



Certified random-number generation from quantum steeringDominick J. Joch ¹, Sergei Slussarenko ^{1,*}, Yuanlong Wang ^{1,†}, Alex Pepper,¹ Shouyi Xie,^{2,‡} Bin-Bin Xu ^{2,§}, Ian R. Berkman ², Sven Rogge ² and Geoff J. Pryde ^{1,¶}¹*Centre for Quantum Dynamics and Centre for Quantum Computation and Communication Technology, Griffith University, Brisbane, Queensland 4111, Australia*²*Centre for Quantum Computation and Communication Technology, School of Physics, The University of New South Wales, Sydney, NSW 2052, Australia*

(Received 8 February 2022; accepted 17 October 2022; published 7 November 2022)

The use of simple quantum processes promises to provide numbers that no physical observer could predict, but in practice, unwanted noise and imperfect devices can compromise fundamental randomness and protocol security. The ultimate random number generators take advantage of quantum nonlocality to certify unpredictability—including to an adversary—even in the absence of trust in devices. We demonstrate a generator of public or private randomness based on the quantum steering task. We use polarization-entangled photon pairs to certify and extract randomness in a one-sided device-independent framework, with the detection loophole closed. Our work enables nonlocality-based certified randomness generation in environmental regimes where fully-device-independent protocols are not feasible.

DOI: [10.1103/PhysRevA.106.L050401](https://doi.org/10.1103/PhysRevA.106.L050401)**I. INTRODUCTION**

Randomness is an essential resource in many applications from simulation to cryptography. For applications where one cares about security, *certified* private randomness is required—randomness that is guaranteed to not be predictable to an adversary or physical observer [1,2]. Purportedly random numbers can be tested for uniformity and the presence of predictable patterns, but such tests can be satisfied by some pseudorandom number generators [1,3]. As these statistical tests can be passed by sets of numbers of deterministic origin, one cannot rely on them to assert unpredictability. Instead, one must certify randomness in the generation process itself [4].

Quantum phenomena display intrinsic randomness and can thus serve as quantum random number generators (QRNG). Standard QRNG [5–8] operates in a trusted-device scenario that relies on assumptions about, and accurate modeling of, physical devices. Imperfections are susceptible to exploitation by adversaries [1,2,9–11], as they can carry side information. Classical side information comes from sources like thermal and electronic noise, which may be of a malicious nature

(known to, or controlled by, an adversary), and quantum side information arises from correlation with another quantum system. Hardware failures in devices could also compromise the output [4], and noise will inevitably be introduced by experimental imperfections [3]. Hence, certification and post-processing are necessary to acquire private randomness that is independent of side information [4,12], which can be accounted for within the strategies of an adversary.

Certified random numbers are produced from a process that any physical observer cannot perfectly predict, under a reasonable set of assumptions—the fewer and weaker the assumptions, the stronger the security. To minimize device-related assumptions as much as experimentally possible, randomness can be certified by device-independent QRNG (DI-QRNG) protocols in a Bell test (or instrumental [3,13]) scenario [1,4,9], offering the highest possible security when loopholes are closed [11]. The realization of such protocols has been achieved only recently [2,9,14,15], with extreme security following the first strong-loophole-free Bell tests [16–18]. Currently, work is still progressing towards reaching the rates desired for commercial applications with loopholes closed [10,19,20]. DI-QRNG is technically demanding, as very high detection efficiencies and low noise are necessary to certify randomness with closed loopholes, which poses a challenge to achieving high rates. Therefore, many partially-device-independent protocols, exploiting the trade-off between security and ease of implementation, have been developed [4,11,21–23], including measurement-device-independent [24,25] and source-independent [12,26–29] protocols.

Here we demonstrate an experimental implementation of a QRNG protocol, based on the quantum steering task [30,31] with polarization-entangled photon pairs, with the detection loophole closed, and extract certified random numbers with

*s.slussarenko@griffith.edu.au

†Present address: Key Laboratory of Systems and Control, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China.

‡Present address: School of Physics, The University of Sydney, Camperdown, NSW 2006, Australia.

§Present address: Beijing Key Laboratory for Precision Optoelectronic Measurement Instrument and Technology, School of Optics and Photonics, Beijing Institute of Technology, Beijing 100081, China.

¶g.pryde@griffith.edu.au

a high security against individual attacks of a quantum adversary. Quantum steering has been proposed as a method to realize one-sided device-independent (1SDI) QRNG [21] and 1SDI quantum key distribution (QKD) [32] (followed by the experimental realizations of 1SDI QKD in a continuous variable scenario [33,34]), which both certify randomness. Among the family of partially DI protocols, steering-based ones offer improved security over trusted-device and other partially DI protocols by assuming trust in only one measurement device (Bob). Due to steering having trust assumptions different from a Bell inequality, states needed for DI-QRNG are steerable, but not all steerable states violate a Bell inequality. Steering provides greater noise tolerance and is more robust to loss, allowing randomness to be certified at lower efficiencies than DI-QRNG [21], although the latter has not yet been investigated in a photonic experiment [35].

II. QUANTUM STEERING

First, we introduce the quantum steering scenario. Consider two parties named Alice and Bob, who receive a bipartite state ρ_{AB} from some untrusted source. One-sided device independence comes from one party (Bob, say) being trusted and the other, Alice, being untrusted. Her measurement device is treated as a black box with classical inputs $x \in \{1, \dots, \mathcal{M}\}$ for \mathcal{M} measurement settings, and classical outcomes $a \in \{0, 1, \emptyset\}$, where \emptyset is the null outcome to account for experimental losses. A trusted Bob is not malicious and has full knowledge of the inner workings of his measurement device. Bob accepts quantum mechanics to be valid and can perform quantum state tomography to construct an *assemblage*—a set of unnormalized quantum states conditional on Alice’s settings and outcomes [31]. Properties of the assemblage determine whether quantum steering pertains. Specifically, in the assemblage picture, quantum steering can be tested via a semidefinite program (SDP) [31,36] (see Supplemental Materials [37]), an approach that proves useful in randomness certification. It is also possible to construct steering protocols where the need to trust Bob is greatly reduced by using quantum instructions [38], although trust in quantum mechanics is still required.

III. RANDOMNESS CERTIFICATION

To certify the local randomness of Alice’s outcomes, an adversarial situation is considered where in a given trial, an eavesdropper (Eve) attempts to predict Alice’s outcome (Fig. 1). We assume that Eve is restricted to *individual attacks*, where trials are independent and identically distributed with respect to her strategy [21], and Eve cannot make *collective attacks* or *coherent attacks*. It is therefore assumed that the untrusted devices lack quantum memory, or the memory’s coherence time is not sufficient to perform multitrial attacks.

If Eve’s guessing probability $P_g(x^*)$ —where x^* is Alice’s setting in a trial—is less than unity, she cannot perfectly predict the outcome of Alice, and some randomness is certified as quantified by the min-entropy

$$H_{\min} = -\log_2[P_g(x^*)]. \quad (1)$$

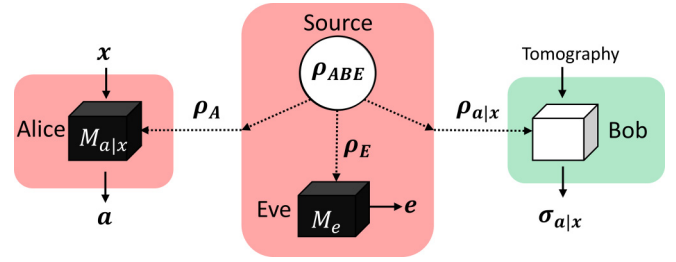


FIG. 1. Adversarial scenario for randomness certification. The eavesdropper, Eve, is assumed to control the source. It is assumed that, while in principle the source distributes bipartite states to Alice and Bob, she may in fact distribute a tripartite state such that $\rho_{AB} = \text{Tr}_E \rho_{ABE}$. She may perform a measurement M_e on her subsystem, acquiring the outcome e which is her guess for Alice’s outcome, and both e and M_e are unknown to Bob. Alice selects a setting x and acquires outcome a from the measurement $M_{a|x}$. Bob performs quantum state tomography and obtains an assemblage $\sigma_{a|x}$ of conditional states.

The upper bound on the certified randomness is found by optimizing Eve’s guessing strategy to maximize $P_g(x^*)$. The source of bipartite states, being untrusted, may be in Eve’s possession, so we assume the states ρ_{AB} are correlated with another quantum system held by Eve, as in Fig. 1. Since Eve’s outcome is unknown, Bob’s observed assemblage theoretically is of the form

$$\sigma_{a|x} = \sum_e \sigma_{a|x}^e = \sum_e \text{Tr}_{AE}[(M_{a|x} \otimes \mathbb{1}_B \otimes M_e) \rho_{ABE}]. \quad (2)$$

Eve’s strategy is accounted for in Bob’s assemblage, and so the optimization is done with respect to $\{\sigma_{a|x}^e\}$ by solving a semidefinite program (SDP) [21,36]:

$$\begin{aligned} \max_{\{\sigma_{a|x}^e\}_{a,x,e}} \quad & P_g(x^*) = \sum_e \text{Tr}(\sigma_{a=e|x^*}^e), \\ \text{s.t.} \quad & \sum_e \sigma_{a|x}^e = \sigma_{a|x} \quad \forall a, x, \\ & \sum_a \sigma_{a|x}^e = \sum_a \sigma_{a|x'}^e \quad \forall e, x \neq x', \\ & \sigma_{a|x}^e \geq 0 \quad \forall a, x, e. \end{aligned} \quad (3)$$

The first constraint ensures compatibility with Bob’s assemblage. The second enforces the nonsignaling condition, that is, to disallow measurement settings at one party to influence outcomes at another. The third is a positive semidefinite constraint to ensure $\{\sigma_{a|x}^e\}$ consists of valid quantum states [21].

As in the Bell scenario (see Ref. [39] for loopholes in Bell tests), certain assumptions open loopholes which would allow for nonlocality to be falsely verified while permitting a local causal explanation [40]. The detection loophole appears under the fair sampling assumption that the statistics of the detected sample accurately represent the total sample. However, loss in the untrusted device may constitute a cheating strategy, therefore a certain heralding efficiency (the probability of one party detecting given that the other party detects) is demanded of Alice to close this loophole. There is no such requirement upon Bob, unlike the Bell scenario.

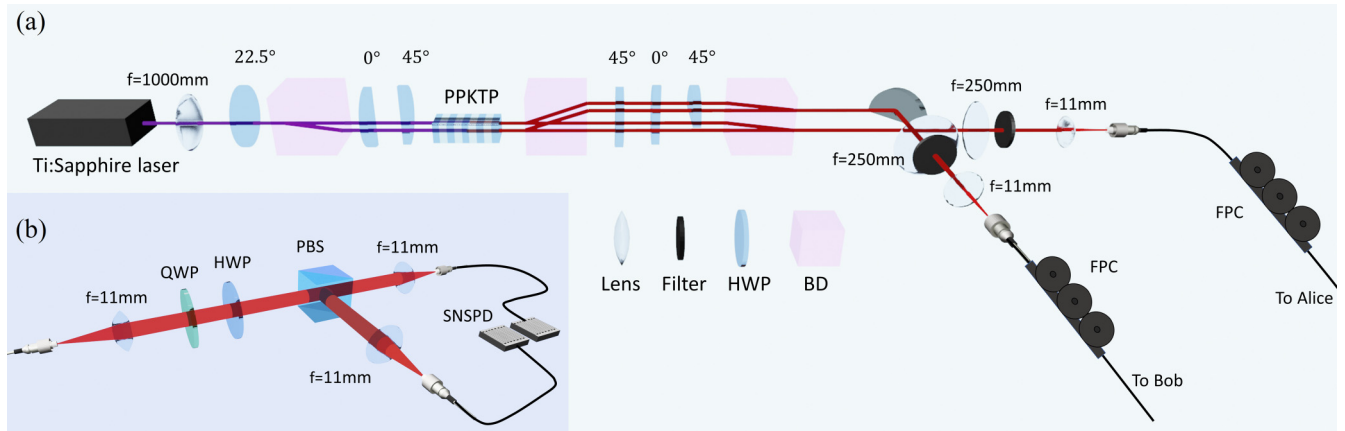


FIG. 2. Experimental setup: (a) The source of bipartite states. A continuous wave 775 nm pump from a Ti:sapphire laser is focused in two locations inside a periodically poled KTiOPO_4 (PPKTP) crystal, creating telecom photons in pairs by type-II spontaneous parametric down-conversion (SPDC). The process occurs within a Mach-Zehnder interferometer comprised of beam displacers (BDs) and a series of cut half waveplates (HWPs) to produce entangled states $\frac{1}{\sqrt{2}}(|00\rangle + e^{-i\phi}|11\rangle)$ by interfering the two SDPC events [41]. The angles of the HWPs relative to their optical axis are annotated. The photon pairs are coupled into single-mode fiber (SMF) and sent to the measurement devices of the two parties. Fiber polarization controllers (FPCs) are used to correct unwanted in-fiber transformations of the qubits, and to implement local unitary rotations to prepare each of the four canonical Bell states. (b) Alice’s and Bob’s measurement devices. Both Alice and Bob have the same physical setup; the combination of a quarter waveplate (QWP), HWP, and polarizing beam splitter (PBS) is used to measure the polarization state of the photons in different settings. Both output modes of the PBS are coupled into SMF and finally detected by superconducting nanowire single-photon detectors (SNSPDs) [42]. Detection events are recorded by trusted devices of the user (time taggers, classical computers).

IV. QRNG PROTOCOL

Our certified quantum random number generator is a two-stage protocol: entropy accumulation followed by randomness extraction. Our protocol involves the parties Eve (source), Alice, Bob, and another (necessarily trusted) party—sometimes called Victor the verifier—being the user on Bob’s side who has access to the data recording and processing devices. In the first stage we acquire two sets of experimental data: that needed for the certification step, and another set which provides many weakly random bits. To do this, many trials of the protocol are performed. Each is structured as in Fig. 1, where a source distributes a state, Alice and Bob perform measurements, and the outcomes are recorded. From the experimental certification data, an assemblage is determined and used with the SDP of Eq. (3) to obtain the min-entropy H_{\min} that quantifies the randomness certified in the weakly random string. The protocol passes (i.e., is able to generate certified randomness) if H_{\min} is nonzero and the number of extractable bits is $m \geq 1$. Conditional on passing, we or Victor (the user) apply a randomness extractor, which is an algorithm that produces random numbers from the raw string. These random bits are certified, which means that an adversary cannot predict them provided they are kept private after generation and the other assumptions of our protocol hold.

V. EXPERIMENTAL IMPLEMENTATION

The experimental realization of the protocol—which uses photonic polarization qubits—is shown in Fig. 2. Our source prepares bipartite entangled states of telecommunications-wavelength photons created by SPDC. A quantum state fidelity of $\mathcal{F} = 0.9933 \pm 0.0005$ with

$|\Psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ was recorded for one data set; other data sets corresponded to generated states with comparable singlet-state fidelities. The photon pairs are coupled into optical fiber and sent to the measurement devices of the two parties [Fig. 2(b)].

In the implementation of the protocol, a certification data acquisition (later used to find H_{\min}) is performed, followed by generation data acquisition; these steps make up the accumulation stage. Bob’s device allows him to measure in three complementary bases and use the data to perform quantum state tomography to determine his local states for each of the $\mathcal{M} = 2$ settings (X, Z) and outcomes $a \in \{0, 1, \emptyset\}$ of Alice. The closest physical assemblage for Bob’s data is obtained with a maximum likelihood reconstruction to ensure the nonsignaling condition [see Eq. (3) conditions] is satisfied even in the presence of statistical noise arising from finite Poissonian data. The semidefinite program Eq. (3) is solved to certify the amount of randomness present in the weakly random data. In Fig. 3(a), we compare our certification results with the theoretical bounds for 1SDI [21] and DI randomness certification methods. The corresponding steering inequality violations [37] are shown in Fig. 3(b). We obtained the highest min-entropy of $H_{\min} = 0.042 \pm 0.003$, at a heralding efficiency of $\eta_{\text{Alice}} = 0.543 \pm 0.001$. Our results demonstrate randomness certification below the lowest heralding efficiency bounds of DI protocols at $2/3$ [17], showing the advantage of the one-sided scheme to add experimental robustness.

During generation data acquisition trials, detection is time tagged to record the exact time of a detection event and the detector channel. In a run of the protocol there are about 100 iterations in the generation data acquisition, and we consume

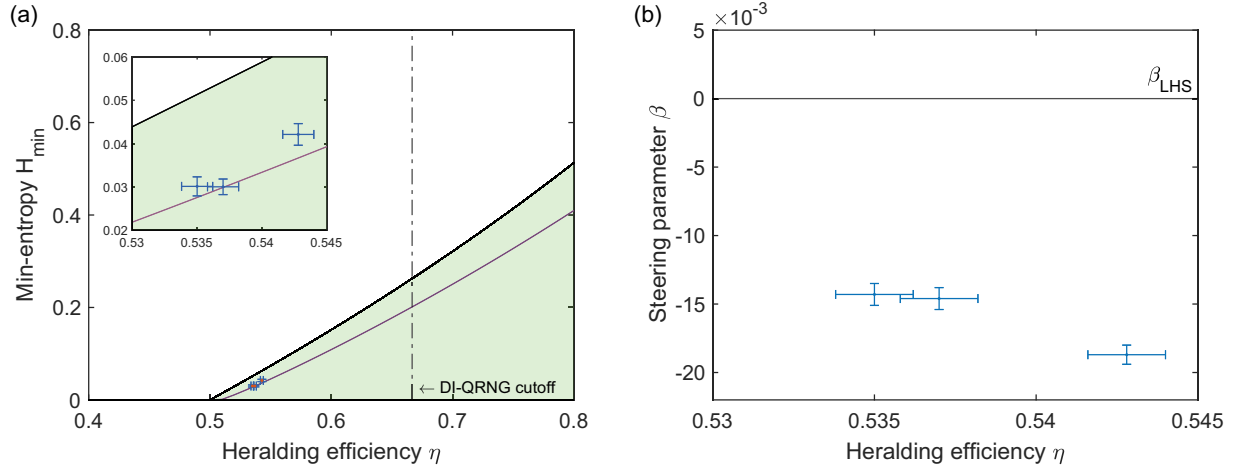


FIG. 3. Randomness certification: (a) Certified min-entropy H_{\min} against the heralding efficiency η of Alice for multiple runs of the protocol. The black line is the theoretical 1SDI bound for a maximally entangled two-qubit Bell state, with a heralding efficiency threshold of 0.5. The purple line is for the Werner state $0.99|\Psi^-\rangle\langle\Psi^-| + 0.01\mathbb{1}/4$. The dashed line is the lowest theoretical device-independent threshold of $\frac{2}{3}$. (b) Steering parameter β vs heralding efficiency of Alice for the three data sets, showing a violation of the steering inequality $\beta := \text{Tr} \sum_{a,x} F_{a|x} \sigma_{a|x} \geq 0$ [37].

8 bits of randomness per iteration that are obtained from a trusted-device QRNG beacon [5,37,43]. The raw time-tag data is postprocessed; thanks to our trust in Bob, we can postselect the successful trials as coincidence events, where the parties detect a pair of photons within a 3 ns window. We convert Alice’s outcomes into a string of bits by assigning detection channels to binary values, and we exclude the null outcomes (which does not compromise the security as long as the certification step, which takes into account null events, has been passed). We note that we do not need to assume that Alice’s measurements are performed accurately or even at all, as long as her “measurement” strategy is the same during certification and generation trials. Alice and Eve should be unaware of the type of trial ahead of time, otherwise they may adapt their strategy accordingly to cheat in generation trials. To prevent this, Bob can decide and inform Alice afterwards which trials contribute to certification. The trials can also be chosen ahead of time with trusted coordination, such as spot-checking in DI-QRNG [20].

In the randomness extraction stage, weakly random data is postprocessed by a classical algorithm to acquire certified random bits. We use an implementation of Trevisan’s extractor [3,44]. This algorithm is a *quantum-proof strong randomness extractor*, meaning that it is secure against both classical and quantum side information, and that the seed randomness is not consumed and can be reused [45]. Our extractor program is modified from the code of Ref. [3], which is based on the construction devised in Ref. [45]. In the case that the protocol passes the certification test, the extractor takes as input the uniform seed, min-entropy, error parameter ϵ , and weak source of randomness, and outputs a string of certified random bits. Note that the extractor is independent of the general scheme of our protocol, so any suitable quantum-proof strong extractor may be used.

From our data sets we extracted certified random bits using seed bits obtained from the trusted-device QRNG beacon [5,43]. From the largest data set ($H_{\min} = 0.030$, $\eta = 0.535$)

we could have, in principle, extracted 111,035 certified random bits uniform to within 2^{-64} , with 8,126,464 seed bits. From the other two data sets in principle we could extract 7018 ($H_{\min} = 0.042$) and 8073 ($H_{\min} = 0.030$, $\eta = 0.537$) certified random bits uniform to within 2^{-64} , with 4,456,448 and 4,718,592 seed bits, respectively. This extractor has low entropy loss versus error and performs well for low min-entropies. However, it requires a large seed, so the full computation was not performed for $\epsilon = 2^{-64}$. Using Trevisan’s extractor with large data sets also becomes computationally demanding [15,20,45] and impractical for low-latency RNG. A solution is to perform extraction with smaller sets of weakly random data to produce the output sequence in blocks [19] with greatly reduced runtime and seed requirement due to the strong extractor property [46]. By processing 20 kb at a time, we extracted 6489 certified random bits uniform to within 10^{-6} generated in 754-bit blocks, with 180,224 seed bits, from the $H_{\min} = 0.042$ data set, and 7131 certified random bits uniform to within 10^{-6} generated in 514-bit blocks, with 147,456 seed bits, from the $H_{\min} = 0.030$ ($\eta = 0.537$) data set. From the $H_{\min} = 0.030$ ($\eta = 0.535$) data set we extracted a total of 94981 certified random bits uniform to within 10^{-6} generated in 514-bit blocks, using 147,456 seed bits.

For each data acquisition run we consumed 800 random bits, and thus achieved randomness expansion. This highlights another advantage of the steering scheme, in which the per-trial violation [2] can be significant, even though the generation of entangled pairs from the source is random and has low probability ($\sim 0.1\%$) per pulse. This is because Bob is a trusted party, and thus a valid trial is defined whenever he receives a detection, regardless of the efficiency of his detection. This contrasts with DI-QRNG with SPDC, where, due to the large vacuum component in the two-mode state, the per-trial violation is low. Such an advantage is especially beneficial in a protocol implementation that closes the freedom of choice loophole. There, additional randomness is also consumed in each trial in order to choose a measurement instruction sent to

untrusted parties. Significantly higher per-trial violation of a steering test leads to a much lower randomness consumption, making randomness expansion easier to achieve than with a Bell test [20,37].

VI. CONCLUSIONS

We demonstrated a steering-based one-sided device-independent random number generator which produces certified random bits with the detection loophole closed. We extract the random bits using a quantum-proof strong extractor, thereby demonstrating a full implementation of a steering-based QRNG protocol. With heralding efficiencies for Alice above the steering threshold and below the threshold for device-independent methods, we performed randomness certification in an experimental regime where no randomness can be certified by DI-QRNG.

Certified QRNGs with levels of device independence will bring improved security to public randomness sources and private randomness for cryptographic applications. Here we have demonstrated a certified QRNG that, by closing the locality loophole and strengthening freedom of choice,

can be extended to a strong-loophole-free one-sided device-independent QRNG, and a viable randomness beacon. Further security improvements can be achieved by adopting a security analysis similar to the one in Ref. [32], which allows for certification against coherent attacks. With this security framework, the heralding efficiency threshold for Alice will increase, but the protocol will retain its other advantages over DI approaches, including higher per-trial inequality violation, lower randomness consumption, and ability to use Bob's detection events to herald successful entanglement distribution trials. In the preparation of this work, we became aware of a related experiment on the generation of steering-based certified randomness with entangled squeezed vacuum states and homodyne measurement [47].

ACKNOWLEDGMENTS

This work was supported in part by ARC Grant No. DP210101651 and in part by ARC Grant No. CE170100012. D.J.J. acknowledges support by the Australian Government Research Training Program (RTP). We thank Lynden K. Shalm and Howard Wiseman for helpful conversations.

-
- [1] L. Masanes and A. Acín, Certified randomness in quantum physics, *Nature (London)*, **213** (2016).
 - [2] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Experimentally generated randomness certified by the impossibility of superluminal signals, *Nature (London)* **556**, 223 (2018).
 - [3] I. Agresti, D. Poderini, L. Guerini, M. Mancusi, G. Carvacho, L. Aolita, D. Cavalcanti, R. Chaves, and F. Sciarrino, Experimental device-independent certified randomness generation with an instrumental causal structure, *Commun. Phys.* **3**, 110 (2020).
 - [4] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, *Rev. Mod. Phys.* **89**, 015004 (2017).
 - [5] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Y. Ng, V. Sharma, P. K. Lam, and T. Symul, Maximization of Extractable Randomness in a Quantum Random-Number Generator, *Phys. Rev. Appl.* **3**, 054004 (2015).
 - [6] T. Gehring, C. Lupo, A. Kordts, D. S. Nikolic, N. Jain, T. Rydberg, T. B. Pedersen, S. Pirandola, and U. L. Andersen, Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information, *Nat. Commun.* **12**, 605 (2021).
 - [7] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, and J.-W. Pan, The generation of 68 Gbps quantum random number by measuring laser phase fluctuations, *Rev. Sci. Instrum.* **86**, 063105 (2015).
 - [8] B. Haylock, D. Peace, F. Lenzini, C. Weedbrook, and M. Lobino, Multiplexed quantum random number generation, *Quantum* **3**, 141 (2019).
 - [9] S. Pironio, A. Acín, S. Massar, A., D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, *Nature (London)* **464**, 1021 (2010).
 - [10] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent randomness expansion against quantum side information, *Nat. Phys.* **17**, 448 (2021).
 - [11] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator, *Phys. Rev. Appl.* **15**, 034034 (2021).
 - [12] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, *Phys. Rev. Lett.* **118**, 060503 (2017).
 - [13] R. Chaves, G. Carvacho, I. Agresti, V. Di Giulio, L. Aolita, S. Giacomini, and F. Sciarrino, Quantum violation of an instrumental test, *Nat. Phys.* **14**, 291 (2018).
 - [14] Y. Liu, X. Yuan, M.-H. Li, W. Zhang, Q. Zhao, J. Zhong, Y. Cao, Y.-H. Li, L.-K. Chen, H. Li, T. Peng, Y.-A. Chen, C.-Z. Peng, S.-C. Shi, Z. Wang, L. You, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, High-Speed Device-Independent Quantum Random Number Generation without a Detection Loophole, *Phys. Rev. Lett.* **120**, 010503 (2018).
 - [15] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer, Randomness Extraction from Bell Violation with Continuous Parametric Down-Conversion, *Phys. Rev. Lett.* **121**, 150402 (2018).
 - [16] B. Hensen, A. E. Bernien, H. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, *Nature (London)* **526**, 682 (2015).
 - [17] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor *et al.*, Strong Loophole-Free Test of Local Realism, *Phys. Rev. Lett.* **115**, 250402 (2015).

- [18] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-A. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin *et al.*, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, *Phys. Rev. Lett.* **115**, 250401 (2015).
- [19] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink, and E. Knill, Experimental Low-Latency Device-Independent Quantum Randomness, *Phys. Rev. Lett.* **124**, 010505 (2020).
- [20] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, M. W. Amaya, W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill, Device-independent randomness expansion with entangled photons, *Nat. Phys.* **17**, 452 (2021).
- [21] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, Optimal randomness certification in the quantum steering and prepare-and-measure scenarios, *New J. Phys.* **17**, 113010 (2015).
- [22] Y. Zhang, H.-P. Lo, A. Mink, T. Ikuta, T. Honjo, H. Takesue, and W. J. Munro, A simple low-latency real-time certifiable quantum random number generator, *Nat. Commun.* **12**, 1056 (2021).
- [23] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Quantum randomness certified by the uncertainty principle, *Phys. Rev. A* **90**, 052327 (2014).
- [24] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, *New J. Phys.* **17**, 125011 (2015).
- [25] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Experimental measurement-device-independent quantum random-number generation, *Phys. Rev. A* **94**, 060301(R) (2016).
- [26] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-Independent Quantum Random Number Generation, *Phys. Rev. X* **6**, 011020 (2016).
- [27] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, *Nat. Commun.* **9**, 5365 (2018).
- [28] D. Drahi, N. Walk, M. J. Hoban, A. K. Fedorov, R. Shakhovoy, A. Feimov, Y. Kurochkin, W. S. Kolthammer, J. Nunn, J. Barrett, and I. A. Walmsley, Certified Quantum Random Numbers from Untrusted Light, *Phys. Rev. X* **10**, 041048 (2020).
- [29] T. Michel, J. Y. Haw, D. G. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. K. Lam, and S. M. Assad, Real-Time Source-Independent Quantum Random-Number Generator with Squeezed States, *Phys. Rev. Appl.* **12**, 034017 (2019).
- [30] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox, *Phys. Rev. Lett.* **98**, 140402 (2007).
- [31] R. Uola, A. C. S. Costa, H. C. Nguyen, and O. Gühne, Quantum steering, *Rev. Mod. Phys.* **92**, 015001 (2020).
- [32] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering, *Phys. Rev. A* **85**, 010301(R) (2012).
- [33] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks, *Nat. Commun.* **6**, 8795 (2015).
- [34] N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H. M. Wiseman, and P. K. Lam, Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution, *Optica* **3**, 634 (2016).
- [35] A. Máttar, P. Skrzypczyk, G. H. Aguilar, R. V. Nery, P. H. S. Ribeiro, S. P. Walborn, and D. Cavalcanti, Experimental multipartite entanglement and randomness certification of the W state in the quantum steering scenario, *Quantum Sci. Technol.* **2**, 015011 (2017).
- [36] D. Cavalcanti and P. Skrzypczyk, Quantum steering: A review with focus on semidefinite programming, *Rep. Prog. Phys.* **80**, 024001 (2017).
- [37] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevA.106.L050401>, which includes Ref. [48], with details on the quantum steering inequality, randomness extraction procedure, and amount of randomness consumed by the protocol.
- [38] S. Kocsis, M. J. W. Hall, A. Bennet, D. J. Saunders, and G. J. Pryde, Experimental measurement-device-independent verification of quantum steering, *Nat. Commun.* **6**, 5886 (2015).
- [39] J.-Å. Larsson, Loopholes in Bell inequality tests of local realism, *J. Phys. A: Math. Theor.* **47**, 424003 (2014).
- [40] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger, Loophole-free Einstein-Podolsky-Rosen experiment via quantum steering, *New J. Phys.* **14**, 053030 (2012).
- [41] N. Tischler, F. Ghafari, T. J. Baker, S. Slussarenko, R. B. Patel, M. M. Weston, S. Wollmann, L. K. Shalm, V. B. Verma, S. W. Nam, H. C. Nguyen, H. M. Wiseman, and G. J. Pryde, Conclusive Experimental Demonstration of One-Way Einstein-Podolsky-Rosen Steering, *Phys. Rev. Lett.* **121**, 100401 (2018).
- [42] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Detecting single infrared photons with 93% system efficiency, *Nat. Photonics* **7**, 210 (2013).
- [43] ANU QRNG – Quantum random numbers, <https://qrng.anu.edu.au/>.
- [44] L. Trevisan, Extractors and pseudorandom generators, *J. ACM* **48**, 860 (2001).
- [45] W. Mauerer, C. Portmann, and V. B. Scholz, A modular framework for randomness extraction based on Trevisan's construction, [arXiv:1212.0520](https://arxiv.org/abs/1212.0520).
- [46] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Post-processing for quantum random-number generators: Entropy evaluation and randomness extraction, *Phys. Rev. A* **87**, 062327 (2013).
- [47] M. Ioannou, B. Longstaff, M. V. Larsen, J. S. Neergaard-Nielsen, U. L. Andersen, D. Cavalcanti, N. Brunner, and J. B. Brask, Steering-based randomness certification with squeezed states and homodyne measurements, *Phys. Rev. A* **106**, 042414 (2022).
- [48] M. M. Weston, S. Slussarenko, H. M. Chrzanowski, S. Wollmann, L. K. Shalm, V. B. Verma, M. S. Allman, S. W. Nam, and G. J. Pryde, Heralded quantum steering over a high-loss channel, *Sci. Adv.* **4**, e1701230 (2018).