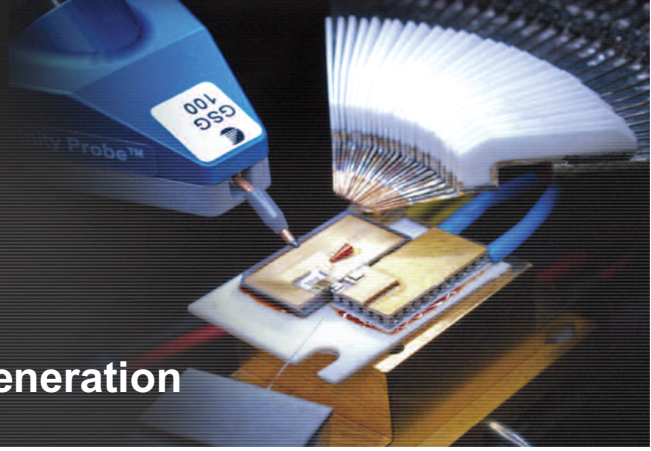


Photonic Integrated Circuits for quantum random number generation

The tremendous growth of the wired and wireless Internet, combined with the cost-effective availability of high-performance micro-electronics processors, has resulted into a humongous increase of inter-networked devices and systems, which are nowadays ubiquitous in all aspects of modern societies. With more and more daily-life activities relying on networked and unattended operation communication devices, *cybersecurity*[1] is of great concern.

Encryption is one of the main primitives in data security, relying on algorithms such as the Advanced Encryption Standard or the Rivest-Shamir-Adleman (RSA). All these algorithms rely on keys generated using *random numbers*. The foreseen developments of ultra-fast computers pose a challenge, since in the coming years they may be able to decipher keys which nowadays are considered strong, i.e., cannot be broken in decades. Hence, with respect to cybersecurity, there is a *need for fast random number generators*, to be able to (re)generate keys faster than computers can break and to deploy new and stronger encryption algorithms. Moreover, fast random number generation finds also applications[2] in simulation and modelling, games and gambling, and random sampling, to name a few.

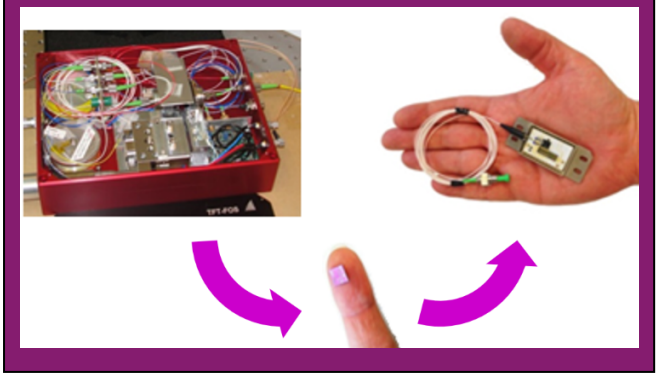
True random numbers can be sampled out of different classical physical phenomena, such as thermal noise and atmospheric processes. However, most are difficult to isolate from correlations that degrade the randomness, therefore resulting in potential security breaches. Furthermore, the rate at which these numbers can be generated is limited, compared to other approaches. On the other hand, random numbers can be harvested from *quantum mechanical* effects. These devices are the so-called quantum random number generators[3] (QRNGs).

A technology that possesses all the ingredients highlighted (truly random and fast effects) is photonics, and in particular *photonic integration* that is amenable for mass manufacturing (ubiquitous). Photonic integration allows for incorporating into a few millimeters square chip all the functions required to generate random numbers based upon quantum effects with photons, such as a laser, passive devices (couplers, delay lines, and hence interferometers) and light detectors.

Photonic Integrated Circuits (PICs)

Also known as optical chips, PICs can contain tens to hundreds of optical components. While electronic ICs consist of transistors, capacitors and resistors, a PIC consists of, for example, lasers, modulators, waveguides, photodetectors and filters, all integrated on a single substrate. These PICs are nowadays extensively used commercially, mainly in datacom and telecom, becoming popular also in sensing.

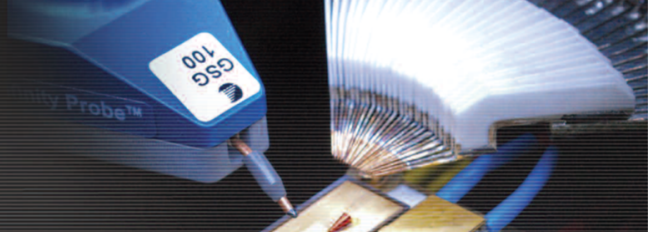
PIC technology has now become accessible to users without a cleanroom, through so-called multi-project wafer runs and open foundries. Indium phosphide based technology is commercially available through SMART Photonics and Heinrich Hertz Institute. Silicon nitride technology is commercially available at LioniX Intl. Access is coordinated by the JePPIX platform: http://www.jeppix.eu/. Silicon photonics and silicon nitride technologies are also commercially accessible through the ePIXfab Silicon photonics alliance platfom http://www.epixfab.eu/



QRNGs on integrated photonic chips

Several QRNGs using photonic integrated circuits (PICs) have been successfully demonstrated recently. In a first implementation combining two lasers, one optical coupler and two photo-detectors on an indium phosphide (InP) chip, Fig. 1, random numbers can be generated at GHz regime, with a footprint of 12 mm^2. The chip[4] has electrical input and output, all required components incorporated, and hence from pins outwards it can be operated and wired as a regular electronic chip, despite using photonics inside.

Another implementation used a silica-substrate based chip with footprint as small as 15x15 μm2 was demonstrated based on surface plasmons (not current in the regular MPW offerings), with QRNGs generated



at MHz rates. The chip[5] was operated as part of a larger laboratory setup, not all the required components were integrated on the same substrate.

Other demonstrations based on silicon photonics resort to Mach-Zehnder interferometers on chip[6,7], with footprints as low as 0.5 mm^2, and operate in the GHz regime. While silicon is the material of choice for digital electronics, these implementations require an external laser diode to operate.

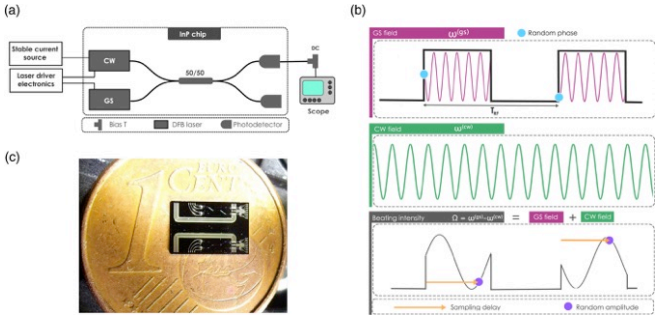


Fig. 1 – InP quantum random number generator[4]. © 2016 Optical Society of America.

Integrated quantum photonic start-ups

Although the aforementioned developments stem from scientific and academic research, these works have resulted into companies pursuing industrial exploitation.

Quside Technologies (https://www.quside.com/) is a spin-off company from ICFO-The Institute of Photonic Sciences in Barcelona (Spain). After a 6+ years of intense R&D effort in developing quantum devices for secure communications, the team incorporated by 2017 to take the industrialization path.

Psi Quantum (https://psiquantum.com/) is a start-up company at Palo Alto (USA), whereas Xanadu (https://www.xanadu.ai/) is based in Toronto (CA). These companies are devoted to quantum computing presumably based upon hardware incorporating PICs. Quantum computers are popularly claimed and acknowledged as candidates to perform faster operations than classic computers, supporting algorithms amenable for cryptographic key deciphering.

Discuss your application with us

If you want to learn more on the use of PIC technologies for the implementation of photonic chips for your application, please contact the PICs4All consortium.

Our consortium can support you in the techno-economic evaluation of photonic integration geared towards your products and applications. Support may be given as well in the design and characterization.

In the framework of the EU H2020 PICs4All project the partners offer free-of-charge guidance to companies, research institutes and academia interested in development and implementation of their commercial products, using photonic devices.

The PICs4All consortium is funded under the EU Horizon 2020 programme and brings together expertise of nine European Application Support Centers (ASCs). The ASCs can guide you through the existing eco-system of design houses, foundries, packaging and test services.

References

[1] "Cybersecurity basics", by Malwarebytes, available online: https://www.malwarebytes.com/cybersecurity/

[2] M. Haahr, "Introduction to randomness and random numbers", https://www.random.org/randomness/

[3] C. Abellán and V. Pruneri, "The future of cybersecurity is quantum," IEEE Spectrum vo. 55(7) pp. 30-35 (2018).

[4] C. Abellán et. al., "Quantum entropy source on an InP photonic integrated circuit for random number generation," Optica 3, 989-994 (2016)

[5] J. T. Francis et. al., "Quantum random number generation using an on-chip plasmonic beamsplitter," Quantum Science and Technology, 2(3), 035004

[6] F. Raffaelli et. al., "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," Opt. Express 26, 19730-19741 (2018)

[7] M. Rudé et. al., "Interferometric photodetection in silicon photonics for phase diffusion quantum entropy sources," Opt. Express 26, 31957-31964 (2018)

Contact information

Prof. Dr. Ing. Pascual Muñoz Muñoz

(PICs4all ASC – Spain)

Photonic Research Labs - iTEAM Research Institute

(Universitat Politècnica de València)

Website: http://www.prl.upv.es

Email: pascual.munoz@upv.es

Acknowledgement

P. Muñoz acknowledges Quside Technologies CEO C. Abellán (cabellan@quside.com) and CTO D. Tulli (dtulli@quside.com) for helpful discussions.