Quantum Random Number Generators: cheaper, faster, more secure

QUANTUM Communication

QRANGE

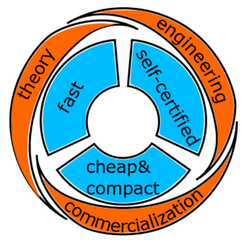
- Randomness plays an increasingly important role: algorithmic and quantum cryptography, simulations, on-line gaming.

Market	Market volumes* by 2020 (yearly)	Target price of QRNG component	Market size (yearly)
Mobile devices	1B	EUR 1	EUR 1B
IoT devices	3B	EUR 1	EUR 3B
HPC	500K	EUR 150	EUR 75M
Data centre security (HSMs)	1M	EUR 150	EUR 150M
Gb/s QKD	10K	EUR 1,000	EUR 10M

- Current problems:
  - ☹ Algorithmic random number generation (RNG) is deterministic
  - ☹ RNG based on classical physics is not a controlled process per construction → open doors for failures and attacks
  - ☹ Quantum RNG (QRNG) needs further development to compete with established products:
    → SWAP, speed, certification, improved security

QRANGE'S GOALS

- Push QRNG device, system and eventually product development towards high TRL devices and systems that are
  - ✓ low-cost and compact
  - ✓ with certified randomness and
  - ✓ at high rates.



- Develop an innovation ecosystem to drive the development of QRNG, expand the market, and train a quantum-aware workforce.
- Realise a certification framework and standards for truly quantum random number generators.

CONSORTIUM

- University of Geneva
- ICFO – The Institute of Photonic Sciences
- Katholieke Universiteit Leuven
- Université libre de Bruxelles
- Universita degli Studi di Trento
- Fondazione Bruno Kessler
- Robert Bosch GmbH
- ID Quantique SA
- Quside Technologies S.L.

USE CASES & SYSTEM ARCHITECTURE

- Systematic approach
- Open-access publications and communication of results

This will allow business to monitor and make informed decisions for investment and entering the market.

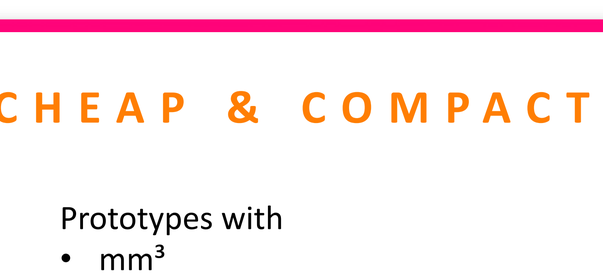
CERTIFICATION FRAMEWORK

- AIS-31: PTG.3 class sufficient?
- Do we need a PTG.Quantum class?
- Device-independent (DI), semi-DI, self-testing?

We aim to have framework and methodology ready for certification authorities by the end of the project.

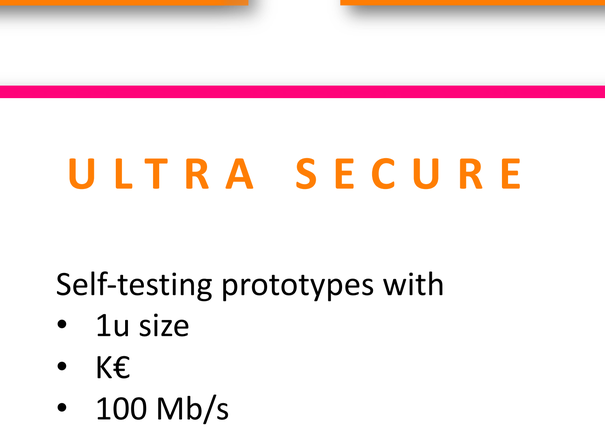
CHEAP & COMPACT

Prototypes with
- mm³
- 1€
- > 1Mb/s
- TRL6-7
- Use cases
  - ✓ IoT domain
  - ✓ system integrators
  - ✓ novel application areas to arise.



ULTRA SECURE

Self-testing prototypes with
- 1u size
- K€
- 100 Mb/s
- TRL5-6
- Use cases
  - ✓ critical infrastructure
  - ✓ security applications for early-adopters.

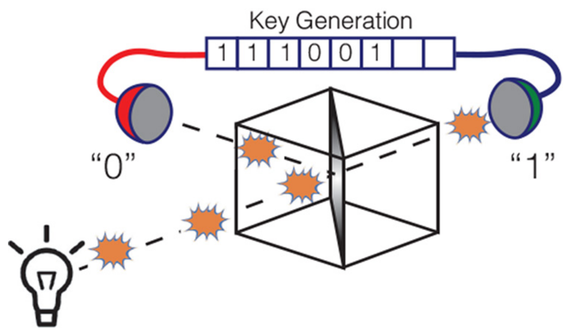


ULTRA FAST

Prototypes with
- 1u size
- K€
- > 10 Gb/s
- TRL7
- Use cases
  - ✓ high-speed QKD
  - ✓ general cryptography
  - ✓ opportunities in HPC.

CONCEPTS & THEORY

- New semi-DI and DI concepts with minimised and testable assumptions
- Market needs and technical constraints considered from the start
- Providing an increased level of trust, facilitating entry into markets where high-security is of paramount importance.



European Commission