

Quantum Probability Estimation for Randomness with Quantum Side Information

Yanbao Zhang,¹ Emanuel Knill,^{2,3} Honghao Fu,⁴ and Peter Bierhorst²

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

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

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

⁴*Joint Institute for Quantum Information and Computer Science, University of Maryland, College Park, Maryland 20740, USA*

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

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

Loophole-free Bell tests have been realized with nitrogen-vacancy (NV) centers [6], with atoms [7] and with photons [8, 9], enabling the possibility of full experimental demonstrations of DIRG. For NV centers or atoms, the rate of trials is low, and for photons, the violation of local realism per trial is small. Considering these facts, none of previously available DIRG protocols [3, 10–18] is ready to be implemented with current loophole-free Bell tests. The reason behind is that the finite-data efficiency of these protocols is too low such that an experimental implementation would require too many trials. Experimental techniques will improve, but the finite-data efficiency of a protocol is important for many applications of randomness generation, which often require short blocks of fresh random bits with minimum delay. Excellent finite-data efficiency was achieved by a method that we described and im-

plemented in Refs. [19, 20], which reduced the time required for generating 1024 low-error random bits with respect to classical side information from hours to minutes for a state-of-the-art photonic loophole-free Bell test. The basis for success of this method motivated our development of the probability estimation (PE) framework [21] for randomness certification against classical side information with better finite-data efficiency. PE has many other advantages, which include asymptotic optimality, unrestricted in-protocol adaptability, and broad applicability. Here we introduce quantum probability estimation (QPE), which has the advantages of PE but with full security against quantum side information. We illustrate the unsurpassed finite-data efficiency on a few examples.

QPE (or PE) obtains a bound on the conditional probability of the observed outcomes given the chosen settings, valid for all quantum (or classical) side information. We show how to obtain conditional entropy estimates from this bound to quantify the number of extractable random bits.

Both QPE and PE are broadly applicable. In particular it is not limited to device-independent scenarios and can be applied to traditional randomness generation with quantum devices, where it enhances the security of random numbers with statistically rigorous certificates. Such applications are enabled by the notion of models, which are sets of accessible classical or quantum side information that capture verified, physical constraints on device behavior. In the case of Bell tests, these constraints include the familiar non-signaling conditions [22, 23]. In the case of two-level systems such as polarized photons, the constraints can capture that measurement angles are within a known range, for example.

Below we first describe the technical features of QPE and the main results that enable its practical use. We then demonstrate the large improvements with QPE in finite-data efficiency (see Figure 1). We also reanalyze the experimental data from Refs. [10] and [19] where randomness with respect to classical side information was certified, while with QPE we are able to obtain random bits even with quantum side information (see Table I).

Theory. Consider an experiment with “inputs” \mathbf{Z} and “outputs” \mathbf{C} . The inputs normally consist of the

random choices made for measurement settings but may include choices of state preparations such as in the protocols of Refs. [24, 25]. The outputs consist of the corresponding measurement outcomes. In the cases of interest, the inputs and outputs are determined in a sequence of n time-ordered trials, where the i 'th trial has input Z_i and output C_i . We refer to the trial inputs and outputs collectively as the trial "results". In this case $\mathbf{Z} = (Z_i)_{i=1}^n$ and $\mathbf{C} = (C_i)_{i=1}^n$. We assume that Z_i and C_i are countable-valued. The upper-case symbols introduced above are treated as random variables. As is conventional, their values are denoted by the corresponding lower-case symbols. The party with respect to which the randomness is intended to be unpredictable is represented by an external quantum system \mathbf{E} , whose initial state before the experiment may be correlated with the devices used. Once the experiment starts, the system \mathbf{E} has no further interaction with the devices or the laboratory that contains them.

The final state after the experiment can be written as $\rho_{\mathbf{CZ}\mathbf{E}} = \sum_{\mathbf{cz}} |\mathbf{cz}\rangle \langle \mathbf{cz}| \otimes \rho_{\mathbf{E}}(\mathbf{cz})$, where $\rho_{\mathbf{E}}(\mathbf{cz})$ is the unnormalized state of \mathbf{E} given results \mathbf{cz} , and $\sum_{\mathbf{cz}} \text{tr}(\rho_{\mathbf{E}}(\mathbf{cz})) = 1$. A model for the experiment is the set of final states that can occur and is normally constructed by chaining models for each individual trial. This construction works under a Markov condition on the trial inputs similar to the Markov condition required for the entropy-accumulation channel chains of Ref. [17]. As a result, QPE does not require independent and identical trials.

Given the final state $\rho_{\mathbf{CZ}\mathbf{E}}$ as above, define $\rho_{\mathbf{E}}(\mathbf{z}) = \sum_{\mathbf{c}} \rho_{\mathbf{E}}(\mathbf{cz})$. For a given state $\rho_{\mathbf{CZ}\mathbf{E}}$, the normalized, sandwiched, conditional α -Rényi power for value \mathbf{cz} , $\hat{\mathcal{R}}_{\alpha}(\rho(\mathbf{cz})|\rho(\mathbf{z}))$, is given by

$$\frac{1}{\text{tr}(\rho(\mathbf{cz}))} \text{tr}((\rho(\mathbf{z}))^{-\beta/(2\alpha)} \rho(\mathbf{cz}) \rho(\mathbf{z})^{-\beta/(2\alpha)})^{\alpha},$$

where $\alpha > 1$ and $\beta = \alpha - 1$. Below we first describe how to estimate the conditional Rényi power for the observed results \mathbf{cz} , and then we relate such an estimate to a lower bound on the smooth conditional min-entropy with respect to quantum side information. See Ref. [26] for detailed proofs and results.

In order to estimate the conditional Rényi power, we construct quantum estimation factors (QEFs). QEFs with power β are functions $F : \mathbf{cz} \mapsto F(\mathbf{cz}) \geq 0$ such that for all states $\rho_{\mathbf{CZ}\mathbf{E}}$ in the model, F satisfies the QEF inequality

$$\sum_{\mathbf{cz}} \text{tr}(\rho(\mathbf{cz})) F(\mathbf{cz}) \hat{\mathcal{R}}_{\alpha}(\rho(\mathbf{cz})|\rho(\mathbf{z})) \leq 1.$$

QEFs yield upper bounds on the conditional Rényi powers with an arbitrary specified confidence level.

The conditional Rényi power estimate provided by a QEF implies a smooth conditional min-entropy

estimate. If the smooth conditional min-entropy estimate is larger than a threshold specified before running the protocol, a quantum-proof strong extractor can be applied to the outputs to obtain a string of nearly uniform random bits. Let $H_{\infty}^{\epsilon}(\mathbf{C}|\mathbf{Z}\mathbf{E}, \Phi)$ denote the smooth conditional min-entropy for the state of $\mathbf{CZ}\mathbf{E}$ conditional on the event Φ defined as a set of values \mathbf{cz} of \mathbf{CZ} . The result is formalized as follows:

Theorem. *Suppose that F is a QEF with power β for a model, and $\rho_{\mathbf{CZ}\mathbf{E}}$ is a state in the model. Fix $1 \geq p > 0$ and $\epsilon > 0$, and define the event $\Phi \doteq \{\mathbf{cz} : F(\mathbf{cz}) \geq 1/(p^{\beta}(\epsilon^2/2))\}$. Let $\kappa \leq \sum_{\mathbf{cz} \in \Phi} \text{tr}(\rho(\mathbf{cz}))$, the probability of the event Φ . Then $H_{\infty}^{\epsilon}(\mathbf{C}|\mathbf{Z}\mathbf{E}, \Phi) \geq -\log_2(p) + \frac{\alpha}{\beta} \log_2(\kappa)$.*

The probability of the event Φ can be interpreted as the probability that the experiment succeeds, and κ is an assumed lower bound on the success probability. When constructing QEFs, the power $\beta > 0$ must be decided before the experiment and cannot be adapted. The QEFs for a sequence of trials can be constructed by multiplying the QEFs for individual trials. If \mathbf{CZ} is generated by a sequence of identical trials and F is obtained by multiplying identical trial-wise QEFs F_0 , then we can define a rate h by $h \doteq -\log(p)/n$. The event Φ can alternatively be expressed as $\Phi = \{\mathbf{cz} : \sum_i \log(F_0(c_i z_i))/\beta \geq nh - 2 \log(\epsilon/\sqrt{2})/\beta\}$. This identifies h as the targeted conditional min-entropy rate, and we can interpret $\log(F_0(c_i z_i))/\beta$ as the trial-wise contributions to the final conditional min-entropy. We define $g(\beta) = \sup_{F_0} \mathbb{E}_{\nu}(\log_2(F_0(CZ))/\beta)$, where \mathbb{E}_{ν} is the expectation functional according to the distribution ν of trial results.

For finite data and applications requiring fresh blocks of randomness, we consider the problem of certifying a fixed number of bits b of randomness at error bound ϵ and with as few trials as possible, where the distribution of each trial results is the same ν . For randomness beacons, good reference values are $b = 512$ and $\epsilon = 2^{-64}$. In view of the above theorem, n needs to be sufficiently large so that

$$ng(\beta) + 2 \log(\epsilon/\sqrt{2})/\beta + \alpha \log_2(\kappa)/\beta \geq b.$$

Thus, the minimum number of trials required to certify b bits of ϵ -smooth conditional min-entropy is

$$n_{\text{QPE},b} = \inf_{\beta} \frac{b\beta - 2 \log_2(\epsilon/\sqrt{2}) - \alpha \log_2(\kappa)}{\beta g(\beta)}.$$

Applications. We consider DIRG with the standard two-party, two-setting, two-outcome Bell-test configuration [27]. The parties are labeled \mathbf{A} and \mathbf{B} . In each trial, each party chooses a random setting (their input) and obtains a measurement outcome

(their output). We write $Z = XY$, where X and Y are the inputs of A and B , and $C = AB$, where A and B are the respective outputs. For this configuration, $A, B, X, Y \in \{0, 1\}$. We assume that at each trial the input distribution is uniform.

We compare $n_{\text{QPE},b}$ with the minimum number of trials, $n_{\text{EAT},b}$, required by the entropy accumulation protocol ‘‘EAT’’ of Ref. [17]. For this purpose, we consider three different families of quantum-achievable trial distributions. For the first family $\nu_{E,\theta}$, A and B share the unbalanced Bell state $|\Psi_\theta\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle$ with $\theta \in (0, \pi/4]$ and apply setting-dependent projective measurements that maximize the violation, \hat{I} , of the CHSH inequality [27]. This determines $\nu_{E,\theta}$. For the second family $\nu_{W,p}$, A and B share a Werner state $\rho = p|\Psi_{\pi/4}\rangle\langle\Psi_{\pi/4}| + (1-p)\mathbb{1}/4$ with $p \in (1/\sqrt{2}, 1]$ and again apply measurements that maximize \hat{I} . In experiments with photons, measurements are implemented with imperfect efficiency detectors. For the third family $\nu_{P,\eta}$, A and B use detectors with efficiency $\eta \in (2/3, 1)$ to implement the measurements and to close the detection loophole [28]. They choose the unbalanced Bell state $|\Psi_\theta\rangle$ and measurements such that the statistical strength for rejecting local realism is maximized, as studied in Refs. [29, 30].

We compare the two protocols over a broad range of \hat{I} for $b \searrow 0$, $\epsilon = 10^{-6}$, and $\kappa = 1$. For each family of distributions above, we compute the improvement factor given by $f_{\text{QPE}} = n_{\text{EAT},0}/n_{\text{QPE},0}$. For $\nu_{W,p}$, the improvement factors depend weakly on \hat{I} : f_{QPE} increases from 41.2 at $\hat{I} = 2.008$ to 42.1 at $\hat{I} = 2\sqrt{2}$. For $\nu_{E,\theta}$ and $\nu_{P,\eta}$, the improvement factors can be much larger and depend strongly on \hat{I} , monotonically decreasing with \hat{I} as shown in Fig. 1. The improvement is particularly notable at small violations which are typical in current photonic loophole-free Bell tests. We remark that similar comparison results were obtained with other choices of the values for b , ϵ and κ .

Finally, we discuss the performance of QPE on published Bell-test experimental data. The first experimental demonstration of conditional min-entropy certification for DIRG is reported in Ref. [10]. The method therein certifies the presence of 42 random bits at $\epsilon = 0.01$ against classical side information, where the trial model \mathcal{Q} consists of quantum achievable distributions with uniform inputs. ($\kappa = 1$ was used implicitly in Ref. [10], so $\kappa = 1$ in the following comparison.) For the same data and the same trial model, QPE certifies the presence of 128 random bits at $\epsilon = 0.01$ against

quantum side information, while EAT requires 54688 trials, more than the number of 3016 trials available in Ref. [10], before certifying any number of random bits at $\epsilon = 0.01$. For the loophole-free Bell-test ex-

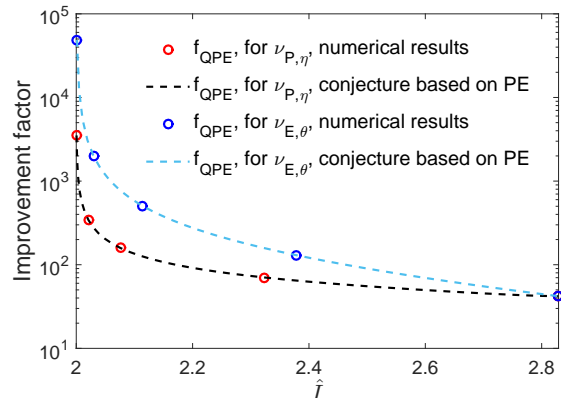


FIG. 1: Improvement factor as a function of \hat{I} . Numerical results are shown as circles. We observed that the probability estimation factors constructed in Ref. [21] are QEFs. The dashed curves show the conjectured behavior based on this observation.

	Original Result	New Result with QPE
Ref. [10]	42 bits	128 bits
Ref. [19]	1033 bits	2078 bits

TABLE I: Reanalysis of previous experiments with error bound $\epsilon = 0.01$. The original results in Refs. [10, 19] are with respect to classical side information, while the results by QPE are with respect to quantum side information. We remark that no randomness can be certified from either experiment by entropy accumulation [17]. See the text for more details.

periment reported in Ref. [9] and analyzed in our previous work Ref. [19], the presence of 1033 random bits at $\epsilon = 0.01$ can be certified against classical side information, where the trial model \mathcal{N} consists of non-signaling distributions with uniform inputs. (The work of Ref. [19] is more than the certification of the presence of randomness, but actually extracted 256 private random bits within total-variation distance of 0.001 from uniform.) With QPE and assuming the trial model \mathcal{Q} , we can certify the presence of 2078 random bits at $\epsilon = 0.01$ against quantum side information, while EAT requires 2.33×10^{12} trials, more than the number of 1.82×10^8 trials available in Ref. [9], before certifying any number of random bits at $\epsilon = 0.01$.

[1] Christof Paar and Jan Pelzl. *Understanding Cryptography*. Springer-Verlag Berlin Heidelberg, New

York, 2010.

- [2] M. J. Fischer. A public randomness service. In *SECRYPT 2011*, pages 434–438, 2011.
- [3] S. Pironio and S. Massar. Security of practical private randomness generation. *Phys. Rev. A*, 87:012336, Jan 2013.
- [4] R. Colbeck. *Quantum and Relativistic Protocols for Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2007.
- [5] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *J. Phys. A: Math. Theor.*, 44(9):095305, 2011.
- [6] B. Hensen et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 km. *Nature*, 526:682, 2015.
- [7] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter. Event-ready Bell-test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.*, 119:010402, 2017.
- [8] M. Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of Bell’s theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.
- [9] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, Dec 2015.
- [10] S. Pironio, A. Acin, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe. Random numbers certified by Bell’s theorem. *Nature*, 464:1021–4, 2010.
- [11] U. Vazirani and T. Vidick. Certifiable quantum dice - or, exponential randomness expansion. In *STOC’12 Proceedings of the 44th Annual ACM Symposium on Theory of Computing*, page 61, 2012.
- [12] S. Fehr, R. Gelles, and C. Schaffner. Security and composability of randomness expansion from Bell inequalities. *Phys. Rev. A*, 87:012335, Jan 2013.
- [13] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *J. ACM*, 63:33, 2016.
- [14] C. A. Miller and Y. Shi. Universal security for randomness expansion from the spot-checking protocol. *SIAM J. Comput.*, 46:1304–1335, 2017.
- [15] K.-M. Chung, Y. Shi, and X. Wu. Physical randomness extractors: Generating random numbers with minimal assumptions. arXiv:1402.4797 [quant-ph], 2014.
- [16] M. Coudron and H. Yuen. Infinite randomness expansion with a constant number of devices. In *STOC’14 Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 427–36, 2014.
- [17] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick. Practical device-independent quantum cryptography via entropy accumulation. *Nat. Commun.*, 9:459, 2018.
- [18] O. Nieto-Silleras, C. Bamps, J. Silman, and S. Pironio. Device-independent randomness generation from several Bell estimators. arXiv:1611.00352, 2016.
- [19] P. Bierhorst, E. Knill, S. Glancy, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, and L. K. Shalm. Experimentally generated random numbers certified by the impossibility of superluminal signaling. arXiv:1702.05178, 2017.
- [20] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm. Experimentally generated random numbers certified by the impossibility of superluminal signaling. *Nature*, 556:223–226, 2018.
- [21] E. Knill, Y. Zhang, and P. Bierhorst. Quantum randomness generation by probability estimation with classical side information. arXiv:1709.06159, 2017.
- [22] S. Popescu and D. Rohrlich. Quantum nonlocality as an axiom. *Found. Phys.*, 24(3):379–85, 1994.
- [23] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts. Nonlocal correlations as an information-theoretic resource. *Phys. Rev. A*, 71:022101, Feb 2005.
- [24] Tommaso Lunghi, Jonatan Bohr Brask, Charles Ci Wen Lim, Quentin Lavigne, Joseph Bowles, Anthony Martin, Hugo Zbinden, and Nicolas Brunner. Self-testing quantum random number generator. *Phys. Rev. Lett.*, 114:150501, Apr 2015.
- [25] Thomas Van Himbeeck, Erik Woodhead, Nicolas J. Cerf, Raúl García-Patrón, and Stefano Pironio. Semi-device-independent framework based on natural physical assumptions. *Quantum*, 1:33, 2017.
- [26] Emanuel Knill, Yanbao Zhang, and Honghao Fu. Quantum probability estimation for randomness with quantum side information. Available by request and to appear on the arXiv soon.
- [27] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.
- [28] P. H. Eberhard. Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment. *Phys. Rev. A*, 47:R747–R750, 1993.
- [29] W. van Dam, R. D. Gill, and P. D. Grunwald. The statistical strength of nonlocality proofs. *IEEE Trans. Inf. Theory.*, 51:2812–2835, 2005.
- [30] Yanbao Zhang, Emanuel Knill, and Scott Glancy. Statistical strength of experiments to reject local realism with photon pairs and inefficient detectors. *Phys. Rev. A*, 81:032117, Mar 2010.