QUANTUM-SAFE SECURITY WORKING GROUP

QUANTUM RANDOM NUMBER GENERATORS

cloud security alliance®

The permanent and official location for Cloud Security Alliance Quantum-Safe Security research is https://cloudsecurityalliance.org/group/quantum-safe-security/

ACKNOWLEDGEMENTS

CO-CHAIRS
Bruno Huttner
Jane Melia

CONTRIBUTORS
Jane Melia
Bruno Huttner
Richard Moulds
Nino Walenta
Anthony Fuller

CSA GLOBAL STAFF
Frank Guanco Research Project Manager

INTRODUCTION – A SHORT STORY ABOUT RANDOM

Secure Sockets Layer (SSL) is still a widely used communications protocol that secures web transactions to support the growth of secure online commerce. In the early days, it was implemented in a well-known web browser using a pseudo-random number generator for key generation. Two graduate students reverse-engineered the code and noticed that the seed used by the pseudo-random number generator depended on the time of day and known system information. It was relatively easy for them to guess these quantities, which reduced the possible keys to test in order to crack the protocol. This serious security flaw reduced the time necessary to discover the key to as little as a few seconds, using only one regular PC.

"Random number generation is too important to be left to chance."
(R.R. Coveyou, 1970 [1])

This true story, reported in The New York Times in 1995, greatly damaged the reputation of the company producing the above web browser. It is one of many examples of security vulnerabilities linked to weak random number generators, highlighting how weak random numbers can significantly reduce the strength of otherwise robust and well designed systems. Other examples are outlined in Figure 1.

Topic	Summary	Additional Information
Dual_EC_DRBG	This algorithm was officially recommended by NIST, until it was discovered that it may contain a backdoor, potentially implanted by NSA.	http://www.wired.com/2013/09/nsa-backdoor/
Low entropy in Linux servers	Initially reported in a Black-Hat conference in 2015.	http://www.bbc.com/news/technology-33839925
Untrusted physical RNGs	FreeBSD developers recommend against using the physical RNGs in the processors manufactured by Intel and Via for fear of a backdoor.	http://arstechnica.com/security/2013/12/we-cannot-trust-intel-and-vias-chip-based-crypto-freebsd-developers-say/
Weak keys	There are now well-documented examples, showing how badly chosen or re-used keys damage encryption systems.	https://freedom-to-tinker.com/blog/haldermanheninger/how-is-nsa-breaking-so-much-crypto/ https://factorable.net/weakkeys12.conference.pdf

Figure 1: Weak random numbers, real world stories

SO, WHAT IS A RANDOM NUMBER ANYWAY?

A random number is generated by a process whose outcome is unpredictable, and which cannot be reliably reproduced. Randomness, quantitatively measured by entropy, is the measure of uncertainty or disorder within a set of data. The higher the level of unpredictability, the more random the data is and the more valuable it becomes, particularly for cryptographic operations.

Random numbers are foundational to information security. They are the building blocks of encryption, authentication, signing, key wrapping, one-time codes, nonces, and other cryptographic applications. They are also vital for modeling and gaming. Modern cryptosystems consume surprising quantities of random data to generate keys and perform cryptographic operations.

Given the example above, it will come as no surprise that the performance and characteristics of random number generators have a strong impact on security. Attackers do not usually attempt to crack encryption, they simply steal or guess keys. Poor quality or insufficient quantity of random numbers make that much easier, reducing security well below its designed level and making the overall system vulnerable. Awareness of these issues is reflected in increased scrutiny of RNGs by standards bodies and industry with emerging formal tests of quality. See for example the new Draft NIST Standard SP800-90B [2]

HOW ARE RANDOM NUMBERS GENERATED?

There are two main classes of generators: software and physical. Software generators are known as Pseudo Random Number Generators or PRNGs. They consist of an algorithm into which some initial value –called the seed – is fed, and which produces by iteration a sequence of pseudo-random numbers. In a well-designed algorithm, this sequence may have most of the properties of a random sequence, and thus pass statistical randomness tests. However, it is important to note that computers are deterministic systems: given a certain input, a program will always produce the same output. Because of this very fundamental property, it is impossible for a program to produce a sequence of truly random numbers. By knowing the seed, it is always possible to reproduce the sequence. NIST offers very clear guidance about how to build and use PRNGs for crypto use. However, when designing a system to be "quantum safe", i.e. protected from attacks by

"Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin." *(J. von Neumann, 1951 [3].)*

quantum computers, then all aspects of the cryptosystem must be upgraded – including the RNG - and in that scenario a PRNG is unlikely to be sufficient.

PHYSICAL RANDOM NUMBER GENERATORS

For security or other applications where high quality randomness is needed, physical approaches are taken to generate random bits. Approaches used include voltage fluctuations, clock jitter, atmospheric radio noise, and quantum measurements.

Some important characteristics to look out for are entropy density and throughput. Entropy density is a characteristic of the randomness of the data, and is measured as the randomness per bit, from 0 for a purely deterministic string, to 1 for a purely random one. Throughput represents the quantity of random data, and is measured as the number of bits per second delivered by the generator. For a given throughput, lower entropy will result in keys that are less random, making them more vulnerable to hacking. Low throughput also limits the frequency at which keys can be rotated. Some random number generators with seemingly high maximum throughputs, only have low entropy density from their seed. They may only deliver high entropy levels at very low throughputs, resulting in a real security risk.

While processes described by classical physics such as sounds, mouse clicks, keyboard strokes, network interrupts, hard drive activity can be used to deliver entropy, classical physics is fundamentally deterministic, i.e. predictable for a given set of conditions. In addition, these effects are subject to external influence. Although random numbers generated by classical physical processes are likely to pass randomness tests (indeed, anything that has been hashed will pass the tests), it can be impossible to verify that they are not influenced by their environment, reducing the output quality. As seen earlier, experience shows that even limited information about the key can enable attackers to completely break a cryptographic system.

QUANTUM RANDOMNESS, THE STRONGEST FOUNDATION FOR SECURITY

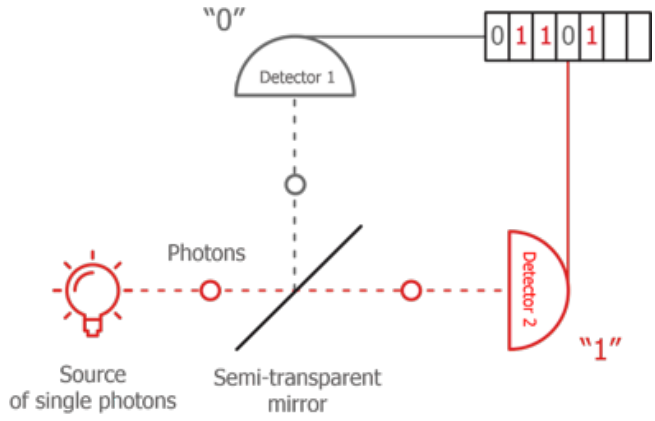

Figure 2: Schematics of a QRNG based on single-photon splitting

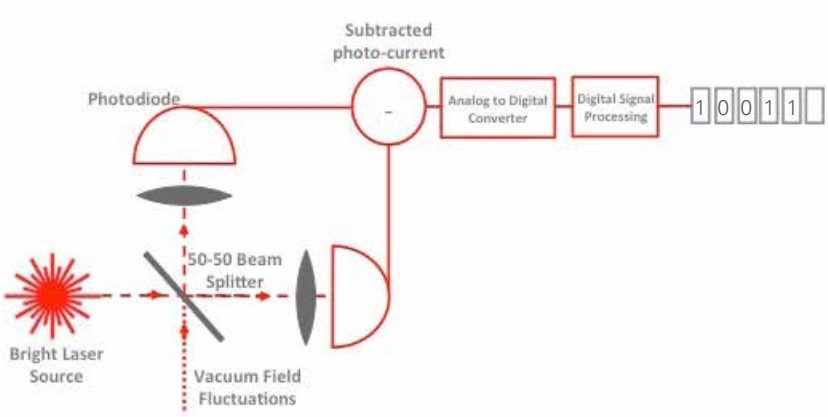

Figure 3: Schematics of a QRNG based on quantum vacuum noise measurements [4]

Generators based on quantum physical processes deliver the highest quality random data. Contrary to classical physics, quantum physics is fundamentally random. This fact was very disturbing to physicists like Einstein who participated in the invention of quantum physics. However, its intrinsic randomness has been confirmed over and over again by theoretical and experimental research conducted since the first decades of the 20th century. It is a natural choice to take advantage of this intrinsic randomness in random number generator design.

Until recently, simple and low cost quantum random number generators did not exist, preventing quantum physics from becoming the dominant source of randomness. However, a number of manufacturers have now been able to address this challenge, leveraging quantum effects in a variety of ways to deliver the highest quality randomness, at high rates and at competitive costs.

One example is a QRNG based on single-photon splitting shown in Figure

2. In this case, single photons impinging on a beam splitter are sent either straight or up. They are then detected by one of the single-photon detectors, to generate a click in one of the detectors. These clicks are registered as either "0" or "1". According to the tenets of Quantum Mechanics, the "choice" made by each photon at the beam splitter is totally random. Another approach is to use a bright laser to measure the vacuum field fluctuations of an electromagnetic field as a source of entropy (see Figure 3). A bright laser beam is split into two beams using a beam splitter and the resulting beams are detected by a pair of detectors. It's at the beam splitter's unused dark input port that the interesting quantum physics occurs. In classical physics, a dark port means there is no input. In the quantum world, however, a vacuum field enters the unused port of the beam splitter and interferes with the laser light on the other input port, imprinting random fluctuations on the phase and amplitude of the output beams at all frequencies. These quantum fluctuations are measured, digitized and digitally processed to generate ultra-high bandwidth random numbers [4]. Further approaches have also been successfully implemented, relying for example on the photon number distribution in a strong beam of light to generate randomness. Several members of CSA's Quantum Safe Security Working Group offer commercial quantum random number generators implementing these techniques: QuintessenceLabs, IDQuantique and Whitewood Encryption.

Given the incomparable quality of the entropy delivered by such solutions, and their commercial viability, the challenges of selecting random number generators that will not expose your data to breaches has suddenly become much simpler. In fact, the question "What source of random should I use" has a simple, safe and commercially viable answer: Use Quantum!

THE QUANTUM-SAFE SECURITY WORKING GROUP (QSSWG)

The focus of the QSS - WG, which was formed within the Cloud Security Alliance, is on cryptographic methods that will remain safe after the widespread availability of the quantum computer. This working group is a forum for corporations, organizations, and individuals who are interested in the topic of quantum-safe security. The mission of the QSS - WG is to stimulate the understanding, adoption, use, and widespread application of quantum-safe cryptography to commercial institutions, policy makers, and all relevant government bodies. Using quantum random numbers is one of the strategies recommended by the QSS - WG to protect and future proof data against improvements to computer power, new attack strategies, weak random number generators, and the emergence of quantum computers.

REFERENCES

[1] R. R. Coveyou, "Random number generation is too important to be left to chance", Studies in Applied Mathematics 3, 70 (1970).

[2] "Recommendation for the Entropy Sources Used for Random Bit Generation", (Second DRAFT) NIST Special Publication 800-90B (2016)

[3] J. von Neumann, "Various techniques used in connection with random digits", Appl. Math. Ser., Notes by G. E. Forstyle, Nat. Bur. Stand., 12, 36, (1951).

[4] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light", Applied Physics Letters 98, 231103 (2011)