Quantum Random Number Generation in low-cost mobile hardware

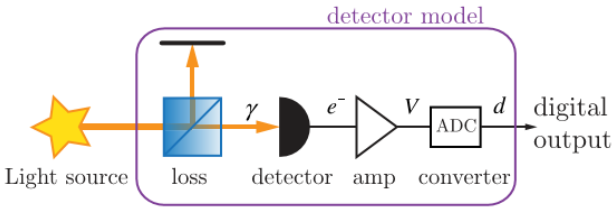
LiU Master Thesis Proposal

Kvantek Systems is a UK-based early stage start-up company which aims to develop a quantum enhanced encryption chip for mobile and Internet of Things (IoT) devices. One constituent component is a quantum random number generator (QRNG) which provides 'true' random numbers to classical encryption protocols in order to improve the strength of their security.

With some estimates predicting that up to 50 billion new connected devices will be in use by 2020, we believe that securing the IoT will be one of the key technological challenges over the next coming years. This therefore also represents a substantial commercial opportunity.

The proposed Master Thesis project involves building and evaluating a proof of concept (PoC) QRNG using low-cost, off-the-shelf, electronic components such as mobile phone parts and mircoprocessors. The results of the evaluation will be used for research grant and venture capital funding proposals.

The basis for the technology can be found in a paper published by Sanguinetti et al (2014)[1], and uses a light source to illuminate a CMOS camera sensor taken from a standard smartphone. The arrival rate of photons on the sensor is a quantum mechanical process and therefore governed by a statistical distribution. This stochastic process is used as a source of entropy for the random number generation by extracting the byte values of each pixel of the sensor and then applying hashing algorithms to that byte stream.



A key metric for measuring the quality of a RNG is its output entropy, and another one is its throughput. These two metrics are particularly interesting because it can be reasonably assumed that there exists a trade-off between them, such that a higher quality can be achieved by reducing the throughput and vice versa. We should therefore be able to evaluate design choices on how well they optimise this trade-off.

The PoC project involves designing and building a test harness with interchangeable light sources and sensors as well as an off-the-shelf microprocessor (e.g. an Arduino or Raspberry Pi). This architecture will allow for the evaluation of various components as well as for tests with different configurations and algorithms in order to find an optimal outcome.

The project would suit an entrepreneurial MSc student with an interest in quantum physics, electrical engineering and cryptography and will be carried out at LiU in cooperation with Kvantek. There may be possibilities for continued involvement at the end of the project.

[1]Sanguinetti, Bruno, et al. "Quantum random number generation on a mobile phone." *Physical Review X* 4.3 (2014): 031056.