Published in final edited form as:

Nature. 2018 April ; 556(7700): 223–226. doi:10.1038/s41586-018-0019-0.

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

Abstract

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 randomness, 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,

*Correspondence and requests for materials should be addressed to P.B. (peter.bierhorst@nist.gov).

†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

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.

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]

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

where the s_{xy}^{ab} 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 $\mathbb{P}(A = a, B = b \mid X = x, Y = y)$ is of the form $\sum_\lambda \mathbb{P}(A = a \mid X = x, \Lambda = \lambda)\mathbb{P}(B = b \mid Y = y, \Lambda = \lambda)\mathbb{P}(\Lambda = \lambda)$ 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:

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

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:

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

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 $\mathbf{XY} = X_1Y_1X_2Y_2\ldots X_nY_n$, and other sequences such as **AB** and **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 $\epsilon_{\mathrm{p}} \in (0, 1)$ and v_{thresh} satisfying $1 \leq v_{\mathrm{thresh}} \leq (1 + (3/2)m)^n \epsilon_{\mathrm{p}}^{-1}$:

$$\mathbb{P}_e(\mathbb{P}_e(\mathbf{AB} \mid \mathbf{XY}) > \delta \mathbf{AND}\ \ V \geq v_{\mathrm{thresh}}) \leq \epsilon_p \tag{4}$$

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

In words, the theorem says that with high probability, if V is at least as large as v_{thresh}, then the output **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 **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 **AB**, we use the TMPS algorithm to obtain an extractor, specifically a function Ext that takes as input the string **AB** and a length d "seed" bit string **S**, where **S** is uniform and independent of **ABXY**. Its output is a length t bit string. **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 **S**. In order for the output to be within

a distance ϵ_{fin} of uniform independent of **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

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

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

The number of seed bits d required satisfies $d = O\left(\log(t)\log(nt/\epsilon_{\text{ext}})^2\right)$, 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 $\epsilon_{\text{p}} = \kappa^2 = \times 9.025 \times 10^{-25}$ 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 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 ± 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.

Supplementary Material

Refer to Web version on PubMed Central for supplementary material.

Acknowledgments

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

References

[1]. Acín A & Masanes L. Certified randomness in quantum physics. Nature 540, 213 (2016). [PubMed: 27929003]

[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). [PubMed: 20393558]

[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). [PubMed: 26503041]

[13]. Shalm LK 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 MJ, 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 JS, Shimony A, Horne MA & Clauser JF. 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 PM. 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 BS. 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).

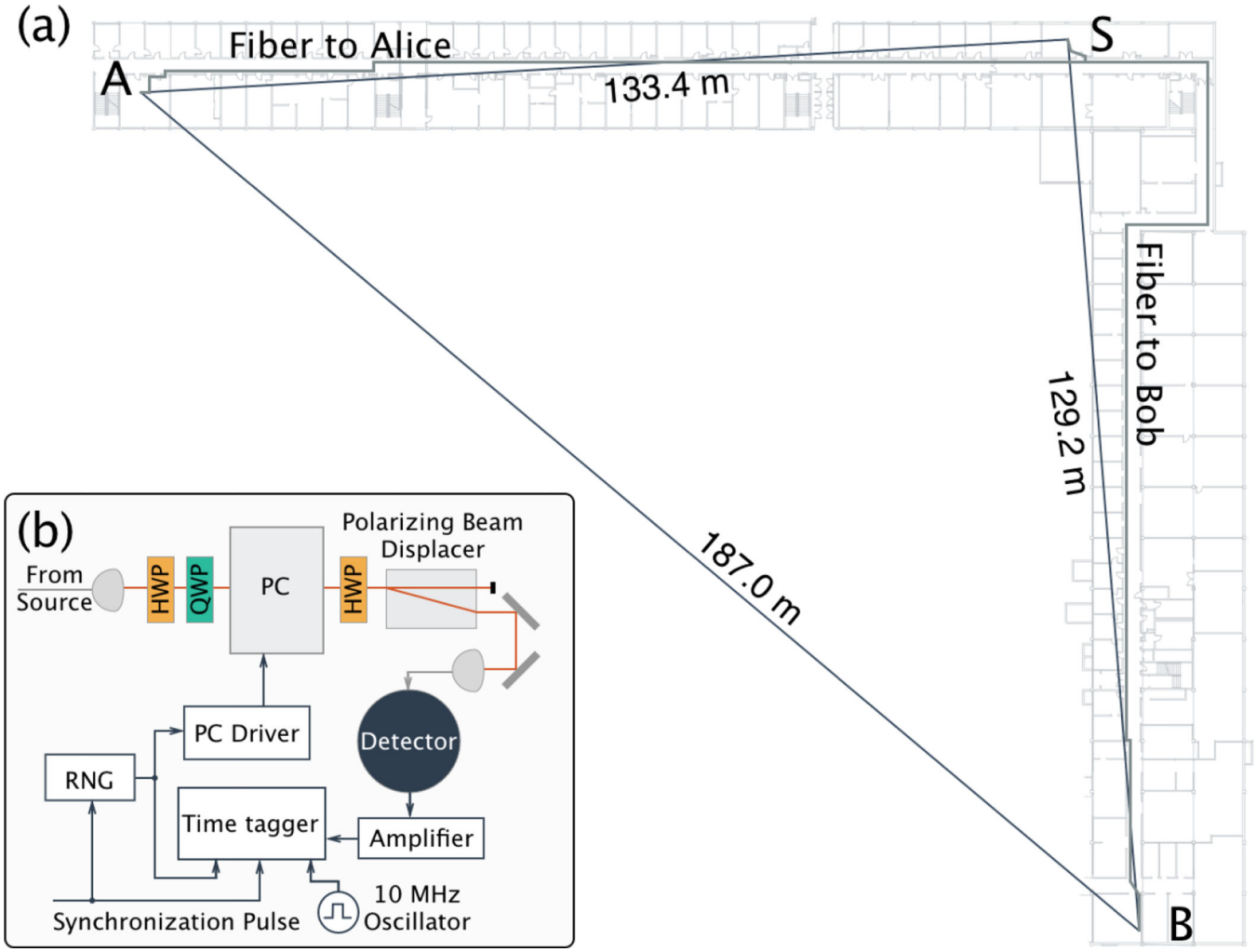

Figure 1: The locations of the Source (S), Alice (A) and Bob (B).

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.

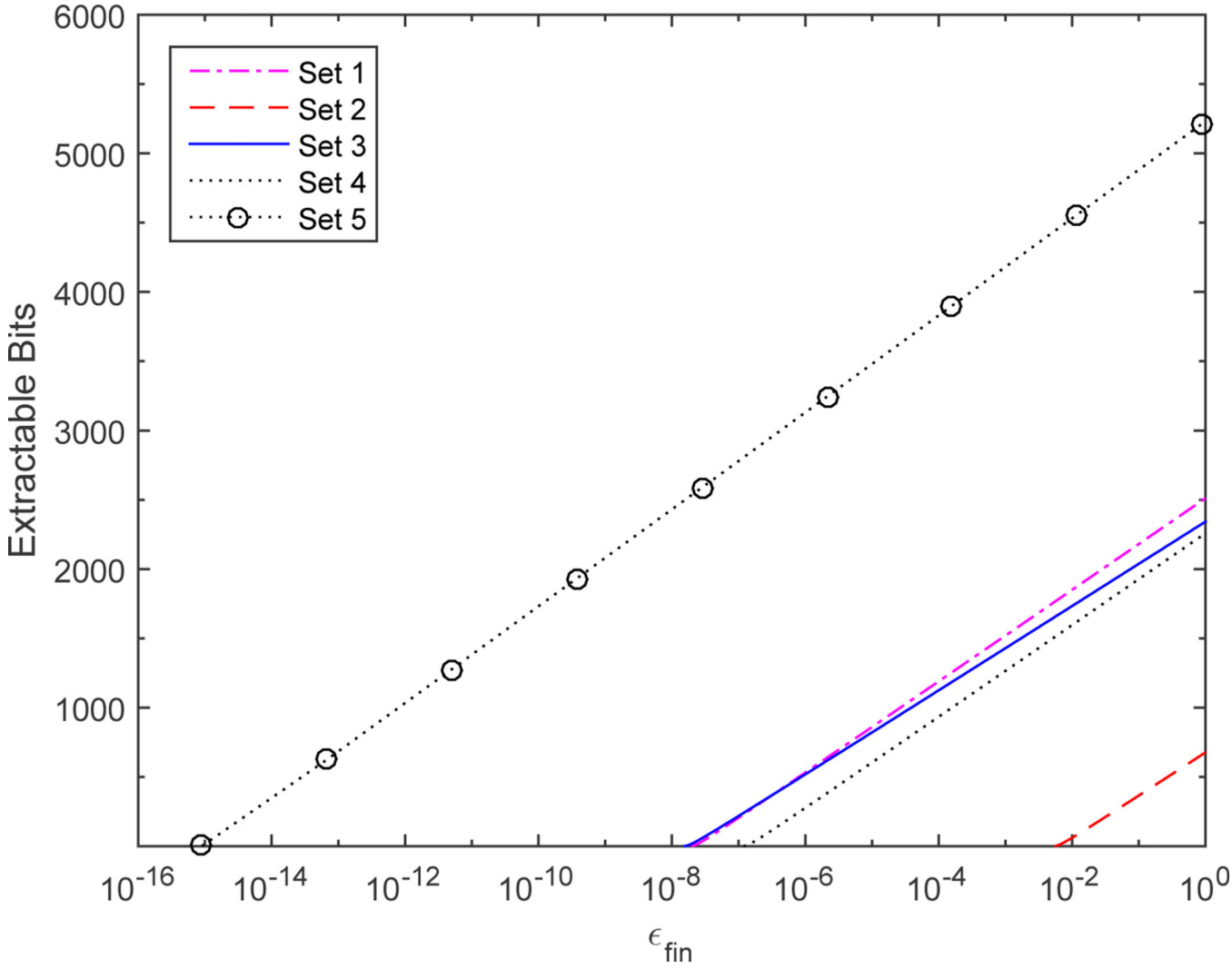

Figure 2: Extractable bits as a function of error.

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}.

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