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

MASTER THESIS PROPOSAL

Dates: April 2021 - September 2022

Laboratory: -
Institution: Quside
City, Country: Castelldefels (Barcelona), Spain

Title of the master thesis: Quantum random number generation using polarization switching in VCSELs

Name of the master thesis supervisor and co-supervisor:
(for external proposals a co-supervisor from the Master program in needed)
Email address: mrude@quside.com
Phone number: +34 934 314 796
Mail address: Quside Technologies S.L., C/Esteve Terradas 1, Of. 304, 08860 Castelldefels (Barcelona)

Keywords: Optics, Quantum random number generation, Laser physics

Summary of the subject (maximum 1 page):

The rapid spreading of Internet of Things (IoT) applications where millions of devices are connected and data is shared across multiple platforms, has created new security problems which are crucial for IoT implementation and wide adoption. This unique technological evolution has posed the priority in implementing stronger cryptographic systems adapted to the IoT device needs.
Currently, data transmissions are protected by cryptographic algorithms based on keys generated by random number generators (RNGs). To be secure, the key must be unpredictable. The higher the randomness of the generated sequence, the harder to break it for an eavesdropper. Many methods have been presented to realize true (hardware based) random number generators (TRNG) to replace pseudo-RNGs (PRNGs)[1], which are based on a deterministic algorithm generated by a computer and thus having repetitive occurrence and patterns. A hardware based RNG, instead, is based on physical noise sources based on

[1] P. Lacharme, A. Rock, V. Strubel, and M. Videau, "The Linux Pseu- ¨ dorandom Number Generator Revisited," International Association for Cryptologic Research, pp. 1–23, 2012.

classical or quantum physics: thermal noise, atmospheric noise, shot noise, radioactive decay, and so on. However, TRNGs based on classical physics, e.g. free running oscillators, are black boxes where deterministic processes run in an uncontrolled and chaotic manner, thus it is not possible to guarantee that an attacker could not manipulate, force or predict the output from a classical TRNG. The only way to produce true and unbreakable randomness is to utilize fundamentally unpredictable processes and understand and validate such physical process by which the randomness is generated.

Quantum random number generators (QRNGs) are a particular case of physical TRNG, where the data is the result of a quantum event, thus unpredictable by nature. Quantum mechanics offers true fundamental randomness which is not based only on a lack of detailed information. The goal in quantum random generators is to utilize set-ups where this fundamental randomness arises in ways that are easy to describe and quantify. Only quantum sources can provide the randomness necessary to realize truly secure encryption systems as well as improved randomized algorithms.

The aim of this thesis is to develop a cost effective, scalable QRNG integrated in a standard electronic package based on vertical cavity surface emitting lasers (VCSELs). In particular, the work will focus on improving the existing optical set-up to characterize and analyse polarization dynamics in directly modulated VCSELs and comparing the results with simulations (Monte Carlo) based on the spin-flip model.
Emphasis will be put on understanding (both theoretically and experimentally) the different regimes of the VCSEL dynamics to find out the most appropriate for quantum random number generation. Moreover, the quality of the generated random numbers will be analyzed using different randomness tests. Finally, the integration roadmap in standard electronic package will be defined.

Additional information (if needed):
* Required skills: Knowledge of optics and physics, Programming (Python/C++)
* Miscellaneous: English