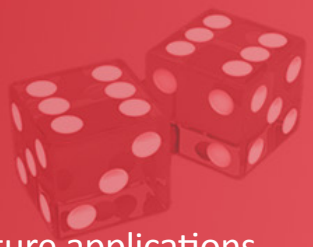
Redefining Randomness

Quantis QRNG Chip

The world smallest QRNG for security, IoT & critical infrastructure applications



ID Quantique introduces the world's smallest true Quantum Random Number Generator (QRNG) chip. Based on a technology concept and patent from IDQ, and designed and manufactured in collaboration with our partners SK Telecom, the Quantis QRNG chip harnesses true quantum randomness from the shot noise of a light source captured by a CMOS image sensor.

The breakthrough derives from the use of low-cost off-the-shelf components, such as a CMOS image sensor, LED and ASIC, which allowed for significant miniaturisation and cost reduction of the technology. The Quantis QRNG chip is ideal for use in the IoT, critical infrastructure and security applications where compact size, low cost, low power consumption and resistance to external environmental perturbations are critical.

The QRNG benefits from the other advantages of IDQ's traditional QRNG solutions, including an information theoretic basis for the randomness generation, health monitoring & detection; and instantaneous entropy for secure key generation.

Applications

- True random numbers for all cryptographic algorithms and protocols
- Seed generation for blockchain
- Computing Device (mobile phones, tablets, servers, etc)
- Artificial Intelligence (Machine and Deep Learning)
- Automotive (V2X, CAN, Infotainment, etc)
- Scientific Modeling & Simulations
- Smart Networks (IoT, SmartGrid, SmartCity, SmartHome, etc)
- Online Gaming and Casinos

Quantis QRNG Chip

The Quantis Quantum Random Number Generator Chip (QRNG chip) is the world's smallest QRNG designed for Internet of Things (IoT), connected cars, critical infrastructure and security applications.

WHY QUANTUM RANDOM NUMBER GENERATION?

The foundation of modern digital security systems lies in the quality of the crypto algorithms and encryption keys. Most commonly used crypto algorithms today are standardised and open for public review. In accordance with the Kerckhoff principle, a crypto system must be secure if everything about it is known, except the encryption key itself. Therefore the entire foundation of security crumbles if the numbers that have been generated to create a key are not unique or sufficiently random. In other words, anything less than true randomness (or entropy) introduces a vulnerability.

Unfortunately, many keys today are currently created by pseudo random number generators (PRNGs) meaning a computer program supplies the randomness for generating keys. It is no secret that computer programs are deterministic, and therefore predictable. This means that, in most cases, the computer tries to draw in entropy from an external source, such the movements of the mouse, disc interrupts, or other effects. However, in many cases, especially in isolated data centers or networks, such external entropy is limited and therefore the numbers generated are not truly random.

A true sequence of random numbers is a sequence generated by a process whose outcome is unpredictable, and which cannot be subsequently reliably reproduced. The only way to produce true randomness is by understanding and validating the physical process by which that randomness was produced. In other words, randomness can only be based on physical phenomena. Since quantum physics is intrinsically random, it is logical to use it as a source of true randomness.

The Quantis QRNG Chip allows live status verification, which means that its operation is continuously monitored. If a failure is detected the random bit stream is immediately disabled and an automatic recovery procedure is performed to reproduce QRNG data again. In addition, unlike PRNGs which need to accumulate external entropy, the Quantis QRNG Chip provides full entropy (randomness) instantaneously from the very first bit.

THE NEED FOR A QUANTUM RNG CHIP

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.

Any cryptographic system is only as strong as the key it uses. Generating strong keys, based on true randomness, is the cornerstone of IoT security. ID Quantique's Quantis QRNG product range is and has always been a trusted and certified source of entropy. However, there are specific challenges in the constrained devices of the IoT ecosystem, where high entropy is hard to achieve due to hardware limitations, which needed to be addressed. IDQ reacted to the market need and solved three specific requirements that are critical to manufacturers: size, power consumption and cost-efficiency.

After being the first company to develop a quantum random number generator (QRNG) in 2001, IDQ is at the forefront of innovation. The development of the Quantis QRNG Chip will allow to embed QRNG into a wide variety of IoT products, autonomous vehicles, drones and smart devices. In addition to its intrinsic trusted security characteristics, the game-changing Quantis QRNG Chip represents the most cost effective option on the market.

BASIC PRINCIPLE OF QUANTUM-BASED RNG

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. These numbers are fed to a randomness-extraction algorithm which distills the entropy of quantum origin and makes it available to the user.

Quantis QRNG Chip

True Randomness

The fundamental principles on which QRNGs rely to generate randomness are information theoretically secure. This ensures that the Quantis QRNG Chip provides extremely high quality of randomness and easy certification.

INFORMATION THEORETIC SECURITY

Since they are deterministic at their core, PRNGs cannot offer full cryptographic security. The resilience of a PRNG is thus evaluated using various practical tools such as statistical tests.

On the other hand, the fundamental principles on which QRNGs rely to generate randomness are information-theoretically secure. This ensures that the Quantis QRNG Chip provides extremely high quality of randomness and easy certification.

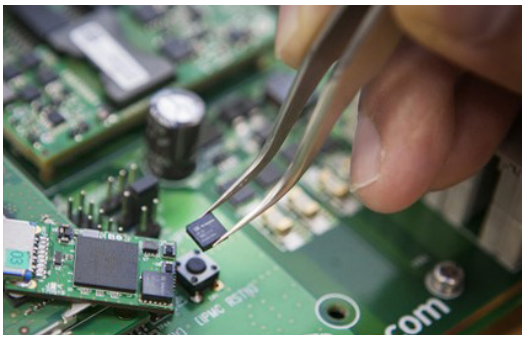
Broadly speaking, this property formalises that even with an unlimited computational power, an adversary could not predict the outcome of a QRNG.

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.

TRUSTED AND CERTIFIED

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 characterised, and since the quantum optics process itself is transparent, it is relatively simple to achieve otherwise stringent certifications of the Quantis QRNG products.

Quantis has been certified by leading commercial entities, well-known international institutes and governments worldwide. The Quantis QRNG Chip is compliant to the NIST 800-90A/B/C Standard and is designed to be certified by the Swiss Federal Office of Metrology (METAS certificate) and by Gaming Laboratories International (GLI).



Why the Quantis QRNG Chip?

- Information Theoretic Security
- Scalable instant entropy
- Long life product
- Integrated post processing
- Ultra small QRNG
- Low cost & high performance
- Low power consumption & sleep-mode capacity
- Resistant to external environmental perturbations

Quantis QRNG Chip at a glance

Model	QChip100	QChip400
QRNG CORE		
Compliant to the Standard NIST 800-90A/B/C	✓	✓
Size	4.2 x 5 x 1.1 mm	4.2 x 5 x 1.1 mm
RNG Data Output	1.5 Mbps (@ SPI Interface)	4.91 Mbps (typical)
Sample Noise Data Output	6 Mbps (@ SPI Interface)	19.64 Mbps (typical)
POWER SUPPLY INFORMATION		
Single Input Voltage (Embedded LDO)	2.8 V	2.8 V
I/O Interface Voltage	1.8 V	1.8 V
POWER CONSUMPTION		
Generation RNG Code	59.94 mW	83.44 mW
Sample Noise Output Mode	58.24 mW	75.88 mW
Soft-Sleep Mode	13.66 mW	20.72 mW
Deep-Sleep Mode	6.96 mW	10.69 mW
OPERATION FREQUENCY CLOCK & TEMPERATURE		
Embedded ROSC	41 MHz ~ 58 MHz (Typ. 48 MHz)	41 MHz ~ 58 MHz (Typ. 48 MHz)
Currently Guaranteed	-30 °C ~ +85 °C	-30 °C ~ +85 °C
Expected Range	-40 °C ~ +125 °C	-40 °C ~ +125 °C
INTERFACE PROTOCOL		
SPI Interface for RNG, Sample Data (Max: 24 MHz)	✓	✓
I2C Interface for RNG (Max: 100 Kbps)	✓	✗

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.