Redefining Randomness

RANDOM NUMBER GENERATION WHITE PAPER

What is the Q in QRNG?

May 2020

ID QUANTIQUE SA
Chemin de la Marbrerie 3

1227 Carouge/Geneva
Switzerland

T +41 22 301 83 71
F +41 22 301 89 79

info@dquantique.com
www.idquantique.com

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.

1. What is the Q in QRNG?

In order to guarantee absolutely random numbers, RNGs (random number generators) must not be vulnerable to prediction or bias, and thus dictated by true randomness. But how can we generate a truly random number?

Instead of relying on a seed number and algorithm, an RNG can rely on an actual physical process to generate numbers. The most reliable processes are quantum physical processes, as quantum physics is fundamentally random.

In fact, the intrinsic randomness of subatomic particles' behavior at the quantum level is one of the few completely random processes in nature. By tying the outcome of an RNG to the random behavior of a quantum particle, it is possible to guarantee a truly unbiased and unpredictable system.

For example, physicists can record the reflection, or lack thereof, of light particles against a mirror to generate a random string of 1s and 0s. Other methods include splitting a beam of light into two beams and then measuring the light intensity of each beam as it fluctuates to generate random numbers.

Quantum RNGs generate outcomes by observing and recording a contained natural process as it happens - making it possible to perform live verification of the numbers and monitor the hardware to ensure it is operating properly.

2. What is a random number?

A random number is a number generated by a process, whose outcome is completely unpredictable. Although it may appear simple at first sight to provide this definition of what a random number is, it proves to be quite difficult in practice.

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

This definition works fine provided that one has some kind of a black box – such a black box is usually called a random number generator – that fulfils this task.

However, if one were to be given a number, it is simply impossible to verify whether it was produced by a random number generator or not. It is hence absolutely essential to consider sequences of numbers in order to study the randomness of the output of such a generator.

It is quite straightforward to define whether a sequence of infinite length is random or not. This sequence is random if the quantity of information it contains – in the sense of Shannon's information theory – is also infinite.

In other words, it must not be possible for a computer program, whose length is finite, to produce this sequence. Interestingly, an infinite random sequence contains all possible finite sequences.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@dquantique.com
www.idquantique.com

Such an infinite sequence does for example contain the Microsoft Windows source code or the text of the Geneva conventions.

Unfortunately, this definition is not very useful, as it is not possible in practice to produce and process infinite sequences.

An infinite sequence should not be compressible by any known or unknown technique

In the case of a finite sequence of numbers, it is formally impossible to verify whether it is random or not. It is only possible to check that it shares the statistical properties of a random sequence – like the equiprobability of all numbers – but this a difficult task.

To illustrate this, let us for example consider a binary random number generator producing sequences of ten bits. Although it is exactly as likely as any other ten bits sequences, 1 1 1 1 1 1 1 1 1 1 does look less random than 0 1 1 0 1 0 1 0 0 0.

In order to cope with this difficulty, definitions have been proposed to characterize "practical" random number sequences.

According to Knuth, a sequence of random numbers is a sequence of independent numbers with a specified distribution and a specified probability of falling in any given range of values.

For Schneier, it is a sequence that has the same statistical properties as random bits, is unpredictable and cannot be reliably reproduced.

A concept that is present in both of these definitions and that must be emphasized is the fact that numbers in a random sequence must not be correlated. Knowing one of the numbers of a sequence must not help predicting the other ones.

Whenever random numbers are mentioned in the rest of this paper, it will be assumed that they fulfil these "practical" definitions.

3. Generating random numbers

In a binary scenario, the probability to obtain 1 vs 0 should be equal to ½. a random number generator is a device that produces sequences of numbers complying with the definitions proposed above.

3.1 Types of random number generators

- PSEUDO RNG
- CLASSICAL PHYSICAL RNG
- QUANTUM PHYSICAL RNG

There exist two main classes of generators: software and physical generators. From a general point of view, software generators produce so-called pseudo random numbers. Although they may be useful in some applications, they should not be used in most applications where randomness is required. These two classes, as well as their respective advantages, are discussed below.

3.2 Software solutions

Computers are deterministic systems. given a certain input, a program will always produce the same output.

Because of this very fundamental property, it is impossible for a program to produce a sequence of random numbers. The sequence may have some of the properties of a random sequence, and thus pass some statistical randomness tests, but it is always possible to reproduce it.

As the sequences they produce look like random sequences, these generators are called pseudo-random number generators. It is however clear that they do not fulfil the definitions given at the beginning of this white paper.

Pseudo-random number generators consist 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.

Although their period can be made very long, the sequence produced by such a generator is always periodic. When working with large sets of random numbers or long sequences, it is important to verify that the period is large enough.

One of the properties of the sequences produced in this way is that, as soon as one element of the sequence is known, all the other elements of the sequence, both preceding and following, can be determined.

It is immediately obvious that this property is especially critical when such numbers are used in cryptography for key generation. The sequences produced by a good pseudo-random generator initialized with an appropriate seed, pass most statistical tests.

However, it is also important to realize that if the sequence considered is long enough, it will always fail at least some tests, because of periodicity.

3.3 Output is determined only by the seed and the generating algorithm

One important issue when using pseudo-random number generators is the choice of the seed value. If one does not want to continuously cycle through the same sequence, it is essential to change periodically the seed value.

How should this seed value be chosen? Ideally, it should be random. As a pseudo-random generator is used, it is likely that no random number generator is available. It is a catch-22 situation.

A solution, which is not always satisfactory, is to use entropy gathering. System information – the clock, the time interval between keystrokes, etc. - is combined to produce a seed. This technique however requires extreme caution.

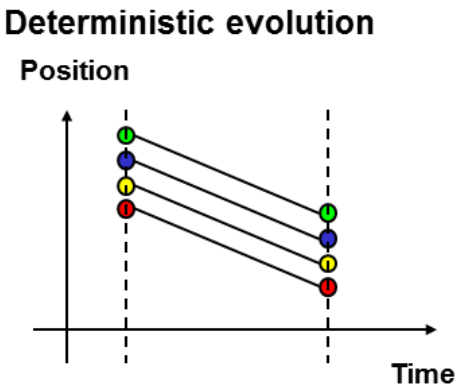
3.4 The same seed will always generate the same output

A security problem encountered by Netscape with its browser in 1995 illustrates the risks associated with the use of pseudo-random numbers in cryptography.

At the time, the web was full of promises for online commerce and Netscape had developed a protocol, called SSL and still in use today, to secure communications over the web.

Like in the case of other cryptographic protocols, the security of SSL crucially depends on the unpredictability of the key. The company implemented this protocol in its browser but relied on a pseudo-random number generator for key generation.

Two Berkeley graduate students reverse-engineered the code of the browser and revealed a serious security flaw. They noticed that the seed used by the pseudo-random number generator depended on the time of the day and some system information (the process ID and the parent process ID).



They showed that it was relatively easy to guess these quantities, and thus to reduce the number of possible keys that one should try to crack the protocol.

This attack reduced the time for a brute force attack of the protocol from more than thirty hours to a few minutes, and as little as a few seconds in some special cases.

This problem is also serious in other industries. For example, in 2014, a group of hackers managed to make millions by targeting and hacking slot machines from a well-known brand in the gaming industry. Casinos from US to Romania to Macau were the main victim of the scam.

It appeared that the hackers managed to figure out how to predict the slot machines' PRNG behavior.

After a prolonged observation and analysis of the slot machines' behavior, they could identify the pattern of the PRNG's algorithm that was used in the slot machines.

This security flaw illustrates why pseudo-random number generators are usually considered inappropriate for high-security cryptographic or other applications.

PRNG generators are used in particular cases where their main disadvantage – namely that the sequences they produce are reproducible – can represent an advantage.

When using random numbers for scientific calculations, it is sometimes useful to be able to replay a sequence of numbers when debugging the simulation program.

This is one of the reasons – the other being the lack of good physical random numbers generators – why these generators are widely used in these applications.

However, it is important, even in this field, to remain careful when using pseudo-random numbers. They have been shown to cause artefacts in certain simulations.

A good approach is to use pseudo- random numbers when debugging, and then resort to a physical generator to refine and confirm the simulation.

3.5 Physical sources of randomness

In applications where pseudo-random numbers are not appropriate, one must resort to using a physical random number generator. When using such a generator, it is essential to consider the physical process used as the entropy source.

This source can be either based on a process described by classical physics or by quantum physics. Classical physics is the set of theories developed by physicists hundreds of years ago, which describes macroscopic systems like falling coins. Quantum physics is a set of theories elaborated by physicists during the first half of the 20th century and describes microscopic systems like atoms or elementary particles. Some examples of generators based on each of these theories, along with their advantages, are presented below, after a brief discussion on bias.

3.6 Bias of a random number generator

As said in part 2, a finite sequence of numbers produced by a random number generator should share the statistical properties of a random sequence – like the equi-probability of all numbers.

A problem encountered with physical random number generators is their bias. A binary generator is said to be biased when the probability of one outcome is not equal to the probability of the other outcome.

Bias arises because of the difficulty to devise precisely balanced physical processes. It is however less of a problem than one might expect at first sight. There exists some post-processing algorithm that can be used to remove bias from a sequence or random numbers.

The simplest of these unbiasing procedures was first proposed by Von Neumann. The random bits of a sequence are grouped in sub sequences of two bits. Whenever the two bits of a subsequence are equal, it is discarded.

When the two bits are different and the subsequence starts with a 1, the subsequence is replaced by a 1. When it starts with a 0, it is replaced by a 0. After this procedure, the bias is removed from the sequence.

The cost of applying an unbiasing procedure to a sequence is that it is shortened. In the case of the Von Neumann procedure, the length of the unbiased sequence will be at most 25% of the length of the raw sequence.

We mentioned previously that randomness tests basically all amount to verifying whether the sequence can be compressed. An unbiasing procedure can be seen as a compression procedure. After its application, the bias is removed and no further compression is possible, guaranteeing that the sequence will pass the tests. Other unbiasing procedures exist. The one proposed by Peres, for example, is significantly more efficient than the Von Neumann procedure.

3.7 Processes described by classical physics – determinism hidden behind complexity

Macroscopic processes described by classical physics can be used to generate random numbers. The most famous random number generator – coin tossing – indeed belongs to this class.

However, it is very important to realize that classical physics is fundamentally deterministic. The evolution of a system described by classical physics can be predicted, assuming that the initial conditions are known.

In the case of a coin, a physicist knowing precisely its weight, its initial position, the force applied to it by the hand, the speed of the wind, as well as all the other relevant parameters, should in principle be able to predict the outcome of the throw.

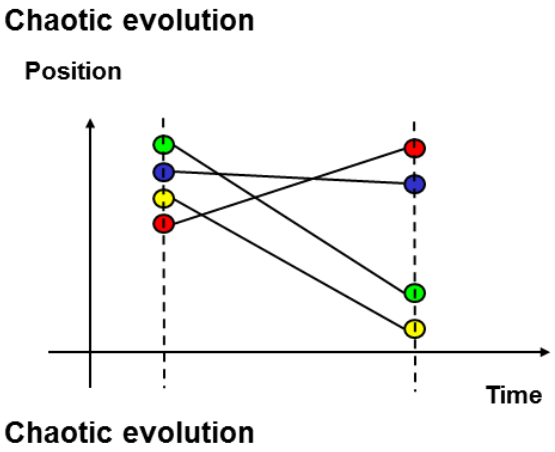
Why is that, that in practice this prediction is not possible? Coin tossing is a chaotic process. Chaos is a type of behavior observed in systems whose evolution exhibits extreme sensitivity to initial conditions.

Coin tossing is not the only physical system with chaotic evolution. Turbulences in a flow (turbulences in a lava lamp have been used to generate random numbers) or meteorological phenomena are good examples of chaotic systems.

The evolution and behavior of these systems are very sensitive to initial conditions. In spite of its popularity, coin tossing is clearly not very practical when many random events need to be known to reach a stable quality of randomness.

Other examples of physical random number generators based on chaotic processes include the monitoring of an electric noise current in a resistor or in a Zener diode, or circuits oscillating between two states (ring oscillators). In this case, the fluctuation of the period – called jitter – is used as a source of entropy. A more detailed study on these RO-based RNGs is available in our white paper: Quantum versus Classical Random Number Generators.

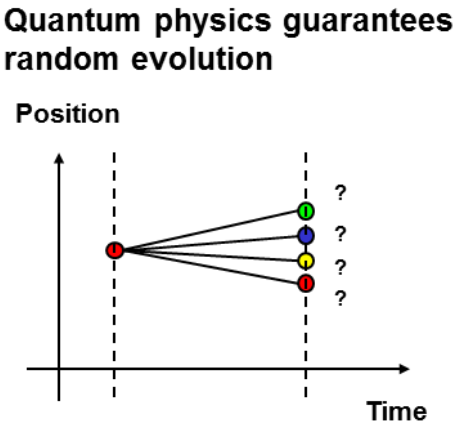
Formally, the evolution of these generators is not random; just very complex.



Although their random numbers are likely to pass randomness tests, these generators are difficult to model. This means that it is impossible to verify, while acquiring numbers, that they are operating properly. In addition, it is difficult to ensure that the system is not interacting – even in a subtle way – with its environment, or manipulated by an attacker, which could alter the quality of the randomness produced.

3.8 Processes described by quantum physics –randomness revealed by simplicity

Contrary to classical physics, quantum physics is fundamentally random. It is the only theory within the fabric of modern physics that integrates randomness.



This fact was very disturbing to physicists like Einstein who invented quantum physics. However, its intrinsic randomness has been confirmed over and over again by theoretical and experimental research conducted since the first decades of the 20th century.

When designing a random number generator, it is a natural choice to take advantage of this intrinsic randomness and to resort to the use of a quantum process as source of randomness.

Formally, quantum random number generators are the only true random number generators. Although this observation may be important in certain cases, quantum random number generators have other advantages.

This intrinsic randomness of quantum physics allows selecting a very simple process as source of randomness. This implies that such a generator is easy to model and its functioning can be monitored in order to confirm that it is operating properly and is actually producing random numbers.

The first quantum random number generators were based on the observation of the radioactive decay of some element. Although they produce numbers of excellent quality, these generators are quite bulky and the use of radioactive materials may cause health concerns. The fact that simple and low cost quantum random number generators did not exist prevented quantum physics to become the dominant source of randomness.

4. The Quantis Quantum Random Number Generators

In 2001, ID Quantique introduced the first commercial quantum random number generator, which generated strong interest. Quantis is a state-of-the-art quantum random number generator, exploiting an optical quantum process as the source of randomness.

Quantis is unique in that it relies on quantum physics to produce truly random bits. The product comes in various form factors: chips, USB device, a PCI express (PCIe) card and Appliance. More information on these products can be found here. It is possible to download random numbers produced by a Quantis Quantum Random Number Generator by visiting www.randomnumbers.info.

4.1 First generation of Quantis product

4.1.1 Physical concept

Optics is the science of light. From a quantum physics point of view, light consists of elementary "particles" called photons. Photons exhibit in certain situations a random behavior.

One such situation, which is very well suited to the generation of binary random numbers, is the transmission upon a semi-transparent mirror. The fact that a photon incident on such a component be reflected or transmitted is intrinsically random and cannot be influenced by any external parameters.

Figure 1 schematically shows this optical system.

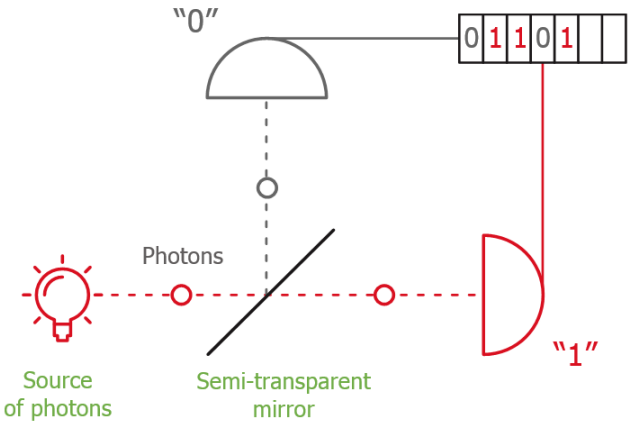


Figure 1: Optical system used to generate random numbers

Figure 2 shows the block diagram of the Quantis random number generator, which consists of three subsystems.

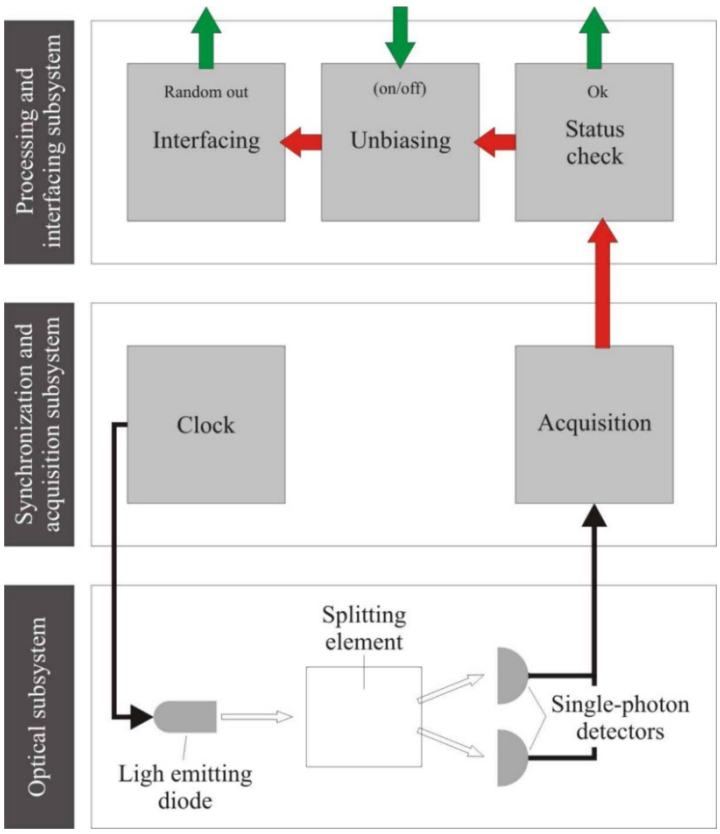


Figure 2: Block diagram of the Quantis RNG

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@dquantique.com
www.idquantique.com

The first one is the core of the generator and contains the optical elements that are used to implement the random process and produce the random outcomes. It comprises a light emitting diode producing the photons, a transmission element, where the random process takes place, and two single-photon detectors – detectors with single-photon resolution – to record the outcomes.

The optical subsystem is controlled by a synchronization and acquisition electronic circuit. This subsystem comprises clock and triggering electronics for the photon source, as well the acquisition electronics for the single-photon detectors. The processing and interfacing subsystem perform statistical and hardware checks, as well as unbiasing of the sequence. This subsystem also shapes the output electronic signals.

4.1.2 Unbiasing of random numbers

As mentioned above, physical processes are difficult to precisely balance. It is thus difficult to guarantee that the probability of recording a 0, respectively a 1, is exactly equal to 50%.

With Quantis, the difference between these two probabilities is smaller than 10% - or equivalently the probabilities are comprised between 45% and 55%. As this bias may not be acceptable in certain applications, the processing unit of Quantis performs unbiasing of the sequence.

4.1.3 Status monitoring

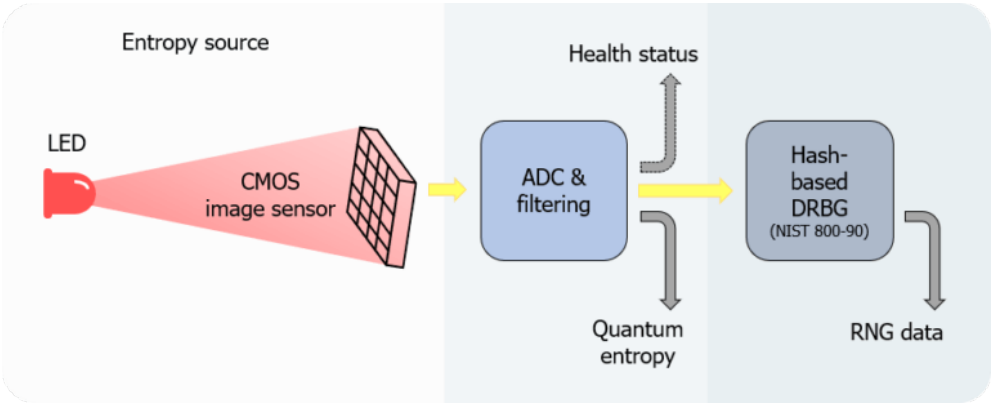
One of the main advantages of quantum random number generators is that they are based on a simple and fundamentally random process that is easy to model and monitor.

The processing unit of Quantis performs a live verification of its functioning. It continuously checks that the light source and the two detectors are correctly working, and that the raw output stream statistics are within certain bounds.

A status bit is output by Quantis. If all the conditions are fulfilled, this bit is equal to 1. If one of the conditions is not fulfilled, the status bit is set to 0 and the bit stream is inhibited. Thanks to this feature, the users of Quantis can have a high level of trust in the random numbers they are using.

4.2 Latest generation of Quantis products

IDQ'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. In IDQ 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.



The structure of the IDQ QRNG chips is shown in the figure above: 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. The raw data from the physical source (. i.e. before any post-processing) already present maximal entropy.

For example, the IDQ QRNG chips successfully passes the IID test suite of NIST SP 800-90B entropy test suite. The IDQ QRNG chips 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 QRNG chips IDQ6MC1 and IDQ20MC1 have a built-in postprocessing (hashed based DRBG) unit to be compliant with NIST SP 800-90A/B/C and AIS 31 PTG.3.

4.2.1 Separating Quantum noise from classical noise

While the IDQ 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.

4.2.2 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.

4.3 Certifications

The simplicity of Quantis is also its strength. As the underlying quantum mechanical processes are well understood and easily characterized, it is relatively easy to certify the Quantis products.

Quantis is the most certified true RNG in the market. It has successfully passed the following certifications or government validations:

- NIST SP800-90/A/B/C Compliance
- NIST SP800-22 Test Suite Compliance
- METAS Certification
- Compliance with the BSI's AIS31 standard (dedicated version of Quantis)
- iTech Labs individual Certificate
- CTL Certification

5. 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 products are declined in several form factors, from chips to appliance.

- Quantis QRNG chip exploits IDQ's latest QRNG technology. It is available in three models that each fit various industry-specific needs:
    - With its low profile, compact size and low power consumption, **IDQ250C2** has been designed specifically for mobile handsets, IoT and edge devices. It is 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.

- 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) board
    - Legacy products: random stream of 4 Mbps and 16 Mbps
    - New Generation products: random stream of 38.3 Mbps and 232 Mbps

The New Quantis QRNG PCIe-40M and PCIe-240M rely on ID Quantique's latest patented QRNG technology, that generates randomness from the shot noise of a simple light source captured by a CMOS image sensor. They can serve multiple applications in a server with true randomness, either directly from the entropy source or after NIST compliant post-processing. Live status verification and entropy source health monitoring performed at component level ensure the Quantis PCIe cards always provide the highest entropy, and because any failure or attacks can be detected, they can be trusted to provide the highest entropy from the very first to the last bit.

Quantis has also been validated according to the German BSI's stringent AIS31 test standard. For more information, see the Quantis AIS31 validated RNG models.

6. Summary

- Random number generation is a critical security and reliability criterion in many demanding applications.
- Because of its intrinsic randomness, quantum physics is an excellent source of randomness.
- ID Quantique's Quantis products exploit a simple quantum optical process as the source of randomness.
- Quantis family passes all statistical tests, in compliancy with NIST and BSI recommendations. It is the most certified QRNG products on the market.

ID QUANTIQUE SA
Chemin de la Marbrerie 3
1227 Carouge/Geneva
Switzerland
T +41 22 301 83 71
F +41 22 301 89 79
info@dquantique.com
www.idquantique.com