Geneva, September 19th 2019

A Major Step in Standardization of Quantum Random Number Generators (QRNG)

Earlier this month, the draft recommendation “Quantum noise random number generator architecture” was consented as an international standard during ITU-T[1] meeting in Geneva, Switzerland. ID Quantique was one the main actors of this success.

Today’s cryptography relies on sequences of random numbers. Pseudo random number generators currently in use seem to provide random bit sequences, but actually these bit sequences have certain patterns, so there is a risk of being hacked. The integration of physical entropy sources in random number generators is the most common method to overcome this security threat. However, classical physics is causal, hence the unpredictability of a bit sequence generated with classical physics cannot be proven. Quantum physics, on the other hand, is random by essence. Numbers generated by a Quantum Random Number Generator (QRNG) cannot be predicted – QRNG is provably unpredictable. So if a quantum random number generator is used in a security system, even a fast supercomputer with a fast arithmetic operation cannot predict the random bit sequences used by this security system.

The newly consented draft recommendation, which is expected to be approved within 2019, deals with a common architecture for quantum entropy sources. This common architecture will allow suppliers and users to make a clear and simple distinction between QRNGs and other physical random number generators called True Random Number Generators (TRNGs). This first standardized quantum technology is already being used for ciphering in various security areas. In particular, the security of IoT, autonomous cars and smart cities based on 5G network will be strengthened.

“The QRNG standard will give the ICT industry a random number generator with proven unpredictability. Success for this standard would be its adoption by most or all QRNG vendors as well as some national security agencies.“ says Grégoire Ribordy, CEO of ID Quantique.

The consented recommendation was created by ID Quantique and SK Telecom at ITU-T in September 2018. At that time, it was the first quantum technology related draft recommendation created at ITU-T. One year later, this recommendation is the first quantum technology recommendation to be consented. This achievement is the result of the collaborative work between ID Quantique and other ITU-T members from several countries including Korea, China, Japan, the US and the UK.

This fast progress at ITU-T would not have been possible without the preparatory work led by ID Quantique and the Quantum Alliance Initiative at a two-day workshop held at the Hudson Institute in December 2018. One of the results of this workshop was the review and agreement by a consortium of 18 companies and entities from eight countries of a voluntary industry standard for QRNGs. This agreed industry standard served as primary input to the draft recommendation on QRNGs at ITU-T.

[1] It means the International Telecommunication Union Telecommunication Standardization Division, the organization under the ITU, the world’s largest telecommunications international organization, which establishes standards for the information and communication field.

“This is a big advance for quantum information technology” says Dr. Arthur Herman, Director of the Quantum Alliance Initiative, “The goal of this standard is not to preclude or compete with standards being completed by other standards bodies, like ETSI or IEEE, but to complement those standards with a foundational version that current users can adopt while waiting for future standards development.”

ID Quantique’s partner SK Telecom has already integrated IDQ’s QRNG in its 5G and LTE subscriber authentication servers in the first half of this year. SK Telecom has also increased security for 5G and LTE data transmission by applying IDQ’s quantum key distribution (QKD) technology to the Seoul-Daejeon section which is a key transport section of data traffic across the country. The two companies are now carrying out standardization tasks related to quantum key distribution in cooperation with other countries and organizations.

About ID Quantique

Founded in 2001 as a spin-off of the Group of Applied Physics of the University of Geneva, ID Quantique is the world leader in quantum-safe crypto solutions, designed to protect data for the future. The company provides quantum-safe network encryption, secure quantum key generation and Quantum Key Distribution solutions and services to the financial industry, enterprises and government organizations globally. IDQ’s quantum random number generator has been validated according to global standards and independent agencies, and is the reference in highly regulated and mission critical industries – such as security, encryption, critical infrastructure and IoT – where trust is paramount.

Additionally, IDQ is a leading provider of optical instrumentation products, most notably photon counters and related electronics. The company’s innovative photonic solutions are used in both commercial and research applications.

IDQ’s products are used by government, enterprise and academic customers in more than 60 countries and on every continent. IDQ is proud of its independence and neutrality, and believes in establishing long-term and trusted relationships with its customers and partners.

For more information, please visit www.idquantique.com.

Contact info:

Catherine Simondi
VP Marketing & Communications
catherine.simondi@idquantique.com
+41 (0) 22 301 83 71