Entropy, Predictability and Post-Quantum RNG Design

© June 16, 2017 Scott A Wilber*

Abstract. The emergence of quantum computers and potential quantum eavesdropping may make many of the current methods of encryption and information security obsolete within a very few years [MOS15, NI16a]. A clear understanding of the fundamentals of randomness and random number generators is required to address the ever-changing needs of security designers. The proper use of entropy can make certain "chaotic" generators as unpredictable as any quantum RNG, while typically used deterministic post processing methods can result in an overestimation of nondetermism. Post-quantum randomness may also need to take into account quantum nonlocality, which puts special new requirements on the design of random number generators.

Keywords: Entropy; Full Entropy; Randomness, Random Number Generators, Post-Quantum Randomness

Randomness and Random Number Generators.

Nondeterministic random number generators are primarily distinguished from pseudorandom number generators in that the future output numbers of the former are considered to be unpredictable in a real or theoretical sense, while the future output numbers of the latter are produced by algorithms that are completely predictable given knowledge of the algorithm design and its current state.

In addition to the broad categories of pseudorandom and nondeterministic random generators, generators that use quantum mechanical measurements to provide entropy or nondeterminism may be distinguishable from generators that measure highly complex or chaotic processes that may only appear to be unpredictable by statistical testing. The outcome of measurements of certain simple quantum mechanical systems can be shown theoretically to be indefinite and non-computable [CAL09]. In practice this means a sequence of numbers produced by such measurements will not only be unpredictable, but subsequences will not repeat beyond normal statistical expectation regardless of how many numbers are produced. This is another way of saying its period, the number of numbers output before it begins to repeat the entire sequence, is unlimited or undefined.

Every pseudorandom generator has a finite and definite period, and the ultimate length of the period is limited by the complexity of the computer or device in which its program is running. That is because every computer is a finite state machine, and by definition, it can only take on a finite number of states before it must begin to repeat a previously produced pattern. Theoretically, every physical device can be considered a finite state machine because it is composed of a finite number of particles that can only take on a finite number of permutations or states. However, in a practical sense no physical device is a perfectly closed system, meaning that it may change over time in a

* President of The Quantum World Corporation

fundamental way. Changes can occur in a number of ways, such as by the addition or loss of either energy, or mass in the form of the particles that compose the system.

Random generators that measure thermal noise as their source of entropy are often considered to be primarily classical and therefore chaotic, even though the charge carriers and their interactions occur at the atomic level. A simple model of a real thermal noise source, such as a resistor, includes a certain amount of parasitic capacitance. The parasitic capacitance appears in parallel with the resistor and forms a first order low-pass filter. Therefore, the voltage noise measured across the resistor's terminals will have a finite bandwidth and a simple theoretical autocorrelation function (ACF). A sequence of random numbers produced from voltage measurements of this thermal noise will have the same ACF. It is possible to calculate the autocorrelation of the sampled sequence at any sampling rate provided the transfer function of the measurement circuitry is included in the calculation of a total ACF. Thermal noise is enormously complex because of the very large number of particles involved. In addition, there is essentially no memory between samples due to much higher rate of interactions than the sample rate (up to several GHz). Finally, Heisenberg's uncertainty principle precludes the possibility of accurately measuring both the positions and momenta of the electrons, so it is would appear theoretically impossible to accurately predict thermal noise of resistors beyond the level of determinism produced by the ACF noted above.

The question of whether a quantum source of entropy, such as a photonic generator, can produce random sequences that are truly superior to any other nondeterministic generator is an interesting and important one. While certain fundamental and desirable properties of quantum sources are described theoretically, such the Born rule [LAN09], this is no proof that other entropy types cannot be used effectively. The question really reduces to asking whether the output sequences from either a quantum generator or other generator types have the properties required to make them equivalent in all practical ways. The generated output sequences must only have three characteristics: 1) they must be iid, 2) uniformly distributed and 3) unpredictable by any means. As the length of such a sequence grows without bound, its min entropy and Shannon entropy converge to exactly 1 bit per output bit.

S. Wilber discusses technology and methods for designing nondeterministic random number generators that can produce output numbers of arbitrarily small levels of statistical defect [WIL12]. This is possible regardless of the source of entropy – whether quantum mechanical, chaotic or a mixture of both. Arguably, it is now possible to design nondeterministic generators that can produce output sequences that appear after an arbitrary period of statistical testing to be indistinguishable from subsequences of theoretically perfect sequences.

Entropy as Predictability.

High-quality nondeterministic random number generators require entropy sources based on physical, inherently random processes. Quantum sources include photonic devices, tunneling diodes or leakage currents due to tunneling, certain zener or noise diodes in which a quantum

process dominates and radioactive sources[1]. Microscopic sources include thermal noise in resistors and circuit elements having resistive components, shot noise in diode and transistor junctions (which may also include a quantum component) and avalanche or breakdown noise in diode and transistor junctions, although this last source is not precisely modeled and quantified theoretically. In addition, the noise measured from the entropy source should be primarily intrinsic, meaning inherent and internal to the source. Extrinsic noise sources are contributed by fluctuations in power supplies, externally applied electromagnetic fields and switching noise from nearby circuits. Extrinsic noise is typically periodic or at least deterministic to some degree and can decrease the true entropy measured from the random noise source.

Predictability is the single characteristic that can specify the quality of a random number generator. Every test devised to detect and measure defects in random sequences looks for patterns that translate into a quantifiable predictability above chance expectation. A direct relation can be shown between predictability and entropy [WIL12]. Briefly:

$$H \text{ (entropy in bits)} = -\big(p(1)Log_2 p(1) + p(0)Log_2 p(0)\big) \quad 1.$$

where $p(1)$ is the probability of a "1" occurring, $p(0)$ is the probability of a "0" occurring and for binary bits, $p(0) = 1 - p(1)$. Replace $p(1)$ with P, the predictability of correctly predicting a "1," and entropy becomes;

$$H_P = -\big(PLog_2 P + (1-P)Log_2(1-P)\big) \quad 2.$$

Finally,

$$P = h^{-1}, \quad 3.$$

where h^{-1} is the mathematical inverse of the H_P equation. The inverse is performed numerically since there is no simple closed-form solution. The inverse of the entropy equation has two solutions, but only the one where $0.5 \leq P \leq 1.0$ is taken.

Equations 2 and 3 can be used to design a random number generator with any arbitrary level of predictability. Predictability minus the mean is approximately equivalent to the error of the mean, so the number of bits required to be tested before an error of predetermined significance will be detected can be calculated. Because entropy and predictability are interchangeable in this context, the level of defect may alternately be specified in terms of a deviation from the theoretical entropy of 1.0 as a design target, such as NIST's "full entropy."

By definition the output of a generator based on one type of entropy source with a given predictability (or entropy level) will be no more or less vulnerable (predictable) than the output from a generator with any other entropy source with the same predictability. To ensure against a potential attacker gaining an advantage based on knowledge of the generator's design, it must use an appropriate quantum or microscopic entropy source and the design of the sampling circuitry must capture the inherent randomness they provide. The design and effectiveness of the sampling circuitry is not critical because the amount of entropy in each bit will ultimately determine how many samples must be used for each output bit to achieve the design goal.

---

[1] Radioactive materials are highly limited as entropy sources because the decay rate of a so-called safe source, like the 1 µCi ^{241}Am source used in smoke detectors (producing 37,000 disintegrations per second) can reasonably produce only about 50,000 bits of entropy per second. In addition, regulatory and safe disposal requirements make radioactive materials difficult to use in products.

However, more efficient entropy sampling (lower bias, less autocorrelation and less extrinsic interference) will result in higher output bit rates.

Quantifying and Combining Bits of Entropy.

The use of equations 2 and 3 requires both a reasonably accurate measurement of the statistical entropy in a sequence and a method of combining bits of entropy. The entropy in the sequence resulting from said combining of bits must be mathematically predictable.

Entropy is conveniently estimated using Maurer's Universal Statistical Test [MAU92] revised to be more precise by Coron and Naccache [COR99] who state, 'Maurer's test parameter is closely related to the source's per-bit entropy, which measures the effective key-size of a cryptosystem keyed by the source's output.' This is precisely the practical measure of entropy we need to use.

Fundamental randomness of microscopic entropy sources versus quantum sources.

Quantum mechanical sources of entropy for random number generators are often touted as being inherently superior to any other type of entropy source. This is due to the fact that current quantum theory[2] indicates certain quantum measurements are inherently non-computable and irreducibly random [CAL09]. Even so, this does not automatically make quantum measurements perfectly random. One common type of quantum random generator uses a photonic source, a beam splitter and two single photon detectors, one in each output port of the beam splitter. These detectors are labeled "0" and "1," and the first detector to respond to a low-intensity light pulse causes a bit corresponding to that detector's label to be produced. Invariably any real measurement system will have some amount of bias in the number of 1s output, i.e., $p(1)\neq 0.5$. Even if the system started with exactly zero bias – which would be impossible to confirm by statistical measurement – it would drift over time. Bias translates directly into a reduction in quantum entropy. For example, if the measurement has a bias, $0.45\leq p(1)\leq 0.55$, the per-bit entropy will only be, $H \geq 0.99277445$ (bits of Shannon entropy). If a true "full entropy" output sequence as defined by NIST is desired, this significant defect in *quantum* entropy can only be repaired by consuming two whole measured bits for every output bit, post processed by a NIST approved hash function [NI16b]. Utilizing some type of randomness or entropy extractor [PER92] does not satisfy the NIST requirement for producing full entropy.

Two types of microscopic random processes are identified as entropy sources commonly used in random number generators. These are thermal or Johnson noise and shot noise. Thermal noise is due to thermally excited variations in the electron density in an imperfect conductor (resistor) in thermal equilibrium and shot noise is due to the quantization of charge carriers in a current flowing across a potential barrier whose arrival time is randomly distributed. These sources are called microscopic because their nondeterminism or randomness is based on the unpredictable movement of charge carriers – usually electrons. The physical sources themselves are macroscopic in scale, involving large numbers of charge carriers. While there are other sources of random signals, such

[2] While still a topic of debate, it is generally accepted that our current theory of quantum mechanics is incomplete.

as avalanche and breakdown noise in reverse-biased semiconductor junctions, they are not as well characterized as thermal and shot noise.

These microscopic entropy sources do not have the same theoretical basis of randomness as "pure" quantum sources and they are sometimes mischaracterized simply as chaotic noise[3]. This does not mean they are actually theoretically predictable. Heisenberg's uncertainty principle precludes the accurate measurement of both position and momentum of particles as small as electrons. But for practical purposes, the physical access required to even attempt such measurements would also make any purely quantum mechanical source vulnerable simply by reading the outcomes of the quantum measurements at the output of the measurement system.

Measuring Randomness.

Random numbers used by most modern devices or applications, especially by computers or any systems containing microprocessors or other binary processing circuitry, are presented in the form of binary bits or binary encoded numbers. The sources of these random numbers most often produce them at specific intervals, resulting in what is generally called a time series. The average statistical properties of a time series of random numbers can be presented as a mean (μ or $\bar{x}$), a standard deviation (σ or SD) and an autocorrelation function (ACF). Random numbers are most often simply represented as a sequence of 1s and 0s; for example, (1,1,0,1,0,0,0,1,…). The mean or bias of a sequence of bits is presented either as the probability of a "1" occurring, $p(1)$, where $0.0 \leq p(1) \leq 1.0$, or a fractional bias, $B_F = 2p(1)\text{-}1$, where $-1.0 \leq B_F \leq 1.0$. The SD can be normalized or treated in such a way that it is not independently related to the quality of randomness of the sequence. Finally, the ACF is a fundamentally important property of a random number sequence that quantifies correlations between bits in a sequence and other bits separated by various sampling intervals or orders. While only the bias and the ACF are necessary to specify the statistical properties of a sequence of binary random numbers, a number of statistical measures have been developed to look for specific patterns in such sequences. These specialized tests may reveal certain patterns more quickly and more dramatically [NIS10].

The presence of patterns, along with their type and size, is one definition of statistical defects in random sequences, while the absence of patterns, meaning a fractional bias of 0.0 and an ACF of 0.0 at all orders, indicates a "perfect" random sequence. Of course, such a perfect random sequence can only exist theoretically since it would have to contain an infinite number of bits to even potentially satisfy these two requirements. In a practical sense, statistical defects in a random sequence produced by a real, physical generator can only be tested during a limited test period. It would be unrealistic to test a generator for many years since the generator's developer must either use it or make it available for sale on a reasonable timeline. Instead, statistical properties of a particular generator's output must be specified as limits, for example, $|B_F| \leq 10^{-8}$, or $|\text{ACF}| \leq 10^{-8}$ for all orders up to 10,000. Asserted limits must be based both on large numbers of electronic and statistical tests *and* on a thorough understanding and mathematical modeling of the random generation process.

[3] For a classical chaotic system, given enough knowledge of the current state of the system and sufficient computational power, future states of the system could be predicted.

To illustrate why theoretical limits must be relied upon, the number of bits, n, required for direct statistical testing to a given confidence interval is $n=p(1-p)(z/error)^2$, where the probability, p, is taken to be 0.5, z is the number of standard deviations that span the confidence interval in the normal distribution and *error* is the absolute value of the deviation from the expected mean. For a 95% confidence interval, z=1.96 (for 99%, z=2.576). Given an example *error* of 10^{-8}, the number of bits that must be tested to achieve a 95% confidence interval is 9.604×10^{15}, or about $1/error^2=10^{16}$ bits. Assuming a generation rate of 1 billion bits per second (1 Gbps), it would take over 3 years of continuous testing to complete. NIST defines "full entropy" for random bit generators in its Draft Special Publication 800-90B [NI16b] effectively as $(1-\varepsilon)$bits/bit, where $0 \leq \varepsilon \leq 2^{-64}$. The specified lower limit on entropy is $H=1-5.421011 \times 10^{-20}$, which can be converted to a predictability by using a numerical inverse of the Shannon entropy equation, $P=H^{-1}$ [WIL12] [4]. The calculated predictability is $P=0.5+1.370686 \times 10^{-10}$. The predictability of a perfectly random binary sequence is exactly 0.5. The error or difference from 0.5 is equivalent to an approximate upper limit of statistical defect: $error=1.370686 \times 10^{-10}$. Finally, the length of a random bit sequence needed to directly test for the level of statistical defect complying with NIST's full entropy definition with 95% confidence is 5.112×10^{19} bits. For the example 1 Gbps generator, the duration of testing would be 1,620 years.

Post-Quantum Randomness.

Beyond the distinctions of quantum and chaotic sources of entropy, encryption and data transmission systems are being developed that are also concerned with other, more subtle effects of what is known as quantum nonlocality. Quantum nonlocality is a theory described by Albert Einstein and others that appears to show correlations of measurements in physically separated system that cannot be simulated by classical mechanics or local hidden variable theories. Einstein called this, "spooky action at a distance." While measurements of this effect are well documented by violations of Bell's inequality, every experiment is still expected to be consistent with special relativity, meaning faster-than-light or superluminal communication of information should not be possible.

The definition of post-quantum randomness must also take into account quantum nonlocality, which puts special requirements on the design of random number generators and devices that utilize their random numbers. For two events to be fully and theoretically independent in both a quantum mechanical and a classical sense, they must occur at locations separated far enough so that information cannot move between them at the speed of light. This requirement persists from the beginning of the event that starts first until the end of the event that ends last. These two events are spacelike separated and no information or influence from either event can affect the outcome of the other.

Both the statistical quality and true entropy content of random numbers are of particular importance. Post processing or conditioning of the random numbers after their production may

[4] NIST uses min-entropy estimates while the analysis of predictability, P, uses Shannon entropy. The random data is expected to be approximately normally distributed so the two measures are nearly equivalent. Entropy estimates for practical generators are obtained with Maurer's Universal Measurement [MAU92], improved according to Coron and Naccache [COR99].

give a false sense of nondeterminism. This is because the post processing is invariably done using deterministic algorithms. The simplest – and often used method – entails performing an Exclusive-Or (XOr) function between the random bits and bits produced by a pseudorandom generator. This simplistic approach in no way increases the entropy of the resultant sequence though a *statistical* measure of entropy implies it has.

NIST defines "full entropy" in two different ways:

1) by a limit on the deviation of entropy from a theoretically perfect sequence as discussed above, ie, the lower limit on entropy is H=1-5.421011x10^{-20} bits per bit of the sequence; or,
2) by using a NIST approved conditioning function that outputs one-half or less than the number of min-entropy bits provided to its input.

Note, NIST does not provide a practical description of how a sequence conforming to definition "1" is to be generated or confirmed by measurement. Full entropy sequences can be produced according to definition "2," but it seems unlikely sequences produced using these two definitions will actually have the same level of entropy or statistical defect. Rather these definitions provide two approaches for producing sequences that are considered effectively "perfect" for their intended cryptographic application.

Some commercial random number generator manufacturers claim "full entropy" for their products' output sequences, but their claims are usually not substantiated by technical documentation.[5] They neither follow definition "1," which consumes substantially higher amounts of entropy to produce each output bit, nor definition "2," which would decrease their generation rate by a factor of at least 2.

Summary.

Microscopic electronic sources and quantum mechanical sources providing equivalent true entropy content per output bit will require an equal effort to be predicted by an attacker. This is shown by a mathematical analysis of entropy and predictability and demonstrating their interchangeability. This makes either source as secure in a cryptographic sense.

Every entropy source and measurement system must be designed to resist obvious forms of physical attack, such as exposure to electromagnetic fields or supply voltage variations. Typical countermeasures are EM shielding, voltage regulation and reasonable physical security. To be sure, properly designed quantum sources may be easier to make more resistant to such attacks, but the cost is greater complexity and difficulty of being integrated into current ICs. Ultimately, if an attacker has full physical access to either type of generator, he can simply read the random output and defeat most security protocols.

Post-quantum entropy sources include the use of principles of nonlocality, which is demonstrated by the use of "Bell tests." This is a topic of much current development effort related to the field of quantum key distribution. In addition to the usual Bell tests, relativistic effects (no superluminal communication) can be used to ensure true independence between physically separated generators operating in spacelike separated systems. These limitations of relativity are

[5] With the exception of the PureQuantum™ family of random number generators made by The Quantum World Corporation and sold under the tradename, ComScire. [WIL12]

independent of assumptions of commonly used Bell tests, so they may provide an even greater degree of data security in the light of loopholes yet to be discovered due to our incomplete understanding of quantum mechanics.

BHK05 Barrett, J.; Hardy, L.: *et al*, No Signaling and Quantum Key Distribution, *Phys. Rev. Lett.*, no. 95, 010503, 2005
CAL09 Calude, C.; Svozil, K., Quantum Randomness and Value Indefiniteness, *CDMTCS Research Reports* CDMTCS-291, 2006.
COR99 Coron, J.-S.; Naccache, D., An Accurate Evaluation of Maurer's Universal Test, In S. Tavares and H. Meijer, Eds., Selected Areas in Cryptography, vol. 1556 of *Lecture Notes in Computer Science*, pp. 57–71, Springer-Verlag, 1999
GJD12 Grimaila, M.; Morris, J.; *et al*, Quantum Key Distribution, *ISSA Journal*, p. 20, June, 2012
LAN09 Landsman, N., The Born rule and its interpretation, in *Compendium of Quantum Physics*, Eds. Greenberger, D., *et al*, pp. 64-70, Springer, 2009
MAU92 U. Maurer, A universal statistical test for random bit generators, *Journal of cryptology*, vol. 5, no. 2, pp. 89–105, 1992.
MOS15 Mosca, M., Cybersecurity in an era with quantum computers: will we be ready?, *IACR Cryptology* ePrint Archive Report 2015/1075, 2015.
NI16a Chen, L.; Jordan, S.; *et al*, Report on Post-Quantum Cryptography, NISTIR 8105 DRAFT, Feb., 2016.
NI16b Barker, E.; Kelsey, J., Recommendation for the Entropy Sources Used for Random Bit Generation, DRAFT SP 800-90B (second draft)
NIS10 Rukhin, A.; Soto, J.; *et al*, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, NIST SP 800-22A, 2010.
PER92 Peres, Y., Iterating von Neumann's Procedure for Extracting Random Bits, *The Annals of Statistics*, 20(1), pp. 590-597, 1992
WIL12 Wilber, S., Entropy Analysis and System Design for Quantum Random Number Generators in CMOS Integrated Circuits.