In today's hyper-connected world, most of our communications with friends, colleagues are now virtual. Without even realizing, all these communications are encrypted in order to protect our privacy. One of the main encryption protocols used today is the asymmetric encryption scheme. In this scheme, Alice generates two keys : one public that is used by Bob to encrypt his message, one private (i.e. known only by Alice) to decrypt the message. The security of such a protocol is based on the difficulty to retrieve the message without the private key. If an eavesdropper can get access to the keys generated by Alice, the protocol becomes completely unsecure. It is therefore necessary for Alice to have access to a random number generator (RNG) in order to generate cryptographically secure keys for her communications with Bob.

What is a RNG ?

A RNG is a device that produce a perfectly unpredictable and unbiased sequence of numbers. However, building such a device can be a tricky business. Indeed, producing randomness out of nothing via mathematical methods is impossible.

"*Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.*", John Von Neumann

Quantum Communications for ALL (QCALL) is a European Innovative Training Network (project 675662) funded by the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015.

In order to produce genuine randomness, it is necessary to have a source of entropy to generate a seed from which we can extract the randomness. Currently, most RNGs used as entropy source a stochastic process to produce randomness. The drawback of these devices is that they are not provably secure. Indeed, their outcome can appear random but in theory, a sufficiently precise description of the system could allow to predict the future outcome.

The appearance of randomness is indeed not a proof of the unpredictability. For example, the digits of pi do appear random but can be perfectly predicted.

‘Quantum’ to the rescue

To overcome this limitations, people started to investigate quantum phenomena. As shown experimentally with the violation Bell inequalities, quantum processes are, by nature, probabilistic. Thanks to this intrinsic property, quantum processes are ideal candidates to build an entropy source. Many implementations have been proposed over the years with entropy rates reaching tens of GHz. However, these often require specific components that could hamper there commercial development in the near future.

Toward a chip-based QRNG

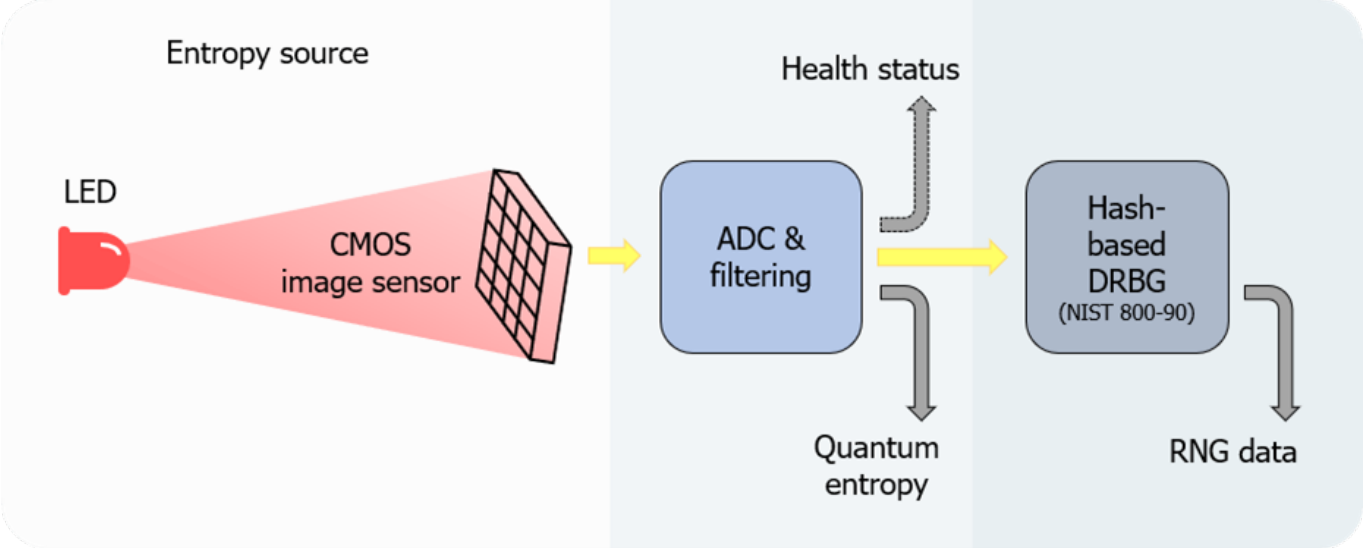
Although some implementations offer extremely high performances in terms of entropy rate, they require the use of specific

These components have many advantages. They are easy to integrate, cost effective and require low power consumption.

IDQ QNRG chip

In ID Quantique, we exploited this idea to build a fully integrated QNRG chip. The security model of this device is detailed in our paper (https://arxiv.org/abs/2011.14129) where we show that a simple filtering of the bits of the ADC allow us to obtain a near-unity quantum entropy per bit. Moreover, this high quality quantum entropy is very robust against imperfections and fluctuations (e.g. of the LED intensity) making it suitable for its deployment in commercial devices.

Quantum Communications for ALL (QCALL) is a European Innovative Training Network (project 675662) funded by the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015.



This chip is already embedded in Samsung mobile phone marking the beginning of the transition of quantum technologies for laboratories to everyday life.

Quantum Communications for ALL (QCALL) is a European Innovative Training Network (project 675662) funded by the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015.