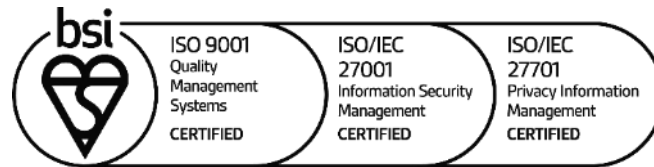


DFG Deutsche
Forschungsgemeinschaft



KRYPTUS, a 22 yo Brazilian Company

NOMINATIONS AND CERTIFICATIONS



FINANCING



KEY OFFERS

Secure Communication
Cyber Defense
Cyber Security
Data Protection
Managed Security Services
Digital Certification
Cryptography

MARKETS

B2G
B2B
Defense

COMPANY NUMBERS

22 years
+ 25 blue chip
customers
+ 19 countries

