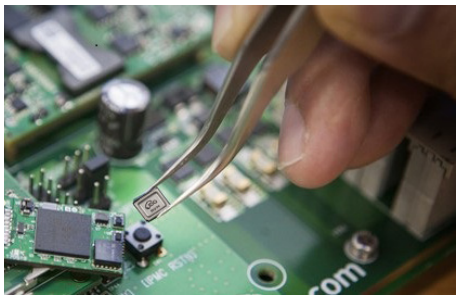
Redefining Randomness

Quantis QRNG Chip

The source of full entropy for automotive, computing, critical infrastructure, IoT, mobile & security applications

ID Quantique introduces its true Quantum Random Number Generator (QRNG) Chip, which offers the highest attainable security and robustness for the generation of random bits. It is ideal for use in the automotive, computing, critical infrastructure, IoT, mobile and security applications where compact size and resistance to external environmental perturbations are critical.

Based on a technology concept and patent from IDQ, the Quantis QRNG Chip harnesses true quantum randomness from the shot noise of a light source captured by a CMOS image sensor.



- Intrinsically and provably random
- Robust and controlled entropy source
- Instant full entropy from the first bit

Only Quantum RNGs are intrinsically random, provably secure and future proof. Quantum physics is probabilistic on a fundamental level, which means that they can produce unpredictable outcomes in a robust, transparent and well controlled way. Since the entropy source is described with fundamental models, all properties of the entropy source are understood and the security can be proven. Additionally, the Quantis QRNG Chip provides full entropy instantaneously from the very first bit.

Applications

- Automotive (V2X, CAN, Infotainment, etc)
- Financial transactions / Blockchain / Point of Sale (POS) terminals
- Any cryptographic algorithms and protocols (IPSEC, TLS, SSH, etc.)
- Artificial Intelligence (Machine and Deep Learning)
- Smart Networks (IoT, SmartGrid, SmartCity, SmartHome, etc)
- Scientific Modeling & Simulations
- Computing Device (mobile phones, laptops, tablets, servers, etc)
- Gaming applications

Quantis QRNG Chip

True, unbreakable and unpredictable randomness

Unlike other sources of entropy that are deterministic or not provably secure, QRNGs are intrinsically random and rely on well-known processes. The Quantis QRNG Chip is a robust source of full entropy, provably unbiased and unpredictable.

WHY QUANTUM RANDOM NUMBER GENERATION?

The foundation of modern digital security systems lies in the quality of the crypto algorithms and encryption keys. In accordance with the Kerckhoff principle, a crypto system must be secure if everything about it is known, except the encryption key itself. Indeed, most commonly used crypto algorithms today are standardised and open for public review. But the entire foundation of security crumbles if the numbers that have been generated to create a key are not unique, sufficiently random or easy to predict. In other words, using a predictable or defective source of entropy introduces a vulnerability.

Unfortunately, many keys today are created by pseudo random number generators (PRNGs) meaning a computer program supplies the randomness for generating keys using a seed and deterministic algorithm. In most cases, the computer uses a random seed from external sources of entropy, such as the movements of the mouse, disc interrupts, or other effects. However, the entropy produced is limited especially in isolated data centers or networks. The numbers generated by PRNGs are not truly unpredictable and random.

True randomness can only be based on physical phenomena. However, hardware-based true random generators based on classical physics (TRNGs), such as self-oscillating digital circuits, are black boxes where classical physical processes run in an uncontrolled and chaotic manner. It is therefore impossible to guarantee that an attacker could not manipulate and force a classical TRNG behavior. The only way to produce true and unbreakable randomness is by understanding and validating the physical process by which that randomness was produced.

By contrast, Quantum RNGs rely on Quantum physics that is probabilistic on a fundamental level, which means that they can produce unpredictable outcomes in a robust and well controlled way, and from the first bit.

Since the entropy source is described with well-known fundamental models, all properties of the entropy source may be understood and the security can be proven. This transparency has far-reaching implications: the design of QRNGs can be optimized to maximize the generated randomness by the entropy source. Well-designed quantum entropy sources have a high quality randomness, while classical entropy sources mainly rely on mathematical post-processing to generate random bits.

QUANTIS QRNG CORE TECHNOLOGY

At its core, the QRNG chip contains a light-emitting diode (LED) and an image sensor. Due to quantum noise, the LED emits a random number of photons, which are captured and counted by the image sensor's pixels, giving a series of raw random numbers that can be accessed directly by the user applications. These numbers are also fed to a deterministic random bit generator algorithm (DRBG) which distills further the entropy of quantum origin to produce random bits in compliancy to NIST 800-90A/B/C standard.

The Quantis QRNG Chip allows live status verification: if a failure is detected in the physical process, the random bit stream is immediately disabled, the user is notified, and an automatic recovery procedure is performed to produce QRNG data again.

SECURING OUR CONNECTED WORLD

Nowadays, in various areas such as IoT, smart devices, V2X and so on, computing devices have been getting smaller and smaller and connected to each other. On the other hand, the security threats have never been stronger. A network is as strong as its weakest link, meaning that only one flaw in a small device can disrupt the entire network, putting all devices at risk. Protecting these kinds of devices is a challenge and is of critical importance, as security means public safety.

However, there are specific challenges in small devices, where high entropy is hard to achieve due to hardware limitations. With the Quantis QRNG chip, IDQ solves four specific requirements that are critical to manufacturers: size, power consumption, cost and reliability. Thanks to its standard interfaces, the Quantis QRNG chip can be easily embedded in a wide variety of IoT products, autonomous vehicles, drones and smart devices.

Quantis QRNG Chip

Trusted for Information Theoretic Security

The Quantis QRNG Chip is a trusted source of full entropy that supports information theoretical security, now and in the future.

INFORMATION THEORETIC SECURITY

Only cryptographic systems using a robust, unpredictable source of full entropy that produce true random numbers can be information theoretically secure.

Both PRNGs based on algorithms and TRNGs based on classical physics are vulnerable. Since they are deterministic and thus predictable at their core, PRNGs cannot offer full cryptographic security. With classical TRNGs, one can never be sure how much true randomness is produced. Typically, health monitoring and sanity checks are used at the post-processing level to detect any issues. This might be good enough for known issues, but the ultimate lack of control and the complexity of the underlying physical process make it difficult to cover all potential scenarios. The resilience of a classical RNG is thus highly dependent on the post-processing and it has to be evaluated using various practical tools such as statistical tests.

On the other hand, the fundamental principles on which QRNGs rely to generate randomness are fundamentally understood, and they may be easily modelled, controlled and optimized to provide full entropy. Besides providing random sequences with high-quality statistical properties, QRNGs thus have the potential to offer true randomness in its most formal and secure meaning to support Information Theoretic Security levels. Even with unlimited computational power, an adversary could not predict the outcome of a QRNG.

CERTIFICATIONS

ID Quantique's Quantis QRNG product range is and has always been a trusted and certified source of entropy. Simplicity is the ally of security and this is the strength of the Quantis QRNG Chip. As the quantum mechanical processes underlying the QRNG are well understood and characterized, and since the quantum optics process itself is transparent, it is relatively simple to achieve otherwise stringent certifications of the Quantis QRNG products.

The Quantis product family has been certified by leading commercial entities, well-known international institutes and governments worldwide, from the Swiss Federal Office of Metrology (METAS certificate) to the Compliance Testing Laboratory UK (CTL certificate). It is also compliant with the German BSI's AIS31 validation criterias.

Quantis chips are compliant with NIST SP800-90A/B/C recommendations and passes IID, non-IID tests, DieHarder and NIST SP800-22 testsuites.

Quantis IDQ6MC1 have also obtained AEC-Q100 certification, demonstrating they can reliably be embedded in any security system of a connected car to ensure trusted and secured in-vehicle and V2X communications.

Why the Quantis QRNG Chip?

- Quantum source of full entropy, intrinsically random
- Full entropy from the first bit
- Provably secure and controlled
- Live status verification & health check output
- Robust to external conditions (AEC-Q100 certified)
- Future proof – Quantum-Safe
- Simple & easy to integrate (standard I2C & SPI interfaces)
- Integrated NIST 800-90A/B/C compliant DRBG post-processing

Quantis QRNG Chip at a glance

Model	IDQ250C2	IDQ6MC1	IDQ20MC1
QRNG CORE			
Compliant to the Standard NIST 800-90A/B/C	✓ (B)	✓	✓
Certified AEC-Q100		✓	
Size	2.5 x 2.5 x 0.84 mm	4.2 x 5 x 1.1 mm	4.2 x 5 x 1.1 mm
RNG Data Output	N/A	1.47 Mbps (@ SPI Interface)	4.90 Mbps
Quantum Entropy Source	250 Kbps (typical)	5.88 Mbps (@ SPI Interface)	19.64 Mbps
POWER SUPPLY INFORMATION			
Single Input Voltage (Embedded LDO)	2.8 V	2.8 V	2.8 V
I/O Interface Voltage	1.8 V	1.8 V	1.8 V
POWER CONSUMPTION			
RNG Output Mode	N/A	59.94 mW	83.44 mW
Entropy Output (sample mode)	15 mW (typical)	58.24 mW	75.88 mW
Soft-Sleep Mode	N/A	13.66 mW	20.72 mW
Deep-Sleep Mode	N/A	6.96 mW	10.69 mW
Power Down Mode	100 uW	N/A	N/A
SET-UP TIME			
Initial set-up time	3 ms	171 ms	184 ms
OPERATION FREQUENCY CLOCK & TEMPERATURE			
Embedded ROSC	11 MHz ~ 14 MHz (Typ. 12 MHz)	41 MHz ~ 58 MHz (Typ. 48 MHz)	41 MHz ~ 58 MHz (Typ. 48 MHz)
Recommended temperature	-30 °C ~ +85 °C	-30 °C ~ +85 °C	-30 °C ~ +85 °C
Absolute maximum rated temperature	-40 °C ~ +105 °C	-40 °C ~ +105 °C	-40 °C ~ +105 °C
INTERFACE PROTOCOL			
SPI		24 MHz	24 MHz x 4 CH
I2C	400 KHz	100 KHz	

ID Quantique

Chemin de la Marbrerie 3,
1227 Carouge/Geneva Switzerland

T +41 22 301 83 71
F +41 22 301 83 79
E info@idquantique.com

www.idquantique.com

ID Quantique (IDQ) is the world leader in quantum-safe security solutions, designed to protect data for the long-term 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 organisations globally.

IDQ also commercialises a quantum random number generator, which is the reference in the gaming and security industries.

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.