Single-System-Based Generation of Certified Randomness Using Leggett-Garg Inequality

Pingal Pratyush Nath,[1] Debashis Saha,[2] Dipankar Home,[3] and Urbasi Sinha[4,5,*]
[1]Indian Institute of Science, C. V. Raman Road, Bengaluru, Karnataka 560012, India
[2]School of Physics, Indian Institute of Science Education and Research Thiruvananthapuram, Thiruvananthapuram, Kerala 695551, India
[3]Center for Astroparticle Physics and Space Science (CAPSS), Bose Institute, Kolkata 700 091, India
[4]Raman Research Institute, C. V. Raman Avenue, Sadashivanagar, Bengaluru, Karnataka 560080, India
[5]Department of Physics and Astronomy, University of Calgary, Alberta T2N 1N4, Canada

(Received 5 February 2024; accepted 4 June 2024; published 10 July 2024)

We theoretically formulate and experimentally demonstrate a secure scheme for semi-device-independent quantum random number generation by utilizing Leggett-Garg inequality violations, within a loophole-free photonic architecture. The quantification of the generated randomness is rigorously estimated by analytical as well as numerical approaches, both of which are in perfect agreement. We securely generate 919 118 truly unpredictable bits at a rate of 3865 bits/ sec. This opens up an unexplored avenue toward an empirically convenient class of reliable random number generators harnessing the quantumness of single systems.

DOI: 10.1103/PhysRevLett.133.020802

Introduction.—The production and characterization of true random numbers as a resource for various applications is currently a cutting-edge topic attracting considerable studies. In particular, the encryption schemes used in all protocols for secure communication, including quantum cryptography, rely on genuinely unpredictable random numbers. This is necessary to ensure that an adversary cannot decipher the encrypted message. Furthermore, the desired security must be guaranteed even in the presence of device imperfections or any tampering by an adversary. Strikingly, these key requirements for ensuring reliable private randomness are not currently satisfied by any random number generator (RNG).[1–4]

On the other hand, studies over the last decade have opened up an avenue for developing fully secure device-independent RNGs Table I based on using quantum entangled states and certifying genuine randomness by using quantum nonlocality evidenced through the statistical violation of Bell inequality [5–16]. But an empirical impediment in realizing practically viable such device-independent RNGs is the requirement of adequate spatial separation between two parties while making the Bell inequality testing measurements on their joint state by preserving their entanglement across distance [17]. To obviate this difficulty, we provide in this Letter a proof of concept demonstration of how the quantumness of an individual system, as evidenced through the observable violation of the temporal counterpart of Bell inequality [18–20], viz., the Leggett-Garg inequality (LGI), can be harnessed to certify and quantify genuine randomness.

Ever since LGI was formulated [21,22] as a consequence of the assumptions characterizing the notion of macrorealism, studies related to LGI have largely focused on using LGI for testing and probing ramifications of the quantum mechanical (QM) violation of macrorealism [23–37]. On the other hand, in the present work, we focus on a specific applicational feature of LGI. Apart from being derivable from macrorealism, LGI can also be derived from the conjunction of the assumptions of perfect predictability and no signaling in time (NSIT) [38], the latter condition meaning that measurement does not affect the outcome statistics of any later measurement, analogous to the way the Bell-CHSH (Clauser-Home-Shimony-Holt) inequality was earlier derived from predictability and no signaling across *spatial* separation [39]. This feature suggests that if an experiment is set up by choosing the relevant parameters such that the measurement outcomes obtained violate LGI and satisfy the NSIT condition, then these outcomes would be guaranteed to be inherently unpredictable. For quantifying such generated randomness, our treatment will be based on the specifics of the recent experimental test using single photons [40] that has demonstrated LGI violation by plugging all the relevant loopholes and rigorously satisfying the relevant NSIT conditions.

The assumptions invoked have been specified with respect to the setup used for the experimental study mentioned earlier, whose key relevant features have been discussed in detail in the Appendix. Thus, the randomness certified in this way is to be regarded as semi-device-independent, being dependent on the extent to which the assumptions invoked have been satisfied.

The scheme.—Consider a single time-evolving system with measurements at various instants of a dichotomic variable Q having eigenvalues $+1$ and -1. The

Leggett-Garg inequality can be written down as

$$\langle Q_1 Q_2\rangle + \langle Q_2 Q_3\rangle - \langle Q_1 Q_3\rangle \leq 1, \tag{1}$$

where $Q_i = Q(t_i)$ is the outcome of the measurement made at time t_i with the flow of time given by, $t_1 < t_2 < t_3$. The correlation functions are defined as

$$\langle Q_i Q_j\rangle = \sum_{a_i,a_j=\pm 1} a_i a_j P(a_i, a_j|Q_i, Q_j), \tag{2}$$

where $P(a_i, a_j|Q_i, Q_j)$ is the probability of getting the outcomes a_i and a_j at times Q_i and Q_j, respectively. The QM violation of this inequality (with the upper bound of 1.5) is attributed to the violation of the assumptions characterizing the notion of macrorealism from which LGI is usually derived [21,22]. However, interestingly, as mentioned earlier, LGI can also be derived from the conjunction of the following assumptions of predictability and no signaling in *time*. The assumption of predictability implies that for any given state preparation procedure, all the observable results of measurements at any instant can be uniquely predicted. In this context of a single time-evolving system we are considering, this assumption can be expressed as

$$P(a_i, a_j|Q_i, Q_j) \in \{0, 1\}. \tag{3}$$

The assumption that a measurement cannot affect the observable results of any later measurement is known as the no-signaling-in-time condition (also known as the no-disturbance condition) [41], which can be expressed as

$$P(a_j|Q_j) = \sum_{a_i} P(a_i, a_j|Q_i, Q_j). \tag{4}$$

Relevant to the three-time LGI given by Eq. (1), the NSIT conditions are as follows:

$$\begin{aligned} P(+|Q_2) &= P(++|Q_1, Q_2) + P(-+|Q_1, Q_2) \\ P(+|Q_3) &= P(++|Q_1, Q_3) + P(-+|Q_1, Q_3) \\ P(+|Q_3) &= P(++|Q_2, Q_3) + P(-+|Q_2, Q_3). \end{aligned} \tag{5}$$

From this derivation of LGI, it can be argued that in an experimental context where LGI is violated while ensuring the validity of NSIT, the LGI-violating observable outcomes are inherently unpredictable. For obtaining the guaranteed lower bound of the LGI-certified randomness in a semi-device-independent way, we make the following assumptions in the context of our specific experimental setup. First, note that the assumption that the selection of the measurement time is independent of the system's state, implicit in the derivation of LGI, is satisfied in our setup by ensuring considerable randomness in the choice of the blockers used in the different subsets of runs corresponding to different measurement times. Then the other assumptions invoked in our evaluation of the LGI-certified randomness bound with respect to our setup are listed below.

The dimension of the system is 2. This assumption clearly follows from our setup since the measurements are performed on the spatial degrees of freedom, and there are two paths in the optical setup. Therefore, the state of the photon or system is parametrized using the three parameters n_x, n_y, n_z and can be written down as

$$\rho = 1/2(I + \vec{n}\cdot\vec{\sigma}), \qquad \vec{n} = (n_x, n_y, n_z) \in \mathbb{R}^3 \tag{6}$$

such that $n_x^2 + n_y^2 + n_z^2 \leqslant 1$. The measurements at times t_1 and t_2 are the projective measurements defined up to unitary transformations,

$$P_+ = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad P_- = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{7}$$

This assumption is sensible here as blockers (pieces of metal) are used for the measurements at t_1, t_2. For the measurements at t_3 we invoke the general form of ± 1—outcome positive operator-valued measure (POVM) measurement,

$$M_\pm = \frac{1}{2}\left((1 \pm a)\mathbb{1} \pm \vec{b}\cdot\vec{\sigma}\right), \qquad \vec{b} \in \mathbb{R}^3, \qquad a \in \mathbb{R}, \tag{8}$$

where $|\vec{b}| \leqslant 1$ and $|\vec{b}| + |a| \leqslant 1$. The measurements at time t_3 are carried out by detectors, which are devices with complicated internal workings, unlike the blockers (which are in principle 100% efficient detectors as has also been characterized in [40]). Hence, we take the general form of the POVM measurement given by Eq. (8), which involves an implicit assumption that the blockers do not signal as the POVM at t_3 does not depend on the placement of the blockers. The initial state is not correlated with any other system thus excluding the possibility of the eavesdropper having any information about the initial state.

Bound on genuine randomness.—We quantify the randomness generated using the minimum entropy [14,42] of the probability distribution, which is defined as

$$\begin{aligned} H_\infty(AB|XY) &= -\log\{\max_{a_i,a_j} P(a_i, a_j|Q_i, Q_j)\} \\ &= -\min_{a_i,a_j} \log\{P(a_i, a_j|Q_i, Q_j)\}. \end{aligned} \tag{9}$$

We now relate the amount of randomness quantified using the minimum entropy to the observed LGI violation. This is done by finding a lower bound on minimum entropy as a function of the LGI violation. We obtain this bound on minimum entropy by solving the following optimization problem

$$\begin{aligned} P^* = &\max P(a_i, a_j|Q_i, Q_j) \\ &\textbf{subject to} \\ &\langle Q_1 Q_2\rangle + \langle Q_2 Q_3\rangle - \langle Q_1 Q_3\rangle = 1 + \alpha \\ &P(+|Q_2) = P(++|Q_1, Q_2) + P(-+|Q_1, Q_2) \\ &P(+|Q_3) = P(++|Q_1, Q_3) + P(-+|Q_1, Q_3) \\ &P(+|Q_3) = P(++|Q_2, Q_3) + P(-+|Q_2, Q_3), \end{aligned} \tag{10}$$

where $\alpha \in (0, 0.5]$. Now the minimal value of the minimum entropy, which is compatible with the LGI violation I, is given by

$$H_\infty(AB|XY) = -\log_2 P^*, \tag{11}$$

where P^* is the solution to the above optimization problem. We derive a bound on minimum entropy as stated in the theorem that follows.

Theorem 1.—Subject to the conditions stated earlier being satisfied, if the three NSIT (5) values are zero and the LGI (1) value is $1 + \alpha$ where $\alpha \in (0, 0.5]$, then

$$P^* = \frac{1}{4}(1 + \alpha + \sqrt{1 - 2\alpha}). \tag{12}$$

Therefore, the guaranteed random bits concerning the amount of violation is given by

$$-\log_2\left(\frac{1 + \alpha + \sqrt{1 - 2\alpha}}{4}\right). \tag{13}$$

We briefly outline the proof here, with detailed calculation of the analytical proof of Theorem 1 and Theorem 2 being presented in the Supplemental Material (SM) [43]. We use the expressions for the joint probabilities in terms of the parameters defining the unknown state, unitaries, and the measurement at t_3 to obtain the expressions for the LGI and NSITs. By suitably utilizing the fact that the NSIT expressions are zero, we establish some relations between the parameters that simplify the LGI expression. The problem then simplifies to maximizing the joint probabilities, under the only constraint that the simplified LGI expression is $(1 + \alpha)$. We observe that three distinct expressions within the simplified LGI expression are crucial in determining the joint probabilities for the three pairs of measurements. Employing the Lagrange multiplier method, some functional analysis, and intricate mathematical calculations, we identify the maximum values of these three expressions while satisfying the constraint that the simplified LGI value is $(1 + \alpha)$. Consequently, these maximum values help us to compute the upper bounds for all 12 joint probabilities from which we obtain an upper bound on P^* Fig. 1. Finally, we present a quantum strategy involving a specific quantum state, unitaries, and measurements that attain this upper bound.

Security against state preparation.—To ensure security against an adversary, say Eve, accessing initial state information, we adapt our scheme. Firstly, if the user's initial state is entangled with Eve's qubit in a Bell state, Eve can predict the user's measurement outcome by performing her own measurement, compromising security. In this case, the key point is whether we can still ensure an appreciable amount of guaranteed random bits. Secondly, another possible scenario is when the initial state is a mixture of different pure quantum states fed randomly into each experimental run. Here, the worst-case scenario from a

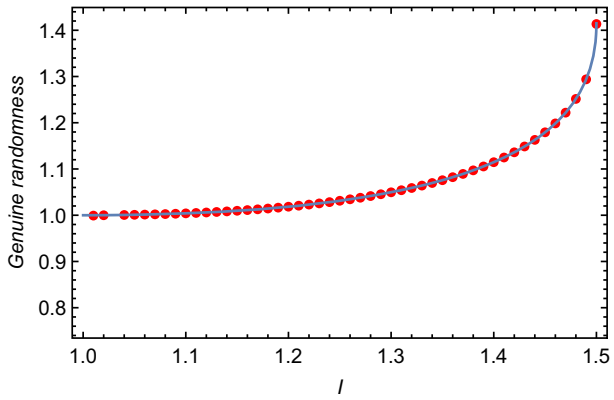

FIG. 1. Bound on the genuine randomness (minimum entropy) for the three-time Leggett-Garg setup. This treatment includes the assumption that the system's initial state is not correlated with any other system, thus generating randomness from the joint probabilities $P(a_i, a_j|Q_i, Q_j)$. The blue line is the analytical bound (12) on the minimum entropy, and the red dots are the numerical data from solving the optimization problem. The amount of randomness for the maximal LGI violation is 1.41.

security viewpoint is when Eve can predict the initially prepared state with maximum success. Even in such a scenario where Eve can maximally guess the outcome of the user's first measurement, we need to ensure that the choice of relevant parameters violates the Leggett-Garg inequality while satisfying all the relevant NSIT conditions, thereby enabling the generation of certified random bits. To achieve the desired security against adversarial attacks, we employ postprocessing by quantifying randomness based on user's second measurement outcomes conditioned on first, evaluating guaranteed randomness amount using maximized conditional probability of joint outcome instead of earlier joint probabilities, i.e., evaluating the maximized conditional probability given by $\bar{P}^*$,

$$\bar{P}^* = \max_{\{a_i, a_j, Q_i, Q_j\}} P(a_j|a_i, Q_i, Q_j) \quad \textbf{subject to constraints in Eq. (10)}, \tag{14}$$

where the mathematical constraints given by Eq. (10) correspond to violating LGI and satisfying the three relevant NSIT conditions, and the conditional probability is given by

$$P(a_j|a_i, Q_i, Q_j) = \frac{P(a_i, a_j|Q_i, Q_j)}{P(a_i|Q_i)}. \tag{15}$$

This procedure is based on considering that, for example, in the extreme case of a maximally entangled state shared between Eve and the user, Eve will be able to guess with certainty the outcome of the first σ_z measurement by the user using the outcome of her own σ_z measurement, which is obviated by the use of conditional probabilities. This is possible only when the first measurement is a perfect σ_z

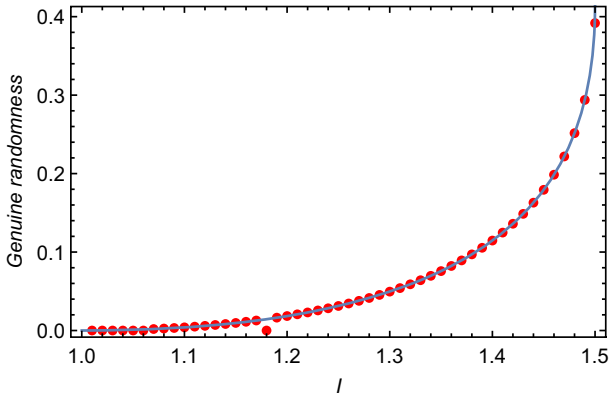

FIG. 2. Bound on the genuine randomness (minimum entropy) for the three-time Leggett-Garg setup with full security against state preparation procedure. This is done by solving the optimization problem using the conditional probabilities. The blue line is the analytical bound (16) on the minimum entropy, and the red dots are the numerical data from solving the optimization problem. The amount of randomness for the maximal LGI violation is 0.41, which is, as expected, less than the 1.41 that was earlier obtained assuming secure state preparation. In both these cases, genuine randomness increases monotonically as the LGI violation increases.

measurement, which is ensured by the 100% efficiency of our blockers. The next key question is whether the amount of certified randomness generated by this conditional probability based scheme will be still appreciable, although maybe less than that obtained by the procedure based on joint probabilities discussed earlier. It is this question that is addressed by the following Theorem 2.

Theorem 2.—Subject to the conditions stated earlier being satisfied, if the three NSIT (5) values are zero and the LGI (1) value is $1+\alpha$ where $\alpha \in (0, 0.5]$, then

$$\bar{P}^* = \frac{1}{2}(1+\alpha+\sqrt{1-2\alpha}). \tag{16}$$

Therefore, the amount of guaranteed random bits as a function of α is given by

$$f(\alpha) = -\log_2\left(\frac{1+\alpha+\sqrt{1-2\alpha}}{2}\right). \tag{17}$$

The proof is essentially an extension of the proof for Theorem 1, and the relevant details are given in Sec. IB of SM. Comparing Eqs. (16) and (12), it follows that $\overline{P^*} = 2P^*$ and from Eq. (17) it follows that the randomness with respect to the maximum LGI violation (i.e., $\alpha = 1/2$) is 0.415 as compared to 1.41 in the earlier case Fig. 2. Thus an appreciable amount of certified randomness is ensured to be secure against state preparation.

This bound is sensitive to the NSIT constraint as shown in the SM, where we solve the optimization problem with a small NSIT violation. A higher threshold value of LGI violation is necessary for meaningful randomness generation as NSIT violation becomes more pronounced. Nonetheless, even with a relatively high NSIT violation, a meaningful quantity of random bits can still be obtained as the LGI violation approaches its maximum value.

Memory effect and experimental results.—To estimate the violation of the LGI, it is necessary to generate data from the device multiple times. However, the device may exhibit variations in performance across different uses, one of the cases being the memory effect, where the output of a particular iteration might depend on the outcome of the previous outputs, hence making it necessary to use a statistical method to account for such memory effects. We have shown in Sec. II of the SM [43] how to determine the randomness produced by the devices without making any assumptions about their internal behavior by combining the previously derived bound with a statistical approach.

Because of the memory effect the exact value can be lower than the observed value $\hat{I}$ up to some ϵ, with some small probability δ,

$$\delta = \exp\left(-\frac{n\epsilon^2}{2(1/q+I_q)^2}\right), \tag{18}$$

where I_q is the maximum inequality violation allowed by quantum theory, $q = \min\{p(t_1,t_2), p(t_1,t_3), p(t_2,t_3)\}$ and ϵ is fixed by the maximum LGI violation I_q, the probability of the inputs q and the number of runs n, as has been defined in Sec. II of SM. So the minimum entropy bound of the n bit string generated is

$$H_\infty(R|S) \geq nf(\hat{I}-\epsilon) \tag{19}$$

with probability at least $1-\delta$. With a confidence level of $1-\delta = .99$ and the experimentally observed LGI violation $I = 1.31$, we have plotted the minimum entropy bound for n runs. In Fig. 3, we show that we start getting a substantial amount of randomness only after a certain number of runs due to the presence of the memory effect. Using $n = 10^5$ runs yields a genuine randomness of 3673 bits, corresponding to 0.03673/bit in the presence of the memory effect. This is lower than expected from the genuine randomness bound derived above, for which we expect a genuine randomness of 0.05406/bit for an LGI violation of $I = 1.31$. Moreover, using biased measurement settings increases the threshold for getting an appreciable amount of randomness, as shown in Fig. 3.

A series of eight experiments were conducted to evaluate various coincidence measurements. Each experiment was repeated multiple times, and the coincidence counts were recorded for 10 s in separate runs. A total of 1000 coincidence datasets were collected for each experiment to estimate the LGI violation Table II. The estimated LGI violation from the experiment is $I = 1.32 \pm 0.04$. Considering experimental nonidealities, the corresponding QM prediction is $I_{\mathrm{QM}} = 1.34 \pm 0.06$. In addition, another experiment was employed

TABLE I. Comparison of generation rate, type of experiment (proof of concept, loophole-free, and randomness expansion), and the spatial separation of Bell inequality (BI) based randomness generation experiments with our case of LGI-based randomness generation experiment. Unlike the BI-based experiments, which require spatial separation or some sort of shielding to ensure no signaling, this spatial separation is irrelevant in our case since we can design our experimental setup in a tabletop experiment to ensure NSIT. BI-based experiments evolved from proof of concept to loophole-free experiments, enhancing generation rates and expansion. Our LGI-based demonstration, a loophole-free proof of concept experiment, provides the base with an appreciable generation rate. Further improvements and work on expansion schemes for our protocol will boost LGI-based state-of-the-art random number generation.

Performed experiments	No. of Bits	Rate (bits/ sec)	Type	Spatial Sep (m)
Pironio *et al.* [14]	42	Not mentioned	Proof of concept, not loophole-free, uses shielding	1
P. Bierhorst *et al.* [8]	1024	Not mentioned	Loophole-free, randomness generation	187
Liu *et al.* [13]	6.2469×10^7	181	Randomness generation	200
Shen *et al.* [58]	617 920	240	Randomness extraction, assumed no signaling	Not mentioned
Zhang *et al.* [59]	512	1.71	Loophole-free	194.8
Ming Hang Li *et al.* [60]	5.47×10^8	11 598	Randomness expansion	191
Wen Zhao Liu *et al.* [61]	$2.57 * 10^7$	13,527	Loophole-free, randomness expansion, uses shielding	Not mentioned
LK Shalm *et al.* [16]	118 126 423	3606	Randomness expansion	194.8
Our current work	**919 118**	**3865**	*Loophole-free proof of concept Randomness generation*	Irrelevant

to estimate the single probabilities at times t_2 and t_3 to verify the NSIT conditions. The experimentally measured values for the three NSIT conditions denoted by v_1, v_2, and v_3 were found to be 0.002 ± 0.017, 0.002 ± 0.016, and 0.004 ± 0.016, respectively. The QM predictions for these probabilities are $v_1^{\mathrm{QM}} = 0$, $v_2^{\mathrm{QM}} = 0$, and $v_3^{\mathrm{QM}} = 0 \pm 0.0261$. These results certify the randomness of the outputs generated by providing insights into the violations of the LGI and the adherence to the NSIT conditions based on experimental measurements. The average generation rate is 3865 bits/ sec, and the total number of bits generated is 919 118, as shown in the Appendix.

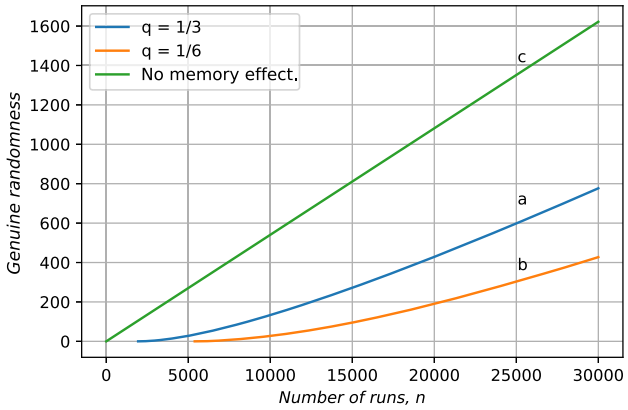

FIG. 3. In the secure state preparation procedure, we investigate the relationship between genuine randomness and the number of runs in the presence of memory effect. Assuming a violation of the Leggett-Garg inequality with a value of 1.31, which was observed in our experiment, with a confidence interval of $1 - \delta = 0.99$, we see that a notable amount of genuine randomness emerges only after approximately 3000 runs (curve (a) due to the memory effect, compared to the case without memory effect (curve c). For 10^5 runs, the measured genuine randomness reaches 3673 with an unbiased seed with probabilities $p(t_1, t_2) = p(t_2, t_3) = p(t_3, t_1) = 1/3$. Additionally, we investigate the relationship between genuine randomness and the number of runs when using a biased seed, where the measurement settings are chosen with unequal probabilities, $p(t_1, t_2) = 1/6$ and $p(t_2, t_3) = p(t_3, t_1) = 5/12$. While in the unbiased case, nonvanishing randomness starts appearing after 3000 runs, this threshold increases to around 6000 runs in the biased case (curve b). For 10^5 runs in the biased case, the measured genuine randomness reaches 2777, lower than the unbiased case, as expected.

Conclusion and outlook.—Our single-system-based RNG scheme's operational advantage over the Bell inequality based RNGs is that there is no requirement to produce and preserve entanglement across distant systems while measuring randomness-certifying correlations between their observed properties. Fundamentally, there is a key difference in how randomness is certified: entanglement schemes violate Bell inequalities invoking no signaling across spacelike separation, while our scheme certifies randomness through LGI violation invoking no signaling in time, which may not hold in any given experimental configuration. Crucially, our scheme uses setups that satisfy NSIT while violating LGI empirically.

Our treatment provides a fully analytical evaluation of how the lower bound on guaranteed randomness varies monotonically with the LGI violation amount, in complete agreement with corresponding numerical results. While this randomness quantification has operational significance, it can also stimulate a line of studies analogous to the way the nuances of the quantitative relationship between Bell inequality violating randomness and nonlocality have been probed in recent years.

Ensuring security against adversary tampering with state preparation in this scheme is distinct from Bell-based schemes. The most general attack in this scenario is when the user's initial state is entangled with the adversary's state. To consider the possibility of such an attack, we evaluate guaranteed random bits against the maximized

conditional probability of obtaining joint outcomes satisfying no-signaling-in-time conditions and violating LGI. This randomness quantification security strategy is unique to LGI-based schemes and could guide security analysis for other single-system quantum randomness generation variants.

In addition to randomness generation through Bell tests, several interesting semi-device-independent and source-independent schemes have been implemented in diverse experimental setups [47–53]. Additionally, some schemes have been theoretically suggested within sequential measurement setups [54,55], distinct from our approach. It would be valuable to thoroughly examine and compare the security of these approaches against the potential loopholes. In contrast to the source-independent setup we do not make any assumptions about the detectors, which is the main measurement part. Detectors are usually intricate devices with complex internal mechanisms, and thus vulnerable to eavesdropping.

It is worth mentioning that selecting smaller measurement time intervals without affecting setup stability can be achieved by automating blocker-position switching using a pseudorandom number generator [16]. A thorough examination of randomness expansion in relation to seed randomness could be a potential avenue for future research.

Interestingly, for counteracting the possible memory effect in the experimental device, our treatment yields results similar to that for the entanglement-based random generation scheme, requiring a significant number of runs to generate a substantial amount of certified randomness. A more rigorous estimation of the amount of randomness taking into account the possible side information available to the adversary and the relevant generation rate by employing randomness extraction and amplification will be presented in future work, along with studies investigating the possibility of other variants of this scheme in terms of experimental setups showing the violation of LGI using different systems.

U.S. acknowledges partial support provided by the Ministry of Electronics and Information Technology (MeitY), Government of India under a grant for Centre for Excellence in Quantum Technologies with Ref. No. 4 (7)/2020-ITEA as well as partial support from the QuEST-DST Project Q-97 of the Government of India. D. S. acknowledges partial support from STARS (STARS/STARS-2/2023-0809), Govt. of India, NASI Senior Scientist Fellowship and Bose Institute. We also thank Aninda Sinha for useful discussions.

Appendix.—We provide thorough details of our experimental setup for LGI violation, addressing all loopholes and meeting NSIT requirements to ensure suitability for randomness generation. Additionally, we outline the process of generating random bits from this experimental setup.

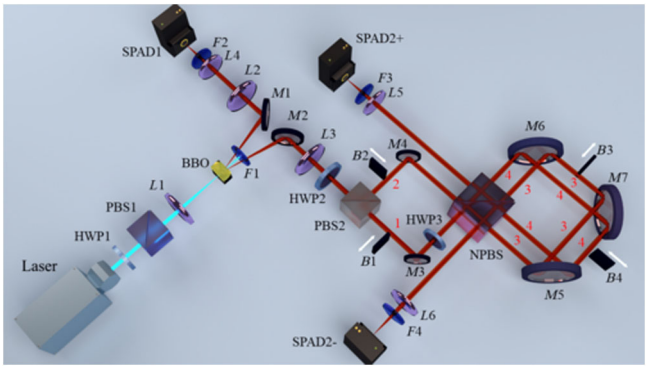

FIG. 4. Schematic of the experimental setup. Here HWP1, HWP2, and HWP3 are the half-wave plates; PBS1 and PBS2 are the polarizing beam splitters; L1, L4, L5, and L6 are the focusing lens; F1 is the long-pass filter; M is the dielectric mirror; L2 and L3 are the collimating lenses; F2, F3, and F4 are the band-pass filters; B1, B2, B3, and B4 are the blockers; NPBS is the nonpolarizing beam splitter; and SPAD1, SPAD2+, and SPAD2− are the single-photon avalanche detectors. Two arms of the AMZI are marked as 1 and 2, representing the +1 and −1 arms, respectively. Similarly, two arms of the DSI are marked as 3 and 4, representing −1 and +1. SPAD2+ and SPAD2− are placed in the +1 and −1 arms, respectively. Adapted with permission from Joarder *et al.*, 2022, PRX Quantum *3* 010307, 2022 [40].

Experimental setup: The experimental setup Fig. 4 of Ref. [40] we are considering for generating LGI-certified randomness consists of three stages: (1) state preparation—this step used a single photon source and a beam splitter to generate a pair of photons, out of which one is sent for heralding and the other is sent to the experimental setup. (2) Unitary transformation—the two unitary transformations ($t_1 \to t_2$ and $t_2 \to t_3$) were implemented using an asymmetric Mach-Zender interferometer (AMZI) and a displaced Sagnac interferometer (DSI). (3) Measurements—measurements were performed using blockers in different arms of the two interferometers for noninvasive measurements and single-photon avalanche detectors (SPAD) for direct detection at the end of the experiment.

State preparation: A heralded twin-photon source was built based on spontaneous parametric down-conversion (SPDC), with a diode laser pumping a beta barium borate (BBO) crystal with a 405 nm wavelength and 10 mW power. The BBO crystal is oriented so that it is phase-matched for degenerate, noncollinear, type-I SPDCs while being pumped with horizontally polarized light. Parametric down-conversion creates pairs of single photons with vertical polarization and 810 nm central wavelength. To increase pair generation, we also place a focusing lens (L1) to focus the pump beam into the central spot of the BBO crystal. A long-pass filter (F1) is placed after the crystal to block the pump beam and pass only the down-converted single-photon pairs. A half-wave plate and polarizing beam splitter PBS1 are placed after the nonlinear crystal to separate the two photons in the two arms of the beam splitter. Two mirrors are

placed to direct one photon to the experiment and the other to a SPAD1 detector for heralding.

Unitary transformation: The experimental setup consists of two interferometers whose arms are denoted by 1,2,3,4, where blockers are placed for noninvasive measurements. The first interferometer is an asymmetric Mach-Zehnder interferometer (AMZI), while the second is a displaced Sagnac interferometer (DSI). The beam-splitting ratio in the two arms of the AMZI is controlled by a combination of a half-wave plate (HWP2) and a polarizing beam splitter (PBS2). For satisfying the two-time NSITs, the two arms of the first Mach-Zehnder interferometer (MZI) are made noninterfering by adding a path difference between the $+1$ and -1 arms. A single nonpolarizing beam splitter (NPBS) with a measured splitting ratio of 80:20 (concerning vertically polarized light at 810 nm wavelength) is used in the DSI. Two detectors (SPAD2+ and SPAD2−) are placed in the two output arms of the DSI to detect single photons.

The times t_1, t_2, and t_3 are being defined in the following manner: t_1 is the time from PBS2 to the first impact on NPBS, t_2 is the time from the first impact to the second impact on NPBS, and t_3 is the time after the impact on NPBS till detection on one of the detectors.

Measurements: Negative result measurements at t_1 and t_2 are performed using motorized blockers (B1 and B2) in arms 1 and 2 and (B3 and B4) in arms 3 and 4. The experiment is completed in three stages corresponding to the measurement of $\langle Q_{t_1} Q_{t_3} \rangle$, $\langle Q_{t_2} Q_{t_3} \rangle$, and $\langle Q_{t_1} Q_{t_2} \rangle$, respectively. For the first two stages, two runs each are performed by placing the blockers on the respective arms and detecting the photon at the end to measure the coincidence events $(++)$, $(+-)$, $(-+)$, and $(--)$. For instance, if a blocker is placed in the $-$ arm of the second interferometer (DSI), and a click is observed in SPAD2+, this will count as a measurement for the probability $P(++|Q_2 Q_3)$ and a click in SPAD2− will count as a measurement for the probability $P(+-|Q_2 Q_3)$. For the third stage, i.e., for the measurement of $\langle Q_{t_1} Q_{t_2} \rangle$, four runs are performed to evaluate the three-time probabilities. For example, when blockers are placed in the—arm of AMZI and in the—arm of DSI, a detection in SPAD2+ will count as $P(+++|Q_1 Q_2 Q_3)$, and a detection in SPAD2− will count as $P(++-|Q_1 Q_2 Q_3)$. These probabilities are then marginalized to evaluate the two-term probabilities at time t_1 and t_2, which leads to $\langle Q_{t_1} Q_{t_2} \rangle$. $P(+|Q_3)$ was computed by conducting the experiment without any blockers and $P(+|Q_2)$ was computed by placing a blocker at the negative arm of the second interferometer and marginalizing the two-time probabilities. Only the coincidence counts measured, i.e., the simultaneous detection of SPAD1 and SPAD2+ or SPAD2−, are considered valid counts in evaluating the probabilities. We have used avalanched photo diode detectors that have inherently a reasonably higher dark count. A follow-up experiment could change this to superconducting nanowire based detectors, which have higher quantum efficiency as well as lower dark counts. This in turn will affect the signal to noise ratio of the results and can lead to higher rate of random bit generation.

Addressing loopholes: To ensure the experiment was loophole-free, various measures were taken. The clumsiness loophole was addressed using noninvasive measurements and tuning the experimental parameters to satisfy the two-time NSIT conditions. The detection efficiency loophole was eliminated by showing that the violation of LGI cannot be reproduced by the hidden variable model, regardless of detection efficiency. The pivotal aspect of our setup, wherein the measurement at t_3 is consistently performed for all the choices of measurement times, plays a crucial role in overcoming this loophole [40]. The multiphoton emission loophole was addressed using a heralded single-photon source and appropriate filtering. The coincidence loophole was eliminated by using a pair of photons as a timing reference and adjusting the coincidence time windows accordingly. Finally, the preparation state loophole was closed by postselecting only those detected photons from the SPDC source and choosing high signal-to-noise ratios for the corresponding coincidence time windows.

Random number generation: From the eight experiments conducted, we selected three datasets from each experiment to generate bit strings composed of 0's and 1's. The generation of random numbers was based on the coincidence clicks of two detectors, SPAD2+ and SPAD2−, with the heralding detector SPAD1. Coincidence counts were identified using information from the heralding detector and employing a $4ns$ time window. We designated detecting a coincidence event at SPAD2+ as 0 and detecting a coincidence event at SPAD2− as 1.

For the evaluation of the probabilities $P(a_i, a_j|Q_1, Q_3)$ and $P(a_i, a_j|Q_2, Q_3)$ in the first and second phases of the experiment, two subruns were conducted for each experiment. In one subrun, the $+$ arm of the first interferometer was blocked, and in the other subrun, the $-$ arm of the interferometer was blocked. In the first case, if a photon from the experimental setup coincidentally hit SPAD2+ with the heralding detector SPAD1, it was counted as 0. If it coincidentally hit SPAD2− with SPAD1, it was counted as 1, thus generating a bit string for this subrun and resulting in the probabilities $P(-+|Q_1, Q_3)$ and $P(--|Q_1, Q_3)$. Similarly, for the second subrun where the $-$ arm was blocked, a bit string was generated based on the detector clicks, leading to the probabilities $P(++|Q_1, Q_3)$ and $P(+-|Q_1, Q_3)$.

Likewise, two more bit strings were generated from the second phase of the experiment, providing the probabilities $P(a_i, a_j|Q_2, Q_3)$. However, the third phase of the experiment, aimed at computing correlations at times t_1 and t_2, involved marginalizing the three-time probabilities $P(a_i, a_j, a_k|Q_1, Q_2, Q_3)$. In this case, blockers were placed

TABLE II. Length of the random bit string generated from the detector counts of the two detectors SPAD2+ and SPAD2− from the eight experiments to evaluate the different joint probabilities.

Experiment	Rate (bits/ sec)	Length
P(−−|23)P(−+|23)	4722	140 382
P(+−|23)P(++|23)	5139	152 405
P(+−−|123)P(+−+|123)	1177	34 981
P(+ + −|123)P(+ + +|123)	4268	127 123
P(−−−|123)P(−− + |123)	3953	117 651
P(−+−|123)P(−++|123)	1180	34 935
P(+−|13)P(++|13)	5158	153 465
P(− − |13)P(− + |13)	5321	158 176

simultaneously on both interferometers in different arms, enabling the computation of all the three-term probabilities in four runs.

For example, when both + arms of the interferometers were blocked, the detector counts yielded bit strings corresponding to the three-term probabilities $P(--+|Q_1, Q_2, Q_3)$ and $P(--+|Q_1, Q_2, Q_3)$. Although these bit strings did not directly originate from the two-term probabilities $P(a_i, a_j|Q_1, Q_2)$, which occur in the LGI expression used for certifying randomness, they eventually contributed to the computation of two-term probabilities. They thus could be used to certify and quantify the randomness.

Subject to the conditions assumed in this approach, eight distinct bit strings can be generated, as shown in Table II, using the available data from the experiments focused on coincidence event calculations. The average generation rate is 3865 bits/ sec, and the total number of bits generated, which is the sum of the eight-bit strings generated, is 919 118. Each bit string had an appropriate length and successfully passed the SP-800-90B entropy test [56,57] for randomness.

*Contact author: usinha@rri.res.in

[1] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[2] Vaisakh Mannalatha, Sandeep Mishra, and Anirban Pathak, A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness, Quantum Inf. Process. **22**, 439 (2023).

[3] Xiongfeng Ma, Xiao Yuan, Zhu Cao, Bing Qi, and Zhen Zhang, Quantum random number generation, npj Quantum Inf. **2**, 16021 (2016).

[4] George Markowsky, The sad history of random bits, J. Cyber Secur. Mobil. **3**, 1 (2014), https://journals.riverpublishers.com/index.php/JCSANDM/article/view/6165.

[5] Carlos Abellán, Waldimar Amaya, Daniel Mitrani, Valerio Pruneri, and Morgan W. Mitchell, Generation of fresh and pure random numbers for loophole-free bell tests, Phys. Rev. Lett. **115**, 250403 (2015).

[6] Antonio Acín and Lluis Masanes, Certified randomness in quantum physics, Nature (London) **540**, 213 (2016).

[7] Antonio Acín, Serge Massar, and Stefano Pironio, Randomness versus nonlocality and entanglement, Phys. Rev. Lett. **108**, 100402 (2012).

[8] Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang, Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu, Bradley Christensen, Sae Woo Nam *et al.*, Experimentally generated randomness certified by the impossibility of superluminal signals, Nature (London) **556**, 223 (2018).

[9] Roger Colbeck, Quantum and relativistic protocols for secure multi-party computation, arXiv:0911.3814.

[10] Roger Colbeck and Adrian Kent, Private randomness expansion with untrusted devices, J. Phys. A **44**, 095305 (2011).

[11] Roger Colbeck and Renato Renner, Free randomness can be amplified, Nat. Phys. **8**, 450 (2012).

[12] Yang Liu, Xiao Yuan, Ming-Han Li, Weijun Zhang, Qi Zhao, Jiaqiang Zhong, Yuan Cao, Yu-Huai Li, Luo-Kan Chen, Hao Li *et al.*, High-speed device-independent quantum random number generation without a detection loophole, Phys. Rev. Lett. **120**, 010503 (2018).

[13] Yang Liu, Qi Zhao, Ming-Han Li, Jian-Yu Guan, Yanbao Zhang, Bing Bai, Weijun Zhang, Wen-Zhao Liu, Cheng Wu, Xiao Yuan *et al.*, Device-independent quantum random-number generation, Nature (London) **562**, 548 (2018).

[14] Stefano Pironio, Antonio Acín, Serge Massar, A. Boyer de La Giroday, Dzmitry N. Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning *et al.*, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[15] Stefano Pironio and Serge Massar, Security of practical private randomness generation, Phys. Rev. A **87**, 012336 (2013).

[16] Lynden K. Shalm, Yanbao Zhang, Joshua C. Bienfang, Collin Schlager, Martin J. Stevens, Michael D. Mazurek, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Mohammad A. Alhejji *et al.*, Device-independent randomness expansion with entangled photons, Nat. Phys. **17**, 452 (2021).

[17] Stefano Pironio, The certainty of quantum randomness, Nature (London) **556**, 176 (2018).

[18] John S Bell, On the Einstein Podolsky Rosen paradox, Phys. Phys. Fiz. **1**, 195 (1964).

[19] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[20] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt, Proposed experiment to test local hidden-variable theories, Phys. Rev. Lett. **23**, 880 (1969).

[21] Clive Emary, Neill Lambert, and Franco Nori, Leggett–Garg inequalities, Rep. Prog. Phys. **77**, 016001 (2013).

[22] Anthony J. Leggett and Anupam Garg, Quantum mechanics versus macroscopic realism: Is the flux there when nobody looks?, Phys. Rev. Lett. **54**, 857 (1985).

[23] Vikram Athalye, Soumya Singha Roy, and T. S. Mahesh, Investigation of the Leggett-Garg inequality for precessing nuclear spins, Phys. Rev. Lett. **107**, 130402 (2011).

[24] Justin Dressel, Curtis J. Broadbent, John C. Howell, and Andrew N. Jordan, Experimental violation of two-party

Leggett-Garg inequalities with semiweak measurements, Phys. Rev. Lett. **106**, 040402 (2011).
[25] Clive Emary, Neill Lambert, and Franco Nori, Leggett-Garg inequality in electron interferometers, Phys. Rev. B **86**, 235447 (2012).
[26] J. A. Formaggio, D. I. Kaiser, M. M. Murskyj, and T. E. Weiss, Violation of the Leggett-Garg inequality in neutrino oscillations, Phys. Rev. Lett. **117**, 050402 (2016).
[27] Michael E. Goggin, Marcelo P. Almeida, Marco Barbieri, Benjamin P. Lanyon, Jeremy L. O'Brien, Andrew G. White, and Geoff J. Pryde, Violation of the Leggett–Garg inequality with weak measurements of photons, Proc. Natl. Acad. Sci. U.S.A. **108**, 1256 (2011).
[28] Hemant Katiyar, Aharon Brodutch, Dawei Lu, and Raymond Laflamme, Experimental violation of the Leggett–Garg inequality in a three-level system, New J. Phys. **19**, 023033 (2017).
[29] Hemant Katiyar, Abhishek Shukla, K. Rama Koteswara Rao, and T. S. Mahesh, Violation of entropic Leggett-Garg inequality in nuclear spins, Phys. Rev. A **87**, 052102 (2013).
[30] George C. Knee, Stephanie Simmons, Erik M. Gauger, John J. L. Morton, Helge Riemann, Nikolai V. Abrosimov, Peter Becker, Hans-Joachim Pohl, Kohei M. Itoh, Mike L. W. Thewalt *et al.*, Violation of a Leggett–Garg inequality with ideal non-invasive measurements, Nat. Commun. **3**, 606 (2012).
[31] Huan-Yu Ku, Neill Lambert, Feng-Jui Chan, Clive Emary, Yueh-Nan Chen, and Franco Nori, Experimental test of non-macrorealistic cat states in the cloud, npj Quantum Inf. **6**, 98 (2020).
[32] Shayan Majidy, Jonathan J. Halliwell, and Raymond Laflamme, Detecting violations of macrorealism when the original Leggett-Garg inequalities are satisfied, Phys. Rev. A **103**, 062212 (2021).
[33] Agustin Palacios-Laloy, François Mallet, François Nguyen, Patrice Bertet, Denis Vion, Daniel Esteve, and Alexander N. Korotkov, Experimental violation of a Bell's inequality in time with weak measurement, Nat. Phys. **6**, 442 (2010).
[34] Yutaro Suzuki, Masataka Iinuma, and Holger F. Hofmann, Violation of Leggett–Garg inequalities in quantum measurements with variable resolution and back-action, New J. Phys. **14**, 103022 (2012).
[35] Kunkun Wang, Clive Emary, Mengyan Xu, Xiang Zhan, Zhihao Bian, Lei Xiao, and Peng Xue, Violations of a Leggett-Garg inequality without signaling for a photonic qutrit probed with ambiguous measurements, Phys. Rev. A **97**, 020101(R) (2018).
[36] Nathan S. Williams and Andrew N. Jordan, Weak values and the Leggett-Garg inequality in solid-state qubits, Phys. Rev. Lett. **100**, 026804 (2008).
[37] Jin-Shi Xu, Chuan-Feng Li, Xu-Bo Zou, and Guang-Can Guo, Experimental violation of the Leggett-Garg inequality under decoherence, Sci. Rep. **1**, 101 (2011).
[38] Shiladitya Mal, Manik Banik, and Sujit K. Choudhary, Temporal correlations and device-independent randomness, Quantum Inf. Process. **15**, 2993 (2016).
[39] Eric G. Cavalcanti and Howard M. Wiseman, Bell nonlocality, signal locality and unpredictability (or what Bohr could have told Einstein at solvay had he known about Bell experiments), Found. Phys. **42**, 1329 (2012).
[40] Kaushik Joarder, Debashis Saha, Dipankar Home, and Urbasi Sinha, Loophole-free interferometric test of macrorealism using heralded single photons, PRX Quantum **3**, 010307 (2022).
[41] Johannes Kofler and Časlav Brukner, Condition for macroscopic realism beyond the Leggett-Garg inequalities, Phys. Rev. A **87**, 052115 (2013).
[42] Shuyang Meng, Fionnuala Curran, Gabriel Senno, Victoria J. Wright, Máté Farkas, Valerio Scarani, and Antonio Acín, Maximal intrinsic randomness of a quantum state, arXiv:2307.15708.
[43] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.133.020802 for the memory effect treatment, which includes Refs. [7,44–46].
[44] J. Barrett, D. Collins, L. Hardy, A. Kent, and S. Popescu, Quantum nonlocality, Bell inequalities, and the memory loophole, Phys. Rev. A **66**, 042111 (2002).
[45] Goh Koon Tong, *Possible Statistics from Bell Violations* (National University of Singapore, 2014).
[46] S. P. Lalley, *Concentration Inequalities*, Lecture Notes (University of Chicago, Chicago, 2013).
[47] Marco Avesani, Davide G. Marangon, Giuseppe Vallone, and Paolo Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, Nat. Commun. **9**, 5365 (2018).
[48] Jonatan Bohr Brask, Anthony Martin, William Esposito, Raphael Houlmann, Joseph Bowles, Hugo Zbinden, and Nicolas Brunner, Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination, Phys. Rev. Appl. **7**, 054018 (2017).
[49] David Drahi, Nathan Walk, Matty J. Hoban, Aleksey K. Fedorov, Roman Shakhovoy, Akky Feimov, Yury Kurochkin, W. Steven Kolthammer, Joshua Nunn, Jonathan Barrett, and Ian A. Walmsley, Certified quantum random numbers from untrusted light, Phys. Rev. X **10**, 041048 (2020).
[50] You-Qi Nie, Jian-Yu Guan, Hongyi Zhou, Qiang Zhang, Xiongfeng Ma, Jun Zhang, and Jian-Wei Pan, Experimental measurement-device-independent quantum random-number generation, Phys. Rev. A **94**, 060301(R) (2016).
[51] Matej Pivoluska, Martin Plesch, Máté Farkas, Natália Ružičková, Clara Flegel, Natalia Herrera Valencia, Will McCutcheon, Mehul Malik, and Edgar A. Aguilar, Semi-device-independent random number generation with flexible assumptions, npj Quantum Inf. **7**, 50 (2021).
[52] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner, Self-testing quantum random number generator, Phys. Rev. Lett. **114**, 150501 (2015).
[53] Zhu Cao, Hongyi Zhou, Xiao Yuan, and Xiongfeng Ma, Source-independent quantum random number generation, Phys. Rev. X **6**, 011020 (2016).
[54] Debarshi Das, Ananda G. Maity, Debashis Saha, and A. S. Majumdar, Robust certification of arbitrary outcome quantum measurements from temporal correlations, Quantum **6**, 716 (2022).
[55] Shubhayan Sarkar, Certification of unbounded randomness without nonlocality, arXiv:2307.01333.

[56] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert *et al.*, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* (US Department of Commerce, Technology Administration, National Institute of…, 2001), Vol. 22.

[57] Meltem Sönmez Turan, Elaine Barker, John Kelsey, Kerry A. McKay, Mary L. Baish, Mike Boyle *et al.*, Recommendation for the entropy sources used for random bit generation, NIST SPec. Publ. **800**, 102 (2018).

[58] Lijiong Shen, Jianwei Lee, Jean-Daniel Bancal, Alessandro Cerè, Antia Lamas-Linares, Adriana Lita, Thomas Gerrits, Sae Woo Nam, Valerio Scarani, Christian Kurtsiefer *et al.*, Randomness extraction from Bell violation with continuous parametric down-conversion, Phys. Rev. Lett. **121**, 150402 (2018).

[59] Yanbao Zhang, Lynden K. Shalm, Joshua C. Bienfang, Martin J. Stevens, Michael D. Mazurek, Sae Woo Nam, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Honghao Fu *et al.*, Experimental low-latency device-independent quantum randomness, Phys. Rev. Lett. **124**, 010505 (2020).

[60] Ming-Han Li, Xingjian Zhang, Wen-Zhao Liu, Si-Ran Zhao, Bing Bai, Yang Liu, Qi Zhao, Yuxiang Peng, Jun Zhang, Yanbao Zhang *et al.*, Experimental realization of device-independent quantum randomness expansion, Phys. Rev. Lett. **126**, 050503 (2021).

[61] Wen-Zhao Liu, Ming-Han Li, Sammy Ragy, Si-Ran Zhao, Bing Bai, Yang Liu, Peter J. Brown, Jun Zhang, Roger Colbeck, Jingyun Fan *et al.*, Device-independent randomness expansion against quantum side information, Nat. Phys. **17**, 448 (2021).