# A REAL-TIME QRNG-TO-QKD STREAM EXPLOITING FPGA FOR HIGH SECURITY QUANTUM COMMUNICATION

ANDREA STANCO

*DEPARTMENT OF INFORMATION ENGINEERING, UNIVERSITY OF PADOVA, ITALY*

Quantum Science Generation - Trento
4/05/2023

ThinKQUANTUM

UNIVERSITÀ DEGLI STUDI DI PADOVA

Agenzia Spaziale Italiana

Iniziativa sostenuta dalla
Fondazione Cassa di Risparmio di Padova e Rovigo

Nell'ambito del Progetto
Quasar

*andrea.stanco@unipd.it*

# OUTLINE

QKD, QRNG and FPGA

The «QRN2Qubit» system

System test and results

Applications, Urban QKD Demonstration

ThinkQuantum company

*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)

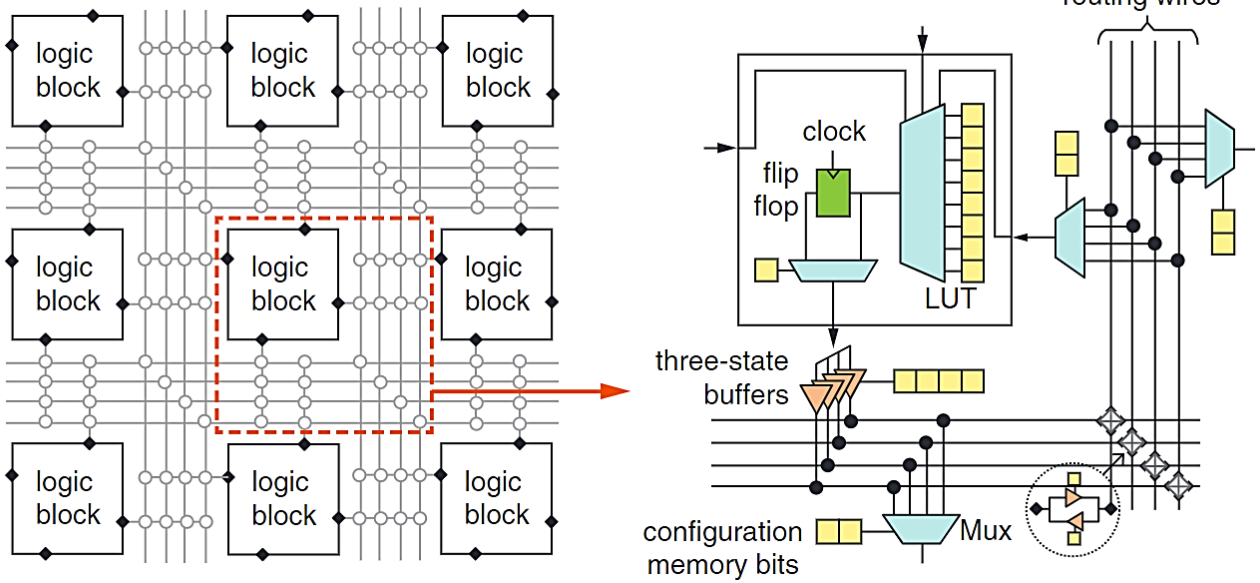
# WHY QKD RELIES ON QRNG?

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

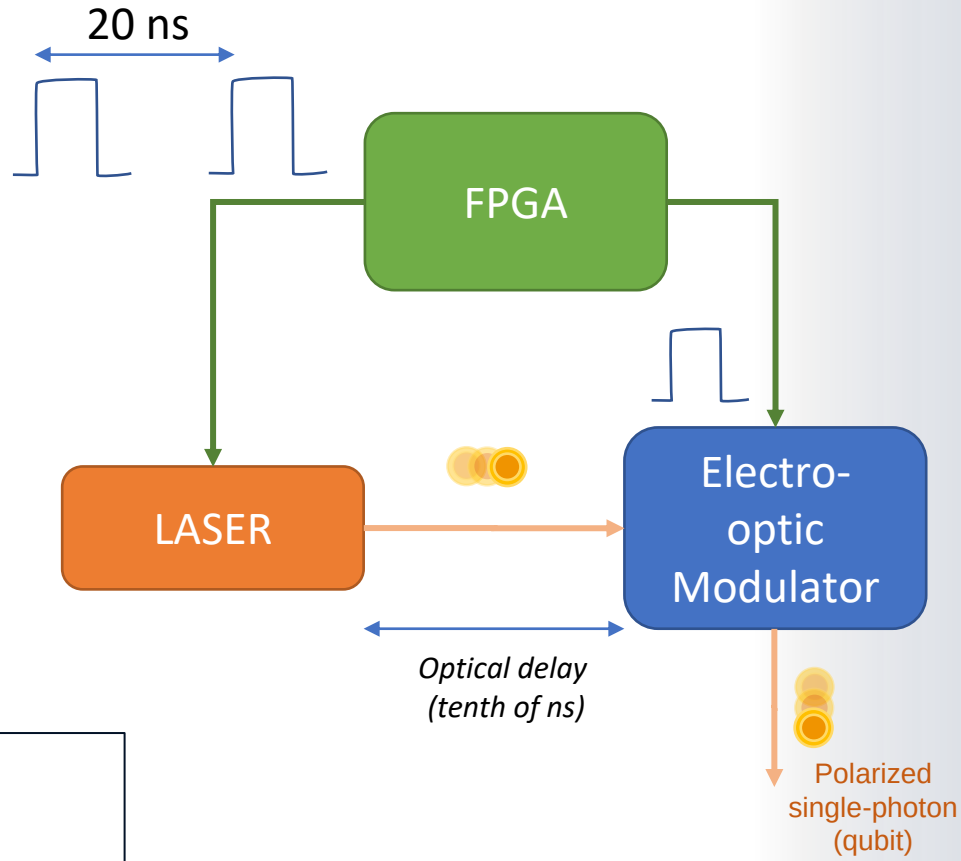
A proper source of randomness (e.g., QRNG) is required to provide the data/qubit sequence

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

# FIELD PROGRAMMABLE GATE ARRAY




*Hubert Kaeslin "Top-Down Digital VLSI Design: From Architectures to Gate-Level Circuits and FPGAs", Morgan Kaufmann, 2014*




- Parallelism
- High speed
- Reconfigurability
- Low Power
- **Determinism!**

# 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 reconfigurability

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** 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 biased strings with efficient BB84)

# 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).

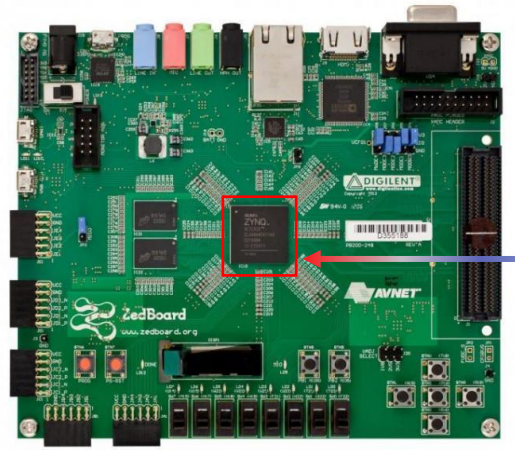
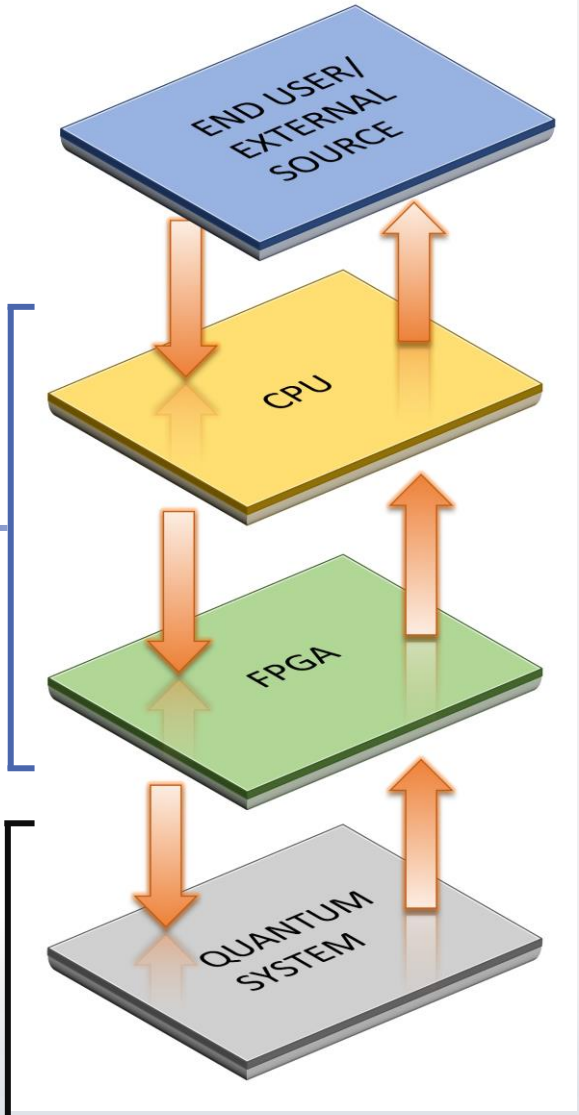



*Figure from avnet.com


*Figures from ixblue.com and excelitas.com



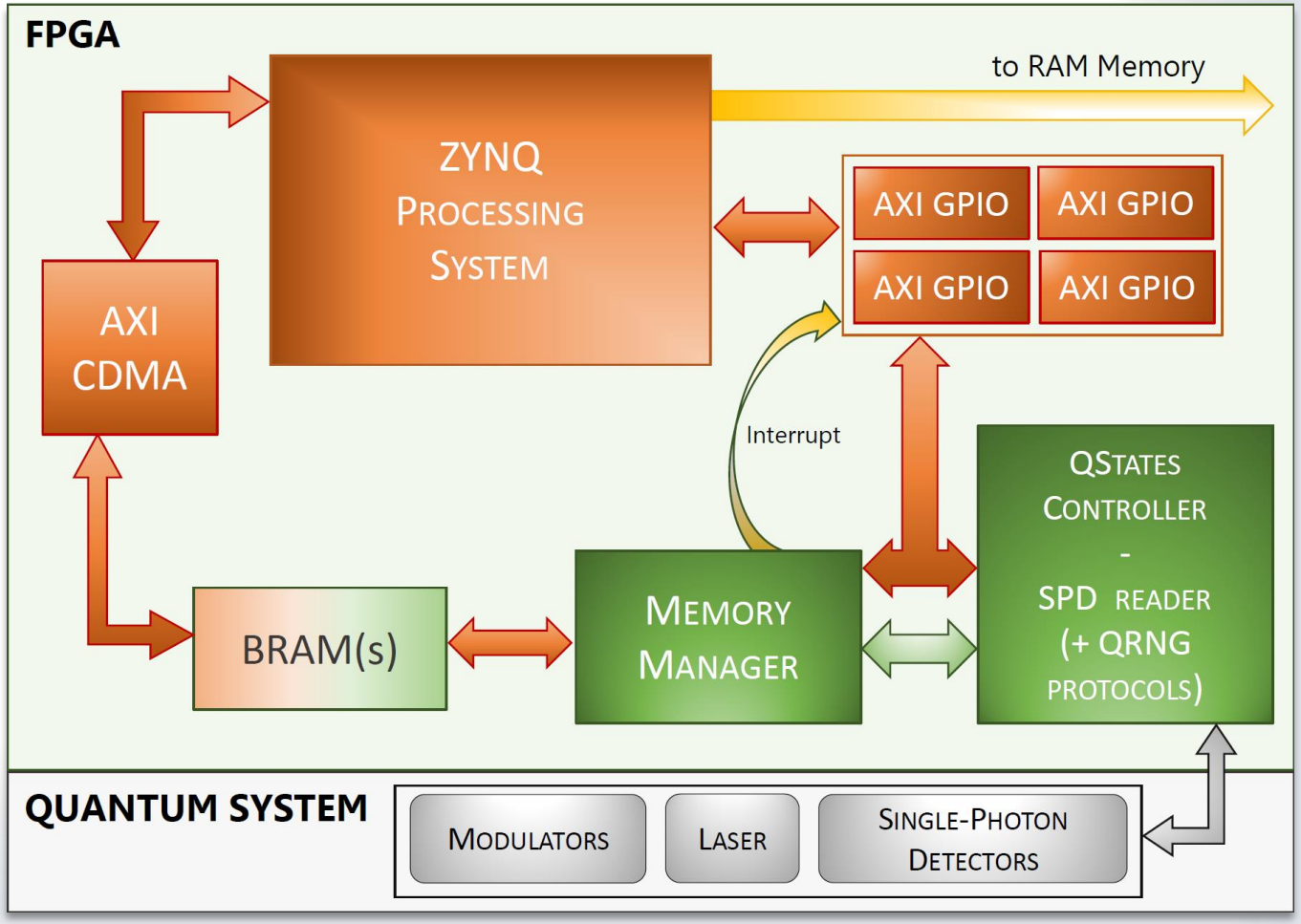
# FPGA-BASED SYSTEM

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

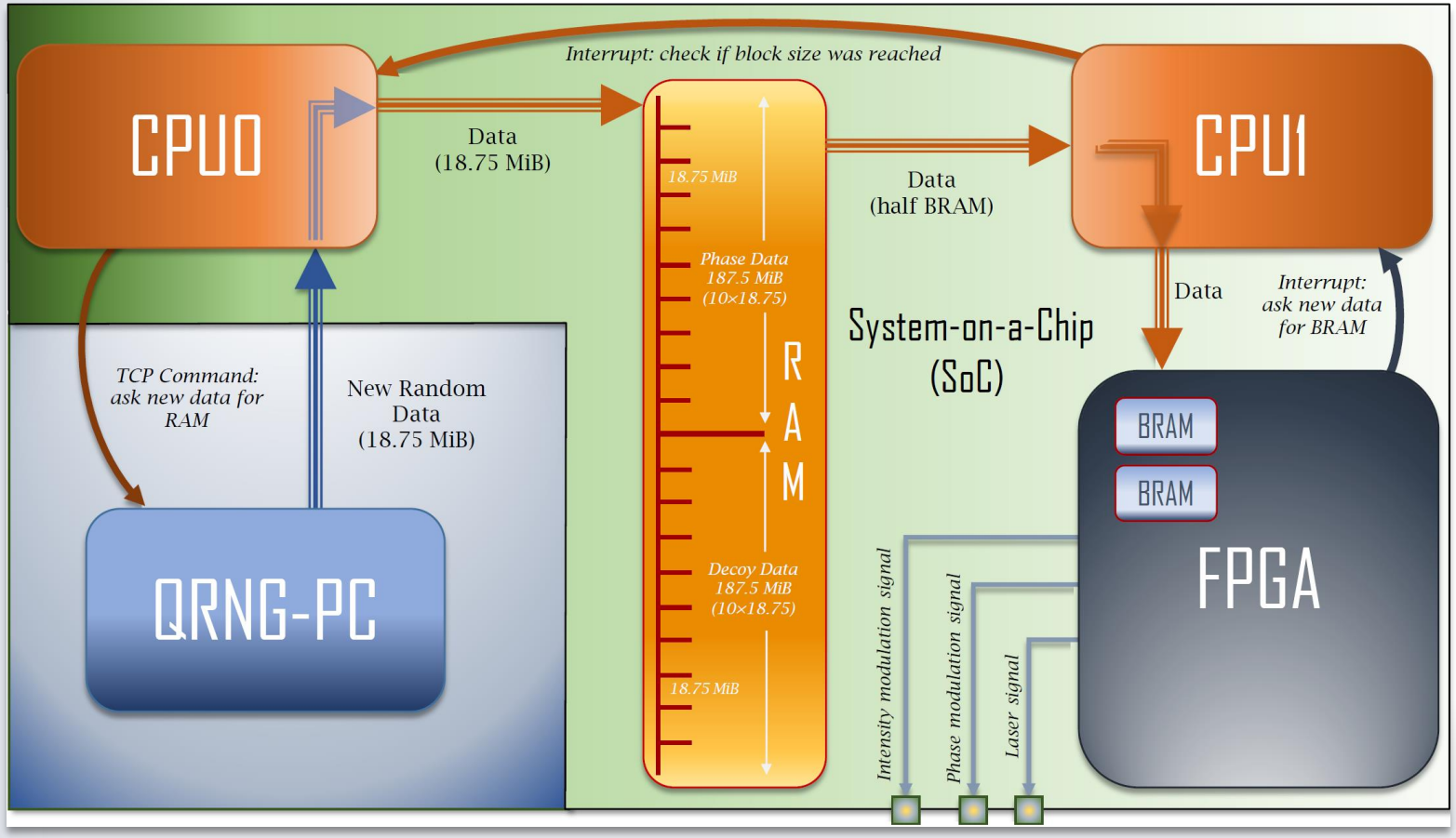
CPU layer is used for commands, parameters, and for communication with the outside world

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

Suitable for **Efficient-BB84** and DV protocols (2-level voltages with **iPognac**). CV protocols require external DAC/ADC

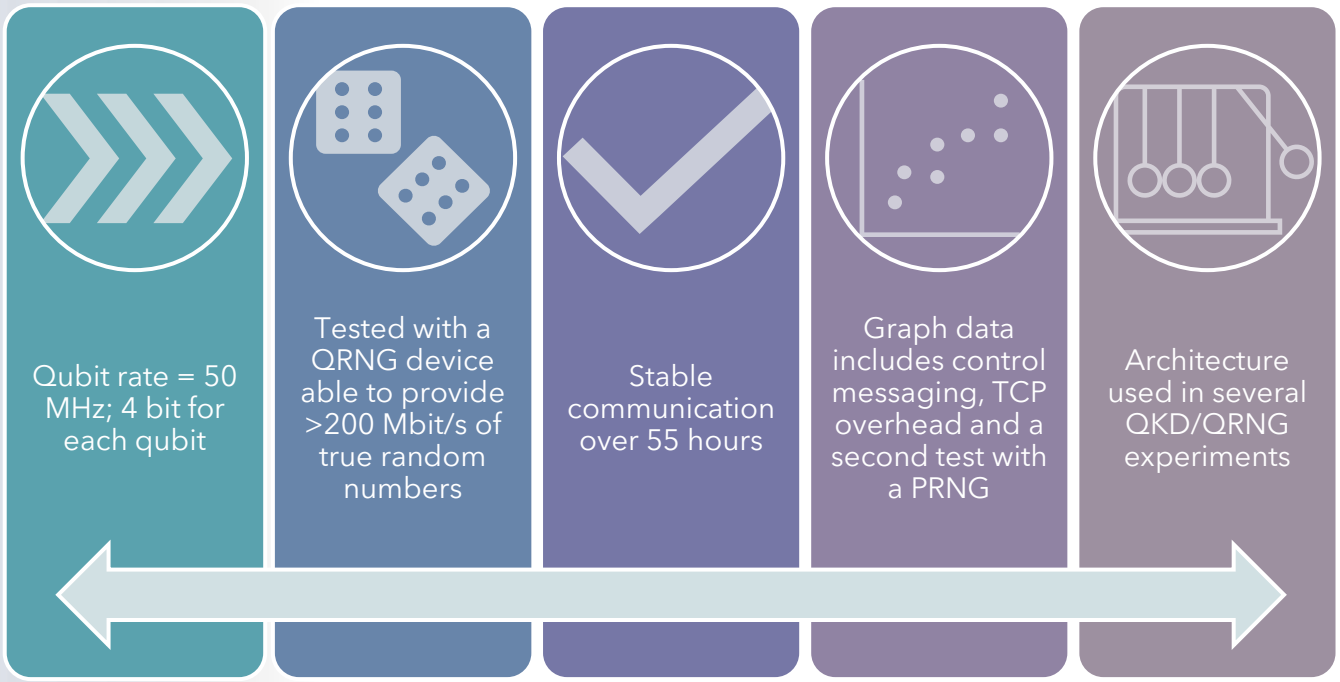


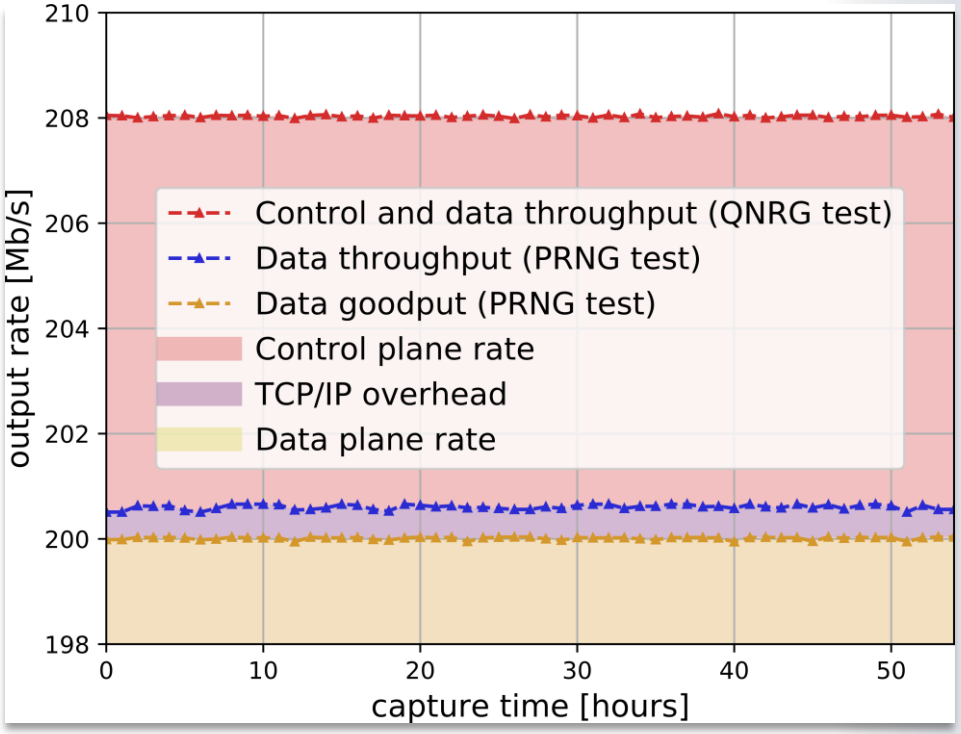
# SYSTEM-ON-A-CHIP VERSATILITY




- 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


output rate [Mb/s]
capture time [hours]
Control and data throughput (QNRG test)
Data throughput (PRNG test)
Data goodput (PRNG test)
Control plane rate
TCP/IP overhead
Data plane rate
210
208
206
204
202
200
198
0
10
20
30
40
50

# 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

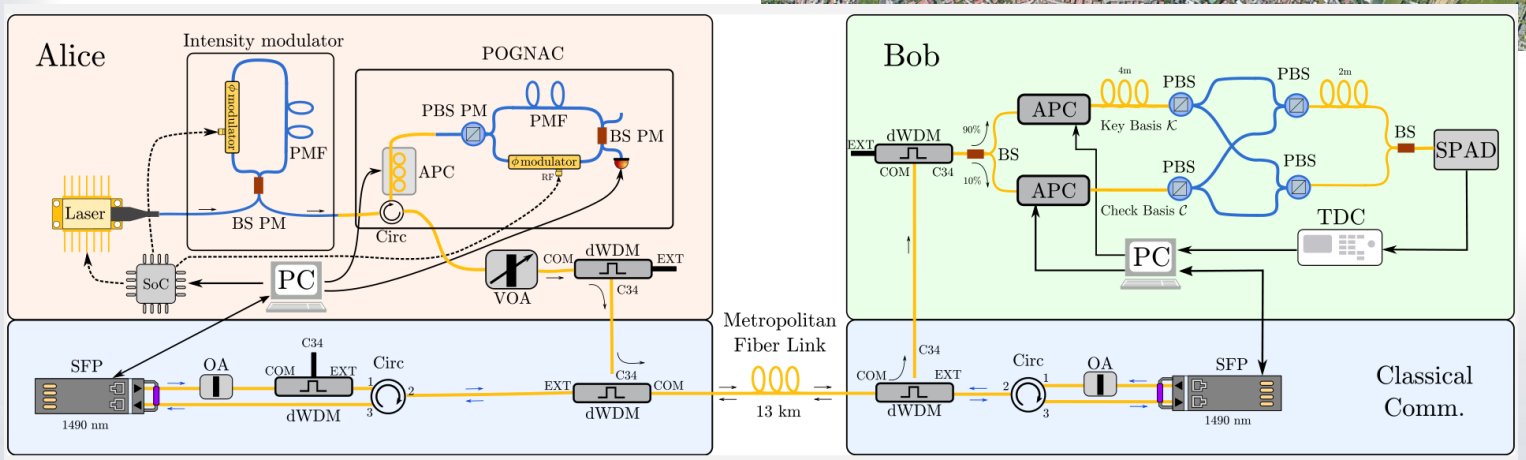
- M. Avesani et al., "Deployment-Ready Quantum Key Distribution Over a Classical Network Infrastructure in Padua," in Journal of Lightwave Technology, vol. 40, no. 6, pp. 1658-1663,2022
- M. Avesani et al., *"Resource-effective quantum key distribution: a field trial in Padua city center," Opt. Lett.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

## Very High-speed QRNG
## Efficient QKD-RX

UPCOMING RESULTS

# URBAN QKD DEMONSTRATION

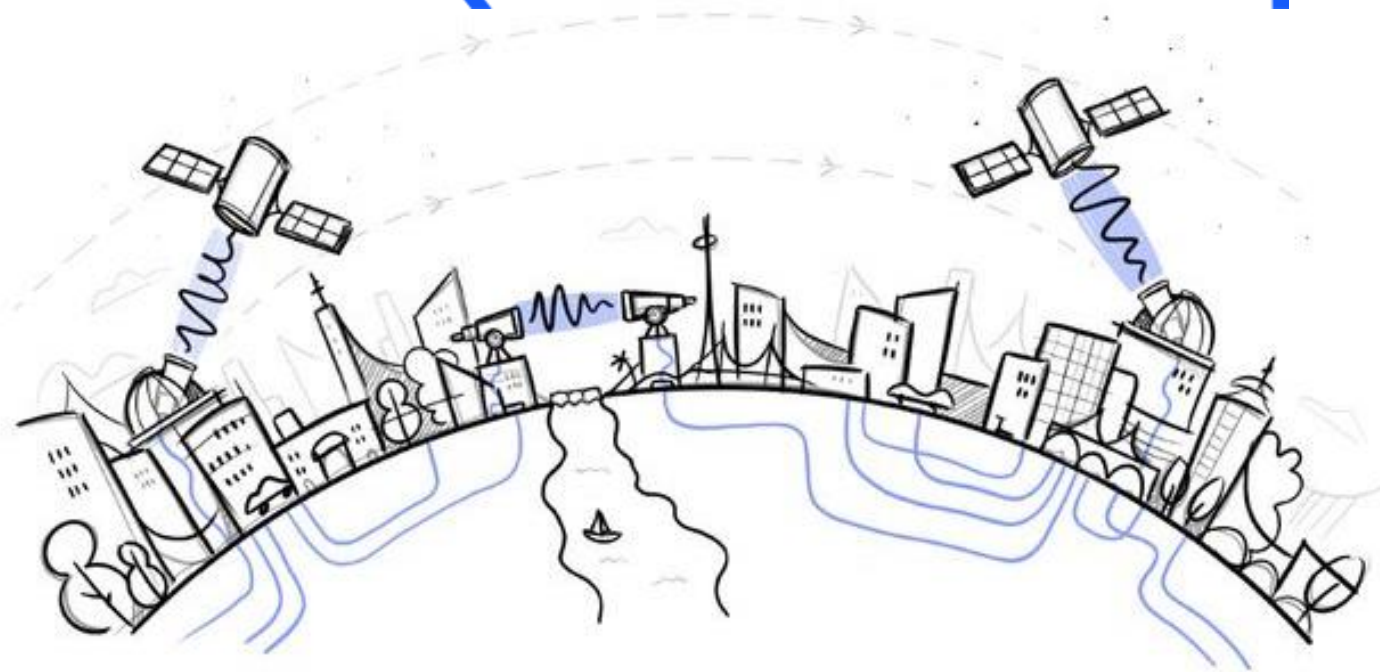
- Both Quantum and Classical Channels on same Fiber (13 km)
- One single photon detector (multiplexing)
- First TQ prototypes


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

# THINKQUANTUM (UNIPD'S SPIN-OFF)

ThinkQUANTUM



**thinkquantum.com**

# THINKQUANTUM – QKD SYSTEM

## FIBER LINK

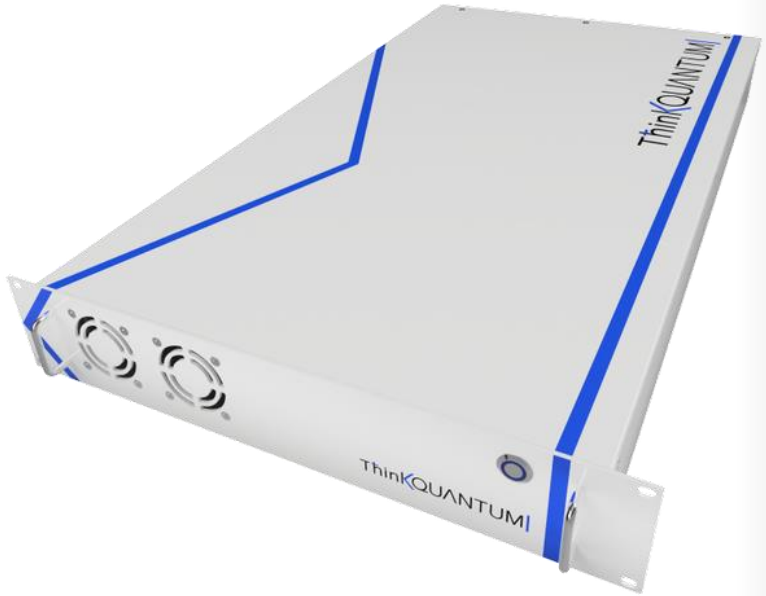
*Communication between fiber-connected sites, typically within the distance of few tents of km*

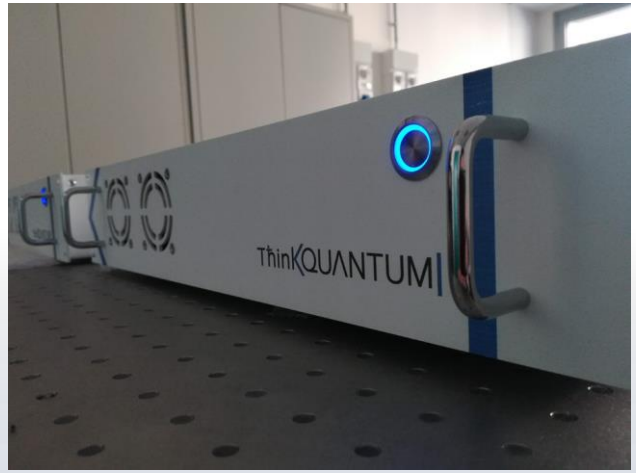
## FREE-SPACE OPTICAL LINK

*Communication between sites that cannot be fiber-connected, temporary or movable nodes.*

## SATELLITE LINK

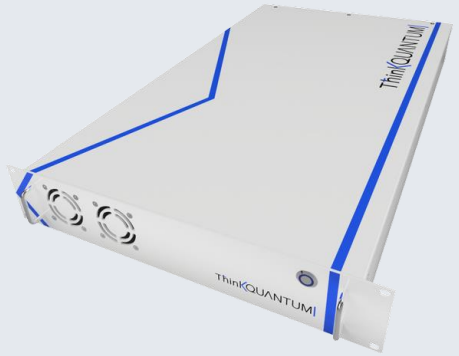
*Satellite-links to cover large distance applications (sat payload & optical ground station)*



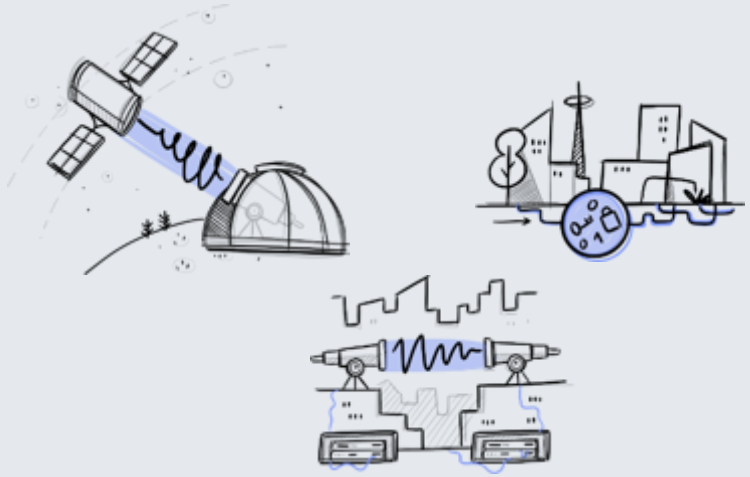



# THINKQUANTUM - QKD SYSTEMS

## ALICE

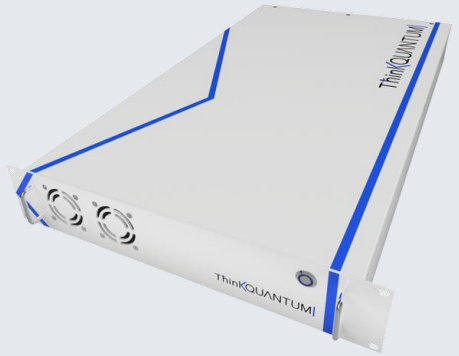



## QRNG

## QUANTUM CHANNEL

## BOB



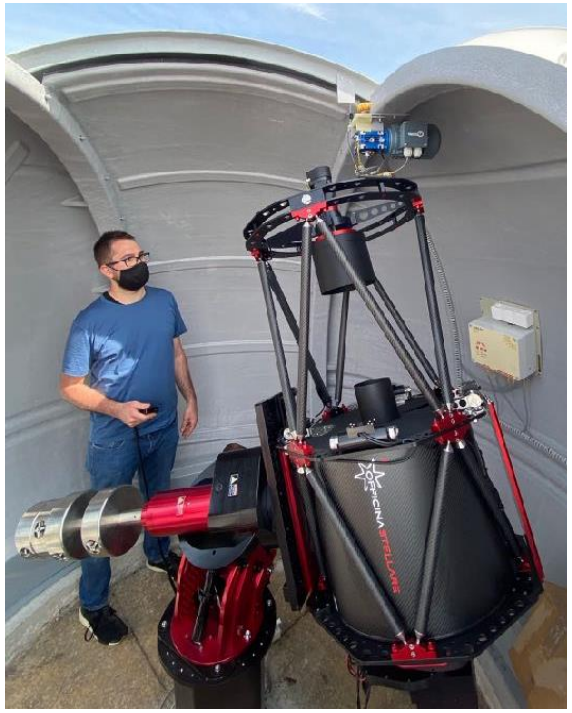
# THINKQUANTUM - PRODUCTS

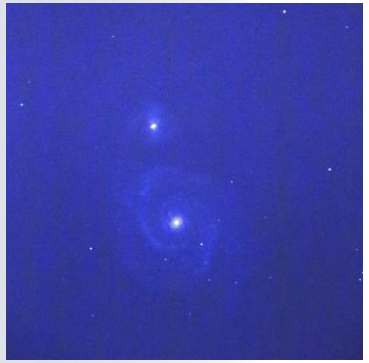

## QuKy

- **QRN2Qubit**
- **Qubit4Sync**
- **iPognac**
- Cross-Channel QKD PLATFORM
- Polarization 3 state efficient BB84 decoy
- SKR = 2.2 kb/s (13 dB) [typ]
- Max Losses: Standard 20dB (100 km , 0.2 dB/km)

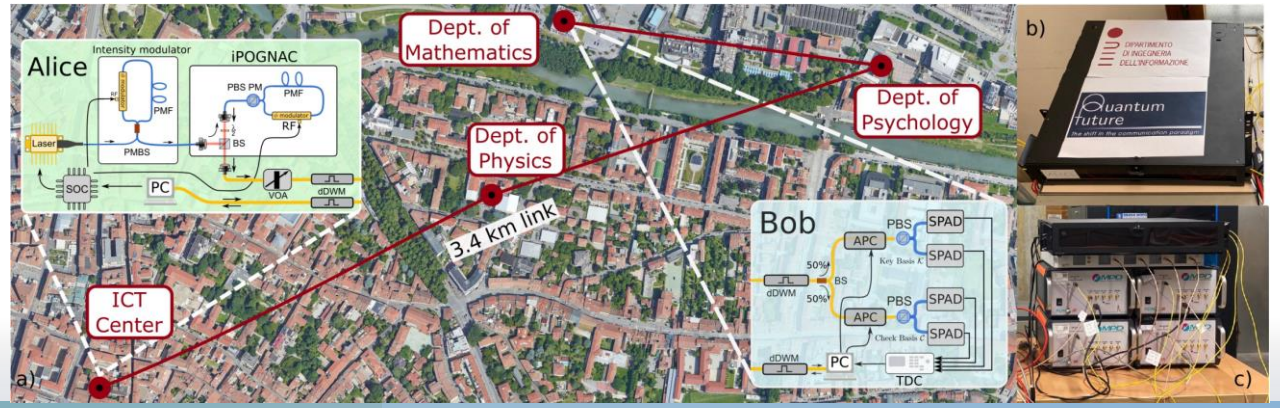
## ThiKe

- **High-rate** (330 Mbps secure random bit rate)
- **Source-device independent**
- **Real time randomness extraction on hardware**



- 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

ThinkQUANTUM

Agenzia Spaziale Italiana

Iniziativa sostenuta dalla

Fondazione Cassa di Risparmio di Padova e Rovigo

Nell'ambito del Progetto

Quasar