Redefining Randomness

RANDOM NUMBER GENERATION
WHITE PAPER

Quantum versus Classical Random Number Generators

March 2023

Table of Content

ID Quantique SA
Ch. de la Marbrerie, 3
1227 Carouge
Switzerland

Tel: +41 (0)22 301 83 71
Fax: +41 (0)22 301 83 79
www.idquantique.com
info@idquantique.com

Information in this document is subject to change without notice.

Definitions

ADC: Analog Digital converter

Autocorrelation: the likelihood of getting the same result as before

Bias: the difference in total “0” and “1” in the output

CIS: CMOS image sensor

DRBG: deterministic random bit generator. A software-based postprocessing to condition the raw random numbers to be usable for cryptographic applications

ES: Entropy Source, a physical source of randomness, which outputs digitized results of measured physical events

LED: light emitting diode

PRNG: Pseudo random number generator. It consists of an algorithm into which some initial value – it is called the seed – is fed and which produces by iteration a sequence of pseudo-random numbers

QRNG: Quantum Random Generator. It generates random from a quantum process

Random number: a number generated by a process, whose outcome is unpredictable, and which cannot be subsequently reliably reproduced.

Stochastic model: It represents a process that has some inherent randomness. As opposed to a deterministic model that is fully determined by its initial condition and some parameter values.

Abstract

Modern digital security systems rely on crypto algorithms and random keys. Using a predictable or defective Random Number Generator (RNG) to generate cryptographic keys introduces a vulnerability to attacks. True randomness can only be achieved based on physical phenomena and not on deterministic algorithms such as Pseudo RNGs (PRNGs).

In this white paper, we compare two different categories of True RNGs (TRNGs): classical TRNGs that rely on classical physical phenomena and Quantum RNGs (QRNGs) that are based on quantum processes.

We demonstrate that QRNGs are safer and more robust than classical TRNGs because the quantum entropy source is based on a simple, controlled and, most importantly, provably secure (i.e. unpredictable) physical process.

IDQ’s QRNG products create raw random bits with a high level of entropy, while classical TRNGs heavily rely on deterministic postprocessing to correct a large range of imperfections. Moreover, thanks to a simple monitoring of a few key parameters, IDQ’s QRNGs offer a high degree of protection against external factors that could affect randomness. In contrast, many classical TRNGs are sensitive to environmental changes and thus vulnerable to undetected attacks or failures.

1. Introduction

The foundation of modern digital security systems lies in the quality of various crypto algorithms and key materials. In accordance with the Kerckhoff principle, a crypto system must be secure even if everything about it is known, except the encryption key itself. Indeed, most crypto algorithms today are standardized and open for public review. The cryptographic system guarantees its security only under the assumption that a sufficient amount of entropy —corresponding to the required security level— is available from a RNG to generate its cryptographic keys. In other words, if the security of the Entropy Source (ES) inside the RNG is jeopardized, for example if it is easy to predict its outcome, then the entire cryptographic system using such random source is no longer secure.

Nowadays, security standards, for example, NIST SP 800-90B and BSI AIS-31, emphasize the importance of the quality of ES. In order to get a certification, vendors should provide not only statistical tests but also a theoretical background and a stochastic modelling that proves the quality and reliability of the ES.

	Classical RNG (TRNG)	Quantum RNG (QRNG)
Source of randomness	Thermal or chaotic processes	Fundamental unpredictability of well-chosen and controlled quantum processes
The ES produces true random output	No or unknown	Yes
Underlying assumptions to calculate the quality of the ES	Ad-hoc assumptions	Fundamental laws of physics
Live monitoring of the ES is possible	No or limited	Highly effective
Attacks on the ES are typically detectable	No or unknown	Yes
Is the random number generator secure?	Unproven	Provably secure

Table 1. classical TRNGs and QRNGs: overview table

Many systems today still use PRNGs that are mathematical algorithms generating randomly looking bit sequences by expanding an initial seed. By nature, PRNGs are deterministic and thus predictable: knowing the seed or intermediate states gives a complete knowledge over the entire future outputs. Consequently, to be secure, the initial seed must be unpredictable and all internal states during the PRNG process must be protected securely against attacks. Without unpredictable ES, the PRNG itself introduce a security vulnerability.

RNGs based on physical processes are usually called TRNGs, regardless of which level of randomness they have. Most TRNGs based on classical physics are using thermal fluctuations of the electronics. The problem is that their quality is inconsistent and difficult to assess. There are fluctuating signals that TRNGs use to extract random bit sequences, while we do not know how the signals are exactly generated and what their current state is.

In case of a QRNG, it is quite easy to measure the quality of ES, because it depends on very simple quantum principles which proves how and how much randomness is generated. The statistical property of the randomness is very clear. Therefore, QRNGs can estimate the produced entropy in real time and easily maintain it.

Table 1 provides a high-level comparison between classical TRNGs and QRNGs. In section 2, a more detailed description of classical TRNGs is presented. In section 3, we describe the concepts used in ID Quantique's QRNG chips and explain why the quantum nature of the ES implies increased robustness, control and higher security. For a comparison, in section 4, we look at TRNGs based on ring oscillators (ROs) and other circuits and show how fluctuating their performance can be, which makes them heavily relying on mathematical (thus deterministic) postprocessing to produce randomness. Section 5 shows how classical TRNGs can suffer from various attacks (frequency injection, contactless attacks, trojans, etc.) because they are sensitive to environmental changes. In the appendix, we outline in a simple way why randomness is an intrinsic property of quantum mechanics.

2. True Random Number Generators (TRNGs)

2.1 Entropy source and post-processing

A TRNG typically consists of two units: an ES as a physical source of randomness, which outputs digitized results of measured physical events; and a software-based postprocessing to condition the raw random numbers to be usable for cryptographic applications. The difference between a QRNG and classical TRNG lies in the ES.

Postprocessing is a mathematical function, implemented in a software that corrects the imperfection of the ES, for example, bias or correlations. TRNGs with a weak ES heavily rely on a strong postprocessing which will remove the effect of imperfections of the physical ES but sometimes may just hide a flaw, .i.e. a vulnerability. Therefore, entropy analysis always requires the direct access to the raw entropy data, instead of the postprocessing ones. Unfortunately, users cannot access to TRNGs' entropy data: there is often no way for users to detect a failure or attacks on the ES of a TRNGs.

2.2 Classical vs Quantum entropy sources

Classical entropy sources use macroscopic physical events such as tossing a coin, electric or thermal noise, or jitters to generate randomness. They usually depend on meta-stable physical conditions or chaos. This adds a risk to any cryptographic application that uses a classical TRNG output, as one can never fully monitor the physical process, nor prove that it is secure. In particular, an attacker could perform attacks on the ES that could not be detected and manipulate the classical TRNGs to break the security of the crypto system.

As opposed to classical TRNGs, QRNGs rely on quantum physics which is fundamentally probabilistic: a quantum process can produce unpredictable outcomes in a robust and well controlled way. Since the ES is described with fundamental models, all its properties and behavior are understood, and one can prove the security (i.e., unpredictability) with *ab initio* calculations.

In the next section, we describe in more details the physical processes used in ID Quantique 's QRNGs to produce high quality randomness, and show with test results that their ES directly produce high quality randomness. In contrast, classical ESs only produce roughly estimated randomness and hence classical TRNGs mainly rely on postprocessing.

Furthermore, the risk of unnoticed attacks on a quantum ES is limited, and potential failures can be anticipated by simple and reliable health monitoring system of a few key parameters. In contrast to "silent breaks" of classical TRNGs, QRNGs "fail gracefully".

3. ID Quantique's Quantum Random Number Generators (QRNGs)

3.1 Physical concept

ID Quantique's patented QRNG chips exploit the simple fact that the number of photons emitted by a generic light source fluctuates around a certain mean value. These fluctuations, also called "quantum shot noise", are purely of a quantum origin, and are therefore fundamentally random as per the laws of physics (see Appendix). In IDQ's QRNG chips, an array of single-photon sensitive pixels is illuminated for a short time during which each pixel receives an undetermined number of incident photons that follows the statistics of a Poisson distribution.

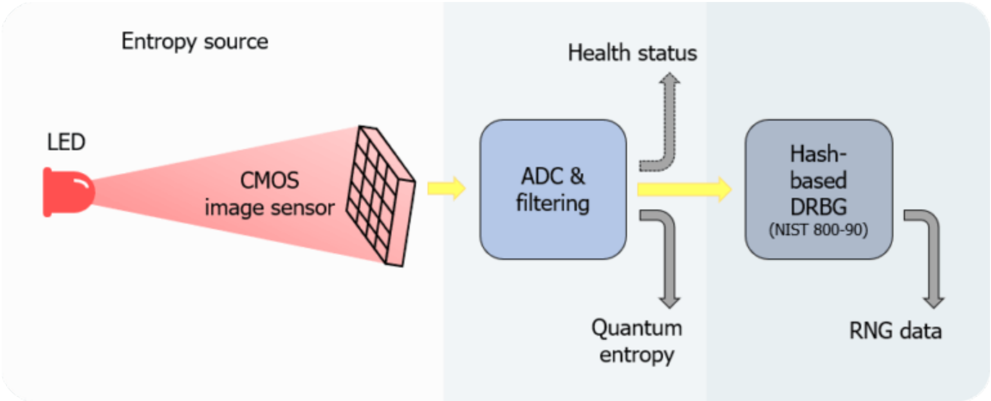

Figure 1. IDQ's QRNG chips concept: ES composed of an LED and a CMOS image sensor, data extraction with an ADC and hash-based postprocessing

The structure of the IDQ's QRNG chips is shown in Figure 1: a light emitting diode (LED) and a CMOS image sensor (CIS) pixel array are embedded in the QRNG chip. All pixel outputs are digitized by a single analog-digital converter (ADC). Based on these ADC output values, the number of detected photons per pixel, as well as their fluctuations, can be measured. Essentially, the quantum shot noise is directly converted into bits at the output of the ADC. The passage from quantum randomness to an actual random number is straightforward and not affected by other unaccounted (and possibly contriving) physical processes that could increase predictability or thwart security. This conceptual simplicity implies robustness, because it is practically impossible to force the light source to have less fluctuations given a certain minimal intensity.

3.2 Highest level of entropy, even without post-processing

The raw data from the physical source (. i.e. before any post-processing) already present maximal entropy. For example, ID Quantique's QRNG chips successfully passes the IID test suite of NIST SP 800-90B entropy test suite [1]. They have the highest level of entropy in the non-IID estimation of the NIST entropy test suite, even though they are not using any conditioning or postprocessing function to increase the entropy rate in bits, in contrast to other technologies, as described in table 2. Note that IDQ's QRNG chips IDQ6MC1 and IDQ20MC1 have a built-in post-processing (hashed based DRBG) unit to be compliant with NIST SP 800-90A/B/C and AIS 31 PTG.3.

ES	Type of TRNG	Using conditioning for the test	# of tests	Non-IID Entropy (per byte)
IDQ Quantis	QRNG	No	200	7.4612
IDQ250C2	QRNG	No	175	7.4648
IDQ6MC1	QRNG	No	52	7.4692
IDQ20MC1	QRNG	No	1000	7.4721
IDQ PCIe-12	QRNG	No	320	7.4175
Random.org	Classical TRNG	Yes	173	7.4543
ComScire	Classical TRNG	Yes	400	7.4606
Intel DRNG	Classical TRNG	Yes	1049	7.4489
RPi4-hwrng	Classical TRNG	Yes	218	7.4534
/dev/urandom	PRNG	Yes	20	7.4710

Table 2. NIST SP800-90B entropy estimation results of the IDQ QRNG chips and other TRNGs. Notably, IDQ's QRNGs achieve an excellent result even without using a mathematical postprocessing (or conditioning).

3.3 Classical noise vs quantum noise

While ID Quantique's QRNG chips produce randomness from quantum processes, one could argue that classical noise, e.g. produced by internal components, is always present and can influence the randomness. Indeed, the light source might fluctuate due to environmental changes and the detectors are neither perfect due to a certain imprecision of measuring the exact photon number. As these noise sources are uncontrolled, they could be exploited by attackers similarly as in the case of classical TRNG.

This potential loophole is simply solved by separating the controlled quantum noise from uncontrolled noise of the components. Every pixel of the CIS counts a photon number between 0 and 1023, hence the result is encoded into 10 bits. Classical noise can only effect on the least significant bits 0 and 1, while random bit transitions on higher bits can only occur because of photon fluctuations [7]. Hence, by using only bits 2 and 3, we separate the quantum noise out of the raw data. These are the random bits that are further processed, while the other bits are neglected.

3.4 Simple auto-calibration

The quantum shot noise of light follows the Poisson distribution, in which the photon number fluctuations equal the square root of the intensity. To achieve high entropy, it is therefore important to guarantee a minimal number of photons impinging on the pixels. Similarly, pixel saturation must be avoided. Environmental and operating conditions fluctuations (e.g. temperature, voltage or current) can affect the optical power. In the IDQ QRNG chips, an autocalibration function controls the optical power by adjusting the current level supplied to the LED as well as the exposure time of the CIS. This sets the average of the ADC outputs in a good range. Security and robustness come from simplicity: As long as the mean photon number is kept in a certain regime, high entropy generation is guaranteed by the laws of quantum physics.

4. Classical TRNGs

A typical implementation of a classical TRNG is based on ROs, which are circuits oscillating between two states. The fluctuation of the period – called jitter – is used as a source of entropy. During the last decades, the architecture of RO-based TRNGs has been improved. As shown in Figure 2 [4].

However, it is difficult to guarantee the quality and well-functioning of the ES. This can be easily seen when looking at the large scattering of the bias (i.e., the difference in total “0” and “1” in the output) and the autocorrelation (i.e., the likelihood of getting the same result as before) results obtained on 45 different Intel ESs (see Figure 3).

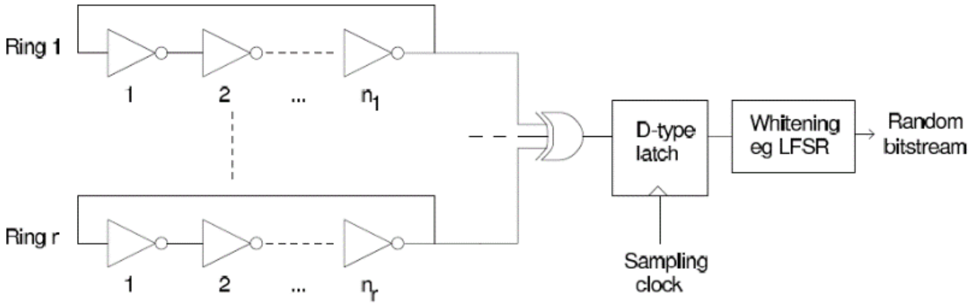

Figure 2. A typical design for TRNGs based on multiple ROs using different number of NOT gates [2]. Every ring has a certain fluctuation in its operation period, which is read out, combined with other rings and compared to the sampling clock

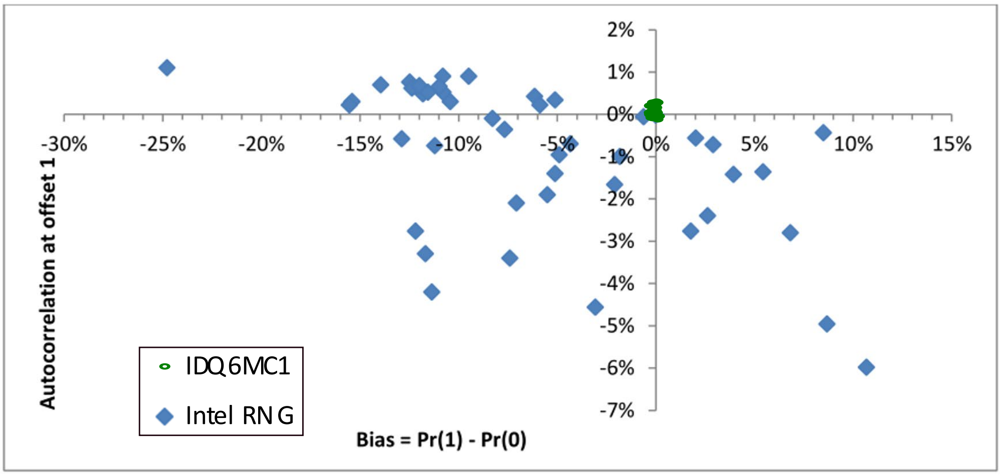

Figure 3. Bias and autocorrelation results from the ES of 45 Intel's RNG (blue diamonds, from [4]) and of 50 QRNG chips IDQ6MC1 (green ellipses, see section 3). While all tested IDQ QRNG IDQ6MC1 chips perform well and in a consistent way, there is a large scattering of the Intel RNG's regarding their bias and autocorrelation results.

Therefore, the health monitoring system, which guarantees a minimal produced entropy, must accept a large bias or correlations. In reference [4], the authors found that even a sample of raw data where 96% of all bits are "1" could pass the health tests and led to apparently perfect randomness after postprocessing. The authors [3] write: "Even if the entropy source is severely degraded, the final output will remain of high quality and cryptographically strong and should appear indistinguishable from true random by computationally-bounded adversaries (despite being non-random from an information theoretic perspective)." This means that the TRNG could output seemingly perfect randomness while at the same time the ES is not working properly, by relying heavily on a postprocessing that is deterministic, thus vulnerable. The lack of "true" random numbers could open a loophole in the cryptographic system, which could be exploited by an attacker who is aware of this situation or has even provoked it.

5. Attacks on classical TRNGs

As classical noise is based on chaotic or meta-stable physical processes, it is very sensitive to the environmental changes like temperature, voltage/power, strong electromagnetic (EM) fields or radiations. By using this weakness, attackers might bring a classical TRNG out of an entropy generating state, without notice. In contrast, QRNGs are typically more robust against environmental changes. For example, light is hardly interfered with any other signals and thus temperature changes, indirect electromagnetic field or laser injection will have no impact on a quantum ES or can be detected by the health monitoring system.

5.1 Temperature changes

Some TRNGs often have shorter operating temperature range, for example, 0°C to 50°C [5] and will not be suitable for applications such as automotive and smartphone that require broader range of operating temperature, typically -40°C to 105°C or more.

The performance of optical components in many QRNGs is well characterized in terms of temperature and can be well controlled despite the temperature change. For example, the LED that produces photons in the IDQ QRNG products guarantees a broad range of operating temperature. The IDQ6MC1 has obtained the AEC-Q100 automotive certification, which requires a functioning ES in the temperature range from -40°C to 105°C.

5.2 Voltage changes

Variation of voltage and power such as glitches, out-of-band frequencies and level will also dramatically change the behavior of a classical TRNG's ES and electronics. For example, an attacker can easily access to input/output (IO) pads of a smartcard and perform a fault injection attack on the voltage IO that will degrade the entropy quality produced by an embedded TRNG [2].

Figure 4 shows a picture of the antenna used to figure out the frequencies of RO inside the smartcard, by reading and analyzing emitted EM signals. It also shows the basic circuit design used to perform a frequency injection attack.

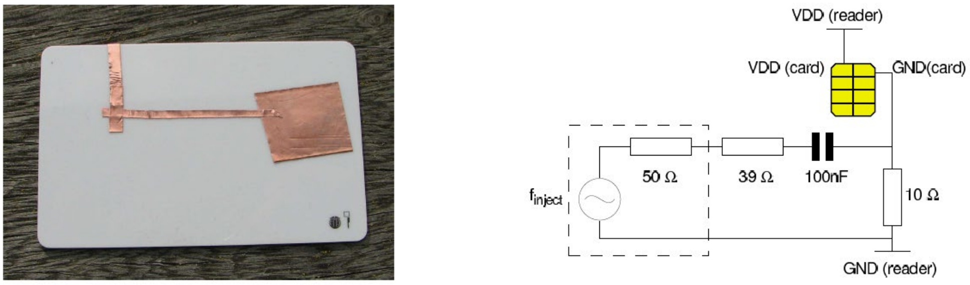

Figure 4: simple set-up for direct injection attacks on RO-based RNGs [2]

5.3 Electromagnetic fields

Strong electromagnetic (EM) fields to the surface of TRNGs can also change and even damage their internal states, without direct contact to IO pads. In the case of a RO-based TRNG, frequencies of ROs can be locked to the injected EM signal's frequency. Figure 5 shows an indirect EM field injection attack platform that can emit via a microprobe pin an appropriate EM field on the surface of TRNG without physical contact. The graphs on the right of the figure 5 show how well the frequencies of ROs inside FPGA chip are locked to the injected signal's frequency [6].

This implies that the sampling clock can no longer read a jittery zone of the RO and an attacker is able to control the output of the ES.

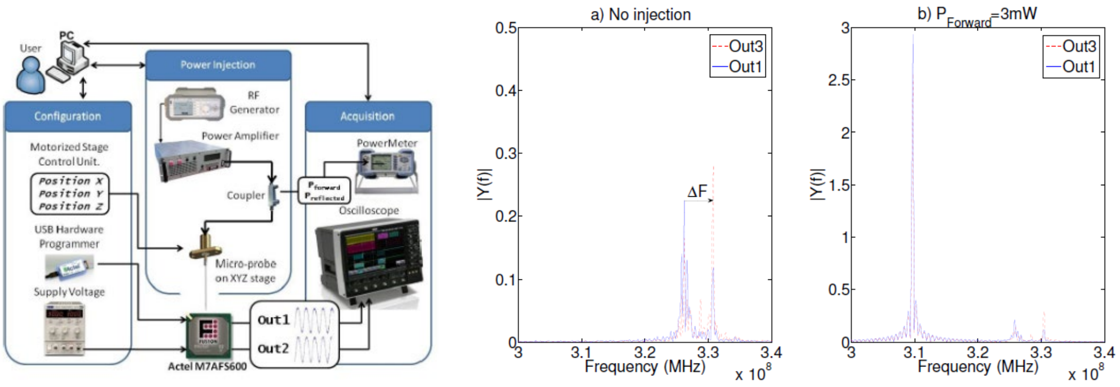

Figure 5. Indirect injection attacks to RO-based TRNGs [6].

Table 3 shows the results of contactless EM field attacks on a RO-based TRNG and on the IDQ QRNG chip IDQ6MC1. The attacks on the classical TRNG were successful, whereas attacks on the IDQM6C1 were unsuccessful even when using higher power levels. While the frequency of the operation clock inside IDQ6MC1 can be slightly changed by this EM attack signal, the basic functioning of the QRNG is not affected because it has a redundant margin of the operational clock frequency. In addition, the chip is also well protected by a metal case.

		Bayon et al. [6]	IDQ tests
Target	RNG device	RO-based TRNG	QRNG IDQ6MC1
Attack signal	Frequency Range (MHz) Strength (mW)	300 ~ 325 ≤ 3	1 ~ 50 ≤ 50
Antenna	Type Material Length (mm) Diameter (mm)	Monopole Tungsten Rod 30 0.2	Monopole Iron Needle 40 0.5
Attack successful		**Yes**	**No**

Table 3. Comparison of a simple EM attack on a classical TRNG [6] and on the QRNG IDQ6MC1.

6. ID Quantique's QRNG products

ID Quantique was the first company to develop a quantum random number generator in 2001 and it remains the market leader in terms of reliability, certifications and Swiss engineering, with its successive versions of hardware RNGs.

IDQ's Quantis family provides instant entropy for high-quality encryption keys and random draws right from boot up. Quantis QRNG productsare declined in several form factors, from chips to appliance.

- Quantis QRNG chip exploits IDQ latest QRNG technology described in part 3.a . **It is available in six models**, that each fit various industry-specific needs:
  - With its low profile, compact size and low power consumption, **IDQ250C2 and IDQ250C3** have been designed specifically for mobile handsets, IoT and edge devices. They are ideal for securing the collection and transfer of sensitive data at the edge.
  - **IDQ6MC1** is ideal for applications where resistance to external environmental perturbations are critical. It has obtained AEC-Q100 certification, demonstrating it can reliably be embedded in any security system of a connected car to ensure trusted and secured in-vehicle and V2X communications.
  - **IDQ20MC1** has the highest entropy throughput and can serve multiple security applications with true and unpredictable randomness. It can be easily embedded in computers, laptops, servers or any security devices.
  - **IDQ20MC1-S1 and IDQ20MC1-S3** are two variations of the IDQ20MC1 QRNG chip that have been specifically designed and tested to ECSS-Q-ST-60-13 Class 1 and Class 3, to withstand the extreme harshness of the space environment.

- Quantis QRNG Appliance is a Quantum random number generator for networked and security applications.

It securely generates and delivers high-quality random numbers for security and cryptographic applications in enterprise, government, gaming, datacenter and cloud environments. The Quantis Appliance is designed for environments, where high availability is necessary. It can be inserted in, or removed from, an operating network with no impact on any other appliance, such as servers, switches and Hardware Security Modules (HSMs).

The Quantis family also features USB and PCIe cards that are compatible with most platforms:

- Quantis QRNG USB device – random stream of 4 Mbps
- Quantis PCI Express (PCIe) boards – random stream of 40 Mbps and 240 Mbps

Quantis QRNG products have been certified by many leading agencies: METAS (Swiss) and CTL (UK) have evaluated and tested Quantis products and confirmed that the quality of its random output complies with the highest requirements.

Gaming systems that embed Quantis products have been certified by leading Gaming certifications agencies such as iTech labs and GLI.

A dedicated AIS31 versions of PCIe-4M and USB-4M use specific AIS31 PTG3.0 compliant post-processing and have been tested and validated according BSI test procedure by French ANSSI.

- METAS Certification
- Compliance with the BSI's AIS31 standard (dedicated version of Quantis)
- iTech Labs individual Certificate
- CTL Certification

For more information, see the Quantis AIS31 validated RNG models.

7. Conclusion

In this white paper, we compare two different categories of TRNGs: classical TRNGs that rely on classical physical phenomena and Quantum RNGs (QRNGs) that are based on quantum processes. The Entropy source of classical TRNGs relies on chaotic processes which add a risk to any cryptographic application that uses a classical TRNG output, as one can never fully monitor the physical process, nor prove that it is secure. Classical TRNGs heavily rely on post-processing to compensate the inconsistent quality of the entropy source. On the opposite, IDQ's QRNG products create raw random bits with a high level of entropy based on a simple, controlled and, most importantly, provably secure (i.e. unpredictable) physical processes. Moreover, many classical TRNGs are sensitive to environmental changes and thus vulnerable to undetected attacks or failures, while IDQ's QRNGs offer a high degree of protection against external factors that could affect randomness thanks to a simple monitoring of a few key parameters.

Using a QRNGs as a source of entropy makes a cryptographic system robust against attacks, for the secure collection and transmission of sensitive data including financial, health, business and personal information. Or protection of IoT and edge devices that are now connecting home, cars, hospitals, factories, infrastructure, schools and shopping locations. QRNGs can be trusted to make our connected world safer.

Appendix: Why quantum physics is intrinsically random

Observation of quantum processes gives rise to unpredictable results, which is a source for true random numbers. While it is difficult to *intuitively* understand why quantum physics is different from our daily-life experience of a deterministic world, it is relatively easy to convince ourselves that quantum randomness is indeed fundamental.

To this end, let us consider a simple experimental setup. Imagine we take a laser as a source of light. The only thing that is relevant here is that a laser emits a very homogenous light beam. We direct the laser to a semi-transparent mirror (i.e., a piece of glass) under a certain angle, such that part of the light goes through the glass (i.e., is transmitted) and part of the light is reflected. If we use the right glass and the right angle, we can manage that half of the light is transmitted and half of it is reflected. We verify this with detectors that measure the intensity of light. We place one of them in the path of the transmitted light and another in the path of the reflected light path, respectively. If we do everything correctly, we will see that both detectors measure a light intensity that is half of the light intensity that is emitted by the laser.

Now, let us have a closer look at the nature of light. Since roughly 1900, we know that light is composed of light particles, called photons. In the case of a laser, the output photons are all identical. This means that photons arriving at the glass are indistinguishable (except by the time of arrival). Moreover, a photon is a particle that cannot be further divided: if the laser beam arrives at the glass, some photons go straight through while others are reflected like a ball on a wall (see Figure 6). By using single-photon detectors, we can exploit this simple idea to generate entropy. We reduce the laser power such that in a certain time interval only one photon is emitted. When it is transmitted, we count it as “1”; if reflected as “0”.

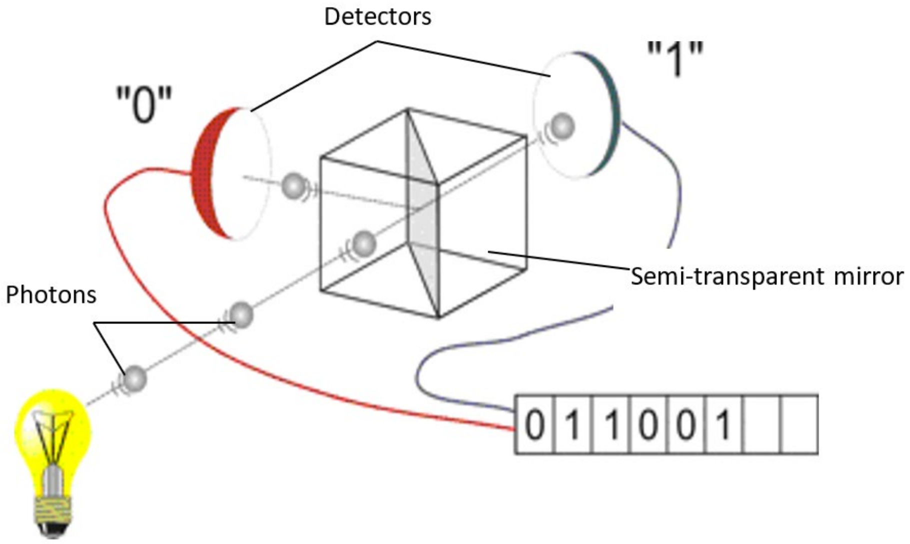

Figure 6: experimental set-up with laser, semi-transparent mirror and single photon detectors

But where is the randomness coming from? What or who does decide whether a photon is transmitted or reflected? When and how is it decided?

First, we note that the laser emits identical photons. Therefore, neither the laser nor the photons themselves decide whether the photon is transmitted or reflected by the glass. In other words, there is no information that is encoded in the photons that influences its interaction with the glass. Similarly, there cannot be any hidden or uncontrolled mechanism inside the glass that decides if a photon is reflected or transmitted. Indeed, every physical process is governed by some laws of physics that are constant in time. Therefore, it is not possible for the glass to treat identical photons differently by letting some through and reflect others.

Consequently, as nothing has taken the decision before of which way the photon will take, it is in an uncertain state without objective existence after the interaction with the glass. Both outcomes ("transmitted" or "reflected") are equally possible. It stays in this undetermined state until a measurement is done that determines the path. Since the information of which path the photon takes is nowhere encoded (not in the light source, neither in the photon, the glass, nor in the detectors), the detection event is truly random. The randomness is "created" at the moment of detection, while it is impossible to identify who or what decided the outcome.

References

[1] NIST SP 800-90B entropy estimation software tool: https://github.com/usnistgov/SP800-90B_EntropyAssessment

[2] Markettos, A. Theodore, and Simon W. Moore. ‘The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators’. In *Cryptographic Hardware and Embedded Systems - CHES 2009*, edited by Christophe Clavier and Kris Gaj, 317–31. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer, 2009. https://doi.org/10.1007/978-3-642-04138-9_23.

[3] ‘Intel® Digital Random Number Generator (DRNG) Software Implementation Guide’, March 2020. https://software.intel.com/en-us/articles/intel-digital-random-number-generator-drng-software-implementation-guide.

[4] Mike, Hamburg, Kocher Paul, and Marson Mark E. ‘ANALYSIS OF INTEL’S IVY BRIDGE DIGITAL RANDOM NUMBER GENERATOR’. Cryptography Research, Inc., 12 March 2012. https://web.archive.org/web/20141230024150/http://www.cryptography.com/public/pdf/Intel_TRNG_Report_20120312.pdf.

[5] ComScire. ‘CryptoStrong™ Model CS128M’. Accessed 6 March 2020. https://comscire.com/product/cs128m/.

[6] Bayon, Pierre, Lilian Bossuet, Alain Aubert, Viktor Fischer, François Poucheret, Bruno Robisson, and Philippe Maurine. ‘Contactless Electromagnetic Active Attack on Ring Oscillator Based True Random Number Generator’. In *COSADE: Constructive Side-Channel Analysis and Secure Design*, edited by W. Schindler and S. A. Huss, LNCS:151–66. Constructive Side-Channel Analysis and Secure Design. Darmstadt, Germany, 2012. https://doi.org/10.1007/978-3-642-29912-4_12.

[7] ID Quantique Quantum Safe White paper: Quantis QRNG chips physical model and test results