Published in final edited form as:
Phys Rev A (Coll Park). 2018 ; A98: . doi:10.1103/PhysRevA.98.040304.

Certifying Quantum Randomness by Probability Estimation

Yanbao Zhang[1,*], **Emanuel Knill**[2,3], **Peter Bierhorst**[2,4]

[1]NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan

[2]National Institute of Standards and Technology, Boulder, Colorado 80305, USA

[3]Center for Theory of Quantum Matter, University of Colorado, Boulder, Colorado 80309, USA

[4]Mathematics Department, University of New Orleans, New Orleans, Louisiana 70148, USA

Abstract

We introduce probability estimation, a broadly applicable framework to certify randomness in a finite sequence of measurement results without assuming that these results are independent and identically distributed. Probability estimation can take advantage of verifiable physical constraints, and the certification is with respect to classical side information. Examples include randomness from single-photon measurements and device-independent randomness from Bell tests. Advantages of probability estimation include adaptability to changing experimental conditions, unproblematic early stopping when goals are achieved, optimal randomness rates, applicability to Bell tests with small violations, and unsurpassed finite-data efficiency. We greatly reduce latencies for producing random bits and formulate an associated rate-tradeoff problem of independent interest. We also show that the latency is determined by an information-theoretic measure of nonlocality rather than the Bell violation.

Randomness is a key enabling resource for computation and communication. Besides being required for Monte-Carlo simulations and statistical sampling, private random bits are needed for initiating authenticated connections and establishing shared keys, both common tasks for browsers, servers and other online entities [1]. Public random bits from "randomness beacons" have applications to fair resource sharing [2] and can seed private randomness sources based on quantum mechanics [3]. Common requirements for random bits are that they are unpredictable to all before they are generated, and private to the users before they are published.

Quantum mechanics provides natural opportunities for generating randomness. The best known example involves measuring a two-level system that is in an equal superposition of its two levels. A disadvantage of such schemes is that they require trust in the measurement apparatus, and undiagnosed failures are always a possibility. This disadvantage is overcome by a loophole-free Bell test [4, 5], which can generate output whose randomness can be certified solely by statistical tests of setting and outcome frequencies. The devices preparing the quantum states and performing the measurements may come from an untrusted source.

* yanbaoz@gmail.com.

This strategy for certified randomness generation is known as device-independent randomness generation (DIRG).

Loophole-free Bell tests have been realized with nitrogen-vacancy (NV) centers [6], with atoms [7] and with photons [8, 9], enabling the possibility of full experimental implementations of DIRG. However, for NV centers and atoms, the rate of trials is too low, and for photons, the violation per trial is too small. As a result, previously available DIRG protocols [3, 10–18] are not ready for implementation with current loophole-free Bell tests. These protocols do not achieve good finite-data efficiency and therefore require an impractical number of trials. Experimental techniques will improve, but for many applications of randomness generation, including randomness beacons and key generation, it is desirable to achieve finite-data efficiency that is as high as possible, since these applications often require short blocks of fresh random bits with minimum delay or latency.

Excellent finite-data efficiency was achieved by a method that we described and implemented in Refs. [19, 20], which reduced the time required for generating 1024 low-error random bits with respect to classical side information from hours to minutes for a state-of-the-art photonic loophole-free Bell test. The method in Refs. [19, 20] is based on the prediction-based ratio (PBR) analysis [21] for hypothesis tests of local realism. Specifically, in Refs. [19, 20] we established a connection between the PBR-based p-value and the amount of randomness certified against classical side information. The basis for success of the method of Refs. [19, 20] motivates our development of probability estimation for randomness certification, with better finite-data efficiency and with broader applications.

In the probability estimation framework, the amount of certified randomness is *directly* estimated without relying on hypothesis tests of local realism. To certify randomness, we first obtain a bound on the conditional probability of the observed outcomes given the chosen settings, valid for all classical side information. Then we show how to obtain conditional entropy estimates from this bound to quantify the number of extractable random bits [22]. By focusing on data-dependent probability estimates, we are able to take advantage of powerful statistical techniques to obtain the desired bound. The statistical techniques are based on test supermartingales [23] and Markov's bounds. Probability estimation inherits several features of the theory of test supermartingales. For example, probability estimation has no independence or stationarity requirement on the probability distribution of trial results. Also, probability estimation supports stopping the experiment early, as soon as the randomness goal is achieved.

Probability estimation is broadly applicable. In particular it is not limited to device-independent scenarios and can be applied to traditional randomness generation with quantum devices. Such applications are enabled by the notion of models, which are sets of probability distributions that capture verified, physical constraints on device behavior. In the case of Bell tests, these constraints include the familiar non-signaling conditions [24, 25]. In the case of two-level systems such as polarized photons, the constraints can capture that measurement angles are within a known range, for example.

In this paper, we first describe the technical features of probability estimation and the main results that enable its practical use. We propose a general information-theoretic rate-tradeoff problem that closely relates to finite-data efficiency. We then show how the general theoretical concepts are instantiated in experimentally relevant examples involving Bell-test configurations. We demonstrate advantages of probability estimation such as its optimal asymptotic randomness rates and show large improvements in finite-data efficiency, which corresponds to great reductions in latency.

Theory.

Consider an experiment with "inputs" **Z** and "outputs" **C**. The inputs normally consist of the random choices made for measurement settings but may include choices of state preparations such as in the protocols of Refs. [26, 27]. The outputs consist of the corresponding measurement outcomes. In the cases of interest, the inputs and outputs are obtained in a sequence of n time-ordered trials, where the ith trial has input Z_i and output C_i, and $\mathbf{Z} = (Z_i)_{i=1}^{n}$ and $\mathbf{C} = (C_i)_{i=1}^{n}$. We assume that Z_i and C_i are countable-valued. We refer to the trial inputs and outputs collectively as the trial "results", and to the trials preceding the upcoming one as the "past". The party with respect to which the randomness is intended to be unpredictable is represented by an external classical system, whose initial state before the experiment may be correlated with the devices used. The classical system carries the side information E, which is assumed to be countable-valued. After the experiment, the joint of **Z**, **C** and E is described by a probability distribution μ. The upper-case symbols introduced in this paragraph are treated as random variables. As is conventional, their values are denoted by the corresponding lower-case symbols.

The amount of extractable uniform randomness in **C** conditional on both **Z** and E is quantified by the (classical) smooth conditional min-entropy $H_{\min}^{\epsilon}(\mathbf{C} \mid \mathbf{Z}E)_{\mu}$ where ϵ is the "error bound" (or "smoothness") and μ is the joint distribution of **Z**, **C** and E. One way to define the smooth conditional min-entropy is with the conditional guessing probability $P_{\text{guess}}(\mathbf{C}|\mathbf{Z}E)_{\mu}$ defined as the average over values **z** and e of the maximum conditional probability $\max_{\mathbf{c}} \mu(\mathbf{c}|\mathbf{z}e)$. The ϵ-smooth conditional min-entropy $H_{\min}^{\epsilon}(\mathbf{C} \mid \mathbf{Z}E)_{\mu}$ is the greatest lower bound of $-\log_2 P_{\text{guess}}(\mathbf{C}|\mathbf{Z}E)_{\mu'}$ for all distributions μ' within total-variation distance ϵ of μ. Our goal is to obtain lower bounds on $H_{\min}^{\epsilon}(\mathbf{C} \mid \mathbf{Z}E)_{\mu}$ with probability estimation.

The application of probability estimation requires a notion of models. A model $\mathscr{H}$ for an experiment is defined as the set of all probability distributions of **Z** and **C** achievable in the experiment conditionally on values e of E. If a joint distribution μ of **Z**, **C** and E satisfies that for all e, the conditional distributions $\mu(\mathbf{CZ}|e)$, considered as distributions of **Z** and **C**, are in $\mathscr{H}$, we say that the distribution μ satisfies the model $\mathscr{H}$.

To apply probability estimation to an experiment consisting of n time-ordered trials, we construct the model $\mathscr{H}$ for the experiment as a chain of models $\mathscr{C}_i$ for each individual trial i in the experiment. The trial model $\mathscr{C}_i$ is defined as the set of all probability distributions of

trial results C_iZ_i achievable at the ith trial conditionally on both the past trial results and the side information E. For example, for Bell tests, $\mathscr{C}_i$ may be the set of non-signaling distributions with uniformly random inputs. Let $\mathbf{z}_{<i} = (z_j)_{j=1}^{i-1}$ and $\mathbf{c}_{<i} = (c_j)_{j=1}^{i-1}$ be the results before the ith trial. The sequences $\mathbf{z}_{\leq i}$ and $\mathbf{c}_{\leq i}$ are defined similarly. The chained model $\mathscr{K}$ consists of all conditional distributions $\mu(\mathbf{CZ}|e)$ satisfying the following two conditions. First, at each trial i the conditional distributions $\mu(C_iZ_i|\mathbf{c}_{<i}\mathbf{z}_{<i}e)$ for all $\mathbf{c}_{<i}$, $\mathbf{z}_{<i}$ and e are in the trial model $\mathscr{C}_i$. Second, at each trial i the input Z_i is independent of the past outputs $\mathbf{C}_{<i}$ given E and the past inputs $\mathbf{Z}_{<i}$. The second condition prevents leaking information about the past outputs through the future inputs, which is necessary for certifying randomness in the outputs $\mathbf{C}$ conditional on both the inputs $\mathbf{Z}$ and the side information E. In the common situation where the inputs are chosen independently with distributions known before the experiment, the second condition is always satisfied.

Since the model $\mathscr{K}$ consists of all conditional distributions $\mu(\mathbf{CZ}|e)$ regardless of the value e, the analyses in the next paragraph apply to the worst-case conditional distribution over e. To simplify notation we normally write the distribution $\mu(\mathbf{CZ}|e)$ conditional on e as $\mu_e(\mathbf{CZ})$, abbreviated as μ_e.

To estimate the conditional probability $\mu_e(\mathbf{c}|\mathbf{z})$, we design trial-wise probability estimation factors (PEFs) and multiply them. Consider a generic trial with trial model $\mathscr{C}$, where for generic trials, we omit the trial index. Let $\beta > 0$. A PEF with power β for $\mathscr{C}$ is a function F: $cz \mapsto F(cz) \geq 0$ such that for all $\sigma \in \mathscr{C}$, $\mathbb{E}_\sigma(F(CZ)\sigma(C \mid Z)^\beta) \leq 1$, where $\mathbb{E}$ denotes the expectation functional. Note that $F(cz) = 1$ for all cz defines a valid PEF with each positive power. For each i, let F_i be a PEF with power β for the ith trial, where the PEF can be chosen adaptively based on the past results $\mathbf{c}_{<i}\mathbf{z}_{<i}$. Other information from the past may also be used, see Ref. [28]. Let $T_0 = 1$ and $T_i = \prod_{j=1}^{i} F_j(C_jZ_j)$. The final value T_n of the running product T_i, where n is the total number of trials in the experiment, determines the probability estimate. Specifically, for each value e of E, each μ_e in the chained model $T_i = \Pi_{j=1}^{i} F_j(C_jZ_j)$, and $\epsilon > 0$, we have

$$\mathbb{P}_{\mu_e}(\mu_e(\mathbf{C}|\mathbf{Z}) \geq U(\mathbf{CZ})) \leq \epsilon, \tag{1}$$

where $\mathbb{P}_{\mu_e}$ denotes the probability according to the distribution μ_e and $U(\mathbf{CZ}) = (\epsilon T_n)^{-1/\beta}$. The proof of Eq. (1) is given in Appendix C1. The meaning of Eq. (1) is as follows: For each e and each $\mu_e \in \mathscr{K}$, the probability that $\mathbf{C}$ and $\mathbf{Z}$ take values $\mathbf{c}$ and $\mathbf{z}$ for which $U(\mathbf{C} = \mathbf{c}, \mathbf{Z} = \mathbf{z}) \leq \mu_e(\mathbf{C} = \mathbf{c}|\mathbf{Z} = \mathbf{z})$ is at most ϵ. This defines $U(\mathbf{CZ}) = (\epsilon T_n)^{-1/\beta}$ as a level-ϵ probability estimator.

A main theorem of probability estimation is the connection between probability estimators and conditional min-entropy estimators, which is formalized as follows:

Theorem 1. *Suppose that the joint distribution μ of $\mathbf{Z}$, $\mathbf{C}$ and E satisfies the chained model $\mathscr{K}$. Let $1 \geq \varkappa$, $\epsilon > 0$ and $1 \geq p \geq 1/|\mathrm{Rng}(\mathbf{C})|$, where $|\mathrm{Rng}(\mathbf{C})|$ is the number of possible*

outputs. Define $\{\phi\}$ *to be the event that* $T_n \geq 1/(p^\beta \epsilon)$, *and let* $\kappa \leq \mathbb{P}_\mu(\phi)$. *Then the smooth conditional min-entropy satisfies*

$$H_{\min}^{\epsilon}(\mathbf{C}|\mathbf{Z}E;\phi) \geq -\log_2(p/k^{1+1/\beta}).$$

The probability of the event $\{\phi\}$ can be interpreted as the probability that the experiment succeeds, and κ is an assumed lower bound on the success probability. The theorem is proven in Appendix C2.

When constructing PEFs, the power $\beta > 0$ must be decided *before* the experiment and cannot be adapted. Thm. 1 requires that p, ϵ and κ also be chosen *beforehand*, and success of the experiment requires $T_n \geq 1/(p^\beta \epsilon)$, or equivalently,

$$\log_2(T_n)/\beta + \log_2(\epsilon)/\beta \geq -\log_2(p). \tag{2}$$

Since $\log_2(T_n) = \sum_i \log_2(F_i)$, *before* the experiment we choose PEFs in order to aim for large expected values of the logarithms of the PEFs F_i. Consider a generic next trial with results CZ and model $\mathscr{C}$. Based on prior calibrations or the frequencies of observed results in past trials, we can determine a distribution $\nu \in \mathscr{C}$ that is a good approximation to the distribution of the next trial's results CZ. Many experiments are designed so that each trial's distribution is close to ν. The PEF can be optimized for this distribution but, by definition, is valid regardless of the actual distribution of the next trial in $\mathscr{C}$. Thus, one way to optimize PEFs *before* the next trial is as follows:

$$\begin{aligned} &\text{Max:} \quad \mathbb{E}_\nu(n\log_2(F(CZ))/\beta + \log_2(\epsilon)/\beta) \\ &\text{With:} \quad \sum_{cz} F(cz)\sigma(c|z)^\beta \sigma(cz) \leq 1 \text{ for all } \sigma \in \mathscr{C}, \\ &F(cz) \geq 0, \text{for all } cz. \end{aligned} \tag{3}$$

The objective function is strictly concave and the constraints are linear, so there is a unique maximum, which can be found by convex programming. More details are available in Appendix E.

Before the experiment, one can also optimize the objective function in Eq. (3) with respect to the power β. During the experiment ϵ and β are fixed, so it suffices to maximize $\mathbb{E}_\nu(\log_2(F(CZ)))$. If during the experiment, the running product T_i with $i < n$ exceeds the target $1/(p^\beta \epsilon)$, we can set future PEFs to $F(CZ) = 1$, which is a valid PEF with power β. This ensures that $T_n = T_i$ and is equivalent to stopping the experiment after trial i. Since the target needs to be set conservatively in order to make the actual experiment succeed with high probability, this can result in a significant reduction in the number of trials actually executed.

A question is how PEFs perform asymptotically for a stable experiment. This question is answered by determining the rate per trial of entropy production assuming constant ϵ and κ independent of the number of trials. In view of Thm. 1, after n trials the entropy rate is given by $(-\log_2(p) + \log_2(\kappa^{1+1/\beta}))/n$. Considering Eq. (2), when n is large the entropy rate is

dominated by $\log_2(T_n)/(n\beta)$, which is equal to $\Sigma_{i=1}^{n}\log_2(F_i)\,/\,(n\beta)$. Therefore, if each trial has distribution ν and each trial model is the same $\mathscr{C}$, then in the limit of large n the asymptotic entropy rate witnessed by a PEF F with power β is given by $\mathbb{E}_\nu(\log_2(F(CZ))\,/\,\beta)$. Define the rate

$$g(\beta) = \sup_F \mathbb{E}_\nu(\log_2(F(CZ))/\beta), \tag{4}$$

where the supremum is over PEFs F with power β for $\mathscr{C}$. The maximum asymptotic entropy rate at constant ϵ and κ witnessed by PEFs is $g_0 = \sup_{\beta>0} g(\beta)$. The rate $g(\beta)$ is non-increasing in β (see Appendix D), so g_0 is determined by the limit as β goes to zero. A theorem proven in Ref. [28] is that g_0 is the worst-case conditional entropy $H(C|ZE)$ over joint distributions of CZE allowed by $\mathscr{C}$ with marginal ν. Since this is a tight upper bound on the asymptotic randomness rate [29], probability estimation is asymptotically optimal and we identify g_0 as the asymptotic randomness rate. We also remark that probability estimation enables exponential expansion of input randomness [28].

For finite data and applications requiring fresh blocks of randomness, the rate g_0 is not achieved. To understand why, consider the problem of certifying a fixed number of bits b of randomness at error bound ϵ and with as few trials as possible, where each trial has distribution ν. In view of Thm. 1, the PEF optimization problem in Eq. (3), and the definition of $g(\beta)$ in Eq. (4), n needs to be sufficiently large so that

$$ng(\beta) + \log_2(\epsilon)/\beta + (1 + 1/\beta)\log_2(\kappa) \geq b\,. \tag{5}$$

The left-hand side is maximized at positive β, whereas $g(\beta)$ increases to g_0 as β goes to zero. As a result the best actual rate b/n is less than g_0.

Setting $\kappa = 1$ in Eq. (5) shows that the number of trials n must exceed $-\log_2(\epsilon)/(\beta g(\beta))$ before randomness can be produced, which suggests that the maximum of $\beta g(\beta)$ is a good indicator of finite-data performance. Another way to arrive at this quantity is to consider $\epsilon = 2^{-\gamma n}$, where $\gamma > 0$ is the "certificate rate". Given ν and the trial model, we can ask for the maximum certificate rate for which it is possible to have positive entropy rate at $\kappa = 1$. It follows from Eq. (5) with $\kappa = 1$ that this rate is at most

$$\gamma_{\mathrm{PEF}} = \sup_{\beta>0} \beta g(\beta)\,. \tag{6}$$

We propose a general information-theoretic rate-tradeoff problem given trial model $\mathscr{C}$ and $\nu \in \mathscr{C}$: For a given certificate rate γ, determine the supremum of the entropy rates achievable by protocols. Eq. (5) implies lower bounds on the resulting tradeoff curve.

Our protocol assumes classical-only side information. There are more costly DIRG protocols that handle quantum side information [11, 13–17], but verifying that side information is effectively classical only requires confirming that the quantum devices used in the experiment have no long-term quantum memory. Verifying the absence of long-term

quantum memory in current experiments is possibly less difficult than ensuring that there are no backdoors or information leaks in the experiment's hardware and software.

Applications.

We consider DIRG with the standard two-party, two-setting, two-outcome Bell-test configuration [30]. The parties are labeled A and B. In each trial, a source prepares a state shared between the parties, and each party chooses a random setting (their input) and obtains a measurement outcome (their output). We write $Z = XY$, where X and Y are the inputs of A and B, and $C = AB$, where A and B are the respective outputs. For this configuration, $A, B, X, Y \in \{0,1\}$.

Consider the trial model $\mathcal{N}$ consisting of distributions of $ABXY$ with uniformly random inputs and satisfying non-signaling [24]. We begin by determining and comparing the asymptotic randomness rates witnessed by different methods. The rates are usually quantified as functions of the expectation $\hat{I}$ of the C-HSH Bell function (Eq. G4) for $\hat{I} > 2$ (the classical upper bound). We prove in Appendix G that the maximum asymptotic randomness rate for any $\nu \in \mathcal{N}$ is equal to $(\hat{I} - 2) / 2$, and the rate g_0 witnessed by PEFs matches this value. Most previous studies, such as Refs. [3, 10, 12, 18, 31–33], estimate the asymptotic randomness rate by the singletrial conditional min-entropy $H_{\min}(AB|XYE)$. We determine that $H_{\min}(AB \mid XY\ E) = -\log_2((6 - \hat{I}) / 4) < g_0$ when $2 < \hat{I} < 4$. As $\hat{I}$ decreases to 2 the ratio of g_0 to $H_{min}(AB|XYE)$ approaches 1.386, demonstrating an improvement at small violations.

Next, we investigate finite-data performance. We consider three different families of quantum-achievable distributions of trial results. For the first family $\nu_{\mathrm{E},\theta}$, A and B share the unbalanced Bell state $|\Phi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $\theta \in (0, \pi/4]$ and apply projective measurements that maximize $\hat{I}$. This determines $\nu_{\mathrm{E},\theta}$. This family contains the goal states for many experiments suffering from detector inefficiency. For the second family $\nu_{\mathrm{W},p}$, A and B share a Werner state $\rho = p\,|\Psi_{\pi/4}\rangle\langle\Psi_{\pi/4}| + (1-p)\mathbb{1}/4$ with $p \in (1/\sqrt{2}, 1]$ and again apply measurements that maximize $\hat{I}$. Werner states are standard examples in quantum information and are among the worst states for our application. In experiments with photons, measurements are implemented with imperfect detectors. For the third family $\nu_{\mathrm{P},\eta}$, A and B use detectors with efficiency $\eta \in (2/3, 1)$ to implement the measurements and to close the detection loophole [34]. They choose the unbalanced Bell state $|\Phi_\theta\rangle$ and measurements such that an information-theoretic measure of nonlocality, the statistical strength for rejecting local realism [35–37], is maximized.

For each family of distributions, we determine the maximum certificate rate γ_{PEF} as given in Eq. (6). For this, we consider the trial model $\mathcal{N}$, but we note that γ_{PEF} does not depend on the specific constraints on the quantum-achievable conditional distributions $\mathbb{P}(AB \mid XY)$ (see Appendix F). As an indicator of finite-data performance, γ_{PEF} depends not only on $\hat{I}$, but also on the distribution ν. To illustrate this behavior, we plot the rates γ_{PEF} as a function of $\hat{I}$ for each family of distributions in Fig. 1. To obtain these plots, we note that $\hat{I}$ is a monotonic function of the parameter θ, p or η for each family. We also find that γ_{PEF} is

given by the statistical strength of the distribution ν for rejecting local realism (see Appendix F for a proof). Conventionally, experiments are designed to maximize $\hat{I}$, but in general, the optimal state and measurements maximizing $\hat{I}$ are different from those maximizing the statistical strength [36, 37].

We further determine the minimum number of trials, $n_{\mathrm{PEF},b}$, required to certify b bits of ϵ-smooth conditional min-entropy with a given distribution ν of trial results. From Eq. (5), we get

$$n_{\mathrm{PEF},\,b} = \inf_{\beta > 0} \frac{b\beta - \log_2(\epsilon) - (1+\beta)\log_2(\kappa)}{\beta g(\beta)},$$

where for simplicity we allow non-integer values for $n_{\mathrm{PEF},b}$. We can upper bound $n_{\mathrm{PEF},b}$ by means of the simpler-to-compute certificate rate γ_{PEF} given in Eq. (6). For the trial model $\mathcal{N}$, γ_{PEF} is achieved when β is above a threshold β_0 that depends on ν (see Appendix F). From γ_{PEF} and β_0, we can determine the upper bound

$$n'_{\mathrm{PEF},\,b} = (b\beta_0 - \log_2(\epsilon) - (1+\beta_0)\log_2(\kappa))/\gamma_{\mathrm{PEF}}$$

on $n_{\mathrm{PEF},b}$. The minimum number of trials required can be determined for other published protocols, which usually certify conditional min-entropy from $\hat{I}$. (An exception is Ref. [18] but the minimum number of trials required is worse.) We consider the protocol "PM" of Ref. [3] and the entropy accumulation protocol "EAT" of Ref. [17]. From Thm. 1 of Ref. [3] with $\kappa = 1$ and $b \searrow 0$, we obtain a lower bound

$$n_{\mathrm{PM},\,0} = -2\log_e(\epsilon)/((\hat{I}-2)/(4+2\sqrt{2}))^2.$$

For the EAT protocol, we determine an explicit lower bound $n_{\mathrm{EAT},b}$ in Appendix H. This lower bound applies for $b \geq 0$ and $\epsilon, \kappa, \in (0, 1]$, and is valid with respect to quantum side information for the trial model consisting of quantum-achievable distributions.

We compare the three protocols over a broad range of $\hat{I}$ for $b \searrow 0$, $\epsilon = 10^{-6}$, and $\kappa = 1$. For each family of distributions above, we compute the improvement factors given by $f_{\mathrm{PM}} = n_{\mathrm{PM},\,0} \,/\, n'_{\mathrm{PEF},\,0}$ and $f_{\mathrm{EAT}} = n_{\mathrm{EAT},\,0} \,/\, n'_{\mathrm{PEF},\,0}$. For $\nu_{\mathrm{W},p}$ the improvement factors depend weakly on $\hat{I}$: f_{PM} increases from 3.89 at $\hat{I} = 2.008$ to 4.36 at $\hat{I} = 2\sqrt{2}$, while f_{EAT} increases from 84.97 at $\hat{I} = 2.008$ to 86.35 at $\hat{I} = 2\sqrt{2}$. For $\nu_{\mathrm{E},\theta}$ and $\nu_{\mathrm{P},\eta}$, the improvement factors can be much larger and depend strongly on $\hat{I}$, monotonically decreasing with $\hat{I}$ as shown in Fig. 2. The improvement is particularly notable at small violations which are typical in current photonic loophole-free Bell tests. We remark that similar comparison results were obtained with other choices of the values for ϵ and κ.

The large latency reduction with probability estimation persists for certifying blocks of randomness. For randomness beacons, good reference values are $b = 512$ and $\epsilon = 2^{-64}$. We also set $\kappa = 2^{-64}$. Setting $\kappa = \epsilon$ is a common conservative choice, but we remark that

soundness for randomness generation can be defined with a better tradeoff between ϵ and κ [28]. We consider the trial model $\mathcal{T}$ of distributions with uniformly random inputs, satisfying both non-signaling conditions [24] and Tsirelson's bounds [38]. Consider the state-of-the-art photonic loophole-free Bell test reported in Ref. [20]. With probability estimation, the number of trials required for the distribution inferred from the measurement statistics is 4.668×10^7, which would require about 7.78 minutes of running time in the referenced experiment. With entropy accumulation [17], 2.887×10^{11} trials taking 802 hours would be required. For atomic experiments, we can use the distribution inferred from the measurement statistics in Ref. [7], for which probability estimation requires 7.354×10^4 trials, while entropy accumulation [17] requires 5.629×10^6. The experiment of Ref. [7] observed 1 to 2 trials per minute, so probability estimation would have needed at least 612.8 hours of data collection, which while impractical is still less than the 5.35 years required by entropy accumulation [17].

Finally, we briefly discuss the performance of probability estimation on DIRG with published Bell-test experimental data. The first experimental demonstration of conditional min-entropy certification for DIRG is reported in Ref. [10]. The method therein certifies the presence of 42 random bits at error bound $\epsilon = 10^{-2}$ against classical side information, where the trial model consists of quantum-achievable distributions with uniform inputs. (The lower bound of the protocol success probability $\kappa = 1$ was used implicitly in Ref. [10], so $\kappa = 1$ in the following comparison.) For the same data but with the less restrictive trial model $\mathcal{T}$, probability estimation certifies the presence of at least nine times more random bits with $\epsilon = 10^{-2}$. With $\epsilon = 10^{-6}$ probability estimation can still certify the presence of 80 random bits, while other methods fail to certify any random bits. For the loophole-free Bell-test data reported in Ref. [9] and analyzed in our previous work Ref. [19], the presence of 894 random bits at $\epsilon = 10^{-3}$ was certified against classical side information with the trial model $\mathcal{N}$. Further, 256 private random bits within 10^{-3} (in terms of the total-variation distance) of uniform were extracted in Ref. [19]. With probability estimation we can certify the presence of approximately two times more random bits at $\epsilon = 10^{-3}$. The presence of four times more bits can be certified if we use the more restrictive trial model $\mathcal{T}$. Furthermore, we can certify randomness even when the input distribution is not precisely known, which was an issue in the experiment of Ref. [9]. Applications to other experimental distributions, complete analyses of the mentioned experiments, and details on handling input choices whose probabilities are not precisely known are in Ref. [28].

In conclusion, probability estimation is a powerful and flexible framework for certifying randomness in data from a finite sequence of experimental trials. Implemented with probability estimation factors, it witnesses optimal asymptotic randomness rates. For practical applications requiring fixed-size blocks of random bits, it can reduce the latencies by orders of magnitude even for high-quality devices. Latency is a notable problem for device-independent quantum key generation (DIQKD). If probability estimation can be extended to accommodate security against quantum side information, the latency reductions may be extendable to DIQKD by means of existing constructions [17].

Finally we remark that if the trial results are explainable by local realism, no device-independent randomness would be certified by probability estimation. The reason is as

follows. For simplicity we assume that the input distribution is fixed and known [52]. Consider a generic trial with results CZ and model $\mathscr{C}$. Let $\mathscr{P}_{\mathrm{LR}}$ be the set of distributions of CZ explainable by local realism, which is a convex polytope with a finite number of extremal distributions $\sigma_{\mathrm{LR},k}$, $k = 1, 2, \ldots, K$. Since $\mathscr{P}_{\mathrm{LR}}$ is a subset of $\mathscr{C}$, by definition a PEF F with power β satisfies the condition

$$\sum_{cz} F(cz)\sigma_{\mathrm{LR},k}(c|z)^{\beta}\sigma_{\mathrm{LR},k}(cz) \leq 1, \tag{7}$$

for each k. For each extremal distribution $\sigma_{\mathrm{LR},k}$ in $\mathscr{P}_{\mathrm{LR}}$ and each cz, the value of $\sigma_{\mathrm{LR},k}(c|z)$ is either 0 or 1, from which it follows that $\sigma_{\mathrm{LR},k}(c|z)^{\beta}\,\sigma_{\mathrm{LR},k}(cz) = \sigma_{\mathrm{LR},k}(cz)$. Eq. (7) now becomes

$$\mathbb{E}_{\sigma_{\mathrm{LR},k}}(F(CZ)) = \sum_{cz} F(cz)\sigma_{\mathrm{LR},k}(cz) \leq 1. \tag{8}$$

Since any local realistic distribution can be written as a convex mixture of extremal distributions $\sigma_{\mathrm{LR},k}$, $k = 1, 2, \ldots, K$, Eq. (8) implies that for all distributions $\nu \in \mathscr{P}_{\mathrm{LR}}$

$$\mathbb{E}_{\nu}(F(CZ)) \leq 1. \tag{9}$$

By the concavity of the logarithm function and Eq. (9) we get that

$$\mathbb{E}_{\nu}(\log_2(F(CZ))) \leq \log_2(\mathbb{E}_{\nu}(F(CZ))) \leq 0.$$

Hence, the asymptotic entropy rate in Eq. (4) cannot be positive if the distribution of trial results is explainable by local realism. Furthermore, Eq. (9) shows that the PEF F is a test factor for the hypothesis test of local realism [21] (see Appendix B for the formal definition of test factors). So, if a finite sequence of trial results is explainable by local realism and F_i is a PEF with power β for the ith trial, according to Ref. [21] the success event $T_n \geq 1/(p^{\beta}\epsilon)$ with $T_n = \Pi_{i=1}^{n} F_i$ in Thm. 1 for randomness certification would happen with probability at most $p^{\beta}\epsilon$.

Acknowledgments

We thank D. N. Matsukevich for providing the experimental data for Ref. [10], Bill Munro, Carl Miller, Kevin Coakley, and Paulina Kuo for help with reviewing this paper. This work includes contributions of the National Institute of Standards and Technology, which are not subject to U.S. copyright.

Appendix

Appendix A: Notation

Much of this work concerns stochastic sequences, that is, sequences of random variables (RVs). RVs are functions on an underlying probability space. The range of an RV is called its value space and may be thought of as the set of its observable values or realizations. Here, all RVs have countable value spaces. We truncate sequences of RVs so that we only

consider finitely many RVs at a time. With this the underlying probability space is countable too. We use upper-case letters such as $A, B, \ldots, X, Y, \ldots$ to denote RVs. The value space of an RV such as X is denoted by $\mathrm{Rng}(X)$. The cardinality of the value space of X is $|\mathrm{Rng}(X)|$. Values of RVs are denoted by the corresponding lower-case letters. Thus x is a value of X, often thought of as the particular value realized in an experiment. When using symbols for values of RVs, they are implicitly assumed to be members of the range of the corresponding RV. In many cases, the value space is a set of letters or a set of strings of a given length. We use juxtaposition to denote concatenation of letters and strings. Stochastic sequences are denoted by capital bold-face letters, with the corresponding lower-case bold-face letters for their values. For example, we write $\mathbf{A} = (A_i)_{i=1}^{N}$ and $\mathbf{A}_{\leq m} = (A_i)_{i=1}^{m}$. Our conventions for indices are that we generically use N to denote a large upper bound on sequence lengths, n to denote the available length and i,j,k,l,m as running indices. By convention, $\mathbf{A}_{\leq 0}$ is the empty sequence of RVs. Its value is constant. When multiple stochastic sequences are in play, we refer to the collection of i'th RVs in the sequences as the data from the i'th trial. We typically imagine the trials as happening in time and being performed by an experimenter. We refer to the data from the trials preceding the upcoming one as the "past". The past can also include initial conditions and any additional information that may have been obtained. These are normally implicit when referring to or conditioning on the past.

Probabilities are denoted by $\mathbb{P}(\ldots)$. If there are multiple probability distributions involved, we disambiguate with a subscript such as in $\mathbb{P}_\nu(\ldots)$ or simply $\nu(\ldots)$, where ν is a probability distribution. We generally reserve the symbol μ for the global, implicit probability distribution, and may write $\mu(\ldots)$ instead of $\mathbb{P}(\ldots)$ or $\mathbb{P}_\mu(\ldots)$. Expectations are similarly denoted by $\mathbb{E}(\ldots)$ or $\mathbb{E}_\mu(\ldots)$. If ϕ is a logical expression involving RVs, then $\{\phi\}$ denotes the event where ϕ is true for the values realized by the RVs. For example, $\{f(X) > 0\}$ is the event $\{x : f(x) > 0\}$ written in full set notation. The brackets $\{\ldots\}$ are omitted for events inside $\mathbb{P}(\ldots)$ or $\mathbb{E}(\ldots)$. As is conventional, commas separating logical expressions are interpreted as conjunction. When the capital/lower-case convention can be unambiguously interpreted, we abbreviate "$X = x$" as "x". For example, with this convention, $\mathbb{P}(x, y) = \mathbb{P}(X = x, Y = y)$. Furthermore, we omit commas in the abbreviated notation, so $\mathbb{P}(xy) = \mathbb{P}(x, y)$. RVs or functions of RVs appearing outside an event but inside $\mathbb{P}(\ldots)$ or after the conditioner in $\mathbb{E}(\ldots \mid \ldots)$ result in an expression that is itself an RV. We can define these without complications because of our assumption that the event space is countable. Here are two examples. $\mathbb{P}(f(X) \mid Y)$ is a function of the RVs X and Y and can be described as the RV whose value is $\mathbb{P}(f(X) = f(x) \mid Y = y)$ whenever the values of X and Y are x and y, respectively. Similarly $\mathbb{E}(X \mid Y)$ is the RV defined as a function of Y, with value $\mathbb{E}(X \mid Y = y)$ whenever Y has value y. Note that X plays a different role before the conditioners in $\mathbb{E}(\ldots)$ than it does in $\mathbb{P}(\ldots)$, as $\mathbb{E}(X \mid Y)$ is not a function of X, but only of Y. We comment that conditional probabilities with conditioners having probability zero are not well-defined, but in most cases can be defined arbitrarily. Typically, they occur in a context where they are multiplied by the probability of the conditioner and thereby contribute zero regardless. An important context involves expectations, where we use the convention that when expanding an expectation over a set of values as a sum, zero-probability values are omitted. We do so without explicitly adding the constraints to the summation variables. We generally use

conditional probabilities without explicitly checking for probability-zero conditioners, but it is necessary to monitor for well-definedness of the expressions obtained.

To denote general probability distributions, usually on the joint value spaces of RVs, we use symbols such as μ, ν, σ, with modifiers as necessary. As mentioned, we reserve the unmodified μ for the distinguished global distribution under consideration, if there is one. Other symbols typically refer to probability distributions defined on the joint range of a subset of the available RVs. We usually just say "distribution" instead of "probability distribution". The terms "distributions on Rng(X)" and "distributions of X" are synonymous. If ν is a joint distribution of RVs, then we extend the conventions for arguments of $\mathbb{P}(\ldots)$ to arguments of ν, as long as all the arguments are determined by the RVs for which ν is defined. For example, if ν is a joint distribution of X, Y, and Z, then $\nu(x|y)$ has the expected meaning, as does the RV $\nu(X|Y)$ in contexts requiring no other RVs. Further, $\nu(X)$ and $\nu(XY)$ are the marginal distributions of X and XY, respectively, according to ν.

In our work, probability distributions are constrained by a "model", which is defined as a set of distributions and denoted by letters such as $\mathscr{H}$ or $\mathscr{C}$. The models for trials to be considered here are usually convex and closed.

The total-variation (TV) distance between ν and ν' is defined as

$$\mathrm{TV}(\nu,\nu') = \sum_x (\nu(x) - \nu'(x))[\![\nu(x) \geq \nu'(x)]\!] = \frac{1}{2}\sum_x |\nu(x) - \nu'(x)|, \tag{A1}$$

where $[\![\phi]\!]$ for a logical expression ϕ denotes the {0,1}-valued function evaluating to 1 iff ϕ is true. True to its name, the TV distance satisfies the triangle inequality. Here are three other useful properties: First, if ν and ν' are joint distributions of X and Y and the marginals satisfy $\nu(Y) = \nu'(Y)$, then the TV distance between ν and ν' is the average of the TV distances of the Y-conditional distributions:

$$\mathrm{TV}(v,v') = \sum_y v(y)\mathrm{TV}(v(X\,|\,y), v'(X\,|\,y))\,. \tag{A2}$$

Second, if for all y, the conditional distributions $\nu(X|y) = \nu'(X|y)$, then the TV distance between ν and ν' is given by the TV distance between the marginals on Y:

$$\mathrm{TV}(v,v') = \mathrm{TV}(v(Y), v'(Y))\,. \tag{A3}$$

Third, the TV distance satisfies the data-processing inequality. That is, for any stochastic process $\mathscr{E}$ on Rng(X) and distributions ν and ν' of X, $\mathrm{TV}(\mathscr{E}(\nu), \mathscr{E}(\nu')) \leq \mathrm{TV}(\nu,\nu')$. We use this property only for functions $\mathscr{E}$, but for general forms of this result, see Ref. [39]. The above properties of TV distances are well known, specific proofs can be found in Refs. [20, 28].

When constructing distributions close to a given one in TV distance, which we need to do for the proof of Thm. 1 in the main text, it is often convenient to work with subprobability distributions. A subprobability distribution of X is a sub-normalized non-negative measure on Rng(X), which in our case is simply a non-negative function $\tilde{\nu}$ on Rng(X) with weight

$w(\tilde{\nu}) = \Sigma_x \tilde{\nu}(x) \leq 1$. For expressions not involving conditionals, we use the same conventions for subprobability distributions as for probability distributions. When comparing subprobability distributions, $\tilde{\nu} \leq \tilde{\nu}'$ means that for all x, $\tilde{\nu}(x) \leq \tilde{\nu}'(x)$, and we say that $\tilde{\nu}'$ "dominates" $\tilde{\nu}$.

Lemma 2. *Let $\tilde{\nu}$ be a subprobability distribution of X of weight $w = 1 - \epsilon$. Let ν and ν' be distributions of X satisfying $\tilde{\nu} \leq \nu$ and $\tilde{\nu} \leq \nu'$. Then* $\mathrm{TV}(\nu, \nu') \leq \epsilon$.

Proof. Calculate

$$\begin{aligned} \mathrm{TV}(\nu, \nu') &= \sum_x (\nu(x) - \nu'(x)) [\![\nu(x) \geq \nu'(x)]\!] \\ &\leq \sum_x (\nu(x) - \tilde{\nu}(x)) [\![\nu(x) \geq \tilde{\nu}(x)]\!] \\ &= \sum_x (\nu(x) - \tilde{\nu}(x)) \\ &= 1 - w = \epsilon . \end{aligned}$$

Lemma 3. *Assume that $p \geq 1/|\mathrm{Rng}(X)|$. Let ν be a distribution of X and $\tilde{\nu} \leq \nu$ a subprobability distribution of X with weight $w = 1 - \epsilon$ and $\tilde{\nu} \leq p$. Then there exists a distribution ν' of X with $\nu' \geq \tilde{\nu}$, $\nu' \leq p$,* and $\mathrm{TV}(\nu, \nu') \leq \epsilon$.

Proof. Because $p \geq 1/|\mathrm{Rng}(X)|$, that is, $\sum_x p \geq 1$, and for all x, $\tilde{\nu}(x) \leq p$, there exists a distribution $\nu' \geq \tilde{\nu}$ with $\tilde{\nu} \leq p$. Since ν' and ν are distributions dominating $\tilde{\nu}$ and by Lem. 2, $\mathrm{TV}(\nu, \nu') \leq \epsilon$.

Appendix B: Test Supermartingales and Test Factors

Definition 4. *A* test supermartingale [23] with respect to a stochastic sequence $\mathbf{R}$ and model $\mathscr{H}$ *is a stochastic sequence* $\mathbf{T} = (T_i)_{i=0}^{N}$ *with the properties that 1) $T_0 = 1$, 2) for all i $T_i \geq 0$, 3) T_i is determined by $\mathbf{R}_{\leq i}$ and the governing distribution, and 4) for all distributions in $\mathscr{H}$, $\mathbb{E}(T_{i+1} \mid \mathbf{R}_{\leq i}) \leq T_i$. The ratios $F_i = T_i / T_{i-1}$ with $F_i = 1$ if $T_{i-1} = 0$ are called the* test factors of $\mathbf{T}$.

Here $\mathbf{R}$ captures the relevant information that accumulates in a sequence of trials. It does not need to be accessible to the experimenter. Between trials i and $i + 1$, the sequence $\mathbf{R}_{\leq i}$ is called the past. In the definition, we allow for T_i to depend on the governing distribution μ. With this, for a given μ, T_i is a function of $\mathbf{R}_{\leq i}$ Below, when stating that RVs are determined, we implicitly include the possibility of dependence on μ without mention. The μ-dependence can arise through expressions such as $\mathbb{E}_\mu(G \mid \mathbf{R}_{\leq i})$ for some G, which is determined by $\mathbf{R}_{\leq i}$ given μ. One way to formalize this is to consider μ-parameterized families of RVs. We do not make this explicit and simply allow for our RVs to be implicitly parameterized by μ. We note that the governing distribution in a given experiment or situation is fixed but usually unknown with most of its features inaccessible. As a result, many RVs used in mathematical arguments cannot be observed even in principle. Nevertheless, they play important roles in establishing relationships between observed and inferred quantities.

Defining $F_i = 1$ when $T_{i-1} = 0$ makes sense because given $\{T_{i-1} = 0\}$, we have $\{T_i = 0\}$ with probability 1. The sequence $\mathbf{F} = (F_i)_{i=1}^{N}$ satisfies the conditions that for all i, 1) $F_i \geq 0$, 2) F_i is determined by $\mathbf{R}_{\leq i}$ and 3) for all distributions in $\mathscr{H}$, $\mathbb{E}(F_{i+1} \mid \mathbf{R}_{\leq i}) \leq 1$. We can define test supermartingales in terms of such sequences: Let $\mathbf{F}$ be a stochastic sequence satisfying the three conditions. Then the stochastic sequence with members $T_0 = 1$ and $T_i = \Pi_{1 \leq j \leq i} F_j$ for $i \geq 1$ is a test supermartingale. It suffices to check that $\mathbb{E}(T_{i+1} \mid \mathbf{R}_{\leq i}) \leq T_i$. This follows from

$$\mathbb{E}(T_{i+1} \mid \mathbf{R}_{\leq i}) = \mathbb{E}(F_{i+1} T_i \mid \mathbf{R}_{\leq i}) = \mathbb{E}(F_{i+1} \mid \mathbf{R}_{\leq i}) T_i \leq T_i,$$

where we pulled out the determined quantity T_i from the conditional expectation. In this work, we construct test supermartingales from sequences $\mathbf{F}$ with the above properties. We refer to any such sequence as a sequence of test factors, without necessarily making the associated test supermartingale explicit. We extend the terminology by calling an RV F a test factor with respect to $\mathscr{H}$ if $F \geq 0$ and $\mathbb{E}(F) \leq 1$ for all distributions in $\mathscr{H}$. Note that $F = 1$ is a valid test factor.

For an overview of test supermartingales and their properties, see Ref. [23]. The notion of test supermartingales and proofs of their basic properties are due to Ville [40] in the same work that introduced the notion of martingales. The name “test supermartingale” appears to have been introduced in Ref. [23]. Test supermartingales play an important theoretical role in proving many results in martingale theory, including that of proving tail bounds for large classes of martingales. They have been studied and applied to Bell tests [21, 41, 42].

The definition implies that for a test supermartingale $\mathbf{T}$, for all n, $\mathbb{E}(T_n) \leq 1$. This follows inductively from $\mathbb{E}(T_{i+1}) = \mathbb{E}(\mathbb{E}(T_{i+1} \mid \mathbf{R}_{\leq i})) \leq \mathbb{E}(T_i)$ and $T_0 = 1$. An application of Markov’s inequality shows that for all $\epsilon > 0$,

$$\mathbb{P}(T_n \geq 1/\epsilon) \leq \epsilon\,. \tag{B1}$$

Thus, a large final value $t = T_n$ of the test supermartingale is evidence against $\mathscr{H}$ in a hypothesis test with $\mathscr{H}$ as the (composite) null hypothesis. Specifically, the RV $1/T$ is a p-value bound against $\mathscr{H}$, where in general, the RV U is a p-value bound against $\mathscr{H}$ if for all distributions in $\mathscr{H}$, $\mathbb{P}(U \leq \epsilon) \leq \epsilon$.

One can produce a test supermartingale adaptively by determining the test factors F_{i+1} to be used at the next trial. If the i’th trial’s data is R_i, including any incidental information obtained, then F_{i+1} is expressed as a function of $\mathbf{R}_{\leq i}$ and data from the $(i+1)$’th trial (a “past-parameterized” function of R_{i+1}), and constructed to satisfy $F_{i+1} \geq 0$ and $\mathbb{E}(F_{i+1} \mid \mathbf{R}_{\leq i}) \leq 1$ for any distribution in the model $\mathscr{H}$. Note that inbetween trials, we can effectively stop the experiment by assigning all future $F_{i+1} = 1$, which is a valid test factor, conditional on the past. This is equivalent to constructing the stopped process relative to a stopping rule. This argument also shows that the stopped process is still a test supermartingale.

More generally, we use test supermartingales for estimating lower bounds on products of positive stochastic sequences **G**. Such lower bounds are associated with unbounded-above confidence intervals. We need the following definition:

Definition 5. *Let U, V, X be RVs and $1 \geq \epsilon \geq 0$. $I = [U, V]$ is a* confidence interval for X at level ϵ with respect to $\mathscr{H}$ *if for all distributions in $\mathscr{H}$ we have $\mathbb{P}(U \leq X \leq V) \geq 1 - \epsilon$. The quantity $\mathbb{P}(U \leq X \leq V)$ is called the* coverage probability.

As noted above, the RVs U, V and X may be μ-dependent. For textbook examples of confidence intervals such as in Ch. 2.4.3 of Ref [43], X is a parameter determined by μ, and U and V are obtained according to a known distribution for an estimator of X. The quantity e in the definition is a significance level, which corresponds to a confidence level of $(1 - \epsilon)$. The following technical lemma will be used in the next section.

Lemma 6. *Let* **F** *and* **G** *be two stochastic sequences with $F_i \in [0, \infty)$, $G_i \in (0, \infty]$, and F_i and G_i determined by $\mathbf{R}_{\leq i}$. Define $T_0 = 1$, $T_i = \Pi_{1 \leq j \leq i} F_i$ and $U_0 = 1$, $U_i = \Pi_{1 \leq j \leq i} G_i$, and suppose that for all $\mu \in \mathscr{H}$, $\mathbb{E}(F_{i+1} / G_{i+1} \mid \mathbf{R}_{\leq i}) \leq 1$. Then $[T_n\epsilon, \infty)$ is a confidence interval for U_n at level ϵ with respect to $\mathscr{H}$.*

Proof. The assumptions imply that the sequence $(F_i / G_i)_{i=1}^{N}$ forms a sequence of test factors with respect to $\mathscr{H}$ and generate the test supermartingale **T/U**, where division in this expression is term-by-term. Therefore, by Eq. (B1),

$$\mathbb{P}(T_n\epsilon \geq U_n) = \mathbb{P}(T_n/U_n \geq 1/\epsilon) \leq \epsilon, \tag{B2}$$

so $[T_n\epsilon, \infty)$ is a confidence interval for U_n at level ϵ.

Appendix C: Proof of Main Results

In this section, we show how to perform probability estimation and how to certify smooth conditional min-entropy by probability estimation.

1. Probability Estimation by Test Supermartingales: Proof of Main Text Eq. (1)

We consider the situation where **CZ** is a time-ordered sequence of n trial results, and the classical side information is represented by an RV E with countable value space. In an experiment, **Z** and **C** are the inputs and outputs of the quantum devices, and the side information E is carried by an external classical system E. Before the experiment, the initial state of E may be correlated with the quantum devices. At each trial of the experiment, we allow arbitrary one-way communication from the system E to the devices. For example, E can initialize the state of the quantum devices via a one-way communication channel. We also allow the possibility that the device initialization at a trial by E depends on the past inputs preceding the trial. This implies that the random inputs **Z** can come from publicrandomness sources, as first pointed out in Ref. [3]. However, at any stage of the experiment the information of the outputs **C** cannot be leaked to the system E. After the experiment, we observe **Z** and **C**, but not the side information E.

A model $\mathscr{H}$ for an experiment is defined as the set of joint probability distributions of $\mathbf{CZ}$ that satisfy the known constraints and consists of all achievable probability distributions of $\mathbf{CZ}$ conditional on values e of E. Thus we say that a joint distribution μ of $\mathbf{CZ}$ and E satisfies the model $\mathscr{H}$ if $\mu(\mathbf{CZ} \mid E = e) \in \mathscr{H}$ for each value e.

We focus on probability estimates with lower bounds on coverage probabilities that do not depend on E. Our specific goal is to prove Eq. (1) in the main text. We will show that the probability bound of $U(\mathbf{CZ}) = (T_n\epsilon)^{-1/\beta}$ in Eq. (1) of the main text is an instance of what we call an "ϵ-uniform probability estimator":

Definition 7. Let $1 \geq \epsilon \geq 0$. *The function* U: $\mathrm{Rng}(\mathbf{CZ}) \rightarrow [0, \infty)$ *is a* level-ϵ E-uniform probability estimator for $\mathscr{H}$ (ϵ-UPE *or with specifics*, $\epsilon - \mathrm{UPE}(\mathbf{C} \mid \mathbf{Z}E; \mathscr{H})$) *if for all* e *and distributions* μ *satisfying the model* $\mathscr{H}$, we have $\mathbb{P}_\mu(U(\mathbf{CZ}) \geq \mu(\mathbf{C} \mid \mathbf{Z}e) \mid e) \geq 1 - \epsilon$. *We omit specifics such as* $\mathscr{H}$ *if they are clear from context.*

We can obtain ϵ-UPEs by constructing test supermartingales. In order to achieve this goal, we consider models $\mathscr{H}(\mathscr{C})$ of distributions of $\mathbf{CZ}$ constructed from a chain of trial models $\mathscr{C}_{i+1 \mid \mathbf{c}_{\leq i}\mathbf{z}_{\leq i}e}$, where the trial model $\mathscr{C}_{i+1 \mid \mathbf{c}_{\leq i}\mathbf{z}_{\leq i}e}$ is defined as the set of all achievable distributions of $C_{i+1}Z_{i+1}$ conditional on both the past results $\mathbf{c}_{\leq i}\mathbf{z}_{\leq i}$ and the value e of E. The chained model $\mathscr{H}(\mathscr{C})$ consists of all conditional distributions $\mu(\mathbf{CZ}|e)$ satisfying the following two properties. First, for all i, $\mathbf{c}_{\leq i}\mathbf{z}_{\leq i}$, and e, the conditional distributions

$$\mu(C_{i+1}Z_{i+1} \mid \mathbf{c}_{\leq i}\, \mathbf{z}_{\leq i}\, e) \in \mathscr{C}_{i+1 \mid \mathbf{c}_{\leq i}\mathbf{z}_{\leq i}e}.$$

Second, the joint distribution μ of $\mathbf{CZ}$ and E satisfies that Z_{i+1} is independent of $\mathbf{C}_{\leq i}$ conditionally on both $\mathbf{Z}_{\leq i}$ and E. The second condition is needed in order to be able to estimate $\mathbf{Z}E$-conditional probabilities of $\mathbf{C}$ and corresponds to the Markov-chain condition in the entropy accumulation framework [17].

In many cases, the trial models $\mathscr{C}_{i+1 \mid \mathbf{c}_{\leq i}\mathbf{z}_{\leq i}e}$ do not depend on the past outputs $\mathbf{c}_{\leq i}$, but probability estimation can take advantage of dependence on the past inputs $\mathbf{z}_{\leq i}$. Such dependence captures the possibility that at the $(i + 1)$'th trial the device initialization by the external classical system E depends on the past inputs $\mathbf{z}_{\leq i}$. In applications involving Bell-test configurations, the trial models capture constraints on the input distributions and on non-signaling or quantum behavior of the devices. For simplicity, we write $\mathscr{C}_{i+1} = \mathscr{C}_{i+1 \mid \mathbf{c}_{\leq i}\mathbf{z}_{\leq i}e}$, leaving the conditional parameters implicit. Normally, models for individual trials $\mathscr{C}_{i+1}$ are convex and closed. If they are not, we note that our results generally extend to the convex closures of the trial models used.

For chained models $\mathscr{H}(\mathscr{C})$, we can construct ϵ-UPEs from products of "probability estimation factors" according to the following definition, see also the paragraph containing Eq. (1) in the main text.

Definition 8. *Let $\beta > 0$, and let $\mathscr{C}$ be any model, not necessarily convex. A* probability estimation factor (PEF) with power β for $\mathscr{C}$ *is a non-negative RV $F = F(CZ)$ such that for all $\sigma \in \mathscr{C}$, $\mathbb{E}_\sigma(F\sigma(C \mid Z)^\beta) \leq 1$.*

We emphasize that a PEF is a function of the trial results CZ, but not of the side information E.

Consider the model $\mathscr{M}(\mathscr{C})$ constructed as a chain of trial models $\mathscr{C}_i$. Let F_i be PEFs with power $\beta > 0$ for $\mathscr{C}_i$, past-parameterized by $\mathbf{C}_{\leq i}$ and $\mathbf{Z}_{\leq i}$. Define $T_0 = 1$, $T_i = \Pi_{1 \leq j \leq i} F_j$ for $i \geq 1$, and

$$U(\mathbf{CZ}) = (T_n \epsilon)^{-1/\beta}. \tag{C1}$$

Then, $U(\mathbf{CZ})$ satisfies the inequality in Eq. (1) of the main text as proven in the following theorem, and is therefore an ϵ-UPE. To simplify notation in the following theorem, we normally write the distribution $\mu(\mathbf{CZ}|e)$ conditional on e as $\mu_e(\mathbf{CZ})$, abbreviated as μ_e.

Theorem 9. *Fix $\beta > 0$. For each value e of E, each $\mu_e \in \mathscr{M}(\mathscr{C})$, and $\epsilon > 0$, the following inequality holds:*

$$\mathbb{P}_{\mu_e}(\mu_e(\mathbf{C} \mid \mathbf{Z}) \geq (\epsilon T_n)^{-1/\beta}) \leq \epsilon. \tag{C2}$$

Note that β cannot be adapted during the trials. On the other hand, before the ith trial, we can design the PEFs F_i for the particular constraints relevant to the ith trial.

Proof. We first observe that for each value e of E,

$$\prod_{j=0}^{i-1} \mu_e(C_{j+1} \mid Z_{j+1} \mathbf{Z}_{\leq j} \mathbf{C}_{\leq j}) = \mu_e(\mathbf{C}_{\leq i} \mid \mathbf{Z}_{\leq i}). \tag{C3}$$

This follows by induction with the identity

$$\begin{aligned} &\mu_e(\mathbf{C}_{\leq j+1} \mid \mathbf{Z}_{\leq j+1}) = \mu_e(C_{j+1} \mid Z_{j+1} \mathbf{Z}_{\leq j} \mathbf{C}_{\leq j}) \mu_e(\mathbf{C}_{\leq j} \mid Z_{j+1} \mathbf{Z}_{\leq j}) \\ &= \mu_e(C_{j+1} \mid Z_{j+1} \mathbf{Z}_{\leq j} \mathbf{C}_{\leq j}) \mu_e(\mathbf{C}_{\leq j} \mid \mathbf{Z}_{\leq j}) \end{aligned}$$

by conditional independence of Z_{j+1} on $\mathbf{C}_{\leq j}$ given $\mathbf{Z}_{\leq j}$ and $E = e$.

We claim that for each e, $F_{i+1} \mu_e(C_{i+1} | Z_{i+1} \mathbf{Z}_{\leq i} \mathbf{C}_{\leq i})^\beta$ is a test factor determined by $\mathbf{C}_{\leq i+1} \mathbf{Z}_{\leq i+1}$. To prove this claim, for all $\mathbf{c}_{\leq i} \mathbf{z}_{\leq i}$, the distributions $\nu = \mu_e(C_{i+1} Z_{i+1} \mid \mathbf{c}_{\leq i} \mathbf{z}_{\leq i}) \in \mathscr{C}_{i+1}$. With $F_{i+1} = F_{i+1}(C_{i+1} Z_{i+1}; \mathbf{c}_{\leq i} \mathbf{z}_{\leq i})$, we obtain the bound

$$\begin{aligned} &\mathbb{E}(F_{i+1} \mu_e(C_{i+1} \mid Z_{i+1} \mathbf{z}_{\leq i} \mathbf{c}_{\leq i})^\beta \mid \mathbf{c}_{\leq i} \mathbf{z}_{\leq i}) = \mathbb{E}_\nu(F_{i+1} \nu(C_{i+1} \mid Z_{i+1})^\beta) \\ &\leq 1, \end{aligned}$$

where we invoked the assumption that F_{i+1} is a PEF with power β for $\mathscr{C}_{i+1}$. By arbitrariness of $\mathbf{c}_{\le i}\mathbf{z}_{\le i}$, and because the factors $F_{i+1}\mu_e(C_{i+1}|\mathbf{Z}_{\le i}\mathbf{C}_{\le i})^\beta$ are determined by $\mathbf{C}_{\le i+1}\mathbf{Z}_{\le i+1}$, the claim follows. The product of these test factors is

$$\begin{aligned}\prod_{j=0}^{i-1} F_{j+1}\mu_e(C_{j+1}\,|\,Z_{j+1}\mathbf{Z}_{\le j}\mathbf{C}_{\le j})^\beta &= T_i\prod_{j=0}^{i-1}\mu_e(C_{j+1}\,|\,Z_{j+1}\mathbf{Z}_{\le j}\mathbf{C}_{\le j})^\beta \\ &= T_i\mu_e(\mathbf{C}_{\le i}\,|\,\mathbf{Z}_{\le i})^\beta,\end{aligned} \tag{C4}$$

with $T_i = \prod_{j=1}^{i} F_j$. To obtain the last equality above, we used Eq. (C3). Thus, for each e, the sequence $Q_0 = 1$ and $Q_i = T_i\mu_e(\mathbf{C}_{\le i}|\mathbf{Z}_{\le i})^\beta$ for $i > 0$ satisfies the supermartingale property $\mathbb{E}_{\mu_e}(Q_{i+1}\,|\,\mathbf{C}_{\le i}\mathbf{Z}_{\le i}) \le Q_i$. We remark that as a consequence, $\mathbb{E}_{\mu_e}(Q_{i+1}) = \mathbb{E}_{\mu_e}(Q_{i+1}\,|\,\mathbf{C}_{\le i}\mathbf{Z}_{\le i})) \le \mathbb{E}_{\mu_e}(Q_i)$. By induction this gives $\mathbb{E}_{\mu_e}(Q_n) = \mathbb{E}_{\mu_e}(T_n\mu_e(\mathbf{C}\,|\,\mathbf{Z})^\beta) \le 1$. Thus, considering that $T_n = \prod_{i=1}^{n} F_i \ge 0$, T_n is a PEF with power β for $\mathscr{H}(\mathscr{C})$, that is, chaining PEFs yields PEFs for chained models.

In Lem. 6, if we replace T_i and U_i there by T_i and $\mu_e(\mathbf{C}_{\le i}|\mathbf{Z}_{\le i})^{-\beta}$ here, then from Eq. (B2) and manipulating the inequality inside $\mathbb{P}(\cdot)$, we get the inequality in Eq. (C2).

That F_{i+1} can be parameterized in terms of the past as $F_{i+1} = F_{i+1}(C_{i+1}Z_{i+1}; \mathbf{C}_{\le i}\mathbf{Z}_{\le i})$ allows for adapting the PEFs based on $\mathbf{CZ}$, but no other information can be used. To adapt the PEF F_{i+1} based on other past information besides $\mathbf{C}_{\le i}\mathbf{Z}_{\le i}$, we need a "soft" generalization of probability estimation as detailed in Ref. [28].

2. Smooth Min-Entropy by Probability Estimation: Proof of Main Text Thm. 1

We want to generate bits that are near-uniform conditional on E and often other variables such as $\mathbf{Z}$. For our analyses, E is not particularly an issue because our results hold uniformly for all values of E, that is, conditionally on $\{E = e\}$ for each e. However this is not the case for $\mathbf{Z}$. For this subsection, it is not necessary to structure the RVs as stochastic sequences, so below we use C and Z in place of $\mathbf{C}$ and $\mathbf{Z}$.

Definition 10. *The distribution μ of CZE has* ϵ-smooth average ZE-conditional maximum probability p *if there exists a distribution ν of CZE with* $\mathrm{TV}(\nu, \mu) \le \epsilon$ *and* $\sum_{ze}\max_c(\nu(c|ze))\nu(ze) \le p$. *The minimum p for which μ has ϵ-smooth average ZE-conditional maximum probability p is denoted by* $P^{\epsilon}_{\max,\mu}(C\,|\,ZE)$. *The quantity* $H^{\epsilon}_{\min,\mu}(C\,|\,ZE) = -\log_2(P^{\epsilon}_{\max,\mu}(C\,|\,ZE))$ *is the* (classical) ϵ-smooth ZE-conditional min-entropy.

We denote the ϵ-smooth ZE-conditional min-entropy evaluated conditional on an event $\{\phi\}$ by $H^{\epsilon}_{\min}(C\,|\,ZE;\phi)$. We refer to the smoothness parameters as "error bounds". Observe that the definitions are monotonic in the error bound. For example, if $P^{\epsilon}_{\max,\mu} \le p$ and $\epsilon' \ge \epsilon$, then $P^{\epsilon'}_{\max,\mu} \le p$. The quantity $\sum_{ze}\max_c(\nu(c|ze))\nu(ze)$ in the definition of $P^{\epsilon}_{\max,\mu}$ can be recognized as the (average) maximum guessing probability of C given Z and E (with respect to ν), whose negative logarithm is the guessing entropy defined, for example, in Ref. [44].

A summary of the relationships between smooth conditional min-entropies and randomness extraction with respect to quantum side information is given in Ref. [22] and can be specialized to classical side information. When so specialized, the definition of the smooth conditional min-entropy in, for example, Ref. [22] differs from the one above in that Ref. [22] uses one of the fidelity-related distances. One such distance reduces to the Hellinger distance h for probability distributions for which $h^2 \leq \mathrm{TV} \leq \sqrt{2}h$.

The Z-conditional maximum probabilities with respect to $E = e$ can be lifted to the ZE-conditional maximum probabilities, as formalized by the next lemma.

Lemma 11. *Suppose that for all e,* $P^{\epsilon_e}_{\max,\,\mu(CZ\,|\,e)}(C \mid Z) \leq p_e$, *and let* $\bar{\epsilon} = \Sigma_e \epsilon_e \mu(e)$ *and* $\bar{p} = \Sigma_e p_e \mu_e$. Then $P^{\bar{\epsilon}}_{\max,\,\mu(CZE)}(C \mid ZE) \leq \bar{p}$.

Proof. For each e, let ν_e witness $P^{\epsilon_e}_{\max,\,\mu(CZ\,|\,e)}(C \mid Z) \leq p_e$. Then $\mathrm{TV}(\nu_e, \mu(CZ|e)) \leq \epsilon_e$ and $\sum_z \max_c(\nu_e(c/z))\nu_e(z) \leq p_e$. Define ν by $\nu(cze) = \nu_e(cz)\mu(e)$. Then the marginals $\nu(E) = \mu(E)$, so we can apply Eq. (A2) for

$$\mathrm{TV}(\nu, \mu) = \sum_e \mathrm{TV}(\nu_e, \mu(CZ|e))\mu(e) \leq \sum_e \epsilon_e \mu(e) = \bar{\epsilon}.$$

Furthermore,

$$\sum_{ze} \max_c(\nu(c|ze))\nu(ze) = \sum_e \mu(e) \sum_z \max_c(\nu_e(c|z))\nu_e(z) \leq \sum_e \mu(e) p_e = \bar{p},$$

as required for the conclusion. □

The level of a probability estimator relates to the smoothness parameter for smooth min-entropy via the relationships established below.

Theorem 12. *Suppose that U is an* $\epsilon - \mathrm{UPE}(C \mid ZE; \mathcal{H})$ *and that the distribution* μ *of CZE satisfies the model* $\mathcal{H}$. *Let* $p \geq 1/|\mathrm{Rng}(C)|$ *and* $\kappa = \mu(U \leq p)$. *Then* $P^{\epsilon/\kappa}_{\max,\,\mu(CZE\,|\,U \leq p)}(C \mid ZE) \leq p \,\big/\, \kappa$.

Proof. Let $\kappa_e = \mu(U \leq p/e)$. Below we show that for all values e of E, $P^{\epsilon/\kappa_e}_{\max,\,\mu(CZ\,|\,e,U \leq p)}(C \mid Z) \leq p \,\big/\, \kappa_e$. Once this is shown, we can use

$$\sum_e \frac{1}{\kappa_e}\mu(e|U \leq p) = \sum_e \frac{1}{\mu(U \leq p|e)}\mu(e|U \leq p) = \sum_e \frac{\mu(e)}{\mu(U \leq p)} = 1/\kappa, \tag{C5}$$

and Lem. 11 to complete the proof. For the remainder of the proof, e is fixed, so we simplify the notation by universally conditioning on $\{E = e\}$ and omitting the explicit condition. Further, we omit e from suffixes. Thus $\kappa = \kappa_e$ from here on.

Let $\kappa_z = \mu(U \leq p|z)$. We have $\sum_z \kappa_z \mu(z) = \kappa$ and

$$\kappa_z = \mu(z|U \leq p)\kappa/\mu(z)\,. \tag{C6}$$

Define the subprobability distribution $\tilde{\mu}$ by $\tilde{\mu}(cz)[U(cz) \geq \mu(c \mid z)]$. By the definition of ϵ-UPEs, we get that the weight of $\tilde{\mu}$ satisfies

$$\begin{aligned} w(\tilde{\mu}) &= \sum_{cz} \mu(cz)[\![U(cz) \geq \mu(c|z)]\!] \\ &= \mu(U(CZ) \geq \mu(C|Z)) \\ &\geq 1 - \epsilon\,. \end{aligned} \tag{C7}$$

Define $\tilde{\nu}(cz) = \tilde{\mu}(cz)[U(cz) \leq p] \,/\, \kappa$. The weight of $\tilde{\nu}$ satisfies

$$\begin{aligned} w(\tilde{\nu}) &= \sum_{cz} \tilde{\mu}(cz)[\![U(cz) \leq p]\!]/\kappa \\ &\leq \sum_{cz} \mu(cz)[\![U(cz) \leq p]\!]/\kappa \\ &= \mu(U \leq p)/\kappa = 1, \end{aligned} \tag{C8}$$

$$\begin{aligned} w(\tilde{\nu}) &= \sum_{cz} \mu(cz)[\![U(cz) \leq p]\!]/\kappa - \sum_{cz} (\mu(cz) - \tilde{\mu}(cz))[\![U(cz) \leq p]\!]/\kappa \\ &= 1 - \sum_{cz} (\mu(cz) - \tilde{\mu}(cz))[\![U(cz) \leq p]\!]/\kappa \\ &\geq 1 - \sum_{cz} (\mu(cz) - \tilde{\mu}(cz))/\kappa = 1 - (1 - w(\tilde{\mu}))/\kappa \\ &\geq 1 - (1 - (1 - \epsilon))/\kappa = 1 - \epsilon/\kappa\,. \end{aligned} \tag{C9}$$

To obtain the last inequality above, we used Eq. (C7). Thus $\tilde{\nu}$ is a subprobability distribution of weight at least $1 - \epsilon/\kappa$. We use $\tilde{\nu}$ to construct the distribution ν witnessing the conclusion of the theorem. For each cz we bound

$$\begin{aligned} \tilde{\nu}(cz)/\mu(z|U \leq p) &= \mu(cz)[\![U(cz) \geq \mu(c|z)]\!]\,[\![U(cz) \leq p]\!]/(\kappa\mu(z|U \leq p)) \\ &= \mu(c|z)[\![U(cz) \geq \mu(c|z)]\!]\,[\![U(cz) \leq p]\!]/\kappa_z \\ &\leq p/\kappa_z, \end{aligned} \tag{C10}$$

where in the second step we used Eq. (C6). Define $\tilde{\nu}(C \mid z)$ by $\tilde{\nu}(c \mid z) = \tilde{\nu}(cz) \,/\, \mu(z \mid U \leq p)$, with $\tilde{\nu}(c \mid z) = 0$ if $\mu(z|U \leq p) = 0$, and let $w_z = w(\tilde{\nu}(C \mid z))$. We show below that $w_z \leq 1$, and so the definition of $\tilde{\nu}(C \mid z)$ extends the conditional probability notation to the subprobability distribution $\tilde{\nu}$ with the understanding that the conditionals are with respect to μ given $\{U \leq p\}$. Applying the first two steps of Eq. (C10) and continuing from there, we have

$$\begin{aligned} \tilde{\nu}(c|z) &= \mu(c|z)[\![U(cz) \geq \mu(c|z)]\!]\,[\![U(cz) \leq p]\!]/\kappa_z \\ &\leq \mu(c|z)[\![U(cz) \leq p]\!]/\kappa_z \\ &= \mu(c, U \leq p\,|z)/\mu(U \leq p\,|z) = \mu(c\,|z, U \leq p)\,. \end{aligned} \tag{C11}$$

Since $\mu(C|z,\ U \leq p)$ is a normalized distribution, the above equation implies that $w_z \leq 1$. For each z, we have that $\tilde{\nu}(C \mid z) \leq p \,/\, \kappa_z$ (Eq. (C10)), $p/\kappa_z \geq p \geq 1/|\mathrm{Rng}(C)|$, and $\mu(C|z,\ U \leq p)$ dominates $\tilde{\nu}(C \mid z)$ (Eq. (C11)). Hence, we can apply Lem. 3 to obtain distributions ν_z of C

such that $\nu_z \geq \tilde{\nu}(C \mid z)$, $\nu_Z \leq p/\kappa_Z$, and $\mathrm{TV}(\nu_Z, \mu(C|z, U \leq p)) \leq 1 - w_Z$. Now we can define the distribution ν of CZ by $\nu(cz) = \nu_Z(c)\mu(z|U \leq p)$. By Eq. (A2), we get

$$\begin{aligned}
&\mathrm{TV}(\nu, \mu(CZ|U \leq p)) = \sum_z \mathrm{TV}(\nu_z \mu(C|z, U \leq p))\mu(z|U \leq p) \\
&\leq \sum_z (1 - w_z)\mu(z|U \leq p) \\
&= 1 - \sum_z w(\tilde{\nu}(C|z))\mu(z|U \leq p) \\
&= 1 - \sum_z \sum_c (\tilde{\nu}(cz))/\mu(z|U \leq p)\mu(z \Big| U \leq p) \\
&= 1 - w(\tilde{\nu} \leq \epsilon/\kappa,)
\end{aligned} \tag{C12}$$

where in the last step we used Eq. (C9). For the average maximum probability of ν, we get

$$\begin{aligned}
&\sum_z \max_c \nu(c|z)\nu(z) = \sum_z \max_c \nu_z(c)\mu(z|U \leq p) \\
&\leq p \sum_z \mu(z|U \leq p)/\kappa_z \\
&= p \sum_z \mu(z)/\kappa = p/\kappa,
\end{aligned} \tag{C13}$$

where to obtain the last line we used Eq. (C6). The above two equations show that for an arbitrary value e of E, $P^{\epsilon}_{\max, \mu(CZ \mid e, U \leq p)}(C \mid Z) \leq p \Big/ \kappa_e$, which together with the argument at the beginning of the proof establishes the theorem. □

The above theorem implies Thm. 1 in the main text as a corollary.

Corollary 13. *Suppose that the distribution μ of CZE satisfies the chained model $\mathscr{H}(\mathscr{C})$. Let $1 \geq p \geq 1/|\mathrm{Rng}(C)|$ and $1 \geq \kappa', \epsilon > 0$. Define $\{\phi\}$ to be the event that $U \leq p$, where U is given in* Eq. (C1). *Let $\kappa' \leq \kappa = \mathbb{P}_\mu(\phi)$. Then the smooth conditional min-entropy satisfies*

$$H^{\epsilon}_{\min}(C|ZE; \phi) \geq -\log_2(p/\kappa'^{1+1/\beta}).$$

Proof. We observe that the event that $U \leq p$ is the same as the event that $U' \leq p/\kappa^{1/\beta}$, where $U' = (T_n \epsilon\kappa)^{-1/\beta}$ and T_n is defined as above Eq. (C1). By Thm. 9, U' is an $\epsilon\kappa$-UPE. In Thm. 12, if we replace U and p there by U' and $p/\kappa^{1/\beta}$ here, then we obtain $P^{\epsilon}_{\max, \mu(CZE \mid \phi)}(C \mid ZE) \leq p \Big/ \kappa^{1+1/\beta}$. Since $\kappa' \leq \kappa$, we also have $P^{\epsilon}_{\max, \mu(CZE \mid \phi)}(C \mid ZE) \leq p \Big/ \kappa'^{1+1/\beta}$. According to the definition of the smooth conditional min-entropy in Def. 10, we get the lower bound in the corollary. □

We remark that, to obtain uniformly random bits, Cor. 13 can be composed directly with "classical-proof" strong extractors in a complete protocol for randomness generation. The error bounds from the corollary and those of the extractor compose additively [28]. Efficient

randomness extractors requiring few seed bits exist, see Refs. [45, 46]. Specific instructions for ways to apply them for randomness generation can be found in Refs. [19, 20, 28].

Appendix D: Properties of PEFs

Here we prove the monotonicity of the functions $g(\beta)$ and $\beta_g(\beta)$: As β increases, the rate $g(\beta)$ as defined in Eq. (4) of the main text is monotonically non-increasing, and $\beta_g(\beta)$ is monotonically non-decreasing. These are the consequence of the following lemma:

Lemma 14. *If F is a PEF with power β for the trial model $\mathscr{D}$, then for any $0 < \gamma \leq 1$, F is a PEF with power β/γ for $\mathscr{C}$, and F^γ is a PEF with poiver $\gamma\beta$ for $\mathscr{C}$.*

Proof. For an arbitrary distribution $\sigma \in \mathscr{C}$, we have $0 \leq \sigma(c|z) \leq 1$ for all cz. By the monotonic property of the exponential function $x \mapsto a^x$ with $0 \leq a \leq 1$, we get that $\sigma(c|z)^{\beta/\gamma} \leq \sigma(c|z)^\beta$ for all cz. Therefore, if a non-negative RV F satisfies that

$$\sum_{cz} F(cz)\sigma(c|z)^\beta \sigma(cz) \leq 1,$$

then

$$\sum_{cz} F(cz)\sigma(c|z)^{\beta/\gamma}\sigma(cz) \leq \sum_{cz} F(cz)\sigma(c|z)^\beta \sigma(cz) \leq 1.$$

Hence, if F is a PEF with power β for $\mathscr{C}$, then F is a PEF with power β/γ for $\mathscr{C}$.

On the other hand, by the concavity of the function $x \mapsto x^\gamma$ with $0 < \gamma \leq 1$, we can apply Jensen's inequality to get

$$\begin{aligned}&\mathbb{E}_\sigma(F(CZ)^\gamma \sigma(C|Z)^{\gamma\beta}) = \mathbb{E}_\sigma\left((F(CZ)\sigma(C|Z)^\beta)^\gamma\right)\\ &\leq (\mathbb{E}_\sigma(F(CZ)\sigma(C|Z)^\beta))^\gamma\\ &\leq 1,\end{aligned}$$

for all distributions $\sigma \in \mathscr{C}$. Hence F^γ is a PEF with power $\gamma\beta$ for $\mathscr{C}$.

The property that $\beta_g(\beta)$ is monotonically non-decreasing in β follows directly from Lem. 14 and the definition of $g(\beta)$ in Eq. (4) of the main text. On the other hand, to prove that $g(\beta)$ is monotonically non-increasing in β, we also need to use the equality that

$$\mathbb{E}_\sigma(\log_2(F^\gamma(CZ))/(\gamma\beta)) = \mathbb{E}_\sigma(\log_2(F(CZ))/\beta).$$

The monotonicity of the function $g(\beta)$ (or $\beta_g(\beta)$) helps to determine the maximum asymptotic randomness rate $g_0 = \sup_{\beta>0} g(\beta)$ (or the maximum certificate rate $\gamma_{\mathrm{PEF}} = \sup_{\beta>0} \beta_g(\beta)$), as one can analyze the PEFs with powers β only in the limit where β goes to 0 (or where β goes to the infinity).

Appendix E: Numerical Optimization of PEFs

We provide more details here on how to perform the optimizations (such as the optimization in Eq. (3) of the main text) required to determine the power β and the PEFs F_i to be used at the ith trial. We claim that to verify that the PEF F satisfies the first constraint in Eq. (3) of the main text for all $\sigma \in \mathscr{C}$, it suffices to check this constraint on the extremal members of the convex closure of $\mathscr{C}$. The claim follows from the next lemma, Carathéodory's theorem, and induction on the number of terms in a finite convex combination.

Lemma 15. *Let $F \geq 0$ and $\beta > 0$. Suppose that the distribution σ can be expressed as a convex combination of two distributions: For all cz, $\sigma(cz) = \lambda\sigma_1(cz) + (1-\lambda)\sigma_2(cz)$ with $\lambda \in [0, 1]$. If the distributions σ_1 and σ_2* satisfy $\sum_{cz} F(cz)\sigma_i(c|z)^\beta \sigma_i(cz) \leq 1$, *then σ satisfies $\sum_{cz} F(cz)\sigma(c|z)^\beta\sigma(cz) \leq 1$.*

Proof. We start by proving that for every cz, the following inequality holds:

$$\sigma(c|z)^\beta\sigma(cz) \leq \lambda\sigma_1(c|z)^\beta\sigma_1(cz) + (1-\lambda)\sigma_2(c|z)^\beta\sigma_2(cz)\,. \tag{E1}$$

If $\sigma_1(z) = \sigma_2(z) = 0$, we recall our convention that probabilities conditional on z are zero, and so for every c, $\sigma_1(c|z) = \sigma_2(c|z) = \sigma(c|z) = 0$. Hence, Eq. (E1) holds immediately (as an equality). If $\sigma_1(z) = 0 < \sigma_2(z)$, then for every c, $\sigma_1(c|z) = 0$ and $\sigma(cz) = (1-\lambda)\sigma_2(cz)$. In this case, one can verify that Eq. (E1) holds. By symmetry, Eq. (E1) also holds in the case that $\sigma_2(z) = 0 < \sigma_1(z)$. Now consider the case that $\sigma_1(z) > 0$ and $\sigma_2(z) > 0$. Let $x_i = \sigma_i(cz)$ and $y_i = \sigma_i(z)$, and consider the function

$$f(\lambda) = (\lambda x_1 + (1-\lambda)x_2)^{1+\beta}(\lambda y_1 + (1-\lambda)y_2)^{-\beta},$$

so $f(0) = \sigma_2(c|z)^\beta\sigma_2(cz)$, $f(1) = \sigma_1(c|z)^\beta\sigma_1(cz)$, and $f(\lambda) = \sigma(c|z)^\beta\sigma(c|z)$. If we can show that $f(\lambda)$ is convex in λ on the interval [0,1], Eq. (E1) will follow. Since $f(\lambda)$ is continuous for $\lambda \in [0,1]$ and smooth for $\lambda \in (0,1)$, it suffices to show that $f''(\lambda) \geq 0$ as follows:

$$\begin{aligned}
&f'(\lambda) = (\lambda x_1 + (1-\lambda)x_2)^\beta(\lambda y_1 + (1-\lambda)y_2)^{-\beta-1} \times ((1+\beta)(x_1-x_2)(\lambda y_1 + (1-\lambda)y_2) \\
&+ (-\beta)(\lambda x_1 + (1-\lambda)x_2)(y_1-y_2)) \\
&f''(\lambda) = (\lambda x_1 + (1-\lambda)x_2)^{\beta-1}(\lambda y_1 + (1-\lambda)y_2)^{-\beta-2} \times \\
&\Big(\beta(1+\beta)(x_1-x_2)^2(\lambda y_1 + (1-\lambda)y_2)^2 + 2(-\beta)(1+\beta)(x_1-x_2)(y_1-y_2)(\lambda x_1 + (1-\lambda)x_2)(\lambda y_1 + (1-\lambda)y_2) \\
&+ (-\beta)(-1-\beta)(y_1-y_2)^2(\lambda x_1 + (1-\lambda)x_2)^2\Big) \\
&= (\lambda x_1 + (1-\lambda)x_2)^{\beta-1}(\lambda y_1 + (1-\lambda)y_2)^{-\beta-2} \times \beta(1+\beta \\
&)((x_1-x_2)(\lambda y_1 + (1-\lambda)y_2) - (y_1-y_2)(\lambda x_1 + (1-\lambda)x_2))^2,
\end{aligned}$$

which is a non-negative multiple of a square. Having demonstrated Eq. (E1), we can complete the proof of the lemma as follows:

$$\begin{aligned}\sum_{cz} F(cz)\sigma(c|z)^{\beta}\sigma(cz) &\le \sum_{cz} F(cz)[\lambda\sigma_1(c|z)^{\beta}\sigma_1(cz) + (1-\lambda)\sigma_2(c|z)^{\beta}\sigma_2(cz)] \\ &= \lambda\sum_{cz} F(cz)\sigma_1(c|z)^{\beta}\sigma_1(cz) + (1-\lambda)\sum_{cz} F(cz)\sigma_2(c|z)^{\beta}\sigma_2(cz) \\ &\le \lambda\times 1 + (1-\lambda)\times 1 \\ &= 1.\end{aligned}$$

Suppose that the trial model $\mathscr{C}$ is a convex polytope with a finite number of extremal distributions $\sigma_k(CZ)$, $k = 1,2, \ldots, K$. In view of the claim before Lem. 15, the optimization problem in Eq. (3) of the main text is equivalent to

$$\begin{aligned}&\text{Max:} \quad n\mathbb{E}_{\nu}\log_2(F(CZ))/\beta + \log_2(\epsilon)/\beta \\ &\text{With:} \quad \sum\nolimits_{cz} F(cz)\sigma_k(c|z)^{\beta}\sigma_k(cz) \le 1, k = 1, 2, \ldots, K, \\ &F(cz) \ge 0, \forall cz\,.\end{aligned} \tag{E2}$$

Given the values of n, β, ϵ, ν, and σ_k with $k = 1, 2, \ldots, K$, the objective function in Eq. (E2) is a concave function of $F(CZ)$, and each constraint on $F(CZ)$ is linear. Hence, the above optimization problem can be solved by any algorithm capable of optimizing nonlinear functions with linear constraints on the arguments. In our implementation, we use sequential quadratic programming. Due to numerical imprecision, it is possible that the returned numerical solution does not satisfy the first constraint in Eq. (E2) and the corresponding PEF is not valid. In this case, we can multiply the returned numerical solution by a positive factor smaller than 1, whose value is given by the reciprocal of the largest left-hand side of the above first constraint at the extremal distributions $\sigma_k(CZ)$, $k = 1, 2, \ldots, K$. Then, the re-scaled solution is a valid PEF. We remark that if the trial model $\mathscr{C}$ is not a convex polytope but there exists a good approximation $\mathscr{C} \subseteq \mathscr{D}$ with $\mathscr{D}$ a convex polytope, then we can enlarge the model to $\mathscr{D}$ for an effective method to determine good PEFs.

Consider device-independent randomness generation (DIRG) in the CHSH Bell-test configuration [30] with inputs $Z = XY$ and outputs $C = AB$, where $A, B, X, Y \in \{0,1\}$. If the input distribution $\mathbb{P}(XY)$ is fixed with $\mathbb{P}(xy) > 0$ for all xy, then we need to characterize the set of input-conditional output distributions $\mathbb{P}(AB \mid XY)$. If we consider all distributions $\mathbb{P}(AB \mid XY)$ satisfying non-signaling conditions [24], then the associated trial model $\mathscr{C}$ is the nonsignaling polytope, which is convex and has 24 extreme points [25]. If we consider only the distributions $\mathbb{P}(AB \mid XY)$ achievable by quantum mechanics, then the associated trial model is a proper convex subset of the above non-signaling polytope. The quantum set has an infinite number of extreme points. In our analysis of the Bell-test results reported in Refs. [9, 10], we simplified the problem by considering instead the set of distributions $\mathbb{P}(AB \mid XY)$ satisfying nonsignaling conditions [24] and Tsirelson's bounds [38], which includes all the distributions $\mathbb{P}(AB \mid XY)$ achievable by quantum mechanics. For a fixed input distribution $\mathbb{P}(XY)$ with $\mathbb{P}(xy) > 0$ for all xy, the associated trial model $\mathscr{C}$ is a convex polytope with 80 extreme points [28]. If the input distribution $\mathbb{P}(XY)$ is not fixed but is contained in a convex polytope, the associated trial model $\mathscr{C}$ is still a convex polytope (see Ref. [28] for more details). Therefore, for DIRG based on the CHSH Bell test [30], the optimizations for

determining the power β and the PEFs F_i can be expressed in the form in Eq. (E2) and hence solved effectively.

Appendix F: Relationship between Certificate Rate and Statistical Strength

We prove that for DIRG in the CHSH Bell-test configuration, the maximum certificate rate γ_{PEF} witnessed by PEFs at a distribution ν of trial results is equal to the statistical strength of ν for rejecting local realism as studied in Refs. [35–37]. To prove this, we first simplify the optimization problem for determining γ_{PEF}. Then, we show that the simplified optimization problem is the same as that for determining the statistical strength. The argument generalizes to any convex-polytope model whose extreme points are divided into the following two classes: 1) classical deterministic distributions satisfying that given the inputs, the outputs are deterministic (here we require that for every cz there exists a distribution in the model where the outcome is c given z), and 2) distributions that are completely non-deterministic in the sense that for no input is the output deterministic. The argument further generalizes to models contained in such a model, provided it includes all of the classical deterministic distributions of the outer model.

In order to determine $\gamma_{\mathrm{PEF}} = \sup_{\beta>0} \beta_g(\beta)$, considering the monotonicity of the function $\beta_g(\beta)$ proved in Sect. D and the definition of $g(\beta)$ in Eq. (4) of the main text, we need to solve the following optimization problem at arbitrarily large powers β:

$$\begin{aligned} &\text{Max:} \quad \mathbb{E}_{\nu}(\log_2(F(CZ))) \\ &\text{With:} \quad \sum_{cz} F(cz)\sigma(c|z)^{\beta}\sigma(cz) \le 1 \text{ for all } \sigma \in \mathscr{C}, \\ &F(cz) \ge 0, \text{for all } cz\,. \end{aligned} \tag{F1}$$

To simplify this optimization, we first consider the case that the trial model $\mathscr{C}$ is the set of non-signaling distributions with a fixed input distribution $\mathbb{P}(Z)$ where $\mathbb{P}(z) > 0$ for all z. The model $\mathscr{C}$ is a convex polytope and has 24 extremal distributions [25], among which there are 16 deterministic local realistic distributions, denoted by σ_{LR_i}, $i = 1, 2, \ldots, 16$, and 8 variations of the Popescu-Rohrlich (PR) box [24], denoted by σ_{PR_j}, $j = 1, 2, \ldots, 8$. According to the discussion in Sect. E, the optimization problem in Eq. (F1) is equivalent to

$$\begin{aligned} &\text{Max:} \quad \mathbb{E}_{\nu}(\log_2(F(CZ))) \\ &\text{With:} \quad \sum_{cz} F(cz)\sigma_{\mathrm{LR}_i}(cz) \le 1, \forall i, \\ &\sum_{cz} F(cz)\sigma_{\mathrm{PR}_j}(c|z)^{\beta}\sigma_{\mathrm{PR}_j}(cz) \le 1, \forall j, \\ &F(cz) \ge 0, \text{ for all } cz, \end{aligned} \tag{F2}$$

where we used the fact that $\sigma_{\mathrm{LR}_i}(c|z)$ is either 0 or 1. Only the second constraint in Eq. (F2) depends on the power β. The distributions σ_{PR_j} satisfy that $\sigma_{\mathrm{PR}_j}(c|z) < 1$ for all cz. Hence $\sigma_{\mathrm{PR}_j})^{\beta} \to 0$ for all cz as $\beta \to \infty$. Because there are finitely many constraints and values of cz, the second constraint becomes irrelevant for sufficiently large β. Let $\beta_{\mathrm{th}}^{\mathrm{NS}}$ be the minimum β for which the second constraint is implied by the first. The threshold $\beta_{\mathrm{th}}^{\mathrm{NS}}$ is independent of the specific input distribution. To see this, the last factors in the sums on the

left-hand sides of the constraints in Eq. (F2) are of the form $\sigma(cz)$, which can be written as $\sigma(c|z)\sigma(z)$ with a fixed $\sigma(z)$. We can define $\widetilde{F}(cz) = F(cz)\sigma(z)$ and optimize over $\widetilde{F}$ instead, thus eliminating the fixed input distribution from the problem. Then the first constraint on $\widetilde{F}$ implies that $\Sigma_{cz}\widetilde{F}(cz)\Sigma_i\sigma_{\mathrm{LR}_i}(c \mid z) \leq 16$. Since $\sum_i \sigma_{\mathrm{LR}_i}(c|z) \geq 4$ for each cz, this constraint implies the second provided that $\sigma_{\mathrm{PR}_j}(c|z)^{1+\beta} \leq 1/4$, which holds for each j and cz for sufficiently large β. Particularly, since $\sigma_{\mathrm{PR}_j}(c|z)$ is either 0 or 1/2 [25], we obtain that $\beta_{\mathrm{th}}^{\mathrm{NS}} \leq 1$. Furthermore, by numerical optimization for a sample of large-enough β we find that $\beta_{\mathrm{th}}^{\mathrm{NS}} \approx 0.4151$. Therefore, when $\beta \geq \beta_{\mathrm{th}}^{\mathrm{NS}}$ the optimization problem in Eq. (F2) is independent of β and becomes

$$\begin{aligned} &\text{Max:} \quad \mathbb{E}_{\nu}(\log_2(F(CZ))) \\ &\text{With:} \quad \sum_{cz} F(cz)\sigma_{\mathrm{LR}_i}(cz) \leq 1, \forall i, \\ &F(cz) \geq 0, \text{ for all } cz\,. \end{aligned} \tag{F3}$$

This optimization problem is identical to the one for designing the optimal test factors for the hypothesis test of local realism [21, 41, 47]. In Ref. [21] it is proven that the optimal value of the optimization problem in Eq. (F3) is equal to the statistical strength for rejecting local realism [35–37], which is defined as

$$s = \min_{\sigma_{\mathrm{LR}}} D_{\mathrm{KL}}(\nu|\sigma_{\mathrm{LR}})\,.$$

Here, σ_{LR} is an arbitrary local realistic distribution and $D_{\mathrm{KL}}(\nu|\sigma_{\mathrm{LR}})$ is the Kullback-Leibler divergence from σ_{LR} to ν [48]. Therefore, when $\beta \geq \beta_{\mathrm{th}}^{\mathrm{NS}}$ we have $\beta_g(\beta) = s$. Considering that the function $\beta_g(\beta)$ is monotonically non-decreasing in β, we have shown that

$$\gamma_{\mathrm{PEF}} = \sup_{\beta > 0} \beta g(\beta) = s\,.$$

Now we consider the case where the trial model $\mathscr{C}$ is the set of quantum-achievable distributions with a fixed input distribution $\mathbb{P}(Z)$ where $\mathbb{P}(z) > 0$ for all z. Since the set of quantum-achievable distributions is a proper subset of the non-signaling polytope, the constraints on $F(CZ)$ imposed by quantum-achievable distributions are a subset of the constraints imposed by non-signaling distributions. Moreover, the set of quantum-achievable distributions contains all local realistic distributions. Therefore, in the quantum case, when $\beta \geq \beta_{\mathrm{th}}^{\mathrm{NS}}$, the constraints on $F(CZ)$ are also implied by the constraints associated with the local realistic distributions. Consequently the maximum certificate rate γ_{PEF} is also equal to the statistical strength s. We remark that as a consequence, if we set $\beta_{\mathrm{th}}^{\mathrm{QM}}$ to be the threshold such that when $\beta \geq \beta_{\mathrm{th}}^{\mathrm{QM}}$ all quantum constraints on $F(CZ)$ are implied by those imposed by the local realistic distributions, then $\beta_{\mathrm{th}}^{\mathrm{QM}} \leq \beta_{\mathrm{th}}^{\mathrm{NS}}$.

We remark that $\beta_0 = \inf[\beta|\beta_g(\beta) = s\}$ is typically strictly less than $\beta_{\mathrm{th}}^{\mathrm{NS}}$ and depends on both the distribution ν as well as the trial model $\mathscr{C}$. One way to understand this behavior is as

follows: When $\beta < \beta_{\text{th}}^{\text{NS}}$, the second constraint in Eq. (F2) is relevant; however, if β is still large enough, it is possible that the constraint does not affect the optimal solution of the optimization problem (F2). By numerical optimization, we find that for the CHSH Bell-test configuration β_0 is typically less than 0.2 when the trial model $\mathscr{C}$ includes all non-signaling distributions with the uniform distribution for inputs.

Appendix G: Analytic Expressions for Asymptotic Randomness Rates

In this section we derive the asymptotic randomness rates for the trial model consisting of non-signaling distributions according to two different methods for DIRG protocol based on the CHSH Bell test [30]. We first consider the maximum asymptotic rate g_0 witnessed by PEFs. Then, we derive the single-trial conditional min-entropy for comparison.

Suppose that the distribution of each trial's inputs XY and outputs AB is $\nu(ABXY) \in \mathscr{C}$, where $\mathscr{C}$ is the model for each trial. The maximum asymptotic rate g_0 is equal to the worst-case conditional entropy that is consistent with the distribution $\nu(ABXY)$ [28]. That is, the rate g_0 is given by the following minimization:

$$g_0 = \min_{\sigma} \{ H_\sigma(AB|XYE) : \sigma(ABXY) = \nu(ABXY) \}, \tag{G1}$$

where σ is the joint distribution of A, B, X, Y and E, and $\sigma(ABXY)$ is its marginal. By the assumption that the value space of E is countable, we can also express the above minimization as

$$g_0 = \min_{w_e, \sigma_e} \{ \sum_e \omega_e H_{\sigma_e}(AB|XY, E = e) : \forall e, \sigma_e \in \mathscr{C} \text{ and } \omega_e \geq 0, \sum_e \omega_e = 1, \sum_e \omega_e \sigma_e = \nu \}, \tag{G2}$$

where σ_e is the distribution of A, B, X and Y conditional on $E = e$ according to σ, and ω_e is the probability of the event $E = e$. By the concavity of the conditional entropy, if any of the σ_e contributing to the sum in Eq. (G2) is not extremal in $\mathscr{C}$, we can replace it by a convex combination of extremal distributions to decrease the value of the sum. Thus, we only have to consider extremal distributions in the above minimization.

For the rest of this section we let $\mathscr{C}$ consist of non-signaling distributions for the CHSH Bell-test configuration with a fixed input distribution $\mathbb{P}(XY)$ where $\mathbb{P}(xy) > 0$ for all xy. As explained in the previous section, $\mathscr{C}$ is a convex polytope with 24 extreme points. Considering the argument below Eq. (G2), the number of terms in the sum of Eq. (G2) is at most 24. As in the previous section, we can divide the 24 extreme points into the two classes consisting of the 16 deterministic local realistic distributions σ_{LR_i}, $i = 1, 2, \ldots, 16$, and the 8 variations of the PR box σ_{PR_j}, $j = 1, 2, \ldots, 8$. Because the σ_{LR_i} are deterministic conditional on the inputs, if $\sigma_e = \sigma_{\text{LR}_i}$ then the conditional entropy satisfies $H_{\sigma_{\text{LR}_i}}(AB|XY, E = e) = 0$. For each PR box σ_{PR_j}, the conditional probabilities $\sigma_{\text{PR}_j}(AB|XY)$ are either 0 or 1/2 [25]. Thus, if $\sigma_e = \sigma_{\text{PR}_j}$, the conditional entropy satisfies $H_{\sigma_{\text{PR}_j}}(AB|XY, E = e) = 1$. Hence, the minimization problem in Eq. (G2) becomes

$$\begin{aligned} g_0 = \text{Min:} \quad & \sum_j \omega_{\text{PR}_j} \\ \text{With:} \quad & \omega_{\text{LR}_i}, \omega_{\text{PR}_j} \geq 0, \forall i, j, \\ & \sum_i \omega_{\text{LR}_i} + \sum_j \omega_{\text{PR}_j} = 1, \\ & \sum_i \omega_{\text{LR}_i} \sigma_{\text{LR}_i} + \sum_j \omega_{\text{PR}_j} \sigma_{\text{PR}_j} = \nu . \end{aligned} \tag{G3}$$

We need to find the minimum total probability of PR boxes in a representation of the distribution ν as a convex combination of the 16 local realistic distributions and the 8 PR boxes. To help solve this problem, we consider the violation of the CHSH Bell inequality [30]. Recall that there is only one PR box that can violate a particular CHSH Bell inequality $\mathbb{E}(I_{\text{CHSH}}) \leq 2$ [25], where I_{CHSH} is the CHSH Bell function

$$I_{\text{CHSH}}(ABXY) = (1 - 2XY)(-1)^{A+B}/\mathbb{P}(XY), \tag{G4}$$

and $A, B, X, Y \in \{0,1\}$. Let σ_{PR_1} be the violating PR box. The expectation of I_{CHSH} according to σ_{PR_1} is maximal, that is, $\mathbb{E}_{\sigma_{\text{PR}_1}}(I_{\text{CHSH}}) = 4$. Without loss of generality, $\hat{I} = \mathbb{E}_{\nu}(I_{\text{CHSH}}) > 2$. The probability ω_{PR_1} in the convex decomposition of ν satisfies the inequality $4\omega_{\text{PR}_1} + (1 - \omega_{\text{PR}_1})2 \geq \hat{I}$, or equivalently, $\omega_{\text{PR}_1} \geq (\hat{I} - 2) \big/ 2$. Hence, according to Eq. (G3), we have $g_0 \geq (\hat{I} - 2) \big/ 2$.

We next show that $g_0 \leq (\hat{I} - 2) \big/ 2$. For this, we directly use the result of Ref. [49]. According to Ref. [49], for any non-signaling distribution $\sigma(ABXY)$, if $\mathbb{E}_{\sigma}(I_{\text{CHSH}}) > 2$, then the distribution $\sigma(ABXY)$ can be decomposed as $\sigma(ABXY) = \omega_{\text{PR}_1}\, \sigma_{\text{PR}_1} + \sum_i \omega_{\text{LR}_i} \sigma_{\text{LR}_i}$, where $\omega_{\text{PR}_1} = (\mathbb{E}_{\sigma}(I_{\text{CHSH}}) - 2) \big/ 2$, $\omega_{\text{LR}_i} \geq 0$, and $\sum_i \omega_{\text{LR}_i} = 1 - \omega_{\text{PR}_1}$. Specializing to the distribution $\nu(ABXY)$, we get that $g_0 \leq (\hat{I} - 2) \big/ 2$ for $\hat{I} > 2$.

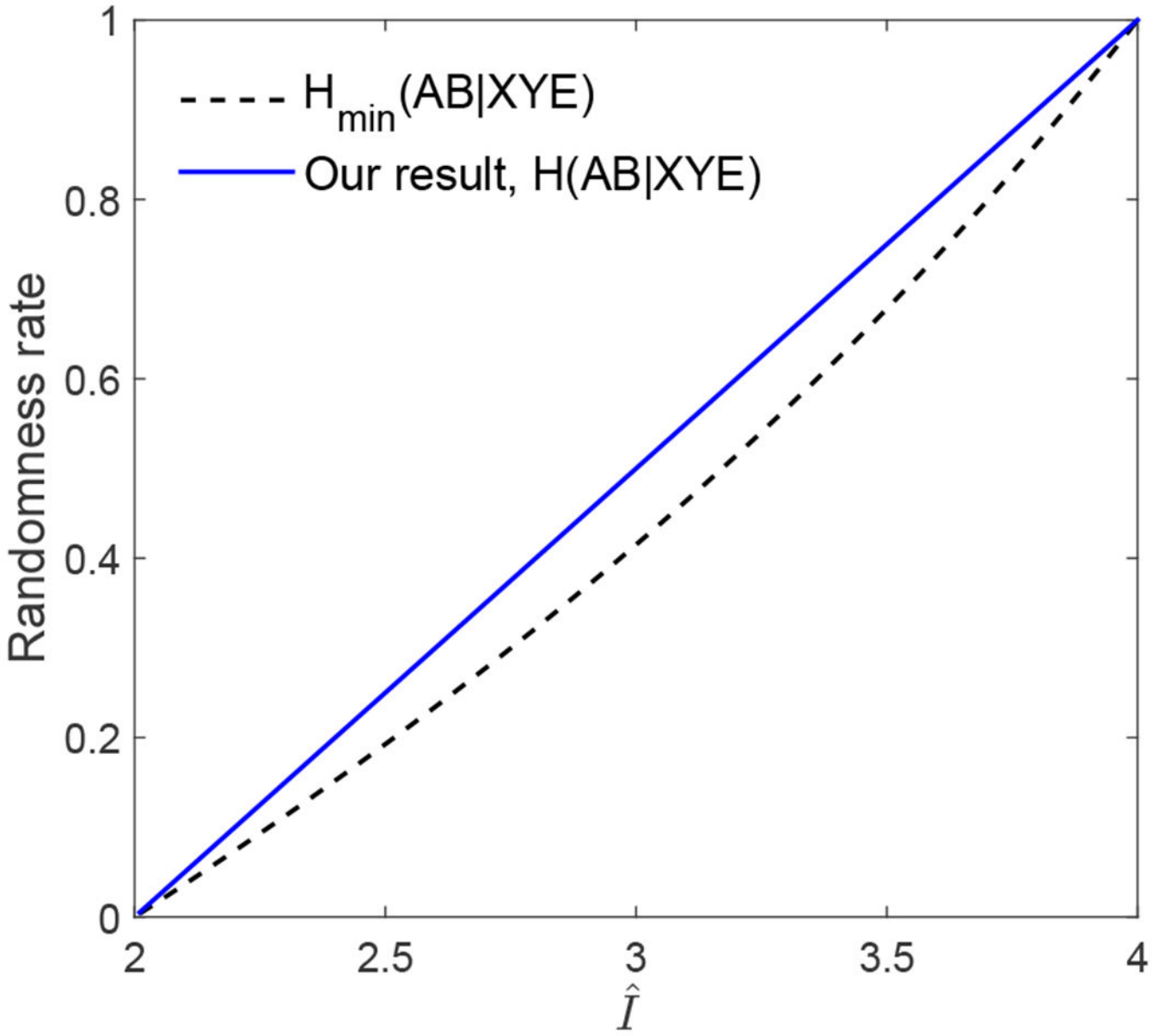

FIG. 3:
Asymptotic randomness rates as a function of $\hat{I}$. Results according to both our method (the solid curve) and Refs. [3, 10, 12, 18, 31–33] (the dashed curve) are shown. Our method witnesses the maximum asymptotic rate $H(AB|XYE)$, which is the worst-case conditional entropy.

The arguments above show that given $\hat{I} > 2$, the maximum asymptotic randomness rate witnessed by PEFs is

$$g_0 = (\hat{I} - 2)/2, \tag{G5}$$

independent of the particular distribution ν realizing $\hat{I}$.

We also numerically evaluated the maximum asymptotic rate according to $g_0 = \sup_{\beta>0} g(\beta)$ with $g(\beta)$ given by Eq. (4) of the main text. The numerical results are presented in Fig. 3, which are consistent with the analytic expression in Eq. (G5).

Next, we consider the quantification of the asymptotic randomness rate by the single-trial conditional min-entropy $H_{\min}(AB|XYE)$, which is a lower bound and is studied in Refs. [3, 10, 12, 18, 31–33]. The single-trial conditional min-entropy is defined by

$$H_{\min}(AB|XY\ E) = -\log_2(P_{\text{guess}}(AB|XY\ E)), \tag{G6}$$

where $P_{\text{guess}}(AB|XYE)$ is the average guessing probability of the output AB given the input XY and the side information E, as defined in Ref. [33]. According to Refs. [32, 33], the guessing probability at xy is given by the following maximization:

$$P_{\text{guess}}(AB|xyE) = \max_{\omega_e,\sigma_e}\left\{\sum_e \omega_e \max_{ab}\sigma_e(ab|xy) :\ \forall e,\sigma_e\in\mathscr{C} \text{ and } \omega_e\geq 0, \sum_e \omega_e = 1, \sum_e \omega_e\sigma_e = \nu\right\}. \tag{G7}$$

If a σ_e contributing to the sum in Eq. (G7) is not extremal in the set $\mathscr{C}$, we can replace it by a convex combination of extremal distributions to increase the value of the sum. Thus, we only have to consider extremal distributions σ_e in the above maximization. Applying the argument that led from Eq. (G2) to Eq. (G3), we obtain

$$\begin{aligned} &P_{\text{guess}}(AB|xyE) = \text{Max:}\quad \textstyle\sum_i \omega_{\text{LR}_i} + \frac{1}{2}\sum_j \omega_{\text{PR}_j} \\ &\text{With:}\quad \omega_{\text{LR}_i},\omega_{\text{PR}_j}\geq 0,\ \forall i,j, \\ &\textstyle\sum_i \omega_{\text{LR}_i} + \sum_j \omega_{\text{PR}_j} = 1, \\ &\textstyle\sum_i \omega_{\text{LR}_i}\sigma_{\text{LR}_i} + \sum_j \omega_{\text{PR}_j}\sigma_{\text{PR}_j} = \nu. \end{aligned} \tag{G8}$$

Since $\Sigma_i\omega_{\text{LR}_i} + \frac{1}{2}\Sigma_j\omega_{\text{PR}_j} = 1 - \frac{1}{2}\Sigma_j\omega_{\text{PR}_j}$ only need to minimize the total probability of PR boxes $\sum_j\omega_{\text{PR}_j}$ in the convex decomposition of the distribution ν. Prom the derivation of g_0 that gave Eq. (G5), we conclude that $\min\left(\Sigma_j\omega_{\text{PR}_j}\right) = (\hat{I}-2)\,/\,2$ for $\hat{I}>2$. Therefore $P_{\text{guess}}(AB\mid xyE) = (6-\hat{I})\,/\,4$ regardless of the particular input xy. Furthermore, the specific convex decomposition over E that achieves the maximum in Eq. (G8) is the same for all the possible inputs. Hence we also have $P_{\text{guess}}(AB\mid XY\ E) = (6-\hat{I})\,/\,4$ independent of the input distribution. Therefore the single-trial conditional min-entropy is

$$H_{\min}(AB|XY\ E) = -\log_2((6-\hat{I})/4), \tag{G9}$$

which is plotted in Fig. 3.

The results of this section are summarized in the following theorem:

Theorem 16. *Suppose that the trial model $\mathscr{C}$ consists of non-signaling distributions with a fixed input distribution $\mathbb{P}(XY)$ where $\mathbb{P}(xy)>0$ for all xy. For any $\nu\in\mathscr{C}$, both the maximum*

asymptotic randomness rate g_0 witnessed by PEFs and the single-trial conditional min-entropy $H_{\min}(AB|XYE)$ depend only on $\hat{I} = \mathbb{E}_\nu(I_{\mathrm{CHSH}}) > 2$ and are given by $g_0 = (\hat{I} - 2) / 2$ and $H_{\min}(AB \mid XY\ E) = -\log_2((6 - \hat{I}) / 4)$.

Appendix H: Entropy Accumulation

Consider DIRG in the CHSH Bell-test configuration. In this section, the input distribution $\mathbb{P}(XY)$ at each trial is assumed to be uniform. Define the winning probability at a trial by $\hat{\omega} = 1 / 2 + \hat{I} / 8$ where $\hat{I} = \mathbb{E}_\nu(I_{\mathrm{CHSH}})$ with ν the distribution of trial results. Entropy accumulation [17] is a framework for estimating (quantum) conditional min-entropy with respect to quantum side information and can be applied to the CHSH Bell-test configuration. The following theorem from Ref. [17] implements the framework:

Theorem 17. *Let $(2 + \sqrt{2}) / 4 \geq \omega_{\mathrm{exp}}, p_t \geq 3 / 4$, and $1 \geq \kappa, \epsilon > 0$. Suppose that after n trials the joint quantum state of the inputs* **XY**, *the outputs* **AB** *and the quantum side information E is ρ.* Define $\{\phi\}$ *to be the event that the experimentally observed winning probability is higher than or equal to ω_{exp},* and suppose that $\kappa \leq \mathbb{P}_\rho(\phi)$. *Denote the joint quantum state conditional on $\{\phi\}$ by $\rho_{|\phi}$. Then the (quantum) smooth conditional min-entropy evaluated at $\rho_{|\phi}$ satisfies*

$$H_{\min}^{\epsilon}(\mathbf{AB}|\mathbf{XY}\ E)_{\rho|\phi} > n\eta(p_t, w_{\mathrm{exp}}, n, \epsilon, \kappa),$$

where η is defined by

$$g(p) = \begin{cases} 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{16p(p-1)+3}\right) & p \in [3/4, (2+\sqrt{2})/4] \\ 1 & p \in [(2+\sqrt{2})/4, 1], \end{cases}$$

$$f_{\min}(p_t, p) = \begin{cases} g(p) & p \leq p_t \\ \frac{\mathrm{d}}{\mathrm{d}p} g(p)\big|_{p_t} p + \left(g(p_t) - \frac{\mathrm{d}}{\mathrm{d}p} g(p)\big|_{p_t} p_t\right) & p > p_t, \end{cases}$$

$$v(p_t, \epsilon, \kappa) = 2\left(\log_2 13 + \frac{\mathrm{d}}{\mathrm{d}p} g(p)\big|_{p_t}\right)\sqrt{1 - 2\log_2(\epsilon\kappa)},$$

$$\eta(p_t, p, n, \epsilon, \kappa) = f_{\min}(p_t, p) - \frac{1}{\sqrt{n}} v(p_t, \epsilon, \kappa),$$

with $h(x) = -x\log_2(x) - (1 - x)\log_2(1 - x)$ *be the binary entropy function.*

The function $f_{\min}$ in the theorem is referred to as a min-tradeoff function. The parameter p_t in the theorem is free, and can be optimized over its range before running the protocol based on the chosen parameters n, ω_{exp}, ϵ and κ. So the optimal entropy rate is $\eta_{\mathrm{opt}}(\omega_{\mathrm{exp}}, n, \epsilon, \kappa) = \max_{p_t} \eta(p_t, \omega_{\mathrm{exp}}, n, \epsilon, \kappa)$.

According to Thm. 17, in order to certify b bits of entropy given ω_{exp}, ϵ and κ, we need that $\eta\eta(p_t, \omega_{\mathrm{exp}}, n, \epsilon, \kappa) \geq b$. Equivalently, $n \geq n_{\mathrm{EAT},b}(p_t)$ where

$$n_{\mathrm{EAT},\,b}(p_t) = \left(\frac{\nu(p_t,\epsilon,\kappa) + \sqrt{\nu(p_t,\epsilon,\kappa)^2 + 4b f_{\min}(p_t,\omega_{\exp})}}{2 f_{\min}\,(p_t,\omega_{\exp})} \right)^2 . \tag{H1}$$

Including the optimization over p_t gives the minimum number of identical trials required:

$$n_{\mathrm{EAT},\,b} = \min_{3/4 \le p_t \le (2+\sqrt{2})/4} n_{\mathrm{EAT},\,b}(p_t) . \tag{H2}$$

To compute $n_{\mathrm{EAT},b}$, we set the parameter $\omega_{\exp}$ to the winning probability $\hat{\omega}$ according to the distribution ν of trial results in a stable experiment.

We finish with several remarks on the comparison between entropy accumulation and probability estimation. First, Thm. 17 based on entropy accumulation holds with respect to quantum side information, while Cor. 13 (Thm. 1 in the main text) based on probability estimation holds with respect to classical side information. Second, in principle both entropy accumulation and probability estimation can witness asymptotically tight bounds on the smooth conditional min-entropies with respect to the assumed side information. Entropy accumulation can witness the maximum asymptotic entropy rate with respect to quantum side information, if an optimal min-tradeoff function is available. However, it is unknown how to obtain such min-tradeoff functions. In particular, the min-tradeoff function $f_{\min}(p, p_t)$ is not optimal for the CHSH Bell-test configuration considered here. A min-tradeoff function is required to be a bound on the single-trial conditional von Neumann entropy $H(AB|XY\,E)$. That $f_{\min}(p, p_t)$ is not optimal is due to the following: 1) $f_{\min}(p, p_t)$ is designed according to a bound on the single-trial conditional von Neumann entropy $H(A|XY\,E)$ derived in Refs. [50, 51]. A tight bound on $H(A|XY\,E)$ is generally not a tight bound on $H(AB|XY\,E)$. 2) The bound on $H(A|XY\,E)$ derived in Refs. [50, 51] is tight if the only information available is the winning probability. However, in practice one can access the full measurement statistics rather than just the winning probability. In contrast to entropy accumulation, probability estimation is an effective method for approaching the maximum asymptotic entropy rate (with respect to classical side information) considering the full measurement statistics and the model constraints. In general, the maximum rate with respect to quantum side information is lower than that with respect to classical side information, as accessing quantum side information corresponds to a more powerful attack. Third and as demonstrated in the main text, probability estimation performs significantly better with finite data.

References

[1]. Paar Christof and Pelzl Jan, Understanding Crypotgraphy (Springer-Verlag Berlin Heidelberg, New York, 2010).

[2]. Fischer MJ, “A public randomness service,” in SECRYPT 2011 (2011) pp. 434–438.

[3]. Pironio S and Massar S, “Security of practical private randomness generation,” Phys. Rev. A 87, 012336 (2013).

[4]. Colbeck R, Quantum and Relativistic Protocols for Secure Multi-Party Computation, Ph.D. thesis, University of Cambridge (2007).

[5]. Colbeck R and Kent A, “Private randomness expansion with untrusted devices,” J. Phys. A: Math. Theor 44, 095305 (2011).

[6]. Hensen B et al., “Loophole-free Bell inequality violation using electron spins separated by 1.3 km,” Nature 526, 682 (2015). [PubMed: 26503041]

[7]. Rosenfeld W, Burchardt D, Garthoff R, Redeker K, Ortegel N, Rau M, and Weinfurter H, “Event-ready Bell-test using entangled atoms simultaneously closing detection and locality loopholes,” Phys. Rev. Lett 119, 010402 (2017). [PubMed: 28731745]

[8]. Giustina M, Marijn AM, Versteegh, Soren Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Ake Larsson, Carlos Abellan, Waldimar Amaya, Valerio Pruneri, Mitchell Morgan W., Joorn Beyer, Thomas Gerrits, Lita Adriana E., Shalm Lynden K., Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger, “Significant-loophole-free test of Bell’s theorem with entangled photons,” Phys. Rev. Lett 115, 250401 (2015). [PubMed: 26722905]

[9]. Shalm LK, Meyer-Scott E, Christensen BG, Bierhorst P, Wayne MA, Stevens MJ, Gerrits T, Glancy S, Hamel DR, Allman MS, Coakley KJ, Dyer SD, Hodge C, Lita AE, Verma VB, Lambrocco C, Tortorici E, Migdall AL, Zhang Y, Kumor DR, Farr WH, Marsili F, Shaw MD, Stern JA, Abellan C, Amaya W, Pruneri V, Jennewein T, Mitchell MW, Kwiat PG, Bienfang JC, Mirin RP, Knill E, and Nam SW, “Strong loophole-free test of local realism,” Phys. Rev. Lett 115, 250402 (2015). [PubMed: 26722906]

[10]. Pironio S, Acin A, Massar S, Boyer A, de la Giroday, Matsukevich DN, Maunz P, Olmschenk S, Hayes D, Luo L, Manning TA, and Monroe C, “Random numbers certified by Bell’s theorem,” Nature 464, 1021–4 (2010). [PubMed: 20393558]

[11]. Vazirani U and Vidick T, “Certifiable quantum dice - or, exponential randomness expansion,” in STOC’12 Proceedings of the 44th Annual ACM Symposium on Theory of Computing (2012) p. 61.

[12]. Fehr S, Gelles R, and Schaffner C, “Security and composability of randomness expansion from Bell inequalities,” Phys. Rev. A 87, 012335 (2013).

[13]. Miller CA and Shi Y, “Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices,” J. ACM 63, 33 (2016).

[14]. Miller CA and Shi Y, “Universal security for randomness expansion from the spot-checking protocol,” SIAM J. Comput 46, 1304–1335 (2017).

[15]. Chung K-M, Shi Y, and Wu X, “Physical randomness extractors: Generating random numbers with minimal assumptions,” (2014), arXiv:1402.4797 [quant-ph].

[16]. Coudron M and Yuen H, “Infinite randomness expansion with a constant number of devices,” in STOC’14 Proceedings of the 46th Annual ACM Symposium on Theory of Computing (2014) pp. 427–36.

[17]. Arnon-Friedman R, Dupuis F, Fawzi O, Renner R, and Vidick T, “Practical device-independent quantum cryptography via entropy accumulation,” Nat. Commun 9, 459 (2018). [PubMed: 29386507]

[18]. Nieto-Silleras O, Bamps C, Silman J, and Pironio S, “Device-independent randomness generation from several Bell estimators,” New J. Phys 20, 023049 (2018).

[19]. Bierhorst P, Knill E, Glancy S, Mink A, Jordan S, Rommal A, Liu Y-K, Christensen B, Nam SW, and Shalm LK, “Experimentally generated random numbers certified by the impossibility of superluminal signaling,” (2017), arXiv:1702.05178.

[20]. Bierhorst P, Knill E, Glancy S, Zhang Y, Mink A, Jordan S, Rommal A, Liu Y-K, Christensen B, Nam SW, , Stevens MJ, and Shalm LK, “Experimentally generated random numbers certified by the impossibility of superluminal signaling,” Nature 556, 223–226 (2018). [PubMed: 29643486]

[21]. Zhang Y, Glancy S, and Knill E, “Asymptotically optimal data analysis for rejecting local realism,” Phys. Rev. A 84, 062118 (2011).

[22]. Konig R, Renner R, and Schaffner C, “The operational meaning of min- and max-entropy,” IEEE Trans. Inf. Theory 55, 4337–4347 (2009).

[23]. Shafer G, Shen A, Vereshchagin N, and Vovk V, “Test martingales, Bayes factors and p-values,” Statistical Science 26, 84–101 (2011).

[24]. Popescu S and Rohrlich D, “Quantum nonlocality as an axiom,” Found. Phys 24, 379–85 (1994).

[25]. Barrett J, Linden N, Massar S, Pironio S, Popescu S, and Roberts D, “Nonlocal correlations as an information-theoretic resource,” Phys. Rev. A 71, 022101 (2005).

[26]. Lunghi Tommaso, Bohr Brask Jonatan, Ci Wen Lim Charles, Lavigne Quentin, Bowles Joseph, Martin Anthony, Zbinden Hugo, and Brunner Nicolas, “Self-testing quantum random number generator,” Phys. Rev. Lett 114, 150501 (2015). [PubMed: 25933297]

[27]. Van Himbeeck Thomas, Woodhead Erik, Cerf Nicolas J., Garcla-Patron Raul, and Pironio Stefano, “Semi-device-independent framework based on natural physical assumptions,” Quantum 1, 33 (2017).

[28]. Knill E, Zhang Y, and Bierhorst P, “Quantum randomness generation by probability estimation with classical side information,” (2017), arXiv:1709.06159.

[29]. Tomamichel M, Colbeck R, and Renner R, “A fully quantum asymptotic equipartition property,” IEEE Trans. Inf. Theory 55, 5840–5847 (2009).

[30]. Clauser JF, Horne MA, Shimony A, and Holt RA, “Proposed experiment to test local hidden-variable theories,” Phys. Rev. Lett 23, 880–884 (1969).

[31]. Acin Antonio, Massar Serge, and Pironio Stefano, “Randomness versus non-locality and entanglement,” Phys. Rev. Lett 108, 100402 (2012). [PubMed: 22463395]

[32]. Nieto-Silleras O, Pironio S, and Silman J, “Using complete measurement statistics for optimal device-independent randomness evaluation,” New J. Phys 16, 013035 (2014).

[33]. Bancal J-D, Sheridan L, and Scarani V, “More randomness from the same data,” New J. Phys 16, 033011 (2014).

[34]. Eberhard PH, “Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment,” Phys. Rev. A 47, R747–R750 (1993). [PubMed: 9909100]

[35]. van Dam W, Gill RD, and Grunwald PD, “The statistical strength of non-locality proofs,” IEEE Trans. Inf. Theory. 51, 2812–2835 (2005).

[36]. Acin Antonio, Gill Richard, and Gisin Nicolas, “Optimal Bell tests do not require maximally entangled states,” Phys. Rev. Lett 95, 210402 (2005). [PubMed: 16384120]

[37]. Zhang Yanbao, Knill Emanuel, and Glancy Scott, “Statistical strength of experiments to reject local realism with photon pairs and inefficient detectors,” Phys. Rev. A 81, 032117 (2010).

[38]. Cirelson BS, “Quantum generalizations of Bell’s inequality,” Lett. Math. Phys 4, 93 (1980).

[39]. Pardo MC and Vajda Igor, “About distances of discrete distributions satisfying the data processing theorem of information theory,” IEEE Trans. Inf. Theory 43, 1288–1293 (1997).

[40]. Ville J, Etude Critique de la Notion de Collectif (Gauthier-Villars, Paris, 1939).

[41]. Zhang Y, Glancy S, and Knill E, “Efficient quantification of experimental evidence against local realism,” Phys. Rev. A 88, 052119 (2013).

[42]. Christensen BG, Hill A, Kwiat PG, Knill E, Nam SW, Coakley K, Glancy S, Shalm LK, and Zhang Y, “Analysis of coincidence-time loopholes in experimental Bell tests,” Phys. Rev. A 92, 032130 (2015).

[43]. Shao Jun, Mathematical Statistics, 2nd ed (Springer, New York, 2003).

[44]. Konig R and Terhal B, “The bounded-storage model in the presence of a quantum adversary,” IEEE Trans. Inf. Theory 54, 749–62 (2008).

[45]. Trevisan L, “Extractors and pseudorandom generators,” Journal of the ACM 48, 860–79 (2001).

[46]. Mauerer W, Portmann C, and Scholz VB, “A modular framework for randomness extraction based on trevisan’s construction,” (2012), arXiv:1212.0520, code available on github.

[47]. Knill E, Glancy S, Nam SW, Coakley K, and Zhang Y, “Bell inequalities for continuously emitting sources,” Phys. Rev. A 91, 032105 (2015).

[48]. Kullback S and Leibler RA, “On information and sufficiency,” Ann. Math. Statist 22, 79 (1951).

[49]. Bierhorst P, “Geometric decompositions of Bell poly-topes with practical applications,” J. Phys. A: Math. Theor 49, 215301 (2016).

[50]. Acin Antonio, Brunner Nicolas, Gisin Nicolas, Massar Serge, Pironio Stefano, and Scarani Valerio, “Device-independent security of quantum cryptography against collective attacks,” Phys. Rev. Lett 98, 230501 (2007). [PubMed: 17677888]

[51]. Pironio Stefano, Acin Antonio, Brunner Nicolas, Gisin Nicolas, Massar Serge, and Scarani Valerio, “Device-independent quantum key distribution secure against collective attacks,” New J. Phys 11, 045021 (2009).

[52]. The argument can be generalized to the case that the input distribution is not precisely known after considering the construction of the corresponding PEFs detailed in Ref. [28].

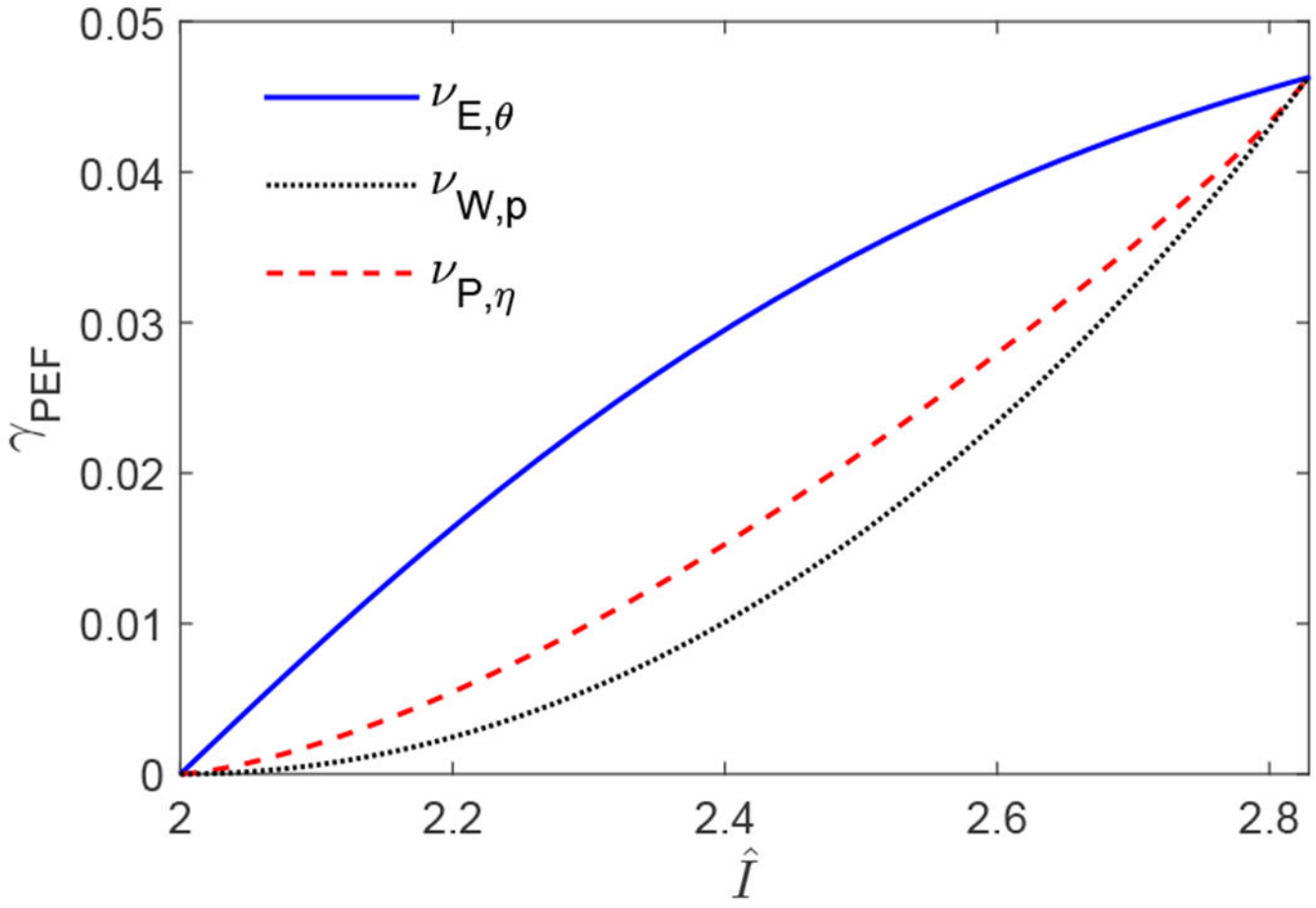

FIG. 1:

Maximum certificate rates γ_{PEF} (Eq. (6)) as a function of $\hat{I}$ for each family of distributions.

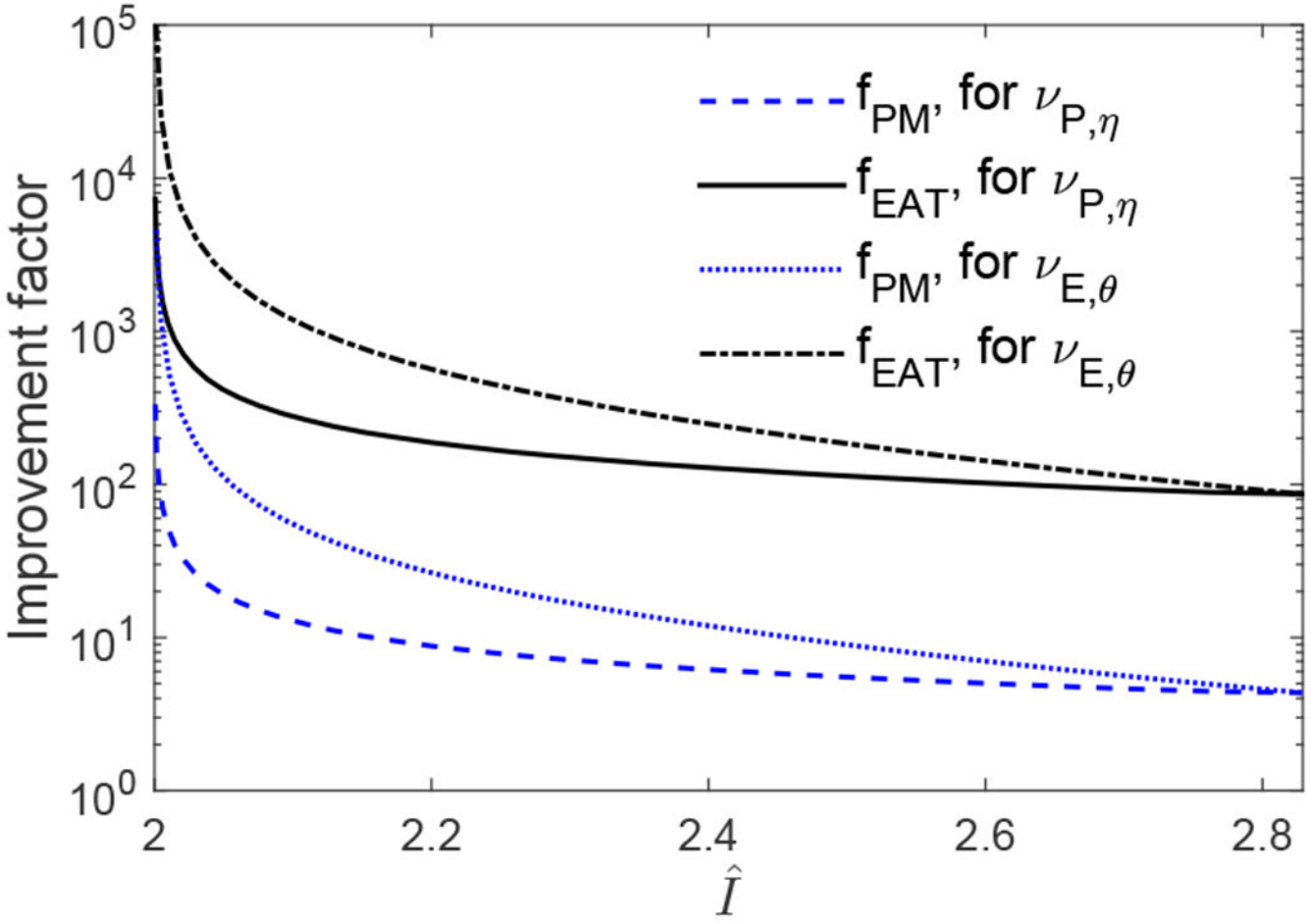

FIG. 2:
Improvement factors as a function of $\hat{I}$.