



QUANTUM RANDOM NUMBER GENERATOR FOR MOBILE PHONE SECURITY

Problem - Challenge

With the advent of ubiquitous internet browsing, purchasing and banking, personal data security is becoming more and more critical.

Solution

Press Release, 14 May 2020: « ID Quantique and SK Telecom Announce the World's First QRNG-Powered 5G Smartphone ».

With its new Quantis QRNG (quantum random number generator) chip, developed by Geneva based ID Quantique, the Samsung Galaxy A Quantum smartphone will allow users to more safely use services like authentication and online payments.

This technology was invented by researchers at the Group of Applied Physics of University of Geneva. In 2014, with the help of their Technology Transfer Office, the researchers filed a patent entitled "Method and Device for Optics Quantum Random Number Generation". The patent family was then licensed to ID Quantique SA.

The working principle of the technology is the following: a light beam is a flow of light particles called photons. The number of photons emitted by a LED in a given time interval is random, by nature.

This fundamental property of the light field is also called "shot noise" or "quantum noise". These photons are captured by a CMOS image sensor which generates a numerical signal. Finally, a "randomness extractor" can then generate perfectly unpredictable random numbers out of this input data.

"This is truly the first mass market application of quantum technologies" said Grégoire Ribordy, CEO of ID Quantique. "With its compact size and low power consumption, our latest Quantis QRNG chip can be embedded in any smartphone. It will bring a new level of security to the mobile phone industry."

To bring this technology to market at this scale, ID Quantique had to industrialize the production significantly. This was achieved with the help of Korean investor SK Telecom.

ID Quantique SA was formed in Geneva in 2001 as a spin-off of the University of Geneva.

