Quantum Random Number Generator (QRNG) Specification Guidelines

Document Version: v3.0
Release Date: Oct 16th, 2024

Prepared by:
Qrypt, Inc.
One World Trade Center, 83rd Floor
New York, NY 10007

Distribution and Ownership
This document is for public consumption and use. Must be distributed intact with Copyright notice.

Qrypt

Table of contents

The continued scaling of quantum computers unlocks computational resources that are infeasible by current classical systems, particularly in encryption breaking and machine learning optimization problems. Apart from encryption protocols, cryptosystem's security also relies on the encryption keys generated from a physical source of entropy with quantifiable randomness. Vulnerabilities arise when terms like 'entropy' and 'randomness' are misunderstood and misrepresented from information theory with an unfounded reliance on statistical measures of randomness compared to actual physical randomness. Conventional entropy sources dependent on a physical process may have some aspects of true unpredictability but are largely deterministic or defective. Generators of random based on probabilistic quantum theory, such as a QRNG, offer an avenue to overcome this vulnerability but must prove that a significant part of its entropy is extracted from a quantum phenomenon while all classical noise signatures vulnerable to pattern recognition are filtered out. These requirements need a standardized approach different from existing methodologies of quantifying and approving random number generators.

1 Scope

This document provides a set of recommendations to evaluate quantum entropy sources as physical generators of true random numbers. We formally define a quantum random number generator (QRNG), describe its general architecture, and propose criteria to evaluate such a device based on first-principles investigation. This document could be considered a guide for establishing QRNG standards by various certification bodies, particularly, the National Institute of Standards and Technology (NIST) and supplements the ITU-T QRNG specification draft issued in 2019 [1].

2 Motivation

The motivation for a QRNG specification standardization is threefold:

1. Outline strategies to evaluate QRNGs that focus on implementation rather than randomness testing. Under NIST's entropy source validation (ESV) program, all RNGs are tested within a common umbrella of entropy sources using standard statistical test suites included in NIST SP 800 – 22 [2] and NIST SP 800 - 90B [3] documents. While these are necessary checks to detect bias in random bit streams, they do not offer completeness in proving absolute randomness or its origin.
2. Based on the evaluated implementation and design, classify the practicability of QRNGs for at-scale deployment and use. This is important as quantum computers that traditionally require substantial infrastructure and isolation are valid sources of randomness but remain infeasible as scalable sources of quantum random (excluding entropy as service methodologies). On the other hand, devices that extract entropy from classical effects (such as CPU jitter, chaotic free-ring oscillators, temperature, etc.) may offer easy scalability, but must be met with caution in regard to verifiable randomness. This effort would supplement the growing need and push to develop and deploy quantum technologies that strengthens national security.
3. Differentiate QRNGs from other classically driven entropy sources. Classical or pseudo-random source of entropy must not be deemed synonymous with true randomness.

3 QRNG Definition

Ideally and broadly, a QRNG may be designed on two necessary requirements – 1) Quantum state preparation 2) Projection measurement on the prepared quantum state. In practical QRNGs, quantum state preparation usually results in a mixed state system (versus a pure one) due to arbitrary system noise (component or conditions based). Additionally, measurement of the prepared quantum state is not perfect and often limited by inefficiencies in hardware elements that make the physical QRNG scheme. These deviations can then generate classical side information on the output of a QRNG source [4]. A conditional min-entropy assessment is needed to determine a lower bound on *true* randomness given all of the side information is known (and can be predicted) by a powerful adversary. This allows us to formally define a QRNG as:

Definition: A QRNG is a device that generates a raw random variable X by applying a projection measurement $\mathbb{P}_s$ on a given quantum state described by the density operator $\boldsymbol{\rho_s}$. The probability distribution P_X of X is given as the trace, $P_X\ (x) = tr(\mathbb{P}_s\boldsymbol{\rho_s})$ for all possible eigenstates of the system. Any classical side information (E) pertaining either to $\boldsymbol{\rho_s}$ (for a noisy mixed state) or to the projection $\mathbb{P}_s$ (as inefficiencies in measurement) is allowed as long as an estimate of E is presented and means to eliminate it are included as a part of QRNG design. The quality of QRNG will be based on the contribution of E to X.

4 QRNG Architecture

Based on the above definition, a QRNG device must have the following functional components:

1. A method or source of preparing a quantum state with probabilities associated for all possible eigenstates.
2. A method to measure or probe the prepared state and produce a digitized probability distribution, defined as raw data.
3. Ability to collect (available during testing) and monitor (available during normal operation) raw data for quantum entropy assessment, system health and calibration.
4. Randomness extraction for eliminating classical side information. This is usually declared as an optional component, however, for any realistic (and practical) QRNG device, the raw entropy is almost always degraded by degrees of freedom external to the quantum measurement and therefore must be a mandatory component of the QRNG design.

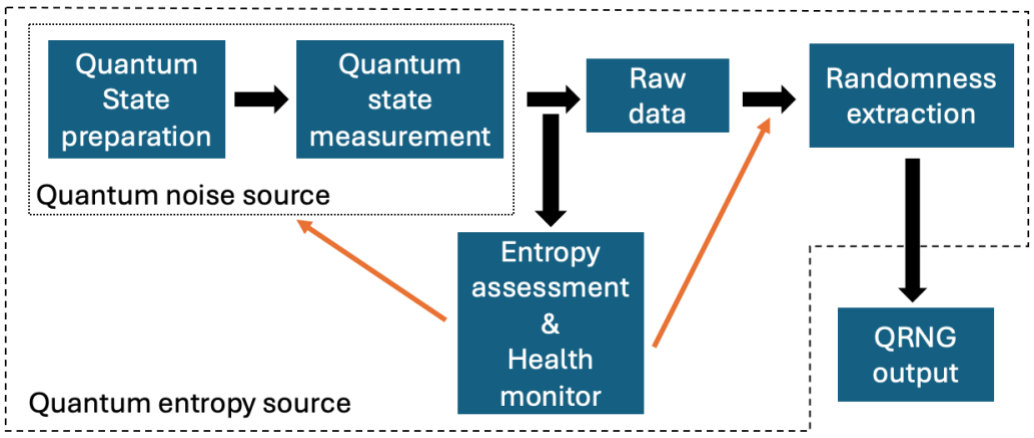

Figure 1 A generic high-level architecture of a QRNG system

5 QRNG Requirements

QRNGs by design must generate entropy based on the probabilistic nature of outcomes contained within the framework of conventional quantum mechanics. The very origin of entropy must be differentiable from classical or semi-classical representations that may generate randomly distributed outputs that are statistically accepted but have nothing to do with performing a quantum measurement. Several requirements are listed below to help make this distinction. It is important to note that QRNGs are broadly classified into three categories – Trusted, Self-Testing (or Device Independent) and Semi-Self-Testing, based on the confidence on the components that make up the physical noise source [5]. For the purpose of this recommendation, we will primarily focus on the Trusted type.

1. Describe the entropy generation process using a quantum mechanical framework. Include alternate classical analogues if any. Must include literature references. Some QNRG examples include (but not limited to) [5]:
    a. **Vacuum noise** – fluctuation in amplitude or phase quadrature of vacuum state
    b. **Optical Shot noise** – fluctuations in the EM field
    c. **Single photon detection/emission** – fluctuations in path probabilities
    d. **Phase diffusion in laser diodes** – fluctuations in phase relationships between spontaneous and stimulated emissions
    e. **Intensity noise in Amplified Spontaneous Emission sources** – fluctuations in photon bunching statistics
    f. **Phase fluctuations in Raman scattering** – fluctuations in photon phase in Raman scattering events
    g. **Tunneling probability through semiconductor junctions** – probabilistic nature of electron tunneling through a barrier
    h. Quantum Computers (using entangled qubits) – Superposition state probabilities of a qubit from a projective measurement.
2. Assuming highest entropy of an un-measured quantum state, describe how the overall entropy reduces once the first measurement is made. Describe how system noise influences the unpredictability of the output.
3. Describe if the output distribution matches the theoretical model. What is the goodness of fit to theory?
4. What is the quantum signal to system noise (QSN) ratio? Provide a quantifiable method to calculate QSN that includes all possible/relevant classical noise influence and side information.
5. Determine the maximum extractable randomness of the measured output, calculated analytically, from the measured distribution.
6. Describe expected variations in output for quantum versus non-quantum entropy generation. The phase space for QRNG generation maybe be narrow for allowed degrees of freedom and design parameters – deviations from constraints may not qualify as performing a quantum measurement or yielding a distribution from a quantum process even if the output *seems or is* randomly distributed. Some examples below:

a. **Phase diffusion in laser diodes**
   The spread (standard deviation) of phase difference ($\Delta\phi$) between two consecutive pulses has a narrow range for QRNG generation. For values $\sigma_\varphi \rightarrow [0, \pi/2)$, transition from an ideal arcsine to gaussian distribution is seen. Although there are quantum processes that generate a gaussian distributed signal, the expected distribution from phase diffusion is arcsine. Raw data from the QRNG should reflect this behavior.
b. **Single photon detection**
   Single photon detectors generate a pulse from avalanche detection of an incident photon, operating at reverse biased voltages close to the breakdown voltage. As a consequence of the design, events based on after-pulsing can generate a trail of pulses that do not correlate with an incident photon or quantum mechanics. These can be arbitrary distributed in the time domain and can't be picked out from standard randomness testing. For QRNGs based on single photon detection, the quantum signal to noise ratio is a direct function of the after-pulsing probability.
c. **Vacuum noise**
   A necessary condition to isolate either the phase or amplitude quadrature of the vacuum (or signa) state is the phase matching with the local oscillator (LO). Classical phase fluctuations (in the LO) can add a component to the balanced output and introduce effects that may deviate from quadrature fluctuations. Moreover, if the responsivity of the two detectors is not identical and deviates with system operational conditions (such a temperature), the quantum quality of the balanced output cannot be preserved unless mechanism are set in place to account for differences.
d. **Tunneling through semiconductor junctions**
   For a tunnel diode, the probability of the electrons to tunnel through the barrier at the junction between *p* and *n-type* semiconductors has a strict dependency on the bias voltage as well as the temperature of device itself. Deviations from electrons tunneling through the barrier from having enough energy to jump over it is minimal as both events produce a gaussian distributed output based on current fluctuations.

7. Describe methods required to verify the quality of entropy generated from QRNG devices under limited access by a third-party user. This will be relevant as QRNG technology becomes feasible and scalable to be easily embedded within a hardware security module or appliance system offering hardware root-of-trust security.

QRNGs must not be entirely validated (or differentiated from pseudo-RNGs) based on statistical tests. The statistical tests are designed to check against null hypothesis for a particular test configuration but cannot give qualitative estimates of randomness originating from a quantum measurement or the degree of randomness. The above requirements (not strictly limited) are therefore based on first-principles methodologies that focuses on functional implementation of the QRNG device.

6 Health Monitoring

The NIST SP 800-90B [3] documents includes health monitoring as a requirement of entropy sources, particularly focusing on entropy degradation and loss via the adaptive proportions test (APT) and repletion count test (RCT). Among other things, it is left up to the designer of the entropy source to include additional health monitors that may address specific failure modes or are more sensitive than APT/RCT tests in detecting entropy loss (such as the sample variance test). For QRNGs, special emphasis must be put to show deviation of data when entropy is extracted from a quantum process versus from a classical event and appropriate monitors must be included to detect this transition. Moreover, factors external to the boundary of the QRNG device, such as operational environment, at its impact on QRNG functionality must be clearly documented.

7 Randomness Extraction

Randomness extraction in QRNG must perform the same function as privacy amplification does in Quantum Key Distribution (QKD) systems. QRNGs based on physical devices generate an output distribution that is most certainly affected by system noise and variable operational conditions. This ultimately degrades entropy quality and is a cause for concern if used as is. As discussed earlier, a measure of true or maximum extractable randomness should be made using conditional min-entropy, assuming all of the classical noise characteristics (from a system design and implementation perspective) are known a priori to an adversary. In this case, conditional min-entropy should then be used to create an extractor with specific criteria to generate an information-theoretic output that closely matches a uniform distribution. To illustrate this point, take the following example of strong extractor based on universal hash functions.

Example: A necessary condition for universal hashing functions to be used as valid randomness extractors is introduced through the famous Leftover Hash Lemma (LHL) [6] which states that to extract ε *-close, m bits* of random out of a probability distribution X with a min-entropy k, the maximum output bit length can be set as $m \leq k - 2\log(1/e)$. Therefore, a minimum entropy loss of $L = k - m \geq 2\log(1/e)$ has to be met. In other words, no method can differentiate the extracted randomness from uniform randomness with an advantage greater than $e = 2^{\sqrt{-L}}$ even if the random seed is completely known.

There are several other methods currently either implemented or discussed in scientific community that have potential to be used as strong-extractors [7], some of which are offered as conditioning components under the auspices of NIST SP 800-90b. For those outside the scope of vetted (by cryptographic algorithm validation program (CAVP)) conditioning components, differentiating between information- and computationally-theoretic implementation is advisable, where the former are more brittle towards entropy loss/degradation, while the latter remain fairly resilient, although less secure in general.

8 Randomness Testing

While the requirements listed in the earlier section may be sufficient to evaluate raw entropy pertaining to a specific QRGN design, any need for statistical testing has already been standardized, in part of the ESV program. Including but not limited to those, we propose several

other statistical methods that are well known in the scientific community with a potential to create a standardized body of statistical test suites broader than the ones implemented using NIST SP 800 – 90B [3] and NIST SP 800 – 22 documents [2]. These are:

1. Statistical test battery for uniform data (post extraction) [8]
    a. NIST STS
    b. Dieharder
    c. ENT
    d. SPRNG
    e. Test U01
    f. Diehard
2. Correlation – Auto and cross correlations (for multiple raw outputs) as a function of bit lag to understand short- or long-range predictability in bits.
3. Borel – Normality (using Calude's criterion) [9], [10]
4. Topological Binary Test [11]
5. Cyclostationarity of statistical parameters defined for the raw distribution (e.g. variance of a gaussian distribution) over longer time periods.

It is important to point out that although statistical test cannot determine true randomness quality, they are powerful checks to detect obvious biases in the output of any RNG device [12], [13], [14], [15]. Statistical randomness testing therefore must be a *necessary but not sufficient* criteria for determining the entropy quality of a RNG device.

9 Future Work

These recommendations are meant to serve as the basis for further discussion and ultimately the establishment of a universal QRNG standard. Due to rising national security concerns by US agencies and private institutions, a need has emerged for technologies that deter future and current cybersecurity threats. QRNGs will be at the foundation of all future cryptography as they directly address the weakest vulnerability of a cryptographic system – the quality of encryption keys. To avoid the biased interests of both established vendors and new entrants into this field, a government architecture and specification will be essential to protect consumers and industry alike.

10 References

[1] ITU-T, 'Quantum noise random number generator architecture', 2019.

[2] L. E. Bassham *et al.*, 'A statistical test suite for random and pseudorandom number generators for cryptographic applications', Gaithersburg, MD, 2010.

[3] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, 'Recommendation for the entropy sources used for random bit generation', Gaithersburg, MD, Jan. 2018.

[4] D. Frauchiger, R. Renner, and M. Troyer, 'True randomness from realistic quantum devices', *ArXiv*, Nov. 2013.

[5] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, 'Quantum random number generation', *npj Quantum Inf*, vol. 2, no. 1, p. 16021, Jun. 2016.

[6] B. Barak *et al.*, 'Leftover Hash Lemma, Revisited', in *Lecture Notes in Computer Science*, 2011, pp. 1–20.

[7] M. J. Ferreira, N. A. Silva, and N. J. Muga, 'Efficient Randomness Extraction in Quantum Random Number Generators', in *Anais do II Workshop de Comunicação e Computação Quântica (WQuantum 2022)*, Sociedade Brasileira de Computação, May 2022, pp. 31–36.

[8] Krister Sune Jakobsson, 'Theory, Methods and Tools for Statistical Testing of Pseudo and Quantum Random Number Generators', *Linköpings universitet, Sweden*, 2014.

[9] A. C. Martínez, A. Solis, R. D. H. Rojas, A. B. U'Ren, J. G. Hirsch, and I. P. Castillo, 'Advanced statistical testing of quantum random number generators', *Entropy*, vol. 20, no. 11, pp. 1–13, 2018.

[10] C. Calude, 'Borel Normality and Algorithmic', *International Conference on Developments in Language Theory*, no. August 1992, pp. 113–129, 1994.

[11] P. M. Alcover, A. Guillamón, and M. D. C. Ruiz, 'A new randomness test for bit sequences', *Informatica (Netherlands)*, vol. 24, no. 3, pp. 339–356, 2013.

[12] D. Hurley-Smith and J. Hernandez-Castro, 'Quam Bene Non Quantum: Bias in a Family of Quantum Random Number Generators', *Cryptology ePrint Archive*, no. 842, 2017.

[13] O. Root and M. Becker, 'Does True Randomness Exist? Efficacy Testing IBM Quantum Computers via Statistical Randomness', pp. 1–12, Jan. 2024.

[14] R. Biswas, D. Roy Talukdar, and U. Roy, 'Verifying the Reliability of Quantum Random Number Generator: A Comprehensive Testing Approach', *SN Comput Sci*, vol. 5, no. 1, 2024.

[15] M. M. Jacak, P. Jóźwiak, J. Niemczuk, and J. E. Jacak, 'Quantum generators of random numbers', *Sci Rep*, vol. 11, no. 1, pp. 1–21, 2021.