Quantum vs Noncontextual Semi-Device-Independent Randomness Certification

Roch I Carceller, Carles; Flatt, Kieran; Lee, Hanwool; Bae, Joonwoo; Brask, Jonatan Bohr

Published in:
Physical Review Letters

Link to article, DOI:
10.1103/PhysRevLett.129.050501

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

Quantum vs Noncontextual Semi-Device-Independent Randomness Certification

Carles Roch i Carceller,[1,*] Kieran Flatt,[2] Hanwool Lee,[2] Joonwoo Bae,[2] and Jonatan Bohr Brask[1]
[1]Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kongens Lyngby, Denmark
[2]School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro Yuseong-gu, Daejeon 34141, Republic of Korea

(Received 18 January 2022; accepted 30 June 2022; published 25 July 2022)

We compare the power of quantum and classical physics in terms of randomness certification from devices which are only partially characterized. We study randomness certification based on state discrimination and take noncontextuality as the notion of classicality. A contextual advantage was recently shown to exist for state discrimination. Here, we develop quantum and noncontextual semi-device independent protocols for random-number generation based on maximum-confidence discrimination, which generalizes unambiguous and minimum-error state discrimination. We show that, for quantum eavesdroppers, quantum devices can certify more randomness than noncontextual ones whenever none of the input states are unambiguously identified. That is, a quantum-over-classical advantage exists.

DOI: 10.1103/PhysRevLett.129.050501

Quantum physics departs radically from everyday experience. Observations on quantum systems can defy classical notions of cause and effect and exploiting quantum effects enables advantages for a number of applications including precision sensing, computing, and information security. Understanding the quantum-classical boundary is both of fundamental importance to the foundations of physics in general and of relevance to characterizing and quantifying quantum-over-classical advantages in specific tasks and applications.

In this work, we compare the power of quantum and classical physics for randomness certification. Random numbers are needed for many tasks in science and technology [1,2]. In particular, high-quality randomness is central to cryptographic security and thus to much of modern information technology. Because of the inherent randomness in quantum measurements, strong guarantees can be established for the extraction of randomness from quantum systems. In fact, randomness can be certified with little or no trust in the devices used to generate it. In setups with multiple, separate parties, randomness can be certified in a device-independent (DI) setting, where the devices are treated as untrusted black boxes [3–5]. In that setting, the relevant notion of classicality is locality (also known as local causality), in the sense of Bell [6,7], and the setup is required to violate a Bell inequality to generate randomness. This is, however, technologically very demanding, as the violation must be loophole free [4,8–12]. Here, we focus on the semi-DI setting, where the black boxes are complemented by a few, general assumptions, representing an increased level of trust in the devices. This renders implementations much more accessible, and semi-DI randomness certification can be realized in simple prepare-and-measure setups [13–24]. As our notion of classicality we adopt noncontextuality [25,26], in the form introduced by Spekkens [27], which is applicable also in scenarios which do not have the multipartite structure of Bell tests.

We consider semi-DI randomness certification based on state discrimination, where the partial trust in the devices consists in an assumption about the distinguishability of the prepared states. In particular, we consider maximum-confidence state discrimination [28]. In the context of randomness certification, a semi-DI protocol based on unambiguous state discrimination was previously demonstrated [29], and in the context of comparing quantum and noncontextual models, a quantum advantage for minimum-error state discrimination was demonstrated by Schmid and Spekkens [30]. Maximum-confidence discrimination is more general, containing minimum-error and unambiguous state discrimination as particular cases. In related work, we demonstrate a quantum-over-noncontextual advantage for maximum-confidence state discrimination [31]. In the present work, we find a rich picture. In a setting where the devices are either quantum or noncontextual, but where the eavesdropper in both cases is allowed quantum powers, quantum devices outperform noncontextual ones. However, comparing a quantum universe with quantum eavesdroppers against a noncontextual universe with noncontextual (hence less powerful) eavesdroppers, the amount of quantum certifiable randomness may be both larger than, smaller than or equal to the amount of noncontextual randomness, depending on the distinguishability of the states and the observed confidence of discrimination.

A prepare-and-measure setting for state discrimination and randomness certification is illustrated in Fig. 1(a). We will restrict our attention to binary inputs $x \in \{0, 1\}$ and ternary outputs $b \in \{0, 1, \emptyset\}$. In the case of state discrimination, b represents a guess for which state was prepared,

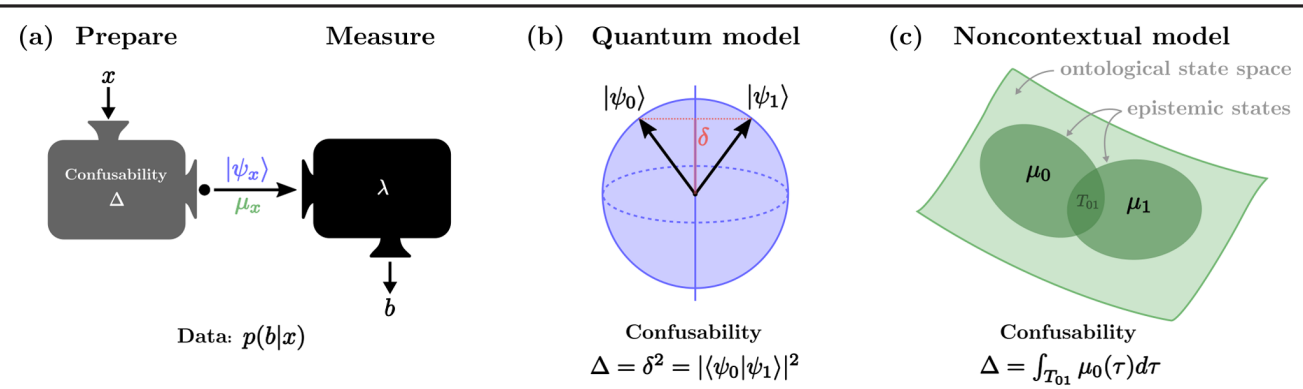

FIG. 1. (a) Prepare-and-measure scenario for state discrimination and randomness certification, in quantum and noncontextual settings. A preparation device takes an input and transmits states to a measurement device, which produces an output. From an assumption about the distinguishability of the states and the observed input-output correlations, the entropy in the raw output can be bounded and random numbers extracted from it. (b) In the quantum setting, the distinguishability is quantified by the overlap of the quantum states. For binary inputs, these can be represented by qubit states. (c) In the noncontextual setting, there is an ontological state space, consisting of perfectly distinguishable states. The preparation device emits epistemic states, given by probability distributions over ontological states. The distinguishability of epistemic states is quantified by the confusability, which measures the overlap of the corresponding distributions.

with ø labeling inconclusive outcomes. For randomness certification, the amount of true randomness present in the output b can be lower bounded based on the observed distribution $p(b|x)$ and an assumption on the distinguishability of the prepared states. We start by considering state discrimination, first in the quantum case and then for noncontextual theories.

In quantum state discrimination, quantum states $\hat{\rho}_x$ are prepared and the measurement device implements a POVM with elements $\hat{\Pi}_b$, resulting in the distribution $p(b|x) = \mathrm{Tr}[\hat{\rho}_x\hat{\Pi}_b]$. For binary inputs, without loss of generality, the state space can be taken to be a qubit space. When the states are furthermore pure, $\hat{\rho}_x = |\psi_x\rangle\langle\psi_x|$, their distinguishability can be quantified simply by their overlap $\delta = |\langle\psi_0|\psi_1\rangle|$. Its estimation will depend on the implementation. For instance, in [29] a time-bin encoding with coherent states was used. In that case, the overlap can be controlled through the amplitude of the pulses. Different quantifiers of performance can be adopted.

In minimum-error state discrimination (MESD), no inconclusive outcomes are permitted, $p(ø|x) = 0$, and the figure of merit is the average error rate $P_e = p_0 p(1|0) + p_1 p(0|1)$, where p_x is the prior probability for input x. Optimal MESD achieves a minimal error rate given by the Helstrom bound $P_e = \frac{1}{2}(1 - \sqrt{1 - 4p_0p_1\delta^2})$ [32]. Thus, errors are unavoidable for nonorthogonal states.

Errors can be suppressed at the cost of a nonzero rate of inconclusive outcomes. In unambiguous state discrimination (USD), the error probabilities are strictly zero, $p(0|1) = p(1|0) = 0$, and the average inconclusive rate $P_ø = p_0 p(ø|0) + p_1 p(ø|1)$ can be taken as the figure of merit. For unbiased inputs, $p_0 = p_1 = \frac{1}{2}$, optimal USD achieves $P_ø = \delta$ [33]. In the case of qubits, USD is possible only for two pure states.

Maximum-confidence discrimination (MCD) generalizes the notions of MESD and USD [28]. The *confidence* C_x is the probability that, given an outcome $b = x$, the input was x. From Bayes' theorem

$$C_x = \frac{p_x}{\eta_x} p(x|x), \tag{1}$$

where $\eta_b = \sum_x p(b|x)p_x$ is the rate of outcome b (i.e., the marginal distribution of the output). In MCD, the figure of merit is a given C_x, or any convex combination of them, and the goal is to maximize this quantity. When $C_x = 1$, the input x is unambiguously identified. Hence, unambiguous discrimination is a particular case of MCD, and if no further constraints are imposed, MCD recovers USD whenever the latter is possible. This is the case for an arbitrary number of linearly independent pure states, and thus in particular always for two distinct pure states, as considered here. MESD can also be recovered by adopting $\eta_0 C_0 + \eta_1 C_1 = 1 - P_e$ as the figure of merit, when the inconclusive rates are zero [33]. In general, MCD is flexible and can handle situations in which both error rates and inconclusive rates are nonzero.

We now proceed to consider noncontextual state discrimination. We start from an ontological model of the prepare-and-measure scenario [30,34]. The system is associated with an ontic state space T in which each point τ completely defines all physical properties, i.e., the outcomes of all possible measurements. Each state preparation x samples the ontic state space according to a probability distribution $\mu_x(\tau)$, referred to as the epistemic state. Each measurement is defined by a set of response functions, that is, non-negative functions $\xi_b(\tau)$ over the ontic space, such that $\sum_b \xi_b(\tau) = 1$ for all $\tau \in T$. The probability of obtaining the outcome b when state μ_x was prepared is

$$p(b|x) = \int_T d\tau\, \mu_x(\tau)\xi_b(\tau). \tag{2}$$

While distinct ontic states can be perfectly discriminated, epistemic states with overlapping distributions cannot. It is the discrimination of epistemic states which we compare against quantum state discrimination.

To compare the two requires a notion analogous to the quantum state overlap. Note that $\delta^2 = |\langle\psi_0|\psi_1\rangle|^2$ can be thought of as the probability that an outcome corresponding to projection onto $|\psi_1\rangle$ occurs when $|\psi_0\rangle$ was prepared (or vice versa). Similarly, in the ontological model we define sharp outcomes as outcomes that are certain to occur for a given preparation. ξ_b is a sharp outcome for μ_x if $p(b|x) = 1$. For discrimination of μ_0 and μ_1, the *confusability* $\Delta_{0,1}$ is then the probability that a sharp outcome for μ_1 occurs when μ_0 was prepared. For preparation-noncontextual models, that we now introduce, one has the same symmetry as in the quantum case $\Delta_{0,1} = \Delta_{1,0} = \Delta$, and the models can be compared for $\Delta = \delta^2$.

Two preparation procedures are said to be operationally equivalent if they cannot be distinguished by any measurement, and the ontological model is said to be *preparation noncontextual* if all operationally equivalent preparations are represented by the same epistemic state. We take preparation noncontextuality as our notion of classicality and refer to it simply as noncontextuality. We impose two requirements on the noncontextual model. First, it reproduces the observed distribution $p(b|x)$. Second, we need an operational equivalence to which noncontextuality can be applied. We take the model to reproduce the existence of complementary states $|\psi_{\bar{x}}\rangle$, with $|\psi_x\rangle\langle\psi_x| + |\psi_{\bar{x}}\rangle\langle\psi_{\bar{x}}| = \mathbb{1}$ and $|\langle\psi_{\bar{0}}|\psi_{\bar{1}}\rangle| = \delta$. That is, in addition to the epistemic states μ_0, μ_1, it must also contain two states $\mu_{\bar{0}}$, $\mu_{\bar{1}}$ such that their confusability is Δ, they obey $\mu_x\mu_{\bar{x}} = 0$, and the convex combinations $\frac{1}{2}\mu_x + \frac{1}{2}\mu_{\bar{x}}$ for $x = 0, 1$ correspond to operationally equivalent preparations. By noncontextuality they must hence be equal $\frac{1}{2}\mu_0 + \frac{1}{2}\mu_{\bar{0}} = \frac{1}{2}\mu_1 + \frac{1}{2}\mu_{\bar{1}}$. It was shown by Schmid and Spekkens, under similar assumptions, that quantum mechanics outperforms noncontextual theory for MESD in the sense that the Helstrom bound is lower than the minimum achievable error rate in the noncontextual model for any value of Δ [30]. In Ref. [31], we study quantum vs noncontextual maximum-confidence discrimination.

The prepare-and-measure state-discrimination setup can be exploited for semi-DI randomness certification by taking Δ as given while the devices are otherwise uncharacterized (the states and measurements are unknown), and then assess the randomness of b based on the observed distribution $p(b|x)$. Intuitively, if $p(b|x)$ is close to optimal discrimination for the given Δ, this constrains the measurements to be close to the optimal ones, and the predictability of b to someone with perfect knowledge of the states and measurements can be estimated. More precisely, we introduce a hidden variable λ, distributed according to q_λ, labeling measurement strategies. The average guessing probability for an eavesdropper with access to λ and the input x

$$p_g = \sum_x p_x \sum_\lambda q_\lambda \max_b p(b|x,\lambda), \tag{3}$$

with $p(b|x,\lambda)$ given by $\mathrm{Tr}[\hat{\rho}_x\hat{\Pi}_b^\lambda]$ when the eavesdropper is quantum and by (2) with response function ξ_b^λ if the eavesdropper is restricted to be noncontextual. Note that λ is assumed to be independent of x (otherwise the discrimination problem becomes trivial). We quantify the randomness by the min-entropy $H_{\min} = -\log_2 p_g$, which gives the number of (almost) uniformly random bits which can be extracted per round of the protocol [35].

Since the measurement strategies are unknown to the user, to certify randomness p_g must be upper bounded by optimizing over all strategies compatible with the observed data. We focus on MCD for the input $x = 0$ and impose only that the rate η_0 and the confidence C_0 are reproduced (as opposed to the full distribution $p(b|x)$. For a quantum eavesdropper, $p_g \le p_g^Q$ with

$$p_g^Q = \max_{q_\lambda,\Pi_b^\lambda} \sum_{x,\lambda} p_x q_\lambda \max_b \mathrm{Tr}[\hat{\rho}_x\hat{\Pi}_b^\lambda], \tag{4}$$

subject to q_λ and $\hat{\Pi}_b^\lambda$ being valid probability distributions and POVMs, respectively, $\sum_{x,\lambda} q_\lambda p_x \mathrm{Tr}[\hat{\rho}_x\hat{\Pi}_0^\lambda] = \eta_0$ and $\sum_\lambda q_\lambda p_0 \mathrm{Tr}[\hat{\rho}_0\hat{\Pi}_0^\lambda] = \eta_0 C_0$. Without loss of generality, the states can be fixed to any pair of states with overlap δ. Thus p_g^Q is a function only of the confusability Δ and the distribution $p(b|x)$. The optimization problem in (4) can be rendered as a semidefinite program (SDP), as we show in [36].

Similarly, the guessing probability for a noncontextual eavesdropper is bounded by $p_g \le p_g^{\mathrm{NC}}$ with

$$p_g^{\mathrm{NC}} = \max_{q_\lambda,M_b^\lambda} \sum_{x,\lambda} p_x q_\lambda \max_b \int_T d\tau\, \mu_x(\tau)\xi_b^\lambda(\tau), \tag{5}$$

where now ξ_b^λ must be valid response functions, and the constraints are the same as in the quantum case with the Born rule replaced by (2).

In a noncontextual theory, a pair of epistemic states must be equal on the overlap of their supports [27,30]. This allows a general response function to be decomposed into four extremal functions, corresponding to integrals over the regions defined by the overlapping supports of μ_0, μ_1 and their nonoverlapping partners. These integrals are, furthermore, functions of the confusability Δ. Using this, in [36] we show that (5) can also be rendered as a semidefinite program.

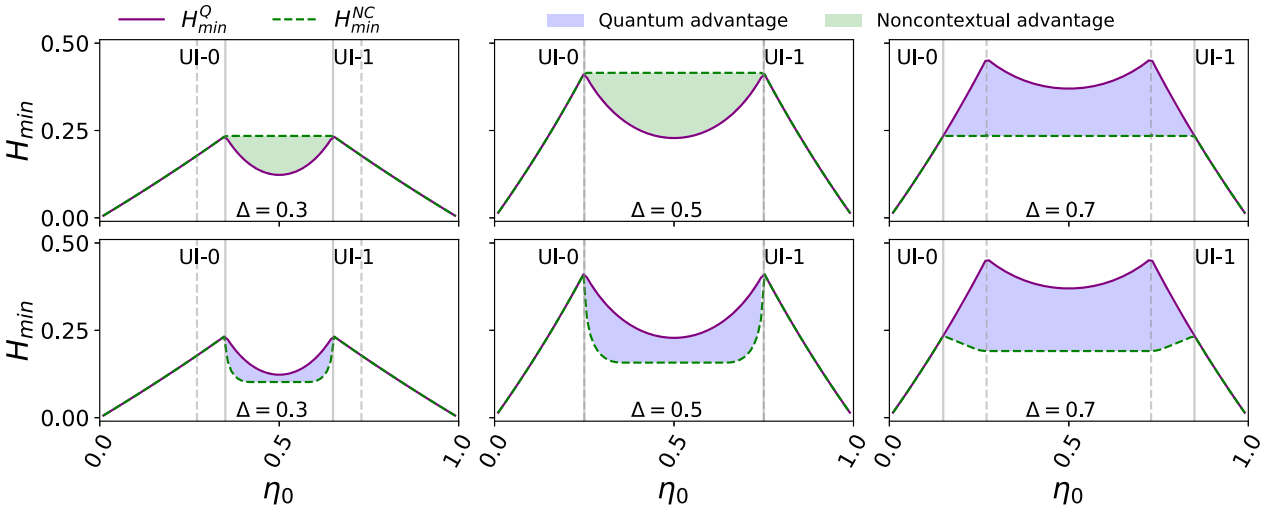

FIG. 2. Quantum $H^Q_{\min}$ and noncontextual $H^{\mathrm{NC}}_{\min}$ certifiable min-entropies vs output rate η_0, for three different confusabilities Δ, optimal confidence C_0, and equal prior probabilities $p_0 = p_1 = \frac{1}{2}$. Solid vertical lines delimit parameter regions in which input x is unambiguously identified, labeled UI-x. Dashed vertical lines indicate rates at which $H^Q_{\min}$ is maximal. The confidences are maximal in all plots. Top row: eavesdroppers in quantum and noncontextual models are respectively quantum and noncontextual. Bottom row: a quantum eavesdropper is considered in both cases.

In Fig. 2, we compare the certifiable quantum and noncontextual min-entropies, $H^Q_{\min}$ and $H^{\mathrm{NC}}_{\min}$, in two different manners, focusing on equal prior probabilities $p_0 = p_1 = \frac{1}{2}$ for simplicity. First, we compute the certifiable $H_{\min}$ within each theory (top row), i.e., $H^Q_{\min}$ when the device attains the maximum quantum confidence and the eavesdropper is also quantum, and $H^{\mathrm{NC}}_{\min}$ for maximum noncontextual confidence and a noncontextual eavesdropper. This is the maximal certifiable randomness in each theory, as $H_{\min}$ is maximized for optimal discrimination. Second, we consider the case in which the eavesdropper is always quantum (bottom row). That is, the minimum entropy is computed via the quantum SDP. Since quantum MCD can reach higher confidences than noncontextual MCD, C_0 is not necessarily the same in the two cases. In [36] we went beyond the study of pure states by studying the case where noisy (mixed) states $\hat{\rho}'_x = (1-r)\hat{\rho}_x + r\mathbb{1}/2$ are prepared. Distinguishablity is still bounded by Δ, and the eavesdropper has no access to decompositions of the mixture. The qualitative behavior in this setting is similar and thus our main conclusions remain valid.

In the first case we find quantum-over-noncontextual as well as noncontextual-over-quantum advantages in terms of certifying randomness. Whenever any of the states is unambiguously identified by the measurement device, the quantum and noncontextual certifiable randomness are equal, $H^Q_{\min} = H^{\mathrm{NC}}_{\min}$. Outside these regions, for confusabilities $\Delta < 1/2$ there is a noncontextual advantage, while for $\Delta > 1/2$ a quantum advantage appears and eventually dominates for large Δ. We interpret this as follows. A quantum eavesdropper is more powerful than a noncontextual one, but optimal quantum discrimination also imposes stronger constraints on the measurement device. For states that are easy to discriminate (low Δ), the former effect wins while for states that a hard to distinguish (high Δ), the second effect dominates. Note that a noncontextual advantage appears only in a universe where the eavesdropper is noncontextual, but does not have access to the ontic state.

In the second case, the eavesdropper is quantum in both models, i.e., we allow the eavesdropper in the noncontextual setting more power. As may be expected, quantum devices are then always at least as powerful as noncontextual ones, with a quantum-over-noncontextual advantage appearing for all values of Δ whenever none of the inputs are unambiguously identified.

The maximal quantum advantage in terms of generating unpredictable (random) measurement outputs for a quantum

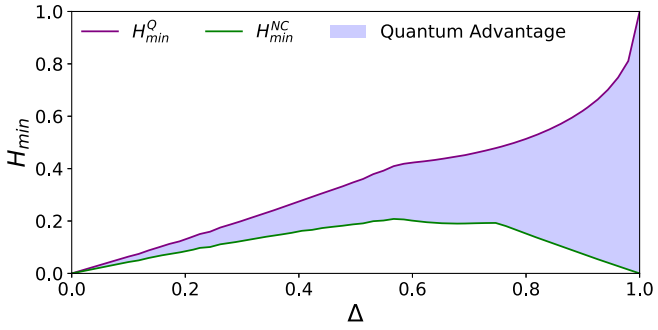

FIG. 3. Minimum entropy corresponding to the output rates with maximal quantum advantage, for quantum and noncontextual discrimination schemes and a quantum eavesdropper.

eavesdropper is plotted against the confusability in Fig. 3. The quantum advantage is largest for nearly indistinguishable states (similar to what was found in Ref. [39]). The eavesdropper's available strategies become more constrained when the optimal confidence has to be reproduced. In a noncontextual scenario, the constraint on the eavesdropper's strategies grows weaker for both nearly distinguishable and indistinguishable states.

In conclusion, we have computed the amount of randomness which can be semi-device-independently certified in maximum-confidence state discrimination setups in both quantum and preparation-noncontextual models. We have derived the maximal randomness within each model, and we find a quantum advantage for MCD-based randomness generation against quantum adversaries. When the adversary in the noncontextual setting is constrained to be noncontextual as well, we find a quantum advantage when the prepared states are difficult to distinguish, but a noncontextual advantage when they are easy to distinguish. In the future, it would be interesting to extend these results to settings with more than two inputs, where more randomness can potentially be generated, and to mixed-state preparations, where correlations between the prepared states and the eavesdropper potentially need to be taken into account.

J. B. B. and C. R. C. were supported by the Independent Research Fund Denmark and a KAIST-DTU Alliance stipend. K. F., H. L., and J. B. were supported by National Research Foundation of Korea (NRF-2021R1A2C2006309), Institute of Information & communications Technology Planning & Evaluation (IITP) grant (Grant No. 2019-0-00831, the ITRC Program/IITP-2022-2018-0-01402).

*crica@dtu.dk

[1] B. Hayes, Randomness as a resource, Am. Sci. **89**, 300 (2001).
[2] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, Randomness in quantum mechanics: Philosophy, physics and technology, Rep. Prog. Phys. **80**, 124001 (2017).
[3] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. Thesis, University of Cambridge, 2009, arXiv:0911.3814.
[4] S. Pironio, A. Acín, A. Massar, S. andBoyer de la Giroday, 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).
[5] A. Acín and L. Masanes, Certified randomness in quantum physics, Nature (London) **540**, 213 (2016).
[6] J. Bell, On the Einstein Podolsky Rosen paradox, Physics **1**, 195 (1964).
[7] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).
[8] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Detection-Loophole-Free Test of Quantum Nonlocality, and Applications, Phys. Rev. Lett. **111**, 130406 (2013).
[9] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent quantum random-number generation, Nature (London) **562**, 548 (2018).
[10] 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).
[11] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. 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).
[12] 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).
[13] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, Phys. Rev. A **84**, 034301 (2011).
[14] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Quantum randomness certified by the uncertainty principle, Phys. Rev. A **90**, 052327 (2014).
[15] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Self-Testing Quantum Random Number Generator, Phys. Rev. Lett. **114**, 150501 (2015).
[16] P. Mironowicz, G. Cañas, J. Cariñe, E. S. Gómez, J. F. Barra, A. Cabello, G. B. Xavier, G. Lima, and M. Pawłowski, Quantum randomness protected against detection loophole attacks, Quantum Inform. Process. **20**, 39 (2021).
[17] Z. Cao, H. Zhou, and X. Ma, Loss-tolerant measurement-device-independent quantum random number generation, New J. Phys. **17**, 125011 (2015).
[18] D. G. Marangon, G. Vallone, and P. Villoresi, Source-Device-Independent Ultrafast Quantum Random Number Generation, Phys. Rev. Lett. **118**, 060503 (2017).
[19] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Source-Independent Quantum Random Number Generation, Phys. Rev. X **6**, 011020 (2016).
[20] F. Xu, J. H. Shapiro, and F. N. C. Wong, Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring, Optica **3**, 1266 (2016).
[21] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, Phys. Rev. Applied **7**, 054018 (2017).

[22] T. Michel, J. Haw, D. Marangon, O. Thearle, G. Vallone, P. Villoresi, P. Lam, and S. Assad, Real-Time Source Independent Quantum Random Number Generator with Squeezed States, Phys. Rev. Applied **12**, 034017 (2019).
[23] D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, Self-testing quantum random-number generator based on an energy bound, Phys. Rev. A **100**, 062338 (2019).
[24] 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).
[25] S. Kochen and E. Specker, The problem of hidden variables in quantum mechanics, Indiana University mathematics Journal **17**, 59 (1967).
[26] C. Budroni, A. Cabello, O. Gühne, M. Kleinmann, and J. Å. Larsson, Quantum contextuality, arXiv:2102.13036.
[27] R. W. Spekkens, Contextuality for preparations, transformations, and unsharp measurements, Phys. Rev. A **71**, 052108 (2005).
[28] S. Croke, E. Andersson, S. M. Barnett, C. R. Gilson, and J. Jeffers, Maximum Confidence Quantum Measurements, Phys. Rev. Lett. **96**, 070401 (2006).
[29] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Megahertz-Rate Semi-Device-Independent Quantum Random Number Generators Based on Unambiguous State Discrimination, Phys. Rev. Applied **7**, 054018 (2017).
[30] D. Schmid and R. W. Spekkens, Contextual Advantage for State Discrimination, Phys. Rev. X **8**, 011015 (2018).
[31] K. Flatt, H. Lee, C. R. i Carceller, J. B. Brask, and J. Bae, Contextual advantages and certification for maximum confidence discrimination, arXiv:2112.09626.
[32] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[33] S. M. Barnett and S. Croke, Quantum state discrimination, Adv. Opt. Photonics **1**, 238 (2009).
[34] R. W. Spekkens, Negativity and Contextuality are Equivalent Notions of Nonclassicality, Phys. Rev. Lett. **101**, 020401 (2008).
[35] R. Konig, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[36] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.129.050501 for quantum vs noncontextual semi-device-independent randomness certification, which includes Refs. [37,38].
[37] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Self-testing nonprojective quantum measurements in prepare-and-measure experiments, Sci. Adv. **6**, eaaw6664 (2020).
[38] J.-D. Bancal, L. Sheridan, and V. Scarani, More randomness from the same data, New J. Phys. **16**, 033011 (2014).
[39] M. Ioannou, J. B. Brask, and N. Brunner, Upper bound on certifiable randomness from a quantum black-box device, Phys. Rev. A **99**, 052338 (2019).