

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

186,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Device Independence and the Quest towards Physical Limits of Privacy

Gopalan Raghavan

Abstract

There is a looming threat over current methods of data encryption through advances in quantum computation. Interestingly, this potential threat can be countered through the use of quantum resources such as coherent superposition, entanglement and inherent randomness. These, together with non-clonability of arbitrary quantum states, offer provably secure means of sharing encryption keys between two parties. This physically assured privacy is however provably secure only in theory but not in practice. Device independent approaches seek to provide physically assured privacy of devices of untrusted origin. The quest towards realization of such devices is predicated on conducting loop-hole-free Bell tests which require the use of certified quantum random number generators. The experimental apparatuses for conducting such tests themselves use non-ideal sources, detectors and optical components making such certification extremely difficult. This expository chapter presents a brief overview (not a review) of Device Independence and the conceptual and practical difficulties it entails.

Keywords: QRNG, QKD, device independence, loop-hole-free Bell tests, nonlocality

1. Introduction

The advent of quantum technologies holds the promise of novel innovations in computing, communication and sensing. Quintessential quantum properties such as superposition and entanglement are perceived as essential resources for the realization of these technologies. Quantum states allow for non-local correlations under no-signaling conditions [1, 2]. Claims to “quantum supremacy” in quantum computing or provable security in quantum cryptography hinges on the assertion that quantum resources are not only needed, but can be gainfully employed for realizing functionalities, which classical resources cannot supply. Quantum cryptography or rather quantum key distribution (QKD) schemes are claimed to be provably secure based on the quantum nature of the carriers of information. The claim on information security relies on the fact, that perfect copies of arbitrary quantum states cannot be made (the “no-cloning” theorem) [3] and the fact that measurements disturb the state of the system in an irreversible fashion, resulting in perfectly random outcomes. In quantum key distribution protocols such as the Ekert’s [4], non-local correlations between a pair of entangled photons are utilized to realize

secure key exchange between two parties in space-like separated regions. One of the key components of a QKD device is a quantum random number generator (QRNG) [5–7]. These devices are believed to generate perfect and inherently random sequences that cannot be produced by any device based on classical phenomena or by using mathematical algorithms however complex they might be. High-speed QRNGs are an important requirement not only for QKD but have potential uses in gambling, commerce, and classical cryptography. Given the importance of this device for cryptography, one should test this device before using it. When a consumer buys a piece of quantum-enabled equipment such as QKD boxes or QRNGs, there is a need to find out whether it is the “real McCoy” and the hardware performs as advertised. For instances, the QRNG, sourced through an untrusted party may generate a seemingly random sequences on demand, but it begs the question, whether these sequences arise from a genuine quantum process and have not been generated through some classical or algorithmic means? Alternately, the supplier of the device could have generated a very large sequence through a quantum process and stored it in the device while retaining copy for herself. Even without assuming any evil intent on part of the supplier, the device could also be unreliable because of imperfections in the source or detectors or even due the noise being well-above permissible thresholds. Standard statistical tests for randomness such as DIEHARD and DIEHARDER provided by NIST, USA [8, 9] are not the solution to this problem. Statistical tests for randomness merely certify the absence of certain patterns in the sequences within the bounds of finite computational power at the disposal of the of the user. It would be logical fallacy to think that absence of evidence is evidence of absence. Statistical tests are therefore not tests of genuine quantum randomness and most certainly do not provide any assurance regarding the privacy of the data that is generated. For the QRNG to satisfy its claimed performance not only should the output of the device be perfectly random to the user, but to any observer including the supplier of device. Then, and only then, could a “QRNG” be deemed to be a Perfect and Private Random Number generator or PPRNG as we shall call it henceforth. The advantages of quantum resources for secure communications or random number generation are a theoretical fact but, demonstrating that a piece of hardware actually exploits quantum properties of matter and fields in an effective manner is a non-trivial problem. The issue at hand is an important one because, it is related to very reliability of the quantum device itself. Extraordinary, though it seems, it is possible that a certain class of QRNGs and QKDs of illicit and unknown provenance, could be certified to be provably secure through the performance of certain class of tests called Bell tests performed on them [10–13]. Such Bell test certified devices are however extremely difficult to realize and currently the rates of random number generation with them are extremely small. Before we get into issues of device independence, we first examine some aspects of randomness, non-locality and non-local correlations.

2. Randomness, nonlocality and non-local correlations

The Famous paper by Einstein, Podolsky and Rosen in Physical Review (1935) [14] was a watershed event setting-off a vigorous debate on the so-called hidden variable theories. Their central conclusion was that quantum mechanical description of physical systems is incomplete and that, quantum mechanical rules must be supplemented with additional variables to exorcize the seemingly inherent randomness of nature. Bohr rebuts these arguments in Physical Review [15] claiming that quantum mechanics deals with the statistical outcomes of the

interactions of a microscopic system with a macroscopic classical apparatus and nothing further. In physical theories, classical or quantum, every system is associated with a mathematical description of it called the state. Given the state of a system at a certain instant of time, the time evolution of the system is described by Newton's laws of motion in classical mechanics and the Schrödinger equation in quantum mechanics respectively. Both these equations are perfectly deterministic and reversible in time. The time evolution of quantum states is described is unitary. In classical systems, randomness arises primarily due to inadequate information about the initial conditions especially when the degrees of freedom are extremely large. Quite often, we may also choose to ignore vast amounts of data simply because we do not have the computational resources to handle it. This sort of coarse graining of data becomes a practical expediency. The solution to handling full-blown turbulence by solving the Navier–Stokes equation would come to mind. In systems exhibiting classical chaos [16], even though the underlying equation of motion are deterministic, the apparent randomness and unpredictability arises because of sensitivity to initial conditions and the finite precision with which the initial conditions are supplied. In summary, classical randomness arises from ignorance or computational limitations and is therefore not an inherent property of nature. Such randomness is deemed to be epistemological in character. In quantum mechanics, while evolution itself is unitary, the outcomes of measurements performed on the quantum state are probabilistic. The expectation value of physical properties associated with observable \hat{A} for an ensemble of measurements is given by the Born rule $\langle \hat{A} \rangle = \text{Tr}(\hat{\rho} \hat{A})$. Given an ensemble of measurements M performed on identically prepared states, the probability of the j th outcome over a set of possible outcomes $\{E_i\}$ is given by $(p_j|M) = \text{Tr}(\hat{\rho} E_j)$ [2]. The Born rule thus provides us the leeway that links the abstract quantum state with observed phenomena. The outcome of single observation measurement is believed to be completely and inherently unpredictable and is an essential aspect of nature herself. Quantum mechanics does not offer any clue as to the physical origins of the observed randomness of outcomes. The implicit assumption is that the God of all things does play dice and is indeed an inveterate and compulsive gambler. Quantum randomness is therefore said to be inherent or ontological (ontic) randomness. It would be wise to bear in mind that there is no finality to any of these assertions. They are provisional to way we understand nature as of now. It is in this context; we should make a distinction between ontic and epistemic randomness; Ontic randomness is intrinsically associated with observable quantities of the system and related to self-adjoint operators. One or the other of the possible eigenvalues of these operators are manifest upon an observation. No a priori value can be associated with properties of the system. It is in this sense that one asserts that “quantum phenomena” are not realistic. Robust average values can however be assigned to average or expectation values of observables, which is what the Born formula helps us compute. Quantum mechanics is then an ensemble theory which provides us with recipe to calculate averages of repeated measurements made on the system. There is rich literature regarding the nature quantum state, the wavefunction itself. There are interpretations of quantum mechanics that significantly differ in their viewpoint. Since our purpose here is not to get deeply mired into foundations of quantum mechanics, we shall desist from such digressions, given the limited ambitions of this chapter.

It is a something of a fundamental theorem that purely local operations performed on single device, cannot be used to establish that the random sequences emitted by a given device has not been simulated using only classical resources. However, Bell tests provide the unimpeachable means of certifying these devices.

Such a QRNG is dubbed Device Independent QRNG or DI-QRNG for short [17–22]. The interesting thing here is that such Quantum Random number generators can be certified, without any knowledge of the inner workings of the device. It is therefore solely through non-local correlations present in quantum states that such a certification becomes feasible. Device Independent QRNG that meets the requirements of the output being perfectly unpredictable to anyone and meets the stringent norm absolute privacy. For the case of QKDs, the successful performance of loop-hole-free Bell tests, provides the information theoretical assurance that QKD supplies perfectly random keys to which only the authenticated parties are privy but no one else is.

3. Bell's inequalities

The fundamental assumption that the properties of a physical entity are independent and prior to any measurement is called realism. The premise that all physical processes are subject to relativistic causality is called locality. When observations are made at two locations and the only way in which the information of a measurement and its outcome in the first location can be made available to the second location prior to the measurement made there is through a superluminal signal, we refer to the locations as being located in space-like separated regions. Any theory which asserts that measurements made at space-like separated regions cannot influence outcomes in other regions is called a local theory. All theories where both these conditions of locality and realism are maintained to be valid, are called local realistic theories [23]. Quantum Mechanics is in good part patently non-local and does not uphold realism. We say to a “good part” because separable states in quantum mechanics do not exhibit this property, only entangled states do. While the experimental certification of any local realistic theory or quantum mechanics as the correct description of nature is logically impossible, the consistency of one or the other with observations is feasible within experimental errors. We may test for the compatibility of local or local-realistic theories with experimental facts by supplementing these theories addition assumptions that account for common causes or prior correlations on two systems that had interacted earlier but are now located in space-like separated regions. Such theories are called local hidden variable theories. In trying to establish the appropriateness of a theory, it is customary to look for theories with fewest assumptions and their explanatory power over a wide variety of phenomena. A single failure would of course render it unacceptable. It is within these restrictions that one would look for the contradistinction between a theory or of possible set of theories with others. In the present case, we are interested in the differences in the predictions made by local realistic theories and quantum mechanics.

John Bell [23] proved an extraordinary and significant theorem that imposes quantitative limits on the correlations allowed by local realistic theories. The central result here is that the correlations exhibited by maximally entangled states exceed these limits. Before venturing into Bell discovery, it is first necessary to appreciate that the tests proposed by Bell are not tests on the validity of quantum mechanics per se. Bell tests merely provide an upper bound on the level of correlations that can be attained by any local realistic theory. In quantum mechanics, given the state of a multipartite system, the decomposition of such a composite state into product states of the subsystems is in general not possible. For example, there are bi-partite systems $|\varphi\rangle_{AB}$ that can in general be written as a convex combination of product of the states of the sub-systems: $|\psi\rangle_{AB} \neq |\varphi\rangle_A \otimes |\chi\rangle_B$. The states that can be so-written are called separable states [2]. States which are not separable are called entangled

states [24]. There are bi-partite states called Bell states that are maximally entangled in that, they exhibit perfect non-local correlations or anti-correlations. The sub-systems for such states could either have been generated through a common process or they could have interacted directly or indirectly in the past and may describe a physical property subject to some conservation law. Rather than giving original references we directed the reader to a review article [24] for further details. As an example of Bell states we consider, two photons prepared through the process of spontaneous parametric down conversion (SPDC) [25] that could be prepared in the following Bell states which describe photons entangled in their polarization degree of freedom:

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle) \quad (1)$$

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|HV\rangle \pm |VH\rangle) \quad (2)$$

Photons being “flying qubits” each of the two photons could travel to two parties separated by an arbitrary distance. When either of the parties makes a measurement in the V/H basis, both photons in the $|\psi^\pm\rangle$ state would be found in the horizontal or vertical polarization with equal probability and the states of polarization of the two photons would be perfectly correlated. In case the $|\phi^\pm\rangle$, a perfect anti-correlation would be the result. Local measurements performed at spacelike separated regions, ensure the no-signaling condition. The Bell states could very well have been prepared in Bell states in some other basis set such as:

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|DD\rangle \pm |AA\rangle) \quad (3)$$

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|DA\rangle \pm |AD\rangle) \quad (4)$$

and so forth. In any case, Alice the source of the qubit and Bob the recipient of the qubit could choose to measure their photon in the {H, V} basis or the {D, A} basis. If the Bell states have been prepared with {H, V} polarizations states, only when both Alice and Bob measure with identical basis sets would they end with perfectly correlated or anti-correlated outcomes else their outcomes are perfectly random with respect to each other since {H, V} and {D, A} basis sets used by Alice and Bob for their local measurements are mutually unbiased. The initial states could then be subject to loop-hole-free Bell test by using the two black boxes procured from the supplier. In the case of an entanglement-based implementation of QKD, so long as it is ensured that no classical information such as the measurement outcomes leaks-out from Alice or Bob, the device outputs are secure. The notion of non-locality may best be understood through a Gedankenexperiment popularized by Popescu and R  hrlich [26]. We will first introduce one version of this experiment. The mathematical treatment laid out here closely follows the treatment in [27]. Let Alice and Bob be two stations that are space-like separated. Let these two stations be provided with two black boxes. These boxes have inputs x and y respectively, where, $x, y \in \{0, 1\}$. Let these two black boxes be designed to produce outputs a, b such that $a, b \in \{-1, +1\}$. The **Figure 1**, illustrates this game.

Quite independent of any physical theory, we are free to impose restrictions on the outputs for various possible inputs. The statistical outcomes of such games that can be repeatedly played these boxes is best described through conditional and joint probabilities. We are interested in computing the joint probability the outputs take



Figure 1.

A and B are two black boxes located in space-like separated regions. Inputs x, y to these boxes take value $\{0, 1\}$. The output of these boxes a, b assume values $\{-1, +1\}$. The joint probability $p(a, b|x, y)$ is the quantity of interest in this Gedankenexperiment.

conditioned by the input setting and their numerical values. Such a joint probability is written as $p(a, b|x, y)$. Here, we have simplified the notation by not writing the setting and the input values separately. When the two boxes are well-separated such that no signal traveling at a finite speed it generally expected that the outputs of the two boxes would be influenced only by the input settings and their values of each box and that the outputs would not be influenced by the input setting of the distant box. This assumption is called a *no-signaling* condition [1]. Under such a constraint, the joint probability would be written as:

$$p(a, b|x, y) = p(a|x).p(b|y). \quad (5)$$

In writing the joint probability in terms of the product of probabilities as above, the additional assumption is that there are no common causes or past influences that would bring about a correlation between the two boxes. To account for all such possibilities, we may rewrite the conditional probability above as:

$$p(a, b|x, y, \lambda) = p(a|x, \lambda).p(b|y, \lambda) \quad (6)$$

where λ accounts for all possible common causes and influences. The parameters (s) are sometimes referred to as hidden variables. As an illustrative example of such factors, let us consider two individuals at two distant location who go shopping for a soap dish or a toothbrush and that these two objects generally come in blue or orange color. If a common supplier had supplied a stock of only blue soap dishes and orange toothbrushes, then it should come as no surprises that whenever the two individuals buy the same object they end-up with the same color and whenever they buy different objects, they are of a different color. To factor-in such possibilities, we may rewrite the above joint conditional probability in terms of the product of the individual conditional probabilities. When the Joint conditional probability can be factored as above, we refer to the condition as being non-local. By assuming that the variable λ has a well-defined probability distribution function $\sigma(\lambda)$ that does depend on the input settings i_a, i_b of either of the boxes, we can integrate over that it might take during various runs of the experiment and arrive at

$$p(a, b|x, y) = \int d\lambda \sigma(\lambda) p(a|x, \lambda).p(b|y, \lambda) \quad (7)$$

This condition is then a formal statement of the locality condition. This gist of this statement is that any local operations carried out on either of the two stations oughtn't have any influence on the other station, when the two stations are in

space-like separated regions. It is implicitly assumed that the choice of input setting is independent of $\sigma(\lambda)$ which is itself independent of the input settings. In actual implementations, the input settings are chosen with the aid of quantum random number generators. Whenever

$$p(x, y|a, b) \neq p(x|a).p(y|b) \quad (8)$$

the two events are not independent of each other but are correlated. In Bell's original formulation [bell24], he considered only perfect correlations or anti-correlation in the outputs. The CHSH inequality considers the experimentally realistic situation and based on the computation of expectation values of the outputs. Given $x, y \in \{0, 1\} \wedge a, b \in \{-1, +1\}$, the expectation value or the average value over an ensemble of repeated measurement of identically prepared states is given by:

$$\langle a_x b_y \rangle = \sum_{a, b} ab p(ab|xy) \quad (9)$$

Under conditions of objective locality or local realism, the following equality holds:

$$S = \langle a_0 b_0 \rangle + \langle a_0 b_1 \rangle + \langle a_1 b_0 \rangle - \langle a_1 b_1 \rangle \leq 2 \quad (10)$$

With quantum systems, S could exceed this value because non-separable states are of a significantly different nature compared local realistic theories. To appreciate this, we may write Bell states in terms of a computational basis as for instance

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle) \quad (11)$$

The vectors $|0\rangle \wedge |1\rangle$ are the eigen vectors of the Pauli operator σ_z . Identifying the inputs x and y with measurements along vectorial directions x and y respectively, the quantum mechanical expectation value $\langle a_x b_y \rangle = x \cdot y$. When a mutually unbiased basis (MUBS) [28] choice is made for x, y, it is trivial to show that $S \leq 2\sqrt{2}$.

4. Experimental tests of Bell's inequalities

Let us now consider the following experiment wherein there are two experimental stations as discussed in the earlier Gedankenexperiment but with a small twist: Here, S is a SPDC source emitting a pair of polarization entangled photons in one of the Bell states and let a and b be randomly obtained from certified QRNGs located and securely isolated at the stations a and b respectively. The two inputs of are then used to choose between the two mutually unbiased $\{V, H\}$ and $\{D, A\}$ where, V/H refers to the vertical/horizontal basis and D/A refers to diagonal/anti-diagonal basis sets respectively (**Figure 2**).

The state emitted from the source is one of the Bell states and let us assume without loss of generality, that the state is ψ^+ . Spontaneous parametric downconversion is a probabilistic process with a very low probability of emitting an entangled photon pair. Hence, for optimal pump laser powers, the probability of multiple pairs being emitted is extremely low. After considering the travel time and setting a coincidence window, when both detectors detect photons, it most likely that the pair of photons were emitted simultaneously and are in an entangled state. The source may be suitably characterized through Quantum State Tomography

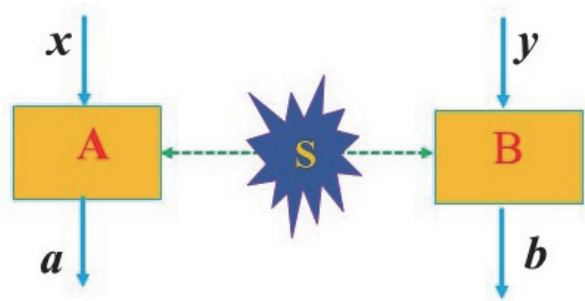


Figure 2. *S is a entangled photon source emitting photon in a Bell state with one photon of each pair reaching stations A and B located in space-like separated regions. Inputs x, y to these boxes take value $\{0, 1\}$. The basis choice at either station is made based on the random inputs x, y . The output of these boxes are a, b assuming values $\{-1, +1\}$ as earlier.*

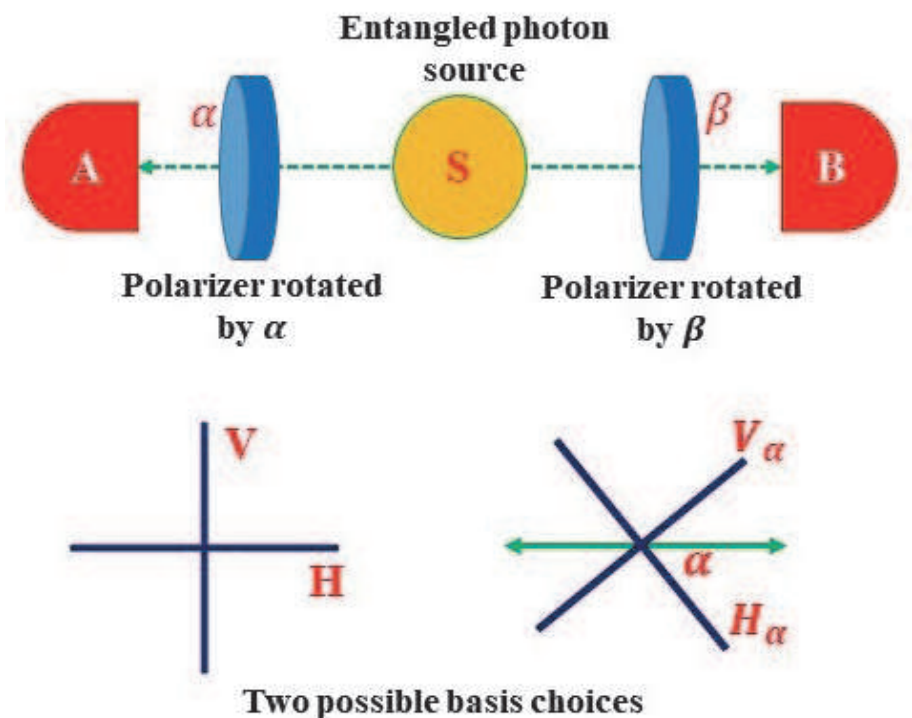


Figure 3. *Basis choices for measurements may be made independently at either station such as $H/V, H_\alpha/V_\alpha$ for arbitrary α .*

(QST) [3]. Usually, local corrections of polarization may be corrected through suitable polarization controllers located at A and B. Once the steps are done and the source is well-characterized, projective measurements are carried out at each of the stations. To carry out measurements, the basis choice at each station is carried out rotating the polarizers by some angle. We may however choose to measure in rotated basis as illustrated (**Figure 3**).

The rotated basis vectors may be expressed as:

$$|H_\alpha\rangle = \cos\alpha|H\rangle - \sin\alpha|V\rangle, |V_\alpha\rangle = \sin\alpha|H\rangle + \cos\alpha|V\rangle \quad (12)$$

If the polarizers at A and B are rotated by angles α and β respectively and an ensemble of measurements are carried out on identically prepared states, quantum mechanics predicts the probability of obtaining coincidence counts when the vertical polarization is measured to be:

$$P_{VV} = |\langle V_\alpha V_\beta | \psi^+ \rangle|^2 = \frac{1}{2} \cos^2(\beta - \alpha) \quad (13)$$

and likewise,

$$P_{HH} = |\langle H_\alpha H_\beta | \psi^+ \rangle|^2 = \frac{1}{2} \cos^2(\beta - \alpha) \quad (14)$$

$$P_{VH} = |\langle V_\alpha H_\beta | \psi^+ \rangle|^2 = \frac{1}{2} \sin^2(\beta - \alpha) \quad (15)$$

$$P_{HV} = |\langle H_\alpha V_\beta | \psi^+ \rangle|^2 = \frac{1}{2} \sin^2(\beta - \alpha) \quad (16)$$

Defining:

$$E(\alpha, \beta) = P_{HH} + P_{VV} - P_{VH} - P_{HV} \quad (17)$$

and

$$S = |E(a, b) - E(a, b')| + |E(a', b) - E(a', b')| \quad (18)$$

For certain angles of the polarizers, this parameter S can acquire values greater than 2. For instance, for $a = \frac{\pi}{4}$, $a' = 0$, $b = \frac{-\pi}{8}$, $b' = \frac{\pi}{8}$, the value of $S = 2\sqrt{2}$. Carefully performed measurements on any of the Bell states are in good agreement with the quantum mechanical predictions. This number can be easily shown to be ≤ 2 for any arbitrary local realistic theory [29]. This inequality is called the CHSH inequality. Thus, a value of S exceeding 2 is indicative of the presence of non-local correlations.

5. Loop-hole-free Bell tests

The actual measurement of quantum states to check for violation of CHSH inequalities involves the use of devices that involves losses and detectors that have an efficiency μ much less than 1. In such a case, the CHSH inequality is obtained by evaluating the expectation values conditional to coincident counts in both the detectors. This is necessary because of finite losses in the communication channels and μ being less than 1 [1].

$$S = |E(a, b)|_{\text{coin}} - E(a, b')|_{\text{coin}}| + |E(a', b)|_{\text{coin}} + E(a', b')|_{\text{coin}}| \leq \frac{4}{\mu} - 1 \quad (19)$$

Therefore, $S > 2$ if and only if $\mu > 0.828$ and hence, Bell's inequality violation would be seen only if the detector efficiency is better than this value. Superconducting nanowire single photon detectors are nowadays commercially available. When detectors of this efficiency are not available, substantial number of coincidences indicating the presence of entangled pairs of photons go undetected. Under these conditions, the sub-ensemble of coincidence detected are assumed to truly representative of the statistics of the entangled photon pairs emitted by the source. This assumption is called the fair sampling assumption. If this assumption holds, then $S \leq 2$ for all local-realistic theories. There is in fact yet another assumption that pertains to detectors which would result in false positive entangled pair detections. Because of experimental expediency, a coincidence event is defined as pairs detected within a coincidence pre-assigned time window. Even uncorrelated pairs of events could result in a seeming coincident event when one or the other

photon is delayed by a suitable time interval. Such an occurrence could result in the Bell's inequality violation for classical source.

In an actual quantum key distribution protocol, it is assumed that the choice of the measurement basis is made randomly and independently. The actual detection set-up looks like that indicated in the **Figure 4** below when either of the following measurement basis choices $\{H/V\}$ or $\{D/A\}$ is made for polarization entangled photon at the source. With such an arrangement, the non-polarizing 50:50 beam splitter sends the incoming photon to either of the polarizing beam splitters with equal probability and hence a random basis choice $\{V, H\}$ or $\{D, A\}$ is made. This choice is not pre-determined and is perfectly random in nature.

Other than the loopholes mentioned earlier, there are very many other possible loopholes that could vitiate experimental demonstration of Bell's inequality violation. For example, the memory loophole wherein it may be posited that somehow the experimental apparatus retains the details of the previous measurements, thereby rendering the conclusions questionable. Another significant loophole is called the locality loophole under a presumed superluminal communication between the two stations. There are many other possible loopholes and remedial measures that could be taken to close them. We shall desist from going into each of them. The interested reader may refer to [1] and some references contained therein. Suffice to say that is experimentally demanding to demonstrate that all the loopholes have been closed in a single experimental. However, closing one or more loophole but not all have been demonstrated in numerous experiments. There are a couple of experiments which claim to have succeeded in closing all the loopholes. The possibility of someone coming up with an ingenious loophole proposal, however improbable, cannot be ruled out (**Figure 4**).

The watertight loop-hole-free experimental demonstration of information security requires a throughgoing analysis of the complete experimental conditions as well as characterization of components used in the experimental apparatus for deviation from the idealized system and a careful characterization of their imperfection. Alternately, the experimental apparatus is accepted as being unreliable. In the latter case, one is left with the option of having rely on a careful statistical

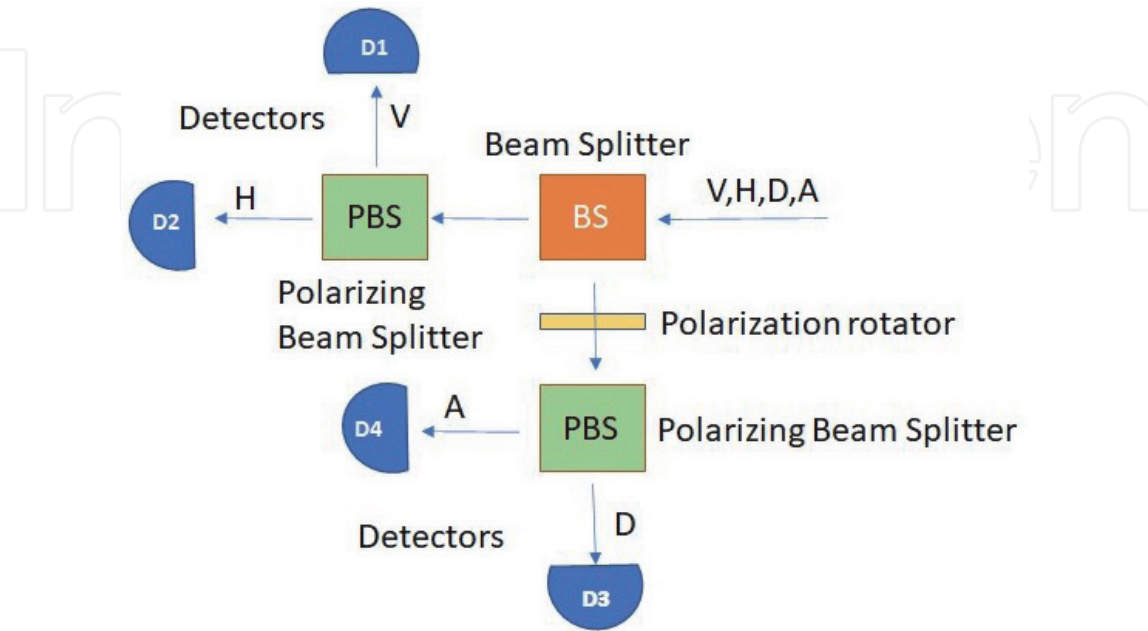


Figure 4.
The experimental arrangement for choosing randomly between two possible polarization choices for polarization is indicated.

analysis of observed nonlocal correlations of the data coupled with an experimental apparatus that comes close to being loophole free to the extent that is possible.

6. Device independence

Quantum Random generators and QKD system are devices that use many components that are imperfect, and their behavior deviates from the ideal systems assumed in theoretical models and as we had argued earlier, their complete characterization is well-nigh impossible because the physics of every single component that is used to build these systems needs to be modeled to perfection.

There exists however an alternate possibility, to obtain certified QRNGs and QKD devices which is inaccessible to classical tools. Surprisingly, in the absence of any superluminal communication, it is possible to use experimentally observed non-local correlation for this purpose. Such an approach does not require the modeling of the devices in question. What is more, the devices can be used as black boxes which have been supplied by a completely untrusted source. In the case of QRNG, the device needs to be intrinsically random, and the privacy of the random sequences needs to be guaranteed. In other words, the QRNG should be PPRNG. The use of non-local correlations certified through loophole-free Bell tests should drive us to physical limits of privacy of the random key generated by Alice and Bob. We shall treat QRNGs and QKDs separately and look at the overall outlook of device independent approaches.

6.1 Device independence QRNG (Di-QRNG)

The very definition of randomness is fraught with problems of philosophical nature. We had earlier alluded to differences between pseudo-random number generators (PRNGs) realized through algorithmic techniques, true random number generators (TRNGs) of epistemic origins and quantum random generators (QRNGs) which is believed to ontological in nature. The task at hand is to certify that the device at hand is a genuine QRNG. The output of such a device should be certifiably random not only to the user but every possible user. The density matrix describing N perfectly random output of 0 or 1 with equal probability is described by completely mixed density matrix given in the computational basis by $\hat{\rho} = \frac{1}{2}$. When this output is perfectly isolated from the environment is described by the product state:

$$\hat{\rho} \otimes \hat{\rho}_E \quad (20)$$

Where, $\hat{\rho}_E$ is the state of environment [2]. Since the nature of random sequences generated is of a physical origin, perfect and perfectly private randomness should be certifiable through quantum process. Therefore, nonlocal correlations witnessed by Bell's inequality violations could be employed to certify the QRNG. It stems from the fact that Bell tests on entangled sources generate perfectly random sequences under local measurements. The perfect randomness of local measurement outcomes attests to the fact that such measurements have been made on maximally entangled pure states. Maximally entangled states are subject to monogamy conditions [2] and hence cannot be entangled with environment. The correlations between measured outcomes are presented in terms of conditional probabilities as explained in the earlier sections. The catch however is that the demonstration of Bell's inequality violation should be loop-hole-free! The worst-case scenario for an unreliable QRNG is when the supplier of the device has packaged the device with pre-generated

random numbers. Such numbers would pass all tests of randomness but would hardly be private, since the supplier could have made copies of the same. The basic idea behind Quantum Mechanics certified randomness is that Bell's inequality violations can guarantee that the observed randomness is not pre-generated. Two conditions need to be fulfilled for demonstrating device independence and they are 1. The basis choice (a.k.a the measurement setting) in the two stations in Bell tests are independent of experimental devices and of any prior information of each of them as might be available and 2. The measurement outcomes of each station are independent of the measurement setting in the other station. The "Free-will" choice is an assumption that is ill-proven and anthropomorphic. In engineered system free-will is replaced by a source of intrinsic private randomness. This is rather curious because, the entire exercise that is undertaken for DI has to do with the certification of such sources. The second condition is however readily satisfied so long as the stations cannot communicate with each other (no signaling condition). This step could involve some public source of quantum random numbers. The initial seed could also be enlarged through the process of random number expansion see [random num exp] and references contained therein. The basic idea is that the numbers obtained through a Bell test are a source of certified randomness. It may be noted here that at least two devices are required to test for device independence.

In summary, DI-QRNGs [30, 31] use Bell inequality violations to certify the quantum state generated within the devices are pure entangled states. The purity of the quantum state ensures an absence of correlation not only between the devices at stations *A* and *B* but also with the environment and observers. Under a local measurement of the sub-system of a pure entangled state generates a completely mixed states resulting in perfect randomness of the output as certified by some entropic measure. Bell certified randomness is of a quantum nature as classical devices always do not violate Bell inequalities. Many DI-QRNG proposals as well experimental realization by various types are available in the literature. We will not attempt any systematic review of the literature. Quantum random number generators which rely on non-locality testified by Bell tests are also called self-testing QRNGs [17], the main problem with such devices is that they are presently too slow.

6.2 Device independence QKD (DI-QKD)

The one-time pad is a provably secure method of encryption [32]. The principle behind one-time pad is extremely simple: To encrypt a message bitstring of N bits called the plain text, a random bitstring of the same size called the key is generated. Then a modular addition of the key and plain text is carried out to create a bitstring called the ciphertext. The ciphertext is then communicated through a public channel to the recipient with whom the key is shared through a secure means. A modular addition of the ciphertext with key by the recipient, yields the plain text or message. Finding the means of sharing the key between the sender and the recipient of the message is called the key distribution problem. Traditionally, a trusted courier was given this job. This of course is not a viable option for encrypting terabits of data per second in the modern context.

A QKD system is device that acts a trusted courier of key between two parties. The security of such systems by the rules of quantum mechanics. The carriers of information are photons derived from a weak coherent source (attenuated laser pulses) or entangled photon sources. The quantum state of a single photon cannot be copied perfectly (No-cloning theorem) and a quantum state will be disturbed by the act of observation due to the Heisenberg Uncertainty principle. These quantum features of photons are exploited to ensure provable security of the key that is

exchanged between two parties. Typically, the sender prepares the photons by choosing randomly different bases for measurement and communicates each photon in one or the other eigenstates of the bases. The eigenstate is again chosen randomly. Usually, the sender uses a QRNG for this purpose. Likewise, the receiver chooses to measure the photon in one or the other basis. After exchanging a large number of photons, the basis choice made by both parties are compared and only those cases where the choice is the same, the corresponding measured outcomes are retained. Under ideal circumstances, this process would result in a privately shared keys that are identical. Practical Quantum Key distributions whether implemented on optical fibers or free-space are however inherently noisy because of photonic losses, and changes in the state during transmission. Such devices also use sources of single, heralded or entangled photons that are not perfect and detectors that usually have efficiencies below the requisite efficiency of $\sim 83\%$. These devices also use a variety of commercial components that are prone to side-channel attacks and are not the ideal ones used in a theory. Thus, the claim of provable security does not apply for practical systems. This makes QKD devices vulnerable to a variety of side-channel attacks. Thus, the raw keys obtained through the quantum channel have to be subjected to a series of post-processing steps for the generation of the final keys. Since most of side-channel attacks were on the detector side, measurement device independent QKDs were proposed and implemented. The final frontier of physical limits of privacy can be guaranteed only by device independent QKD systems. As in DI-QRNGs, DIQKD [33–35] also necessitate the performance of Bell tests between two distant parties. Bell tests typically use the Clauser-Horne-Shimony-Holt (CHSH) variant of Bell tests, which employs maximally entangled states. The rate of key generation, distance of transmission and security assurance levels are all inter-related in practical systems. Usually when low efficiency detectors are employed and significant line losses occur, fair sampling is implicitly assumed. In DI-QKD or measurement device independent MDI-QKD [36–38], the measuring device is with the quantum hacker Eve and fair-sampling arguments are no longer valid. Security of DI-QKD depends on the monogamy of shared correlations between maximally entangled photonic states. As in the case of DI-QRNG, device independence accrues through the conduct of loop-hole-free Bell tests. Mayers and Yao [33] proposed an early version of DI-QKD dealing with specific case of imperfect sources. In this pioneering work, they proposed that the security of a QKD protocol may be tested using entanglement-based protocols. Jonathan Barrett, Lucien Hardy, and Adrian Kent showed that single shared bit with guaranteed security can be exchanged though the use of Bell tests. Since these early results a variety of proposals and proofs of concept implementations have been published in the literature. As in the case of QRNGs, DI-QKD systems are extremely difficult to implement because, the ultimate guarantee of physically assured privacy relies on the performance of loop-hole free Bell tests.

7. Conclusions

In this chapter, we have attempted to provide a brief overview of device independent QRNGs and QKD systems that exploit Bell tests to guarantee privacy and randomness. In a reasonably complete manner, no attempt has however been made to review the field in a systematic and cogent fashion. The realization of device independence based on Bell's inequality violation was discussed. The central idea is to show that device independence of quantum devices is as hard to achieve as loop-hole-free Bell tests. The performance of such tests requires random generators that are provably secure. While there are large number of reports in the literature where

subsets of possible certain loopholes have been closed in certain experiments, there are but a couple of them that claim to have closed all loopholes.

Acknowledgements


I would like to thank Srimathi and Vakul for being there for me. I thank Dr. Srinivasan, DIAT, for his help with the figures. I thank DIAT for providing a very congenial academic environment and the support it provides. I wish to convey my sincere thanks and gratitude for the patience and diligence of Maja Bozicenic, Author Services Manager and the Editors.

Author details

Gopalan Raghavan
School of Quantum Technology, Defence Institute of Advanced Technology, Pune,
India

*Address all correspondence to: go.raghavan@gmail.com

IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Barrett, J., Hardy, L., and Kent, A. No-signalling and quantum key distribution. *Phys. Rev. Lett.* 95, 010503 (2005).
- [2] Masanes, L., Acin, and Gisin, N. General properties of nonsignaling theories. *Phys. Rev. A.* 73, 012112 (2006).
- [3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press.
- [4] Ekert, A. *Phys. Rev. Lett.* 67, 661-663, 1, 991 (2005).
- [5] Rarity, J., Owens, P., and Tapster, P. Quantum random-number generation and key sharing. *J. Mod. Opt.* 41, 2435–2444 (1994).
- [6] Liu, Y. et al. Device-independent quantum random-number generation. *Nature* 562, 548–551 (2018).
- [7] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang. Quantum random number generation, *npj Quantum Information* (2016) 2
- [8] The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness. Available at (<http://www.stat.fsu.edu/pub/diehard/>) (2008).
- [9] Rukhin, A. et al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (Special Publication 800–22 Revision 1, National Institute of Standards and Technology, 2008); available at (<http://csrc.nist.gov/publications/PubsSPs.html>).
- [10] Bell's inequality, N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, *Rev. Mod. Phys.* 86, 419 (2014)
- [11] Hensen, B. et al. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* 526, 682–686 (2015).
- [12] Shalm, L. K. et al. Strong loophole-free test of local realism*. *Phys. Rev. Lett.* 115, 250402 (2015).
- [13] Giustina, M. et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* 115, 250401 (2015).
- [14] Einstein, A., Podolsky, B. and Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* 48, 777-780 (1935)
- [15] N. Bohr. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* 48, 696 (1935)
- [16] Uchida, A. et al. Fast physical random bit generation with chaotic semiconductor lasers. *Nat. Photon.* 2, 728–732 (2008).
- [17] Lunghi, T. et al. Self-testing quantum random number generator. *Phys. Rev. Lett.* 114, 150501 (2015).
- [18] Cao, Z., Zhou, H. and Ma, X. Loss-tolerant measurement-device-independent quantum random number generation. *New J. Phys.* 17, 125011 (2015).
- [19] Liu, Y. et al. Device-independent quantum random-number generation. *Nature* 562, 548–551 (2018).
- [20] Marangon, D. G., Vallone, G. and Villoresi, P. Source-device-independent ultrafast quantum random number generation. *Phys. Rev. Lett.* 118, 060503 (2017).
- [21] Acín, A., Massar, S. and Pironio, S. Randomness versus nonlocality and

- entanglement. Phys. Rev. Lett. 108, 100402 (2012).
- [22] Avesani, M., Marangon, D. G., Vallone, G. and Villoresi, P. Source-device-independent heterodyne-based quantum random number generator at 17 gbps. Nat. Commun. 9, 5365 (2018).
- [23] J.S. Bell, Physics I, 195, 1965.
- [24] Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, Karol Horodecki. Quantum entanglement. Rev. Mod. Phys, 81, 865 (2009)
- [25] P. Kwiat; et al. (1995). New High-Intensity Source of Polarization-Entangled Photon Pairs. Phys. Rev. Lett. 75 (24): 4337–4341.
- [26] Popescu, S. and Rohrlich, D. Quantum nonlocality as an axiom. Found. Phys. 24(3) 379-385 (1994)
- [27] Antonio Acin and Luis Masanes. Certified Randomness in Quantum Physics. Nature 540, 213 (2016)
- [28] Benston Ingemar (2007). Three Ways to Look at Mutually Unbiased Bases. AIP Conference Proceedings. 889. pp. 40–51
- [29] Clauser, J. F., Horne, M. A., Shimony, A. and Holt, R. A. Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett. 23, 880–884 (1969).
- [30] Giustina, M. et al. Bell violation using entangled photons without the fair-sampling assumption. Nature 497, 227 (2013).
- [31] Pironio, S. et al., Random Numbers certified by Bell’s Theorem. Nature 464, 1021-1024 (2010).
- [32] Vernam, G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. J. Am. Inst. Electr. Eng. 45, 109–115 (1926).
- [33] Mayers, D. and Yao, A. Self-testing quantum apparatus. Quant. Inform. Comput. 4 273-286 (2004).
- [34] Acin, A., Gisin, N. and Masanes, L. From Bell’s Theorem to Secure Quantum Key Distribution. Phys. Rev. Lett. 97, 120405 (2006).
- [35] Masanes, L., Pironio, S. and Acin, A. Secure device-independent quantum key distribution with causally independent measurement devices. Nature Comm. 2, 238 (2011).
- [36] Liu, Y. et al. Experimental measurement-device-independent quantum key distribution. Phys. Rev. Lett. 111, 130502 (2013)
- [37] Tang, Z. et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Phys. Rev. Lett. 112, 190503 (2014).
- [38] Yin, H.-L. et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. 117, 190501 (2016).