arXiv:1803.06219v1 [quant-ph] 22 Feb 2018

Experimentally Generated Randomness Certified by the Impossibility of Superluminal Signals

Peter Bierhorst,[1*] Emanuel Knill,[1,6] Scott Glancy,[1] Yanbao Zhang,[1†]
Alan Mink,[2,3] Stephen Jordan,[2] Andrea Rommal,[4] Yi-Kai Liu,[2]
Bradley Christensen,[5] Sae Woo Nam,[1] Martin J. Stevens,[1] Lynden K. Shalm[1]

[1]National Institute of Standards and Technology, Boulder 80305, CO, USA
[2] National Institute of Standards and Technology, Gaithersburg 20899, MD, USA
[3] Theiss Research, La Jolla, CA, 92037, USA
[4] Muhlenberg College, Allentown, PA, 18104, USA
[5] Department of Physics, University of Wisconsin, Madison, WI, 53706, USA
[6]Center for Theory of Quantum Matter, University of Colorado, Boulder, Colorado 80309, USA
[†]Present address: NTT Basic Research Laboratories and NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan
[*] E-mail: peter.bierhorst@nist.gov

From dice to modern complex circuits, there have been many attempts to build increasingly better devices to generate random numbers. Today, randomness is fundamental to security and cryptographic systems, as well as safeguarding privacy. A key challenge with random number generators is that it is hard to ensure that their outputs are unpredictable [1–3]. For a random number generator based on a physical process, such as a noisy classical system or an elementary quantum measurement, a detailed model describing the underlying physics is required to assert unpredictability. Such a model must make a number of assumptions that may not be valid, thereby compromising the integrity of the device. However, it is possible to exploit the phenomenon of quantum nonlocality with a loophole-free Bell test to build a random number generator that can produce output that is unpredictable to any adversary limited only by general physical principles [1–11]. With recent technological developments, it is now possible to carry out such a loophole-free Bell test [12–14]. Here we present certified randomness obtained from a photonic Bell experiment and extract 1024 random bits uniform to within 10^{-12}. These random bits could not have been predicted within any physical theory that prohibits superluminal signaling and allows one to make independent measurement choices. To certify and quantify the ran-

domness, we describe a new protocol that is optimized for apparatuses characterized by a low per-trial violation of Bell inequalities. We thus enlisted an experimental result that fundamentally challenges the notion of determinism to build a system that can increase trust in random sources. In the future, random number generators based on loophole-free Bell tests may play a role in increasing the security and trust of our cryptographic systems and infrastructure.

The search for certifiably unpredictable random number generators is motivated by applications, such as secure communication, for which the predictability of pseudorandom strings make them unsuitable. Private randomness is required to initiate and authenticate virtually every secure communication [15], and public randomness from randomness beacons can be used for public certification and resource distribution in many settings [16]. To certify randomness, one can perform an experiment known as a Bell test [17], which in its simplest form performs measurements on an entangled system located in two physically separated measurement stations, with each station choosing between two types of measurements. After multiple experimental trials with varying measurement choices, if the measurement data violates conditions known as "Bell inequalities," then the data can be certified to contain randomness under weak assumptions.

Our randomness generation employs a "loophole-free" Bell test, which notably is characterized by high detection efficiency and space-like separation of the measurement stations during each experimental trial. The bits are unpredictable assuming that (1) the choices of measurement settings are independent of the experimental devices and pre-existing classical information about them and (2) in each experimental trial, the measurement outcomes at each station are independent of the settings choices at the other station. The first assumption is ultimately untestable, but the premise that it is possible to choose measurement settings independently of a system being measured is often tacitly invoked in the interpretation of many scientific experiments and laws of physics [18]. The second assumption can only be violated if one admits a theory that permits sending signals faster than the speed of light, given our trust that the space-like separation of the relevant events in the experiment is accurately verified by the timing electronics and that results are final when recorded. We also trust that the classical computing equipment used to process the data operates according to specification.

Under the above assumptions, the output randomness is certified to be unpredictable with respect to a real or hypothetical actor "Eve" in possession of the pre-existing classical information, physically isolated from the devices while they are under our control, and without access to data produced during the protocol. The bits remain unpredictable to Eve if she learns the settings at any time after her last interaction with the devices. If the devices are trusted, which is reasonable if we built them, then this may be well before the start of the protocol, in which case the settings can come from public randomness [2,10]. In particular, one can use an existing public randomness source, such as the NIST random beacon [16], to generate much needed private randomness as output. Since the assumptions do not constrain the specific physical realization of the devices and do not require specific states or measurements, they implement a "device-independent" framework [19] which allows an individual user to assure security with minimal assumptions about the devices. If Eve has quantum memory, it is possible to ensure that Eve's side information is effectively classical by verifying that the devices have no long-term quantum memory of past interactions with Eve. While this introduces weak device-dependence, for the foreseeable future this verification task is comparable to that required to enforce the absence of communication from the devices to Eve.

The only previous experimental production of certified randomness from Bell test data was reported in the ground-breaking paper by Pironio et al. [5]. Their Bell test was implemented with ions in two separate ion-traps, closing the detection loophole [20] but without space-like separation. Indeed, Bell tests achieving space-like separation without other experimental loopholes have been performed only recently [12–14, 21]. Under more restrictive assumptions than ours, the maximum amount of randomness in principle available in the data of Pironio et al. was quantified as 42 bits with an error parameter of 0.01, but they did not extract a uniformly distributed bit string from their data. Pironio et al. argue that any interaction between measurement stations in their experiment is negligible, because they are located in separate ion-traps, each in its own vacuum chamber. However, any shielding between the stations is necessarily incomplete; for example they must have an open quantum channel to establish entanglement. Mundane physical effects can allow local-realistic systems to appear to violate Bell inequalities when shielding is incomplete. Relying instead on the impossibility of faster-than-light communication provides stronger assurance of the unpredictability of the randomness.

We generated randomness using an improved version of the loophole-free Bell test reported in Ref. [13]. Five new data sets were collected, with the best-performing data set yielding 1024 new random bits uniform to within 10^{-12}. We also obtained 256 random bits from the main data set analyzed in Ref. [13], albeit only uniform to within 0.02. The experiment, illustrated in Fig. 1, consisted of a source of entangled photons and two measurement stations named "Alice" and "Bob". During an experimental trial, at each station a random choice was made between two measurement settings labeled 0 and 1, after which a measurement outcome of detection (+) or nondetection (0) was recorded. Each station's implementation of the measurement setting was space-like separated from the other station's measurement event, and no postselection was employed in collecting the data. See the Methods section for details. For trial i, we model Alice's settings choices with the random variable X_i and Bob's with Y_i, both of which take values in the set $\{0, 1\}$. Alice's and Bob's measurement outcome random variables are respectively A_i and B_i, both of which take values in the set $\{$+$, 0\}$. When referring to a generic single trial, we omit indices. With this notation, a general Bell inequality for our scenario can be expressed in the form [22]

$$\sum_{abxy} s^{ab}_{xy} \mathbb{P}(A = a, B = b|X = x, Y = y) \leq \beta, \tag{1}$$

where the s^{ab}_{xy} are fixed real coefficients indexed by a, b, x, y that range over all possible values of A, B, X, Y. The upper bound β is required to be satisfied whenever the settings-conditional outcome probabilities are induced by a model satisfying "local realism" (LR). LR distributions, which cannot be certified to contain randomness, are those for which $\mathbb{P}(A = a, B = b|X = x, Y = y)$ is of the form $\sum_\lambda \mathbb{P}(A = a|X = x, \Lambda = \lambda)\mathbb{P}(B = b|Y = y, \Lambda = \lambda)\mathbb{P}(\Lambda = \lambda)$ for a random variable Λ representing local hidden variables. The Bell inequality is non-trivial if there exists a quantum-realizable distribution that can violate the bound β.

It has long been known that experimental violations of Bell inequalities such as Eq. 1 indicate the presence of randomness in the data. To quantify randomness with respect to Eve, we represent Eve's initial classical information by a random variable E. We formalize the assumption that measurement settings can be generated independently of the system being measured and Eve's information with the following condition:

$$\mathbb{P}(X_i = x, Y_i = y | E = e, \text{past}_i) = \mathbb{P}(X_i = x, Y_i = y) = \frac{1}{4} \quad \forall x, y, e, \tag{2}$$

where past_i represents events in the past of the i'th trial, specifically including the trial settings and outcomes for trial 1 through $i - 1$. Our other assumption, that measurement outcomes are independent of remote measurement choices, is formalized as follows:

$$\begin{aligned} \mathbb{P}(A_i = a | X_i = x, Y_i = y, E = e, \text{past}_i) &= \mathbb{P}(A_i = a | X_i = x, E = e, \text{past}_i) \\ \mathbb{P}(B_i = b | X_i = x, Y_i = y, E = e, \text{past}_i) &= \mathbb{P}(B_i = b | Y_i = y, E = e, \text{past}_i) \quad \forall x, y, e. \end{aligned} \tag{3}$$

These equations are commonly referred to as the "non-signaling" assumptions, although they are often stated without the conditionals E and past_i. Our space-like separation of settings and remote measurements provide assurance that the experiment obeys Eqs. 3. We remark that if one assumes the measured systems obey quantum physics, stronger constraints are possible [23,24].

Given Eqs. 2 and 3, our protocol produces random bits in two sequential parts. For the first part, "entropy production", we implement n trials of the Bell test, from which we compute a statistic V related to a Bell inequality (Eq. 1). V quantifies the Bell violation and determines whether or not the protocol passes or aborts. If the protocol passes, we certify an amount of randomness in the outcome string even conditioned on the setting string and E. In the second part, "extraction," we process the outcome string into a shorter string of bits whose distribution is close to uniform. We used our customized implementation of the Trevisan extractor [25] derived from the framework of Mauerer, Portmann and Scholz [26] and the associated open source code. We call this the TMPS algorithm, see Supplementary Information (SI) S.4 for details.

We applied a new method of certifying the amount of randomness in Bell tests. Previous methods for related models with various sets of assumptions [2–8, 27–29] are ineffective in our experimental regime (SI S.7), which is characterized by a small per-trial violation of Bell inequalities. Other recent works that explore how to effectively certify randomness from a wider range of experimental regimes assume that measured states are independent and identically distributed (i.i.d.) or that the regime is asymptotic [9–11, 30]. Our method, which does not require these assumptions, builds on the Prediction-Based Ratio (PBR) method for rejecting LR [31]. Applying this method to training data (see below), we obtain a real-valued "Bell function" T with arguments A, B, X, Y that satisfies $T(A, B, X, Y) > 0$ with expectation $\mathbb{E}(T) \leq 1$ for any LR distribution satisfying Eq. 2. From T we determine the maximum value $1 + m$

of $\mathbb{E}(T)$ over all distributions satisfying Eqs. 2 and 3, where we require that $m > 0$. Such a function T induces a Bell inequality (Eq. 1) with $\beta = 4$ and $s_{xy}^{ab} = T(a, b, x, y)$. Define $T_i = T(A_i, B_i, X_i, Y_i)$ and $V = \prod_{i=1}^{n} T_i$. If the experimenter observes a value of V larger than 1, this indicates a violation of the Bell inequality and the presence of randomness in the data. The randomness is quantified by the following theorem, proven in the SI S.2. Below, we denote all of the settings of both stations with $\mathbf{XY} = X_1Y_1X_2Y_2...X_nY_n$, and other sequences such as $\mathbf{AB}$ and $\mathbf{ABXY}$ are similarly interleaved over n trials.

Entropy Production Theorem. Suppose T is a Bell function satisfying the above conditions. Then in an experiment of n trials obeying Eqs. 2 and 3, the following inequality holds for all $\epsilon_{\text{p}} \in (0, 1)$ and v_{thresh} satisfying $1 \leq v_{\text{thresh}} \leq (1 + (3/2)m)^n \epsilon_{\text{p}}^{-1}$:

$$\mathbb{P}_e \left(\mathbb{P}_e(\mathbf{AB}|\mathbf{XY}) > \delta \text{ AND } V \geq v_{\text{thresh}} \right) \leq \epsilon_p \tag{4}$$

where $\delta = [1 + (1 - \sqrt[n]{\epsilon_{\text{p}} v_{\text{thresh}}})/(2m)]^n$ and $\mathbb{P}_e$ denotes the probability distribution conditioned on the event $\{E = e\}$, where e is arbitrary. The expression $\mathbb{P}_e(\mathbf{AB}|\mathbf{XY})$ denotes the random variable that takes the value $\mathbb{P}_e(\mathbf{AB} = \mathbf{ab}|\mathbf{XY} = \mathbf{xy})$ when $\mathbf{ABXY}$ takes the value $\mathbf{abxy}$.

In words, the theorem says that with high probability, if V is at least as large as v_{thresh}, then the output $\mathbf{AB}$ is unpredictable, in the sense that no individual outcome $\{\mathbf{AB} = \mathbf{ab}\}$ occurs with probability higher than δ, even given the information $\{\mathbf{XY}E = \mathbf{xy}e\}$. The theorem supports a protocol that aborts if V takes a value less than v_{thresh}, and passes otherwise. If the probability of passing were 1, then $-\log_2(\delta)$ would be a so-called "smooth min-entropy", a quantity that characterizes the number of uniform bits of randomness that are in principle available in $\mathbf{AB}$ [32, 33]. We show in the SI S.3 that for constant ϵ_{p}, $-\log_2(\delta)$ is proportional to the number of trials. How many bits we can actually extract depends on ϵ_{fin}, the final output's maximum allowed distance from uniform. We also show in the SI that the Entropy Production Theorem can still be proved if Eq. 2 is weakened so that settings probabilities need not be known but are constrained to be within α of $1/4$ with $\alpha < 1/4$, while still being conditionally independent of earlier outcomes given earlier settings. Such a weakening is relevant for experiments [12–14] that use physical random number generators to choose the settings, for which the settings probabilities cannot be known exactly.

To extract the available randomness in $\mathbf{AB}$, we use the TMPS algorithm to obtain an extractor, specifically a function Ext that takes as input the string $\mathbf{AB}$ and a length d "seed" bit string $\mathbf{S}$, where $\mathbf{S}$ is uniform and independent of $\mathbf{ABXY}$. Its output is a length t bit string. $\mathbf{S}$ can be obtained from d additional instances of the random variables X_i, so Eq. 2 ensures the needed independence and uniformity conditions on $\mathbf{S}$. In order for the output to be within a distance ϵ_{fin} of uniform independent of $\mathbf{XY}$ and E, the entropy production and extractor parameters must satisfy the constraints given in the next theorem, proven in the SI S.5. In the statement of the theorem, the measure of distance used is the "total variation (TV) distance," expressed by the left side of Eq. 6, and "pass" is the event that V exceeds v_{thresh}.

Protocol Soundness Theorem. Let $0 < \epsilon_{\text{ext}}, \kappa < 1$. Suppose that $\mathbb{P}(\text{pass}) \geq \kappa$ and suppose that that the protocol parameters satisfy

$$t + 4\log_2 t \leq -\log_2 \delta + \log_2 \kappa + 5\log_2 \epsilon_{\text{ext}} - 11. \tag{5}$$

Then the output $\mathbf{U} = \text{Ext}(\mathbf{AB}, \mathbf{S})$ of the function obtained by the TMPS algorithm satisfies

$$\frac{1}{2}\sum_{\mathbf{u},\mathbf{xys}e} \Big|\mathbb{P}\big(\mathbf{U}=\mathbf{u}, \mathbf{XYS}E = \mathbf{xys}e|\text{pass}\big) - \mathbb{P}^{\text{unif}}(\mathbf{U}=\mathbf{u})\mathbb{P}\big(\mathbf{XY}E = \mathbf{xy}e|\text{pass}\big)\mathbb{P}^{\text{unif}}(\mathbf{S}=\mathbf{s})\Big| \leq \epsilon_{\text{p}}/\mathbb{P}(\text{pass}) + \epsilon_{\text{ext}}, \tag{6}$$

where $\mathbb{P}^{\text{unif}}$ denotes the uniform probability distribution.

The number of seed bits d required satisfies $d = O(\log(t)\log(nt/\epsilon_{\text{ext}})^2)$, and SI S.4 gives an explicit bound.

The theorem provides several options for quantifying the uniformity of the randomness produced. A goal is for the protocol to be nearly indistinguishable according to TV distance from an ideal protocol, where in an ideal protocol the randomness is perfectly uniform conditional on passing. For this, the ideal protocol can be chosen to have the same probability of passing with behavior matching that of the real protocol when aborting. The theorem implies that the unconditional distribution of the protocol is within TV distance $\max(\epsilon_{\text{p}} + \epsilon_{\text{ext}}, \kappa)$ of that of an ideal protocol (SI S.5). For this distance, if the probability of passing is comparable to κ, then the conditional TV distance from uniform, given in Eq. 6, could be large. It is desirable that even for the worst case probability of passing, the conditional TV distance be small. Accordingly, we quantify the uniformity for our implementation with $\epsilon_{\text{fin}} = \max(\epsilon_{\text{p}}/\kappa + \epsilon_{\text{ext}}, \kappa)$. Then, for any probability of passing greater than ϵ_{fin}, conditionally on passing, the TV distance from uniform is at most ϵ_{fin}.

We applied our protocol to five data sets using the setup based on that described in Ref. [13] with improvements described in the Methods section. Each data set was collected in five to ten minutes, improving on the approximately one month duration of data acquisition reported in Ref. [5]. Before starting the protocol, we set aside the first 5×10^6 trials of each data set as training data, which we used to choose parameters needed by the protocol. With the training data removed, the number n of trials used by the protocol was between 2.5×10^7 and 5.5×10^7 for each data set. We used the training data to determine a Bell function T with statistically strong violation of LR on the training data according to the PBR method [31]; see SI S.3. The function T obtained for the fifth data set, which was longest in duration and produced the most randomness, is given in Table 1 as an example. We computed thresholds v_{thresh} so that a sample of n i.i.d. trials from the distribution inferred from the training data would have a high probability for exceeding v_{thresh}.

For the fifth data set, a sample of n i.i.d. trials from the distribution inferred from the training data would have approximately 0.99 probability of exceeding a threshold of $v_{\text{thresh}} = 1.5 \times 10^{32}$. This would allow the extraction of 1024 bits uniform to within $\epsilon_{\text{fin}} = 10^{-12}$, using $\epsilon_{\text{p}} = \kappa^2 =$

Table 1: **Bell function T obtained from Data Set 5.** We used a numerical method based on maximum likelihood to infer a non-signaling distribution based on the raw counts of the training trials, namely the first 5×10^6 trials. We then determined the function T that maximizes $\mathbb{E}(\ln T)$ according to this distribution, subject to the constraints that $\mathbb{E}(T)_{LR} \leq 1$ for all LR distributions and $T(0, 0, x, y) = 1$ for all x, y. The latter constraint improves the signal-to-noise for our data. The function T yields $m = 0.0100425$, and $\mathbb{E}(T) = 1.000003931$ for the non-signaling distribution inferred from the training data. One can also interpret the numbers below as the coefficients s_{xy}^{ab} in Eq. 1, which defines a Bell inequality with $\beta = 4$. The values of T are rounded down at the tenth digit.

	$ab = ++$	$ab = +0$	$ab = 0+$	$ab = 00$
$xy = 00$	1.0243556353	0.9704647804	0.9735507658	1
$xy = 01$	1.0256127409	0.9491951243	0.9960775334	1
$xy = 10$	1.0227274988	0.9962782754	0.9461091383	1
$xy = 11$	0.9273040563	1.0037217225	1.0039224645	1

9.025×10^{-25} and $\epsilon_{\text{ext}} = 5 \times 10^{-14}$. These values were chosen based on a numerical study of the constraints on the number t of bits extracted for fixed values of $\epsilon_{\text{fin}} = 10^{-12}$. Running the protocol on the remaining $55, 110, 210$ trials with these parameters, the product $\prod_{i=1}^{n} T_i$ exceeded v_{thresh}, and so the protocol passed. Applying the extractor to the resulting output string $\mathbf{AB}$ with a seed of length $d = 315, 844$, we extracted 1024 bits, certified to be uniform to within 10^{-12}, the first ten of which are 1110001001. Figure 2 displays the extractable bits for alternative choices of ϵ_{fin} for all five data sets.

We also applied the protocol to data from the experiment of Ref. [13]. This experiment was more conservative in taking additional measures to ensure that it was loophole-free, including space-like separation of the measurement choices from both the downconversion event and the remote measurement outcomes. We extracted 256 bits at $\epsilon_{\text{fin}} = 0.02$ from the best data set, XOR 3, reported in Ref. [13]. The distance from an ideal protocol as explained after the Protocol Soundness Theorem was 4.00×10^{-4}, without accounting for possible bias in the random source used. For details see SI S.6.

For the data set producing 1024 new near random bits, our protocol used 1.10×10^8 uniform bits to choose the settings and 3.16×10^5 uniform bits to choose the seed. Because the extractor used is a "strong" extractor, the seed bits are still uniform conditional on passing, so they can be recovered at the end of the protocol for uses elsewhere. This is not the case for the settings-choice bits because the probability of passing is less than 1. To reduce the entropy used for the settings, our protocol can be modified to use highly biased settings choices [5]. Reducing settings entropy is not a priority if the settings and seed bits come from a public source of randomness, in which case the output bits can still be certified to be unknown to external observers such as Eve and the current protocol is an effective method for private randomness generation [2, 10].

For future work, we hope to take advantage of the adaptive capabilities of the Entropy

Production Theorem (SI S.2) to dynamically compensate for experimental drift during run time. In view of advances toward practical quantum computing it is desirable to study the protocol in the presence of quantum side information, which may require more conservative randomness generation. We also look forward to technical improvements in experimental equipment for larger violation and higher trial rates. These will enable faster generation of random bits with lower error and support the use of biased settings choices.

Existing randomness generation systems rely on detailed assumptions about the specific physics underlying the devices. With the advent of loophole-free Bell tests, it is now possible to build quantum devices that exploit quantum nonlocality to remove many of the device-dependent assumptions in current technological implementations. Our device-independent random number generator is an example of such a system. Such generators can provide the best method currently known for physically producing randomness, thereby improving the security of a wide range of applications.

Methods We used polarization-entangled photons generated by a nonlinear crystal pumped by a pulsed, picosecond laser at approximately 775 nm in a configuration similar to that reported in Ref. [13], but with several improvements to increase the rate of randomness extraction. The laser's repetition rate was 79.3 MHz, and each pulse that entered the crystal had a probability of ≈ 0.003 of creating an entangled photon pair in the state $|\psi\rangle \approx 0.982\,|HH\rangle + 0.191\,|VV\rangle$ at a center wavelength of 1550 nm. By pumping the crystal with approximately five times as much power, and using a 20 mm long crystal, we were able to substantially increase the per-pulse probability of generating a downconversion event compared with Ref. [13] while maintaining similar overall system efficiencies. The two entangled photons from each pair were separately sent to one of the two measurement stations (187 ± 1) m apart. At Alice and Bob, a Pockels cell and polarizer combined to allow the rapid switching of measurement bases and measurement of the polarization state of the incoming photons. Each Pockels cell operated at a rate of 100 kHz, allowing us to perform 100,000 trials per second (the driver electronics on the Pockels cells sets this rate). The photons were then detected using fiber-coupled superconducting single-photon nanowire detectors, with Bob's detector operating at approximately 90% efficiency and Alice's detector operating with approximately 92% efficiency [34]. For this experiment, the total symmetric system heralding efficiency was $(75.5 \pm 0.5\%)$, which is above the 71.5% threshold required to close the detection-loophole for our experimental configuration after accounting for unwanted background counts at our detectors and slight imperfections in our state preparation and measurements components.

With this configuration, Bob completed his measurement (294.4 ± 3.7) ns before a hypothetical switching signal travelling at light speed from Alice's Pockels cell could arrive at his station. Similarly, Alice completed her measurement (424.2 ± 3.7) ns before such a signal from Bob's Pockels cell could arrive at her location. Each trial's outcome values were obtained by aggregating the photon detection or non-detection events from several short time intervals lasting 1024 ps, each of which is timed to correspond to one pulse of the pump laser. If any photons were detected in the short intervals, the outcome is "+", and if no photons were detected, the outcome is “0”. The experiment of Ref. [13] used at most 7 short intervals, but here we were able to include 14 intervals while maintaining space-like separation, which further increased the probability of observing a photon during each trial. For demonstration purposes, Alice and Bob each used Python’s `random.py` module with the default generator (the Mersenne twister) to pick their settings at each trial. This pseudorandom source is predictable, and for secure applications of the protocol in an adversarial scenario, such as if the photon pair source or measurement devices are obtained from an untrusted provider, settings choices must be based on random sources that are effectively not predictable. However, based on our knowledge of device construction, we know that our devices have no physical resources for predicting pseudo-random numbers and expect that measurement settings were effectively independent of relevant devices so that Eqs. 2 and 3 still hold. We remark that the settings choices for the XOR 3 data set were based on physical random sources.

With the improved detection efficiency, the higher per-trial probability of for Alice and Bob to detect a photon, and a higher signal-to-background counts ratio we are able to improve both the magnitude of our Bell violation as well as reduce the number of trials required to achieve a statistically significant violation by an order of magnitude.

References

[1] Acín, A. & Masanes, L. Certified randomness in quantum physics. *Nature* **540**, 213 (2016).

[2] Pironio, S. & Massar, S. Security of practical private randomness generation. *Phys. Rev. A* **87**, 012336 (2013).

[3] Miller, C. & Shi, Y. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM* **63**, 33:1–33:63 (2016).

[4] Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A: Math. Theor.* **44**, 095305 (2011).

[5] Pironio, S. *et al.* Random numbers certified by Bell’s theorem. *Nature* **464**, 1021–4 (2010).

[6] Vazirani, U. & Vidick, T. Certifiable quantum dice - or, exponential randomness expansion. In *STOC’12 Proceedings of the 44th Annual ACM Symposium on Theory of Computing*, 61 (2012).

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

[8] Chung, K.-M., Shi, Y. & Wu, X. Physical randomness extractors: Generating random numbers with minimal assumptions (2014). ArXiv:1402.4797 [quant-ph].

[9] Nieto-Silleras, O., Pironio, S. & Silman, J. Using complete measurement statistics for optimal device-independent randomness evaluation. *New Journal of Physics* **16**, 013035 (2014).

[10] Bancal, J.-D., Sheridan, L. & Scarani, V. More randomness from the same data. *New Journal of Physics* **16**, 033011 (2014).

[11] Thinh, L., de la Torre, G., Bancal, J.-D., Pironio, P. & Scarani, V. Randomness in post-selected events. *New Journal of Physics* **18**, 035007 (2016).

[12] Hensen, B. *et al.* Loophole-free Bell inequality violation using electron spins separated by 1.3 km. *Nature* **526**, 682 (2015).

[13] Shalm, L. K. *et al.* Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).

[14] Giustina, M. *et al.* Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).

[15] Paar, C. & Pelzl, J. *Understanding Crypotgraphy* (Springer-Verlag Berlin Heidelberg, New York, 2010).

[16] Fischer, M. J., Iorga, M. & Peralta, R. A public randomness service. In *SECRYPT 2011*, 434–38 (2011).

[17] Bell, J. On the Einstein Podolsky Rosen paradox. *Physics* **1**, 195–200 (1964).

[18] Bell, J. S., Shimony, A., Horne, M. A. & Clauser, J. F. An exchange on local beables. *Dialectica* **39**, 85–96 (1985).

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

[20] Pearle, P. M. Hidden-variable example based upon data rejection. *Phys. Rev. D* **2**, 1418–1425 (1970).

[21] Rosenfeld, W. *et al.* Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.* **119**, 010402 (2017).

[22] Brunner, N., Cavalcanti, D., Pironio, S., Scarani, V. & Wehner, S. Bell nonlocality. *Rev. Mod. Phys.* **86**, 419–78 (2014).

[23] Cirel'son, B. S. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.* **4**, 93–100 (1980).

[24] Navascués, M., Pironio, S. & Acín, A. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics* **10**, 073013 (2008).

[25] Trevisan, L. Extractors and pseudorandom generators. *J. ACM* **48**, 860–79 (2001).

[26] Mauerer, W., Portmann, C. & Scholz, V. A modular framework for randomness extraction based on Trevisan's construction (2012). ArXiv:1212.0520 [cs.IT].

[27] Coudron, M. & 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*, 427–36 (2014).

[28] Dupuis, F., Fawzi, O. & Renner, R. Entropy accumulation (2016). ArXiv:1607.01796 [quant-ph].

[29] Arnon-Friedman, R., Renner, R. & Vidick, T. Simple and tight device-independent security proofs (2016). ArXiv:1607.01797 [quant-ph].

[30] Miller, C. & Shi, Y. Universal security for randomness expansion from the spot-checking protocol (2014). ArXiv:1411.6608 [quant-ph].

[31] Zhang, Y., Glancy, S. & Knill, E. Asymptotically optimal data analysis for rejecting local realism. *Phys. Rev. A* **84**, 062118 (2011).

[32] Trevisan, L. & Vadhan, S. Extracting randomness from samplable distributions. In *FOCS '00 Proceedings of the 41st Annual Symposium on Foundations of Computer Science* (IEEE Computer Society, Washington, DC, 2000).

[33] Renner, R. *Security of Quantum Key Distribution*. Ph.D. thesis, ETH, ETH, Switzerland (2006). ArXiv:quant-ph/0512258.

[34] Marsili, F. *et al.* Detecting single infrared photons with 93% system efficiency. *Nature Photonics* **7**, 210–214 (2013).

Acknowledgments We thank Carl Miller and Kevin Coakley for comments on the manuscript. A.M. acknowledges financial support through NIST grant 70NANB16H207.

Author Contributions P.B. led the project and implemented the protocol. P.B., E.K., S.G. and Y.Z. developed the protocol theory. A.M., S.J., A.R. and Y.-K. L. were responsible for extractor theory and implementation. B.C., S.W.N., M.J.S. and L.K.S. collected and interpreted the data. PB., E.K., S.G. and L.K.S. wrote the manuscript.

Author Information This work is a contribution of the National Institute of Standards and Technology and is not subject to U.S. copyright. The authors declare no competing financial interests. Correspondence and requests for materials should be addressed to P.B. (peter.bierhorst@nist.gov).

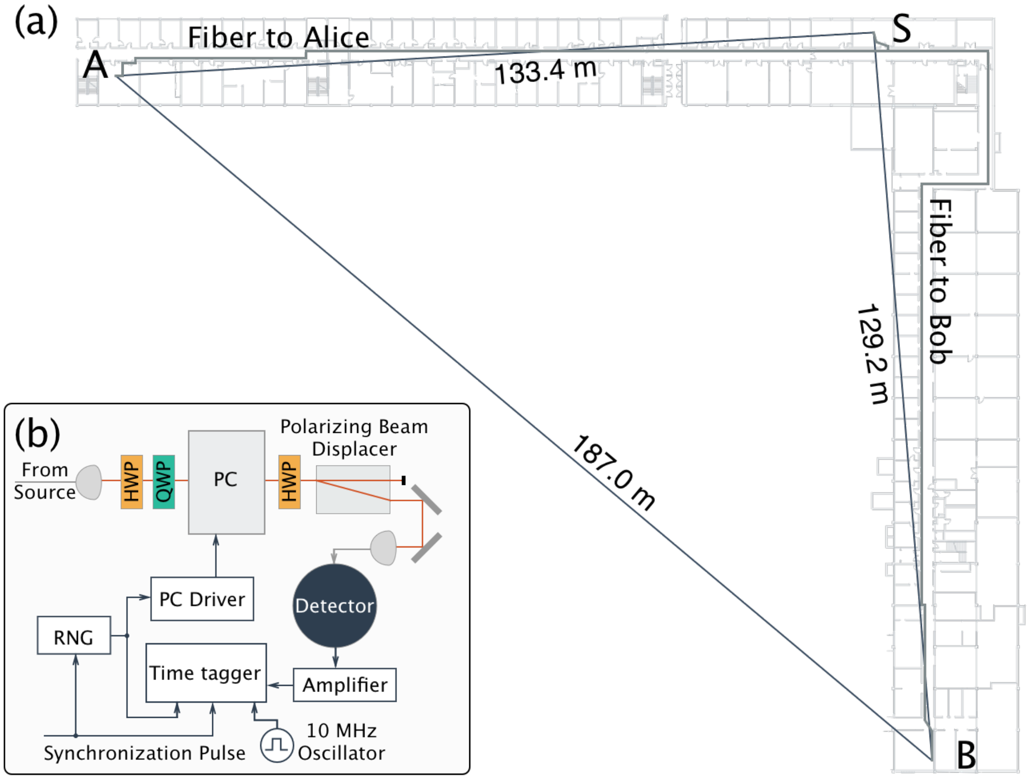

Figure 1: **The locations of the Source (S), Alice (A) and Bob (B)**. Each trial, the source lab produces a pair of photons in the non-maximally polarization-entangled state $|\psi\rangle \approx 0.982\,|HH\rangle + 0.191\,|VV\rangle$, where H (V) denotes horizontal (vertical) polarization. One photon is sent to Alice's lab while the other is sent to Bob's lab to be measured as shown in inset (b). Alice's computed optimal polarization measurement angles, relative to a vertical polarizer, are $\{a = -3.7^o, a' = 23.6^o\}$ while Bob's are $\{b = 3.7^o, b' = -23.6^o\}$. Both Alice and Bob use a fast Pockels cell (PC), two half-waveplates (HWP), a quarter-waveplates (QWP), and a polarizing beam displacer to switch between their respective polarization measurements. A pseudorandom number generator (RNG) governs the choice of each measurement setting every trial. After passing through the polarization optics, the photons are coupled into a single-mode fiber and sent to a superconducting nanowire detector. The signals from the detector are then amplified and sent to a time tagger where their arrival times are recorded and the measurement outcome is fixed. A 10 MHz oscillator keeps Alice and Bob's timetagger clocks locked. Alice and Bob are (187 ± 1) m apart. At this distance, Alice's measurement outcome is space-like separated from the triggering of Bob's Pockels cell and vice-versa.

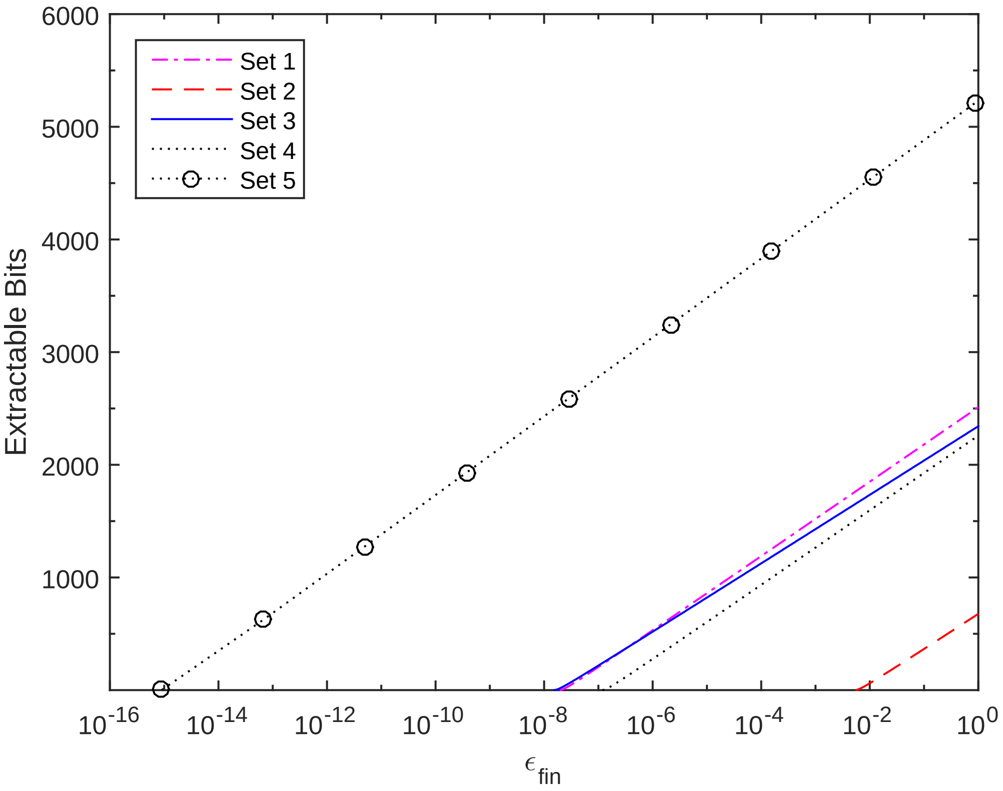

Figure 2: **Extractable bits as a function of error.** The figure shows the tradeoff between final error ϵ_{fin} and number of extractable bits t for values of v_{thresh} pre-chosen to yield estimated passing probabilities exceeding 95%. These thresholds were met in each case. For all data sets we set $\epsilon_{\text{p}} = \kappa^2 = (0.95\,\epsilon_{\text{fin}})^2$ and $\epsilon_{\text{ext}} = 0.05\,\epsilon_{\text{fin}}$, a split that was generally found to be near-optimal when numerically maximizing t in Eq. 5 for fixed values of ϵ_{fin}.

Experimentally Generated Randomness Certified by the Impossibility of Superluminal Signals
(Supplementary Information)

Peter Bierhorst, Emanuel Knill, Scott Glancy, Yanbao Zhang,
Alan Mink, Stephen Jordan, Andrea Rommal, Yi-Kai Liu,
Bradley Christensen, Sae Woo Nam, Martin J. Stevens, Lynden K. Shalm

After preliminaries to establish notation and summarize needed properties of total variation distance and non-signaling distributions in S.1, we give the proof of the Entropy Production Theorem in S.2. We explain how we chose the Bell function T, whose product determines whether we obtained the desired amount of randomness, in S.3. We then discuss the parameters of the extractors obtained by the TMPS algorithm (S.4) and prove the Protocol Soundness Theorem (S.5). Details on how we analyzed the experimental data sets are in S.6. Justification for our claim that previous methods do not obtain any randomness from our low per-trial-violation data is given in S.7.

S.1 Preliminaries

We use the standard convention that capital letters refer to random variables (RVs) and corresponding lowercase letters refer to values that the RVs can take. All our RVs take values in finite sets such as the set of bit strings of a given length or a finite subset of the reals, so that our RVs can be viewed as functions on a finite probability space. We usually just work with the induced joint distributions on the sets of values assumed by the RVs. When working with conditional probabilities, we implicitly exclude points where the conditioner has zero probability whenever appropriate. We use $\mathbb{P}(\ldots)$ to denote probabilities and $\mathbb{E}(\ldots)$ for expectations. Inside $\mathbb{P}(\ldots)$ and when used as conditioners, logical statements involving RVs are event specifications to be interpreted as the event for which the statement is true. For example, $\mathbb{P}(R > \delta)$ is equivalent to $\mathbb{P}(\{\omega : R(\omega) > \delta\})$, which is the probability of the event that the RV R takes a value greater than δ. The same convention applies when denoting events with $\{\ldots\}$. For example, the event in the previous example is written as $\{R > \delta\}$. While formally events are sets, we commonly use logical language to describe relationships between events. For example, the statement that $\{R > \delta\}$ implies $\{S > \epsilon\}$ means that as a set, $\{R > \delta\}$ is contained in $\{S > \epsilon\}$. When they appear outside the the mentioned contexts, logical statements are constraints on RVs. For example, the statement $R > \delta$ means that all values r of R satisfy $r > \delta$, or equivalently, for all ω, $R(\omega) > \delta$. As usual, comma separated statements are combined conjunctively (with “and”). (In the main text, for clarity, we have used an explicit “AND” for this purpose.)

If there are free RVs inside $\mathbb{P}(\ldots)$ or in the conditioner of $\mathbb{E}(\ldots|\ldots)$ outside event specifications, the final expression defines a new RV as a function of the free RVs. An example from the Entropy Production Theorem is the expression $\mathbb{P}(\mathbf{AB}|\mathbf{XY})$, which defines the RV that takes the value $\mathbb{P}(\mathbf{AB} = \mathbf{ab}|\mathbf{XY} = \mathbf{xy})$ when the event $\{\mathbf{ABXY} = \mathbf{abxy}\}$ occurs. Values of RVs such as $\mathbf{x}$ appearing by themselves in $\mathbb{P}(\ldots)$ denote the event $\{\mathbf{X} = \mathbf{x}\}$. Thus we abbreviate expressions such as $\mathbb{P}(\mathbf{AB} = \mathbf{ab}|\mathbf{XY} = \mathbf{xy})$ by $\mathbb{P}(\mathbf{ab}|\mathbf{xy})$. Sometimes it is necessary to disambiguate the probability distribution with respect to which $\mathbb{E}(\ldots)$ is to be computed. In such cases we use a subscript at the end of the expression consisting of a symbol for the probability distribution, so $\mathbb{E}(T)_{\mathbb{Q}}$ is the expectation of T with respect to the distribution $\mathbb{Q}$. In a few instances, we use $[\![\phi]\!]$ for logical expressions ϕ to denote the $\{0,1\}$-valued function evaluating to 1 iff ϕ is true.

The amount of randomness that can be extracted from an RV R is quantified by the *min-entropy*, defined as $-\log_2 \max_r \mathbb{P}(R = r)$. The error of the output of an extractor is given as the *total variation* (TV) distance from uniform. Given two probability distributions $\mathbb{P}_1$ and $\mathbb{P}_2$ for R, the TV distance between them is given by

$$\begin{aligned}
\mathrm{TV}(\mathbb{P}_1, \mathbb{P}_2) &= \frac{1}{2}\sum_r |\mathbb{P}_1(R=r) - \mathbb{P}_2(R=r)| \\
&= \sum_{r:\mathbb{P}_1(r)>\mathbb{P}_2(r)} (\mathbb{P}_1(R=r) - \mathbb{P}_2(R=r)) \\
&= \sum_r [\![\mathbb{P}_1(r) > \mathbb{P}_2(r)]\!] \left(\mathbb{P}_1(R=r) - \mathbb{P}_2(R=r)\right). \qquad \text{(S1)}
\end{aligned}$$

As the name implies, the TV distance is a metric. In particular, it satisfies the triangle inequality:

$$\mathrm{TV}(\mathbb{P}_1, \mathbb{P}_3) \leq \mathrm{TV}(\mathbb{P}_1, \mathbb{P}_2) + \mathrm{TV}(\mathbb{P}_2, \mathbb{P}_3). \qquad \text{(S2)}$$

See Ref. [35] for this and other basic properties of TV distances.

We sometimes compute TV distances for distributions of specific RVs, conditional or unconditional ones. For this we introduce the notation $\mathbb{P}_X$ for the distribution of values of X according to $\mathbb{P}$, and $\mathbb{P}_{X|Y=y}$ for the distribution of X conditioned on the event $\{Y = y\}$. With this notation, $\mathbb{P}_X\mathbb{P}_Y$ refers to the product distribution that assigns probability $\mathbb{P}_X(X = x)\mathbb{P}_Y(Y = y)$ to the event $\{X = x, Y = y\}$.

For the proof of the Protocol Soundness Theorem, we need two results involving the TV distance. According to the first result, if $\mathbb{P}$ and $\mathbb{Q}$ are joint distributions of RVs V and W, where the marginals of W satisfy $\mathbb{P}(w) = \mathbb{Q}(w)$, then the distance between them is given by the average conditional distance. This is explicitly calculated as follows:

$$\begin{aligned}
\mathrm{TV}(\mathbb{P}_{VW}, \mathbb{Q}_{VW}) &= \sum_w \sum_v [\![\mathbb{P}(v,w) > \mathbb{Q}(v,w)]\!] \left(\mathbb{P}(v,w) - \mathbb{Q}(v,w)\right) \\
&= \sum_w \sum_v [\![\mathbb{P}(v|w)\mathbb{P}(w) > \mathbb{Q}(v|w)\mathbb{Q}(w)]\!] \left(\mathbb{P}(v|w)\mathbb{P}(w) - \mathbb{Q}(v|w)\mathbb{Q}(w)\right) \\
&= \sum_w \sum_v [\![\mathbb{P}(v|w) > \mathbb{Q}(v|w)]\!] \left(\mathbb{P}(v|w) - \mathbb{Q}(v|w)\right)\mathbb{P}(w) \\
&= \sum_w \mathrm{TV}(\mathbb{P}_{V|W=w}, \mathbb{Q}_{V|W=w})\mathbb{P}(w). \qquad \text{(S3)}
\end{aligned}$$

The second result is a special case of the data-processing inequality for TV distance. See Ref. [36] for this and many other data-processing inequalities. Let V be a random variable taking values in a finite set $\mathcal{V}$, and let $F : \mathcal{V} \to \mathcal{W}$ be a function so that $F(V)$ is a random variable taking values in the set $\mathcal{W}$. Then if $\mathbb{P}$ and $\mathbb{Q}$ are two distributions of V,

$$\text{TV}\big(\mathbb{P}_V, \mathbb{Q}_V\big) \geq \text{TV}\big(\mathbb{P}_{F(V)}, \mathbb{Q}_{F(V)}\big). \tag{S4}$$

Here is a proof of this inequality. Write $\mathcal{W} = \{s_1, ..., s_c\}$, and for each $i \in \{1, \ldots, c\}$, define $\mathcal{V}_i = \{v : f(v) = s_i\}$. The $\mathcal{V}_i$ form a partition of $\mathcal{V}$. Then we have

$$\begin{aligned} \text{TV}\big(\mathbb{P}_{F(V)}, \mathbb{Q}_{F(V)}\big) &= \frac{1}{2}\sum_{i=1}^{c} |\mathbb{P}(V \in \mathcal{V}_i) - \mathbb{Q}(V \in \mathcal{V}_i)| \\ &= \frac{1}{2}\sum_{i=1}^{c} \left| \sum_{v \in \mathcal{V}_i} [\mathbb{P}(V = v) - \mathbb{Q}(V = v)] \right| \\ &\leq \frac{1}{2}\sum_{i=1}^{c} \sum_{v \in \mathcal{V}_i} |\mathbb{P}(V = v) - \mathbb{Q}(V = v)| \\ &= \text{TV}\big(\mathbb{P}_V, \mathbb{Q}_V\big). \end{aligned} \tag{S5}$$

We need to refer to the sequences of RVs associated with the first $i - 1$ trials. To do this we use notation such as $(\mathbf{AB})_{<i}$ for the outcome sequence $A_1B_1A_2B_2...A_{i-1}B_{i-1}$, $(\mathbf{XY})_{<i}$ for the settings sequence $X_1Y_1...X_{i-1}Y_{i-1}$, and $(\mathbf{ABXY})_{<i}$ for the joint outcomes and settings sequence $A_1B_1X_1Y_1...A_{i-1}B_{i-1}X_{i-1}Y_{i-1}$. In general we often juxtapose RVs to indicate the "joint" RV. From our assumption Eqs. 2 and 3 and the fact that past_i subsumes the trial settings and outcomes from trials 1 through $i - 1$, we obtain

$$\forall i \in (1, ..., n), \quad \mathbb{P}_e\left(X_iY_i|(\mathbf{ABXY})_{<i}\right) = \mathbb{P}_e(X_iY_i) = 1/4, \tag{S6}$$

and

$$\begin{aligned} \mathbb{P}_e(A_i|X_iY_i, (\mathbf{ABXY})_{<i}) &= \mathbb{P}_e(A_i|X_i, (\mathbf{ABXY})_{<i}) \\ \mathbb{P}_e(B_i|X_iY_i, (\mathbf{ABXY})_{<i}) &= \mathbb{P}_e(B_i|Y_i, (\mathbf{ABXY})_{<i}). \end{aligned} \tag{S7}$$

Eq. S6 can be weakened to accommodate imperfect settings randomness by replacing it with the following two assumptions, where $\alpha \in [0, 1/4)$ is a parameter controlling deviation from uniformity:

$$\forall i \in (1, ..., n), \quad 1/4 - \alpha \leq \mathbb{P}_e\left(X_iY_i|(\mathbf{ABXY})_{<i}\right) \leq 1/4 + \alpha \tag{S8}$$

$$P_e(X_iY_i|(ABXY)_{<i}) = P_e(X_iY_i|(XY)_{<i}) \tag{S9}$$

Eq. S6 is a strictly stronger assumption as it implies both Eq. S8 (with $\alpha = 0$) and Eq. S9. Eqs. S7, S8, and S9 are the forms of our assumptions used in the proof of the Entropy Production

Theorem. Eq. S9 expresses conditional independence of all past outcomes and the upcoming settings given the past settings. It is a special case of the Markov-chain condition in Ref. [28].

For a generic trial of a two station Bell test, a distribution is defined to be non-signaling if

$$\mathbb{P}(A|XY) = \mathbb{P}(A|X) \quad \text{and} \quad \mathbb{P}(B|XY) = \mathbb{P}(B|Y). \tag{S10}$$

Such distributions form a convex polytope and include the *local realist* (LR) distributions. Using the conventions of [22], these are defined as follows: Let λ range over the set of sixteen four-element vectors of the form (a_0, a_1, b_0, b_1) with elements in $\{+, 0\}$. Each λ induces settings-conditional deterministic distributions according to

$$\mathbb{P}^{\lambda}(ab|xy) = \begin{cases} 1, & \text{if } a = a_x \text{ and } b = b_y, \\ 0, & \text{otherwise.} \end{cases} \tag{S11}$$

Then a probability distribution $\mathbb{P}$ is LR iff its conditional probabilities $\mathbb{P}(ab|xy)$ can be written as a convex combination of the $\mathbb{P}^{\lambda}(ab|xy)$. That is

$$\mathbb{P}(ab|xy) = \sum_{\lambda} q_{\lambda} \mathbb{P}^{\lambda}(ab|xy), \tag{S12}$$

with q_{λ} a λ-indexed set of nonnegative numbers summing to 1. This definition agrees with the one given in the main text.

The eight "Popescu-Rohrlich (PR) boxes" [37] are examples of non-signaling distributions that are not LR. One of the PR boxes is defined by

$$\mathbb{P}_{\text{PR}}(ab|xy) = \begin{cases} 1/2 & \text{if } xy \neq 11 \text{ and } a = b, \text{ or if } xy = 11 \text{ and } a \neq b, \\ 0 & \text{otherwise,} \end{cases} \tag{S13}$$

and the other seven are obtained by relabeling settings or outcomes. We take advantage of the facts that a PR box contains one bit of randomness conditional on the settings and that the PR boxes together with the 16 deterministic LR distributions of Eq. S11 form the set of extreme points of the non-signaling polytope [38].

S.2 Proof of the Entropy Production Theorem

The conditions on T given in the main text are that (1) $T > 0$, (2) $\mathbb{E}(T)_{\mathbb{P}} \leq 1$ for every LR distribution $\mathbb{P}$, (3) there exists an $m > 0$ such that $\mathbb{E}(T)_{\mathbb{Q}} \leq 1+m$ for every non-signaling distribution $\mathbb{Q}$ if the settings distribution is uniform as in Eq. 2, and (4) the bound $1+m$ is achievable. Our proof of the Entropy Production Theorem does not require that the fourth condition is satisfied. Furthermore, we prove the Entropy Production Theorem with a weakened form of the second and third conditions, assuming that T satisfies conditions (2) and (3) with any settings distribution satisfying Eq. S8. In the following, we call this relaxed version of conditions (1)-(3)

"the Bell-function conditions with bound m and settings parameter α". We also generalize the Entropy Production Theorem by allowing the T_i to be chosen based on $(\mathbf{abxy})_{<i}$. We call T_i a "past-parametrized family of Bell functions" if for all $(\mathbf{abxy})_{<i}$, $T_i(a_ib_ix_iy_i, (\mathbf{abxy})_{<i})$ satisfies the Bell-function conditions with bound m and settings parameter α when considered as a function of the results $a_ib_ix_iy_i$ from the i'th trial. By proving the theorem for past-parametrized Bell functions T, we allow for the possibility of dynamically adapting T during run time, a feature that could compensate for experimental drift in future implementations of the protocol. The theorem and its proof can also be directly applied to the special case where T_i is the same function for all trials i and $\alpha = 0$.

Theorem 1. *Let T_i be a past-parametrized family of Bell functions as defined in the previous paragraph. Then in an experiment of n trials obeying Eq. S7, Eq. S8 and Eq. S9, the following inequality holds for all $\epsilon_\mathrm{p} \in (0,1)$ and v_thresh satisfying $1 \leq v_\mathrm{thresh} \leq (1+(3/2)m)^n\epsilon_\mathrm{p}^{-1}$:*

$$\mathbb{P}_e\left(\mathbb{P}_e(\mathbf{AB}|\mathbf{XY}) > \delta, V \geq v_\mathrm{thresh}\right) \leq \epsilon_\mathrm{p} \tag{S14}$$

where $\delta = [1+(1-\sqrt[n]{\epsilon_\mathrm{p}v_\mathrm{thresh}})/2m]^n$ and $\mathbb{P}_e$ represents the probability distribution conditioned on the event $\{E = e\}$.

We include the constraint $v_\mathrm{thresh} \leq (1+(3/2)m)^n\epsilon_\mathrm{p}^{-1}$ for technical reasons. Higher values of v_thresh are unreasonably large and result in pass probabilities that are too low to be relevant. Note that this bound ensures $\delta \geq 2^{-2n}$, a fact that will be useful in proving the Protocol Soundness Theorem in (S.5).

Proof. Since the condition on $\{E = e\}$ appears uniformly throughout, in this proof we omit the subscript on $\mathbb{P}_e$ specifying conditioning on $\{E = e\}$.

The strategy of the proof is to first obtain an upper bound on the one-trial outcome probabilities from the expectations of Bell functions T. This bound can be chained to give a bound on the probabilities of the outcome sequence as a monotonically decreasing function of the product of the conditional expectations of the T_i. That is, a larger product of expectations yields a smaller maximum probability and therefore more extractable randomness. This product cannot be directly observed, so we relate it to the observed product V of the T_i via the Markov inequality applied to an associated positive, mean-1 martingale. In the following, we suppress the arguments $a_ib_ix_iy_i$ and $(\mathbf{ABXY})_{<i}$ of T_i.

The one-trial outcome probabilities are bounded by means of the following lemma:

Lemma 1. *Let T satisfy the Bell-function conditions with bound $m > 0$ and settings parameter α. For any non-signaling distribution $\mathbb{P}$ satisfying Eq. S8,*

$$\max_{abxy} \mathbb{P}(ab|xy) \leq 1 + \frac{1 - \mathbb{E}[T(A,B,X,Y)]_\mathbb{P}}{2m}. \tag{S15}$$

Proof. The settings-conditional distribution $\mathbb{P}(ab|xy)$ is non-signaling, so it can be obtained as a convex combination of extremal such distributions. The convex combination requires at most one PR box ([39], Corollary 2.1), so we write $\mathbb{P}(ab|xy) = p\mathbb{Q}(ab|xy) + (1-p)\mathbb{Q}'(ab|xy)$, where $\mathbb{Q}$ is the PR box and $\mathbb{Q}'$ is LR. We thus have

$$\begin{aligned}\mathbb{E}(T)_{\mathbb{P}} = \sum_{abxy} T(abxy)\mathbb{P}(abxy) &= \sum_{xy}\left(\sum_{ab} T(abxy)\mathbb{P}(ab|xy)\right)\mathbb{P}(xy)\\ &= p\sum_{abxy} T(abxy)\mathbb{Q}(ab|xy)\mathbb{P}(xy) + (1-p)\sum_{abxy} T(abxy)\mathbb{Q}'(ab|xy)\mathbb{P}(xy)\\ &\leq p(1+m) + (1-p) = 1 + pm, \end{aligned} \tag{S16}$$

where the inequality above holds because $\mathbb{Q}(ab|xy)\mathbb{P}(xy)$ and $\mathbb{Q}'(ab|xy)\mathbb{P}(xy)$ respectively define non-signaling and LR distributions satisfying Eq. S8, and hence these distributions respectively satisfy $\mathbb{E}(T) \leq 1 + m$ and $\mathbb{E}(T) \leq 1$. The above inequality can be re-written as $p \geq (\mathbb{E}(T)_{\mathbb{P}} - 1)/m$. Now since the PR box assigns xy-conditional probability $1/2$ to at least one outcome different from ab, it follows that the xy-conditional probability relative to $\mathbb{P}$ of an outcome different from ab is at least $p/2$. Therefore, $\mathbb{P}(ab|xy) \leq 1 - p/2 \leq 1 - (\mathbb{E}(T)_{\mathbb{P}} - 1)/(2m)$. Since ab and xy are arbitrary, this gives the inequality the lemma. □

We can now establish a bound on $\mathbb{P}(\mathbf{ab}|\mathbf{xy})$ as follows:

$$\begin{aligned}\mathbb{P}(\mathbf{ab}|\mathbf{xy}) &= \prod_{i=1}^{n} \mathbb{P}(a_i b_i|(\mathbf{ab})_{<i}, \mathbf{xy})\\ &= \prod_{i=1}^{n} \mathbb{P}(a_i b_i|(\mathbf{abxy})_{<i}, x_i y_i)\\ &\leq \prod_{i=1}^{n}\left[1 + \frac{1 - \mathbb{E}(T_i|(\mathbf{abxy})_{<i})}{2m}\right]. \end{aligned} \tag{S17}$$

Here, the first identity is the chain rule for conditional probabilities, and the second follows from repeated applications of the following identity, which holds for all j in $(i+1, i+2, ..., n)$ (where we recall that $(\mathbf{xy})_{<n+1} = \mathbf{xy}$ and $(\mathbf{ab})_{<i}(\mathbf{xy})_{<i+1} = (\mathbf{abxy})_{<i}, x_i y_i$). The third equality below is a consequence of Eq. S9:

$$\begin{aligned}\mathbb{P}(a_i b_i|(\mathbf{ab})_{<i}, (\mathbf{xy})_{<j+1}) &= \frac{\mathbb{P}(a_i b_i, (\mathbf{ab})_{<i}, (\mathbf{xy})_{<j+1})}{\mathbb{P}((\mathbf{ab})_{<i}, (\mathbf{xy})_{<j+1})}\\ &= \frac{\mathbb{P}(x_j y_j|a_i b_i, (\mathbf{ab})_{<i}, (\mathbf{xy})_{<j})\mathbb{P}(a_i b_i, (\mathbf{ab})_{<i}, (\mathbf{xy})_{<j})}{\mathbb{P}(x_j y_j|(\mathbf{ab})_{<i}, (\mathbf{xy})_{<j})\mathbb{P}((\mathbf{ab})_{<i}, (\mathbf{xy})_{<j})}\\ &= \frac{\mathbb{P}(x_j y_j|(\mathbf{xy})_{<j})\mathbb{P}(a_i b_i, (\mathbf{ab})_{<i}, (\mathbf{xy})_{<j})}{\mathbb{P}(x_j y_j|(\mathbf{xy})_{<j})\mathbb{P}((\mathbf{ab})_{<i}, (\mathbf{xy})_{<j})}\\ &= \mathbb{P}(a_i b_i|(\mathbf{ab})_{<i}, (\mathbf{xy})_{<j}). \end{aligned} \tag{S18}$$

Finally, the inequality in Eq. S17 is a consequence of our assumption in Eq. S7 that the past-dependent distributions are non-signaling, which allows us to apply the bound from Lemma 1.

Now, by twice using the fact that the geometric mean of a set of positive numbers is always less than or equal to their arithmetic mean, we continue from the last line of Eq. S17:

$$\begin{aligned}
\prod_{i=1}^{n}\left[1+\frac{1-\mathbb{E}(T_i|(\mathbf{abxy})_{<i})}{2m}\right] &= \left(\left\{\prod_{i=1}^{n}\left[1+\frac{1-\mathbb{E}(T_i|(\mathbf{abxy})_{<i})}{2m}\right]\right\}^{\frac{1}{n}}\right)^{n} \\
&\leq \left(\frac{\sum_{i=1}^{n}\left[1+\frac{1-\mathbb{E}(T_i|(\mathbf{abxy})_{<i})}{2m}\right]}{n}\right)^{n} \\
&= \left(1+\frac{1}{2m}-\frac{\sum_{i=1}^{n}\left[\frac{\mathbb{E}(T_i|(\mathbf{abxy})_{<i})}{2m}\right]}{n}\right)^{n} \\
&\leq \left(1+\frac{1}{2m}-\left[\prod_{i=1}^{n}\frac{\mathbb{E}(T_i|(\mathbf{abxy})_{<i})}{2m}\right]^{\frac{1}{n}}\right)^{n} \\
&= \left(1+\frac{1-[\prod_{i=1}^{n}\mathbb{E}(T_i|(\mathbf{abxy})_{<i})]^{\frac{1}{n}}}{2m}\right)^{n}. \qquad \text{(S19)}
\end{aligned}$$

Referring back to the statement of the theorem, we see that δ can be expressed as $f(\epsilon_{\text{p}}v_{\text{thresh}})$ where $f(x) = [1+(1-\sqrt[n]{x})/2m]^n$. Expressing Eq. S19 in terms of this same function f, we see that the event $\{\mathbb{P}(\mathbf{AB}|\mathbf{XY}) > \delta\}$ implies the event $\{f\left(\prod_{i=1}^{n}\mathbb{E}(T_i|(\mathbf{ABXY})_{<i})\right) > \delta\}$. The latter event is the same as $\{\prod_{i=1}^{n}\mathbb{E}(T_i|(\mathbf{ABXY})_{<i}) < f^{-1}(\delta) = \epsilon_{\text{p}}v_{\text{thresh}}\}$, since f^{-1} is strictly decreasing. Conjoining the event $\{V \geq v_{\text{thresh}}\}$ to both sides of the implication, we have $\{\mathbb{P}(\mathbf{AB}|\mathbf{XY}) > \delta, V \geq v_{\text{thresh}}\}$ implies $\{\prod_{i=1}^{n}\mathbb{E}(T_i|(\mathbf{ABXY})_{<i}) < \epsilon_{\text{p}}v_{\text{thresh}}, V \geq v_{\text{thresh}}\}$, and so by the monotonicity of probabilities,

$$\mathbb{P}\left(\mathbb{P}(\mathbf{AB}|\mathbf{XY}) > \delta, V \geq v_{\text{thresh}}\right) \leq \mathbb{P}\left(\prod_{i=1}^{n}\mathbb{E}(T_i|(\mathbf{ABXY})_{<i}) < \epsilon_{\text{p}}v_{\text{thresh}}, V \geq v_{\text{thresh}}\right). \qquad \text{(S20)}$$

The event $\{\Phi\}$ whose probability appears on the left-hand side of this equation is the event in the theorem statement whose probability we are required to bound. For any values of the RVs, the two inequalities in the event on the right-hand side imply the inequality in the event $\{\Psi\} = \{V/\prod_{i=1}^{n}\mathbb{E}(T_i|(\mathbf{ABXY})_{<i}) \geq 1/\epsilon_{\text{p}}\}$. Hence $\mathbb{P}(\Phi) \leq \mathbb{P}(\Psi)$. It remains to show that $\mathbb{P}(\Psi) \leq \epsilon_{\text{p}}$. For this purpose we define the sequence $\{W_c\}_{c=1}^{n}$ of RVs by

$$W_c = \prod_{i=1}^{c}\frac{T_i}{\mathbb{E}(T_i|(\mathbf{ABXY})_{<i})}, \qquad \text{(S21)}$$

so that $\{\Psi\} = \{W_n \geq 1/\epsilon_{\text{p}}\}$.

By definition, $W_c > 0$ and the factors $T_i/\mathbb{E}(T_i|(\mathbf{ABXY})_{<i})$ have expectation 1 conditional on the past. Sequences of RVs with these properties are referred to as test martingales [40] and satisfy that $\mathbb{E}(W_n) = 1$, which can be verified directly by induction:

$$\begin{aligned}
\mathbb{E}(W_c|(\mathbf{ABXY})_{<c}) &= \mathbb{E}\left(\prod_{i=1}^{c} \frac{T_i}{\mathbb{E}(T_i|(\mathbf{ABXY})_{<i})}\middle|(\mathbf{ABXY})_{<c}\right) \\
&= \mathbb{E}\left(\left(\prod_{i=1}^{c-1} \frac{T_i}{\mathbb{E}(T_i|(\mathbf{ABXY})_{<i})}\right)\frac{1}{\mathbb{E}(T_c|(\mathbf{ABXY})_{<c})}T_c\middle|(\mathbf{ABXY})_{<c}\right) \\
&= \left(\prod_{i=1}^{c-1} \frac{T_i}{\mathbb{E}(T_i|(\mathbf{ABXY})_{<i})}\right)\frac{1}{\mathbb{E}(T_c|(\mathbf{ABXY})_{<c})}\mathbb{E}\left(T_c|(\mathbf{ABXY})_{<c}\right) \\
&= W_{c-1}, \qquad \text{(S22)}
\end{aligned}$$

where in the second last line, we pulled out factors that are functions of the conditioner $(\mathbf{ABXY})_{<c}$ by applying the rule that if F is a function of H, then $\mathbb{E}(FG|H) = F\mathbb{E}(G|H)$. Taking the unconditional expectation of both sides of Eq. S22 and invoking the law of total expectation, we have $\mathbb{E}(W_c) = \mathbb{E}(W_{c-1})$, and so inductively, $\mathbb{E}(W_n) = \mathbb{E}(W_1)$. Since $\mathbb{E}(W_1) = 1$, the claim follows. To finish the proof of the Entropy Production Theorem, we apply Markov's inequality to obtain $\mathbb{P}(W_n \geq 1/\epsilon_\text{p}) \leq \epsilon_\text{p}$ and consequently $\mathbb{P}(\Phi) \leq \epsilon_\text{p}$.

□

Now that we have proved the Entropy Production Theorem for any past-parametrized family of Bell functions, we can justify a strategy of setting the remaining Bell functions to $T_i = 1$ after v_thresh is exceeded by the running product mid-protocol. Formally, since the running product $V_{i-1} = \prod_{i=j}^{i-1} T_j$ is a function of $(\mathbf{ABXY})_{<i}$, we can define $T_i = T$ conditional on $\{V_{i-1} < v_\text{thresh}\}$ and $T_i = 1$ conditional on the complement. This optional strategy can be used to eliminate the possibility that statistical fluctuations or experimental drift could cause $\prod_{i=1}^{n} T_i$ to be less than v_thresh even though the running product exceeded v_thresh at some point prior to n.

S.3 Choosing the Bell Function T

The Entropy Production Theorem does not indicate how to find functions T satisfying the specified conditions. We seek a high typical value of $V = \prod_{i=1}^{n} T_i$, as this permits larger values of v_thresh and consequently more extractable randomness at the same values of ϵ_p and m. Here, we describe a procedure for constructing a function T that can be expected to perform well if the trial results are i.i.d. with known distribution. We estimate the distribution from an initial portion of the run that we set aside as training data, and in a stable experiment we expect that the trial results' statistics are i.i.d. to a good approximation. Note however that the optimistic i.i.d. assumption is only used as a heuristic to construct T; once T is chosen the guarantees of the Entropy Production Theorem hold regardless of whether the trial results are actually i.i.d.

We first focus on the scenario where Eq. S6 is assumed to hold, then show how to proceed if this is replaced with the weaker assumptions Eq. S8 and Eq. S9.

The observed measurement outcome frequencies for training data generally yield a weakly signaling distribution that does not exactly satisfy the non-signaling constraints in Eq. S10, due to statistical fluctuation. Hence one can obtain an estimated distribution by determining the maximum likelihood non-signaling distribution for the observed measurement outcomes frequencies as described in Ref. [31]. Let $N(xy)$ be the number of training trials at setting xy and $f(ab|xy) = N(ab|xy)/N(xy)$ be the empirical frequencies of outcome ab given setting xy. Let $\mathbb{Q}(a, b, x, y)$ be a candidate for the probability distribution from which these frequencies were sampled. Then up to an additive term independent of $\mathbb{Q}$ accounting for the settings probabilities, the log-likelihood of f given $\mathbb{Q}$ is $L(\mathbb{Q}) = \sum_{a,b,x,y} N(xy)f(ab|xy)\ln(\mathbb{Q}(a, b|x, y))$. We maximized a variant of this function to find our estimated distribution $\mathbb{Q}(a, b, x, y)$:

$$\begin{array}{llcll}
\underset{\mathbb{Q}}{\text{Maximize}} \displaystyle\sum_{abxy} f(ab|xy)\ln\mathbb{Q}(a,b,x,y) & & & & \\
\text{Subject to} \quad \mathbb{Q}(x,y) & = & 1/4 & \text{for} & x,y\in\{0,1\} \\
\mathbb{Q}(a|x,y) & = & \mathbb{Q}(a|x) & \text{for} & x,y\in\{0,1\}, \quad a\in\{+,0\} \\
\mathbb{Q}(b|x,y) & = & \mathbb{Q}(b|y) & \text{for} & x,y\in\{0,1\}, \quad b\in\{+,0\}.
\end{array} \tag{S23}$$

The first group of constraints encode our knowledge that all settings combinations are equally likely, and the remaining constraints are the non-signaling constraints. Note that the conditional expressions in these constraints are equivalently expressed as linear functions of $\mathbb{Q}(a, b, x, y)$ after using the identities $\mathbb{Q}(x, y) = 1/4$.

Once the estimated distribution $\mathbb{Q}$ is obtained, we maximize the typical values of V by taking advantage of the observation that the conditions on T imply that V^{-1} is a conservative p-value against local realism [31]. Such p-values were studied in Ref. [31], which gives a general strategy, the PBR method, for maximizing $\mathbb{E}(\ln(V))_{\mathbb{Q}}$. This is useful because typical values of V are close to $\exp(n\mathbb{E}(\ln(T))_{\mathbb{Q}})$: Since $\ln(V) = \sum_{i=1}^{n}\ln(T_i)$ is a sum of i.i.d. bounded terms (given our optimistic assumption), the central limit theorem ensures that $\ln V$ is approximately normally distributed with mean $n\mathbb{E}(\ln(T))_{\mathbb{Q}}$. We therefore perform the following optimization problem to find T:

$$\begin{array}{lcll}
\underset{T}{\text{Maximize}}\ \mathbb{E}(\ln(T))_{\mathbb{Q}} & & & \\
\text{Subject to} \quad \mathbb{E}(T)_{\mathbb{P}^\lambda} & \leq & 1 & \forall\lambda \\
T(0,0,x,y) & = & 1 & \forall x,y,
\end{array} \tag{S24}$$

where $\mathbb{P}^\lambda$ refers to the 16 conditionally deterministic LR distributions in Eq. S11 with uniform settings distributions. This ensures that $\mathbb{E}(T)_{\mathbb{P}_{LR}} \leq 1$ for all LR distributions $\mathbb{P}_{LR}$ with uniform settings distributions. The second constraint is motivated by the fact that in our experiments, an overwhelming fraction of the trials have no detections for both stations. While it is possible that a better $\mathbb{E}(\ln(T))_{\mathbb{Q}}$ can be obtained without this constraint, we have found that the improvement is small and likely not statistically significant given the amount of training data used to determine the results distribution. Since the objective functions are concave and the constraints are linear, the optimization problems given in Eq. S23 and Eq. S24 are readily solved numerically with standard tools.

Given the assumption that the trial results are i.i.d., the previous paragraph shows that the typical values for V are exponential in the number of trials, $V = e^{-n\mathbb{E}(\ln(T))-o(n)}$. If the experiment is successful in showing violation of local realism, $\mathbb{E}(\ln(T))$ is positive. Neglecting the contribution from $o(n)$, with $v_{\text{thresh}} = e^{n\mathbb{E}(\ln(T))}$, we can bound $-\ln(\delta)$ as

$$\begin{aligned}
-\ln(\delta) &= -n\ln(1+(1-(\epsilon_{\text{p}}e^{n\mathbb{E}(\ln(T))})^{1/n})/(2m)) \\
&= -n\ln(1+(1-e^{\mathbb{E}(\ln(T))+\ln(\epsilon_{\text{p}})/n})/(2m)) \\
&\geq -n(1-e^{\mathbb{E}(\ln(T))+\ln(\epsilon_{\text{p}})/n})/(2m) \\
&= n(e^{\mathbb{E}(\ln(T))+\ln(\epsilon_{\text{p}})/n}-1)/(2m) \\
&\geq (n\mathbb{E}(\ln(T))+\ln(\epsilon_{\text{p}}))/(2m). \qquad \text{(S25)}
\end{aligned}$$

where we used $-\ln(1+x) \geq -x$ and $e^x - 1 \geq x$. This shows that asymptotically (with ϵ_{p} constant) we get at least $\mathbb{E}(\ln(T))\log_2(e)/(2m) = \mathbb{E}(\log_2(T))/(2m)$ bits of randomness per trial. For the empirical distribution obtained from the fifth data set (“Data Set 5”) used for the protocol according to Eq. S23, we obtain $\mathbb{E}(\log_2(T))/2m = 1.42\times 10^{-4}$. The bound in Eq. S25 shows that we can get an asymptotically positive number of bits of randomness per trial even with ϵ_{p} exponentially small in n.

Now we turn to the problem of finding a function satisfying the condition $\mathbb{E}(T)_{\mathbb{P}_{LR}} \leq 1$ for all LR distributions $\mathbb{P}_{LR}$ with settings distribution constrained only by the weaker condition Eq. S8, which replaces the stronger exact uniformity condition of Eq. S6. To do this, we show that it is sufficient to check only distributions with the extremal settings distributions where two settings have probability $1/4+\alpha$ and the two other settings distributions have probability $1/4-\alpha$. To see why this is possible, for a fixed positive Bell function T, let $\mathbb{P}$ be an LR distribution whose settings distribution is constrained by Eq. S8. Taking advantage of the representation in Eq. S12,

$$\begin{aligned}
\mathbb{E}(T)_{\mathbb{P}} = \sum_{abxy} T(abxy)\mathbb{P}(ab|xy)\mathbb{P}(xy) &= \sum_{abxy} T(abxy)\left(\sum_{\lambda} q_\lambda \mathbb{P}^\lambda(ab|xy)\right)\mathbb{P}(xy) \\
&= \sum_{\lambda} q_\lambda \sum_{abxy} T(abxy)\mathbb{P}^\lambda(ab|xy)\mathbb{P}(xy) \leq \max_{\lambda} \sum_{abxy} T(abxy)\mathbb{P}^\lambda(ab|xy)\mathbb{P}(xy), \qquad \text{(S26)}
\end{aligned}$$

so the expected value of T with respect to $\mathbb{P}$ is always less than or equal to the expected value of T with respect to a conditionally deterministic LR distribution $\mathbb{P}^\lambda$ with the same settings distribution. Since each deterministic LR distribution assigns conditional probability 1 to a single outcome ab for each of the four setting choices xy, the sum $\sum_{abxy} T(abxy)\mathbb{P}^\lambda(ab|xy)\mathbb{P}(xy)$

contains only four nonzero terms. Consider the two largest values of $T(abxy)$ and the two smallest values of $T(abxy)$ appearing in the four nonzero terms. Note that $\sum_{abxy} T(abxy)\mathbb{P}^{\lambda}(ab|xy)\mathbb{P}(xy) \leq \sum_{abxy} T(abxy)\mathbb{P}^{\lambda}(ab|xy)\mathbb{P}^{*}(xy)$, where $\mathbb{P}^{*}(XY)$ is the distribution that assigns probability $1/4+\alpha$ to the two settings corresponding to the two largest T, and probability $1/4-\alpha$ to the two settings corresponding to the two smallest T. Hence for any T, we can ensure that $\mathbb{E}(T)_{\mathbb{P}} \leq 1$ holds for all LR distributions by checking that $\mathbb{E}(T)_{\mathbb{P}} \leq 1$ holds for each conditional distribution $\mathbb{P}^{\lambda}_{AB|XY}$ coupled with each of the $i = 1, \ldots, \binom{4}{2} = 6$ settings distributions $\mathbb{S}^{i}_{XY}$ assigning probability $1/4+\alpha$ to two settings and $1/4-\alpha$ to two other settings. This leads us to the maximization problem

$$\begin{aligned} &\underset{T}{\text{Maximize}}\ \mathbb{E}(\ln(T))_{\mathbb{Q}} && && \\ &\text{Subject to}\quad \mathbb{E}(T)_{\mathbb{P}^{\lambda}_{AB|XY}\mathbb{S}^{i}_{XY}} &&\leq\ 1 && \forall\lambda, i \\ &\qquad\qquad T(0,0,x,y) &&=\ 1 && \forall x, y. \end{aligned} \tag{S27}$$

The new problem maximizes the same objective function as in Eq. S24 subject to a larger, but still finite, number of constraints. It can be solved numerically to find a Bell function for the weak settings distribution.

S.4 The TMPS Algorithm

A strong randomness extractor with parameters $(\sigma, \epsilon, q, d, t)$ is a function Ext : $\{0,1\}^{q} \times \{0,1\}^{d} \rightarrow \{0,1\}^{t}$ with the property that for any random string R of length q and min-entropy at least σ, and an independent, uniformly distributed seed string S of length d, the distribution of the concatenation Ext(RS) with S of length $t+d$ is within TV distance ϵ of uniform. There are constructions of extractors that extract most of the input min-entropy σ with few seed bits. For a review of the achievable asymptotic tradeoffs, see Ref. [41], chapter 6. For explicit extractors that perform well if not optimally, we used a version of Trevisan's construction [25] implemented by Mauerer, Portmann and Scholz [26], which we adapted[1] to make it functional in our environment and to incorporate recent constructions achieving improved parameters [42]. We call this construction the TMPS algorithm. For a fixed choice of σ, ϵ and q, the TMPS algorithm can construct a strong randomness extractor for any value t obeying the following bound:

$$t + 4\log_2 t \leq \sigma - 6 + 4\log_2(\epsilon). \tag{S28}$$

Given t, the length of the seed satisfies

$$d \leq w^2 \cdot \max\left\{2, 1 + \lceil[\log_2(t-e) - \log_2(w-e)]/[\log_2 e - \log_2(e-1)]\rceil\right\}, \tag{S29}$$

where w is the smallest prime larger than $2 \times \lceil\log_2(4qt^2/\epsilon^2)\rceil$. We note that the TMPS extractors are secure against classical and quantum side information [26], and this security is reflected in the parameter constraints. Since we do not take direct advantage of this security, it is in principle

[1] Our adapted source code is available at `https://github.com/usnistgov/libtrevisan`.

possible to improve the parameters in the Protocol Soundness Theorem. It may also be possible relax the requirement of seed uniformity with more advanced constructions. For the purpose randomness amplification this is theoretically accomplished in Ref. [43].

For the bound on the the number of seed bits given after the Protocol Soundness Theorem in the main text, we have $q = 2n$ and $\epsilon = \epsilon_{\text{ext}}/2$. Since for any r, there is a prime w satisfying $r < w \leq 2r$, $w = O(\log(n) + \log(t/\epsilon)) = O(\log(nt/\epsilon))$, where we pulled out exponents from the $\log$, and dropped and arbitrarily increased the implicit constants in front of each term to match summands. The coefficient of w^2 in the bound on d is $O(\log(t))$, because of the "minus" sign in front of the term containing w. Multiplying gives $d = O(\log(t)\log(nt/\epsilon_{\text{ext}})^2)$.

S.5 Proof of the Protocol Soundness Theorem

The distinction between the stations was needed to establish the inequality in the Entropy Production Theorem and plays no further role in this section. We therefore simplify the notation by abbreviating $\mathbf{C} = \mathbf{AB}$ and either $\mathbf{Z} = \mathbf{XY}$ or $\mathbf{Z} = \mathbf{XY}E$. In the former case $\mathbb{P}(\ldots)$ refers to probabilities conditional on $\{E = e\}$. Otherwise, $\mathbb{P}(\ldots)$ involves no implicit conditions. The Protocol Soundness Theorem holds regardless of which definition of $\mathbf{Z}$ is in force. We write R_{pass} to refer to the RV that takes value 1 conditional on the passing event $\{V \geq v_{\text{thresh}}\}$ and 0 otherwise. The constants ϵ_{p} and δ appearing below are the same as in the Entropy Production Theorem.

Theorem 2. *Let $0 < \epsilon_{\text{ext}}, \kappa < 1$. Suppose $\mathbb{P}(\text{pass}) \geq \kappa$, and suppose t is a positive integer satisfying*

$$t + 4\log_2 t \leq -\log_2 \delta + \log_2 \kappa + 5\log_2 \epsilon_{\text{ext}} - 11. \tag{S30}$$

Then if Ext $: \{0,1\}^{2n} \times \{0,1\}^d \to \{0,1\}^t$ is obtained by the TMPS algorithm with parameters $\sigma = -\log_2[2\delta/(\kappa\epsilon_{\text{ext}})]$ and $\epsilon = \epsilon_{\text{ext}}/2$, and $\mathbf{S}$ is a random bit string of length d independent of the joint distribution of $\mathbf{C}, \mathbf{Z}$, R_{pass}, then the joint distribution of $\mathbf{U} = \text{Ext}(\mathbf{CS})$, $\mathbf{Z}$, $\mathbf{S}$ and R_{pass} satisfies

$$\text{TV}\big(\mathbb{P}_{\mathbf{UZS}|R_{\text{pass}}=1}, \mathbb{P}^{\text{unif}}_{\mathbf{U}}\mathbb{P}^{\text{unif}}_{\mathbf{S}}\mathbb{P}_{\mathbf{Z}|R_{\text{pass}}=1}\big) \leq \epsilon_{\text{p}}/\mathbb{P}(\text{pass}) + \epsilon_{\text{ext}}, \tag{S31}$$

where $\mathbb{P}^{\text{unif}}$ denotes the uniform probability distribution.

At this point it is tempting to just apply an extractor to $\mathbf{AB}$ with parameter σ given by the nominal ϵ_{p}-smooth min-entropy $\sigma = -\log_2(\delta)$. However, this does not guarantee the strong condition Eq. S31. Specifically, there are three reasons that Eq. S14 of the Entropy Production Theorem does not immediately support the application of an extractor to $\mathbf{AB}$. The first is that as specified, the extractor input should have min-entropy $-\log_2 \max_{\mathbf{ab}} \mathbb{P}(\mathbf{AB} = \mathbf{ab}) = \sigma$ with no smoothness error. The second is that the settings-conditional smooth min-entropies can be substantially smaller than the nominal one. The third is that the min-entropy is also affected by the probability of passing being less than 1. Accounting for these effects requires an analysis of the settings- and pass-conditional distributions and the extractor parameters specified in the theorem.

Proof. The proof proceeds in two main steps inspired by the corresponding arguments in Ref. [2]. In the first we determine a probability distribution $\mathbb{P}^*$ that is within $\epsilon_{\rm p}$ of $\mathbb{P}$ but satisfies an appropriate bound on the conditional probabilities of $\mathbf{C}$ with probability 1 rather than $1-\epsilon_{\rm p}$. The distribution $\mathbb{P}^*$'s marginals agree with those of $\mathbb{P}$ on $\mathbf{ZS}$. The probabilities conditional on aborting also agree, and uniformity and independence of $\mathbf{S}$ is preserved. In the second step, we apply a proposition from Ref. [44] on applying extractors to distributions such as $\mathbb{P}^*$ whose average maximum conditional probabilities satisfy a specified bound. The proposition enables us to determine the extractor parameters that achieve the required final distance $\epsilon_{\rm p}/\mathbb{P}(\text{pass})+\epsilon_{\rm ext}$ in the theorem.

The Entropy Production Theorem guarantees that $\mathbb{P}(\mathbb{P}(\mathbf{C}|\mathbf{Z})>\delta, R_{\text{pass}}=1)\leq\epsilon_{\rm p}$. In the case where E is included in $\mathbf{Z}$, this follows by the uniformity in $\{E=e\}$ of the theorem's conclusion:

$$\begin{aligned}
\mathbb{P}(\mathbb{P}(\mathbf{C}|\mathbf{Z},E)>\delta, R_{\text{pass}}=1) &= \sum_e \mathbb{P}(\mathbb{P}(\mathbf{C}|\mathbf{Z},E)>\delta, R_{\text{pass}}=1|E=e)\mathbb{P}(E=e)\\
&= \sum_e \mathbb{P}(\mathbb{P}(\mathbf{C}|\mathbf{Z},E=e)>\delta, R_{\text{pass}}=1|E=e)\mathbb{P}(E=e)\\
&\leq \sum_e \epsilon_{\rm p}\mathbb{P}(e)\\
&= \epsilon_{\rm p}. \qquad\qquad (S32)
\end{aligned}$$

Using the following construction, one may observe that for any random variable U with values in a set of cardinality K and γ satisfying $1/K\leq\gamma$, and any distribution $\mathbb{P}'$ of U, there exists $\mathbb{P}''$ such that $\mathbb{P}''(U=u)\leq\gamma$ for all possible outcomes u and $\mathbb{P}''$ is within TV distance $\mathbb{P}'(\mathbb{P}'(U)>\gamma)$ of $\mathbb{P}'$. To construct $\mathbb{P}''$, for u such that $\mathbb{P}'(u)>\gamma$, set $\mathbb{P}''(u)=\gamma$. To compensate for the reduced probabilities, increase the values of $\mathbb{P}'$ to obtain those of $\mathbb{P}''$ without exceeding γ on the set $\{u:\mathbb{P}'(u)\leq\gamma\}$ so that $\mathbb{P}''$ is a normalized probability distribution. This is possible because in constructing $\mathbb{P}''$ from $\mathbb{P}'$, the total reduction in probability on $\{u:\mathbb{P}'(u)>\gamma\}$ given by $r_-=\sum_{u:\mathbb{P}'(u)>\gamma}(\mathbb{P}'(u)-\gamma)$ is less than the maximum total increase possible given by $r_+=\sum_{u:\mathbb{P}'(u)\leq\gamma}(\gamma-\mathbb{P}'(u))$, as a consequence of $\gamma\geq 1/K$. To see this, compute $r_+-r_-=\sum_u(\gamma-\mathbb{P}'(u))\geq\sum_u(1/K-\mathbb{P}'(u))=0$. The distance $\text{TV}(\mathbb{P}',\mathbb{P}'')$ is given by $\sum_{u:\mathbb{P}'(u)>\gamma}(\mathbb{P}'(u)-\gamma)\leq\mathbb{P}'(\mathbb{P}'(U)>\gamma)$. We can now construct $\mathbb{P}^*$ by defining its conditional distributions on $\mathbf{C}$. For this, substitute $U\leftarrow\mathbf{C}$, $\mathbb{P}'(U)\leftarrow\mathbb{P}(\mathbf{C}|\mathbf{z},R_{\text{pass}}=1)$, $\gamma\leftarrow\delta/\mathbb{P}(R_{\text{pass}}=1|\mathbf{z})$ and $\mathbb{P}''(U)\leftarrow\mathbb{P}^*(\mathbf{C}|\mathbf{z},R_{\text{pass}}=1)$. The constraint on γ is satisfied because the upper bound on v_{thresh} in the statement of the Entropy Production Theorem ensures that $\delta\geq 2^{-2n}$. Each conditional distribution satisfies $\mathbb{P}^*(\mathbf{C}|\mathbf{z},R_{\text{pass}}=1)\leq\delta/\mathbb{P}(R_{\text{pass}}=1|\mathbf{z})$, which is equivalent to $\mathbb{P}^*(\mathbf{C},R_{\text{pass}}=1|\mathbf{z})\leq\delta$, and is within TV distance $\mathbb{P}\big(\mathbb{P}(\mathbf{C}|\mathbf{z},R_{\text{pass}}=1)>\delta/\mathbb{P}(R_{\text{pass}=1}|\mathbf{z})\big|\mathbf{z},R_{\text{pass}}=1\big)$ of $\mathbb{P}_{\mathbf{C}|\mathbf{z},R_{\text{pass}}=1}$. The joint probability distribution $\mathbb{P}^*$ is determined pointwise from the already assigned values of $\mathbb{P}^*(\mathbf{c}|\mathbf{z}r_{\text{pass}})$ for $r_{\text{pass}}=1$ as

$$\mathbb{P}^*(\mathbf{czs}r_{\text{pass}})=\begin{cases}\mathbb{P}^*(\mathbf{c}|\mathbf{z}r_{\text{pass}})\mathbb{P}(\mathbf{zs}r_{\text{pass}}) & \text{if } r_{\text{pass}}=1\\ \mathbb{P}(\mathbf{czs}r_{\text{pass}}) & \text{otherwise.}\end{cases} \qquad (S33)$$

Since the marginal distribution of $\mathbf{ZS}R_{\text{pass}}$ is unchanged, the full TV distance between $\mathbb{P}$ and $\mathbb{P}^*$ is given by the average conditional TV distance with respect to $\mathbf{ZS}R_{\text{pass}}$, see Eq. S3. Since the conditional TV distance is zero when $R_{\text{pass}} = 0$ and from independence of $\mathbf{S}$, we obtain

$$\begin{aligned}
&\mathrm{TV}(\mathbb{P}^*_{\mathbf{CZS}R_{\text{pass}}}, \mathbb{P}_{\mathbf{CZS}R_{\text{pass}}}) \\
&\quad= \sum_{\mathbf{zs}r_{\text{pass}}} \mathrm{TV}\big(\mathbb{P}^*_{\mathbf{C}|\mathbf{zs}r_{\text{pass}}}, \mathbb{P}_{\mathbf{C}|\mathbf{zs}r_{\text{pass}}}\big)\mathbb{P}(\mathbf{zs}r_{\text{pass}}) \\
&\quad= \sum_{\mathbf{zs}r_{\text{pass}}} \mathrm{TV}\big(\mathbb{P}^*_{\mathbf{C}|\mathbf{zs}r_{\text{pass}}}, \mathbb{P}_{\mathbf{C}|\mathbf{zs}r_{\text{pass}}}\big)\llbracket r_{\text{pass}} = 1\rrbracket\mathbb{P}(\mathbf{zs}r_{\text{pass}}) \\
&\quad\leq \sum_{\mathbf{zs}r_{\text{pass}}} \mathbb{P}\big(\mathbb{P}(\mathbf{C}, R_{\text{pass}} = 1|\mathbf{z}) > \delta\big|\mathbf{z}, R_{\text{pass}} = 1\big)\llbracket r_{\text{pass}} = 1\rrbracket\mathbb{P}(\mathbf{zs}r_{\text{pass}}) \\
&\quad= \sum_{\mathbf{z}r_{\text{pass}}} \mathbb{P}\big(\mathbb{P}(\mathbf{C}, R_{\text{pass}} = 1|\mathbf{z}) > \delta\big|\mathbf{z}, R_{\text{pass}} = 1\big)\llbracket r_{\text{pass}} = 1\rrbracket\mathbb{P}(\mathbf{z}r_{\text{pass}}) \\
&\quad= \sum_{\mathbf{cz}r_{\text{pass}}} \llbracket\mathbb{P}(\mathbf{c}r_{\text{pass}}|\mathbf{z}) > \delta\rrbracket\mathbb{P}(\mathbf{c}|\mathbf{z}r_{\text{pass}})\llbracket r_{\text{pass}} = 1\rrbracket\mathbb{P}(\mathbf{z}r_{\text{pass}}) \\
&\quad= \sum_{\mathbf{cz}r_{\text{pass}}} \llbracket\mathbb{P}(\mathbf{c}r_{\text{pass}}|\mathbf{z}) > \delta\rrbracket\llbracket r_{\text{pass}} = 1\rrbracket\mathbb{P}(\mathbf{cz}r_{\text{pass}}) \\
&\quad= \mathbb{P}(\mathbb{P}(\mathbf{C}R_{\text{pass}}|\mathbf{Z}) > \delta, R_{\text{pass}} = 1) \\
&\quad\leq \mathbb{P}(\mathbb{P}(\mathbf{C}|\mathbf{Z}) > \delta, R_{\text{pass}} = 1) \\
&\quad\leq \epsilon_{\text{p}}.
\end{aligned} \tag{S34}$$

At this point we can also bound the TV distance conditional on passing. Since $\mathbb{P}^*(R_{\text{pass}}) = \mathbb{P}(R_{\text{pass}})$, we can apply Eq. S3 and the above bound on the distance to get

$$\begin{aligned}
\epsilon_{\text{p}} &\geq \mathrm{TV}\big(\mathbb{P}^*_{\mathbf{CZS}R_{\text{pass}}}, \mathbb{P}_{\mathbf{CZS}R_{\text{pass}}}\big) \\
&= \sum_{r} \mathrm{TV}\big(\mathbb{P}^*_{\mathbf{CZS}|R_{\text{pass}}=r}, \mathbb{P}_{\mathbf{CZS}|R_{\text{pass}}=r}\big)\mathbb{P}(R_{\text{pass}} = r) \\
&= \mathrm{TV}\big(\mathbb{P}^*_{\mathbf{CZS}|R_{\text{pass}}=1}, \mathbb{P}_{\mathbf{CZS}|R_{\text{pass}}=1}\big)\mathbb{P}(R_{\text{pass}} = 1).
\end{aligned} \tag{S35}$$

We conclude that

$$\mathrm{TV}\big(\mathbb{P}^*_{\mathbf{CZS}|R_{\text{pass}}=1}, \mathbb{P}_{\mathbf{CZS}|R_{\text{pass}}=1}\big) \leq \epsilon_{\text{p}}/\mathbb{P}(R_{\text{pass}} = 1). \tag{S36}$$

For the second main step, we need the average “guessing probability” of $\mathbf{C}$ given $\mathbf{Z}$ conditional on $\{R_{\text{pass}} = 1\}$. This is given by

$$\begin{aligned}
\sum_{\mathbf{z}} \max_{\mathbf{c}}(\mathbb{P}^*(\mathbf{c}|\mathbf{z}, R_{\text{pass}} = 1))\mathbb{P}(\mathbf{z}|R_{\text{pass}} = 1) &\leq \sum_{\mathbf{z}} \frac{\delta}{\mathbb{P}(R_{\text{pass}} = 1|\mathbf{z})}\mathbb{P}(\mathbf{z}|R_{\text{pass}} = 1) \\
&= \delta\sum_{\mathbf{z}} \frac{\mathbb{P}(\mathbf{z})}{\mathbb{P}(R_{\text{pass}} = 1)} \\
&\leq \delta/\kappa.
\end{aligned} \tag{S37}$$

We remark that here it is necessary to assume the lower bound κ on $\mathbb{P}(R_{\text{pass}} = 1)$ in order to proceed; otherwise the bound in Eq. S37 would become unbounded due to potentially arbitrarily small values of $\mathbb{P}(R_{\text{pass}} = 1)$. Now we can apply Proposition 1 of Ref. [44]. The next lemma extracts the conclusion of this proposition in the form we need. It is obtained by substituting the variables and expressions in the reference as follows: $X \leftarrow \mathbf{C}$, $Y \leftarrow \mathbf{S}$, $E \leftarrow \mathbf{Z}$, $\mathsf{E}(X,Y) \leftarrow \text{Ext}(\mathbf{CS})$, $k \leftarrow -\log_2(\delta/\kappa) - \log_2(2/\epsilon_{\text{ext}})$, $\epsilon \leftarrow \epsilon_{\text{ext}}/2$ and the distributions are replaced with the corresponding ones that are conditional on $\{R_{\text{pass}} = 1\}$. The guessing entropy in the reference is the negative logarithm of the the average guessing probability in Eq. S37.

Lemma 2. *Suppose that* Ext *is a strong extractor with parameters* $(-\log_2(2\delta/(\kappa\epsilon_{\text{ext}})), \epsilon_{\text{ext}}/2, 2n, d, t)$. *Write* $\mathbf{U} = \text{Ext}(\mathbf{CS})$. *Then we have the following bound:*

$$TV\big(\mathbb{P}^*_{\mathbf{UZS}|R_{\text{pass}}=1}, \mathbb{P}^{\text{unif}}_{\mathbf{U}}\mathbb{P}_{\mathbf{S}}\mathbb{P}^*_{\mathbf{Z}|R_{\text{pass}}=1}\big) \leq \epsilon_{\text{ext}}. \tag{S38}$$

To apply the lemma, we obtain Ext by the TMPS algorithm with the parameters in the lemma. Expanding the logarithms as $\sigma = -\log_2(\delta) + \log_2(\kappa) + \log_2(\epsilon_{\text{ext}}) - 1$ and $\log_2(\epsilon) = \log_2(\epsilon_{\text{ext}}) - 1$ and substituting in Eq. S28 gives the requirement

$$t + 4\log_2 t \leq -\log_2(\delta) + \log_2(\kappa) + 5\log_2(\epsilon_{\text{ext}}) - 11, \tag{S39}$$

as asserted in the Protocol Soundness Theorem. The number of seed bits d is obtained from Eq. S29.

It remains to determine the overall TV distance conditional on passing. Applying Eq. S4 with $V = \mathbf{C}, \mathbf{Z}, \mathbf{S}$ and F defined as $F(\mathbf{C}, \mathbf{Z}, \mathbf{S}) = \big(\text{Ext}(\mathbf{C}, \mathbf{S}), \mathbf{Z}, \mathbf{S}\big)$, and applying Eq. S36, we have

$$\text{TV}\big(\mathbb{P}^*_{\mathbf{UZS}|R_{\text{pass}}=1}, \mathbb{P}_{\mathbf{UZS}|R_{\text{pass}}=1}\big) \leq \text{TV}\big(\mathbb{P}^*_{\mathbf{CZS}|R_{\text{pass}}=1}, \mathbb{P}_{\mathbf{CZS}|R_{\text{pass}}=1}\big) \leq \epsilon_{\text{p}}/\mathbb{P}(R_{\text{pass}} = 1). \tag{S40}$$

Then by Eq. S2, Eq. S38 and Eq. S40, we have

$$\text{TV}\big(\mathbb{P}_{\mathbf{UZS}|R_{\text{pass}}=1}, \mathbb{P}^{\text{unif}}_{\mathbf{U}}\mathbb{P}^{\text{unif}}_{\mathbf{S}}\mathbb{P}^*_{\mathbf{Z}|R_{\text{pass}}=1}\big) \leq \epsilon_{\text{ext}} + \epsilon_{\text{p}}/\mathbb{P}(R_{\text{pass}} = 1). \tag{S41}$$

As $\mathbb{P}^*_{\mathbf{Z}|R_{\text{pass}}=1} = \mathbb{P}_{\mathbf{Z}|R_{\text{pass}}=1}$, the statement of the theorem follows. □

As discussed in the main text, the Protocol Soundness Theorem implies that the unconditional TV distance from an "ideal protocol" can be bounded by $\max(\epsilon_{\text{p}} + \epsilon_{\text{ext}}, \kappa)$. This error parameter is closely related to the security definitions appearing in, for instance, Equation (1) of [45] and Definition 4 of [29]. To explain how we arrive at $\max(\epsilon_{\text{p}} + \epsilon_{\text{ext}}, \kappa)$, note that an ideal protocol may abort with positive probability, but conditioned on not aborting it produces perfectly uniform output independent of side information. That is, the distribution of an ideal protocol $\mathbb{P}^{\text{ideal}}_{\mathbf{UZS}R_{\text{pass}}}$ must satisfy $\mathbb{P}^{\text{ideal}}_{\mathbf{UZS}|R_{\text{pass}}=1} = \mathbb{P}^{\text{unif}}_{\mathbf{U}}\mathbb{P}^{\text{unif}}_{\mathbf{S}}\mathbb{P}^{\text{ideal}}_{\mathbf{Z}|R_{\text{pass}}=1}$, but the distribution of the ideal protocol is otherwise unconstrained when $R_{\text{pass}} = 0$. Given our actual protocol distribution $\mathbb{P}$ we can define a particular ideal distribution with the same probability of passing as the actual protocol by setting $\mathbb{P}^{\text{ideal}}_{\mathbf{UZS}|R_{\text{pass}}=1} = \mathbb{P}^{\text{unif}}_{\mathbf{U}}\mathbb{P}^{\text{unif}}_{\mathbf{S}}\mathbb{P}_{\mathbf{Z}|R_{\text{pass}}=1}$, $\mathbb{P}^{\text{ideal}}_{\mathbf{UZS}|R_{\text{pass}}=0} = \mathbb{P}_{\mathbf{UZS}|R_{\text{pass}}=0}$, and

$\mathbb{P}^{\text{ideal}}(R_{\text{pass}} = 1) = \mathbb{P}(R_{\text{pass}} = 1)$. If $\mathbb{P}(R_{\text{pass}} = 1) \geq \kappa$, the unconditional TV distance from $\mathbb{P}$ to this ideal protocol can be bounded by

$$\begin{aligned} TV(\mathbb{P}_{\mathbf{UZS}R_{\text{pass}}}, \mathbb{P}^{\text{ideal}}_{\mathbf{UZS}R_{\text{pass}}}) &= \sum_{r=0,1} TV(\mathbb{P}_{\mathbf{UZS}|R_{\text{pass}}=r}, \mathbb{P}^{\text{ideal}}_{\mathbf{UZS}|R_{\text{pass}}=r})\mathbb{P}(R_{\text{pass}} = r) \\ &= TV(\mathbb{P}_{\mathbf{UZS}|R_{\text{pass}}=1}, \mathbb{P}^{\text{ideal}}_{\mathbf{UZS}|R_{\text{pass}}=1})\mathbb{P}(R_{\text{pass}} = 1) \\ &\leq [\epsilon_{\text{p}}/\mathbb{P}(R_{\text{pass}} = 1) + \epsilon_{\text{ext}}]\,\mathbb{P}(R_{\text{pass}} = 1) \\ &\leq \epsilon_{\text{p}} + \epsilon_{\text{ext}}, \end{aligned} \tag{S42}$$

where above we used, in order, Eq. S3, $\mathbb{P}^{\text{ideal}}_{\mathbf{UZS}|R_{\text{pass}}=0} = \mathbb{P}_{\mathbf{UZS}|R_{\text{pass}}=0}$, Eq. S31, and $\mathbb{P}(R_{\text{pass}} = 1) \leq 1$. Alternatively, if $\mathbb{P}(R_{\text{pass}} = 1) < \kappa$, we have

$$\begin{aligned} TV(\mathbb{P}_{\mathbf{UZS}R_{\text{pass}}}, \mathbb{P}^{\text{ideal}}_{\mathbf{UZS}R_{\text{pass}}}) &= TV(\mathbb{P}_{\mathbf{UZS}|R_{\text{pass}}=1}, \mathbb{P}^{\text{ideal}}_{\mathbf{UZS}|R_{\text{pass}}=1})\mathbb{P}(R_{\text{pass}} = 1) \\ &\leq 1 \cdot \kappa \\ &= \kappa, \end{aligned} \tag{S43}$$

as the TV distance can never be greater than one. Thus we see that the distance from the ideal protocol is bounded by $\max(\epsilon_{\text{p}} + \epsilon_{\text{ext}}, \kappa)$. However, as noted in the main text, we considered a more conservative overall error parameter $\epsilon_{\text{fin}} = \max(\epsilon_{\text{p}}/\kappa + \epsilon_{\text{ext}}, \kappa)$. This ensures that for all pass probabilities exceeding κ, the pass-conditional distribution of the output is within $\epsilon_{\text{p}}/\mathbb{P}(\text{pass}) + \epsilon_{\text{ext}} \leq \epsilon_{\text{p}}/\kappa + \epsilon_{\text{ext}} \leq \epsilon_{\text{fin}}$ of $\mathbb{P}^{\text{unif}}_{\mathbf{U}}\mathbb{P}^{\text{unif}}_{\mathbf{S}}\mathbb{P}_{\mathbf{Z}|R_{\text{pass}}=1}$.

S.6 Protocol Application Details

The Protocol Soundness Theorem supports the protocol given in Table S1, with overall soundness error given by $\epsilon_{\text{fin}} = \max(\epsilon_{\text{p}}/\kappa + \epsilon_{\text{ext}}, \kappa)$. A protocol is furthermore *complete* if there exist real-world systems that pass the protocol with reasonably high probability. The completeness of our protocol is supported by quantum mechanics, which predicts experimental distributions that violate nontrivial Bell inequalities [17] and pass the protocol with high probability. Completeness is also witnessed by our repeated successful implementations of the protocol.

The five new data sets reported in the main paper were taken in 2017. Each trial in a data set encompassed fourteen time intervals, and in a given trial, the outcome "+" was recorded if there was a detection in any one of these intervals and "0" otherwise. The number of intervals was fixed and chosen in advance of running the protocol. The five data sets were analyzed in the order in which they were taken. We determined the Bell function T from training data consisting of the first 5×10^6 trials as explained in S.3. We chose 5×10^6 trials so that we could obtain a Bell function T using an accurate estimate of the experimental distribution of measurement outcomes without sacrificing too much data that could be used for randomness generation. After the protocol was officially run on a data set, the same data set was re-analyzed using different lengths of training portions to see if a different length should be used for subsequent data sets, but there was never clear evidence to suggest that we should have used a different length for the training portion.

Table S1: Protocol for Randomness Generation

1. Choose a Bell function T satisfying the conditions of the Entropy Production Theorem, a number of trials n to be run, a threshold for passing $v_{\text{thresh}} > 1$, error parameters $\epsilon_{\text{p}}, \epsilon_{\text{ext}}, \kappa > 0$, and a positive integer t for which Eq. 5 is satisfied.

2. (Entropy Production) Run a succession of n experimental trials, where in each trial i Alice and Bob randomly and uniformly choose respective settings $X_i, Y_i \in \{0, 1\}$, and record respective outputs $A_i, B_i \in \{+, 0\}$. (Optional) Calculate $\prod_{j=1}^{i} T(A_j, B_j, X_j, Y_j)$ after each trial and re-set T to the constant function 1 for the remainder of the experiment if $\prod_{j=1}^{i} T(A_j, B_j, X_j, Y_j) > v_{\text{thresh}}$.

3. Compute $\prod_{i=1}^{n} T(A_i, B_i, X_i, Y_i)$ and abort if this quantity does not exceed v_{thresh}.

4. (Extraction) Generate a random and uniform d-bit seed string $\mathbf{S}$ where d is given by Eq. S29 with $q = 2n, \epsilon = \epsilon_{\text{ext}}/2$. Output $\mathbf{U} = \text{Ext}(\mathbf{AB}, \mathbf{S})$ with the security guarantee given by Eq. 6.

After training, we inferred an expected value $n\mu$ and variance $n\sigma^2$ of $\sum_{i=1}^{n} \ln(T_i)$ on the remaining trials assuming i.i.d. trials and Gaussian statistics according to the central limit theorem, where n and μ were calculated according to the distribution obtained from the optimization problem of Eq. S23. Note that under these assumptions, we treat $\sum_{i=1}^{n} \ln(T_i)$ as if it were a sum of independent and bounded RVs. Since $V = \exp\left(\sum_{i=1}^{n} \ln(T_i)\right)$ we can then choose v_{thresh} so that it has a 0.95 chance of being exceeded according to the Gaussian approximation, by setting $v_{\text{thresh}} = e^{n\mu - 1.645\sqrt{n}\sigma}$. For Data Sets 3, 4 and 5, v_{thresh} was chosen to be smaller than this value to increase the chance of passing the protocol while still meeting desirable benchmarks for extractable randomness.

We now discuss our application of the protocol to Data Set 5, and then summarize the main results for all five data sets in Table S4. Data Set 5 set consists of 60,110,210 trials, roughly twice as long as each of the first four data sets. The counts for each trial outcome from the first 5×10^6 trials are shown in Table S2. The maximum likelihood non-signaling distribution corresponding to these counts is shown in Table S3. We determined T from this distribution, the values of T are shown in Table 1 of the main text.

Table S2: Result counts for the first 5×10^6 trials of Data Set 5.

	$ab = ++$	$ab = +0$	$ab = 0+$	$ab = 00$
$xy = 00$	3166	1851	2043	1243520
$xy = 01$	3637	1338	13544	1230633
$xy = 10$	3992	13752	1226	1230686
$xy = 11$	357	17648	16841	1215766

The 0.95 rule for determining v_{thresh} given that there are 55,110,210 trials for the protocol yields $v_{\text{thresh}} = 8.79 \times 10^{36}$. We chose a more conservative value of $v_{\text{thresh}} = 1.5 \times 10^{32}$ to

Table S3: Maximum likelihood non-signaling distribution according to the counts in Table S2, rounded to eight decimal places.

	$ab =$ ++	$ab =$ +0	$ab =$ 0+	$ab =$ 00
$xy = 00$	0.00063301	0.00036794	0.00041085	0.24858820
$xy = 01$	0.00073159	0.00026936	0.00270824	0.24629081
$xy = 10$	0.00080002	0.00277179	0.00024384	0.24618435
$xy = 11$	0.00007087	0.00350093	0.00336896	0.24305924

improve the odds of passing the protocol, while still allowing for the extraction of 1024 bits uniform to within 10^{-12}. This threshold corresponds to a probability of passing of roughly 0.9916 according to the i.i.d. scenario described above. Running the protocol, this threshold was exceeded, with a final value of $V = 2.018 \times 10^{41}$.

The running product $\prod_{i=1}^{c} T_i$ first exceeded v_{thresh} at trial number $c = 41,243,976$, and one has the option of setting the remaining $T_i = 1$ regardless of outcome for the rest of the data run. The soundness of this procedure is justified by the adaptive properties of the Entropy Production Theorem. In our application of the protocol, we implemented a similar strategy without technically changing the Bell function, by relabeling all outcomes to 0 starting at trial number $c + 1$. This also results in $T_i = 1$ for the remainder of the experiment. This strategy is justified as our assumptions allow for Alice and Bob to cooperatively make arbitrary changes to the experiment in advance of a trial based on the past, which includes the current running product. Turning off the detectors to guarantee outcomes of 0 is one such change, and in principle there was sufficient time (at least $5\,\mu s$) for the necessary communication to take place after the previous trial.

Throughout, we did not consider the length d of the seed in making our choices and determined d from the other parameters according to Eq. S29. For applying the extractor to Data Set 5, we used 315,844 seed bits. The seed bits were collected from one of the random number generators used to select the settings in [13]. Specifically, each seed bit came from the XOR of two bits generated by the photon-sampling random number generator described in [13]. It took 317 seconds for our computer to construct the extractor according to the TMPS algorithm and generate the explicit final output string. Here is the final output string that results from applying the extractor to the string $\mathbf{AB}$, when $\mathbf{AB}$ is obtained with relabeling of all outcomes to 0 starting at trial number $41,243,977$ (after v_{thresh} is exceeded by the running product).

```
11100010011111111101001100001111100101010101001101111001111010110101101000011011000111010001101000111010011110011100101101100100
10111111110011000101100101101111011001011110100110011011011110101001110010110101111111011110010100110010001010110000011111111101
11011001110001111100010010011100011100000000010110010101101111001011001001000001101110110000000111110111001110001100101110001100
10110110001100011101001001001010101000100001010101001001011101010100101010011100110100101000101010000110111111101100110111110000
11100110100110010111001011000110010100101000110101100100000010111000101101001101110110111111001110110011100000001111001111101100
10110000111110011100110111111011010111100000101000101011010001001110101100000010010111000101101011011111100110100001110101110110101
10001010011111011110111001000000100011011111111001110100111010011100000010010110001001110111010000111010111100100101111111001100
01111011101001101010101011000100100000111111100101010110101111111000111110110001010111011000001111000011111101100100010001001000001
```

After the protocol was run, we ran consistency checks on the data sets to look for potential inconsistencies with Eq. 3, the no-signaling assumption. Using the tests described in Ref. [13], we examined the four signaling equalities: 1: $\mathbb{P}(A|X = 0, Y) = \mathbb{P}(A|X = 0)$, 2: $\mathbb{P}(A|X =$

Table S4: Summary of application of protocol to data sets. For fixed goal choices of ϵ_{fin}, the error parameters were computed according to the formula $\epsilon_{\text{p}} = \kappa^2 = (0.95\,\epsilon_{\text{fin}})^2$, $\epsilon_{\text{ext}} = 0.05\,\epsilon_{\text{fin}}$. Error parameters were chosen in advance of running the protocol for Data Sets 3, 4 and 5; the ϵ_{fin} and t values for Data Sets 1 and 2 are marked with an asterisk as they were not chosen in advance and are only included for illustrative purposes. We remark that the quantity $1/v_{\text{thresh}}$ can also be interpreted as a p-value against local realism [31].

Data Set	n	m	95% cut off	v_{thresh}	ϵ_{fin}	t	$V > v_{\text{thresh}}$
1	24865320	0.01066	4.68×10^{16}	4.68×10^{16}	10^{-6*}	512^*	Yes
2	24809970	0.01126	1.30×10^{5}	1.30×10^{5}	0.01^*	61^*	Yes
3	24818959	0.01163	9.74×10^{19}	10^{17}	10^{-6}	512	Yes
4	24846822	0.01063	6.57×10^{15}	10^{15}	10^{-6}	256	Yes
5	55110210	0.01004	8.79×10^{36}	1.5×10^{32}	10^{-12}	1024	Yes

Table S5: 2-tail p-values for consistency checks

Data Set	Sig. 1	Sig. 2	Sig. 3	Sig. 4
Data Set 1	0.507	0.777	0.290	0.323
Data Set 2	0.765	0.965	0.115	0.684
Data Set 3	0.633	0.072	0.381	0.099
Data Set 4	0.144	0.320	0.844	0.356
Data Set 5	0.879	0.131	0.554	0.885

$1, Y) = \mathbb{P}(A|X = 1)$, 3: $\mathbb{P}(B|X, Y = 0) = \mathbb{P}(B|Y = 0)$, and 4: $\mathbb{P}(B|X, Y = 1) = \mathbb{P}(B|Y = 1)$. For these tests we used statistics whose asymptotic distributions would approach the standard normal with mean 0 and variance 1, if the trials were i.i.d. We report the p-values obtained from these tests for all data sets in Table S5, which do not suggest any inconsistencies.

Prior to the analysis of the five data sets reported in the main text, the protocol was applied to data sets taken as part of the experiment reported in Ref. [13]. These results are described in [46]. After setting aside the first 5×10^7 trials of the data set XOR 3 as a training set to construct the function T and choose a threshhold v_{thresh} based on the 95% rule, the protocol was applied to the rest of the data set with parameters $\epsilon_{\text{p}} = 3.1797 \times 10^{-4}$ and $\epsilon_{\text{ext}} = 3.533 \times 10^{-5}$, which were chosen to minimize $\epsilon_{\text{p}}/\kappa + \epsilon_{\text{ext}}$ for $\kappa = 1/3$ while satisfying Eq. 5. This choice of parameters was suboptimal for minimizing either ϵ_{fin} or $\max(\epsilon_{\text{p}} + \epsilon_{\text{ext}}, \kappa)$, the two figures of merit disucssed in the main text. However, the instance of the TMPS algorithm induced by the above choice of parameters would have been induced by other choices of parameters that perform better according to these figures of merit. The same extraction is induced by $\epsilon_{\text{p}} = 3.6509 \times 10^{-4}$, $\epsilon_{\text{ext}} = 3.5330 \times 10^{-5}$, and $\kappa = 4.0042 \times 10^{-4}$, which leads to a distance of $\max(\epsilon_{\text{p}} + \epsilon_{\text{ext}}, \kappa) = 4.0042 \times 10^{-4}$ from an ideal protocol for the extraction of 256 bits. We can also choose $\epsilon_{\text{p}} = 3.370 \times 10^{-4}$, $\epsilon_{\text{ext}} = 3.533 \times 10^{-5}$, and $\kappa = 0.0184$ to induce the same extraction with an ϵ_{fin} parameter of 0.0184.

Statistically significant settings nonuniformity was detected for some of the sets examined in [46]. This was consistent with the finding in [13] that a combination of uncontrolled environmental variables and the synchronization electronics introduced small biases in the settings. This effect is not present in the 2017 data sets, which used a reliable pseudorandom source for settings randomness. As the Entropy Production Theorem can tolerate small biases in the settings distribution, we can explore how the protocol would have performed on XOR 3 had we selected, prior to running the protocol, a nonzero settings-bias parameter α. We note that the protocol parameters must be chosen prior to executing a secure protocol, and since we did not choose a nonzero α in advance of examining XOR 3, we report the following calculations only as a retrospective diagnostic. In principle it is impossible to measure α through statistical tests of the output of the random number generators that choose the settings, because the settings probability can appear random, unbiased, and independent even while changing from trial to trial within the bounds of a potentially large α. To choose an example α to study, we examined 95 % confidence intervals for the individual settings probabilities from the six data sets in [13]. The largest absolute difference from 0.5 among the endpoints of these six intervals was 0.000211 for Alice and 0.000150 for Bob. Assuming independence between Alice and Bob (an assumption which was not contradicted by our statistical tests), we computed the most and least likely measurement configurations given this largest difference from 0.5 for Alice's and Bob's settings probability, and found that these would be contained in the interval $(0.25-\alpha, 0.25+\alpha)$ for $\alpha = 0.000181$. For this example choice of α, performing the modified optimization problem described in S.3 yields a T function with $m = 0.01179$, and for this T function, the expected threshold computed according to the 95 % rule is $v_{\text{thresh}} = 5.25 \times 10^5$, if we assume the "worst-case" settings distribution among the six extremal settings distributions that assign probability $0.25 + \alpha$ to two settings configurations and $0.25 - \alpha$ to two other settings configurations. This threshold is passed when the protocol is re-run now with this non-zero α. For ϵ_{p} values of $(0.01, 0.001, 0.0001, 0.00001)$ we get corresponding $-\log_2 \delta$ values of $(524, 383, 242, 101)$, which is a moderate reduction compared to the corresponding values of $(582, 444, 306, 168)$ obtained by the running the protocol with $\alpha = 0$. Alternatively, we can fix ϵ_{p} and study how $-\log_2 \delta$ changes with α. For one particular choice of $\epsilon_{\text{p}} = 3.1797 \times 10^{-4}$, which was the smallest ϵ_{p} value considered earlier in analyses of XOR 3, α values of (0, 0.00001, 0.0001, 0.001) yield $-\log_2 \delta$ values of (367, 366, 321, 94). The largest value $\alpha = 0.001$ in this list may be considered a conservative choice: if in the first calculation above we had used $99.999998\,\%$ instead of $95\,\%$ confidence intervals, we would have obtained a value of $\alpha \approx 0.001/3$ instead of $\alpha = 0.000181$.

S.7 Performance of Previous Protocols.

Other protocols in the literature could not be used for our data sets for various reasons. Many protocols apply to different measurement scenarios. For instance, [4] describes a protocol involving three separated measurement stations, and while [27] provides impressive expansion rates and is secure against quantum side information, it requires eight separate devices. Other protocols exploring quantum side information in Refs. [3, 8, 30] either also apply to different experimental setups or provide only asymptotic security results as the number of trials n approaches infinity. The first protocol achieving security against quantum side information [6] applies to a bipartite experiment like ours but requires systems that achieve per-trial Bell violations much higher than ours. Another study [11] of bipartite experiments with data regimes characteristic of photonic systems applies to i.i.d. scenarios.

The protocols of Refs. [5, 29] are applicable to our experimental scenario while making minimal assumptions, and given enough trials could work for any violation regime. Ref. [5] obtained protocols for assumptions equivalent to ours, but considered also the case where the distributions are in addition assumed to be quantum achievable. Ref. [29], which uses the Entropy Accumulation Theorem of Ref. [28], obtained protocols assuming that the distributions are quantum achievable, but allowing for quantum side information. However, these protocols are ineffective for the numbers of trials in our data sets, which we illustrate with a heuristic argument. Both protocols are based on the Clauser-Horne-Shimony-Holt (CHSH) Bell function [47]

$$T^c(a,b,x,y) = \begin{cases} 1 & \text{if } (x,y) \neq (1,1) \text{ and } a = b \\ 1 & \text{if } (x,y) = (1,1) \text{ and } a \neq b \\ 0 & \text{otherwise.} \end{cases} \tag{S44}$$

The statistic $\overline{T^c} = n^{-1}\sum_{i=1}^n T_i^c$ used by these protocols for witnessing accumulated violation satisfies $\mathbb{E}(\overline{T^c}) \leq 0.75$ under LR, while $\mathbb{E}(\overline{T^c}) = 0.75009787$ for the distribution in Table S3. The completely predictable LR theory that only produces "00" outcomes regardless of the settings satisfies $\mathbb{E}(\overline{T^c}) = 0.75$, but in an experiment of $n = 55,110,210$ trials, this theory can produce a value of $\overline{T^c}$ exceeding 0.75009787 with probability roughly 0.047. Thus, based on this statistic alone, we cannot infer the presence of any low-error randomness.

The protocol of Ref. [5] (the PM protocol for short, see [2, 7] for amendments), can be modified to work with any Bell function, and there are methods for obtaining better Bell functions [9, 10] or simultaneously using a suite of Bell functions [48]. Here, we demonstrate that for any choice of Bell function, the method of [5] as refined in [2] cannot be expected to effectively certify any randomness from an experiment distributed according to Table S3 unless the number of trials exceeds 1.56×10^8, which is larger than the number of trials in our data runs.

For the most informative comparison to our protocol, we consider the PM protocol without their additional constraint that the distribution be induced by a quantum state. To derive a bound on the performance of the PM protocol, we refer to Theorem 1 of [2]. This theorem involves a choice of Bell function denoted by I (analogous to our T), a threshold J_m (analogous to our v_{thresh}) to be exceeded by the Bell estimator $\bar{I} = n^{-1}\sum_{i=1}^n I_i$, and a function f that we discuss below. To be able to extract some randomness, the theorem requires that

$$nf(J_m - \mu) > 0. \tag{S45}$$

The parameter μ is given by $(I_{\text{max}} + I_{\text{NS}})\sqrt{(2/n)\ln(1/\epsilon)}$ where I_{max} is the largest value in the range of the Bell function I, $I_{\text{NS}} \leq I_{\text{max}}$ is the largest possible expected value of I for non-signaling distributions, and $0 < \epsilon \leq 1$ is a free parameter that is added to the TV distance from uniform for the final output string. Smaller choices of ϵ, which is analogous to our ϵ_{p}, are desirable but require larger n for the constraint Eq. S45 to be positive as we will see below. We also note that Eq. S45 is a necessary but not sufficient condition for extracting randomness; in particular, we ignore the negative contribution from the parameter ϵ' of [2] (somewhat analogous to the parameter κ in the statement of the Protocol Soundness Theorem in S.5) as well as any error introduced in the extraction step.

For Eq. S45, we can without loss of generality consider only Bell functions for which $0 \leq I_L < I_{\text{NS}} \leq I_{\text{max}}$, where I_L is the maximum expectation of I for LR distributions. Further, because the relevant quantities below are invariant when the Bell function is rescaled, we can assume $I_L = 1$. According to Ref. [2]'s Eq. 8 and the following paragraph, we can write $f(x) = -\log_2(g(x))$, where g is monotonically decreasing and concave, and satisfies

$$\max_{ab} \mathbb{P}(ab|xy) \leq g(\mathbb{E}(I)_{\mathbb{P}}) \tag{S46}$$

for all xy and non-signaling distributions $\mathbb{P}$. (Recall that we are not using the stronger constraint that $\mathbb{P}$ be induced by a quantum state.) According to Eq. S15 we can define $g(x) = 1 + (1 - x)/(2(I_{\text{NS}} - 1))$. Later we argue that this definition of g cannot be improved. Substituting into Eq. S45 we get the inequality

$$-n\log_2\left[1 + \frac{1 - J_m + (I_{\text{max}} + I_{\text{NS}})\sqrt{\frac{2}{n}\ln\frac{1}{\epsilon}}}{2(I_{\text{NS}} - 1)}\right] > 0. \tag{S47}$$

Since $2(I_{\text{NS}} - 1)$ is positive, this is equivalent to

$$\sqrt{\frac{2}{n}\ln\frac{1}{\epsilon}} < \frac{J_m - 1}{I_{\text{max}} + I_{\text{NS}}}. \tag{S48}$$

Noting that $I_{\text{max}} + I_{\text{NS}} \geq 2I_{\text{NS}}$, this implies

$$\sqrt{\frac{2}{n}\ln\frac{1}{\epsilon}} < \frac{J_m - 1}{2I_{\text{NS}}}. \tag{S49}$$

Thus, the number of trials needed to extract randomness by the PM protocol is bounded below according to

$$n > 8\frac{\ln(1/\epsilon)I_{\text{NS}}^2}{(J_m - 1)^2}. \tag{S50}$$

For a given anticipated experimental distribution $\mathbb{P}_{\text{ant}}$, J_m is best chosen to be at most $\mathbb{E}(I)_{\mathbb{P}_{\text{ant}}}$. Otherwise, the probability that $\bar{I}$ exceeds J_m is small. However, for the maximum amount of extractable randomness, J_m should be close to $\mathbb{E}(I)_{\mathbb{P}_{\text{ant}}}$. Consider the inferred distribution from the first 5×10^6 trials of Data Set 5. By following the procedure given in Section 2 of [39], we can write this distribution as a convex combination of a PR box with weight $p = 3.915 \times 10^{-4}$

and an LR distribution with weight $1-p$. From this we see that one should choose $J_m \leq \mathbb{E}(I)_{\mathbb{P}_{\text{ant}}} = pI_{\text{NS}} + (1-p) \leq pI_{\text{NS}} + 1$. Substituting into Eq. S50 and using $\epsilon \leq 0.05$ (a rather high bound on the allowable TV distance from uniform) gives

$$n > 8\frac{\ln(1/\epsilon)}{p^2} \geq 1.56 \times 10^8, \tag{S51}$$

which is already more than twice the number of trials used to generate randomness in Data Set 5. For smaller error values comparable to the ones we report, this bound only increases: achieving $\epsilon = 10^{-12}$ would require at least 1.44×10^9 trials.

To finish our argument that the PM protocol cannot improve on this bound under our assumptions, consider the definition of g. If we could find a function $g' \leq g$ with $g'(x) < g(x)$ for some $x \in (1, I_{\text{NS}}]$, then $f = -\log_2(g')$ might yield a smaller lower bound on n. Note that for $x \leq 1$, $g'(x) \geq g'(1)$ and $g'(1)$ must be at least 1 because, referring to Eq. S46, there is a conditionally deterministic LR distribution $\mathbb{P}$ satisfying $\mathbb{E}(I)_{\mathbb{P}} = 1$ and $\max_{ab} \mathbb{P}(ab|xy) = 1$. Hence Eq. S45 cannot be satisfied for arguments x of $f(x) = -\log_2(g'(x))$ with $x \leq 1$. Given $x \in (1, I_{\text{NS}}]$, write $x = (1-p) + pI_{\text{NS}}$. Let $\mathbb{Q}$ be the PR box achieving $\mathbb{E}(I)_{\mathbb{Q}} = I_{\text{NS}}$ and $\mathbb{Q}'$ a conditionally deterministic LR theory achieving $\mathbb{E}(I)_{\mathbb{Q}'} = 1$. Then $\mathbb{E}(I)_{(1-p)\mathbb{Q}'+p\mathbb{Q}'} = x$. Furthermore, there is a setting xy at which the LR theory's outcome is inside the support of the PR box's outcomes. To see this, by symmetry it suffices to consider the PR box of Eq. S13. Its outcomes are opposite at setting 11 and identical at the other three. A deterministic LR theory's outcomes are opposite at an even number of settings, so either it is opposite at setting 11, or it is identical at one of the others. For setting xy, the bound in Eq. S46 is achieved for our definition of g. Hence any other valid replacement g' for g must satisfy $g'(x) \geq g(x)$ for $x \in (1, I_{\text{NS}}]$, and so Eq. S45 with $f(x) = -\log_2(g'(x))$ implies Eq. S45 with $f(x) = -\log_2(g(x))$. Thus the lower bound on n derived above will apply to g' as well.

References

[35] Levin, D. A., Peres, Y. & Wilmer, E. L. *Markov chains and mixing times* (American Mathematical Soc., 2009).

[36] Pardo, M. & Vajda, I. About distances of discrete distributions satisfying the data processing theorem of information theory. *IEEE transactions on information theory* **43**, 1288–1293 (1997).

[37] Popescu, S. & Rohrlich, D. Quantum nonlocality as an axiom. *Found. Phys.* **24**, 379–85 (1994).

[38] Barrrett, J. *et al.* Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A* **71**, 022101 (2005).

[39] Bierhorst, P. Geometric decompositions of Bell polytopes with practical applications. *J. Phys. A: Math. Theor.* **49**, 215301 (2016).

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

[41] Vadhan, S. P. *Pseudorandomness*, vol. 7 of *Foundations and Trends in Theoretical Computer Science* (2012).

[42] Ma, X., Zhang, Z. & Tan, X. Explicit combinatorial design (2012). ArXiv:1109.6147v2 [math.CO].

[43] Kessler, M. & Arnon-Friedman, R. Device-independent randomness amplification and privatization (2017). ArXiv:1705.04148 [quant-ph].

[44] König, R. & Terhal, B. The bounded-storage model in the presence of a quantum adversary. *IEEE T. Inform. Theory* **54**, 749–62 (2008).

[45] Portmann, C. & Renner, R. Cryptographic security of quantum key distribution (2014). ArXiv:1409.3525 [quant-ph].

[46] Bierhorst, P. *et al.* Experimentally generated random numbers certified by the impossibility of superluminal signaling (2017). ArXiv:1702.05178 [quant-ph].

[47] Clauser, J., Horne, A., Shimony, A. & Holt, R. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.* **23**, 880–884 (1969).

[48] Nieto-Silleras, O., Bamps, C., Silman, J. & Pironio, S. Device-independent randomness generation from several Bell estimators (2016). ArXiv:1611.00352 [quant-ph].