Quantum Technologies in Space: QRNGs

Why do we need QRNGs in Space?

Quantum Conclave; New Delhi

Bruno Huttner

24/03/2023

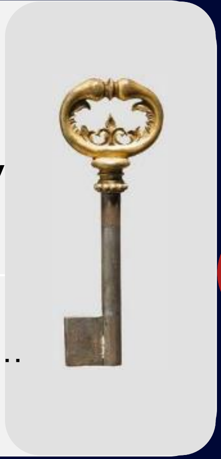
Why randomness: The basis of Modern Cryptography

RANDOM KEYS

Bad key

☒

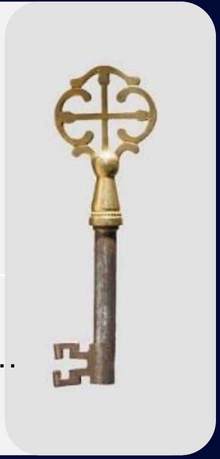
0 0 0 0 0 0 0 0...



Better key

✓

0 1 0 0 0 1 1 0...



“HARD” MATHS

- Aka: Computational Security
- Example: factoring large integers

452,165,896,684,141,009

= __________ X __________ ?

= 553,105,253 X 817,504,253 !

BOTH MAY BE THREATENED BY THE QUANTUM COMPUTER

Remember Kerckhoff: Randomness is only one aspect

To provide adequate security the key must be:

- Unique (known only by you)
- Truly random (unpredictable)
- Stored, distributed & managed securely

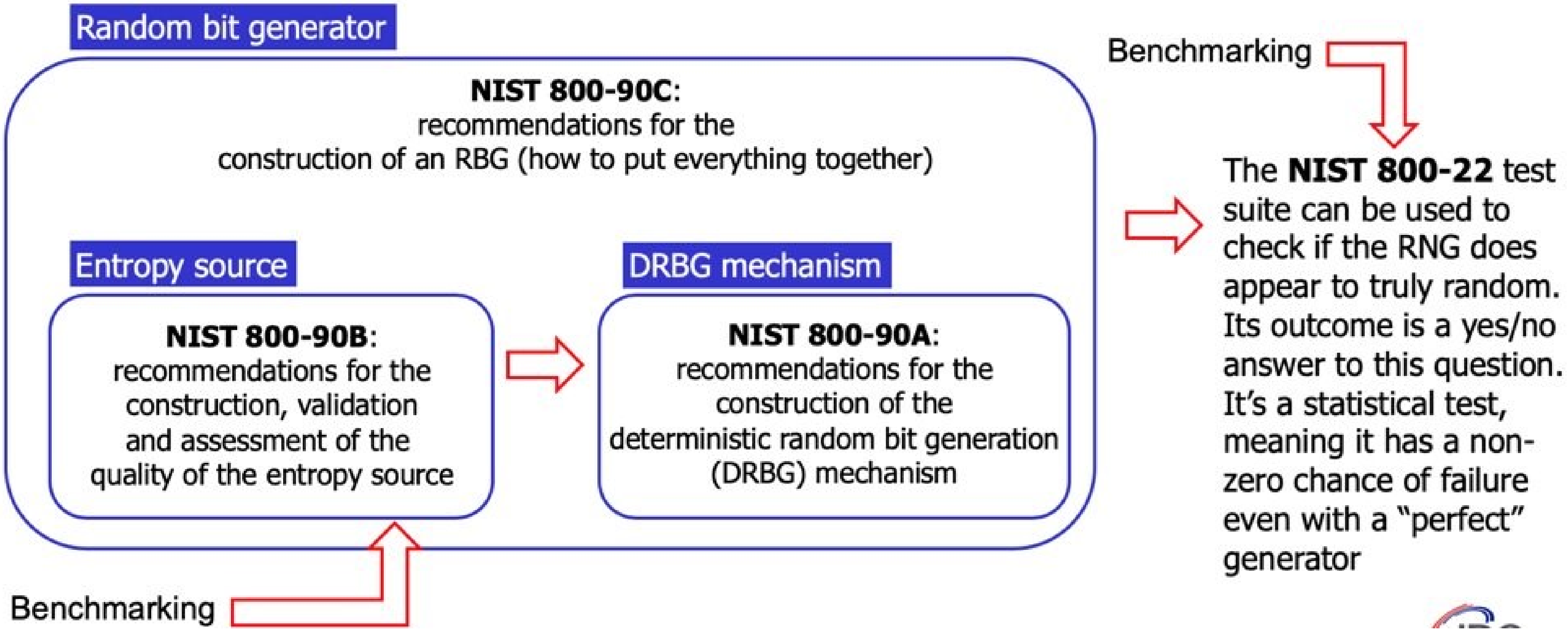
Cryptographic randomness is **private**

Most secure keys should be generated locally

Auguste Kerckhoffs (1835 – 1903)

Building an RNG: Entropy source + DRBG + Tests!

One approach : The NIST published and maintains a set of recommendations on how to build and certify a random bit generator (NIST 800-90A/B/C) and on how to test if it appears like a true RBG (NIST 800-22)



NIST 800-90C: recommendations for the construction of an RBG (how to put everything together)

NIST 800-90B: recommendations for the construction, validation and assessment of the quality of the entropy source

NIST 800-90A: recommendations for the construction of the deterministic random bit generation (DRBG) mechanism

The **NIST 800-22** test suite can be used to check if the RNG does appear to truly random. Its outcome is a yes/no answer to this question. It's a statistical test, meaning it has a non-zero chance of failure even with a "perfect" generator

Entropy generation is the main issue

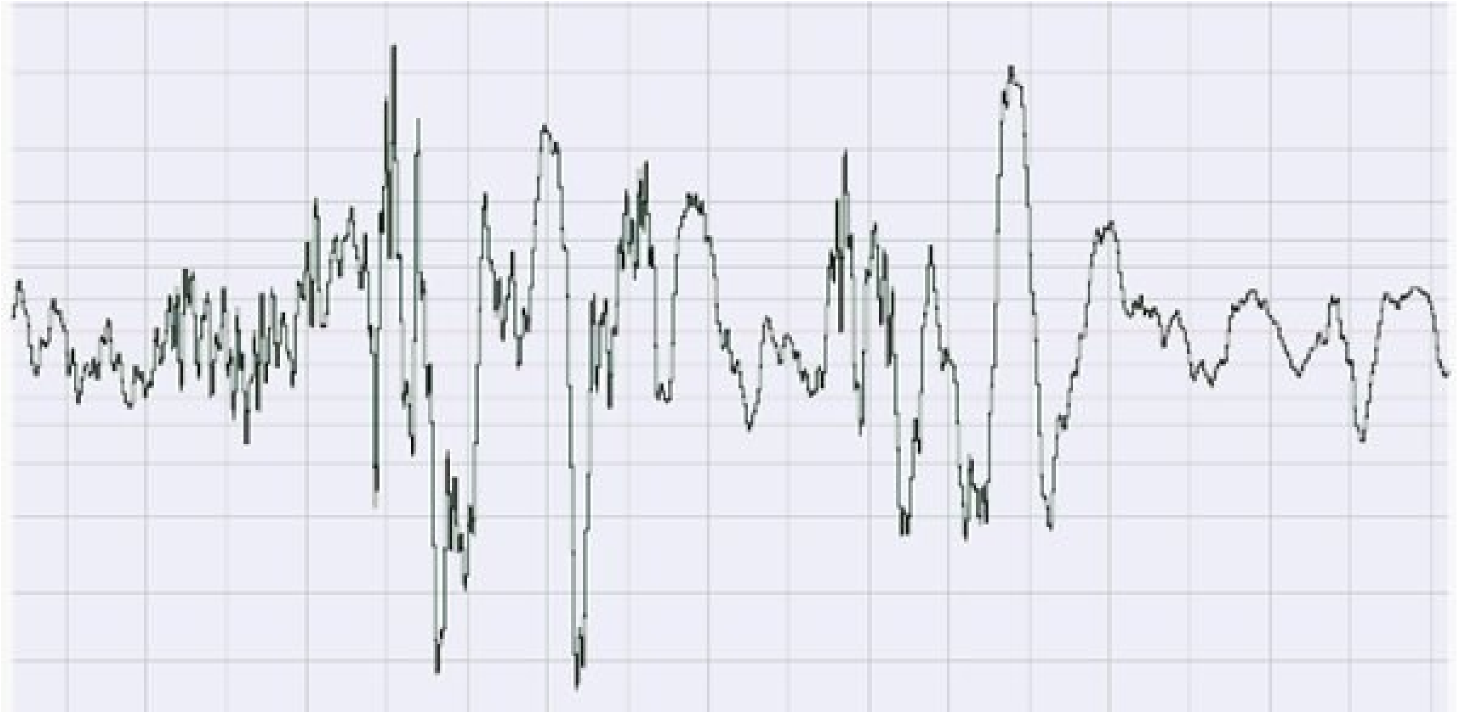
Generation of Entropy:
On the use of pseudo-random number generators…

> *Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin. For, as has been pointed out several times, there is no such thing as a random number – there are only methods to produce random numbers, and a strict arithmetic procedure of course is not such a method.*

John von Neumann

Entropy from Classical Systems: External Noise

- May have hidden regularities
- Could be manipulated
- Not always available (unmanned locations, IoTs...)



INVOLVES RISK: QUANTUM IS THE SOLUTION

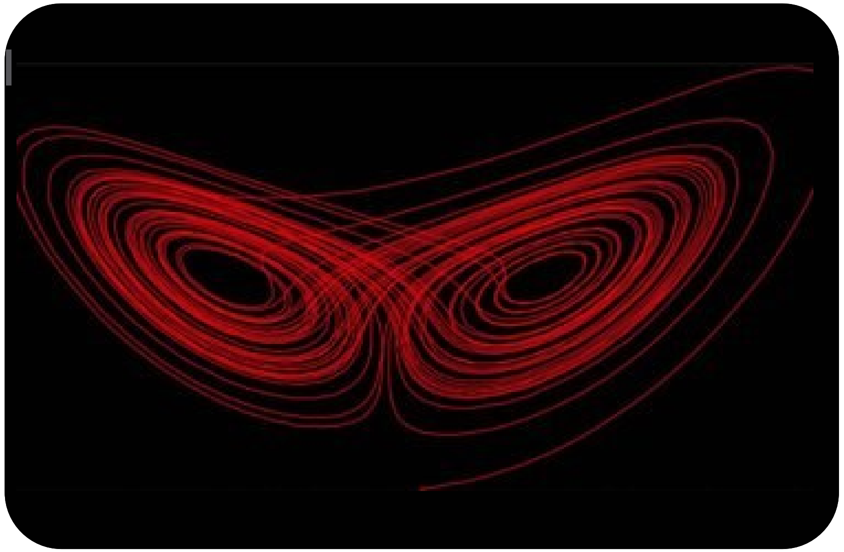
Entropy from Classical Systems: Chaos

Many Physical-RNG's or True-RNG's (TRNG's) are based on classical chaotic systems.

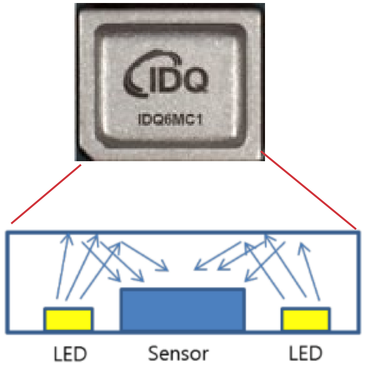
- Chaos: extreme sensitivity to initial conditions, which prevents any long-term prediction of the behavior of the system

Potential issues :

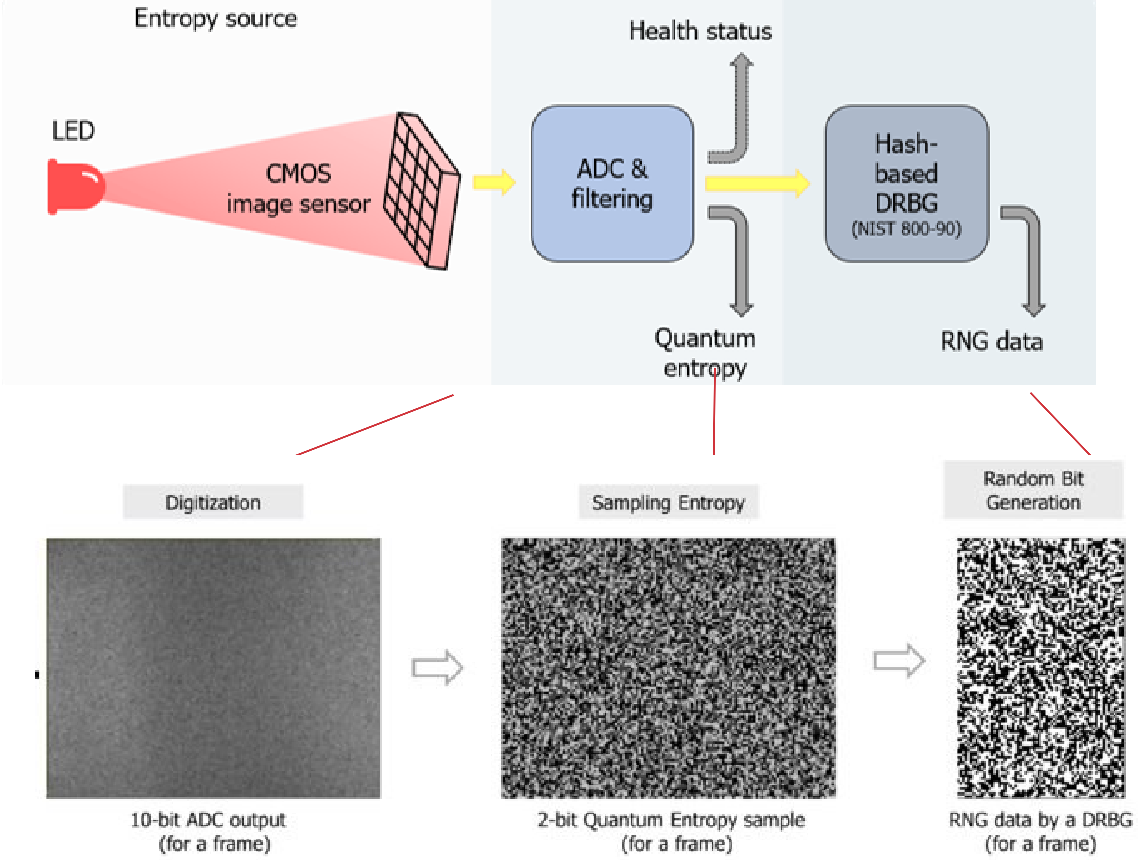
- Different initial conditions may lead to non-chaotic behavior
- Influence of environment
- Requires complex live monitoring to detect any attempt to influence the process
- Speed : needs time to accumulate entropy
- New techniques (AI and ML) can be used to predict the chaotic behaviour



Entropy from Quantum : IDQ’s QRNG chips principle



Not perfectly uniform illumination



QRNG Applications

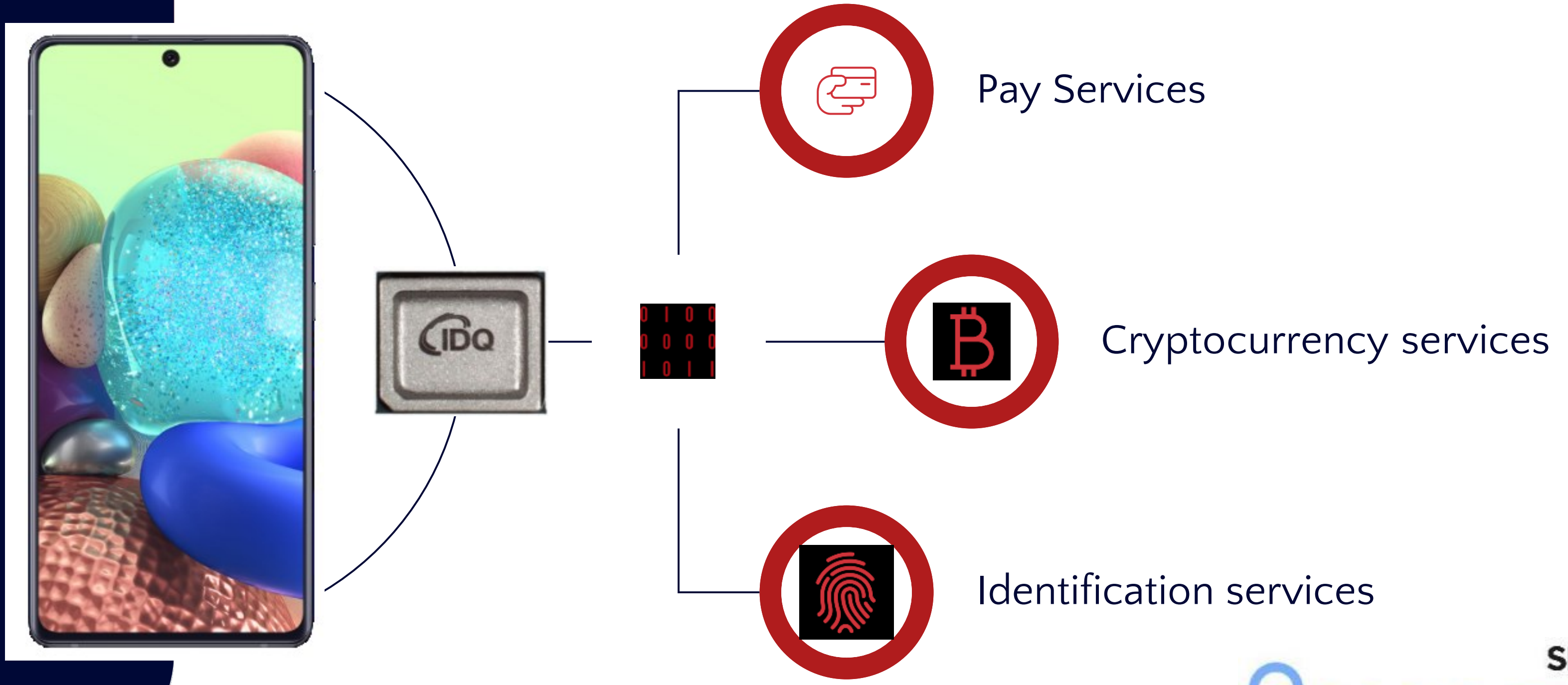
Applications

- Banking
- Datacenter Telco/MSP
- Gaming
- Cryptography
- Critical Infrastructure
- IoT

QRNG chip in mobile phones

IDQ brings a new level of Quantum enhanced phone security allowing differentiated security solutions for ICT services.

Phone Applications and Services use Security Algorithms



Pay Services

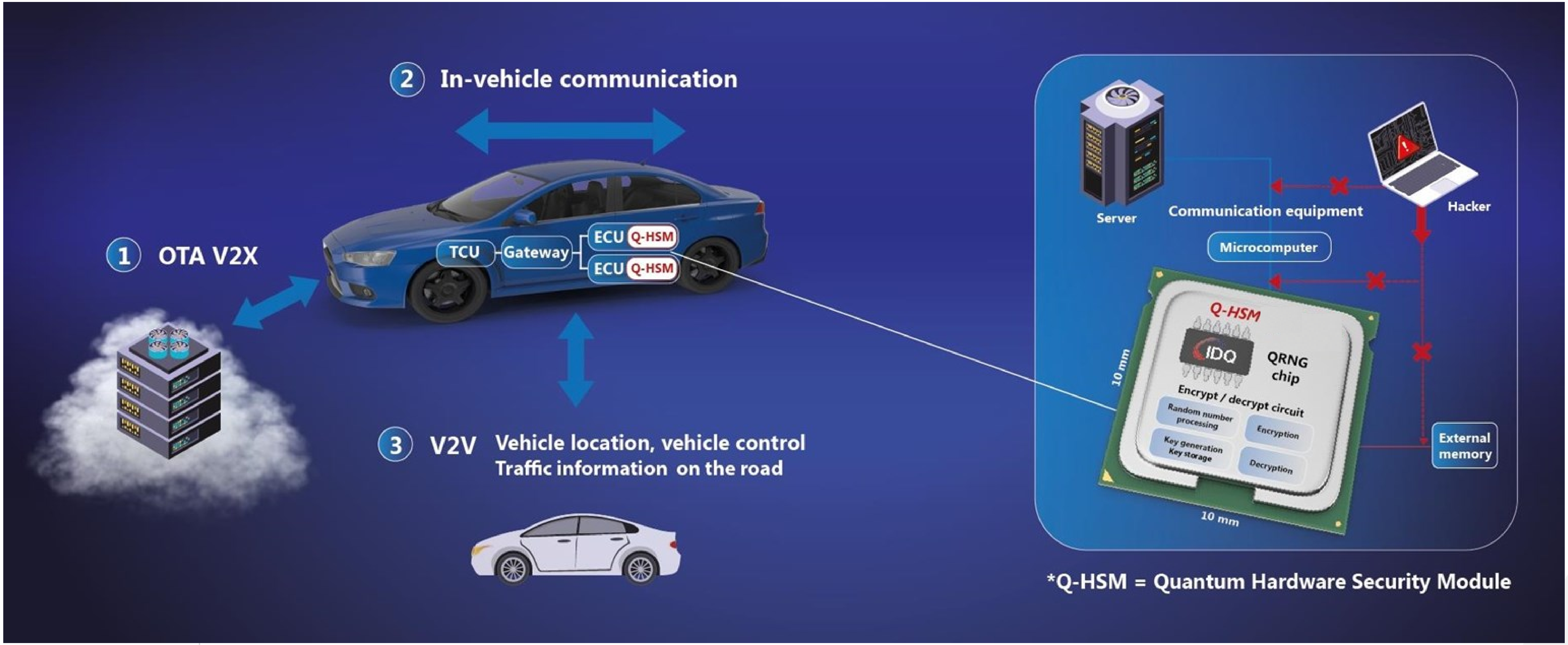
Cryptocurrency services

Identification services

SKT 5GX QUANTUM

Secured by Swiss Quantum

QRNG chip in connected vehicules



*Q-HSM = Quantum Hardware Security Module

QRNG in space

Space communication requires a good entropy source

Main requirements:

- SWAP (Size, Weight and Power)
- Radiation hardened
- Harsh environment

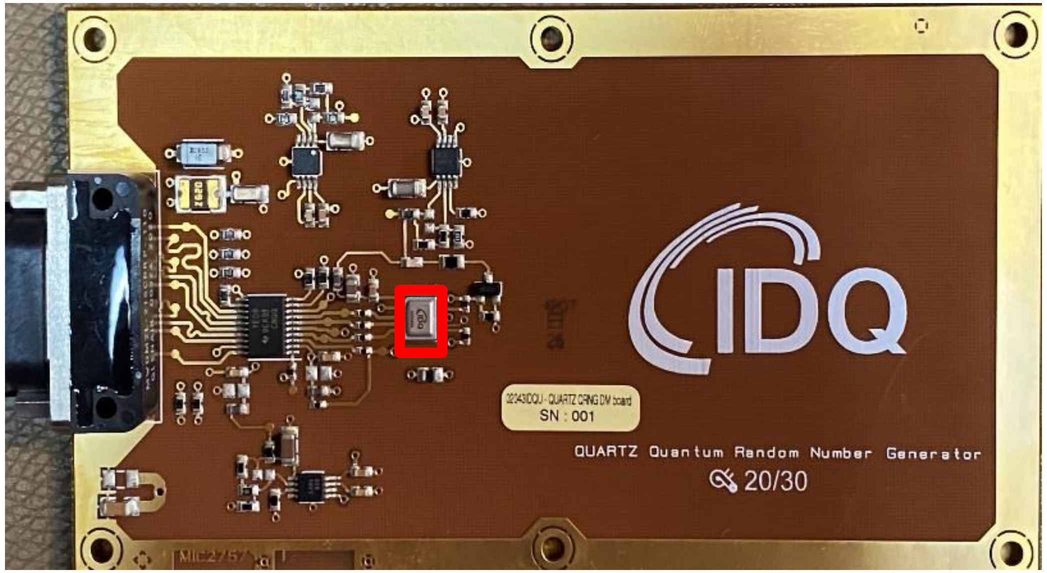
⇒ Space-grade component

Quantis QRNG chip checks all boxes!

QRNG in space

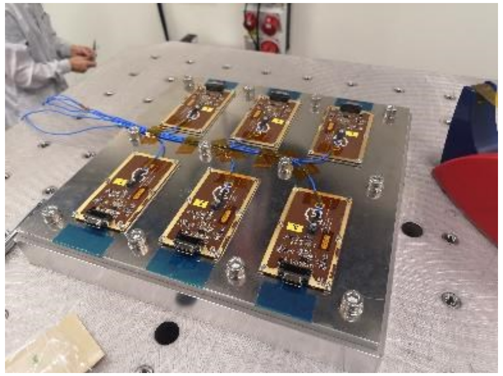
Integration into a Physical board

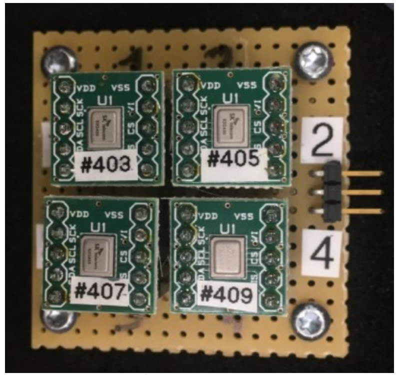
- First IDQ QRNG space project with ESA
- Developed an Engineering Model that follows European Space design rules
  - Bill of Material composed of military grade component
  - PCB space grade
  - SPI connector space grade
- Different environmental qualifications have been performed to ensure robustness in space environment
  - Radiation
  - Thermal vacuum
  - Shocks and vibration tests


IDQ
22043IDQU - QUARTZ QRNG DM board
SN : 001
QUARTZ Quantum Random Number Generator
20/30

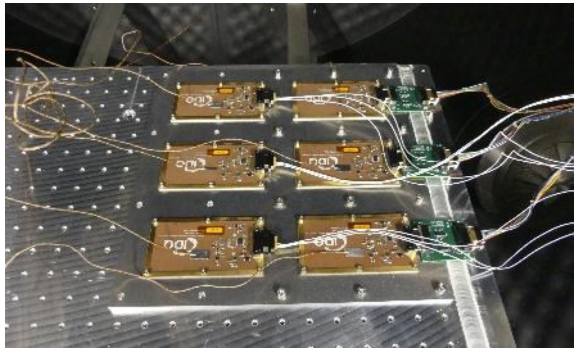
QRNG in space

Type of test	Requirements	Max level applied	Results
Total Irradiation Dose (TID)	12 krad	100 krad	PASS
Single Event Effect	No Latchup	Neutron particles during 24h	PASS
Thermal Vacuum Operating Temp	0/40°C	-5/45°C	PASS
Thermal Vacuum Non-Operating Temp	-30/55°C	-40/60°C	PASS
Sine Vibration test	5-22.3 Hz / Level 12.5 mm 22.3-100 Hz / Level 25g	Same	PASS
In Plane Random Vibration test	20-80 Hz / 3 (dB/oct) 80-400 Hz / 0.5 (g^2/Hz) 400-2000 Hz / -5 (dB/oct)	Same	PASS
Shock test	100 Hz/ Level 50g 1500 Hz / Level 2000g 10000 Hz / Level 2000g	Same	PASS
The QRNG shall have a total mass loss (TML) of less than 1%			PASS


MGSE and the 6 QRNG EM for vibration tests



Samples for TID tests


6 QRNG EM for TVAC tests

Thermal chamber with QRNG EM

Results of the project: **100 % compliant** with all requirements; QRNG chips and QRNG boards now available

Summary: Key points

1. True randomness is needed for all cryptographic applications
2. Even more so in the Quantum Era
3. Quantum Technology is the safest way to generate randomness
4. Space-qualified QRNGs are now available
5. Improve security by using them for Satellite Communications

ID Quantique

Quantum.
Trust enabled for the future

Q & A

info@idquantique.com | www.idquantique.com

ID Quantique

Founded in 2001

3 Product lines:

1. Quantum Random Number Generation
2. Quantum-Safe Security
3. Quantum Sensing

High-quality engineering

Best-in-class performance

Trust

Operational simplicity