A REVOLUTION IN RANDOMNESS

How quantum technologies are helping to secure our digital future
Ubiquitous Entropy

Here's a little-known fact: the key to securing our digital world is not order and discipline. In fact, it's the complete opposite. The key to securing our digital world is entropy. A good entropy source is at the core of randomness generation.

Random numbers are used everywhere, from generating cryptographic keys to data sampling, computer simulation to lottery and gaming applications.

If we stop and look around us, randomness is everywhere. Random numbers are used to ensure the legitimacy of gaming operations, to protect the privacy on sensitive data, and anyone with online access to their bank account relies on random numbers to generate security access keys for two-factor authentication. However, perhaps the most pervasive use of random numbers is in modern cryptography.

The Public Key Infrastructure we all rely upon to secure the internet is dependent upon random numbers, as are all forms of data encryption. Random numbers are the source of encryption keys, used to secure data both at rest and in motion as it travels around an increasingly connected world.
Encrypt Everything

Cryptographic systems play an essential role in securing all types of sensitive data; protecting the privacy of data in the event of a breach, but also ensuring the integrity and authenticity of data used in a wide variety of industries and applications.
What happens when the unpredictable becomes predictable?

Any cryptographic system is only as secure as its keys. In turn, the strength of the keys is dependent upon unpredictability.

Unfortunately, there have been several examples in recent years of a lack of entropy used in key generation, leading to systems vulnerabilities.

When systems become predictable, they become vulnerable, exposing data owners and processors to a multitude of risks.

According to the IBM 2020 Cost of a Data Breach Report, the average total cost of a breach sits at $3.86 million.

This cost is comprised of detection, escalation and notification costs, plus post-breach response costs. It also factors the anticipated loss of business associated with the breach.

- Arguably, the indirect costs associated with a breach may be more significant than mere financial penalties.
- A loss of intellectual property may damage an organization’s ability to maintain competitive advantage
- A breach of compliance obligations may result in an inability to operate until the required standards have been met
- The long-term impact on brand equity and trust may have a significant impact on future revenue generation opportunities
- In the event of a negligent breach, organisations, or individuals, may find themselves subject to judicial proceedings

Kerckhoffs’ Principle

“A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.”

To provide adequate security the key must be:

- Unique
- Truly random (unpredictable)
- Stored, distributed and managed securely
The Quantum Opportunity

Quantum computing, quantum sensing and quantum communications represent a massive opportunity. Quantum technologies will have a revolutionary effect on almost every aspect of modern life, making unprecedented achievements possible.

The exponential power of quantum computing will drive massive progress in scientific discovery, business efficiency and communications, which will have huge benefits for mankind.

Not all applications of quantum technology may be benign. The power of a quantum computer represents a very real threat to contemporary cryptography. Today's encryption solutions will be no match for a quantum computer's ability to solve complex problems, leaving organizations vulnerable to future cyber-attacks. As organizations embrace digitization, they are exposed to ever increasing cybersecurity risks.

However, all is not lost. The answer to the quantum threat lies in quantum technology itself. **Quantum random number generators are perfectly placed to help cybersecurity experts combat the next generation of cyber-criminals.**
Random Number Generators compared

PRNG
(algo-based)
Randomness: **Good** (testable)
Security: **Weak** (keep seed secret)

TRNG
Option 1: Get randomness from environment
Randomness: **Good** (testable)
Security: **Medium** (not available for isolated systems)

Option 2: Based on chaotic processes
Randomness: **Good** (testable)
Security: **Medium** (attacks by improved systems)

QRNG
(based on quantum physics)
Randomness: **Great** (provable & testable)
Security: **High** (relies on implementation)

As you might expect, not all random number generators (RNG) are created equal. The degree of entropy generated is subject to several internal and external factors.

RNGs can basically be divided into two fundamental types: software and hardware. Software RNGs are also known as pseudo RNGs, which gives you a clue to exactly how random the output is.

Although they offer a low-cost introduction to randomness, the problem with software RNGs is that they are deterministic, so what you get is closer to simulated randomness.

Hardware devices allow us to get closer to true randomness. However, different types of True Random Number Generators (TRNGs) produce different amounts of entropy.

TRNGs require a physical source of randomness, which output digitized results of a measured physical event.

In the case of TRNGs that rely on classical physics, it is not possible to fully monitor the physical process, nor ensure its integrity. This introduces uncertainty in the cryptographic system and compromises its security.

For provably secure random number generation, you need to look to quantum physics for the answer.

Quantum physics is fundamentally random, producing unpredictable outcomes in a robust and controlled environment.
Quantis Range of QRNG

ID Quantique has been a pioneer in the field of QRNG for 20 years.

The Quantis range of products is used as a trusted source of randomness for a broad range of applications that require cryptography or guaranteed unpredictability.

The Quantis Chip represents a revolution in randomness. Its miniaturized form enables solution and product developers to integrate a source of true randomness into mobile and remote solutions like never before.

In a connected, IoT world, this represents a major breakthrough in terms of systems security, delivering a trusted source of entropy, all the way to the network edge.

While providing the highest attainable security and robustness, the Quantis Chip is designed as a low-cost solution for mass market devices.

With a low profile, compact size and low power consumption, the Quantis range is ideal for a wide range of applications across mobile, IoT and data storage.

Quantis products are available in a range of form factors; including PCIe, USB, network appliance and, since 2020, the innovative QRNG chip.
Since we’ve launched our ultra-small QRNG chip...

**March 2020**
Hitachi Energy embeds IDQ’s QRNG chip into its Quantum-enhanced encryption cards

**April 2020**
ID Quantique and SK Telecom announce the world’s first 5G smartphone equipped with a QRNG chipset: the Samsung Galaxy A Quantum

**May 2020**
ID Quantique integrates its quantum chip in Vsmart Aris 5G Smartphone

**July 2020**
ID Quantique and SK Telecom announce the world’s first 5G smartphone equipped with a QRNG chipset: the Samsung Galaxy A Quantum

**May 2020**
ID Quantique integrates its quantum chip in Vsmart Aris 5G Smartphone

**May 2020**
ID Quantique and KCS combine their technology to increase IoT & video surveillance security and protect against hacking

**October 2020**
ID Quantique integrates its quantum chip in Vsmart Aris 5G Smartphone

**December 2020**
ID Quantique and KCS combine their technology to increase IoT & video surveillance security and protect against hacking

**April 2021**
IDQ and SK Telecom unveil the Samsung Galaxy Quantum2, the second QRNG-Powered 5G smartphone with even more embedded secured applications

**April 2021**
Thales Trusted Cyber Technologies (TCT) partners with ID Quantique to provide high-assurance key protection backed by quantum randomness

**June 2021**
Alibaba adds IDQ’s QRNG to its cloud-based services, to improve the security of financial transactions

**July 2021**
SK Telecom, Octacto and IDQ unveil EzQuant, the world’s first fingerprint recognition security key equipped with a QRNG

**February 2022**
IDQ and SK Telecom unveil the Samsung Galaxy Quantum 3, the third QRNG-Powered 5G smartphone with additional secured apps and services

**April 2022**
IDQ and CryptoNext partner to deliver next-gen, quantum-safe messaging, leveraging Samsung’s embedded QRNG chip

**July 2022**
Alibaba adds IDQ’s QRNG to its cloud-based services, to improve the security of financial transactions
3 Pillars of Quantis QRNG

**Truly Random**
Quantis products use simple quantum physical processes that are intrinsically random to generate true randomness from the first bit. As the quantum processes underlying the QRNG are well understood and characterized, their inner working can be clearly modelized and controlled.

**Provably Secure**
Quantis Quantum Random Number Generators (QRNG) embed elementary components that can be easily monitored to detect any failure or attacks. Environmental perturbations can be ruled out by simple health checks, guaranteeing QRNG always produce high quality entropy.

**Independently Certified**
ID Quantique follows best practices and continually performs quality and security testing on its Quantis products to reach compliancy with the most demanding standards. Quantis products have been certified by accredited test institutions worldwide to ensure national independence and quality.
We help you build a trusted future

Feeding quantum randomness to your crypto systems is the first, easy step on your quantum journey.

A robust cybersecurity strategy is fundamental to continued growth in any organization that relies on digital systems to manage their operations.

Regardless of when quantum technology reaches its full potential, organizations need to prepare a quantum security strategy now which enables them to secure their future and seize the opportunities of a quantum world.
QRNG: a world of infinite applications

QRNG technology has become mainstream in recent years. The exponential increase in real world applications has coincided with the miniaturization of the technology, expanding QRNG use beyond the traditional network security to a new world, dominated by mobility and the IoT.

As the volume and variety of connected devices increases, QRNG is helping to secure a wide variety of mass-market applications.

QRNGs are helping to secure the next generation of mobile phone communications, providing long-term data protection for sensitive or personally identifiable information used in financial transactions, securing big data transmitted to and from cloud and datacenter services, even helping to secure the future of V2X communications. QRNG has also huge benefits for applications in computing and financial simulations, as well as in providing instantaneous true randomness for next-generation algorithms.

What’s more? You don’t have to wait: you can apply quantum-enhanced security to your existing encryption engine today.