SOC-BASED ARCHITECTURE FOR HIGH-SECURITY SATELLITE QUANTUM COMMUNICATION

ANDREA STANCO

DEPARTMENT OF INFORMATION ENGINEERING, UNIVERSITY OF PADOVA, ITALY

SEFUW 2023 - ESTEC
15/03/2023

Agenzia Spaziale Italiana

DEPARTMENT OF INFORMATION ENGINEERING
UNIVERSITY OF PADOVA

UNIVERSITÀ DEGLI STUDI DI PADOVA

ThinkQUANTUM

Quango

H2020
GA 101004341

andrea.stanco@unipd.it

OUTLINE

Brief introduction to Quantum Communiction and Quantum Random Number Generation

Key features of the system and the «QRN2Qubit» technology

SoC Architecture overview

System test and results

*A. Stanco et al., *Versatile and concurrent FPGA-based architecture for practical quantum communication systems*, IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-8, Art no. 6000108 (2022)

QUANTUM COMMUNICATION

Quantum Key Distribution (QKD) allows to reach Unconditional Security thanks to the law of Quantum Mechanics

Works with **Qubit** instead of the classical bit

Can be implemented exploiting quantum properties of light (single photon)

Practical (keyrate) limits due to:

Current technological limitations (e.g., repetition rate of a laser source)	Losses: a qubit cannot be re-generated (point-to-point communication) → Intrinsic distance limit of both fiber and free-space implementations

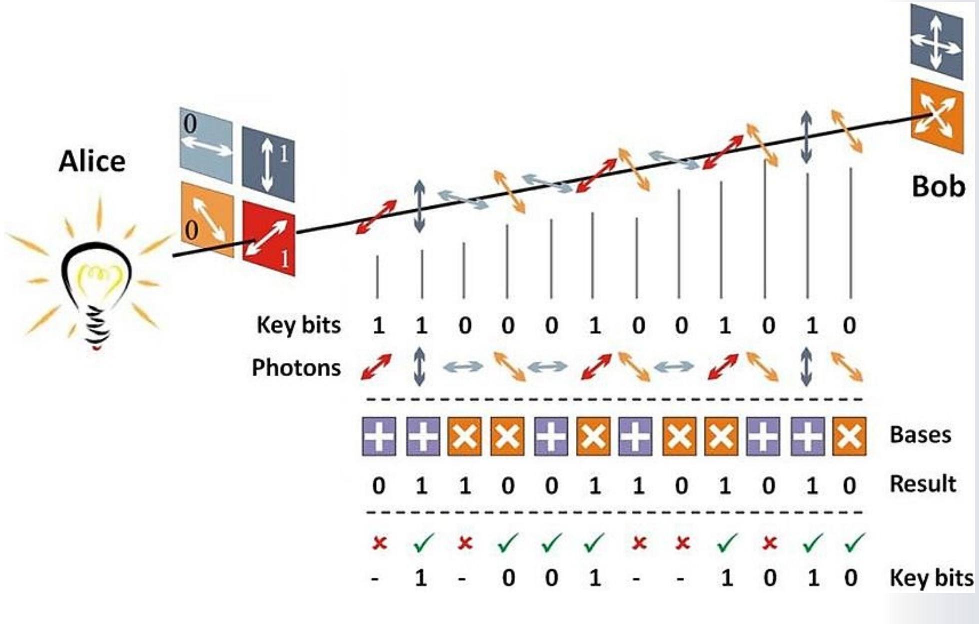
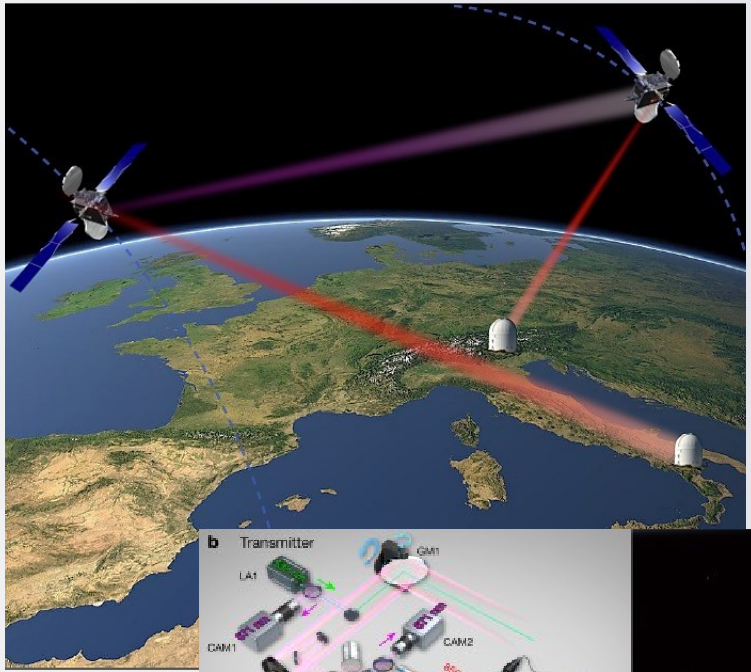


Figure from doi: 10.1007/978-3-319-30201-0_27

SATELLITE QUANTUM COMMUNICATION



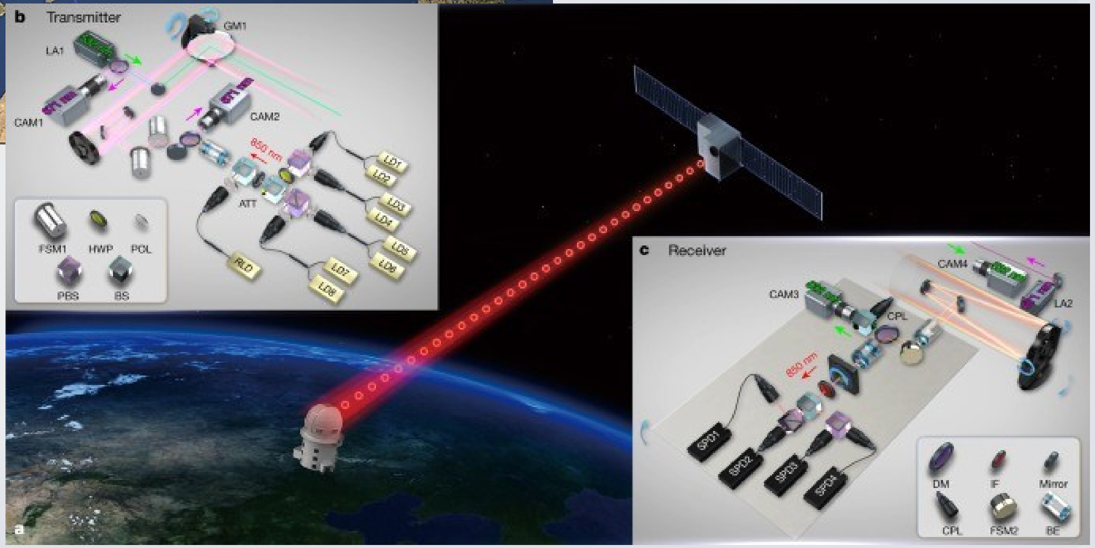


Figure from doi: 10.1038/nature23655

QKD can exploit space to overcome channel distance limits on ground

QKD transmitter on a satellite can communicate with several QKD receivers on ground (ground station) and bring QKD potentially everywhere.

Micius was the first QKD satellite transmitter (realized by the Chinese Academy of Science). Eagle-1and Eagle-2 are the two European QKD satellites to be launched in the next years.

Future scenarios will implement also satellite-to-satellite communication (requiring also a QKD receiver on satellite)

QUANTUM RANDOM NUMBER GENERATION

Generates true randomness thank to the law of QM

Can be realized exploiting the quantum properties of light

Deeply connected with QKD as a fully secure QKD apparatus should include a QRNG device

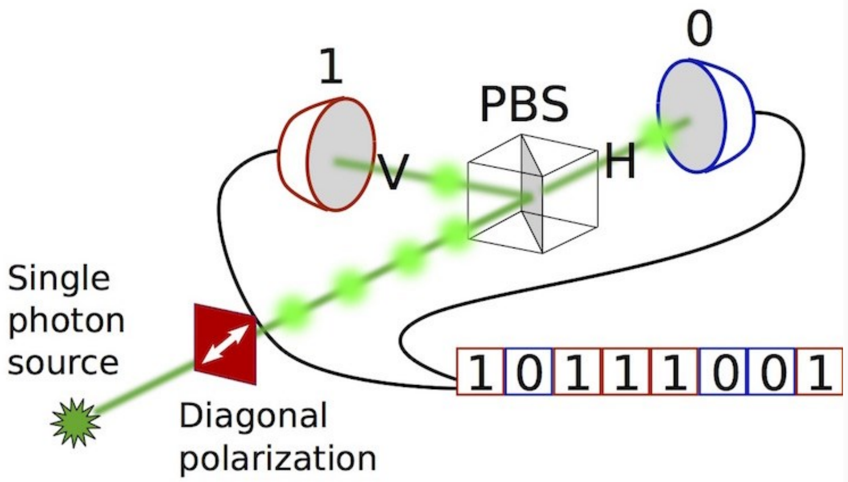


*Figure from https://quasar.dei.unipd.it

WHY QKD RELIES ON QRNG?

QKD allows to reach Unconditional Security **ONLY** if the initial qubit sequence is truly random

A proper source of randomness (e.g., QRNG) is required to provide the data/qubit sequence

Using the same (or derived from an exspansion) random data to encode multiple qubits opens a **security breach**

Fundamental security requirement, especially for Satellite Quantum Communication where I do not have a direct access to my system

SYSTEMS COMPARISON (QKD-TX)

Common Systems

Include a low bitrate QRNG device (or PRNG). Require a low bitrate communication with the QKD source

Random numbers are expanded to required bitrate. **Security breach** as the final string is derived by deterministic expansion → **Eve can attack the sequence itself instead of the QKD**

No exploitation of System-on-a-Chip (SoC) capabilities; poor flexibility

Cannot transmit an arbitrary sequence

This System

Can sustain communication with high rate QRNG to implement a «1-random-1-qubit» scheme, namely **QRN2Qubit**

No Expansion → Full security as it prevents attacks on the raw key randomness

The exploitation of the **SoC** (Zynq-7020) capabilities allows to change configuration to QKD-RX or QRNG and it also eases the design workflow

Allows to transmit any desidered sequence (convenient for non-uniform strings used in specific protocols)

FPGA-BASED SYSTEM

4-layer system (includes the 2-layer SoC system) implemented on COTS device (ZedBoard with Zynq-7020 chip)

Suitable for QKD transmitter, QKD receiver, and also QRNG

Improved flexibility thanks to functions separation between FPGA and CPU (the SoC system).

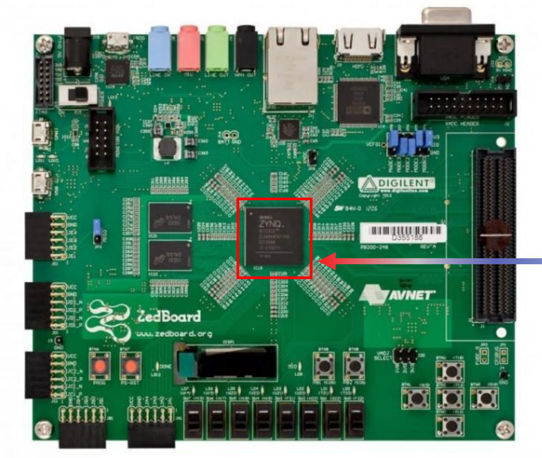
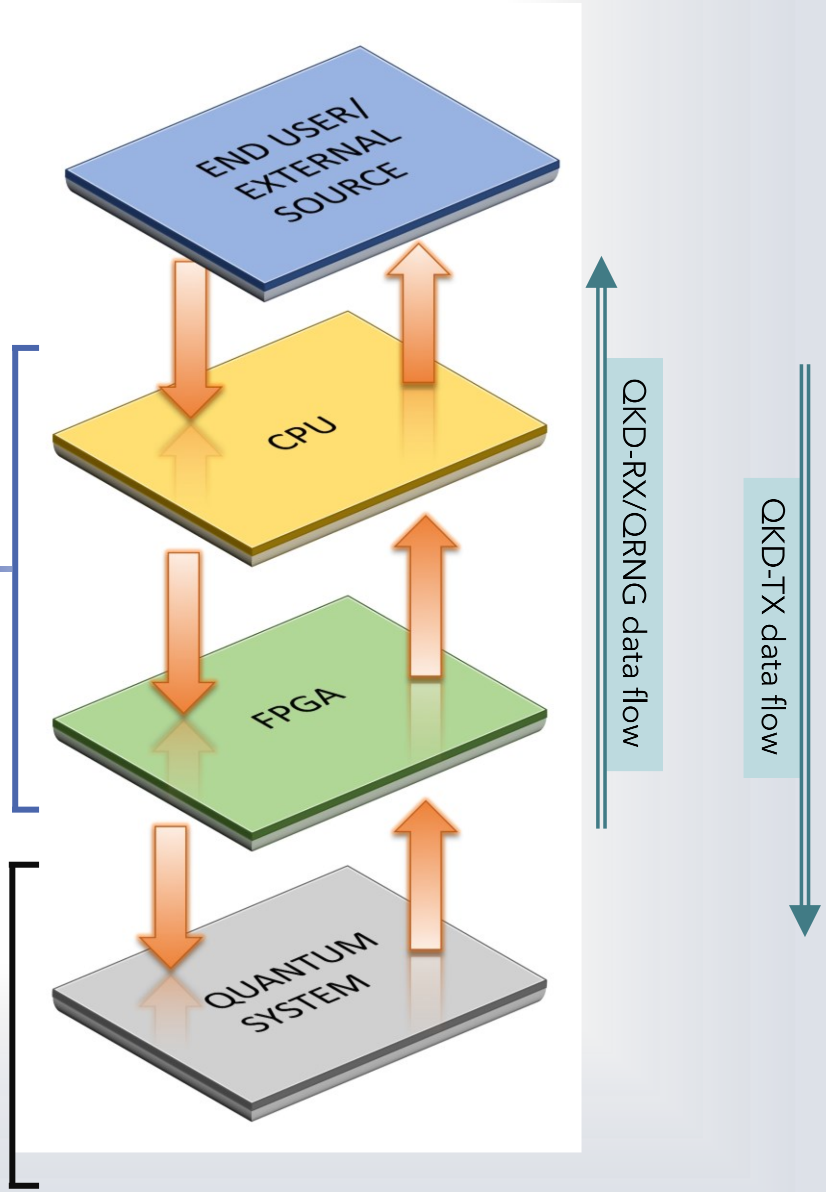


Figure from avnet.com

Figures from ixblue.com and excelitas.com

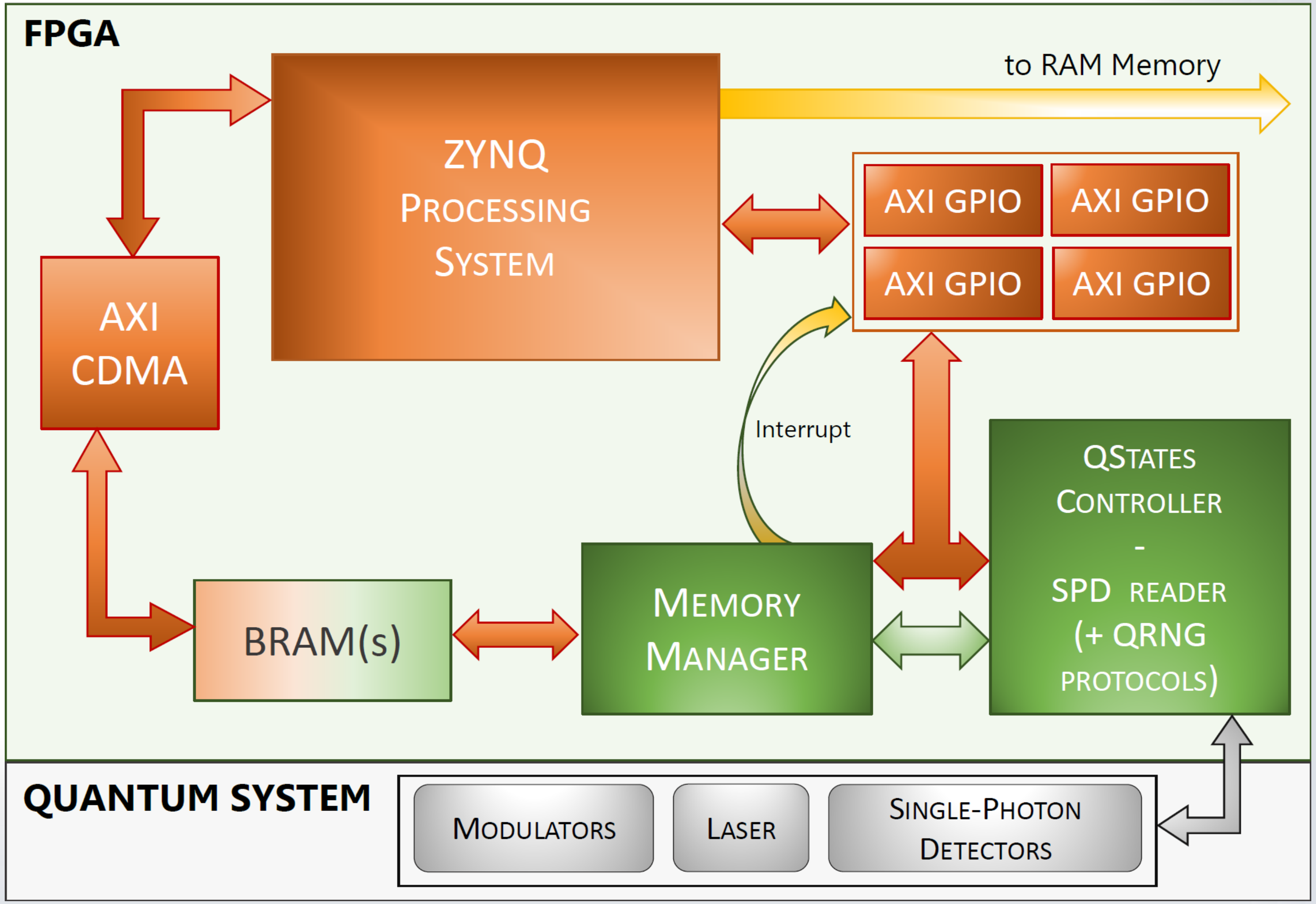


FPGA-BASED SYSTEM

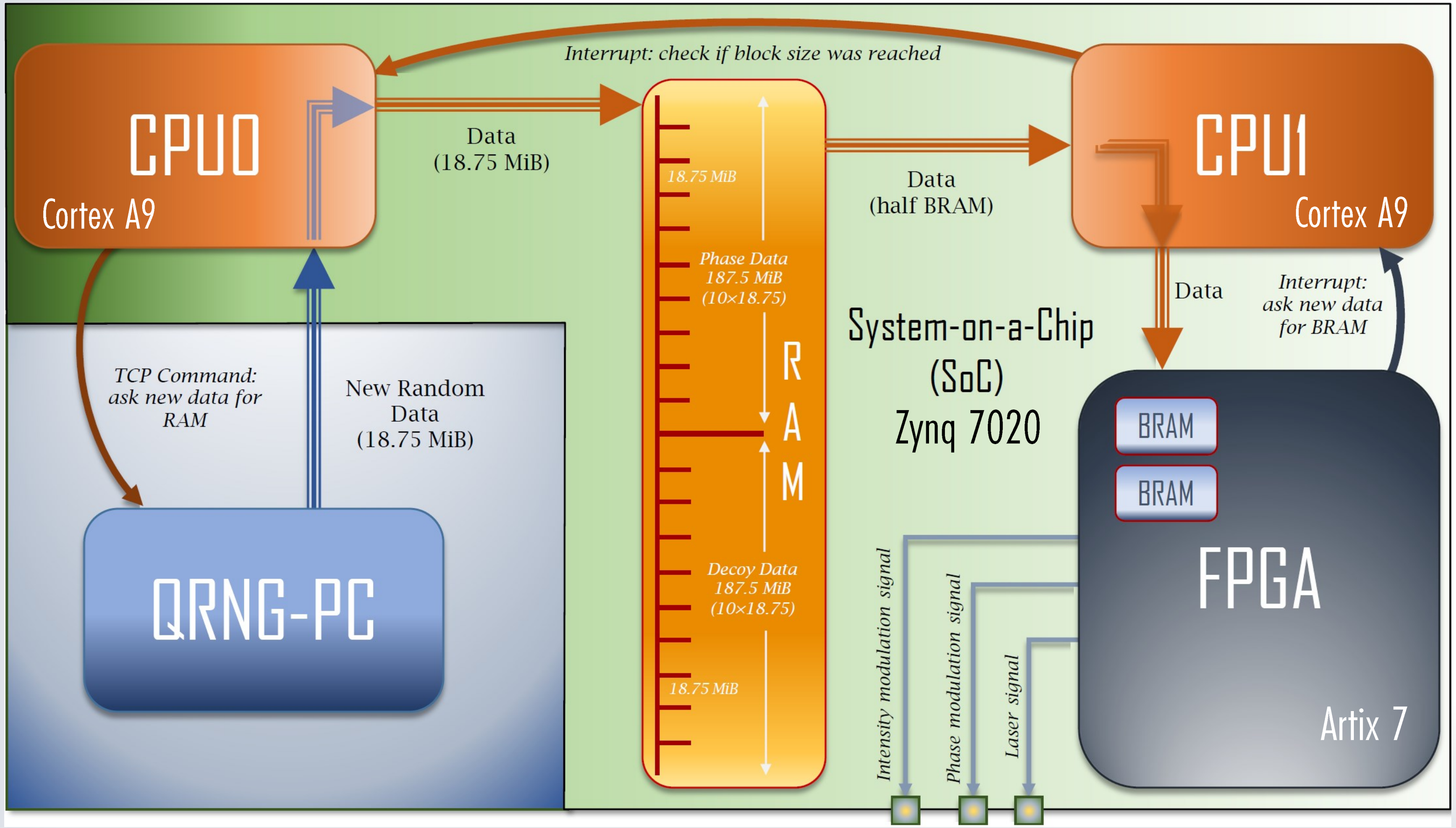
FPGA layer is used only for high speed and deterministic functions (e.g., generating pulse for triggering laser and electro-optical modulators)

CPU layer is used for commands, parameters, and for communication with the outside world

Data transfer to (from) the FPGA is handled with BRAM memories and interrupts



SYSTEM-ON-A-CHIP VERSATILITY



- Dual Core capabilities of the SoC to sustain a **continuous** stream from an external source (QRNG or PC)
- TCP connection (1 Gbit/s nominal speed)
- Blocks structure in BRAM and RAM + interrupt routines and TCP commands

SYSTEM TEST

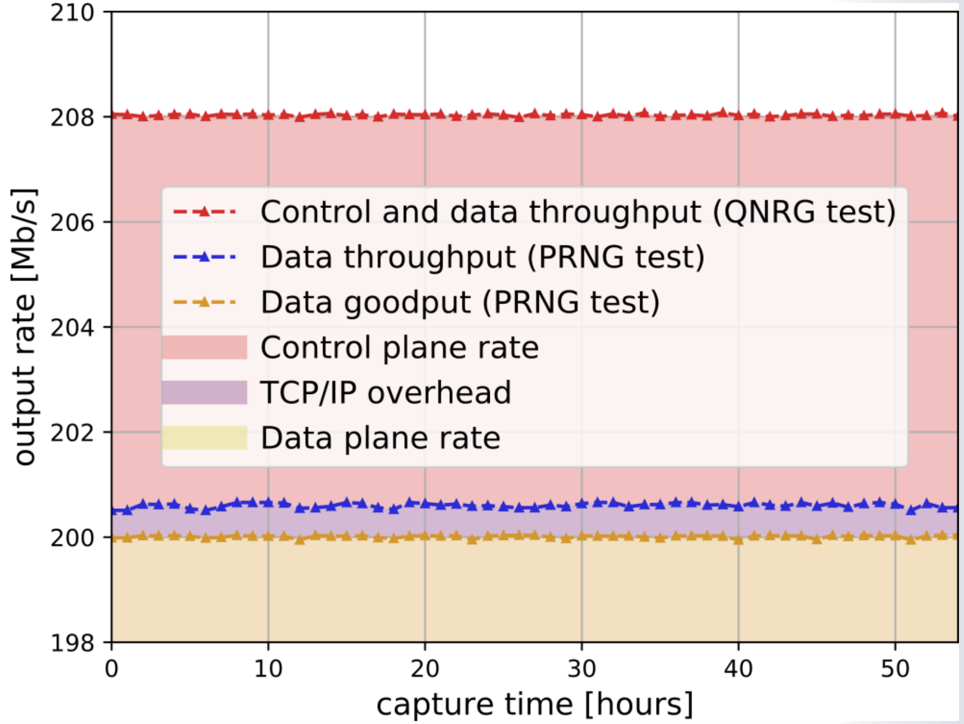
Qubit rate = 50 MHz; 4 bit for each qubit

Tested with a QRNG device able to provide >200 Mbit/s of true random numbers

Stable communication over 55 hours

Graph data includes control messaging, TCP overhead and a second test with a PRNG

Architecture used in several QKD/QRNG experiments



SOC-SYSTEM TRACK RECORD

Breadboard model for Satellite QKD

- F. Berra et al., "Modular source for near-infrared quantum communication", arXiv preprint, 10.48550/ARXIV.2301.12882
- A. Balossino et al., "SeQBO—A miniaturized system for quantum key distribution," in Proc. 71st Int. Astronaut. Congr., vol. 2020, Oct. 2020, Art. no. 166680. [Online]. Available: http://iafastro.directory/iac/paper/id/59867/summary/

Delayed-Choice experiment expanded to Space Scale

- F. Vedovato et al., "Extending wheeler's delayed-choice experiment to space," Sci. Adv., vol. 3, no. 10, 2017, Art. no. e1701180

Free space daylight QKD demonstration

- M. Avesani et al., "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics", npj Quantum Information (2021)7:93

Discrete Variable QRNG

- A. Stanco et al., "Efficient random number generation techniques for CMOS single-photon avalanche diode array exploiting fast time tagging units," Phys. Rev. Res., vol. 2, Jun. 2020, Art. no. 023287

SOC-SYSTEM TRACK RECORD

Pognac/iPognac encoders

- M. Avesani et al., "Stable, low-error, and calibration-free polarization encoder for free-space quantum communication," Opt. Lett., vol. 45, no. 17, pp. 4706–4709, Sep. 2020
- C. Agnesi et al., "All- fiber self-compensating polarization encoder for quantum key dis- tribution," Opt. Lett., vol. 44, no. 10, pp. 2398–2401, May 2019

Fiber-based QKD

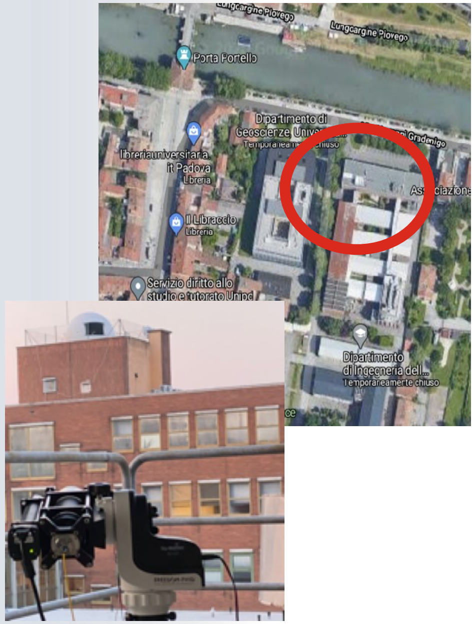
- D. Scalcon et al., "Cross-Encoded Quantum Key Distribution Exploiting Time-Bin and Polarization States with Qubit-Based Synchronization", *Adv Quantum Technol.* 2022, 5, 2200051.
- C. Agnesi et al., "Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder," Optica, vol. 7, no. 4, pp. 284–290, Apr. 2020

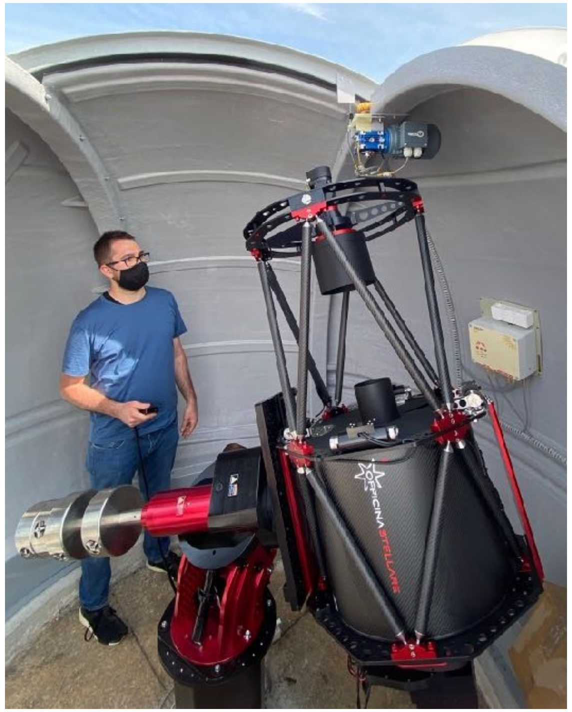
Urban QKD fiber demonstrations

- M. Avesani et al., "Deployment-Ready Quantum Key Distribution Over a Classical Network Infrastructure in Padua," in Journal of Lightwave Technology, vol. 40, no. 6, pp. 1658-1663,2022
- M. Avesani et al., *"Resource-effective quantum key distribution: a field trial in Padua city center," Opt. Lett. 46, 2848-2851 (2021)*

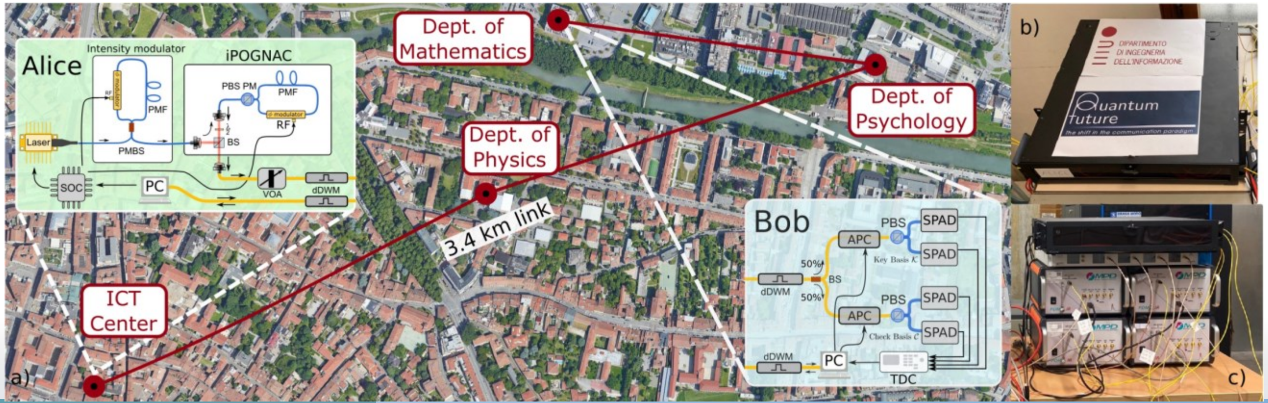
High-speed QRNG
Efficient QKD-RX

UPCOMING RESULTS





- Recent installation of a **Telescope** on Department's roof:
  - 40 cm - class telescope, adaptive optics focalplane
  - from visible, 780-850nm, up to 1600 nm wavelength range
  - fiber connected to ground network
  - different detection protocols
- Recent QKD **Demonstrations:**
  - M. Avesani et al., *Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics*, npj Quantum Information (2021)7:93 (in collaboration with ASI and Scuola Superiore Sant'Anna)
  - M. Avesani et al., *Deployment-Ready Quantum Key Distribution Over a Classical Network Infrastructure in Padua*, Journal of Lightwave Technology, vol. 40, no. 6, pp. 1658-1663, 15 March15, 2022, doi: 10.1109/JLT.2021.3130447
- Recent founded University Spin-off (**ThinkQuantum**) and University Quantum Technology Center (**QTech Center**)



andrea.stanco@unipd.it
paolo.villoresi@unipd.it
giuseppe.vallone@unipd.it
quantumfuture.dei.unipd.it
qtech.unipd.it
thinkquantum.com

THANK YOU FOR YOUR ATTENTION

Andrea Stanco, Francesco Bruno Leonardo Santagiustina, Luca Calderaro, Marco Avesani, Tommaso Bertapelle, Daniele Dequal, Giuseppe Vallone and Paolo Villoresi

Versatile and concurrent FPGA-based architecture for practical quantum communication systems,
IEEE Transactions on Quantum Engineering, vol. 3, pp. 1-8, Art no. 6000108 (2022)

Università degli Studi di Padova

Department of Information Engineering
University of Padova

Agenzia Spaziale Italiana

ThinkQUANTUM

Quango
H2020
GA 101004341