Deloitte.

Quantum Random Number Generators— What's all the fuss about?

As the development of quantum technologies accelerates, a lot is said about the threats to, and benefits of, these technologies within cybersecurity. One such example of an advancement is the ability to build a quantum random number generator (QRNG), with potentially superior properties to currently used RNGs.

In this blog, Itan Barmes (Global Quantum Cyber Readiness Capability Lead at Deloitte Risk Advisory B.V.), Carlos Abellan (Co-founder and CEO at Quside) and Colin Soutar (Global Quantum Cyber Readiness Leader at Deloitte & Touche LLP) discuss the topic of RNGs and how quantum technologies provide unique features to strengthen security properties.

Introduction

The security of our digital society relies strongly on cryptographic methods. Confidentiality, integrity, and authenticity of data are preserved by various cryptographic algorithms. The security of these algorithms is continually challenged by the evolution of computing power and new attack methods. An impending attack that is on many people's minds is quantum-computing based algorithms, most notably Shor's algorithm, which could pose a major threat to asymmetric cryptography.

In response to the quantum threat, global efforts to develop so-called quantum-secure solutions are underway, including post quantum cryptography, quantum key distribution, and new symmetric key exchange schemes. The security of these schemes depends on various factors, but they have one aspect in common: their security characteristics are predicated upon unpredictable random numbers.

Randomness is crucial in cryptography as it is used to create a wide range of security parameters, as for instance cryptographic keys. Without unpredictable randomness, an attacker could guess or predict the values of these parameters, which could compromise the security of data and communications. In other words, using a strong cryptography algorithm with a poor random number source could be the equivalent of using a strong safe but leaving the key hanging at the door.

The Foundation of Randomness: Entropy Sources and DRBGs

At the heart of RNG lies two fundamental components: the entropy source and the Deterministic Random Bit Generator (DRBG).

The **entropy source** is akin to the unpredictable natural phenomena of the physical world. It harnesses external physical processes—such as thermal noise, atmospheric noise, or even quantum phenomena—to produce true randomness. This randomness is not just a theoretical ideal; it's a necessary ingredient for strong security protocols, cryptographic applications, and simulations.

However, entropy sources alone are not used in cryptography for various reasons, one of which is due to insufficient throughput. For that reason, a DRBG is employed, which is a sophisticated mechanism that stretches the initial randomness from the entropy source (also known as a seed), to produce a larger stream of random bits. However, it's important to note that the DRBG itself does not generate randomness and must always be used alongside entropy sources for security applications.

It is the combination of entropy sources and DRBGs that make a strong RNG for cryptographic applications. However, it's crucial to understand that randomness originates exclusively from the entropy source. Understanding the distinction

between DRBGs and entropy sources is critical to avoid common implementation mistakes, as the use of insufficiently random values may lead to severe security vulnerabilities.

How do you measure the quality of an RNG

The use of unpredictable random numbers from an entropy source is fundamental to security. In practice, however, how is it known if unpredictable random bits or only random-looking bits are being used? Making the distinction is crucial to understand if the right level of randomness is there to protect the data. However, in practice, a widespread mistake is to use the tools designed to test the quality of DRBGs to assess the unpredictability of entropy sources, as this does not allow a proper understanding of the security strength of communications.

On April 29, 2022, NIST updated their random number testing documentation[1] to precisely bring awareness to this common mistake. In particular, *"to clarify the purpose and use of the statistical test suite, in particular rejecting its use for assessing cryptographic random number generators".*

A global and unified standard to test entropy quality is still on-going, with the main security agencies collaborating toward a common approach[2].

Navigating the Levels of Random Number Generation

The journey of RNG spans a spectrum from the predictable to the rigorously unpredictable. Understanding these gradations is essential for applications demanding various degrees of randomness, from simple simulations to high-stakes cryptographic operations.

Level 1: The illusion of randomness

At this foundational level, there's a facade of randomness rather than its actual presence. Unfortunately, failing to use a random number is a common mistake in cryptography implementations. For example, in 2010 an attack was shown that could bypass the security measures of the Sony PlayStation. The attack was attributed to an implementation error, using the same number over and over again instead of generating a random number[3].

Level 2: Opportunistic Randomness

In the quest for randomness, Level 2 strategies leverage everyday processes that exhibit seemingly unpredictable behavior as non-dedicated entropy sources. Common examples include keyboard typing rhythms, mouse movements, disk drive timings, clock jitter and variations in network traffic. These RNGs are not specifically designed for generating randomness but are utilized because they contain elements potentially unpredictable inherent in human actions and complex systems.

The appeal of using such sources lies in their accessibility and the perceived randomness they offer. However, these are opportunistic because they rely on external, often uncontrolled factors. For instance, keyboard strokes depend on the user's typing pattern, which can vary but might also contain consistent habits or rhythms predictable over time. In fact, such typing patterns are sometimes used as a mode of behavioral biometric technologies that look to match such (non-random) patterns.

The major drawback of Level 2 RNGs is the lack of control over the quality of randomness. Since these sources are not originally designed for random number generation, they may include tendencies or patterns unrecognized by the implementers. For example, network time jitter might seem random, but if most traffic follows predictable peak and off-peak patterns, the randomness extracted can be less than assumed. Insufficient entropy is a known and documented weakness[4].

Level 3: Engineered Chaos

Level 3 RNGs elevate the concept of randomness by incorporating dedicated entropy sources specifically engineered for the purpose of random number generation. Examples of such devices include ring oscillators and avalanche diodes, which are designed to exploit physical processes known for their apparent inherent unpredictability.

These dedicated devices are linchpins in the architecture of high-grade random number generation. Unlike opportunistic sources used in Level 2, these components are tailored to generate entropy by design. Ring oscillators, for example, use feedback loops in electronic circuits to produce chaotic, high-frequency signals. Avalanche diodes, on the other hand, utilize noise created by electron avalanche breakdown—a

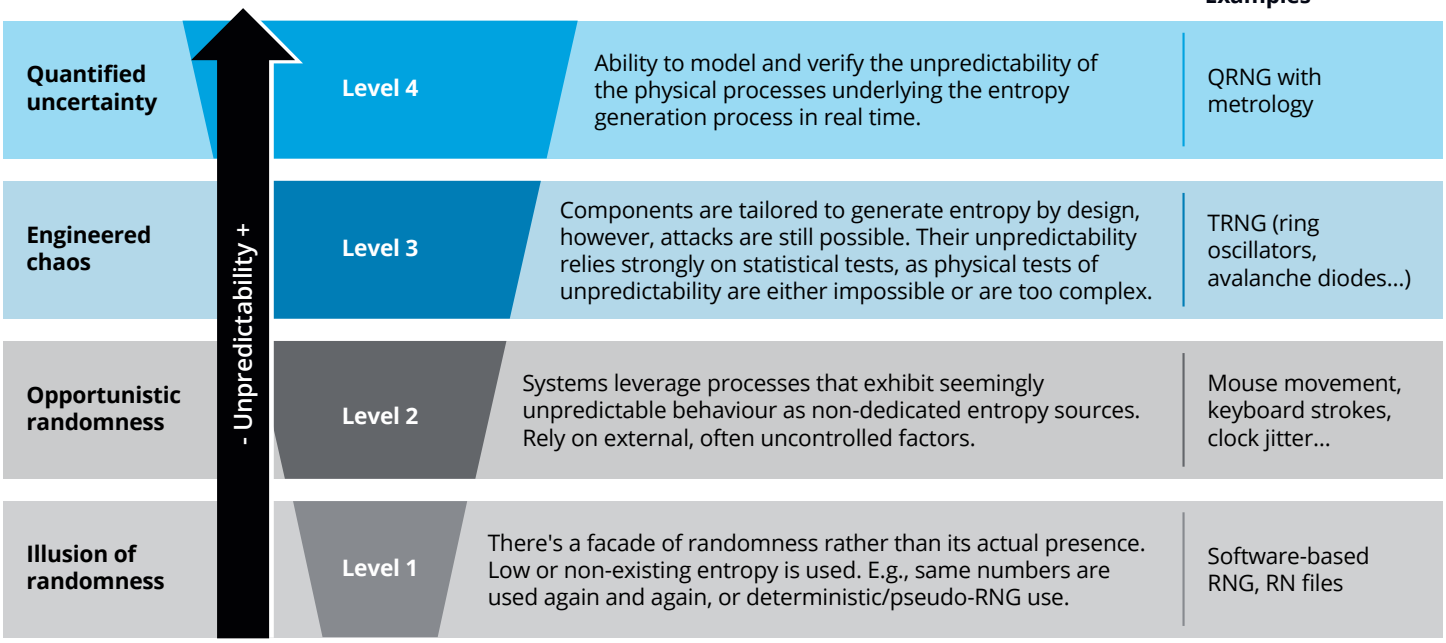
1 Random Bit Generation | CSRC (nist.gov)

2 https://csrc.nist.gov/csrc/media/Presentations/2023/bridging-the-gap-between-the-sp-800-90-series-and/images-media/session-2-mckay-bridging-the-gap.pdf

3 Sony Says PlayStation Hacker Got Personal Data—The New York Times (nytimes.com)

4 https://cwe.mitre.org/data/definitions/332.html, https://nvd.nist.gov/vuln/detail/CVE-2024-31497

Classification of RNG sources



quantum mechanical effect that potentially offers genuine randomness.

Despite the improvement that Level 3 RNGs represent, attacks are still possible[5,6], and entropy quality management is of the essence to ensure security. Unfortunately, understanding the efficacy of most modern designs still relies strongly on statistical tests, as physical tests of unpredictability are either impossible or are too complex to be run in today's devices, which may lead to a limited number of demonstrable RNG solutions.

Level 4: Quantified Uncertainty

Level 4 RNGs represent the zenith of random number generation technology, employing measurable entropy sources that are not only purposefully designed (Level 3 RNGs) but are also provably quantifiable. These systems go beyond merely generating randomness; they provide a framework for continuously assessing the quality of the entropy produced, ideally while operating in the field.

The defining feature of Level 4 systems is therefore the ability to model and verify the unpredictability of the physical processes underlying the entropy generation process; in other words, solely engineering a dedicated physical system (Level 3 RNG) is not enough to guarantee that an operating entropy source is continually producing unpredictable random numbers. This unique security property can be achieved by proper physical randomness tests and verification.

QRNGs provide unique characteristics that fit the objectives of Level 4 RNG security designs. By leveraging the fundamental randomness properties of quantum systems, rigorous physical entropy tests and verification methods can be easily implemented. That said, note that a QRNG can also fall into the Level 3 RNG category unless proper entropy verification means are implemented.

Today, there are several commercial QRNG solutions in form factors ranging from small chips to data center appliances. Operational deployments in space, governmental, data center and even mobile systems are already using this technology today.

Conclusion

The security of billions of devices and petabytes of daily internet traffic is rooted in the proper use of RNGs. Although Level 3 RNG designs still comply with most security standards, it is evident that Level 4 RNGs represent a natural evolution in random number generation and should be used wherever possible. QRNGs stand out as strong candidates for Level 4 RNG designs, due to their inherent advantages. However, widespread adoption of these Level 4 RNGs will depend on various key factors, including cost-effectiveness of these solutions, ease of deployment and the leadership of enterprises, and vendors to overcome inertia and embed the right security components for every element of the IT infrastructure.

5 arXiv:1604.03304v2 [quant-ph] 21 Oct 2016

6 David Lubicz, Viktor Fischer. Entropy Computation for Oscillator-based Physical Random Number Generators. 2024. ffhal-04372984

Deloitte.