# FPGA-based streaming architecture for high-security Quantum Communication


Andrea Stanco [1,*], Francesco B. L. Santagiustina[1], Luca Calderaro[2], Marco Avesani[1], Tommaso Bertapelle[1], Daniele Dequal[3], Giuseppe Vallone[1,4], and Paolo Villoresi[1]

[1] Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, 35131, Padova, Italy
[2] ThinkQuantum S.r.l., 36030 Sarcedo, Italy
[3] Unità Telecomunicazioni e Navigazione, Agenzia Spaziale Italiana, 75100 Matera, Italy
[4] Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, 35131 Padova, Italy



## SUMMARY

We present an FPGA-based architecture implemented on a Zynq7020 chip for Quantum Communication applications [1]. The architecture fully exploits the FPGA/CPU duality of the System-on-a-Chip (SoC) and can be adapted to work as a control system for Quantum Key Distribution (QKD) transmitter, as a readout system for QKD receiver and as a system for Quantum Random Number Generation (QRNG). Over the year, this architecture was used in different Quantum Communication experiments by the QuantumFuture group [2-5]. Furthermore, the dual core capability of the Zynq7020 was exploited to implement a continuous stream (through a TCP connection) for a high-level security QKD system. As a matter of fact, a proper QKD transmitter should be provided with a true random string of data in order to make the transmitted qubit sequence fully random (this prevents an attack on the non-randomness of the qubit sequence). The full system (QRNG+QKD tx) was tested with a qubit rate of 50 MHz and a continuous stream of 200 Mbps.


## QUANTUM KEY DISTRIBUTION (QKD)

- QKD allows to reach Unconditional Security thanks to the law of Quantum Mechanics
- Works with the qubit instead of the classical bit
- Can be implemented exploiting quantum properties of light (single photon)

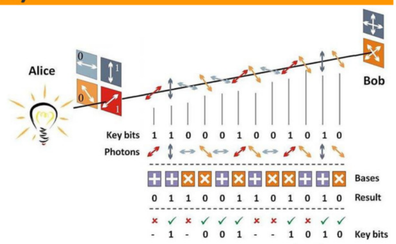



*Figure from doi: 10.1007/978-3-319-30201-0_27

## QUANTUM RANDOM NUMBER GENERATION (QRNG)

- 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

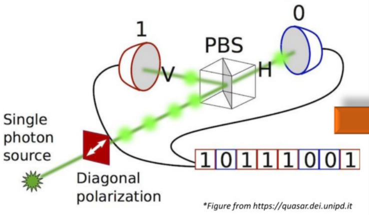



*Figure from https://quasar.dei.unipd.it

## FPGA-BASED SYSTEM

- Overview of the 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).

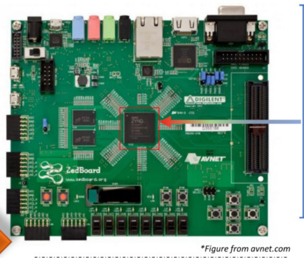


*Figure from avnet.com

*Figures from ixblue.com and excelitas.com

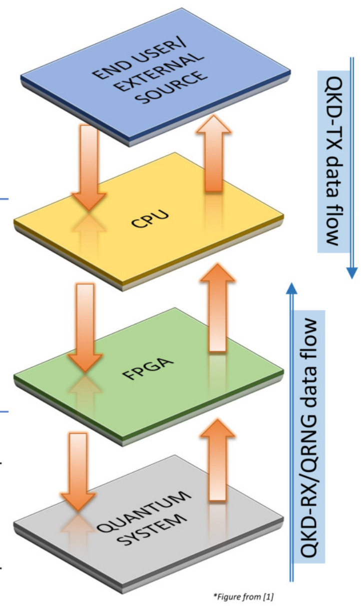
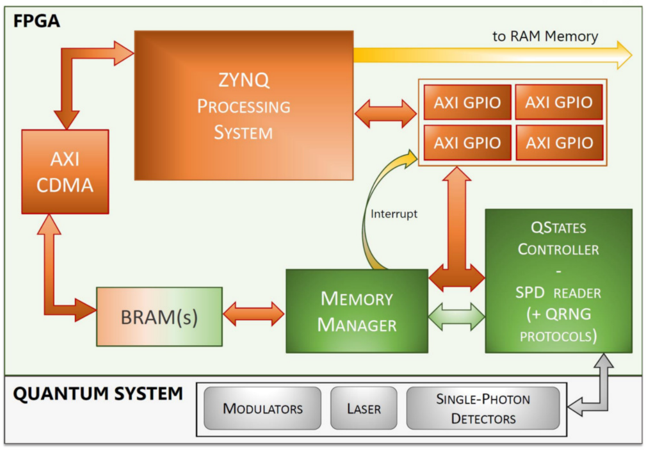



*Figure from [1]

- 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

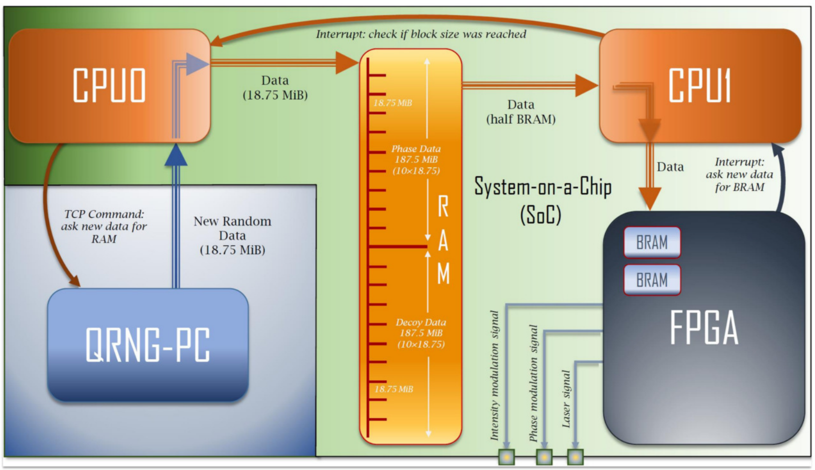
*Figure from [1]




## QKD-QRNG DUAL CORE SYSTEM WITH CONTINUOUS STREAM

- 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

*Figure from [1]





## REFERENCES

[1] 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).
[2] F. Vedovato et al., *Extending wheeler's delayed-choice experiment to space*, Sci. Adv., vol. 3, no. 10, 2017, Art. no. e1701180
[3] 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
[4] 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
[5] 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




*andrea.stanco@unipd.it