EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Multi-bit quantum random number generator from path-entangled single photons

K. Muhammed Shafi[1], Prateek Chawla[2,3], Abhaya S. Hegde[1], R.S. Gayatri[1], A. Padhye[1] and C.M. Chandrashekar[1,2,3*]

*Correspondence: chandracm@iisc.ac.in
[1] Quantum Optics & Quantum Information, Department of Instrumentation and Applied Physics, Indian Institute of Science, Bengaluru 560012, India
[2] The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India
Full list of author information is available at the end of the article

Abstract

Measurement outcomes on quantum systems exhibit inherent randomness and are fundamentally nondeterministic. This has enabled quantum physics to set new standards for the generation of true randomness with significant applications in the fields of cryptography, statistical simulations, and modeling of the nondeterministic behavior in various other fields. In this work, we present a scheme for the generation of multi-bit random numbers using path-entangled single photons. For the experimental demonstration, we generate a path-entangled state using single photons from spontaneous parametric down-conversion (SPDC) and assign a multi-qubit state for them in path basis. One-bit and two-bit random numbers are then generated by measuring entangled states in the path basis. In addition to passing the NIST tests for randomness, we also demonstrate the certification of quantumness and self-certification of quantum random number generator (QRNG) using Clauser, Horne, Shimony and Holt (CHSH) inequality violation. We also record the significantly low autocorrelation coefficient from the raw bits generated and this along with CHSH violation rules out multi-photon events and ensure the protection from photon splitting attack. Distribution of photons along multiple paths resulting in multiple bits from one photon extends the limit on bit generation rate imposed by the detection dead time of the individual detector. Thus, the path-entangled states can generate higher bitrates compared to scheme using entangled photon pair which are limited by the coincidence counts. We demonstrate this by generating a high rate of about 80 Mbps when the single photon detector saturates at around 28 Mcps and still show violation of CHSH inequality.

1 Introduction

True random numbers are a valuable resource with applications in cryptography [1, 2] and cybersecurity, where security is assured by unpredictability [3–5]. Randomness in general is a very useful resource [6] in various science and engineering applications like statistical simulations [7, 8] and modeling of nondeterministic behavior across fields like artificial intelligence, neural networks, and genetic algorithms. There are many statistical tests which can certify the randomness of the observed sequence [9–12]. However, even if a sequence of random numbers passes all the statistical tests, it is almost impossible to discriminate between a predetermined random string of bits that comes from a dishonest provider or malicious random number generator (RNG) and a truly random sequence. Genuine randomness cannot be generated and unconditionally certified using purely classical methods. In other words, true randomness can only occur through physical processes involving inherent randomness. Till date, the only systems displaying processes with intrinsic randomness are those based on the principles of quantum physics [13]. Recent developments in controlling quantum systems and extracting intrinsic randomness from measurement outcomes have led to new standards in generation and certification of true randomness for use in practical applications [14, 15]. The use of nonlocal correlation between two particles has been shown to reduce the device dependence of quantum random number generators (QRNGs) [16–18]. Device-independent QRNGs can not only allow one to validate randomness, but also to certify that it is private randomness; the produced random numbers are ensured to be unknown to an adversary. Therefore, nonlocality of pure entangled states has been an invaluable resource for information processing tasks such as random number generation [19, 20], randomness expansion [21, 22], quantum key distribution [23–25] and privacy amplification protocols [26, 27].

Various approaches to build an efficient QRNG have been developed and evolved over the years as it remains a topic of active interest. For example, QRNG based on quantum shot noise limit [28], phase noise [29], quantum vacuum fluctuations [30–33], phase fluctuations [34], single photon emitters in gallium nitride [35], defect centers arising from nitrogen vacancies in diamond [36], hexagonal boron nitride single photon emitters [37] along with several other approaches have been reported [38–44]. Efforts have also gone into the generation of truly random bits from the entangled pairs of photons obtained from spontaneous parametric down-conversion (SPDC) processes [45–48] and from single-photon entanglement states [49, 50]. Each of these protocols involves sources that can be broadly classified into three categories, namely, trusted device, device-independent sources [51] and semi-device independent sources [14]. Although device-independent QRNGs based on nonlocality and entangled states are more secure compared to the sources from the other two categories, they are considered unsuitable for applications which require higher rates of generation of random numbers. The coincidence counts in the measurements of two entangled photons limits the bitrates of these sources. Any proposal in the direction of increasing the generation rate of random numbers based on violation of the Clauser, Horne, Shimony, and Holt (CHSH) inequality will thus increase the scope of device-independent QRNGs.

In this work, we present a scheme for the generation of multi-bit random numbers using path-entangled single photons. Using different configurations of path-entangled single photon states [52, 53], different distributions along the path can be engineered to extract random numbers. The violation of CHSH inequality ensures the intrinsic randomness in the scheme despite having control over the components in the device, thereby making it a device-independent and self-testing QRNG. For the experimental demonstration, we have used single photons from SPDC process resulting from a nonlinear periodically-poled potassium titanyl phosphate (PPKTP) crystal. We demonstrate the generation of one-bit and two-bit random numbers from each detected single photon in position basis by assigning two-qubit state to the position basis of the path-entangled photons. The raw bits generated as such are able to pass most of the 15 standard NIST tests used for certifying randomness. After a round of XOR or Toeplitz post-processing [54, 55], the generated bits are capable of passing all the randomness tests in the NIST suite [12]. We also demonstrate the certification of quantumness using CHSH inequality violation. Significantly low auto correlation coefficient of the order of $10^{-3} - 10^{-4}$ recorded from the raw bits rules out multi-photon events and protects QRNG from photon splitting attack. We also demonstrate the transition of from CHSH inequality violation and to validity with decrease in entanglement visibility and the same results in increase of autocorrelation coefficient. The path entanglement-based scheme demonstrated in this work presents major advantages over current implementations, including, but not limited to:

1. Each detected photon translates to a two-bit random number. Moreover, the approach presents scalability to generate a higher number of bits either by increasing the number of paths and/or by including other degrees of freedom such as polarization.
2. Compared to other two-particle entanglement-based schemes that use rarer coincidence counts, this scheme uses single photon detection events to generate random bits. Thus, the scheme benefits from the improvements in bitrates.
3. Due to path entanglement of states, photon detection events gets distributed among multiple detectors, allowing for a higher output bitrates as the limiting factor of detector dead time is effectively bypassed. We are able to achieve an output bitrate of about 45×10^6 bps (bits per second) and 80×10^6 bps with path entanglement certification of heralded and unheralded single photons, respectively. Such high rate is recorded despite each detector is being limited to a photon count of 28×10^6 cps (counts per second) on its own. It is possible to achieve bitrates of up to 100–130 Mbps by increasing pump power in our setup before the detectors begin to saturate and multi-photon detection dominates resulting in absence of CHSH violation.

This paper is organized as follows. In Sect. 2 we have outlined the theoretical description of the path-entangled photon state and the scheme for generating multi-bit random numbers, along with discussion on the visibility of path-entangled state and post-processing analysis. In Sect. 3 experimental setup to generate one-bit and two-bit random numbers is described. Experimental results, tests of QRNG and details of certification are presented in Sect. 3. We conclude and summarize our results in Sect. 4.

2 Multi-bit QRNG from path-entangled state

Measurements on quantum states of light with inherent randomness in various parameters is one of the most commonly employed methods to extract quantum randomness. Quantum states in an entangled basis have been used in device-independent schemes for QRNG. Various choices of apparatus exist for the generation of quantum states of light, however, the affordability of single-photon sources and the ready availability of detectors have made them a convenient choice for constructing QRNGs.

An elementary realization of a QRNG is based on excessively attenuated laser sources. Single photons generated via attenuation techniques is only an approximation to single photons and are thus affected by photon statistics of coherent states, along with single photons many two and multi-photons states will also occur. Single photon events are isolated by discarding all coincidence detection when they are passed through the beam splitter. Fidelity of single photons from attenuated source is limited due to significant level of post selection [56]. A mature and convenient method to enter the single photon regime is to employ SPDC of photons caused by a χ^2 non-linear crystal. By heralding one of the photons from the down converted pair, single photons are generated. The pair of photons resulting from the down-conversion can also be entangled in polarization degree of freedom with a careful post selection of the down converted photons pairs. Among various schemes for QRNG using single and entangled photons, device-independent schemes have been reported using entangled photon sources. However, a QRNG using entangled photon pairs relying on coincidence events suffers from low bit generation rates. Here we present a scheme using single path-entangled photons certified via CHSH inequality violation [52, 53] to convert every detected photon into a random multi-bit sequence.

A single photon state that is in superposition along m path can be written in the form,

$$|\Psi\rangle_P = \sum_{x=1}^{m} \alpha_x |x\rangle. \tag{1}$$

In path-entangled representation the state exists in a Hilbert space $\mathcal{H} = \bigotimes_{i=1}^{m} \mathcal{H}_{p_i}$, where $\mathcal{H}_{p_i}$ is the Hilbert space of the ith path. Each $\mathcal{H}_{p_i}$ will be spanned by $\{|0\rangle_{p_i}, |1\rangle_{p_i}\}$ representing the absence and presence of the photon in the path, respectively,

$$|\Psi\rangle_{PE} = \sum_{x=1}^{m} \alpha_x |x\rangle = \sum_{p_1,\ldots,p_m \in \{0,1\}} \alpha_{p_1,\ldots,p_m} |p_1 \cdot p_m\rangle\,. \tag{2}$$

The output state of the photon passing through a 50:50 beam splitter in path-entangled representation will be,

$$|\Psi\rangle_{PE} = \frac{1}{\sqrt{2}}\big[|0\rangle_{P_1}|1\rangle_{P_2} + i|1\rangle_{P_1}|0\rangle_{P_2}\big]. \tag{3}$$

The CHSH parameter calculated for the above state following the procedure given in [53] is $S = 2\sqrt{2}$. This path-entangled state which violates CHSH inequality can be further split into m level using array of beam splitters. By assigning a multi-bit state to each path, it can be rewritten as an entangled multi-qubit state. When $m = 2^n$, the multi-qubit representation will be,

$$|\Psi\rangle_{MQ} = \sum_{q_1,\ldots,q_n \in \{0,1\}} \alpha_{q_1,\ldots,q_n} |q_1 \cdot q_n\rangle\,. \tag{4}$$

The measurement on the preceding path-entangled state collapses the state to one of the m paths and returns a multi-bit value assigned to that path. With some redundancy, a n-qubit state can be used to represent m paths even when $m < 2^n$. Figure 1 illustrates the configuration of beam splitters in the path of a single photon to generate a two qubit state. One- and two-bit random numbers can be extracted from the measurement outcomes on this state with the detectors and bit assignment corresponding to the detector. The path-entangled state after passing through the first beam splitter will take the form given in Eq. (3). When the state is further passed through a beam splitter given by the operation,

$$B(\theta) = \begin{bmatrix} \cos(\theta) & i\sin(\theta) \\ i\sin(\theta) & \cos(\theta) \end{bmatrix} \tag{5}$$

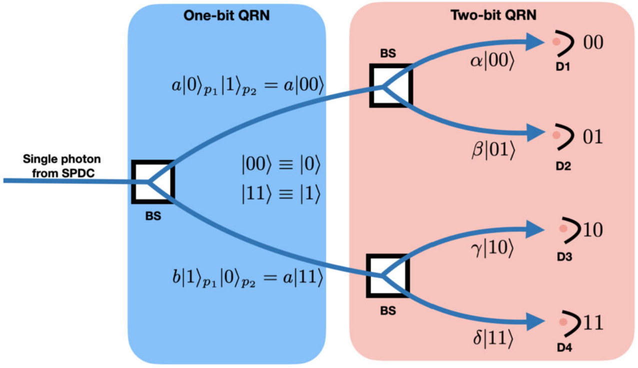

One-bit QRN
Two-bit QRN
Single photon from SPDC
BS
BS
BS
$a|0\rangle_{p_1}|1\rangle_{p_2} = a|00\rangle$
$|00\rangle \equiv |0\rangle$
$|11\rangle \equiv |1\rangle$
$b|1\rangle_{p_1}|0\rangle_{p_2} = a|11\rangle$
$\alpha|00\rangle$
$\beta|01\rangle$
$\gamma|10\rangle$
$\delta|11\rangle$
00
D1
01
D2
10
D3
11
D4

Figure 1 Schematic representation of a scheme to generate path-entangled single photon states mapped to a two-qubit state for each photon detection. A measurement operation after passing the beam through the first beam splitter will return one-bit random numbers, and after passing the second stage beam splitter pair, we can extract two-bit random numbers

along each path, the two-qubit state representation will be,

$$|\Psi_{2Q}\rangle = \frac{1}{\sqrt{2}}\big[\cos(\theta)|00\rangle + i\sin(\theta)|01\rangle + i\sin(\theta)|10\rangle + \cos(\theta)|11\rangle\big]. \tag{6}$$

Measurement will result in two-bit random number. If we consider polarization degree of freedom of photons in addition to path encoding we will obtain,

$$|\Psi\rangle_{P-PE} = \sum_{p_1,\ldots,p_m\in\{0,1\}} [\alpha_{p_1,p_2,\ldots,p_m} |H\rangle \otimes |p_1p_2 \cdot p_m\rangle + \beta_{p_1,p_2,\ldots,p_m} |V\rangle \otimes |p_1p_2 \cdot p_m\rangle], \tag{7}$$

where $\{|H\rangle, |V\rangle\}$ are the eigenbasis of the polarization Hilbert space, and α_k, β_k are chosen such that the state is normalized. This can be used to generate another random bit in addition to bits from the path-entangled states. One of the established practical ways to generate the above described photon-path entangled state with the multi-qubit mapping is via quantum walks [57]. Generation of multi-bit quantum random numbers using discrete-time quantum walk and increase in intrinsic randomness and entropy with increase in path degree of freedom has also been reported using a similar construct [58].

Therefore, assuming ideal photon generation and detection, the measurement output from the above scheme is guaranteed to be intrinsically random where quantumness is certified by the violation of CHSH inequality. The action of a depolarizing noise channel on path-entangled photons reduces entanglement visibility, as indicated by a corresponding decrease in value of the CHSH parameter S. Loss of quantumness is then characterized by $S \leq 2$. The visibility of path-entangled quantum state can also be controlled by changing the splitting ratio directly along the paths or by controlling the polarization degree of freedom using a combination of quarter wave plates and half wave plate along with polarizing beam splitter. Thus, by controlling the visibility, the effect of depolarizing noise on path-entangled photons can be mimicked. When $m = 2$, visibility can be obtained from the number of counts of photons detected on detectors D_1 and D_2,

$$\mathcal{P} = \frac{(C_{D_1} + C_{D_2}) - |C_{D_1} - C_{D_2}|}{(C_{D_1} + C_{D_2}) + |C_{D_1} - C_{D_2}|}. \tag{8}$$

It has been shown that achieving a value $S > 2$ corresponds to the setup wherein visibility $\mathcal{P}$ exceeds 0.7 [53]. This is a useful technique to generate and test the quality of random numbers generated for different visibility values as it determines the threshold to certify the quantumness of the devices.

2.1 Post-processing analysis

Theoretically, a QRNG should be able to produce truly random bitstrings in its output. However, in practical realizations, it is inevitable that some other classical signals (noise) will affect the output correlations. Optical fiber coupling and detector correlations are just two examples of many such possibilities. While noise cannot be controlled by the device designer, it remains a liability and can affect the randomness of the output. To illustrate the correlation of QRNG to effects that mimic noise, we may consider an example of imperfect detector D, which can detect a photon in the optical mode subspace spanned by $\{|D_\uparrow\rangle, |D_\downarrow\rangle\}$, denoting the presence of no photon or a single incoming photon respectively. Assume that the detection happens with the positive operator-valued measure (POVM) $\{K^\uparrow, K^\downarrow\}$, and that probability of detection is bounded by ϵ. Thus,

$$\begin{aligned} K^\downarrow &= \epsilon\, |D_\downarrow\rangle \langle D_\downarrow|, \\ K^\uparrow &= \mathbb{1} - K^\downarrow, \end{aligned} \tag{9}$$

where $\mathbb{1}$ is the identity operation in the optical mode subspace. To describe K as a POVM, we can consider the extension of K into an additional space of the subsystem S, which decides if the detector will detect this incoming photon. Thus the detector D is described by the subsystem K, which detects the incoming photon, and the subsystem S, which determines if the the incoming photon can be detected at all. In other words, the subsystem S controls the sensitivity of the detector, while the subsystem K performs the actual detection via a POVM. Let us assume that the Hilbert Space of system S is spanned by the basis $\{|S_\uparrow\rangle, |S_\downarrow\rangle\}$, denoting the case of no detection and successful detection, respectively. Then the outcome of the projective measurement $\{K^\uparrow, K^\downarrow\}$ applied to the joint system of the detector and an external system E with the following purification

$$\sigma_{DE} = \sqrt{1-\epsilon}\, |S_\uparrow\rangle \otimes |E_\uparrow\rangle + \sqrt{\epsilon}\, |S_\downarrow\rangle \otimes |E_\downarrow\rangle \tag{10}$$

will result in information about the sensitivity of the detector. Here, E is chosen to be a purifying system, i.e. the joint state of the QRNG setup and E is a pure state. For simplicity, we model our scheme assuming that the number of photons emitted by the source follows a Poisson-distribution. A photon detection event in a detector is assigned the bit 1 whereas no detection corresponds to bit 0. Assuming an imperfect detector in such a case reveals that with a higher number of photons emitted by the source, the guessing probability of the state 11 tends towards a higher quantity. This results in adversary having information about, say, the detection sensitivity of the subsystem, and thus being able to completely determine the output of the supposed QRNG. Thus, the elementary QRNG model in this regime will output a classical noise and not quantum randomness. In order to guarantee that the output will be free of such correlations, we need to implement post-processing procedures that remove these extraneous correlations and extract the randomness from the generated bit strings.

We use two kinds of post-processing – one using the XOR extractor [54], and another using the Toeplitz extractor [55]. The XOR extractor is implemented by the XOR operation on bits equidistant from each end of the sequence, and discarding the latter half of the sequence. This method, while useful for data that has a high amount of extractable randomness (min-entropy), begins to fail as the min-entropy decreases. The Toeplitz extractor is able to extract randomness from the output data, however, the losses become higher as the visibility reduces. This is evident from tests on random bit generated using states with reduced entanglement visibility, as detailed in Sect. 3.4.

3 Experiment

3.1 Setup

We used single photons generated from SPDC process to experimentally demonstrate a path-entangled multi-bit quantum random number generator. The schematic of the experimental setup is shown in Fig. 2. A 10-mm-long PPKTP nonlinear crystal (Raicol) with an aperture size of 1×2 mm^2 was pumped by a continuous-wave diode laser (Surelock, Coherent) at 405 nm. The crystal was type-II phase-matched with a poling period of Λ = 10 μm. The pump laser was spatial-mode-filtered by coupling to a single-mode optical fiber (SMF) and a half-wave plate (H_1) was used to set the pump polarization. A plano-convex lens (L_1) of 300 mm was used to focus the laser into the center of the crystal with a spot size of 85 μm. The variation in the wavelength of down-converted photons with temper-

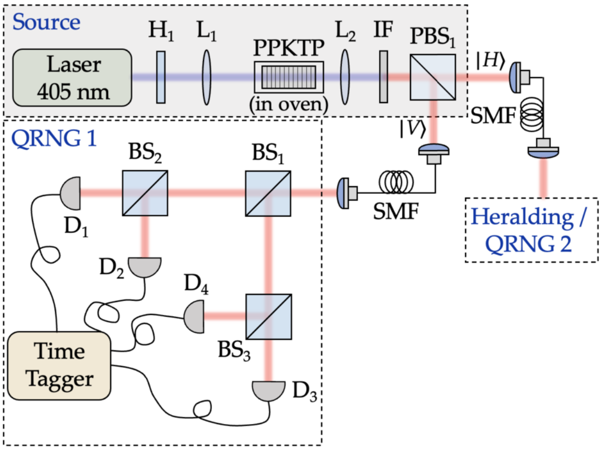


Figure 2 Schematic of the experimental setup. *Single photon source:* PPKTP nonlinear crystal enclosed in an oven is pumped by 405 nm laser. A half wave plate (H_1) is used to control pump polarization and lens (L_1 of 300 mm) is used to focus the laser beam into the center of the crystal. Lens (L_2 of 35 mm) is used collimate the down-converted photons. A bandpass interference filter (IF of 810 ± 10 nm) is used for filtering the pump. Polarization beam splitter (PBS_1) is used to separate generated orthogonally polarized photons. *QRNG unit*: $|V\rangle$ polarized single photons are coupled into single-mode optical fiber (SMF). Three non-polarizing 50:50 beam splitters (BS_1-BS_3) are used to generate two-bit random numbers. Four single photon counting modules (D_1-D_4) are used to detect single photons at the output of BS_2 and BS_3. The output of the SPCMs are fed to a time-correlated single photon counter (Time Tagger)

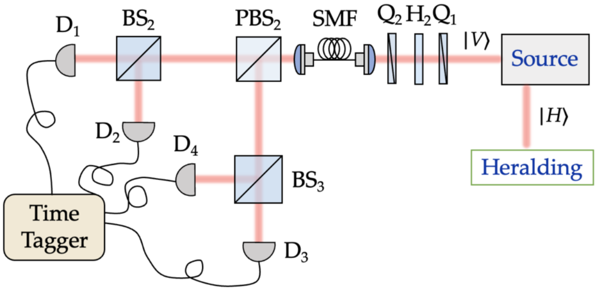


Figure 3 Schematic of the experimental setup to control the visibility of the path entangled state. The whole QRNG unit is identical to the main setup except for the use of PBS in place of BS$_1$ and the combination of Q-H-Q is used to control the input polarization of the source

ature was studied using a spectrometer and the temperature was maintained at 39°C for obtaining down-converted photons at 810 nm. The orthogonally polarized photon pairs ($|H\rangle$, $|V\rangle$) generated were collimated using a plano-convex lens (L$_2$) of 35 mm and separated using a polarization beam splitter (PBS$_1$). The $|V\rangle$ polarized single photons were coupled into a single-mode optical fiber (SMF) or multi-mode optical fiber (MMF) using appropriate collection optics. A bandpass interference filter (IF) at 810 nm center wavelength with a bandwidth of 10 nm FWHM was used for filtering the residual pump light. It should be noted that only $|V\rangle$ polarized single photons are used as a source to generate path-entangled photons. The $|H\rangle$ photon in our setup is used for heralding when heralded photons are used for QRNG and it is left unused when unheralded photons are used for QRNG. In such case, it can serve as a source for second independent path-entangled QRNG unit (QRNG 2). Maintaining fixed temperature or 810 nm of the down converted photons are not crucial for the experiment, a deviation of temperature by ±15°C for PP-KTP crystal did not alter much of our results.

For a two-bit QRNG unit from single photon source, a configuration of three non-polarizing 50:50 beam splitters (BS$_1$- BS$_3$) in the path of single photons was used as shown in the Fig. 2. Single photons at the output of the beam splitters BS$_2$ and BS$_3$ were coupled to multi-mode optical fibers (MMF) and detected using four single photon counting modules (SPCM-800-44-FC, Excelitas) with efficiencies of 65%, dead time of 22 ns and dark counts < 100 Hz. The output of the SPCMs were fed to a time-correlated single photon counter (Time Tagger, Swabian instruments), and the arrival times of the photons were recorded with a time resolution of 4 ps. The same setup was used to generate one-bit random numbers by detecting photons at the output of the beam splitter BS$_1$.

The effect of noise on path-entangled state can be mimicked by controlling the photon detection visibility in the path-entangled photons. A schematic of the experimental setup to control the visibility of path-entangled state is shown in Fig. 3. The polarization degree of freedom is used to control the photon's superposition in path. In the main QRNG unit, BS$_1$ is replaced by the PBS, and a combination of Q-H-Q (two quarter-wave plates and a half-wave plate) are used to control the input state that can resulting in asymmetry in photons superposition along the paths. By varying the angles in the wave plates, visibility of path-entangled state can be controlled.

3.2 Randomness tests on experimental data

After the experiment was set up as illustrated in the preceding section, data was acquired for a wide range of controllable parameters in the setup. The photons originating from the PPKTP crystal were passed through the first beam-splitter (BS_1) and the counts were recorded with time tagging along the paths from the second (BS_2) and third (BS_3) beam-splitters, which were then passed on for bit assignment and subsequent post-processing. As per the preset, bit assignment of 0 and 1 for each click on detectors D_1 and D_2 along the output of BS_1 (not shown explicitly in the schematic) were acquired to generate one-bit random numbers. Two-bit data was acquired with bit mapping of 00, 01, 10 and 11 for the clicks on the detectors D_1, D_2, D_3 and D_4 as shown in Fig. 2. A series of statistical tests were carried out on various rates of bit-generation for prolonged time duration's to ascertain randomness in the acquired data. Raw data of length averaging between 1 Mbits and 3 Mbits passed around 12–13 of the 15 tests in the NIST suite. Raw data passed all the 15 tests after the post-processing as discussed in Sect. 3.3. When the visibility of path-entangled state was reduced to 50% the raw data passed only around 5 tests and even after XOR post-processing the bits generated passed only about 11 tests. The same data subjected to either repeated post-processing or stringent rules for removing non-random data passed all the 15 tests even for data with low visibility at the cost of post-processing time and significant loss of bits.

Photon detection rates are limited by the detectors' detection dead time. In the proposed scheme, photons in path-entangled state and two-bit mapping for each detection can approximately generate bits at up to 8 times the maximum rate of photons each detector can resolve. To validate this advantage, we present the experimental data in Fig. 4, showing the number of unheralded single photon counts detected with increasing pump power using SPCM before sourcing it to QRNG unit, as well as the number of one- and two-bit generated after sourcing it to the QRNG unit using two and four SPCM, respectively. In Fig. 4(a), a plot of single photon count, one-bit and two-bit photon counts/sec with increase in power is shown when SMF was used to couple the source with the QRNG unit. Due to the high filtering of photons with SMF, the counts remained well within the detectors' saturation limit. Even after accounting for the loss of photons due to detector efficiency, the advantage of using path-entangled photons with two bit mapping with each path is seen by registering approximately 1.7 times the number of photons generated.

In Fig. 4(b) we present the same result when MMF is used to couple the source with the QRNG unit. Since MMF does not result in a huge loss of photons, we can see that the number of photons detected begins to show saturation when the pump power crosses 15 mW. This is an indication of arrival of multiple photons within the detector's dead time resulting in null contributions to the counts. When a photon is in path-entangled state, the load on the detectors gets shared among two detectors for one-bit generation and among four detectors for two-bit generation. Thus, the distribution of photons among four paths increases the effective photon resolution and saturation counts by as many as 8 times in the case of two-bit. It can be observed from the Fig. 4 that the usage of two detectors for generating one-bit sequences, the saturation of photon counts occurs at a higher pump power. Likewise, employing four detectors in order to produce two-bit sequences pushes the saturation point further. This enabled us to record about 80 Mbps when single photon detection saturation was seen around 28 Mcps. The bit rate of the setup was limited by the maximum power of the pump, and with a more powerful pump, this setup would

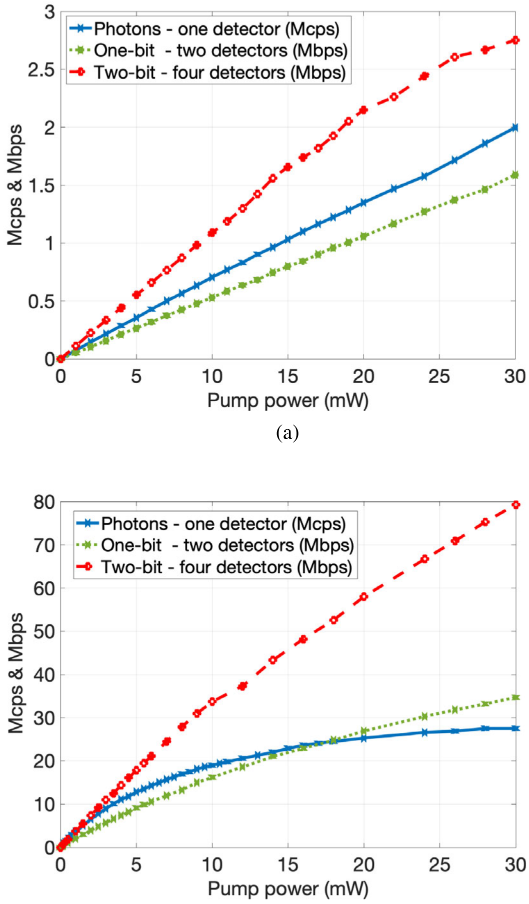


Figure 4 This plot illustrates the number of photons recorded per second in one SPCM (blue solid), two SPCMs (green dotted) and four SPCMs (red dash-dotted) with increasing pump power. The photons are collected by coupling (a) SMF and (b) MMF to the QRNG source. The raw data for one-bit generation is possible from photon counts obtained through two SPCMs and two-bit generation requires four SPCMs. Due to the path-entanglement and two-bit mapping, one can see nearly 1.7 times higher bits generation compared to the photons detected when SMF is used and when counts were well below the detector saturation point. When MMF is used at a high power in this setup, we eliminate the limitation imposed by the dead time of each detector which would have caused in a loss of number of photon detections. Distributing the detection events across multiple paths increases the effective saturation point by spreading the photon among all detectors. Thus, we could record around a total of 80 Mbps, while the single photon detectors have a saturation point close to 28 Mcps

be able to record around 150–200 Mbps before saturating the detectors. However, in the following section we will see the decrease in CHSH parameter with increase in the photon counts/sec due to increase in multi-photon detection. That will set the bit rate for which we can see violation of CHSH inequality.

The output at 80 Mbps from two bit mapping for each detected photon, which was generated using pump power of 30 mW, passed 12 of the NIST suite tests in raw form, and could pass all 15 tests after XOR post-processing. The visibility of the state was found to be close to 100%. However, one-bit raw data with the same power passed a lesser number of tests. We attribute this to saturation happening at the detector affecting the visibility of the quantum state.

3.3 Post-processing of experimental data

In the case where random numbers are used for cryptographic or security applications, the randomness of the output data from a RNG becomes an important property as it has strong correlations with the security of associated protocols. A good RNG has three properties – the output random numbers must be unpredictable, uniformly distributed, and uncorrelated. The latter two are proved by using statistical tests on the output of the RNG, which in our case are the tests in the NIST test suite for RNGs. In order to prove unpredictability, one must prove that in the absence of knowledge of the input, the maximum probability of an adversary correctly guessing the next output bit from the RNG must be 0.5.

For device independent QRNGs, an important parameter is the guessing probability p_g, which is the probability of the most probable outcome. This is related to the min-entropy of the system, defined as $H_{\min} = -2\log_2(p_g)$. The min-entropy can be used to quantify randomness in the system in the presence of noise [59]. The quantity, however, is not conditioned on the noise itself. We thus uniformly distribute the final randomness by the use of a randomness extractor function, to obtain a sequence of bits that is completely random. By the Leftover hash lemma with side information, a higher min-entropy corresponds to a higher extractable randomness independent of the system [60]. We thus use min-entropy to determine the number of extractable bits from a sequence of n bits (in this case, $n = 256$). In the one-bit QRNG setup, we are able to see from the results that the distribution is $\epsilon < 2^{-50}$ close to a uniform distribution. We are able to achieve an average data rate of 8.348 Mbps with a XOR extractor and 1.143 Mbps with a Toeplitz extractor (with multiprocessing). The data loss in the XOR extraction is 50.00%, and the data loss in the

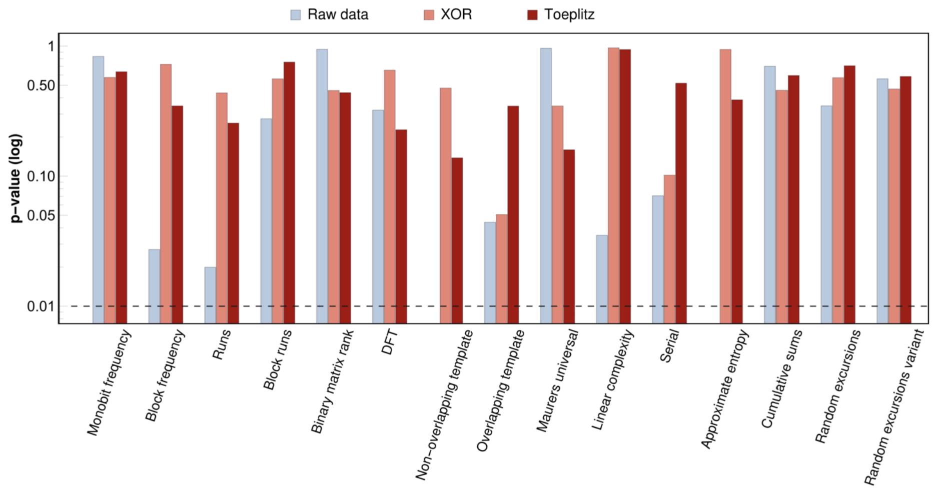


Figure 5 An overview of NIST randomness test results for the raw and post-processed two-bit sequences generated at a rate of 1 Mbps recorded from the arrangement as shown in Fig. 3. The raw data is of 3 Mbits long and passes 13 out of 15 tests. Toeplitz post-processing brings the bit length down by only 0.5% (post-processed bit length ∼ 2.985 Mbits) while passing all the tests. XOR post-processing also passes all statistical tests but results in a loss of 50% bits. The dashed line ($p = 0.01$) represents the critical p-value above which the sequence is considered random. These results indicate that no statistical patterns were found in the tested samples of random bits. The same analysis done on two-bit generated at 50% visibility in the experimental setup for noise revealed that raw data passes only 5 tests while XOR post-processed data passes 11 tests. Similarly, the raw data generated at 60% visibility passes only 4 tests, but is able to pass 12 tests after XOR post-processing

Toeplitz extraction is 7.71%. In case of the two-qubit setup, however, we observe that the XOR post-processing achieves an average bitrate of 42.97 Mbps, while Toeplitz extraction is able to achieve 6.42 Mbps. The higher bitrates may be attributed to efficient processing of larger file sizes generated by the system. The Toeplitz matrix used in the procedure may be constructed by using a private key as a seed. It is possible to use a pseudo-random number generator (PRNG) output for this purpose, however, to eliminate the possibility of the PRNG being compromised, we have set aside a 511-bit sequence to function as the key, and the first $255 + m$ bits of it are used as a private key (where m is the length of the output bitstring, and is determined by the min-entropy of the system). It may be noted that due to the Leftover Hash Lemma, it is possible to reuse the seed, and we need not re-generate the private key. An overview of the results obtained for NIST randomness tests may be seen in Fig. 5.

3.4 Certification of the device

3.4.1 CHSH inequality test for path-entanglement

CHSH parameter S for an entangled system can be calculated from combination of detection events obtained with different setting spanning over all basis states,

$$S = \left|E(\theta,\delta) - E\big(\theta,\delta'\big)\right| + \left|E\big(\theta',\delta\big) + E\big(\theta',\delta'\big)\right|. \tag{11}$$

Violation of CHSH inequality ($S \leq 2$) is observed when $S > 2$. For path-entangled state used for QRNG and described in Fig. 2, $E(\theta,\delta)$ can be calculated from P_{ij}, probabilities of different basis states of the system for parameters θ and δ,

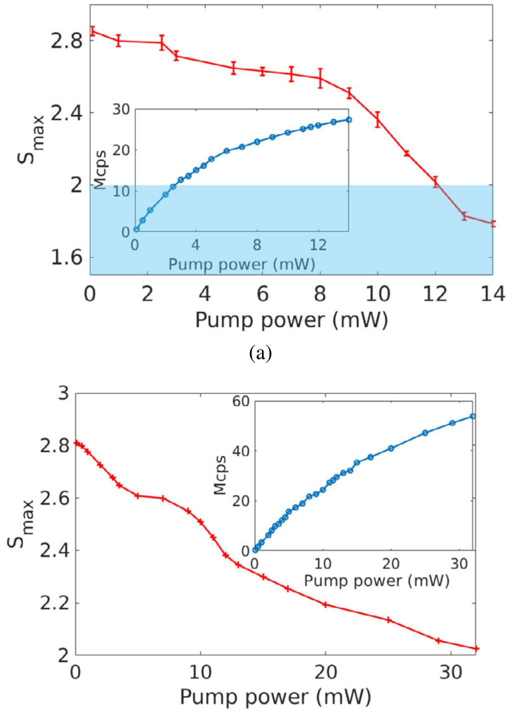
$$E(\theta,\delta) = P_{00}(\theta,\delta) + P_{11}(\theta,\delta) - P_{01}(\theta,\delta) - P_{10}(\theta,\delta). \tag{12}$$

Parameters θ and δ can be introduced by replacing standard beam splitter with a variable beam splitters in operational form,

$$B(\theta) = \begin{bmatrix} \cos(\theta) & i\sin(\theta) \\ i\sin(\theta) & \cos(\theta) \end{bmatrix}. \tag{13}$$

This procedure is identical to the scheme where two detector combination was used in repeated measurement setting to obtain values for all four basis states [53]. Variable beam splitter in place of BS_1 will introduce θ and identically rotated variable beam splitters in place of BS_2 and BS_3 will introduce δ. However, resetting θ to $\pi/4 + \theta$ on the first variable beam splitter and $\delta = \delta$ we will get the state $\frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$ when $\theta = \delta = 0$.

In Fig. 6(a) and (b) we show the maximum value of CHSH parameter obtained experimentally with increase in the pump power (photon counts) for heralded and unheralded single photon in path-entangled state, respectively. In Fig. 6(a) we note a decrease in CHSH parameter with increase in pump power. Initially the decrease is very small, the region where single photons are well separated in time and multi-photon events are very small. For higher pump power, multi photons detection in measurement window (detectors dead time) increases resulting in faster decrease in CHSH parameters and it goes below 2 for pump power corresponding to photon detection rate of ≈ 27 Mcps. This is also a saturation point of the single photon detector used for heralding. Since each detection cor-



(a)

(b)

Figure 6 Maximum value of CHSH parameter S_{max} for (a) heralded and (b) unheralded single photons in path-entangled state. The inset shows the photon counts recorded across 4 detectors for both the cases. With increase in pump power, S_{max} is seen to decrease due to increase in detection of multi-photons across the detectors in the set time window (detector dead time). Due to saturation imposed by the heralding detector, a lower rate of bit generation is observed when compared to the case of using unheralded single photons as the source. The S parameter ensures that the bit generation is limited to a rate that qualifies the entanglement certification

responds to two-bit of random numbers, we can generate a maximum of 54 Mbps of entanglement certified random numbers in our setup using heralded single photons in path-entangled state. When single photons are not heralded, we can bypass the detection limit of the heralding detector and generate more number of bits taking advantage of spread of photon detection along multiple paths. In Fig. 6(b) we show that photon detection rate of approximately 55 Mcps are recorded when we still get $CHSH > 2$. This corresponds to random number generation at the rate of 110 Mbps. The CHSH parameter ensures that even when all the four detectors have not reached saturation point when unheralded photons are used, however the CHSH parameter decreases for higher pump powers due to an increase in detection of multi-photons.

In Fig. 7 we show the theoretical expected value and experimental value for $S(\theta, 0)$ when $\theta' = 3\pi/8$ and $\delta' = \pi/4$. When $\theta = \pi/8$, that is when θ and δ are orthogonal to θ' and δ' we see maximum violation, $S = 2\sqrt{2} > 2$. For the above configuration $\delta = 0$ and $\delta' = \pi/4$ will be equivalent to absence of BS_2 and BS_1 and presence of BS_2 and BS_1, respectively. Parameter S calculated from experimental output (Expt 100%) is in close agreement with theoretical value. Purity of path entangled state can be reduced by reducing the entanglement visibility using waveplates as shown in Fig. 3. With decrease in entanglement visibility we see the decrease in the maximum value of S. Transition from violation of CHSH inequality

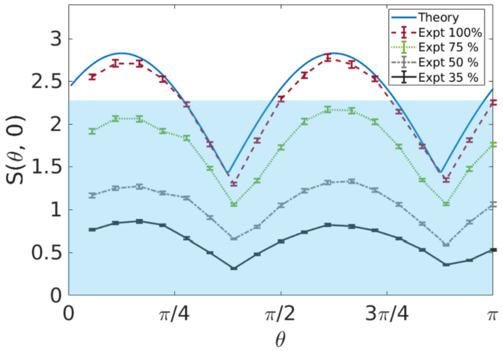


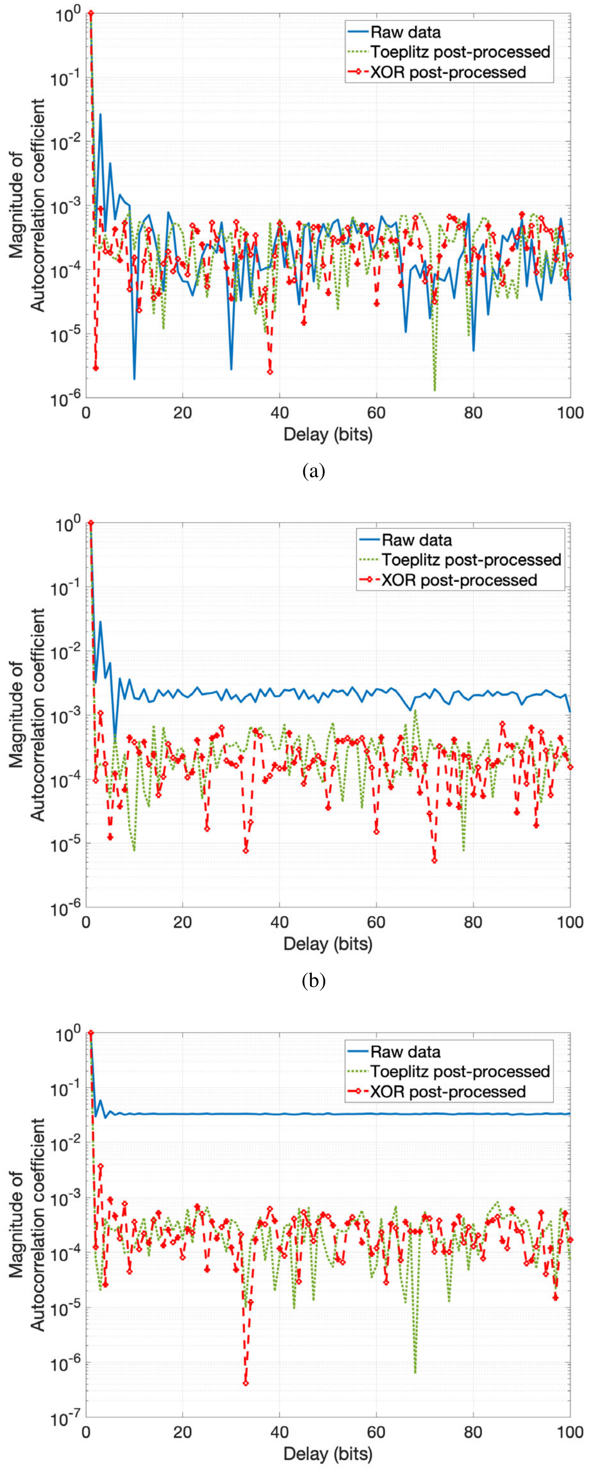
Figure 7 CHSH parameter S as a function of θ when $\delta = 0$, $\delta' = \pi/4$ and $\theta' = 3\pi/8$. Maximum violation of CHSH inequality is obtained when pairs θ, θ' and δ, δ' are orthogonal to each other. With decrease in entanglement visibility we see decrease in the maximum value of *S* and transition from violation of CHSH inequality to validation of CHSH inequality is seen around when visibility crosses 70%

to validation of inequality is seen when visibility decreases below 70%, in agreement with previous results [53]. Fidelity of single photon events in attenuated laser source is lower than this threshold to show CHSH violation. This effectively self-certifies the device for the production of random bitstrings based on measurement of a coherent entangled state. As a result, the CHSH parameter *S* serves as a reliable witness to the quantumness of the path-entangled QRNG setup. The threshold value of *S* can thus be used as a certification that the randomness of the output contains a significant contribution from the quantum measurement. A value of *S* greater than the classically expected maximum also provides a qualitative measure of entanglement, and therefore, purity of the state.

3.4.2 Autocorrelation test

Another metric to analyse the randomness of raw data is its autocorrelation. Figure 8 shows a plot of the magnitude of autocorrelation coefficients up to a delay of 100 bits for a subsequence formed from the first 10^7 bits of the output sequence. We find that beyond a delay of 100 bits, the mean and standard deviation of the autocorrelation coefficients do not change significantly. For a truly random sequence, the autocorrelation coefficients should have zero mean and a standard deviation of $1/\sqrt{N}$. For a 10^7-bit sequence, this value is about 3.162×10^{-4}. For raw device output, in the cases illustrated in Figs. 8(a)-8(c), the standard deviation is found to be 2.684×10^{-3}, 3.586×10^{-3}, and 3.340×10^{-2} respectively.

It can be clearly observed from Fig. 8(a)–8(b) that the autocorrelation in the raw output is prominently seen for a delay of 2 bits for the 90% visibility case, which is not present in the 100% visibility scenario. The case shown in 8(c) corresponds to a suboptimal operational regime where the QRNG is unable to self-certify, as indicated by the high autocorrelation in the raw output from the device. It can be observed from the figure that the QRNG when operating at high visibility (quantum regime) produces an output which is much closer to the extracted randomness than the output at lower visibility states (classical regime). QRNG output obtained at lower visibility is not able to pass all the NIST tests, even after XOR randomness extraction. Toeplitz extraction is still able to recover the randomness from this data, however, there are significant data loss at this point, and the QRNG functions sub-optimally.



(a)

(b)

(c)

Figure 8 Magnitude of autocorrelation coefficients corresponding to datasets generated at (a) 100%, (b) 90% and, (c) 50% visibility, respectively. Autocorrelation between bits is higher for data obtained from lower visibility setups indicating suboptimal performance

We have measured the autocorrelation between the bit commitment assigned to the detector output. If multiple detectors were triggered simultaneously due to muti-photon events, then multiple bit-commitments would be made together, and one would be able to detect region of high autocorrelation at longer delays. In our data, we do not see significant variation in autocorrelation beyond a delay of 100 bits under full visibility. Therefore results from the raw bits rules out multi-photon events and protects QRNG from photon splitting attack.

4 Conclusion

We have proposed a scheme for multi-bit QRNG from a controlled path-entangled single photon state. An experimental demonstration of one-bit and two-bit QRNG from proposed scheme has also been reported. In addition to being certified for quantumness via CHSH inequality violation, the raw data generated from various different settings in the system have been able to pass about 12 of the 15 NIST suite tests used to certify randomness. Using two different methods of post-processing, the generated random numbers are able to pass these statistical tests. We also show a reduction in the number of tests passing with a corresponding decrease in entanglement visibility in the path-entangled state. Unlike other entanglement-based QRNG schemes that rely on coincidence events, path-entangled demonstration relies on single photon detection events resulting in higher bitrates of true random number generation. Furthermore, since the photons are produced by the SPDC process, the system can self-certify even in the presence of a poisoned source, making it much less vulnerable to quantum non-demolition measurement-based attacks as well as photon-number splitting attacks. The generation of single photons using an SPDC process is experimentally tunable, and thus one can control the output bitrate up to the maximum power of the pump laser or up to the detectors' saturation limit. Therefore, it is plausible for one to engineer the scheme as per their requirements without compromising on the quantumness in the generated states of photons.

The use of path-entangled states distributes the photon among the detectors, which allows our setup to bypass the bitrate limitation imposed due to the dead time of the detectors to some extent. This contributes significantly towards the generation of higher bit rates. In our results, we show the limit of photon detection at ~ 28 Mcps in our detector is bypassed to generate ~ 80 Mbps in path-entangled state. It is also possible to extend this scheme by setting up two independent two-bit QRNG units along each path of SPDC photons, making it a highly resourceful way to develop two completely independent QRNG units from a single SPDC photon source. On-chip tunable photon sources can be generated using directional couplers and nonlinear waveguides [61], which lends our scheme a lot of flexibility in terms of implementation platforms and can be extended to any other form of single photon source. It also enables one to consider the possibility of future on-chip integration with dedicated hardware-based post-processing.

Acknowledgements
We acknowledge the support from the Office of Principal Scientific Advisor to Government of India, project no. Prn.SA/QSim/2020.

Availability of data and materials
Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Competing interests
The authors declare no competing interests.

Author contributions
CMC developed the scheme, obtained the numerical results and conceived the experiment. KMS, AP and RSG performed the experiments and collected the data. PC and ASH performed the theoretical analysis. PC, ASH and CMC wrote the manuscript. All authors reviewed the manuscript.

Author details
[1]Quantum Optics & Quantum Information, Department of Instrumentation and Applied Physics, Indian Institute of Science, Bengaluru 560012, India. [2]The Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai 600113, India. [3]Homi Bhabha National Institute, Training School Complex, Anushakti Nagar, Mumbai 400094, India.

Received: 2 May 2023 Accepted: 6 October 2023 Published online: 13 October 2023

References

1. Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J. 1949;28:656–715.
2. Blahut RE. Cryptography and secure communication. Cambridge: Cambridge University Press; 2014.
3. Ekert AK. Quantum cryptography based on Bell's theorem. Phys Rev Lett. 1991;67:661.
4. Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. J Cryptol. 1992;5:3–28.
5. Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. Rev Mod Phys. 2002;74:145.
6. Hayes B. Randomness as a resource. Am Sci. 2001;89:300–4.
7. Metropolis N, Ulam S. The Monte Carlo method. J Am Stat Assoc. 1949;44:335–41.
8. Rubinstein RY, Kroese DP. Simulation and the Monte Carlo method. New York: Wiley; 2016.
9. Maurer AM. A universal statistical test for random bit generators. J Cryptol. 1992;5:89.
10. Marsaglia G. Diehard: a battery of tests of randomness. 1996. http://stat.fsu.edu/pub/diehard/.
11. Kolmogorov N. On tables of random numbers. Theor Comput Sci. 1998;207:387–95.
12. Rukhin A, Soto J, Nechvatal J, Smid M, Barker E. A statistical test suite for random and pseudorandom number generators for cryptographic applications. NIST Special Publication **800**. 2001.
13. Schmidt H. Quantum mechanical random number generator. J Appl Phys. 1970;41:462.
14. Collantes MH, Escartin JCG. Quantum random number generators. Rev Mod Phys. 2017;89:015004.
15. Jacak MM, Jóźwiak P, Niemczuk J, Jacak JE. Quantum generators of random numbers. Sci Rep. 2021;11:16108.
16. Barrett J, Hardy L, Kent A. No signaling and quantum key distribution. Phys Rev Lett. 2005;95:010503.
17. Masanes L, Acin A, Gisin N. General properties of nonsignaling theories. Phys Rev A. 2006;73:012112.
18. Acín A, Masanes L. Certified randomness in quantum physics. Nature. 2016;540:213–9.
19. Pironio S, Acín A, Massar S, Boyer de la Giroday A, Matsukevich DN, Maunz P, Olmschenk S, Hayes D, Luo L, Manning TA, Monroe C. Random numbers certified by Bell's theorem. Nature. 2010;464:1021–4.
20. Ma X, Yuan X, Cao Z, Qi B, Zhang Z. Quantum random number generation. npj Quantum Inf. 2016;2:16021.
21. Colbeck R, Kent A. Private randomness expansion with untrusted devices. J Phys A, Math Theor. 2011;44:095305.
22. Coudron M, Yuen H. Infinite randomness expansion with a constant number of devices. In: Proceedings of the forty-sixth annual ACM symposium on theory of computing. 2014. p. 427–36.
23. Bennett CH, Wiesner SJ. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. Phys Rev Lett. 1992;69:2881.
24. Acín A, Gisin N, Masanes L. From Bell's theorem to secure quantum key distribution. Phys Rev Lett. 2006;97:120405.
25. Pironio S, Acín A, Brunner N, Gisin N, Massar S, Scarani V. Device-independent quantum key distribution secure against collective attacks. New J Phys. 2009;11:045021.
26. Colbeck R. Quantum and relativistic protocols for secure multi-party computation. 2009. arXiv:0911.3814.
27. Colbeck R, Renner R. Free randomness can be amplified. Nat Phys. 2012;8:450–3.
28. Symul T, Assada SM, Lamb PK. Real time demonstration of high bitrate quantum random number generation with coherent laser light. Appl Phys Lett. 2011;98:231103.
29. Qi B, Chi Y-M, Lo H-K, Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. Opt Lett. 2010;35:312–4.
30. Haylock B, Peace D, Lenzini F, Weedbrook C, Lobino M. Multiplexed quantum random number generation. Quantum. 2019;3:141.
31. Zheng Z, Zhang Y, Huang W, Yu S, Guo H. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation. Rev Sci Instrum. 2019;90:043105.
32. Dandasi A, Ozel H, Hasekioglu O, Durak K. Effect of photon statistics on vacuum fluctuations based QRNG. J Opt. 2021;23:065201.
33. Ferreira MJ, Silva NA, Pinto AN, Muga NJ. Characterization of a quantum random number generator based on vacuum fluctuations. Appl Sci. 2021;11(16):7413.
34. Xu F, Qi B, Ma X, Xu H, Zheng H, Lo H-K. Ultrafast quantum random number generation based on quantum phase fluctuations. Opt Express. 2012;20:12366–77.
35. Luo Q, Cheng Z, Fan J, Tan L, Song H, Deng G, Wang Y, Zhou Q. Quantum random number generator based on single-photon emitter in gallium nitride. Opt Lett. 2020;45:4224–7.
36. Chen X, Greiner JN, Wrachtrup J, Gerhardt I. Single photon randomness based on a defect center in diamond. Sci Rep. 2019;9:18474.
37. White SJU et al. Quantum random number generation using a hexagonal boron nitride single photon emitter. J Opt. 2021;23:1.
38. Dynesa JF, Yuanb ZL, Sharpe AW, Shields AJ. A high speed, post-processing free, quantum random number generator. Appl Phys Lett. 2008;93:031109.

39. Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A. A fast and compact quantum random number generator. Rev Sci Instrum. 2000;71:1675.
40. Wayne MA, Kwiat PG. Low-bias high-speed quantum random number generator via shaped optical pulses. Opt Express. 2010;18:9351–7.
41. Jacak JE, Jacak WA, Donderowicz WA, Jacak L. Quantum random number generators with entanglement for public randomness testing. Sci Rep. 2020;10:164.
42. Li Y-H, Han X, Cao Y, Yuan X, Li Z-P, Guan J-Y, Yin J, Zhang Q, Ma X, Peng C-Z, Pan J-W. Quantum random number generation with uncharacterized laser and sunlight. npj Quantum Inf. 2019;5:97.
43. Gehring T, Lupo C, Kordts A, Nikolic DS, Jain N, Rydberg T, Pedersen TB, Pirandola S, Andersen UL. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information. Nat Commun. 2021;12:605.
44. Lu Z, Liu J, Wang X, Wang P, Li Y, Peng K. Quantum random number generator with discarding-boundary-bin measurement and multi-interval sampling. Opt Express. 2021;29:12440–53.
45. Qiang MH, Mei WS, Da Z, Tao CJ, Ling JL, Xue HY, An WL. A random number generator based on quantum entangled photon pairs. Chin Phys Lett. 2004;21:1961.
46. Branning D, Bermudez M. Testing quantum randomness in single-photon polarization measurements with the NIST test suite. J Opt Soc Am B. 2010;27:1594–602.
47. Xu F, Shapiro JH, Wong FNC. Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring. Optica. 2016;3:1266–9.
48. Kwon O, Cho Y-W, Kim Y-H. Quantum random number generator using photon-number path entanglement. Appl Opt. 2009;48:1774–8.
49. Mazzucchi S, Leone N, Azzini S, Pavesi L, Moretti V. Entropy certification of a realistic quantum random-number generator based on single-particle entanglement. Phys Rev A. 2021;104:022416.
50. Leone N, Azzini S, Mazzucchi S, Moretti V, Pavesi L. Certified quantum random-number generator based on single-photon entanglement. Phys Rev Appl. 2022;17:034011.
51. Avesani M, Marangon DG, Vallone G, Villoresi P. Source-device-independent heterodyne-based quantum random number generator at 17 Gbps. Nat Commun. 2018;9:5365.
52. Pasini M, Leone N, Mazzucchi S, Moretti V, Pastorello D, Pavesi L. Bell-inequality violation by entangled single-photon states generated from a laser, an LED, or a halogen lamp. Phys Rev A. 2020;102:063708.
53. Shafi KM, Gayatri RS, Padhye A, Chandrashekar CM. Bell-inequality in path-entangled single photon and purity test. arXiv:2112.05039.
54. Levin LA. One way functions and pseudorandom generators. Combinatorica. 1987;7:357–63.
55. Krawczyk H. LFSR-based hashing and authentication. In: Advances in cryptology-CRYPTO'94. CRYPTO. vol. 839. 1994. p. 129–39.
56. Brown R, Twiss R. Correlation between photons in two coherent beams of light. Nature. 1956;177:27–9.
57. Alderete CH, Singh S, Nguyen NH, Zhu D, Balu R, Monroe C, Chandrashekar CM, Linke NM. Quantum walks and Dirac cellular automata on a programmable trapped-ion quantum computer. Nat Commun. 2020;11:3720.
58. Sarkar A, Chandrashekar CM. Multi-bit quantum random number generator from a single qubit quantum walk. Sci Rep. 2019;9:12323.
59. Ma X, Xu F, Xu H, Tan X, Qi B, Lo H-K. Postprocessing for quantum random-number generators: entropy evaluation and randomness extraction. Phys Rev A. 2013;87:062327.
60. Frauchiger D, Renner R, Troyer M. True randomness from realistic quantum devices. arXiv:1311.4547 [quant-ph].
61. Setzpfandt F, Solntsev AS, Titchener J, Wu CW, Xiong C, Schiek R, Pertsch T, Neshev DN, Sukhorukov AA. Tunable generation of entangled photons in a nonlinear directional coupler. Laser Photonics Rev. 2016;10:131–6.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.