REVIEW

A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness

Vaisakh Mannalath[a], Sandeep Mishra[a], Anirban Pathak[a]

[a]Jaypee Institute of Information Technology, A-10, Sector-62, Noida, 201309, India

Abstract
Random numbers are central to cryptography and various other tasks. The intrinsic probabilistic nature of quantum mechanics has allowed us to construct a large number of quantum random number generators (QRNGs) that are distinct from the traditional true number generators. This article provides a review of the existing QRNGs with a focus on their various possible features (e.g., device independence, semi-device independence) that are not achievable in the classical world. It also discusses the origin, applicability, and other facets of randomness. Specifically, the origin of randomness is explored from the perspective of a set of hierarchical axioms for quantum mechanics, implying that succeeding axioms can be regarded as a superstructure constructed on top of a structure built by the preceding axioms. The axioms considered are: (Q1) incompatibility and uncertainty; (Q2) contextuality; (Q3) entanglement; (Q4) nonlocality and (Q5) indistinguishability of identical particles. Relevant toy generalized probability theories (GPTs) are introduced, and it is shown that the origin of random numbers in different types of QRNGs known today are associated with different layers of nonclassical theories and all of them do not require all the features of quantum mechanics. Further, classification of the available QRNGs has been done and the technological challenges associated with each class are critically analyzed. Commercially available QRNGs are also compared.

1. Introduction

The need for randomness is eternal; even in the epics, we see games based on specific devices' random outcomes. In fact, lottery and gambling of some form or other were also in existence in all the early civilizations. With time the relevance of random numbers has been widened, and new applications of random numbers have been found in weather prediction to Monte Carlo simulation [1–3], cryptography to statistical sampling [4,5]. In daily life, knowingly or unknowingly, we often use the output of random number generators. For example, one-time passwords (OTPs) received for various purposes, pins provided by the bank, and CAPTCHAs that appear on your screen when you try to log in at some website are all expected to be the output of a random number generator.

Vaisakh Mannalath. Email: vaisakhmannalath@gmail.com

Sandeep Mishra. Email: sandeep.mtec@gmail.com

Anirban Pathak. Email: anirban.pathak@gmail.com

Naturally, there is intense interest among scientists and technologists in building random number generators, and various types of random number generators have been built and/or proposed in the recent past [6–9]. The output from the random number generator should ideally conform to the principles of uniformity and independence. i.e., the random numbers produced should be equiprobable and there should be no correlations between them. Further, privacy is another crucial parameter for application in cryptography. Interestingly, many of these random number generators are not true random number generators (TRNGs) and can best be referred to as pseudo-random number generators (PRNGs). PRNGs [6,10,11] are based on some deterministic algorithms which convert a small input string into a larger set of strings that satisfy specific tests such as NIST test [12], Die-Hard test [13], etc. to be useful in certain situations. PRNGs can produce random numbers fast, but such random numbers are not truly random as if one knows the algorithm and the initial input string, then all the random numbers can be predicted. Such random numbers can be helpful in situations where privacy is not essential such as simulations and weather forecasting, but not so for the case of secure communication and computation.

TRNGs are different from PRNGs in that it is based on an unpredictable physical process.The solution to get a true random number sequence is to exploit the randomness associated with certain natural phenomena such as atmospheric noise [14], cosmic background radiation [15], thermal noises [16], noises in electronic circuits [17], chaotic systems [18], etc. Such phenomena are so complex that they can produce non-deterministic random numbers. However, the quality of such random numbers is hard to quantify [19]. It is challenging to certify the source of randomness as we cannot discard the possibility that a mature theory in the future will be able to accurately model the physical phenomenon that appears too complex to model at the moment, and hence the generated random numbers become predictable. So, it is always good to rely on a source with intrinsic randomness associated with it. We all know that quantum mechanics is inherently non-deterministic [20,21], so a quantum system can serve as an ideal source to generate truly random numbers [22]. Further, the laws of quantum mechanics can be used to quantify the quality of random numbers. The current quantum technology is quite mature that it is now possible to generate high-quality random numbers which can be used in unconditionally secure cryptography applications [9]. The random number generators which use quantum sources to produce a certifiable source of randomness are known as quantum random number generators (QRNGs) [7,8]. Quantum systems have fascinating facets such as the existence of superposition states, collapse on the measurement, entangled but space-like separated particles, the existence of non-local correlations, the existence of indistinguishable particles [23,24]. Such features are counter-intuitive to our classical minds. These features play pivotal role in making the quantum systems intrinsically random and, hence, provide the sources for a new class of random number generators (QRNGs).

The early QRNGs mainly exploited the property of uncertainty principle of quantum mechanics to build random number generators based on the phenomena of radioactivity [25–27], shot noise in electronic circuits [28–31], etc. Such systems had some drawbacks. For example, we may mention difficulty associated with the handling of radioactive sources and differentiating between shot and thermal noises. Further, they were also slow. To overcome these shortcomings, scientists looked towards exploiting the features of quantum optics and built generators based single-photon detectors [32–43] as well as macroscopic photodetection [44–51]. Similarly, atomic systems were also used to demonstrate QRNGs [52,53], for example, by exploiting the spin noise [54–56].Provided a complete control over the setup, there even exists a QRNG proposal, offering expo-

nential speed-up in public randomness testing. The protocol in $ref.$ [57] achieves this by generating a set of random sequences at once such that randomness of any one those sequences can be evaluated by testing just one sequence among the set. This reduces the complexity in testing the randomness of all the generated sequences. The devices mentioned till now work on the assumption of the trust on the vendors, but there may be situations in which one needs to certify whether the device is working properly or not. Further, the privacy of the output is of utmost importance for applications in unconditionally secure communications. So, the self-testing QRNGs are the next generational devices in which the user can test the devices for privacy and randomness of the output without assuming trust in the vendors. Such self-testing QRNGs usually exploit the nonlocal correlations present in quantum systems. Many interesting experiments on the development of such devices have already been reported in the last decade [58–63]. The major drawback of self-testing devices is that they have very low generation speeds in comparison to trusted devices. So, the solution lies in between with current focus on semi-self testing devices [64–73] which try to optimize the generation rates with the certification.

Above discussion clearly indicates that there are different type of random number generators. A brief classification of known random number generators is shown in Figure 1. Each class and subclass mentioned in Figure 1 will be discussed with appropriate importance in the subsequent sections. However, before we proceed to do that we would like to note that currently, the field of developing QRNG is very active with a slew of companies that have now come up with commercial QRNGs such as ID Quantique [74], Toshiba [75], PicoQuant [76], QuantumCTek [77] with excellent generation speeds and newer startups are coming up every year with new products. In short, exciting developments have been happening and this review aims to share that excitement with the readers.

This review aims not only to track the progress in the development of QRNGs but also to explore the facets of randomness associated with available devices and their applications in specific systems and situations. In particular, we will explore the origin of the randomness of the currently available QRNGs as well as the futuristic devices from the perspective of a set of hierarchical axioms for quantum mechanics [78] in which succeeding axioms can be regarded as superstructure built on top of the structure provided by the preceding axioms. The set of axioms to be used in this review can be briefly described as (Q1) incompatibility and uncertainty; (Q2) contextuality; (Q3) entanglement; (Q4) nonlocality and (Q5) indistinguishability of identical particles. Each of the mentioned axioms has an associated facet of the quantum systems. We know that quantum mechanics has different flavours of non-classicality, and these flavors have a multitude of different origins. The related debates among the researchers working in the foundations of quantum mechanics are still to be settled conclusively. Various people have devised mathematical constructs such as generalized probability theory (GPT) [79,80], generalized no-signalling theory (GNST) [81] and generalized nonlocal theory (GNLT) [82] to throw some light on the origin of quantum mechanical features. Our aim here is not to settle these hotly debated foundational questions, but to classify the QRNGs into new classes based on the origin of the randomness. We will come back to this in the latter part of the review after elaborating on the different classes of QRNGs shown in Figure 1. Further, another area of interest is regarding the certification of QRNGs with respect to the classical and quantum adversaries. Quantum adversaries are more powerful than their classical counterparts as they also have quantum resources in their hand. So, in this article we will also try to compare different QRNGs based on adversarial model.
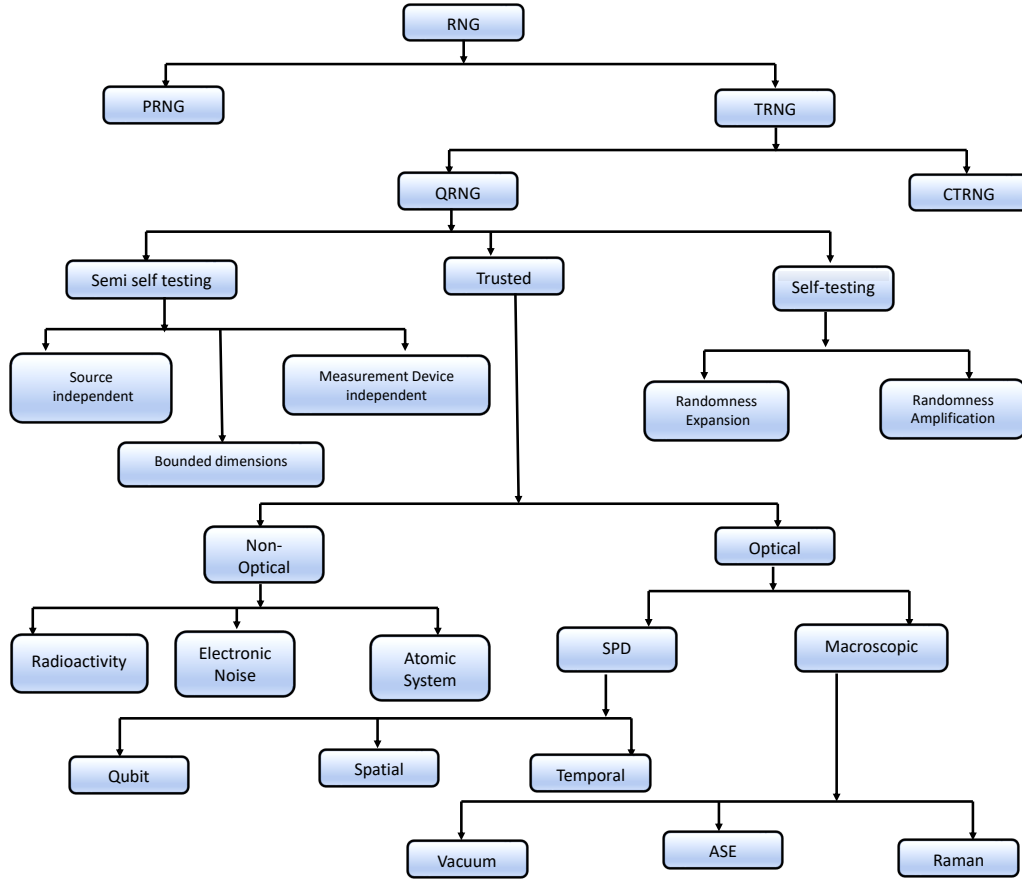
Figure 1. (Color online) Classification of random number generators. The classification is not strict and all-inclusive, with many generators overlapping in more than one class. RNG-Random Number Generator, PRNG-Pseudo Random number generator, TRNG-True Random Number Generator, QRNG-Quantum Random Number Generator, CTRNG-Classical True Random Number Generator, SPD-Single Photon Detector, ASE-Amplified Spontaneous Emission

This review is organized as follows: In Section 2, randomness is mathematically defined in terms of entropy and it's shown that the randomness can be quantified. Subsequently, the differences between PRNGs and TRNGs are explicitly described in Section 3. Then, a detailed overview of the trusted QRNGs is provided in Section 4. Thereafter, we move towards the self-testing QRNGs in Section 5 and semi-self testing QRNGs in Section 6, respectively in sequence. Afterwards, we explore the origin of the randomness in QRNGs in Section 7. Finally, we conclude the review in Section 8 with a brief mention of the commercially available QRNGs.

2. Quantifying randomness via entropy

Entropy measures the amount of randomness present in a system or equivalently the amount of information that can be gained from a system. A simple measure of randomness is given by the so-called Shannon entropy [83]. It gives the average amount of information (measured in bits) that we can extract or gain from the system. For a random variable X with a probability distribution $P_X(x)$, the Shannon entropy $H(X)$ is defined as

$$H(X) = -\sum_{x \in X} P_X(x) \log_2 P_X(x),$$

where X denotes the set of possible values of the random variable x. It measures the ignorance or information gained from knowing the value of the random variable. If some events are more likely than others, the average information gained from knowing an outcome will be less than a uniform distribution. A higher value of Shannon entropy implies that the probability distribution is relatively closer to uniform and vice versa. Clearly, we can see that if the random variable takes only a single value, the entropy is zero, while the entropy will be more if it can take many values with the entropy maximizing at the point when all possible outcomes are equiprobable. We can see an intrinsic connection between randomness and entropy of the system [20,21,84], i.e., the greater the entropy, the more randomness is. Consequently, entropy can be used as a measure of randomness. However, not all entropy measures are appropriate to use in the context of QRNGs. For example, Shannon entropy can only be used under the assumption that the random variables are independent and identically distributed in the asymptotic limit. This is hardly the case in practical setups where device imperfections come into play. For this reason, various other generalized entropies are also defined and connected to randomness [85].

A family of entropies that generalizes the Shannon entropy are the Rényi entropies [86], defined as

$$H_\alpha(X) = \frac{1}{1-\alpha} \log_2 \sum_{x \in \mathcal{X}} P_X(x)^\alpha,$$

where α is the order of the entropy. Rényi entropy reduces to Shannon entropy in the limit $\alpha \to 1$. In general, for different orders of entropy α and β satisfying $\alpha \leq \beta$ we have the relation between the Rényi entropies

$$H_\alpha(X) \geq H_\beta(X)$$

for any distribution X.

A widely used instance of it is the min-entropy $H_\infty(X)$ which is obtained in the limit $\alpha \to \infty$ as,

$$H_\infty = -\log_2[\max_{x \in \mathcal{X}} P_X(x)].$$

It is easy to see that min-entropy acts as a lower bound to all the Rényi entropies. Given a distribution X, $2^{-H_\infty(x)}$ gives the lower bound to the success probability of guessing one of the outcomes. In other words, min-entropy of p implies that every event has a bounded probability of $P_X(x) \leq 2^{-p}$ to happen, and thus we can represent the probability distribution as distributions uniform in p bits. Since k bits can be extracted from a distribution uniform in k bits, for a distribution with min-entropy p, for every outcome, we can extract p uniform bits [87,88].

These measures of randomness via entropy can be extended to study joint distribution where the information content of a random variable may conditionally depend on other random variables. For example, a situation where part of the system is with A and the rest with B. If we denote the combined system with the density matrix ρ_{AB} in the Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \bigotimes \mathcal{H}_B$, where $\mathcal{H}_A$ and $\mathcal{H}_B$ are the sub-spaces of the system accessible to A and B, respectively, we can define the conditional min-entropy [89] as

$$H_\infty(A \mid B)_\rho = \sup_{\sigma_B}\left(-\log_2 \lambda\right),$$

where σ_B is the reduced density matrix of B and λ is the smallest real number such that

$$\lambda I_A \otimes \sigma_B - \rho_{AB}$$

is non-negative.

Conditional min-entropy measures the information gained from the subsystem of A given complete information about the subsystem of B. In other words, $2^{-H_\infty(A|B)_\rho}$ gives the lower bound to the probability of guessing outcomes of A given complete knowledge of B [90]. If the distribution is uncorrelated, we get back the original min-entropy. Further, Konig and Renner [91] introduced the concept of smooth min-entropy defined as

$$H_\infty^\epsilon(A \mid B)_\rho = \sup_{\tilde{\rho}} H_\infty(A \mid B)_{\tilde{\rho}}$$

with $\tilde{\rho}$ such that $\|\tilde{\rho}_{AB} - \rho_{AB}\| \leq \epsilon, \|A\| = \mathrm{tr}\sqrt{A^\dagger A}$. This entropy measures the valid outcomes for any particular sample rather than in the asymptotic limit. It becomes useful in the entropy estimation of randomness generators or in quantifying the capability of the randomness extractors to produce bits as close to a uniform distribution. However, in general, the estimation of min-entropy for a general unknown source is highly non-trivial [92,93]. Repeated measurements can only provide a crude estimate. In most cases, bounds for the entropy are generated using analysis done on the physical source. QRNGs provide a clear advantage in this aspect. Quantum theory describes the randomness source precisely, compared to other generators based on physical processes, say, atmospheric noise. Even in the presence of classical noise or an eavesdropper, available min-entropy can be bounded using the accurate predictions provided by quantum

theory. The existence of good randomness sources with easily quantifiable entropy is not enough if we don't have an efficient way for randomness extraction. Most random number generators with physical sources of entropy do not produce uniform bits; one needs to extract the available min-entropy into a uniform string using a randomness extractor for its practical use. In order to generate secure random numbers at high rates, various practical challenges have to be overcome, and various assumptions used during entropy estimation have to be satisfied. We will expand more on this in the subsequent sections.

3. Pseudo and true random number generators

Deterministic algorithms can create strings of numbers that try to imitate the distribution statistics of random numbers. These algorithms constitute the so-called pseudo-random number generators (PRNGs). On the other hand, if the source of random numbers is unpredictable physical events, they are called true random number generators (TRNG). Albeit not being truly random, PRNGs have the advantage of being extremely fast, and for many applications, it is sufficient to have numbers generated by PRNG. In general, PRNGs use deterministic algorithms to convert a small string of input bits (*seed*) to a larger string of bits that satisfies a specific set of randomness tests that a genuinely random sequence should satisfy [94]. Note that with knowledge of the initial seed and the algorithm used, one can easily predict the output of the PRNG [95,96]. This demands the input seed to be random in each run of the PRNG. The standard approach is to use sequences of uniform distribution from which other distributions can be generated using various transformations [10,97]. Usually, PRNGs are based on the principles of number theory. For example, Lehmer introduced [98] linear congruential generators, which generates random numbers using the recursive formula

$$X_{n+1} = (aX_n + b) \quad mod\ m, \quad n \geq 0,$$

where X_i is the ith digit; which is multiplied by a ($0 \leq a < m$), b ($0 \leq b < m$) is used as the increment, and $m > 0$ is used as the modulus to obtain X_{i+1}. Output numbers are sensitive on these input parameters and are also periodic, though the period is so large that they can be approximated to be random. Thus, the PRNGs are modeled to have considerable repetition periods to be still used as a random sequence. One of the most common pseudo-random number generators used in scientific software nowadays is the MT19937, based on Mersenne Twister (linear shift feedback registers [99]) [100], having a period of $2^{19937} - 1$. PRNGs also need to satisfy additional criteria to be used in cryptographic applications. They follow stricter conditions than previously mentioned generators to increase the security of use in cryptographic protocols and are usually referred to as the cryptographically secure PRNGs (CSPRNG) [7]. Such generators should satisfy forward and backward security, meaning that no algorithm can use the knowledge of a part of the generated sequence to predict any preceding or succeeding bits with a probability greather than achieved by random guessing [101,102]. A notable example of that is the Blum-Blum-Shub generators [103] which are based on the bi-prime factorization problem.

$$X_{i+1} = X_i^2 \quad \mod N$$
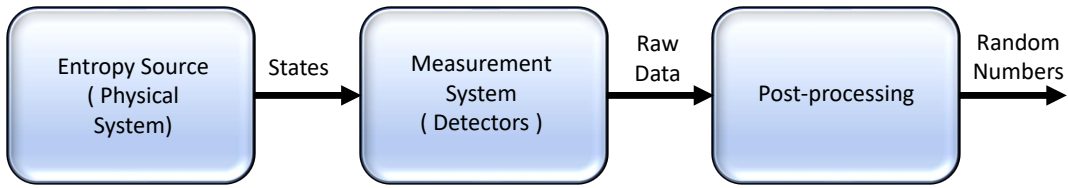
Figure 2. (Color online) Schematic of a true random number generator

where $N = pq$ where p and q are prime numbers. Breaking this generator is shown to be equivalent to the bi-prime factorization problem, which is considered to be computationally secure [104].

PRNGs provide an edge over other randomness generation methods for applications that require fast rates and reproducibility. Under appropriate conditions, they can be used for scientific simulations [105], and cryptographic protocols [106] which requires large amounts of data that only need to mimic random statistics. Not all PRNGs are suitable for this task. It has been shown that linear congruential generators may have correlations undetected by standard randomness tests [107]. Low-quality randomness has been shown to adversely affect the outcomes of scientific simulations [108], and cryptographic protocols [109]. Although PRNGs are faster than alternative random number generators, it is not entirely unpredictable. Since numbers generated using PRNGs can be replicated if one knows the initial value of the seeds, their security will be compromised if an adversary gets hold of it. To take care of this problem, one needs to look beyond the deterministic algorithms used by PRNGs. Certain physical processes are known to be good sources of randomness, whether due to our ignorance of the system or from something intrinsic. A TRNG uses such physical processes as its entropy sources and attempts to extract randomness. The schematic of a TRNG is shown in Figure 2.

In fact, TRNGs are not without their own set of issues that hinder their wider adoption. They generally have a limited generation rate compared to PRNGs. They are limited by the physical processes that function as their randomness. The physical processes used in TRNGs could be anything from user's disk access times in an operating system, mouse motion, or keystrokes [110], to the noise in circuit electronics [17], and chaotic systems [18]. These processes provide a consistent entropy source and can also be complemented with other RNGs for added security [111]. The randomness they do generate is based on our ignorance of a particular physical system, and it is generally hard to quantify the amount of randomness generated. An example would be a TRNG using electrical noise in a circuit as its entropy source. Noise in such systems arises from the shot noise or the thermal noise. It is hard to differentiate between these two sources [112] which becomes an issue when calculating the entropy. This failure to form tight bounds to the entropy makes testing the device for failures much more difficult. For the same reason, the failures occurring within a TRNG are harder to detect, making it prone to attacks [19]. QRNGs are a special case of TRNGs where the physical process that acts as a source of randomness is of quantum origin. For clarity, we will denote TRNGs that can be clearly modelled with the quantum theory as QRNGs and the rest of the TRNGs as Classical TRNGs or CTRNGs.A clear distinction should be made between QRNGs and CTRNGs. The physical processes used in CTRNGs are often difficult to predict due to the incomplete knowledge of the system. Some so-believed CTRNGs,

such as those using thermal noise and data in an electric circuit, may also take advantage of quantum phenomena. The only problem is that we do not know how to evaluate the amount of intrinsic randomness from basic physical principles. In this work, we only refer to QRNGs as devices whos working principles can be clearly modelled using quantum mechanics. Since QRNGs are backed by a well-defined mathematical model of quantum theory one can get a certified source of randomness, which can be checked using the laws of quantum mechanics. The rest of the text will detail various QRNGs, including theoretical models, practical implementations, generation rates, etc.

4. Trusted device QRNGs

Trusted device QRNG assumes that the devices used to extract randomness and the provided source are well characterized. Their simplicity in theory and ease in implementation make them suitable for practical applications. They are only fit for application use if the implementation adequately fits the model. This is highly demanding in an experimental setup since controlling quantum systems is hard. These devices cannot certify whether the output bits are genuinely random or in the control of an adversary. This is why it is referred to as a trusted device. If you trust that your device is working as intended, you could choose appropriate quantum protocols to generate random numbers. In what follows, we will classify trusted device QRNGs into two subclasses: non-optical trusted device QRNGs and optical trusted device QRNGs. Under each subclass, various possible implementations exist, and those are briefly described below with specific attention to their merits and demerits. To begin with, let us discuss different possible implementations of non-optical trusted QRNGs.

4.1. Non-optical trusted device QRNGs

This section will discuss various trusted device QRNGs that do not use optical elements in the randomness generation process. These include random number generators based on radioactive decays and other atomic systems and the systems based on electronic noise present in circuits.

4.1.1. Radioactive Decay

Radioactive decay of particles was one of the first quantum phenomena used to generate random numbers [25]. Radioactivity can only be explained by using the uncertainty principle in quantum mechanics. Hence, QRNGs based on radioactivity effectively exploits the Q1 axiom only i.e. incompatibility and uncertainty. The radioactivity based random number generators depended on sensitive Geiger-Müller (GM) tubes and well-characterized radioactive sources of α, β, and γ radiations. Detectors for β radiations are much simpler and hence widely used. GM tubes produce a pulse for each detected particle using a Townsend avalanche [113]. The probability of decay within the time interval 'dt' is given by

$$P(t)dt = \lambda_m e^{\lambda_m t}dt,$$

where λ_m is the decay constant of the particular radioactive source. The pulses form a Poisson distribution, and the exact rate depends on many factors like the half-life of the sample, position of the sample, state of gas in the GM tube. From the random arrival of
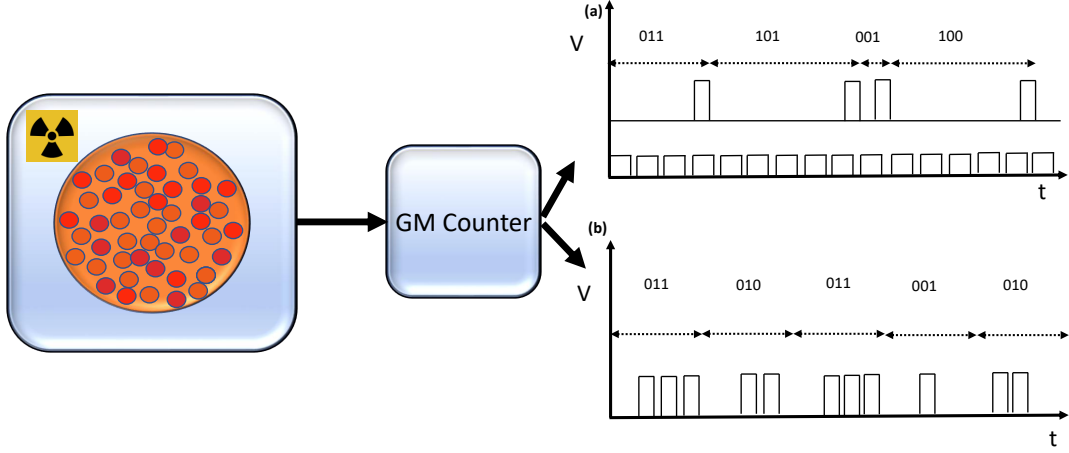
Figure 3. (Color online) Schematic of radioactivity-based TRNG with (a) Fast clock method: Random number generated equals the number of clock cycles between detections made by Geiger detector. [7] (b) Slow clock method: The number of detection made by the Geiger detector in a fixed interval is taken to be the random number generated. [7].

pulses [114], random numbers can be generated using a couple of different ways: (i) Fast clock method [28] (Fig. 3(a)), where the frequency of the clock is greater than the mean rate of detection and (ii) Slow clock method [25] (Fig. 3(b)), where the counts occur more frequently than a clock cycle. By measuring the clock cycles between two successive clicks, the randomness in the time of arrival is converted to bits. Every time detection is made, the fast clock reads and resets itself back to zero, and the corresponding time is used to generate a random number [26]. We can make the obtained distribution more uniform by taking the counts' parity (odd/even). If the counts are taken in binary, this is equivalent to taking the least significant digit or the coefficient of 2^0 in the binary form. For example, if the number of counts is '2', it is written as '10' in binary, and the random number generated would be '0'. For an odd number, let us say '3' or '11' in binary; the generated number would be '1'. The slow clock method utilizes the number of counts in a fixed period to generate random numbers. One should restrict the number of counts to some integer N; a modulo counter. Furthermore, using modulo addition of different counts, one can obtain distributions with arbitrarily small bias [25]. This will decrease the bias at the cost of reducing string length.

Some modern radioactive decay-based random number generators use semiconductor devices instead of GM tubes as it requires less voltage to operate and are convenient [27,115]. Even though the output signals are weaker, they can be amplified further. They simplify the design of the generators. Interestingly, the proposals in [115] produce uniform distribution by using an RC circuit that converts an exponential or Poissonian random variable to one having uniform distribution.

QRNGs based on radioactive sources face severe drawbacks which limit their practical use. Since the randomness source is radioactive, it requires special care (improved safety measures) and knowledge. The radioactivity can also affect the detectors, decreasing their efficiency over time. Detector dead-time due to a buildup of ions inside the detector also poses a limitation. Due to the detector dead-time, GM tubes and semiconductor tubes need some time to recover their full detection abilities after a successful detection event [113]. All of this needs to be taken into account while generating random bits, along with the appropriate post-processing steps [116].

10

4.1.2. Electronic Noise

The noise present in electronic circuits can also be used as a source of entropy in extracting randomness. Typical random number generators based on electronic noises use circuit elements like resistors or diodes as the source of entropy. The noise typically arises due to the quantum nature of the charge carriers. Again, this is due to the uncertainty principle of quantum mechanics, hence only Q1 axiom is utilized. The noise, once generated, can be amplified and used for extraction. A simple method would be to compare the voltage output of the noisy element against a threshold value to generate random bits [28,29]. Another way would be to use the time of arrival methods detailed in Sec. 4.1.1 [30,31].

The noise present in such systems can be broadly classified as shot-noise [117] and thermal noise [118,119]. Shot noise arises due to the quantum nature of the current carriers and is hence truly probabilistic in nature [120]. It is caused by carriers tunneling through quantum barriers created by $p-n$ junctions to create reverse or leakage current, which causes shot-noise. This jumping of quantum carriers shows up as voltage peaks across a diode under adequately low current. Thermal noise, however, is caused by the motion of the carriers in response to the ambient temperature. Ideally, one would want to extract randomness from shot-noise since it's a quantum process in the true sense. However, in practice, it is difficult to isolate these effects [112] and hence extraction of randomness from shot noise suffers from this drawback. They are also known to have memory effects as voltage spikes depend on previous charge flow in the diode and thereby effects the quality of randomness extracted from it [121]. Zener diodes and transistors have been known to predominantly exhibit shot-noise effects under the right conditions [122,123], and there are also commercial QRNGs that use shot-noise as a source of entropy [124,125].

4.1.3. Atomic systems

Apart from the approaches mentioned above for quantum random number generation, there have been proposals for random number generation using atomic systems. For example, in Refs. [52,53], trapped ions were used for random number generation. The experimental setups needed for random number generation using trapped ions are much more complex, and such setups produce random numbers with low generation rates. Still, various proposals for generating random numbers using atomic systems have been reported. Specifically, in Ref. [54], a QRNG based on the spin noise of an alkali metal vapor was proposed. The spin noise arises due to inherent quantum uncertainty and the noise arising due to the interaction between different atoms of the system. Here again, only Q1 axiom is exploited to generate randomness. The signal acquired from such a process has been proved to be arising from a quantum noise and not from optical pumping effects [126]. In the proposed method, the spin noise of the Rubidium vapor was probed optically using a laser and converted to the polarization of a light beam. Under proper conditions, the spin noise can be separated from other background noises, generating random numbers. Further, increase in the bit generation rate have also been reported by the use of solid-state systems [55,56].

4.2. Optical Trusted Device QRNG

Optical QRNGs take advantage of the quantum nature of photons for generating random bits. Optics-based protocols are easier to implement than the methods mentioned above

due to the ease of equipment availability and extensive research that has already been performed for various other purposes. Sources of entropy in this class of QRNGs are the light emitted from LASERs, LEDs, single-photon sources. The light is then manipulated using optical elements and eventually measured. Different protocols utilize different aspects of the quantum nature of light to extract randomness. We classify the different optical QRNGs based on the type of detector used as QRNGs using single-photon and QRNGs using macroscopic detectors.

4.2.1. QRNGs using single photon detectors

The devices belonging to this class utilize single-photon detectors (SPDs) for their functioning. Various techniques can be used to construct single-photon sources (often an approximate one), but we will not go into those details. For more details regarding single-photon generation and detection one may refer to [127,128]. Instead of providing details of single-photon sources, in what follows, we will briefly describe a set of popularly used approaches for the realization of QRNGs using single-photon detectors.

4.2.1.1. Qubit state. These devices generate randomness by measuring qubits in superposition. The principle behind these devices lies in quantum theory's axioms that include collapse upon measurement. Hence, such devices can be explained based on the Q1 axiom only. Specifically, the quantum state of a photon can be in a superposition of possible polarisation states or a superposition of possible paths. For example, if a photon is passed through a beam splitter (BS) then it exists in the superposition state of the sate in the reflected side ($|R\rangle$) as well as the state in the transmitted side ($|T\rangle$). Similar is the case when a linearly polarized photon (typically a photon polarized at an angle 45º with respect to the horizontal) inserts on a polarising Beam splitter (PBS)- a device that transmits horizontally polarized light and reflects vertically polarized light, then at the output the photon exists in a superposition of horizontal($|H\rangle$) and vertical($|V\rangle$) polarization (Fig 4(a)). Any quantum system can exist in a superposition of the basis states, and one can easily design a QRNG using this quantum property of photon along with the collapse on measurement postulate that states that a quantum state would collapse to one of the basis states upon measurement. In the computational basis $\{|0\rangle, |1\rangle\}$ with $|0\rangle$ and $|1\rangle$ respectively, representing absence or presence of the photon, we can define a state $|1\rangle_1|0\rangle_2$ which represents one photon in the first path and no photon in the second path, and a state $|0\rangle_1|1\rangle_2$ with the photon in the second path and no photon in the first path. Then their superposition would look like,

$$\frac{|1\rangle_1|0\rangle_2 + |0\rangle_1|1\rangle_2}{\sqrt{2}}.$$

Measuring the photons at both the arms would yield just one of the superposed states at random. Since there are only two possible outcomes, each detected photon would generate at most one random bit. There have been various implementations based on this principle involving beam splitters, and photo-multiplier tubes as detectors [32,129], Fresnel multiple prism and avalanche photo-diodes [33], and the fiber-based implementations [130]. The bit generation is limited to tens of Mbps [32].

One can also think of a non-optical equivalent of these QRNGs. As a simple example, we may consider that we are using a cloud-based quantum computer of IBM [131] which gives free access to superconductivity based 5-qubit quantum computer, where all the qubits are initially set to state $|0\rangle$, if we now place one Hadamard gate in each qubit

line and subsequently perform measurement on each qubit line. Each measurement will randomly yield 0 or 1, and after each run of the experiment, we can have a 5-bit random number. IBM allows us to run an experiment 8192 times in a go and store the output in a sequence using the command "$result.get\_memory()$" [132]. Thus, a single run of such a simple cloud-based experiment can give a $8192 \times 5 = 40960$ bit long string of random numbers. Of course, repeated runs or access to larger quantum computers can increase the size of the random numbers, thus generating the speed equivalently. This is noted just as an illustrative example to show that there are non-optical equivalents of the optical RNGs, and one can realize such a thing through cloud-based access of the quantum computer- a much more costly resource than a usual QRNG.

QRNGs based on the quantum state of photons suffer from practical drawbacks related to the detectors used. After every detection event, the detectors are inactive for a certain period during which they cannot detect photons. This period of inactivity is referred to as the dead-time of the detector. This will lead to correlations between the bits generated and increase the time required for acquisition. This could be avoided by using just one detector as in [34]. They connected two fibers of different lengths to the same detector and used the delay to distinguish between the two paths. Detectors could also detect multiple photons at once and may click even when no photons are present due to device imperfections. All of these effects influence the randomness and generation rate of the bits produced [32,35,130,133,134]. The random bit generation rates could also be improved if the generator measures multiple paths [36]. If the photons take more than two paths (say, n paths), we can represent it as

$$|W_n\rangle = \frac{|10\cdots00\rangle + |01\cdots00\rangle + \cdots + |00\cdots01\rangle}{\sqrt{n}}.$$

Measurement in the path basis on the n paths would result in one of the detectors clicking, yielding $\log_2(n)$ bits of randomness. Unfortunately, this requires a much more complicated setup than the previously mentioned ones.

4.2.1.2. ***Temporal mode:.*** Temporal QRNGs generate randomness from the arrival time of photons. They are very similar to the QRNGs based on radioactive decay discussed in Section 4.1.1, hence use only the Q1 axiom. Typically they have improved random number generation rate compared to radioactive decay since photon production is much faster. A standard temporal mode QRNG consists of a weak photon source, detectors, and timers. These devices generally use LEDs or LASERs for photon generation, and they follow an exponential distribution given by $\lambda e^{-\lambda t}$, where λ is the average photon number [37]. A simple approach to generate random numbers from the arrival time of photons would be to represent t_1 and t_2 as the arrival time of consecutive pulses and assigning 1 if $t_2 > t_1$ and 0 if $t_1 > t_2$ (cf. Fig 4(b)), giving a uniform random bit [38,135]. The precision of the measured arrival time limits the randomness generation rate. Counts registered during a specified interval of time would be considered instantaneous due to the limited precision of the measuring instrument. The basic scheme that we mentioned would raise an error, and the counts would be unsuitable for random number generation. Yet another way of generation would be to count the number of clicks (cycles) using a fast (slow) clock, as in 4.1.1. All such methods need to convert the randomness obtained from the exponential distribution to a more uniform bit sequence. There have also been implementations that use a uniform distribution of arriving photons. The generators in [136] uses special circuitry to convert the exponential
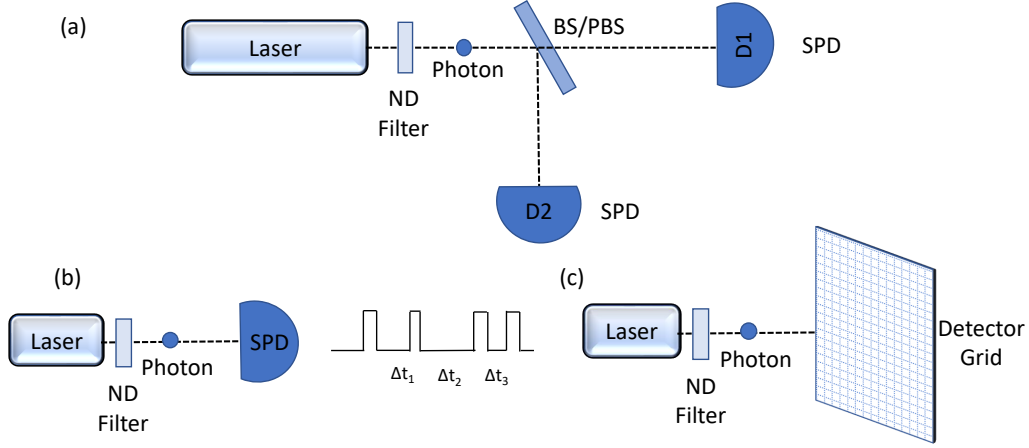
Figure 4. (Color online) Schematic of (a) Qubit based QRNG where a photon in the $(|H\rangle + |V\rangle)/\sqrt{2}$ state (Horizontal and Vertical) is prepared. A polarizing beam splitter (PBS) selectively permits one of the vertical or horizontal states. In case of beam splitter (BS), a photon exists in the superposition state $(|T\rangle + |R\rangle)/\sqrt{2}$ (Reflected and Transmitted). A random bit can be generated by measuring the photon using two single-photon detectors (SPDs) (b) Random bits generated by measuring the time interval between two detection events (c) QRNG based on measurements of photon spatial mode. The SPD array detects photons with some probability depending on the spatial position of the detected photon [8].

distribution of incoming photons to a uniform one. The temporal-mode alleviates the impact of detection dead-time, unlike the methods based on superposition states (say, qubits) and generally has higher bit generation speeds. Generation rates are around around 109 Mbps [37] with an entropy of 5.5 bits per detection.

4.2.1.3. Spatial mode:. Yet another method to generate random numbers is by measuring the spatial mode of a photon. [39,40]. This is usually done with a space-resolving detection system as shown in (Fig 4(c)). Here also, only the Q1 axiom is sufficient for theoretical explanation. Experimental demonstration of the spatial mode technique using an array of detectors was done in [41]. The spatial distribution of the light's intensity and the detector's efficiency affects the random numbers generated. Multiple random numbers can be generated per run with this method. Correlations formed by a large number of detectors make it impractical for commercial purposes. The practical implementation was able to generate up to 16 bits per detection with an entropy of 0.999856 at a speed of 8 Mbps [39]. There also exist generators that use both time and space uncertainties associated with the photons to generate randomness [137,138].

4.2.1.4. Multiple photon-number states:. These devices generate randomness from measuring quantum states containing multiple photons [42,43,139,140]. For example, by measuring the photon number of a coherent state,

$$|\alpha\rangle = e^{\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

14

which is a superposition of photon-number states with $|\alpha|^2$ as the mean photon number, we can obtain random numbers that follows Poisson distribution. This is usually achieved by utilizing a multi-pixel detector arrangement. Since the photon number follows a Poisson distribution, suitable post-processing is required to make the distribution uniform. Some generators use time difference comparisons, similar to what is already discussed in the previous section [141], while others generate randomness based on the counted photon number, but the working of such devices can by explained by considering Q1 axiom only. A particular implementation of such a scheme of random number generation with 1.99 random bits per detection and a speed of 144 Mbps was reported in [142]. The photon count variations have also been applied in random number generation using a mobile phone [143]. Interestingly, these schemes are sensitive to photon number statistics and the detector's efficiencies.

The devices discussed so far use weak coherent sources as their single-photon source. The mean photon number of such sources should be attenuated around 0.1 to be considered a single-photon source, whereas a genuine single-photon source can achieve a mean photon number of 1. Solid-state single-photon emitters are a promising prospect in this direction, and much research has been focused on it over the past decade. Recently, there has been various implementations of QRNGs using solid-state single-photon emitters based on nitrogen vacancies in diamond [144], gallium nitride [145], hexagonal boron nitride single-photon emitters [146]. Such devices have great potential in integrated quantum devices, although technical challenges pertaining to the complex mesoscopic environment of the solid-state need to be addressed [147].

4.2.2. Macroscopic Photo-detection

In this type of QRNGs, more classical quantities, like intensity, amplitude, etc., are measured instead of single photons to generate random numbers. Modeling these QRNGs is more complicated, and care must be taken to ensure that the dominant source of randomness is quantum. One upside is that these devices can circumvent the SPD dead-time limitation and hope to achieve a higher generation rate. The advantage obtained in this scenario is quite similar to the one obtained in the case of quantum key distribution protocols involving optical homodyne detection [148] achieving higher key rates over a low loss channel. We will discuss two examples of this class based on vacuum noise and amplified spontaneous emission.

4.2.2.1. Vacuum noise:. These QRNGs utilize the randomness in the zero-point fluctuation of the electromagnetic field, which is based on Q1 axiom. In quantum optics, the vacuum state is represented by a two-dimensional Gaussian distribution centered at the origin with an uncertainty of 1/4 (see Figure 5 (a) for its representation in the phase space). The amplitude and phase quadratures of the field can be measured repeatedly, thereby generating random numbers [44]. This uncertainty is present even though the vacuum state has zero photon number. The vacuum state, the source of randomness, can be easily prepared with high fidelity. Being a continuous variable, the measurement of the field quadrature of vacuum generates more than one random bit per measurement. In a particular example [45], 3.25 bits of random numbers were generated per measurement. A strong laser pulse is sent through one end of a symmetric beam splitter, and the other port is blocked to simulate a vacuum state. The output is then measured through two detectors, and the signal is obtained by taking the difference between the two outputs. The detection is done using the balanced homodyne detection scheme (cf. Figure 5 (b)). Detector losses can be compensated by increasing the oscillator power.
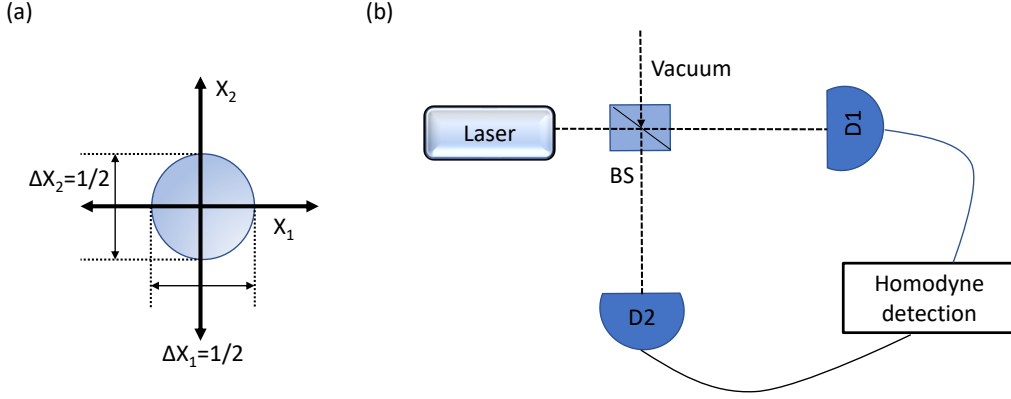
Figure 5. (Color online) (*a*) Phasor diagram for the vacuum state. The uncertainties in the two field quadrature are identical, with $\Delta X_1 = \Delta X_2 = \frac{1}{2}$. (*b*) Schematic of QRNG based on vacuum noise measurements [8].

The random number generation rate of these devices is limited by the speed of the detector in the shot-noise region where the overall observed noise is dominated by vacuum noise [46]. Realistically, shot noise is not the only noise present in the detectors, and an adversary can control the additional noises. Practical implementations have reached a generation rate of 3 Gbps [47].

4.2.2.2. Amplified spontaneous emission:. Phase noise of amplified spontaneous emission is quantum mechanical in nature and can be used to generate randomness [48]. It is not limited by the shot noise region for detectors, as in the case of generators based on vacuum noise and is usually faster than them. In this particular class of QRNG, field quadratures of phase-randomized weak coherent states are measured to obtain random numbers [49]. Again, the randomness can be explained by considering the Q1 axiom. The uncertainty in the quadrature of the signal state is of the order $n \left\langle (\Delta\theta)^2 \right\rangle$, where n is the average photon number and $\left\langle (\Delta\theta)^2 \right\rangle$ is the phase noise variance. If n is sufficiently large, the phase uncertainty can be significantly larger than the vacuum noise. Hence, it is generally robust against detector noise. One way of implementation is using lasers, and heterodyne measurement [149]. Interference of laser beams causes a variance in the output signal caused by the phase difference between the two input beams [150]. Phase difference due to the unequal lengths of the interferometer is taken into account in the randomness generation process. Implementation involving pulsed laser sources where the phase difference between consecutive pulses is used to generate random numbers has also been demonstrated [151,152].

4.2.2.3. Raman Scattering:. The inelastic scattering of photons by vibrational modes of molecules is known as Raman scattering. Various QRNGs use the phenomena of Raman scattering for gathering entropy in the form of randomized phase [50], or amplitude [51] of the output field. We will be discussing random number generation based on two types of Raman scattering processes, namely spontaneous Raman scattering (SpRS) and stimulated Raman scattering (SRS) processes. In SpRS, a photon is
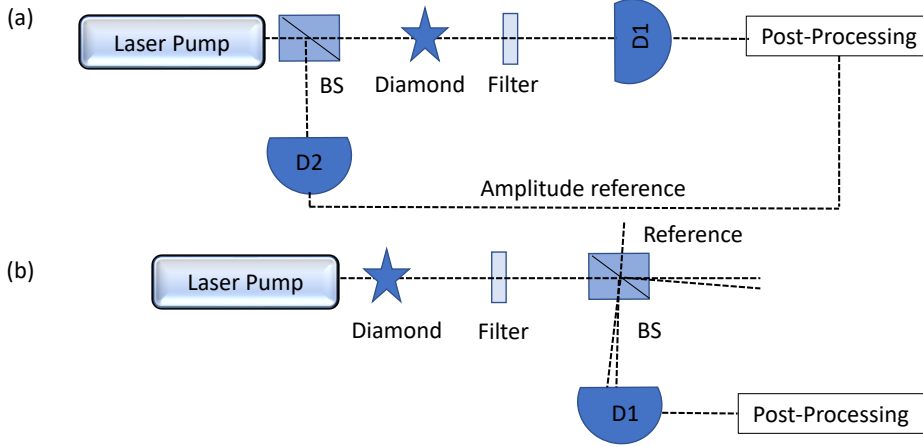
Figure 6. (Color online) Schematic of QRNG using Raman scattering (a) with the amplitude fluctuations as a randomness source [51] (b) optical phase as randomness source [50].

scattered as it interacts with a molecular lattice that absorbs or creates a phonon to spontaneously generate photons of a higher frequency (anti-stokes) or lower frequency (stokes). In the case of SRS, some Stokes photons that have previously been generated by SpRS process amplify the emitted light as incoming photon interacts with the lattice. QRNGs based on Raman scattering work in a manner similar to ASE noise generators; SpRS photons that are produced at random from quantum noise are amplified in an SRS process [153]. Fluctuations in the phonon field of the material induce the spontaneous emission to the Stokes field [154] and the generated photons induce new Raman scattering processes, and the field is amplified to a macroscopic level. The quantum fluctuations at the initiating process can be viewed as uncertainty in amplitude (photon number) and the optical phase at the output field. So, Q1 axiom is sufficient to explain the randomness os such devices. In a generator based on phase, difference [50], optically pumped diamonds are used to generate Stokes field of random phase. These are then detected as interference patterns, the intensity patterns of which can be converted to a random sequence. For generators based on amplitude fluctuations [51] interference is not required, making it a simpler detection scheme Figure 6(a). The intensity values measured for the output field are compared with a reference and corrected. Intensity ranges are subsequently assigned to bit strings for generating random numbers.

Several other trusted device QRNGs exist, which do not fit into the abovementioned classes. In order to reduce the physical dimensions, QRNGs have been implemented in different substrates such as indium phosphide (InP) [155], lithium niobate (LN) [156], silicon-on-insulator (SOI) [157], silicon nitride (Si_3N_4). Such devices have applications in photonic integrated circuits. These devices use electron-beam lithography to etch directional couplers that form the basis of the on-chip beam splitter. They are sensitive to temperature changes as the protocol depends on the substrate's refractive index, which is temperature-dependent. Sensitivity to the wavelength used and large optical losses are some of the other drawbacks. A brief history and comparison of several trusted device QRNGs implemented over the years are presented in Table 1. They are compared based on the type of assumptions, usage of detectors, and their bit generation speeds.

17

Year	Physical principle	Detection	Speed	Adversary Model
2000	Electronic Noise[31]	IC	1.4 Mbps	Classical Adversary
2000	Spatial Superposition [32]	SPD	1 Mbps	Classical Adversary
2000	Spatial Superposition [158]	SPD	100 Kbps	Classical Adversary
2005	Radioactive decay [27]	PIN photo diode	1.6Kbps	Classical Adversary
2008	Time of arrival statistics [159]	SPD	4 Mbps	Classical Adversary
2008	Spin Noise[54]	Polarimeter	1 Kbps	Classical Adversary
2009	Time of arrival statistics [160]	SPD	40 Mbps	Classical Adversary
2009	Spatial Superposition [161]	PNRD	500 Kbps	Classical Adversary
2010	Photon number statistics [42]	PNRD	50 Mbps	Classical Adversary
2010	Laser Phase Noise[150]	Self-Heterodyne	500 Mbps	Classical Adversary
2010	Vacuum fluctuations[44]	Homodyne	6.5 Mbps	Classical Adversary
2010	Vacuum fluctuations[45]	Homodyne	12 Mbps	Classical Adversary
2010	Time of arrival statistics [136]	SPD	110 Mbps	Classical Adversary
2011	Vacuum fluctuations [47]	Homodyne	2 Gbps	Classical Adversary
2011	Electronic Noise [162]	PIN photo diode	4 Gbps	Classical Adversary
2011	Raman Scattering [50]	Homodyne	6 Kbps	Classical Adversary
2011	Photon number statistics [141]	PNRD	2.4 Mbps	Classical Adversary
2011	Time of arrival statistics [163]	SPD	152 Mbps	Classical Adversary
2012	Laser Phase Noise [164]	Self-Heterodyne	6 Gbps	Classical Adversary
2014	Time of arrival statistics [37]	SPD	96 Mbps	Classical Adversary
2014	Time of arrival statistics [165]	SPD	1 Mbps	Classical Adversary
2014	Photon number statistics [140]	SPD	200 Mbps	Classical Adversary
2014	Electronic Noise [166]	IC	32 Mbps	Classical Adversary
2015	Laser Phase Noise [49]	Self-Heterodyne	68 Gbps	Classical Adversary
2015	Vacuum fluctuations [167]	Homodyne	3.55 Gbps	Classical Adversary
2015	Electronic Noise[123]	PIN photo diode	23 Kbps	Classical Adversary
2015	Photon number statistics [142]	PNRD	143 Mbps	Classical Adversary
2015	Time of arrival statistics [38]	SPD	1 Mbps	Classical Adversary
2016	Laser Phase Noise [168]	Self-Heterodyne	5.4 Gbps	Classical Adversary
2017	Electronic Noise [169]	SMU	3.5 Kbps	Classical Adversary
2018	Photon number statistics [170]	PNRD	100 Mbps	Classical Adversary
2018	Spatial Superposition [171]	PNRD	18.2 Mbps	Classical Adversary
2018	Laser Phase Noise[172]	Self-Heterodyne	600 Mbps	Classical Adversary
2018	Vacuum fluctuations[173]	Homodyne	8 Gbps	Quantum Adversary
2019	Vacuum fluctuations [174]	Homodyne	1.5 Gbps	Classical Adversary
2019	Vacuum fluctuations [175]	Homodyne	6 Gbps	Classical Adversary
2019	Vacuum fluctuations [176]	Homodyne	8.25 Gbps	Classical Adversary
2021	Vacuum fluctuations [177]	Homodyne	2.9 Gbps	Quantum Adversary
2021	Electronic Noise [178]	SMU	90 Kbps	Classical Adversary
2021	Time of arrival statistics [179]	SPD	200 Kbps	Quantum Adversary

Table 1. A comparison of various trusted QRNGs; SPD-single photon detector, PNRD-photon number resolving detector, IC-Integrated Circuit, SMU- Source Measure Unit

5. Self testing QRNGs

The methods described until now for the generation of random numbers rely on absolute trust in the used devices. However, this is not valid in realistic scenarios. Moreover, the trusted QRNGs exploit only the Q1 axiom for generation of randomness. In practice, the devices may be defective or could even be in the control of an adversary and hence the generated random numbers become vulnerable. So, some form of testing system should be in place to verify the output sequence of the random number generator [180]. They can be modeled to monitor the internal state of the generator and notify the user of a sudden failure of the device or if its output is biased [181,182]. However, now the user is required to trust the checking device, and we run into the same problem again. The implementations that we have detailed so far in the previous sections cannot rule out the possibility of a malicious vendor who supplies the checking devices. However, without an appropriate checking system, trusted device QRNGs cannot even differentiate the effects of classical noise from the generated numbers, thus putting a risk on the security of generated random numbers. Hence, it is better to include at least some self-testing systems in terms of security. We will now explore existing protocols in certifying generated random numbers from QRNGs.

If we assume that the vendor is not malicious but that devices may not be working perfectly, then the security of the protocols discussed so far can be increased by adding a checking system to them. For example, the quantum random number generator proposed in [183] uses a circuit that evaluates the time of arrival of pulses from a Geiger counter against a Poisson distribution for any discrepancies. Only sequences that pass this test are used in the extraction stage, while the others are discarded. [184] uses tomography techniques to estimate the matrix which describes the entropy source. Although this reduces the privacy of the numbers, it enables the user to estimate a lower bound on the min-entropy of the sequence based on the input quantum state. Further, the characterization of the input state offers protection against attackers that can alter the system's state. Vallone et al. [185] provides a solution that does not require tomography of the system by randomly choosing between mutually unbiased bases for detection as they use the uncertainty principle to prove a bound on the amount of correlation the output sequence can have with the environment. The experimental demonstration was done using entangled photons, then measured based on polarization angles.

Another intriguing and conceptually interesting approach to certifying random numbers from a QRNG is by ignoring the device's details and focusing only on the input-output statistics. Certification is done by comparing the output distribution against the distributions dictated by physical laws that one assumes to be true [58]. Self-testing QRNGs exploit this idea in the form of witnessing non-locality [186] by observing a Bell inequality violation (Figure 7). The term self-testing was first used in ref. [187] in the context of quantum cryptography with imperfect sources. Essentially, such tests enables one to rule out local deterministic models of description for a particular setup by exploiting the Q4 axiom of quantum mechanics i.e. non-locality. Experimental results have supported quantum theory, and more sophisticated experiments are continually closing loopholes and alternative explanations. Classical randomness can be differentiated from genuine randomness from the amount of non-locality. Although this method has high credibility, it is hard to implement experimentally. It also suffers from the drawback of meager speed for generating random numbers. Further, if we consider a completely device-independent setting, the devices should have randomized strategies and should invoke some form of non-locality. If the devices follow a deterministic protocol, then an adversary needs only to supply the devices with a set of data that passes the test
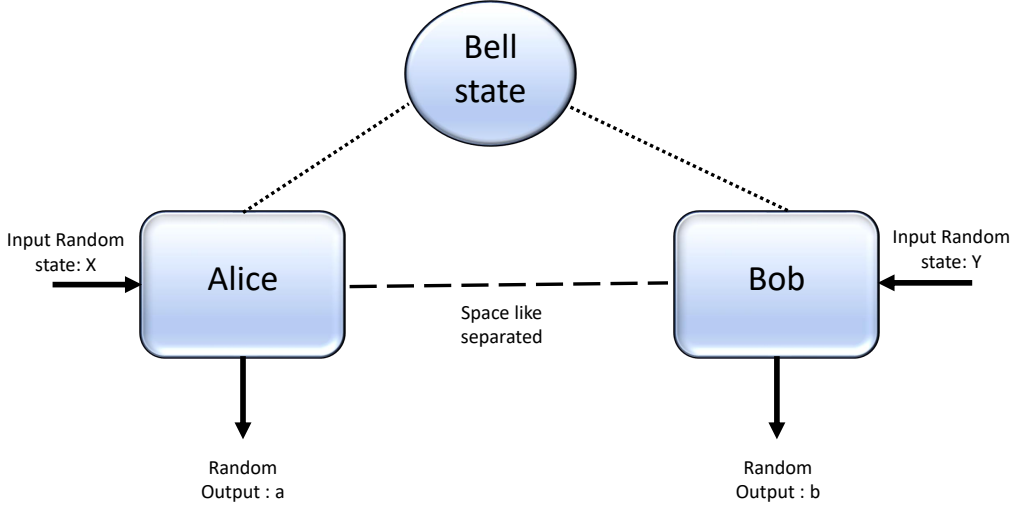
Figure 7. (Color online) Schematic representation of self-testing QRNG based on a Bell type inequality. Alice and Bob are space-like separated and share entangled state ρ between them. For some random input random numbers X and Y, Alice and Bob will respectively obtain the outputs a and b. The device can be tested via the violation of some Bell-type inequality [8].

that we have put in place. On the other hand, if the protocol is local, an adversary could supply the devices with the outputs with every choice of the input operation, rendering the test useless. Thus, it requires the user to access genuine random numbers and non-local states initially. In a sense, such protocols essentially expand the amount of randomness one has access to rather than generating randomness out of nothing, and thus it can be also be viewed as a device for random number expansion [58].

As the discussion above indicates that there may be schemes for random number expansion, We will now look at various random number expansion protocols in detail.

5.1. Self testing Random number expansion

Random numbers generated using practical devices may depend on some classical variables, depending on the classical noise present in the system. This opens up security issues that have no easy fix. Colbeck [59] was the first to suggest that untrusted devices can expand randomness. Since then, many protocols have been proposed, along with their security analysis. Self-testing randomness expansion protocols secure against classical adversaries were proposed by Fehr et al. [60], and Pironio et al. [61], based on the Clauser–Horne– Shimony–Holt (CHSH) inequality [188] which are based on exploiting the Q4 axiom. They used a setup with two devices. Each device had two possible settings, where choosing each setting yields one of the two outcomes. Based on the probability of these outcomes, one can form a correlation function. It admits a classical value that can be violated if one uses non-local (quantum) resources.

$$I = \sum_{x,y}(-1)^{xy}[P(a = b \mid xy) - P(a \neq b \mid xy)].$$

20

This correlation function can be estimated by repeating the measurement a large number of times. It can then be used to estimate the min-entropy of the measurement output. Recently, Miller and Shi [189] demonstrated that as soon as the device violated CHSH inequality, genuine randomness could be obtained. These protocols rely on the faithful realization of the Bell test. This is easier said than done, as the Bell tests are subject to locality and detection loopholes. Pironio et al. demonstrated a proof-of-concept experiment of such randomness expansion protocol against classical adversaries [190] in an ion-trap system, which closes the detection loophole. However, they were only able to generate 42 random bits over a period of one month, consuming more randomness than what was generated. Bit generation rates are typically low for these devices due to the increased complexity of the setup. Later proposals relaxed some conditions in order to have higher bit generation rates using optical components [62]. Recently, the generation speeds have reached around the order of 10 kbps, proven to be secure against quantum [191,192] and classical [193] adversaries.

In place of Bell inequality testing for non-locality, one can also consider other properties of quantum mechanics for verification. Generators reported in [53,194] used contextuality present in quantum mechanics [195] for generating random numbers. It is related to the existence of non-commuting observables where the order of measurement is important, and there is no predefined model that can give the outcomes of two successive incompatible measurements. So, instead of exploiting the Q4 axiom which is at a higher level, the working of contextuality based devices can be explained by incorporation of Q2 axiom alone. These QRNGs work on untrusted devices but not on adversarial ones. Since contextuality tests do not require entanglement or space-like separation, their implementation is relatively easier than those based on Bell inequality.

A fully device-independent protocol requires randomized settings as its input. A local-realist theory could explain the violation of Bell inequality if the measurement settings are correlated with the hidden variables. This is known as the Super-determinism loophole [196]. The protocols mentioned so far require a perfect input random number to conduct loophole-free Bell inequality violations. In the following subsection, we will discuss how imperfect random numbers could generate perfect random numbers. In a sense, they 'amplify' the randomness present in the input and are hence called randomness amplification protocol.

5.2. *Self testing Randomness amplification*

A device-independent randomness expansion protocol requires an initial seed of randomness. Without it, the protocol would become deterministic, and it will be possible for an adversary to predict the outcome and change their strategy accordingly [197]. Randomness amplification protocol bypasses the need for a uniform seed. A model for weak randomness was described in ref. [198], known as a Santha-Vazirani source. A sequence of random numbers $x_1 x_2 \cdots x_n$ of a Santha-Vazirani source is called ϵ free if

$$\epsilon \leq p\left(x_j \mid x_1, x_2, \ldots, x_{j-1}, e\right) \leq 1 - \epsilon,$$

where $p\left(x \mid y\right)$ is the conditional probability and e denotes all the classical variables that could possibly influence x_j. Given a weak source of random numbers, it is impossible to produce certifiable randomness classically [198]. Colbeck and Renner proposed the first randomness amplification protocol using quantum systems in [197]. They proved that any weak source of randomness with a critical threshold value of randomness could be amplified into arbitrarily free random bits. Weak randomness sources are used to choose

the measurement settings of quantum systems. Measurement outputs are then used to produce uniform random bits using chained Bell inequalities [199]. Later, Gallego et al. [200] improved upon the result by showing that perfectly random bits could be generated from arbitrary weak randomness. Practical ways to use these protocols were developed in [63], where only a limited number of independent devices were used. This is desirable since making sure that quantum devices are independent is difficult in practice. There have also been results on randomness amplification for more general sources taking any weak input with a bounded nonzero min-entropy[201–203]. Randomness amplification, apart from providing the initial seed in expansion protocols, also influence fundamental tests in science where initial randomness is required. The 'free will' loophole in Bell tests is an example of how imperfect randomness decreases the validity of such results [204].

6. Semi-self testing QRNGs

Realistically, parts of the random number generation device may be well characterized than others. In practice, one can choose to trust parts of the device and ignore details about other parts. This is especially relevant if we are only concerned about device imperfections, noisy channels, and not an adversarial situation. The security of such a device is intermediate to the trusted device and fully self-testing devices. It is a trade-off between practical trusted devices that provide high performance with low cost and low credibility and self-testing QRNGs with high credibility but low performance. One can consider a variety of these devices based on which part of the system is characterized. We will now go over different models, namely source device-independent, measurement device-independent, and bounded dimension QRNGs.

6.1. Source device independent QRNGs

As the name implies, in these devices, uncharacterized randomness sources are used. A trusted measurement device is used to monitor the source. Typically, measurement bases are chosen randomly from a complementing pair so that the presence of noise can be detected. This essentially means that uncertainty relations are exploited by such devices for which Q1 alone is sufficient. An initial random seed is required to choose the different measurement settings [179]. The generator could be modeled on a fixed set of assumptions or be made flexible, trading security for data rates [205]. The source-independent QRNG of [64] makes no assumptions about the dimension of the source (multiphoton emissions) and has demonstrated experimental bit rates up to 5×10^3bits/sec. Their generator takes into account the finite-key effect with the composable security definition. Composable security for a protocol is the most rigorous and functional security model since it can be used in conjunction with other protocols while remaining secure. Random number generators following a composable security definition can be used in arbitrary applications in cryptography, with no loss in security. Recently, Drahi *et. al.* have implemented a source-independent model generating composably secure quantum random numbers at a rate of 8.05 Gbps. Certification measurements were performed on an untrusted light source mixed with a trusted vacuum. In the composable security definition they considered, protocols with certification failure ϵ_1 and ϵ_2 can be composed into a joint protocol with a total security parameter $\epsilon \le \epsilon_1 + \epsilon_2$. They were able to provide a composable security parameter of 10^{-10} for their generator. The generator of [65] generates random numbers from the quadratures of an electromagnetic field without any
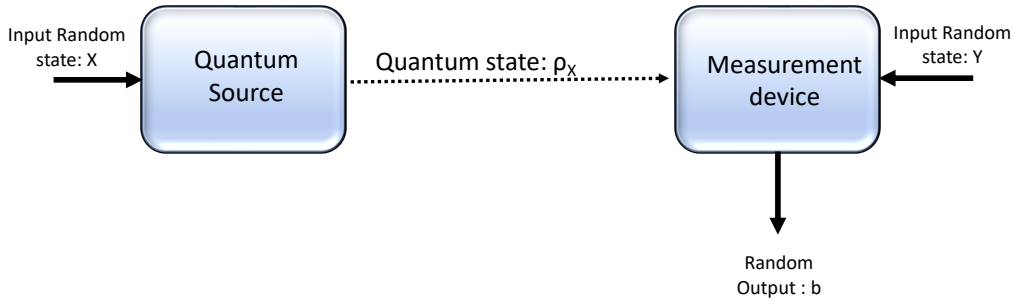
Figure 8. (Color online) Depending upon the input state X emits a quantum state ρ_x. The measurement device measures the state ρ_x based on the random input state Y and gets an output b [8]

assumption on the input state. They estimated a bound on the conditional min-entropy based on the entropic uncertainty principle for position and momentum observables of infinite-dimensional quantum systems. The randomness generation rates reach up to 1.7 Gbit/sec. [66] uses the phase randomized homodyne detection of gain-switched lasers [206] to generate random bits at the rate of 270 Mbits/sec. Higher rates were achieved in [67] with generation rates around 15 Gbit/sec using quadrature fluctuations of a quantum optical field. They have quantitatively analyzed the effects of excess noise, finite sampling range, finite resolution, and asymmetric conjugate quadratures while developing the security analysis of the QRNG. Avesani et al. [68] experimentally demonstrated a source independent QRNG based on heterodyne detection with randomness generation rates over 17 Gbps. Recently, a source-independent QRNG was also implemented using cloud quantum computers [207].

6.2. Measurement-device-independent QRNGs

If the input source is well characterized, whereas the measurement device is untrusted, we can still generate randomness using measurement device-independent QRNGs. In such devices, randomly chosen states are used to check the measurement device. Thus, in a sense, it is complementary to the source-independent QRNG. Again, here Q1 can explain the working of such devices. Cao et al. [69] proposed a protocol that is implementable using standard optical components. Nie et al. [70] used an all-fiber setup to realize an MDI-QRNG based on time-bin encoding. Randomness certification in a network independent of the measurement devices used was considered in [208]. [71] recently introduced a prepare-measure framework based on bounded fidelity on the prepared states and subsequent certification of random numbers. The advantage of such QRNGs is that since the measurement devices are not required to be characterized, they remove possible attacks involving detector inefficiencies. The obvious downside is that any imperfection in the source will adversely affect the protocol since there is no way to account for that. As usual, high bit rates could be achieved using continuous-variable systems, but faces the challenges of continuous-variable entanglement witness and measurement tomography.

6.3. Self-testing QRNGs with bounded dimensions

Rather than trusting the source or the measurement device, one can assume some bound on the dimension of the system used and a witness to certify the randomness generation process. For example, the preparation and measurement devices could be thought of as operating in a two-dimensional quantum subspace [72]; the randomness of the protocol can be certified by adopting a particular dimension witness. Any value of dimension witness greater than 0 certifies the randomness in the given example. Generation rates are typically low, reaching about 23 bps. Generator of [72] assumes that the preparation and measurement device shares no classical randomness. They used a function presented in [209], which acts as a 'dimension witness'.

$$\mathbf{W} = \left(\begin{array}{cc} p(0,0) - p(1,0) & p(2,0) - p(3,0) \\ p(0,1) - p(1,1) & p(2,1) - p(3,1) \end{array} \right)$$

where $p(x,y) = p(b = 0 \mid x,y)$. Whenever $\mathbf{W} > 0$ randomness certification is proved to be possible. Li. et al. [73] proposed a protocol based on quantum random access codes (QRAC)[210,211] which does not make any assumption regarding classical correlations between the preparation and measurement devices. They are based on the class of dimension witnesses introduced in [212]. The protocol in [213] improves the randomness generation rates to its optimal value [214] using a $3 \rightarrow 1$ QRAC. In a dimensionally bounded prepare-measure scenario, the randomness of the output can also be verified using non-inequality paradoxes such as Hardy's paradox [215] or Cabello's paradox [216], as demonstrated in [217]. A contextuality-based protocol was given in [218] using Mermin's magic-square proof of Kochen–Specker contextuality [219].

Apart from the aforementioned protocols, there are various other semi-device independent random number expansion protocols based on different assumptions. A fair assumption to make in a practical prepare-measure setup would be a bound on the overlap between the prepared states [220]; say a light pulse. A bound on the energy implies a lower bound on the overlap between the prepared states [221]. If the states are not orthogonal, randomness can be extracted from the measurement outcomes of an unambiguous state discrimination protocol. Protocols based on this assumption include [222–225]. Randomness certification from state discrimination was recently explored using non-contextuality as the notion of classicality [226]. They have shown that quantum theory could certify more randomness than non-contextual ones. The notion of *randomness amplification* explored in subsection 5.2 also have a semi-device independent analogue. Using just an additional assumption of either the dimension [227] or energy bound [228] randomness amplification of weak sources have shown to be possible using quantum systems.

A brief history and comparison of several self-testing QRNGs implemented over the years are presented in Table 2. They are compared based on the type of assumptions, usage of the detectors, and their bit generation speeds.

7. Origin of randomness in nonclassical theories

We have already discussed the limitations of PRNGs and CTRNGs in the previous sections. Further, we have delved upon the advantages offered by QRNGs and elaborated on the various class of QRNGs currently being available or in the development phase. This

Year	Type	Detection	Speed	Adversary Model
2010	Device Independent [190]	Ion-trap	Very Low	Quantum Adversary
2013	Device Independent [62]	SPD	0.4 bps	Quantum Adversary
2015	Source Independent [229]	SPD	5 Kbps	Classical Adversary
2015	Dimension Bound[72]	SPD	23 bps	Classical Adversary
2016	Measurement Independent [70]	SPD	5.7 Kbps	Classical Adversary
2017	Measurement Independent [230]	SPD	16.5 Mbps	Classical Adversary
2017	Source Independent [231]	Heterodyne	1.7 Gbps	Classical Adversary
2018	Device Independent[252]	SPD	Very Low	Quantum Adversary
2018	Source Independent [68]	Homodyne	17 Gbps	Classical Adversary
2018	Device Independent[232]	SPD	181 bps	Quantum Adversary
2019	Source Independent [66]	Homodyne	270 Mbps	Classical Adversary
2019	Source Independent [233]	SPD	1 Mbps	Classical Adversary
2019	Source Independent [234]	Homodyne	8.2 Kbps	Classical Adversary
2020	Source Independent[235]	Homodyne	8.05 Gbps	Classical Adversary
2020	Energy Bound[224]	Homodyne	145 Mbps	Classical Adversary
2020	Device Independent[251]	SPD	1.7 bps	Quantum Adversary
2021	Device Independent[191]	SPD	13.5 Kbps	Quantum Adversary
2021	Device Independent[193]	SPD	3.6 Kbps	Quantum Adversary
2021	Energy Bound[236]	Heterodyne	113 Mbps	Classical Adversary

Table 2. A comparison of various self-testing QRNGs; SPD-single photon detector

section will further explore the origin of randomness in the studied QRNGs. Precisely, we would aim to identify the nonclassical features of quantum mechanics responsible for the origin of randomness in a particular realization of QRNG and to investigate whether the kind of randomness obtained in that specific realization can also be obtained in a nonclassical toy theory which is not exactly quantum mechanics. A nonclassical toy theory $\mathcal{T}$ may be viewed as a theory having some features (axioms) which are not present in the classical world. For example, we may think of a nonclassical toy theory $\mathcal{T}_1$ that has all the features of the classical world, including "superposition," which is a manifestation of linearity of the theory and "collapse on measurement" postulate of quantum mechanics. As no other features (postulates) of quantum mechanics (e.g., entanglement, nonlocality) are included, $\mathcal{T}_1$ is a nonclassical theory (as a nonclassical feature, collapse on measurement is included) local (as nonlocality is not included) theory which is not equivalent to quantum mechanics (as all features of quantum mechanics is not present in $\mathcal{T}_1$. Now it's easy to visualize that even in such a toy theory, the commercially available QRNG device called QUANTIS [74] will work as its function involves only the collapse of a superposition state (qubit) on measurement using a reasonable basis. All the realizations of QRNGs are illustrated in Fig. 4(a)). $\mathcal{T}_1$ is just an example of nonclassical toy theory that can help us to lucidly describe the nonclassical origin of the unique features of QRNGs (more appropriately, TRNGs that are not CTRNGs or nonclassical RNGs) noted in this work. In what follows, we will follow this line of argument to profoundly investigate the origin of the so-called unique features of the QRNGs.

To begin with the analysis, we may note that quantum mechanics is intrinsically random and has various features such as entanglement, nonlocality, non-vanishing discord, etc., which are absent in the classical systems. Further, quantum mechanics has various interpretations, but the most accepted version is *Copenhagen interpretation* [237]. In the Copenhagen interpretation, the physical states correspond to vectors in the Hilbert space, which evolve under unitary evolution. Even though Copenhagen interpretation

has stood the test of time, many issues are still yet to be resolved, such as measurement problems. In contrast to other theories in physical sciences, quantum mechanics, as described by Copenhagen interpretation, is built upon the axioms that are more mathematical rather than having a physical motivation with terminology such as Hilbert space which cannot be directly observed. Various researchers are working on to derive (obtain) quantum mechanics from physically motivated axioms. Theories such as generalized probability theory (GPT) [79,80], generalized no-signalling theory (GNST) [81] and generalized nonlocal theory (GNLT) [82] have been developed in which classical mechanics and quantum mechanics come up as just one the cases.

Generalized no-signaling theory (GNST) [81] is based on two axioms, namely (i) no signal can propagate faster than the speed of light, and (ii) existence of non-local correlations, which can violate Bell inequality. Quantum mechanics is a particular case of GNST, but there are other theories (other special cases of GNST) too, such as PR box [238]. Further, the PR box is known to be more non-local than quantum mechanics as the maximum value of Clauser-Horne-Shimony-Holt (CHSH) sum of correlations for QM is $2\sqrt{2}$ (Tsirelson bound) [239] while for that for PR box is 4. A natural question to consider is what bounds the non-local correlations of QM to $2\sqrt{2}$. Generalized non-local theory (GNLT) [82] tries to answer that by considering a set of theories that are only bound by no-signaling conditions and found that Tsirelson's bound restricts the use of quantum mechanics as a resource in distributed tasks. In another work, the principle of information causality is considered as the reason for separating quantum mechanics from the set of other non-signaling theories [240]. The principle of information causality states that using only local operations and classical communication (LOCC), the information accessible to one party is bounded by the information volume of communication from the other party. This principle separates the class of physical theories from non-physical theories.

Generalized probability theory (GPT) [79,80] is based on the framework in which the set of equivalent classes of preparation states and measurement outcomes form the basis. If ω represents an element of operationally equivalent class of preparation states and effect e denotes an operationally equivalent class of one bit measurement outcome ('yes-no' type of answers), then $e(\omega) = p(e|\omega)$ denotes the probability that en experiment chosen from equivalence classes e and ω produces a '1' (yes). Several authors have tried to describe quantum mechanics through a set of physically inspired axioms [80,241], but these axioms have no hierarchy. In a unique effort in this line of studies, some of the present authors explored the origin of quantum mechanics from the viewpoint of associating the axioms with different nonclassical features that have been experimentally observed [78]. Further, they identified a hierarchy of five axioms where each succeeding axiom can be regarded as a superstructure built on top of the structure provided by the preceding axioms. These axioms have been named in as per the nonclassical features they are associated with: (Q1) incompatibility and uncertainty; (Q2) contextuality; (Q3) entanglement; (Q4) nonlocality and (Q5) indistinguishability of identical particles with each axiom associated with a relevant toy GPT model. It may be further noted that it's intrinsically assumed that any nonclassical theory $\mathcal{T}$ having one or more of the above axioms also contains classical features: (C1) Linearity, which leads to superposition in any linear theory (equivalently in any theory positing wave nature, e.g., classical optics); (C2) Tensor product space which in association with C1 gives classical entanglement (as pointed out by Simon et al. [242]); (C3) Norm preserving evolution leading to unitarity which is satisfied by any theory with rotational invariance and satisfying C1 and C2; and (C4) No-signaling. In what follows, we would like to investigate which of these hierarchical axioms (or equivalently what kind of

nonclassicality) are essential for realizing a specific type of QRNG and thus identifying the nonclassical toy theories that would allow the existence of such nonclassical RNGs.

For the convenience of the discussion, we may describe five toy theories: $\mathcal{T}_i' : i \in \{1, \cdots, 5\}$, where a toy nonclassical theory $\mathcal{T}_i'$ would contain C1 to C4 and the hierarchical axioms up to Qi. For example, $\mathcal{T}_1'$ would be a nonclassical theory that will have features of classical world and Q1. A careful analysis of the various experimental methods that can be used to construct QRNGs would easily reveal that most of the QRNGs belonging to the class of trusted QRNG, $\mathcal{T}_1'$ (i.e., the inclusion of Q1) is sufficient. However, to obtain features like self-testing and semi-self-testing QRNGs, one would require theories placed hierarchically above as those would require the inclusion of a set of other axioms. Before we elaborate on that, we may note that the early QRNGs were mainly based on radioactive sources, and the random numbers generated from radioactive sources essentially follow the uncertainty principle. We all know that explanation of the radioactivity process requires the uncertainty principle. Thus, for a radioactivity-based nonclassical random number generator, $\mathcal{T}_1'$ would be sufficient. It may be noted that toy theory $\mathcal{T}_1'$ is nonclassical, but it is a local theory, and such a theory would not only support radioactivity based RNGs it will also allow the construction of most of the trusted TRNGs that requires nonclassical features. As incompatibility implies collapse on measurement toy theory $\mathcal{T}_1$ described as an example above will be a particular case of $\mathcal{T}_1'$ and QUANTIS and other nonclassical RNGs allowed in $\mathcal{T}_1$ will also be allowed in $\mathcal{T}_1'$. Similar is the case for QRNGs based on the presence of shot noise in the electronic circuits, as it can be explained by quantum uncertainty relations alone. If one looks at QRNGs based on spin noise in atomic systems, one would also see that such systems would require Q1 only as spins noise arises due to inherent uncertainty relations. The QRNGs based on macroscopic photo-detection via vacuum noise exploit the uncertainty in the field quadratures. Similarly, only uncertainty relations are sufficient for randomness sources in QRNGs based on Raman scattering. In all the above scenarios, one can see that trusted QRNGs can be built in a nonclassical local theory $\mathcal{T}_1'$. Another class of nonclassical local toy theory is $\mathcal{T}_2'$, which has all features of $\mathcal{T}_1'$ along with the contextuality Q2. Such a local nonclassical theory will be sufficient to support the self-testing devices which are based on contextuality [53,194] by observing the violation of contextuality expressions [195] for certification of the devices against the presence of any adversary. It is important to note that such certification is only local in nature. Now, let us look at the self-testing QRNGs. They exploit the features of entanglement and non-locality. We all know that any local realistic hidden variable theory cannot explain the quantum correlations. Self-testing devices work by focusing only on input-output statistics. So, the self-testing devices can be certified by the violation of Bell-type inequalities [188]. Consequently, a nonlocal toy theory $\mathcal{T}_4'$ which includes Q1, Q2, Q3, and Q4 will be required for such devices. Note that even $\mathcal{T}_1'$ is not equivalent to quantum mechanics as it does not require Q5. We conclude this section by noting that keys generated in quantum key distribution protocols are essentially random, and naturally, different protocols can be supported by different toy theories and analysis in the line of the present section in relation to the schemes of QKD can be found in our earlier work [78,243].

8. Conclusions

A comprehensive overview of the existing random number generation methods using quantum systems has been done in this article. We have described QRNGs of various

Company	QRNG	Speed	Interface	Certifications
IDQ[74]	Quantis-IDQ250C2	250 Kbps	Chip	NIST SP800-22/90B, DieHarder
	Quantis-USB-4M	4 Mbps	USB	NIST SP800-22, CTL, METAS, AIS31
	Quantis-IDQ6MC1	6 Mbps	Chip	NIST SP800-22/90A/B/C, DieHarder, AEC-Q100
	Quantis-IDQ20MC1	20 Mbps	Chip	NIST SP800-22/90A/B/C, DieHarder
	Quantis-PCIe-16M	16 Mbps	PCLe	NIST SP800-22, CTL, METAS, BSI AIS 31
	Quantis-PCIe-40M	40 Mbps	PCLe	NIST SP800-22/90A/B/C, DieHarder
	Quantis-PCIe-240M	240 Mbps	PCLe	NIST SP800-22/90A/B/C, DieHarder
	Quantis-Appliance 2.0	232 Mbps	Ethernet	NIST SP800-22/90B, DieHarder
PicoQuant [76]	PQRNG150	150 Mbps	USB	TESTU01
QuatumCTek [77]	QRNG100E	200 Mbps	USB	NIST SP800-22, GM/T 0005-2012
	QRNG100E	600 Mbps	Ethernet	NIST SP800-22, GM/T 0005-2012
ComScire [125]	PQ4000KS	4 Mbps	USB	ComScire QNGmeter
	PQ128MS	128 Mbps	USB	ComScire QNGmeter
	CS128M	128 Mbps	USB	ComScire QNGmeter
Quitessence Labs [244]	qStream 100	1 Gbps	Ethernet	NIST SP800-22/90A/B/C, DieHarder
	qStream 200	1 Gbps	Ethernet	NIST SP800-22/90A/B/C, DieHarder, OASIS KMIP 1.0/1.1/1.2/1.3/1.4
Quantum eMotion [245]	QNG2	1 Gbps	Chip	NIST SP800-22, Diehard
EYL [246]	QRNG-H	1 Gbps	USB	NIST SP800-22/90B, BSI AIS 31
	QRNG-L	1 Mbps	USB	NIST SP800-22/90B, BSI AIS 31
	MQRNG	1 Gbps	PCLe	NIST SP800-22/90B, BSI AIS 31
qutools [247]	quRNG	50 Mbps	USB	NIST SP800-22, DieHarder
MPD [248]	QRN-16	16 Mbps	USB	NIST SP800-22, DieHarder, TESTU01
	QRN-32	32 Mbps	USB	NIST SP800-22, DieHarder, TESTU01
	QRN-64	64 Mbps	USB	NIST SP800-22, DieHarder, TESTU01
	QRN-128	128 Mbps	USB	NIST SP800-22, DieHarder, TESTU01
Quside [249]	Quside FMC 400	400 Mbps	Ethernet	Quside randomness metrology toolkit
	Quside PCLe 400	400 Mbps	PCLe	Quside randomness metrology toolkit
	Quside PCLe One	2 Gbps	PCLe	Quside randomness metrology toolkit
QNU [250]	TROPOS QNL-QRNG-X100	100 Mbps	Ethernet	NIST SP800-22, DieHard

Table 3. Commercially available Quantum Random Number Generators.

kinds in the previous sections. The discussion above clearly establishes the advantages of QRNGs and the technological challenges associated with implementing different classes of QRNGs. It also establishes that despite some existing technological challenges, there are many alternatives to produce QRNGs. The associated technology is much more mature than the majority of other aspects of quantum technologies that are expected to have a substantial impact (say, a scalable quantum computer). Naturally, a large number of commercial products (QRNGs) have been launched. Specifically, the development of QRNGs has advanced to a point where off-the-shelf QRNGs are now commercially available and not costly. A brief overview of the available products is provided in Table 3. The table lists commercially available QRNGs along with their bit generation speed, types of connectivity available, and the different tests passed by the corresponding QRNGs [9]. It is to be mentioned that the commercial QRNGs available now belong to the class of trusted devices. The next-generation devices belonging to the self-testing and semi-self-testing classes are still in the developmental stage, and their commercial utilization is expected sooner than later.

This review has briefly compared the various methods for random number generation so that a user who wishes to employ random numbers in their schemes can make an informed decision. Further, it is difficult, if not impossible, to declare that a particular method is the best without knowing the necessities of the end-user. A large number of variables (e.g., bit generation rate, cost, ease of usage, availability, form factor, certifiability) need to be considered simultaneously for comparing any two or more schemes for QRNGs. In general, generators based on homodyne or heterodyne detection like the vacuum noise-based or ASE-based ones have significantly higher bit rates. Commercial products would be a better choice in terms of the form factor and ease of availability. Microchip or USB-based RNGs provide the ultimate portability, and most of such products come with accompanying software which makes it very easy to use for an end-user who may be a non-technical person. Device-independent methods have the highest

certifiably albeit with lower generation rates. Along with the review of the generation methods for different classes of QRNGs, we have also tried to trace the origin of the randomness in the nonclassical sources of entropy, and that effort has provided a deeper insight into the world of randomness. This has provided completeness to this review, and it may provide some new insights to the researchers towards the ultimate goal of having a near-perfect random number generator.

Data availability

No additional data is needed for this work.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

All the authors have contributed equally. AP conceptualized the article and the foundational aspects of the problem. VM and SM performed a critical and rigorous analysis of the existing quantum random number generation schemes. All the authors contributed equally in the writing part to reveal the inherent symmetry leading to classification.

References

[1] Metropolis N, Ulam S. The Monte Carlo Method. Journal of the American Statistical Association. 1949 Sep;44(247):335-41. Available from: `https://www.tandfonline.com/doi/abs/10.1080/01621459.1949.10483310`.

[2] Karp RM. An introduction to randomized algorithms. Discrete Applied Mathematics. 1991 Nov;34(1):165-201. Available from: `https://www.sciencedirect.com/science/article/pii/0166218X9190086C`.

[3] Motwani R, Raghavan P. Randomized Algorithms. ACM Computing Surveys. 1996 mar;28(1):33–37. Available from: `https://doi.org/10.1145/234313.234327`.

[4] Shannon CE. Communication theory of secrecy systems. Bell System Technical Journal. 1949 Oct;28(4):656-715. Available from: `https://ieeexplore.ieee.org/document/6769090`.

[5] Gennaro R. Randomness in cryptography. IEEE Secur Priv. 2006 Apr;4(2):64-7. Available from: `https://ieeexplore.ieee.org/abstract/document/1621063`.

[6] James F. A review of pseudorandom number generators. Comput Phys Commun. 1990 Oct;60(3):329-44. Available from: `https://www.sciencedirect.com/science/article/pii/001046559090032V`.

[7] Herrero-Collantes M, Garcia-Escartin JC. Quantum random number generators. Rev Mod Phys. 2017 Feb;89(1):015004. Available from: `https://link.aps.org/doi/10.1103/RevModPhys.89.015004`.

[8] Ma X, Yuan X, Cao Z, et al. Quantum random number generation - npj Quantum Information. npj Quantum Inf. 2016 Jun;2(16021):1-9. Available from: `https://doi.org/10.1038/npjqi.2016.21`.

[9] Jacak MM, Jóźwiak P, Niemczuk J, Jacak JE. Quantum generators of random numbers. Scientific Reports. 2021 Aug;11(1):16108. Available from: `https://doi.org/10.1038/s41598-021-95388-7`.

[10] Hörmann W, Leydold J, Derflinger G. Automatic Nonuniform Random Variate Generation. Berlin, Germany: Springer; 2004. Available from: `https://link.springer.com/book/10.1007/978-3-662-05946-3`.

[11] Hull TE, Dobell AR. Random Number Generators. SIAM Rev. 1962 Aug. Available from: `https://epubs.siam.org/doi/abs/10.1137/1004061?mobileUi=0`.

[12] Bassham LE, Rukhin AL, Soto J, et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST. 2017 Feb. Available from: `https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic`.

[13] DIEHARD; 2001. [Online; accessed 22. Feb. 2022]. Available from: `https://tams.informatik.uni-hamburg.de/paper/2001/SA_Witt_Hartmann/cdrom/Internetseiten/stat.fsu.edu/diehard.html`.

[14] Haahr M. RANDOM.ORG - Introduction to Randomness and Random Numbers; 1999. [Online; accessed 28. Feb. 2022]. Available from: `https://www.random.org/randomness`.

[15] Lee JS, Cleaver GB. The cosmic microwave background radiation power spectrum as a random bit generator for symmetric- and asymmetric-key cryptography. Heliyon. 2017 Oct;3(10):e00422. Available from: `https://www.sciencedirect.com/science/article/pii/S2405844017310897`.

[16] Zhun H, Hongyi C. A truly random number generator based on thermal noise. In: ASICON 2001. 2001 4th International Conference on ASIC Proceedings (Cat. No.01TH8549). IEEE; 2001. p. 862-4. Available from: `https://ieeexplore.ieee.org/abstract/document/982700`.

[17] Hamburg M, Kocher P, Marson ME. Analysis of Intel's Ivy Bridge digital random number generator (2012). Available from: `https://cdn.atraining.ru/docs/Intel_TRNG_Report_20120312.pdf`.

[18] Stojanovski T, Pihl J, Kocarev L. Chaos-based random number generators. Part II: practical realization. IEEE Trans Circuits Syst I. 2001 Mar;48(3):382-5. Available from: `https://ieeexplore.ieee.org/document/915396`.

[19] Killmann W, Schindler W. A proposal for: Functionality classes for random number generators. ser BDI, Bonn. 2011. Available from: `https://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/15ss/15ss-taoc/01_AIS31_Functionality_classes_for_random_number_generators.pdf`.

[20] Bera MN, Acín A, Kuś M, et al. Randomness in quantum mechanics: philosophy, physics and technology. Rep Prog Phys. 2017 Nov;80(12):124001. Available from: `http://dx.doi.org/10.1088/1361-6633/aa8731`.

[21] Yuan X, Zhou H, Cao Z, Ma X. Intrinsic randomness as a measure of quantum coherence.

Phys Rev A. 2015 Aug;92:022124. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.92.022124`.

[22] How to Turn a Quantum Computer Into the Ultimate Randomness Generator | Quanta Magazine; 2019. [Online; accessed 28. Feb. 2022]. Available from: `https://www.quantamagazine.org/how-to-turn-a-quantum-computer-into-the-ultimate-randomness-generator-20190619`.

[23] Nielsen MA, Chuang IL. Quantum Computation and Quantum Information: 10th Anniversary Edition. Cambridge, England, UK: Cambridge University Press; 2010. Available from: `https://www.cambridge.org/highereducation/books/quantum-computation-and-quantum-information/01E10196D0A682A6AEFFEA52D53BE9AE#overview`.

[24] Pathak A. Elements of Quantum Computation and Quantum Communication. Andover, England, UK: Taylor & Francis; 2013. Available from: `https://www.taylorfrancis.com/books/mono/10.1201/b15007/elements-quantum-computation-quantum-communication-anirban-pathak`.

[25] Schmidt H. Quantum-Mechanical Random-Number Generator. Journal of Applied Physics. 1970;41(2):462-8. Available from: `https://doi.org/10.1063/1.1658698`.

[26] Ishida M. Random number generator. Annals of Institute of Statistical Mathematics. 1956;8:119-26. Available from: `https://ci.nii.ac.jp/naid/30040870857/en/`.

[27] Alkassar A, Nicolay T, Rohe M. Obtaining True-Random Binary Numbers from a Weak Radioactive Source. In: Computational Science and Its Applications – ICCSA 2005. Berlin, Germany: Springer; 2005. p. 634-46. Available from: `https://link.springer.com/chapter/10.1007/11424826_67`.

[28] Vincent CH. The generation of truly random binary numbers. Journal of Physics E: Scientific Instruments. 1970 aug;3(8):594-8. Available from: `https://doi.org/10.1088/0022-3735/3/8/303`.

[29] Gude M. Concept for a High Performance Random Number Generator Based on Physical Random Phenomena. Frequenz. 1985;39(7-8):187-90. Available from: `https://doi.org/10.1515/FREQ.1985.39.7-8.187`.

[30] Holman WT, Connelly JA, Dowlatabadi AB. An integrated analog/digital random noise source. IEEE Trans Circuits Syst I. 1997 Jun;44(6):521-8. Available from: `https://ieeexplore.ieee.org/document/586025`.

[31] Petrie CS, Connelly JA. A noise-based IC random number generator for applications in cryptography. IEEE Trans Circuits Syst I. 2000 May;47(5):615-21. Available from: `https://ieeexplore.ieee.org/document/847868`.

[32] Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A. A fast and compact quantum random number generator. Review of Scientific Instruments. 2000;71(4):1675-80. Available from: `https://doi.org/10.1063/1.1150518`.

[33] Wang PX, Long GL, Li YS. Scheme for a quantum random number generator. Journal of Applied Physics. 2006;100(5):056107. Available from: `https://doi.org/10.1063/1.2338830`.

[34] Stefanov A, Gisin N, Guinnard O, Guinnard L, Zbinden H. Optical quantum random number generator. Journal of Modern Optics. 2000 Mar;47(4):595–598. Available from: `http://dx.doi.org/10.1080/09500340008233380`.

[35] Bronner P, Strunz A, Silberhorn C, et al. Demonstrating quantum random with single photons. Eur J Phys. 2009 Aug;30(5):1189-200. Available from: `http://dx.doi.org/10.1088/0143-0807/30/5/026`.

[36] Gräfe M, Heilmann R, Perez-Leija A, et al. On-chip generation of high-order single-photon W-states - Nature Photonics. Nat Photonics. 2014 Oct;8(10):791-5. Available from: `https://doi.org/10.1038/nphoton.2014.204`.

[37] Nie YQ, Zhang HF, Zhang Z, Wang J, Ma X, Zhang J, et al. Practical and fast quantum random number generation based on photon arrival time relative to external reference. Applied Physics Letters. 2014;104(5):051110. Available from: `https://doi.org/10.1063/1.4863224`.

[38] Khanmohammadi A, Enne R, Hofbauer M, et al. A Monolithic Silicon Quantum Random Number Generator Based on Measurement of Photon Detection Time. IEEE Photonics J. 2015 Sep;7(5):1-13. Available from: `https://ieeexplore.ieee.org/document/7270265`.

[39] Yan Q, Zhao B, Liao Q, Zhou N. Multi-bit quantum random number generation by measuring positions of arrival photons. Review of Scientific Instruments. 2014 Oct;85(10):103116. Available from: `https://doi.org/10.1063/1.4897485`.

[40] Burri S, Stucki D, Maruyama Y, et al. SPADs for quantum random number generators and beyond. In: 2014 19th Asia and South Pacific Design Automation Conference (ASP-DAC). IEEE; 2014. p. 788-94. Available from: `https://ieeexplore.ieee.org/document/6742986`.

[41] Yan Q, Zhao B, Liao Q, Zhou N. Multi-bit quantum random number generation by measuring positions of arrival photons. Review of Scientific Instruments. 2014;85(10):103116. Available from: `https://doi.org/10.1063/1.4897485`.

[42] Fürst H, Weier H, Nauerth S, Marangon DG, Kurtsiefer C, Weinfurter H. High speed optical quantum random number generation. Opt Express. 2010 Jun;18(12):13029-37. Available from: `http://opg.optica.org/oe/abstract.cfm?URI=oe-18-12-13029`.

[43] Jian Y, Ren M, Wu E, et al. Two-bit quantum random number generator based on photon-number-resolving detection. Rev Sci Instrum. 2011 Jul;82(7):073109. Available from: `https://doi.org/10.1063/1.3613952`.

[44] Shen Y, Tian L, Zou H. Practical quantum random number generator based on measuring the shot noise of vacuum states. Phys Rev A. 2010 Jun;81:063814. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.81.063814`.

[45] Gabriel C, Wittmann C, Sych D, Dong R, Mauerer W, Andersen UL, et al. A generator for unique quantum random numbers based on vacuum states. Nature Photonics. 2010 Oct;4(10):711-5. Available from: `https://doi.org/10.1038/nphoton.2010.197`.

[46] Xiao M, Wu LA, Kimble HJ. Precision measurement beyond the shot-noise limit. Phys Rev Lett. 1987 Jul;59:278-81. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.59.278`.

[47] Symul T, Assad SM, Lam PK. Real time demonstration of high bitrate quantum random number generation with coherent laser light. Applied Physics Letters. 2011;98(23):231103. Available from: `https://doi.org/10.1063/1.3597793`.

[48] Li X, Cohen AB, Murphy TE, Roy R. Scalable parallel physical random number generator based on a superluminescent LED. Optics Letters. 2011 Mar;36(6):1020. Available from: `http://dx.doi.org/10.1364/OL.36.001020`.

[49] Nie YQ, Huang L, Liu Y, Payne F, Zhang J, Pan JW. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. Review of Scientific Instruments. 2015 Jun;86(6):063105. Available from: `http://dx.doi.org/10.1063/1.4922417`.

[50] Bustard PJ, Moffatt D, Lausten R, Wu G, Walmsley IA, Sussman BJ. Quantum random bit generation using stimulated Raman scattering. Opt Express. 2011 Dec;19(25):25173-80. Available from: `http://opg.optica.org/oe/abstract.cfm?URI=oe-19-25-25173`.

[51] Bustard PJ, England DG, Nunn J, Moffatt D, Spanner M, Lausten R, et al. Quantum random bit generation using energy fluctuations in stimulated Raman scattering. Opt Express. 2013 Dec;21(24):29350-7. Available from: `http://opg.optica.org/oe/abstract.cfm?URI=oe-21-24-29350`.

[52] Pironio S, Acín A, Massar S, de la Giroday AB, Matsukevich DN, Maunz P, et al. Random numbers certified by Bell's theorem. Nature. 2010 Apr;464(7291):1021-4. Available from: `https://doi.org/10.1038/nature09008`.

[53] Um M, Zhang X, Zhang J, Wang Y, Yangchao S, Deng DL, et al. Experimental Certification of Random Numbers via Quantum Contextuality. Scientific Reports. 2013 Apr;3(1):1627. Available from: `https://doi.org/10.1038/srep01627`.

[54] Katsoprinakis GE, Polis M, Tavernarakis A, Dellis AT, Kominis IK. Quantum random number generator based on spin noise. Phys Rev A. 2008 May;77:054101. Available

from: `https://link.aps.org/doi/10.1103/PhysRevA.77.054101`.

[55] Oestreich M, Römer M, Haug RJ, Hägele D. Spin Noise Spectroscopy in GaAs. Phys Rev Lett. 2005 Nov;95:216603. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.95.216603`.

[56] Stich D, Zhou J, Korn T, Schulz R, Schuh D, Wegscheider W, et al. Effect of Initial Spin Polarization on Spin Dephasing and the Electron g Factor in a High-Mobility Two-Dimensional Electron System. Phys Rev Lett. 2007 Apr;98:176401. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.98.176401`.

[57] Jacak JE, Jacak WA, Donderowicz WA, Jacak L. Quantum random number generators with entanglement for public randomness testing. Scientific Reports. 2020;10(1):1-9. Available from: `https://www.nature.com/articles/s41598-019-56706-2`.

[58] Colbeck R. Quantum And Relativistic Protocols For Secure Multi-Party Computation. arXiv. 2009 Nov. Available from: `https://arxiv.org/abs/0911.3814v2`.

[59] Colbeck R, Kent A. Private randomness expansion with untrusted devices. Journal of Physics A: Mathematical and Theoretical. 2011 Feb;44(9):095305. Available from: `http://dx.doi.org/10.1088/1751-8113/44/9/095305`.

[60] Fehr S, Gelles R, Schaffner C. Security and composability of randomness expansion from Bell inequalities. Phys Rev A. 2013 Jan;87:012335. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.87.012335`.

[61] Pironio S, Massar S. Security of practical private randomness generation. Physical Review A. 2013 Jan;87(1). Available from: `http://dx.doi.org/10.1103/PhysRevA.87.012336`.

[62] Giustina M, Mech A, Ramelow S, Wittmann B, Kofler J, Beyer J, et al. Bell violation using entangled photons without the fair-sampling assumption. Nature. 2013 May;497(7448):227-30. Available from: `https://doi.org/10.1038/nature12012`.

[63] Brandão FGSL, Ramanathan R, Grudka A, et al. Realistic noise-tolerant randomness amplification using finite number of devices - Nature Communications. Nat Commun. 2016 Apr;7(11345):1-6. Available from: `https://doi.org/10.1038/ncomms11345`.

[64] Cao Z, Zhou H, Yuan X, Ma X. Source-Independent Quantum Random Number Generation. Physical Review X. 2016 Feb;6(1). Available from: `http://dx.doi.org/10.1103/PhysRevX.6.011020`.

[65] Marangon DG, Vallone G, Villoresi P. Source-Device-Independent Ultrafast Quantum Random Number Generation. Physical Review Letters. 2017 Feb;118(6). Available from: `http://dx.doi.org/10.1103/PhysRevLett.118.060503`.

[66] Smith PR, Marangon DG, Lucamarini M, Yuan ZL, Shields AJ. Simple source device-independent continuous-variable quantum random number generator. Phys Rev A. 2019 Jun;99:062326. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.99.062326`.

[67] Xu B, Chen Z, Li Z, Yang J, Su Q, Huang W, et al. High speed continuous variable source-independent quantum random number generation. Quantum Science and Technology. 2019 apr;4(2):025013. Available from: `https://doi.org/10.1088/2058-9565/ab0fd9`.

[68] Avesani M, Marangon DG, Vallone G, Villoresi P. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. Nature Communications. 2018 Dec;9(1):5365. Available from: `https://doi.org/10.1038/s41467-018-07585-0`.

[69] Cao Z, Zhou H, Ma X. Loss-tolerant measurement-device-independent quantum random number generation. New Journal of Physics. 2015 Dec;17(12):125011. Available from: `http://dx.doi.org/10.1088/1367-2630/17/12/125011`.

[70] Nie YQ, Guan JY, Zhou H, Zhang Q, Ma X, Zhang J, et al. Experimental measurement-device-independent quantum random-number generation. Phys Rev A. 2016 Dec;94:060301. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.94.060301`.

[71] Tavakoli A. Semi-Device-Independent Framework Based on Restricted Distrust in Prepare-and-Measure Experiments. Phys Rev Lett. 2021 May;126(21):210503. Avail-

able from: `https://link.aps.org/doi/10.1103/PhysRevLett.126.210503`.

[72] Lunghi T, Brask JB, Lim CCW, Lavigne Q, Bowles J, Martin A, et al. Self-Testing Quantum Random Number Generator. Physical Review Letters. 2015 Apr;114(15). Available from: `http://dx.doi.org/10.1103/PhysRevLett.114.150501`.

[73] Li HW, Yin ZQ, Wu YC, Zou XB, Wang S, Chen W, et al. Semi-device-independent random-number expansion without entanglement. Phys Rev A. 2011 Sep;84:034301. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.84.034301`.

[74] Quantique I. Quantis QRNG (Quantum Random Number Generator) - ID Quantique;. (Accessed on 25/02/2022). `https://www.idquantique.com/random-number-generation/products`.

[75] Toshiba. https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/quantum-random-number-generators;. (Accessed on 25/02/2022). `https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/quantum-random-number-generators`.

[76] PicoQuant. Quantum Random Number Generator — PicoQuant;. (Accessed on 25/102/2022). `https://www.picoquant.com/scientific/product-studies/pqrng-150-product-study`.

[77] CTek. Quantum Random Number Source_QuantumCTek– Quantum Secures Every Bit;. (Accessed on 25/02/2022). `http://www.quantum-info.com/English/product/pfour/liangzisuijishuyuan/2019/0731/579.html`.

[78] Aravinda S, Pathak A, Srikanth R. Hierarchical axioms for quantum mechanics. Eur Phys J D. 2019 Sep;73(9):207-7. Available from: `https://doi.org/10.1140/epjd/e2019-90452-2`.

[79] Janotta P, Hinrichsen H. Generalized probability theories: what determines the structure of quantum theory? J Phys A: Math Theor. 2014 Jul;47(32):323001. Available from: `http://dx.doi.org/10.1088/1751-8113/47/32/323001`.

[80] Barrett J. Information processing in generalized probabilistic theories. Phys Rev A. 2007 Mar;75(3):032304. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.75.032304`.

[81] Masanes Ll, Acin A, Gisin N. General properties of nonsignaling theories. Phys Rev A. 2006 Jan;73(1):012112. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.73.012112`.

[82] Barrett J, Linden N, Massar S, et al. Nonlocal correlations as an information-theoretic resource. Phys Rev A. 2005 Feb;71(2):022101. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.71.022101`.

[83] Shannon CE. A mathematical theory of communication. Bell System Technical Journal. 1948 Jul;27(3):379-423. Available from: `https://ieeexplore.ieee.org/document/6773024`.

[84] Yuan X, Zhao Q, Girolami D, Ma X. Quantum coherence and intrinsic randomness. Advanced Quantum Technologies. 2019;2(11):1900053. Available from: `https://onlinelibrary.wiley.com/doi/10.1002/qute.201900053`.

[85] Amigó JM, Balogh SG, Hernández S. A Brief Review of Generalized Entropies. Entropy. 2018;20(11). Available from: `https://www.mdpi.com/1099-4300/20/11/813`.

[86] Rényi A. On Measures of Entropy and Information. In: Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics. vol. 4.1. Ewing, NJ, USA: University of California Press; 1961. p. 547-62. Available from: `https://projecteuclid.org/proceedings/berkeley-symposium-on-mathematical-statistics-and-probability/Proceedings-of-the-Fourth-Berkeley-Symposium-on-Mathematical-Statistics-and/Chapter/On-Measures-of-Entropy-and-Information/bsmsp/1200512181`.

[87] Chor B, Goldreich O. Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity. SIAM J Comput. 2006 Jul. Available from: `https://epubs.siam.org/doi/10.1137/0217015`.

[88] Zuckerman D. General weak random sources. In: Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science. IEEE; 1990. p. 534-543vol.2. Available

from: `https://ieeexplore.ieee.org/document/89574`.

[89] Renner R. Security of quantum key distribution. ETHZ; 2005. Available from: `http://hdl.handle.net/20.500.11850/72791`.

[90] König R, Renner R, Schaffner C. The Operational Meaning of Min- and Max-Entropy. IEEE Trans Inf Theor. 2009 sep;55(9):4337–4347. Available from: `https://doi.org/10.1109/TIT.2009.2025545`.

[91] Konig R, Renner R. Sampling of Min-Entropy Relative to Quantum Knowledge. IEEE Trans Inf Theory. 2011 Jun;57(7):4760-87. Available from: `https://ieeexplore.ieee.org/document/5895072`.

[92] The complexity of estimating min-entropy; 2022. [Online; accessed 22. Feb. 2022]. Available from: `https://www.springerprofessional.de/en/the-complexity-of-estimating-min-entropy/11640276`.

[93] Lyngsø RB, Pedersen CNS. The consensus string problem and the complexity of comparing hidden Markov models. Journal of Computer and System Sciences. 2002 Nov;65(3):545-69. Available from: `https://www.sciencedirect.com/science/article/pii/S0022000002000090`.

[94] L Ecuyer P. Random number generation. Springer; 2012. Available from: `https://link.springer.com/book/10.1007/978-3-642-21551-3`.

[95] National Institute Of Standards and Technology. Security Requirements for Cryptographic Modules. CSRC | NIST. 2002 Dec. Available from: `https://csrc.nist.gov/publications/detail/fips/140/2/final`.

[96] Barker E, Kelsey J, Secretary JB. NIST DRAFT Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation; 2012. Available from: `http://www.gocs.de/pages/kryptologie/archiv/SP800-90b.pdf`.

[97] Knuth DE. The art of computer programming, volume 3: (2nd ed.) sorting and searching. Addison Wesley Longman Publishing Co., Inc.; 1998. Available from: `https://dl.acm.org/doi/10.5555/280635`.

[98] LEHMER DH. Mathematical methods in large-scale computing units. Annu Comput Lab Harvard Univ. 1951;26:141-6. Available from: `https://ci.nii.ac.jp/naid/20000729744/en/`.

[99] Klein A. Linear Feedback Shift Registers. In: Stream Ciphers. London, England, UK: Springer; 2013. p. 17-58. Available from: `https://doi.org/10.1007/978-1-4471-5079-4_2`.

[100] Matsumoto M, Nishimura T. Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator. ACM Trans Model Comput Simul. 1998 Jan;8(1):3-30. Available from: `https://dl.acm.org/doi/10.1145/272991.272995`.

[101] Yao AC. Theory and application of trapdoor functions. In: 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982). IEEE; 1982. p. 80-91.

[102] Blum M, Micali S. In: How to Generate Cryptographically Strong Sequences of Pseudo Random Bits. New York, NY, USA: Association for Computing Machinery; 2019. p. 227–240. Available from: `https://doi.org/10.1145/3335741.3335751`.

[103] Blum L, Blum M, Shub M. A Simple Unpredictable Pseudo-Random Number Generator. SIAM Journal on Computing. 1986;15(2):364-83. Available from: `https://doi.org/10.1137/0215025`.

[104] Vazirani UV, Vazirani VV. Efficient And Secure Pseudo-Random Number Generation. In: 25th Annual Symposium onFoundations of Computer Science, 1984. IEEE; 1984. p. 458-63. Available from: `https://ieeexplore.ieee.org/document/715948`.

[105] Metropolis N, Ulam S. The Monte Carlo Method. Journal of the American Statistical Association. 1949;44(247):335-41. PMID: 18139350. Available from: `https://www.tandfonline.com/doi/abs/10.1080/01621459.1949.10483310`.

[106] Ferguson N, Schneier B, Kohno T. Cryptography Engineering: Design Principles and Practical Applications. Hoboken, NJ, USA: Wiley; 2010. Available from: `https://www.wiley.com/en-be/Cryptography+Engineering:+Design+Principles+and+Practical+Applications+-p-9780470474242`.

[107] Marsaglia G. RANDOM NUMBERS FALL MAINLY IN THE PLANES. Proc Natl Acad Sci USA. 1968 Sep;61(1):25-8. Available from: `http://www.pnas.org/content/61/1/25.abstract`.

[108] Matsumoto M, Wada I, Kuramoto A, Ashihara H. Common Defects in Initialization of Pseudorandom Number Generators. ACM Trans Model Comput Simul. 2007 sep;17(4):15–es. Available from: `https://doi.org/10.1145/1276927.1276928`.

[109] Bouda J, Pivoluska M, Plesch M, Wilmott C. Weak randomness seriously limits the security of quantum key distribution. Phys Rev A. 2012 Dec;86:062308. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.86.062308`.

[110] Gutterman Z, Pinkas B, Reinman T. Analysis of the Linux random number generator. In: 2006 IEEE Symposium on Security and Privacy (S&P'06). IEEE; 2006. p. 15pp.-385. Available from: `https://ieeexplore.ieee.org/document/1624027`.

[111] Becker GT, Regazzoni F, Paar C, et al. Stealthy Dopant-Level Hardware Trojans. In: Cryptographic Hardware and Embedded Systems - CHES 2013. Berlin, Germany: Springer; 2013. p. 197-214. Available from: `https://link.springer.com/chapter/10.1007/978-3-642-40349-1_12`.

[112] Landauer R. Solid-state shot noise. Phys Rev B. 1993 Jun;47:16427-32. Available from: `https://link.aps.org/doi/10.1103/PhysRevB.47.16427`.

[113] Friedman H. Geiger Counter Tubes. Proc IRE. 1949 Jul;37(7):791-808. Available from: `https://ieeexplore.ieee.org/document/1698087`.

[114] Silverman MP, Strange W, Silverman CR, Lipscombe TC. Tests of alpha-, beta-, and electron capture decays for randomness. Physics Letters A. 1999;262(4):265-73. Available from: `https://www.sciencedirect.com/science/article/pii/S0375960199006684`.

[115] Duggirala R, Lal A, Radhakrishnan S. Radioisotope Decay Rate Based Counting Clock. In: Radioisotope Thin-Film Powered Microsystems. New York, NY, USA: Springer, New York, NY; 2010. p. 127-70. Available from: `https://link.springer.com/book/10.1007/978-1-4419-6763-3`.

[116] Vincent CH. Precautions for accuracy in the generation of truly random binary numbers. Journal of Physics E: Scientific Instruments. 1971 nov;4(11):825-8. Available from: `https://doi.org/10.1088/0022-3735/4/11/007`.

[117] Schottky W. Über spontane Stromschwankungen in verschiedenen Elektrizitätsleitern. Annalen der Physik. 1918;362(23):541-67. Available from: `https://onlinelibrary.wiley.com/doi/abs/10.1002/andp.19183622304`.

[118] Nyquist H. Thermal Agitation of Electric Charge in Conductors. Phys Rev. 1928 Jul;32:110-3. Available from: `https://link.aps.org/doi/10.1103/PhysRev.32.110`.

[119] Johnson JB. Thermal Agitation of Electricity in Conductors. Phys Rev. 1928 Jul;32:97-109. Available from: `https://link.aps.org/doi/10.1103/PhysRev.32.97`.

[120] Reznikov M, de Picciotto R, Heiblum M, Glattli DC, Kumar A, Saminadayar L. Quantum shot noise. Superlattices and Microstructures. 1998;23(3):901-15. Available from: `https://www.sciencedirect.com/science/article/pii/S0749603697905590`.

[121] Stipčević M. Quantum random number generators and their use in cryptography. In: 2011 Proceedings of the 34th International Convention MIPRO. IEEE; 2011. p. 1474-9. Available from: `https://ieeexplore.ieee.org/document/5967293`.

[122] Stipčević M. Fast nondeterministic random bit generator based on weakly correlated physical events. Review of Scientific Instruments. 2004;75(11):4442-9. Available from: `https://doi.org/10.1063/1.1809295`.

[123] Platt C, Logue A. Really, Really Random Number Generator - Make:;. (Accessed on 12/07/2021). `https://makezine.com/projects/really-really-random-number-generator/`.

[124] Wilber SA. Device and Method for Quantum Random Number Generation;. (Accessed on 12/07/2021). `https://comscire.com/files/whitepaper/Pure_Quantum_White_Paper.pdf`.

[125] ComScire. Generator Selection Guide Page — ComScire;. (Accessed on 25/02/2022). `https://comscire.com/random-number-generator-selection-guide/`.

[126] Katsoprinakis GE, Dellis AT, Kominis IK. Measurement of transverse spin-relaxation rates in a rubidium vapor by use of spin-noise spectroscopy. Phys Rev A. 2007 Apr;75:042502. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.75.042502`.

[127] Eisaman MD, Fan J, Migdall A, Polyakov SV. Invited Review Article: Single-photon sources and detectors. Review of Scientific Instruments. 2011;82(7):071101. Available from: `https://doi.org/10.1063/1.3610677`.

[128] Buller GS, Collins RJ. Single-photon generation and detection. Measurement Science and Technology. 2009 nov;21(1):012002. Available from: `https://doi.org/10.1088/0957-0233/21/1/012002`.

[129] Weihs G, Jennewein T, Simon C, Weinfurter H, Zeilinger A. Violation of Bell's Inequality under Strict Einstein Locality Conditions. Phys Rev Lett. 1998 Dec;81:5039-43. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.81.5039`.

[130] Xu MXM, Huang JHJ, Liang WLW, Zhang CZC, Wang SWS, Yin ZYZ, et al. Adjustable unbalanced quantum random-number generator. Chinese Optics Letters. 2015;13(2):021405-9. Available from: `https://doi.org/10.3788/col201513.021405`.

[131] IBM Quantum; 2022. [Online; accessed 28. Feb. 2022]. Available from: `https://quantum-computing.ibm.com`.

[132] Result.get_memory — Qiskit 0.19.6 documentation; 2021. [Online; accessed 27. Feb. 2022]. Available from: `https://qiskit.org/documentation/stable/0.19/stubs/qiskit.result.Result.get_memory.html#qiskit.result.Result.get_memory`.

[133] Rarity JG, Owens PCM, Tapster PR. Quantum Random-number Generation and Key Sharing. J Mod Opt. 1994 Dec;41(12):2435-44. Available from: `https://www.tandfonline.com/doi/abs/10.1080/09500349414552281`.

[134] Experimental realization of quantum random number generator; 2003. [Online; accessed 28. Feb. 2022]. Available from: `https://www.spiedigitallibrary.org/conference-proceedings-of-spie/5259/0000/Experimental-realization-of-quantum-random-number-generator/10.1117/12.545053.short?SSO=1`.

[135] Stipčević M, Rogina BM. Quantum random number generator based on photonic emission in semiconductors. Rev Sci Instrum. 2007 Apr;78(4):045104. Available from: `https://aip.scitation.org/doi/abs/10.1063/1.2720728`.

[136] Wayne MA, Kwiat PG. Low-bias high-speed quantum random number generator via shaped optical pulses. Opt Express. 2010 Apr;18(9):9351-7. Available from: `http://www.osapublishing.org/oe/abstract.cfm?URI=oe-18-9-9351`.

[137] Li S, Wang L, Wu LA, et al. True random number generator based on discretized encoding of the time interval between photons. J Opt Soc Am A, JOSAA. 2013 Jan;30(1):124-7. Available from: `https://opg.optica.org/josaa/abstract.cfm?uri=josaa-30-1-124`.

[138] Thamrin NM, Witjaksono G, Nuruddin A, et al. A Photonic-based Random Number Generator for Cryptographic Application. In: 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. IEEE; 2008. p. 356-61. Available from: `https://ieeexplore.ieee.org/document/4617397`.

[139] de Jesus Lopes Soares E, Mendonca FA, Ramos RV. Quantum Random Number Generator Using Only One Single-Photon Detector. IEEE Photonics Technol Lett. 2014 Jan;26(9):851-3. Available from: `https://ieeexplore.ieee.org/document/6729066`.

[140] Tisa S, Villa F, Giudice A, et al. High-Speed Quantum Random Number Generation Using CMOS Photon Counting Detectors. IEEE J Sel Top Quantum Electron. 2014 Nov;21(3):23-9. Available from: `https://ieeexplore.ieee.org/document/6967758`.

[141] Ren M, Wu E, Liang Y, Jian Y, Wu G, Zeng H. Quantum random-number generator based on a photon-number-resolving detector. Phys Rev A. 2011 Feb;83:023820. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.83.023820`.

[142] Applegate MJ, Thomas O, Dynes JF, Yuan ZL, Ritchie DA, Shields AJ. Efficient and ro-

bust quantum random number generation by photon number detection. Applied Physics Letters. 2015;107(7):071106. Available from: `https://doi.org/10.1063/1.4928732`.

[143] Sanguinetti B, Martin A, Zbinden H, Gisin N. Quantum Random Number Generation on a Mobile Phone. Phys Rev X. 2014 Sep;4:031056. Available from: `https://link.aps.org/doi/10.1103/PhysRevX.4.031056`.

[144] Chen X, Greiner JN, Wrachtrup J, et al. Single Photon Randomness based on a Defect Center in Diamond - Scientific Reports. Sci Rep. 2019 Dec;9(18474):1-10. Available from: `https://doi.org/10.1038/s41598-019-54594-0`.

[145] Luo Q, Luo Q, Cheng Z, et al. Quantum random number generator based on single-photon emitter in gallium nitride. Opt Lett. 2020 Aug;45(15):4224-7. Available from: `https://opg.optica.org/ol/abstract.cfm?uri=ol-45-15-4224`.

[146] White SJU, Klauck F, Tran TT, et al. Quantum random number generation using a hexagonal boron nitride single photon emitter. J Opt. 2020 Dec;23(1):01LT01. Available from: `http://dx.doi.org/10.1088/2040-8986/abccff`.

[147] Aharonovich I, Englund D, Toth M. Solid-state single-photon emitters - Nature Photonics. Nat Photonics. 2016 Oct;10(10):631-41. Available from: `https://doi.org/10.1038/nphoton.2016.186`.

[148] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using gaussian-modulated coherent states. Nature. 2003 Jan;421(6920):238-41. Available from: `https://doi.org/10.1038/nature01289`.

[149] Shakhovoy R, Sych D, Sharoglazova V, Udaltsov A, Fedorov A, Kurochkin Y. Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator. Opt Express. 2020 Mar;28(5):6209-24. Available from: `http://opg.optica.org/oe/abstract.cfm?URI=oe-28-5-6209`.

[150] Qi B, Chi YM, Lo HK, Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. Opt Lett. 2010 Feb;35(3):312-4. Available from: `http://opg.optica.org/ol/abstract.cfm?URI=ol-35-3-312`.

[151] Jofre M, Curty M, Steinlechner F, Anzolin G, Torres JP, Mitchell MW, et al. True random numbers from amplified quantum vacuum. Opt Express. 2011 Oct;19(21):20665-72. Available from: `http://opg.optica.org/oe/abstract.cfm?URI=oe-19-21-20665`.

[152] Abellán C, Amaya W, Jofre M, Curty M, Acín A, Capmany J, et al. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. Opt Express. 2014 Jan;22(2):1645-54. Available from: `http://opg.optica.org/oe/abstract.cfm?URI=oe-22-2-1645`.

[153] Penzkofer A, Laubereau A, Kaiser W. High intensity Raman interactions. Progress in Quantum Electronics. 1979;6(2):55-140. Available from: `https://www.sciencedirect.com/science/article/pii/0079672779900119`.

[154] Raymer MG, Walmsley IA. III The Quantum Coherence Properties of Stimulated Raman Scattering. vol. 28 of Progress in Optics. Elsevier; 1990. p. 181-270. Available from: `https://www.sciencedirect.com/science/article/pii/S0079663808702907`.

[155] Abellan C, Amaya W, Domenech D, et al. Quantum entropy source on an InP photonic integrated circuit for random number generation. Optica. 2016 Sep;3(9):989-94. Available from: `https://opg.optica.org/optica/fulltext.cfm?uri=optica-3-9-989&id=349912`.

[156] Haylock B, Peace D, Lenzini F, et al. Multiplexed Quantum Random Number Generation. Quantum. 2019 May;3:141. Available from: `https://quantum-journal.org/papers/q-2019-05-13-141`.

[157] Prokhodtsov A, Kovalyuk V, An P, et al. Silicon nitride Mach-Zehnder interferometer for on-chip quantum random number generation. J Phys Conf Ser. 2020 Dec;1695(1):012118. Available from: `http://dx.doi.org/10.1088/1742-6596/1695/1/012118`.

[158] Stefanov A, Gisin N, Guinnard O, et al. Optical quantum random number generator. J Mod Opt. 2000 Mar;47(4):595-8. Available from: `https://www.tandfonline.com/doi/abs/10.1080/09500340008233380`.

[159] Dynes JF, Yuan ZL, Sharpe AW, Shields AJ. A high speed, postprocessing free, quantum

random number generator. Applied Physics Letters. 2008;93(3):031109. Available from: https://doi.org/10.1063/1.2961000.

[160] Wayne MA, Jeffrey ER, Akselrod GM, Kwiat PG. Photon arrival time quantum random number generation. Journal of Modern Optics. 2009;56(4):516-22. Available from: https://doi.org/10.1080/09500340802553244.

[161] Kwon O, Cho YW, Kim YH. Quantum random number generator using photon-number path entanglement. Appl Opt. 2009 Mar;48(9):1774-8. Available from: http://opg.optica.org/ao/abstract.cfm?URI=ao-48-9-1774.

[162] Vartsky D, Bar D, Gilad P, Schon A. High-speed, true random-number generator. Google Patents; 2011. US Patent 7,930,333.

[163] Wahl M, Leifgen M, Berlin M, Röhlicke T, Rahn HJ, Benson O. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. Applied Physics Letters. 2011;98(17):171105. Available from: https://doi.org/10.1063/1.3578456.

[164] Xu F, Qi B, Ma X, Xu H, Zheng H, Lo HK. Ultrafast quantum random number generation based on quantum phase fluctuations. Opt Express. 2012 May;20(11):12366-77. Available from: http://opg.optica.org/oe/abstract.cfm?URI=oe-20-11-12366.

[165] Stipčević M, Rogina BM. Quantum random number generator based on photonic emission in semiconductors. Review of Scientific Instruments. 2007;78(4):045104. Available from: https://aip.scitation.org/doi/abs/10.1063/1.2720728.

[166] Wilber SA. Entropy analysis and system design for quantum random number generators in CMOS integrated circuits; 2013. Available from: https://comscire.com/files/whitepaper/Pure_Quantum_White_Paper.pdf.

[167] Haw JY, Assad SM, Lance AM, Ng NHY, Sharma V, Lam PK, et al. Maximization of Extractable Randomness in a Quantum Random-Number Generator. Phys Rev Applied. 2015 May;3:054004. Available from: https://link.aps.org/doi/10.1103/PhysRevApplied.3.054004.

[168] Yang J, Liu J, Su Q, Li Z, Fan F, Xu B, et al. 5.4 Gbps real time quantum random number generator with simple implementation. Opt Express. 2016 Nov;24(24):27475-81. Available from: http://opg.optica.org/oe/abstract.cfm?URI=oe-24-24-27475.

[169] Bernardo-Gavito R, Bagci IE, Roberts J, et al. Extracting random numbers from quantum tunnelling through a single diode. Sci Rep. 2017 Dec;7(17879):1-6. Available from: https://doi.org/10.1038/s41598-017-18161-9.

[170] Balygin KA, Zaitsev VI, Klimov AN, Kulik SP, Molotkov SN. A Quantum Random Number Generator Based on the 100-Mbit/s Poisson Photocount Statistics. Journal of Experimental and Theoretical Physics. 2018 Jun;126(6):728-40. Available from: https://doi.org/10.1134/S1063776118060018.

[171] Xu H, Perenzoni D, Tomasi A, et al. A 16 × 16 Pixel Post-Processing Free Quantum Random Number Generator Based on SPADs. IEEE Trans Circuits Syst II. 2018 Apr;65(5):627-31. Available from: https://ieeexplore.ieee.org/document/8329139.

[172] Huang M, Chen Z, Zhang Y, Guo H. A Phase Fluctuation Based Practical Quantum Random Number Generator Scheme with Delay-Free Structure. Applied Sciences. 2020 Apr;10(7):2431. Available from: http://dx.doi.org/10.3390/app10072431.

[173] Gehring T, Lupo C, Kordts A, et al. Ultra-fast real-time quantum random number generator with correlated measurement outcomes and rigorous security certification. arXiv. 2018 Dec. Available from: https://arxiv.org/abs/1812.05377v3.

[174] Zhou Q, Valivarthi R, John C, Tittel W. Practical quantum random-number generation based on sampling vacuum fluctuations. Quantum Engineering. 2019;1(1):e8. E8 QUE-2019-0003.R1. Available from: https://onlinelibrary.wiley.com/doi/abs/10.1002/que2.8.

[175] Zheng Z, Zhang Y, Huang W, Yu S, Guo H. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. Review of Scientific Instruments. 2019;90(4):043105. Available from: https://doi.org/10.1063/1.5078547.

[176] Guo X, Cheng C, Wu M, Gao Q, Li P, Guo Y. Parallel real-time quantum random

number generator. Opt Lett. 2019 Nov;44(22):5566-9. Available from: `http://opg.optica.org/ol/abstract.cfm?URI=ol-44-22-5566`.

[177] Gehring T, Lupo C, Kordts A, Solar Nikolic D, Jain N, Rydberg T, et al. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. Nature Communications. 2021 Jan;12(1):605. Available from: `https://doi.org/10.1038/s41467-020-20813-w`.

[178] Aungskunsiri K, Amarit R, Wongpanya K, et al. Random number generation from a quantum tunneling diode. Appl Phys Lett. 2021 Aug;119(7):074002. Available from: `https://doi.org/10.1063/5.0055955`.

[179] Zhang Y, Lo HP, Mink A, Ikuta T, Honjo T, Takesue H, et al. A simple low-latency real-time certifiable quantum random number generator. Nature Communications. 2021 Feb;12(1):1056. Available from: `https://doi.org/10.1038/s41467-021-21069-8`.

[180] Turan MS, Barker E, Kelsey J, McKay KA, Baish ML, Boyle M, et al. Recommendation for the entropy sources used for random bit generation. NIST Special Publication. 2018;800(90B):102. Available from: `https://csrc.nist.gov/publications/detail/sp/800-90b/final`.

[181] Fischer V. A Closer Look at Security in Random Number Generators Design. In: Constructive Side-Channel Analysis and Secure Design. Berlin, Germany: Springer; 2012. p. 167-82. Available from: `https://link.springer.com/chapter/10.1007/978-3-642-29912-4_13`.

[182] Bucci M, Luzzi R. Design of testable random bit generators. In: CHES'05: Proceedings of the 7th international conference on Cryptographic hardware and embedded systems. Berlin, Germany: Springer-Verlag; 2005. p. 147-56. Available from: `https://dl.acm.org/doi/10.1007/11545262_11`.

[183] Saito T, Ishii K, Tatsuno I, Sukagawa S, Yanagita T. Randomness and genuine random number generator with self-testing functions. SNA + MC2010: Joint international conference of supercomputing in nuclear applications and Monte Carlo. Japan; 2010. Available from: `http://inis.iaea.org/search/search.aspx?orig_q=RN:43020174`.

[184] Fiorentino M, Munro WJ, Santori CM, et al. All-fiber-optic quantum random number generator. In: 2006 Conference on Lasers and Electro-Optics and 2006 Quantum Electronics and Laser Science Conference. IEEE; 2006. p. 1-2. Available from: `https://ieeexplore.ieee.org/document/4628717`.

[185] Vallone G, Marangon DG, Tomasin M, Villoresi P. Quantum randomness certified by the uncertainty principle. Phys Rev A. 2014 Nov;90:052327. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.90.052327`.

[186] Bell JS. On the Einstein Podolsky Rosen paradox. Physics Physique Fizika. 1964 Nov;1(3):195-200. Available from: `https://link.aps.org/doi/10.1103/PhysicsPhysiqueFizika.1.195`.

[187] Mayers D, Yao A. Quantum Cryptography with Imperfect Apparatus. arXiv. 1998 Sep. Available from: `https://arxiv.org/abs/quant-ph/9809039v1`.

[188] Clauser JF, Horne MA, Shimony A, et al. Proposed Experiment to Test Local Hidden-Variable Theories. Phys Rev Lett. 1969 Oct;23(15):880-4. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.23.880`.

[189] Miller CA, Shi Y. Universal Security for Randomness Expansion from the Spot-Checking Protocol. SIAM J Comput. 2017 Aug. Available from: `https://epubs.siam.org/doi/10.1137/15M1044333`.

[190] Pironio S, Acín A, Massar S, de la Giroday AB, Matsukevich DN, Maunz P, et al. Random numbers certified by Bell's theorem. Nature. 2010 Apr;464(7291):1021–1024. Available from: `http://dx.doi.org/10.1038/nature09008`.

[191] Liu WZ, Li MH, Ragy S, Zhao SR, Bai B, Liu Y, et al. Device-independent randomness expansion against quantum side information. Nature Physics. 2021 Apr;17(4):448-51. Available from: `https://doi.org/10.1038/s41567-020-01147-2`.

[192] Li MH, Zhang X, Liu WZ, Zhao SR, Bai B, Liu Y, et al. Experimental Realization of Device-Independent Quantum Randomness Expansion. Phys Rev Lett. 2021

Feb;126:050503. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.126.050503`.

[193] Shalm LK, Zhang Y, Bienfang JC, Schlager C, Stevens MJ, Mazurek MD, et al. Device-independent randomness expansion with entangled photons. Nature Physics. 2021 Apr;17(4):452-6. Available from: `https://doi.org/10.1038/s41567-020-01153-4`.

[194] Deng DL, Zu C, Chang XY, et al. Exploring Quantum Contextuality to Generate True Random Numbers. arXiv. 2013 Jan. Available from: `https://arxiv.org/abs/1301.5364v2`.

[195] Kochen S, Specker EP. The Problem of Hidden Variables in Quantum Mechanics. In: The Logico-Algebraic Approach to Quantum Mechanics: Volume I: Historical Evolution. Dordrecht, The Netherlands: Springer; 1975. p. 293-328. Available from: `https://doi.org/10.1007/978-94-010-1795-4_17`.

[196] Larsson JÅ. Loopholes in Bell inequality tests of local realism. J Phys A: Math Theor. 2014 Oct;47(42):424003. Available from: `http://dx.doi.org/10.1088/1751-8113/47/42/424003`.

[197] Colbeck R, Renner R. Free randomness can be amplified. Nature Physics. 2012 May;8(6):450–453. Available from: `http://dx.doi.org/10.1038/nphys2300`.

[198] Santha M, Vazirani UV. Generating quasi-random sequences from semi-random sources. J Comput System Sci. 1986 Aug;33(1):75-87. Available from: `https://dl.acm.org/doi/10.1016/0022-0000%2886%2990044-9`.

[199] Braunstein SL, Caves CM. Wringing out better Bell inequalities. Ann Phys. 1990 Aug;202(1):22-56. Available from: `https://www.sciencedirect.com/science/article/pii/000349169090339P`.

[200] Gallego R, Masanes L, De La Torre G, Dhara C, Aolita L, Acín A. Full randomness from arbitrarily deterministic events. Nature Communications. 2013 Oct;4(1). Available from: `http://dx.doi.org/10.1038/ncomms3654`.

[201] Chung KM, Shi Y, Wu X. General randomness amplification with non-signaling security. Online] Available: https://ix cs uoregon edu/˜ xiaodiwu/papers/csw16 pdf. 2016.

[202] Plesch M, Pivoluska M. Device-independent randomness amplification with a single device. Physics Letters A. 2014;378(40):2938-44. Available from: `https://www.sciencedirect.com/science/article/pii/S0375960114008032`.

[203] Bouda J, Pawłowski M, Pivoluska M, et al. Device-independent randomness extraction from an arbitrarily weak min-entropy source. Phys Rev A. 2014 Sep;90(3):032313. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.90.032313`.

[204] Koh DE, Hall MJW, Setiawan, Pope JE, Marletto C, Kay A, et al. Effects of Reduced Measurement Independence on Bell-Based Randomness Expansion. Phys Rev Lett. 2012 Oct;109:160404. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.109.160404`.

[205] Pivoluska M, Plesch M, Farkas M, et al. Semi-device-independent random number generation with flexible assumptions - npj Quantum Information. npj Quantum Inf. 2021 Mar;7(50):1-12. Available from: `https://doi.org/10.1038/s41534-021-00387-1`.

[206] Lovic V, Marangon DG, Lucamarini M, Yuan Z, Shields AJ. Characterizing Phase Noise in a Gain-Switched Laser Diode for Quantum Random-Number Generation. Phys Rev Applied. 2021 Nov;16:054012. Available from: `https://link.aps.org/doi/10.1103/PhysRevApplied.16.054012`.

[207] Li Y, Fei Y, Wang W, Meng X, Wang H, Duan Q, et al. Quantum random number generator using a cloud superconducting quantum computer based on source-independent protocol. Scientific Reports. 2021 Dec;11(1):23873. Available from: `https://doi.org/10.1038/s41598-021-03286-9`.

[208] Šupić I, Skrzypczyk P, Cavalcanti D. Measurement-device-independent entanglement and randomness estimation in quantum networks. Phys Rev A. 2017 Apr;95:042340. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.95.042340`.

[209] Bowles J, Quintino MT, Brunner N. Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-Measure Scenario with Independent Devices. Phys

Rev Lett. 2014 Apr;112:140407. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.112.140407`.

[210] Ambainis A, Leung D, Mancinska L, et al. Quantum Random Access Codes with Shared Randomness. arXiv. 2008 Oct. Available from: `https://arxiv.org/abs/0810.2937v3`.

[211] Vaisakh M, Patra Rk, Janpandit M, Sen S, Banik M, Chaturvedi A. Mutually unbiased balanced functions and generalized random access codes. Phys Rev A. 2021 Jul;104:012420. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.104.012420`.

[212] Gallego R, Brunner N, Hadley C, Acín A. Device-Independent Tests of Classical and Quantum Dimensions. Phys Rev Lett. 2010 Nov;105:230501. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.105.230501`.

[213] Li HW, Pawłowski M, Yin ZQ, et al. Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes. Phys Rev A. 2012 May;85(5):052308. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.85.052308`.

[214] Mannalath V, Pathak A. Bounds on semi-device-independent quantum random-number expansion capabilities. Phys Rev A. 2022 Feb;105:022435. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.105.022435`.

[215] Hardy L. Quantum mechanics, local realistic theories, and Lorentz-invariant realistic theories. Phys Rev Lett. 1992 May;68(20):2981-4. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.68.2981`.

[216] Cabello A. Bell's theorem with and without inequalities for the three-qubit Greenberger-Horne-Zeilinger and W states. Phys Rev A. 2002 Feb;65(3):032108. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.65.032108`.

[217] Li HW, Pawłowski M, Rahaman R, et al. Device- and semi–device-independent random numbers based on noninequality paradox. Phys Rev A. 2015 Aug;92(2):022327. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.92.022327`.

[218] Pan AK. Semi-device-independent randomness certification using Mermin's proof of Kochen–Specker contextuality. Eur Phys J D. 2021 Mar;75(3):98-8. Available from: `https://doi.org/10.1140/epjd/s10053-021-00105-8`.

[219] Mermin ND. Simple unified form for the major no-hidden-variables theorems. Phys Rev Lett. 1990 Dec;65(27):3373-6. Available from: `https://link.aps.org/doi/10.1103/PhysRevLett.65.3373`.

[220] Van Himbeeck, T., Woodhead, E., Cerf, N., Garcıa-Patron, R. & Pironio, S. Semi-device-independent framework based on natural physical assumptions. *Quantum.* **1** pp. 33 (2017) Available from:`https://quantum-journal.org/papers/q-2017-11-18-33`

[221] Van Himbeeck T, Pironio S. Correlations and randomness generation based on energy constraints. arXiv. 2019 May. Available from: `https://arxiv.org/abs/1905.09117v1`.

[222] Tebyanian H, Zahidy M, Avesani M, et al. Semi-device independent randomness generation based on quantum state's indistinguishability. Quantum Sci Technol. 2021 Sep;6(4):045026. Available from: `http://dx.doi.org/10.1088/2058-9565/ac2047`.

[223] Tebyanian H, Avesani M, Vallone G, et al. Semi-device-independent randomness from *d*-outcome continuous-variable detection. Phys Rev A. 2021 Dec;104(6):062424. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.104.062424`.

[224] Rusca D, Tebyanian H, Martin A, et al. Fast self-testing quantum random number generator based on homodyne detection. Appl Phys Lett. 2020 Jun;116(26):264004. Available from: `https://doi.org/10.1063/5.0011479`.

[225] Rusca D, van Himbeeck T, Martin A, Brask JB, Shi W, Pironio S, et al. Self-testing quantum random-number generator based on an energy bound. Phys Rev A. 2019 Dec;100:062338. Available from: `https://link.aps.org/doi/10.1103/PhysRevA.100.062338`.

[226] Carceller, C., Flatt, K., Lee, H., Bae, J. & Brask, J. Quantum vs Noncontextual Semi-Device-Independent Randomness Certification. Phys. Rev. Lett.**129**, 050501 (2022) Available from: `https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.129.050501`.

[227] Zhou YQ, Li HW, Wang YK, et al. Semi-device-independent randomness expansion with partially free random sources. Phys Rev A. 2015 Aug;92(2):022331. Available from: https://link.aps.org/doi/10.1103/PhysRevA.92.022331.

[228] Senno G, Acín A. Semi-device-independent full randomness amplification based on energy bounds. arXiv. 2021 Aug. Available from: https://arxiv.org/abs/2108.09100v1.

[229] Cao Z, Zhou H, Yuan X, Ma X. Source-Independent Quantum Random Number Generation. Phys Rev X. 2016 Feb;6:011020. Available from: https://link.aps.org/doi/10.1103/PhysRevX.6.011020.

[230] Brask JB, Martin A, Esposito W, Houlmann R, Bowles J, Zbinden H, et al. Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination. Phys Rev Applied. 2017 May;7:054018. Available from: https://link.aps.org/doi/10.1103/PhysRevApplied.7.054018.

[231] Marangon DG, Vallone G, Villoresi P. Source-Device-Independent Ultrafast Quantum Random Number Generation. Phys Rev Lett. 2017 Feb;118:060503. Available from: https://link.aps.org/doi/10.1103/PhysRevLett.118.060503.

[232] Liu Y, Zhao Q, Li MH, Guan JY, Zhang Y, Bai B, et al. Device-independent quantum random-number generation. Nature. 2018 Oct;562(7728):548-51. Available from: https://doi.org/10.1038/s41586-018-0559-3.

[233] Li YH, Han X, Cao Y, Yuan X, Li ZP, Guan JY, et al. Quantum random number generation with uncharacterized laser and sunlight. npj Quantum Information. 2019 Nov;5(1):97. Available from: https://doi.org/10.1038/s41534-019-0208-1.

[234] Michel T, Haw JY, Marangon DG, et al. Real-Time Source-Independent Quantum Random-Number Generator with Squeezed States. Phys Rev Appl. 2019 Sep;12(3):034017. Available from: https://link.aps.org/doi/10.1103/PhysRevApplied.12.034017.

[235] Drahi D, Walk N, Hoban MJ, Fedorov AK, Shakhovoy R, Feimov A, et al. Certified Quantum Random Numbers from Untrusted Light. Phys Rev X. 2020 Dec;10:041048. Available from: https://link.aps.org/doi/10.1103/PhysRevX.10.041048.

[236] Avesani M, Tebyanian H, Villoresi P, Vallone G. Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator. Phys Rev Applied. 2021 Mar;15:034034. Available from: https://link.aps.org/doi/10.1103/PhysRevApplied.15.034034.

[237] Stapp HP. The Copenhagen Interpretation. Am J Phys. 2005 Jul;40(8):1098. Available from: https://aapt.scitation.org/doi/10.1119/1.1986768.

[238] Popescu S, Rohrlich D. Quantum nonlocality as an axiom. Found Phys. 1994 Mar;24(3):379-85. Available from: https://doi.org/10.1007/BF02058098.

[239] Cirel'son BS. Quantum generalizations of Bell's inequality. Lett Math Phys. 1980 Mar;4(2):93-100. Available from: https://doi.org/10.1007/BF00417500.

[240] Pawłowski M, Paterek T, Kaszlikowski D, et al. Information causality as a physical principle - Nature. Nature. 2009 Oct;461(7267):1101-4. Available from: https://doi.org/10.1038/nature08400.

[241] Hardy L. Quantum Theory From Five Reasonable Axioms. arXiv. 2001 Jan. Available from: https://arxiv.org/abs/quant-ph/0101012v4.

[242] Simon BN, Simon S, Gori F, Santarsiero M, Borghi R, Mukunda N, et al. Nonquantum Entanglement Resolves a Basic Issue in Polarization Optics. Phys Rev Lett. 2010 Jan;104:023901. Available from: https://link.aps.org/doi/10.1103/PhysRevLett.104.023901.

[243] Aravinda S, Srikanth R, Pathak A. On the origin of nonclassicality in single systems. J Phys A: Math Theor. 2017 Oct;50(46):465303. Available from: http://dx.doi.org/10.1088/1751-8121/aa8d29.

[244] Labs Q. Quantum Random Number Generator — QuintessenceLabs;. (Accessed on 25/02/2022). https://www.quintessencelabs.com/products/qstream-quantum-true-random-number-generator/.

[245] eMotion. Products - Quantum eMotion Inc.;. (Accessed on 25/02/2022). https://www.quantumemotion.com/products/.

[246] EYL. Quantum Random Number Generator – EYL;. (Accessed on 25/02/2022). `https://www.eylpartners.com/index.php/product-overview/?ckattempt=1`.

[247] quRNG. quRNG_datasheet.cdr;. (Accessed on 25/02/2022). `https://www.qd-latam.com/_libs/dwns/639.pdf`.

[248] MPD. Micro Photon Devices - Quantum Random Number;. (Accessed on 25/02/2022). `http://www.micro-photon-devices.com/Docs/Datasheet/QRNG.pdf`.

[249] quside. quside;. (Accessed on 25/02/2022). `https://quside.com`.

[250] QNU. Quantum Random Number Generator (QRNG) - QNu Labs - How it works?; 2021. [Online; accessed 26. Feb. 2022]. Available from: `https://www.qnulabs.com/tropos-quantum-random-number-generator`.

[251] Zhang, Y., Shalm, L., Bienfang, J., Stevens, M., Mazurek, M., Nam, S., Abellán, C., Amaya, W., Mitchell, M., Fu, H. & Others Experimental low-latency device-independent quantum randomness. *Physical Review Letters*. **124**, 010505 (2020)

[252] Bierhorst, P., Knill, E., Glancy, S., Zhang, Y., Mink, A., Jordan, S., Rommal, A., Liu, Y., Christensen, B., Nam, S. & Others Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature*. **556**, 223-226 (2018)