Master in Photonics – "PHOTONICS BCN"
Master ERASMUS Mundus "EuroPhotonics"

MASTER THESIS PROPOSAL

Dates: April 2023 – July or September 2023

Laboratory: Optoelectronics
Institution: ICFO
City, Country: Barcelona, SPAIN

Title of the master thesis: "Design and characterization of a FPGA-based sub-nanosecond resolution time-tagger for Quantum Key Distribution experiments"

Name of the master thesis supervisor and co-supervisor: Valerio Pruneri / Lorenzo Castelvero
Email address: lorenzo.castelvero@icfo.eu
Phone number: +34 93 553 4002
Mail address: ICFO - The Institute of Photonic Sciences / Av. Carl Friedrich Gauss, 3 / 08860 Castelldefels / Barcelona - SPAIN

Keywords: Quantum Key Distribution (QKD); Single Photon Detection; FPGA; Time-tagging

Summary of the subject:

Secure communications are of paramount importance in the increasingly globalized world. The standard cryptographic methods holding Computational-Security (such as RSA) are vulnerable to disruptive advancements in machine computational power and to the potential development of a key-breaking algorithm. In particular, it has been shown that quantum computers, which are expected to become commercially available in the next decade, will be able to efficiently solve the prime factorization and discrete logarithm problems upon which the most widely-used cryptographic protocols are based [1]. Quantum Key Distribution (QKD) encompasses a family of protocols that exploits the physics of quantum mechanics to ensure that cryptographic keys generated by these means are uncompromised by ``eavesdropping'' adversarial parties [2] allowing remote users to achieve information theoretically-secure communication in a practical way. QKD has been widely implemented in both fiber experiments [3] and also in satellite-to-ground demonstrations [4] in the last decade. To enable a high enough cryptographic key generation rate to support encrypted communications in real time the demonstration of practical implementations of QKD requires devices GHz symbol repetition rate presenting robust designs.

At ICFO, we are developing a QKD system based on a self-stabilized polarization state transmitter. The device is conceived in such a way as to be robust against temperature changes and mechanical vibrations. A mating receiver is designed and constructed to properly match the transmitter characteristics. In such communication systems, the employed receivers should guarantee an efficient acquisition of the arrival time of single photons (time-tagging). Thanks to their high performance, low development costs and short time to market, field-programmable gate arrays (FPGA) are attractive for many applications, including the implementation of time-to-digital converters (TDCs) [4].
In this project we propose one or more of the following tasks:

- Characterization [5] and hardware optimization of the FPGA-based multi-channel TDC currently used for the QKD receiver. Possible development of a GUI for control and analysis of the TDC.
- In-lab or field QKD experiments with the TDC. As part of the work, the integration of the different building blocks required for the QKD receiver will be carried out (Single photon detectors, polarization stabilization units, polarization detection optoelectronics, etc).
- Design of alternative FPGA-based TDCs with state-of-the-art performance (ps resolution and Mcps count rate) for use in future experiments. Comparison of different implementation strategies and development platforms.

Given the above possibilities, the specific content of the project will be consolidated according to the interest and background of the candidate.

Objectives:

- Study the state of the art of practical QKD implementations
- Get familiar with experimental aspects of QKD and FPGA development environments
- Development and integration of a FPGA-based TDCs for the QKD receiver
- Perform in lab or field QKD experiments using the developed devices
- Documentation of the results in a written form

Additional information:
Required skills:

- Experimental experience in quantum mechanics and photonics desirable
- Experience in development with FPGA-based systems-on-chip and HW/SW co-design desirable (Verilog, VHDL, device driver design, Linux environment)
- Solid programming skills (e.g. Python, Matlab or C++)

[1] Rivest, Ronald L., Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems." *Communications of the ACM* 21.2 (1978): 120-126.
[2] Bennett, Charles H., and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." *arXiv preprint arXiv:2003.06557* (2020).
[3] Grande, IH Lopez, et al. "Adaptable transmitter for discrete and continuous variable quantum key distribution." *Optics Express* 29.10 (2021): 14815-14827.
[Liao2017] Liao, Sheng-Kai, et al. "Satellite-to-ground quantum key distribution." *Nature* 549.7670 (2017): 43-47.
[4] R. Machado, J. Cabral and F. S. Alves, "Recent Developments and Challenges in FPGA-Based Time-to-Digital Converters," in *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 11, pp. 4205-4221, Nov. 2019, doi: 10.1109/TIM.2019.2938436
[5] Dadouche, F. & Turko, Timothé & Skilitsi, Anastasia & Malass, Imane & Uhring, Wilfried & Leonard, Jeremie. “Design, Implementation and Characterization of Time-to-Digital Converter on Low-Cost FPGA.” 2016