Quantis: Quantum Random Number Generator – QRNG

When randomness cannot be left to chance

In today's world, the assets of governments, enterprises and individuals are increasingly held in digital format. Securing these digital assets is vital and depends on modern cryptographic techniques to ensure their confidentiality, authenticity, integrity and non-repudiation. Certes Networks provides encryption without compromise and leads the field in ensuring that today's demand for highly secure solutions for Zero Trust architectures is met. Following continuous innovation efforts in the security market, Certes Networks has adopted QRNG as the default source of randomness so that the encryption keys generation process cannot be left to chance, but rather perfected.

The Importance of Keys in Today's Crypto Systems

All modern cryptographic systems are based on mathematical models (algorithms) which turn plaintext into ciphertext by rearranging the elements – either by replacing or transforming them. Every algorithm works in a pre-defined manner according to a set of mathematical formulas and transformations. What is unique to each crypto-system is the encryption key. An algorithm can be thought of as a padlock – several persons can acquire the same brand of lock. Although all padlocks work according to the same mechanism, each one of them holds a distinct and unique key which locks or unlocks each individual padlock. Similarly, an encryption key acts as the opener and closer of an algorithm. Therefore, the security of the overall system actually depends on the encryption key.

This principle was further elaborated by the mathematician Auguste Kerckhoff in 1883, where he stated that the security of any cryptographic scheme must never rely on the secrecy of the algorithm but rather solely depend on the secrecy of the key.

This principle is now widely accepted as the cornerstone of building robust cryptosystems. Hence, in order to ensure security, encryption keys need to be fresh, securely generated, and properly managed.

The generation of unique and truly random numbers plays a critical role in a number of important applications. In applications such as cryptographic services, numerical simulations, and even in the gaming industry, high-quality random numbers are absolutely vital.

What is the Risk of Weak Keys

For the sake of illustration, let us consider the case of data that needs to be encrypted. A wise choice to secure this is to use AES with a key of 256 bits. Clearly, more than 20 years of continued efforts by prominent researchers and enthusiastic hackers have failed to show any weakness in this algorithm. However, this security relies on the key to be perfectly random.

The same reasoning applies to public-key cryptography. Concretely, in the case of RSA, security relies on finding two large prime numbers given their product. Again, the implicit assumption behind this statement is that both prime numbers are truly random.

Two real-world cases in which the failure of complying with this statement lead to dramatic results.

In a seminal work, Lenstra and his colleagues (https://eprint.iacr.org/2012/064.pdf) gathered about 11.4 million public RSA keys from public internet-facing servers and analysed their security. Some of these keys were 1024 bit long while the rest were 2048 bit long. Regardless of the key size, they were able to find 30,000 private keys. The reason for this weakness was that the public keys had a common prime factor that could be detected. This is simply caused by improper or insufficient seeding of the random number generator that is used to feed the RSA key generation algorithm.

Another case, also applicable to RSA, was showcased by Heninger and Shacham (https://eprint.iacr.org/2008/510.pdf). In this work, they were able to show that with the knowledge of 27% of the prime factor bits, they could recover the whole RSA private key. In other words, by manipulating the random generator to reveal some of the bits composing the secret prime factors, or by having an unbalanced random number generator, an attacker can recover the private RSA key.

Again, we stress that the cryptographic algorithm RSA was not to blame in either case as these issue solely concerned the quality of randomness that was provided in the key generation.

The Difficulty in Generating Random Numbers

A security risk arises if the numbers that have been generated to create a key are not 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 perfectly 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 centres or networks, such external entropy is limited and therefore the numbers generated are not truly random.

The risk of having a key that is not generated by a true random number generator (TRNG) is great and the consequence of an attack on such a key is immense.

The problem is compounded by the fact that randomness is very difficult to assess. Most certifications are based on an a posteriori mathematical analysis of a set of numbers – in other words, after they have been produced. Unfortunately, there is no way to prove that these numbers actually are random, we can merely qualify if they have the appearance of randomness.

ID Quantique has come up with a solution to solve the problem with randomness once and for all by harnessing the underlying randomness of quantum physics therefore mitigating traditional PRNG vulnerabilities with its innovative QRNG approach.

Quantum Random Number Generation

A true random number is a number generated by a process, whose outcome is unpredictable, and which cannot be subsequently reliably reproduced. As described above, it is unwise to use only mathematical analysis to determine whether a number is indeed random. 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.

ID Quantique launched their Quantis Quantum Random Number Generator (QRNG) family in 2004. Quantis exploits an elementary quantum optics process to generate true random numbers. Optics is the science of light. From a quantum physics point of view, light consists of elementary "particles" called photons. Photons are sent, one by one, onto a semi-transparent mirror and detected. The exclusive events (reflection or transmission) are associated to "0" or "1" bit values. Such quantum processes are intrinsically and provably random, and provide instantaneous and inexhaustible entropy.

Quantum random number generators have the advantage over conventional randomness sources of being invulnerable to environmental perturbations and of allowing live status verification. The operation of Quantis is continuously monitored and if a failure is detected the random bit stream is immediately disabled. In addition, unlike PRNGs which need to accumulate external entropy, Quantis provides full entropy (randomness) instantaneously from the very first photon (bit).

The strength of Quantis also lies in its simplicity. Since 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 certification of the Quantis QRNG products. Quantis has been certified by leading commercial and government entities, from the Swiss Federal Office of Metrology (METAS certificate), to the French ANSSI in accordance with the German BSI's AIS31 validation criteria.

Certes Networks partnered with ID Quantique and has adopted Quantis RNG card (QRNG) as the mechanism for generating the seed material for the encryption algorithm within its proprietary key management lifecycle. Quantis RNG card is available for purchase as an option for hardware-based CFNC Management servers ensuring that Certes Networks continues to innovate and use the best available security tools in the market as part of its Zero Trust Security Overlay architecture.

Why Certes Networks?

Certes Networks Zero Trust Security solutions protect data and applications in motion with a range of software defined security solutions. Our Zero Trust framework protects application traffic over any environment to any user, device or location; all this without affecting network or application performance whatsoever. Our patented and industry leading layer 4 stealth encryption solution gives you "Encryption without Compromise".

For more information visit **CertesNetworks.com**

Why ID Quantique?

ID Quantique (IDQ) is the world leader in quantum-safe security solutions designed to protect data for the long-term future. The company provides high-performance quantum-safe network encryption solutions for the protection of data in transit, supporting up to 100Gbps on local and storage area networks for data center interconnect & DRC, as well as on fully meshed global WAN networks for international operations.

By using state-of-the-art algorithms and highly secure quantum key generation and quantum key distribution (quantum cryptography), IDQ ensures that the solutions are quantum-safe for the long-term protection of sensitive data into and beyond the quantum era when quantum computers will render most of today's conventional encryption algorithms vulnerable.

For more information visit **www.idquantique.com**

Global Headquarters
300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108
Tel: +1(888) 833-1142
Fax: +1(412)262-2574
www.CertesNetworks.com

North America Sales
sales@certesnetworks.com

Government Sales
sales@certesnetworks.com

Asia-Pacific Sales
apac@certesnetworks.com

Central & Latin America Sales
sales@certesnetworks.com

Europe, Middle East and Africa Sales
emea@certesnetworks.com

V1-09-21-2017