Maximizing device-independent randomness from a Bell experiment by optimizing the measurement settings

S. M. Assad,* O. Thearle, and P. K. Lam

Centre for Quantum Computation and Communication Technology, Department of Quantum Science, Research School of Physics and Engineering, The Australian National University, Canberra ACT 2601, Australia

(Received 1 March 2016; published 5 July 2016)

The rates at which a user can generate device-independent quantum random numbers from a Bell-type experiment depend on the measurements that the user performs. By numerically optimizing over these measurements, we present lower bounds on the randomness generation rates for a family of two-qubit states composed from a mixture of partially entangled states and the completely mixed state. We also report on the randomness generation rates from a tomographic measurement. Interestingly in this case, the randomness generation rates are not monotonic functions of entanglement.

DOI: 10.1103/PhysRevA.94.012304

I. INTRODUCTION

Quantum mechanics is a probabilistic theory. It does not assign definite outcomes to certain measurements. A physicist performing identical measurements on two identically prepared systems might get different measurement outcomes. Quantum mechanics postulates that the outcomes of some measurements are undetermined before the measurement. This randomness in the measurement outcomes has been used to generate random numbers.

It might be argued that the randomness in the measurement outcome is not really undetermined before the measurement. It is perhaps determined by some hidden variables that provide a more complete description of the system, but they are unknown to the physicist. However, this hidden-variable description of nature was recently tested in three Bell test experiments and was found to be incompatible with the observed experimental data [1–3]. The observed data were consistent with quantum mechanics. In other words, we see in our experiments that nature behaves randomly, as postulated by quantum mechanics. This implies that if the experimental observations obey some relations and on the condition that the experiment was performed correctly, we can certify the measurement outcomes were undetermined before the measurement was performed. That is, their outcomes generated new random numbers.

The conditions that need to be satisfied are those for a loophole-free Bell experiment. Remarkably, these conditions do not include that the physicist know the mechanisms of the measuring device. This observation makes the realization of a device-independent (DI) quantum random-number generator (QRNG) possible. In a DIQRNG, the user is able to certify the creation of new random numbers despite being ignorant of the device mechanisms.

In certifying the generation of new random numbers, the user trusts that quantum mechanics provides a complete description of nature. Based on the statistics of the measurement outcomes, the user can put a bound on the number of correlations between his or her measurement outcomes and any other system that exists outside of his or her lab [4]. This bound allows the user to extract new random numbers from the measurement outcomes, that is, random numbers which are not correlated to any system outside of his or her laboratory.

The first proof-of-concept DIQRNG used entangled photons generated in an atomic ion trap to certify 42 new random numbers over a period of about one month [5]. More recently, using a more efficient entanglement source, 4350 bits of new randomness were created at a rate of 0.4 bits/s [6]. Both setups used the Clauser-Horne-Shimony-Holt (CHSH) value [7] to certify the randomness. The CHSH value is a function of the measurement statistics, and this value sets a lower bound on the DI randomness that can be certified. It turns out that using different Bell operators, that is, different functions of the measurement statistics, will give different equally valid lower bounds to the DI randomness from the same measurement statistics. In [8], several previously known as well as 25 000 randomly generated Bell operators were tested and shown to certify varying amount of randomness from the two-qubit Werner state. These operators were chosen in an *ad hoc* manner, and no single operator was found to be optimal for all the Werner states.

In [9,10], the complete measurement statistics were used to obtain a bound on the DI randomness instead of resorting to a specific Bell operator. This gives the highest lower bound on the DI randomness. A by-product of this process is the optimal Bell operator that would have given the same bound. This Bell operator gives the maximum DI randomness for the given measurement statistics.

In a Bell setup for generating new random numbers, the physicist has a choice of the measurement operators to use. By optimizing these operators, the physicist can get a better bound on the DI randomness. This is the question that we address: How much randomness can the physicist certify by using the optimal measurement operator? Recently, this question was also addressed in [11] for an experimentally relevant optical Bell experiment setup and in [12], where the requirement for full device independence was relaxed.

II. BACKGROUND

We consider the usual Bell setup for generating DI random numbers. The user inputs two random and independent measurement settings, $x \in \{1,\ldots,M_x\}$ and $y \in \{1,\ldots,M_y\}$, and receives two measurement outcomes, $a,b \in \{-1,1\}$. In a DI setup, the user does not have any knowledge of the

*cqtsma@gmail.com

measurement device. The behavior of the apparatus is solely characterized by the conditional probabilities $p(a,b|x,y)$, which we view as the components of the vector $\mathbf{p}$. The user will use one measurement setting, (x^*,y^*), to generate the random numbers; the other settings are only used to obtain bounds on the DI randomness.

Following [9,10], the maximum guessing probability for an adversary, Eve, who is constrained by quantum mechanics and has perfect knowledge of the measurement apparatus is

$$G[\mathbf{p}] = \max_{\{q_{ab},\mathbf{p}_{ab}\}} \sum_{ab} q_{ab} p_{ab}(a,b|x^*,y^*), \tag{1}$$

such that

$$\sum_{ab} q_{ab}\mathbf{p}_{ab} = \mathbf{p} \tag{2}$$

and

$$\mathbf{p}_{ab} \in \mathcal{Q}\,. \tag{3}$$

The notation $\mathbf{p} \in \mathcal{Q}$ means that the conditional probabilities $\mathbf{p}$ can be realized in quantum mechanics. In other words, there exist a state ρ and some measurement operators π_x^a and π_y^b such that $p(a,b|x,y) = \mathrm{Tr}\{\rho\,\pi_x^a \otimes \pi_y^b\}$. The constraint (2) ensures that the weighted sum of the particular behaviors $\mathbf{p}_{ab}$ gives the observed behavior $\mathbf{p}$. Eve can realize the guessing probability $G[\mathbf{p}]$ if the measurement device behaves according to $\mathbf{p}_{ab}$ with probability q_{ab} and Eve knows the particular behavior of each measurement. For each instant of a particular behavior $\mathbf{p}_{ab}$, Eve's guess of the measurement outcome will be (a,b). If the maximum guessing probability is less than 1, then the lower bound to the amount of certifiable DI randomness is quantified by the minimum entropy $H_{\min} = -\log_2 G$.

The optimization problem (1) is a conic linear program, and its dual can be formulated as

$$D[\mathbf{p}] = \min_{\mathbf{f}} \mathbf{f}\cdot\mathbf{p}, \tag{4}$$

such that

$$p'(a,b|x^*,y^*) \leqslant \mathbf{f}\cdot\mathbf{p}' \quad \text{for } a,b \in \{-1,1\},$$

and all

$$\mathbf{p}' \in \mathcal{Q}. \tag{5}$$

The solution of the dual program coincides with the solution of the primal program: $D[\mathbf{p}] = G[\mathbf{p}]$. The optimization variable vector $\mathbf{f}$ corresponds to a Bell expression that gives rise to a guessing probability of $\mathbf{f}\cdot\mathbf{p}$. The optimal $\mathbf{f}$ that achieves the minimum then corresponds to the optimal Bell expression that minimizes Eve's guessing probability given the behavior $\mathbf{p}$.

In general, the optimization problems (1) and (4) can be computationally hard to solve. However, the constraints (2) and (5) can be relaxed [13,14] to give upper bounds to the guessing probabilities in a way that the programs can be cast as a semidefinite program (SDP) which can be solved efficiently. These relaxations can be progressively tightened to give bounds that are successively tighter.

III. RANDOMNESS MAXIMIZATION

While the user of a DIRNG has no access to the workings of the device, the physicist who builds the device has a choice of the quantum state ρ and the measurement operators $\boldsymbol{\pi}$ that he or she wants to implement in the operation of the device. The vector $\boldsymbol{\pi}$ has components $\pi(a,b,x,y) = \pi_x^a \otimes \pi_y^b$ which are rank-one projectors and satisfy

$$\begin{aligned} \mathrm{Tr}\{\pi_x^a\,\pi_x^{a'}\} &= \delta_{aa'} \quad \text{for } x \in \{1,\ldots,M_x\},\\ \mathrm{Tr}\{\pi_y^b\,\pi_y^{b'}\} &= \delta_{bb'} \quad \text{for } y \in \{1,\ldots,M_y\}. \end{aligned} \tag{6}$$

For example, if the physicist's machine can prepare the pure entangled two-qubit state $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, then as shown in [15], by designing the measurement operators to be projectors along $(|0\rangle\cos\alpha_x^a/2 + |1\rangle\sin\alpha_x^a/2) \otimes (|0\rangle\cos\beta_y^b/2 + |1\rangle\sin\beta_y^b/2)$ with the angles

$$\begin{aligned} &\alpha_1^{\pm1} = (0,\pi), \quad \alpha_2^{\pm1} = \left(\frac{\pi}{2}, -\frac{\pi}{2}\right), \quad \beta_1^{\pm1} = \left(\frac{\pi}{4}, -\frac{3\pi}{4}\right),\\ &\beta_2^{\pm1} = \left(\frac{3\pi}{4}, -\frac{\pi}{4}\right), \quad \beta_3^{\pm1} = (0,\pi), \end{aligned} \tag{7}$$

the device will be able to certify two bits of randomness with the measurement settings (2,3). However, if the measurement operators used were not optimal, the machine will exhibit a different behavior and may certify less randomness.

So if the builder can prepare a maximally entangled two-qubit state and use the optimal measurement operator, then the device will be able to certify two bits of randomness, and all is good. However, if the builder is technologically limited to preparing some other state ρ, then in general the measurement operators in (7) will not be optimal anymore. In this case, the builder is then interested in finding the measurement operator he or she should implement that would certify the maximum randomness given that he or she is restricted to the state ρ [16]. This is the task that we shall now investigate. More precisely, we want to find

$$H[\rho] = \max_{\boldsymbol{\pi}} D[p(\boldsymbol{\pi})], \tag{8}$$

where $p(\boldsymbol{\pi}) = \mathrm{Tr}\{\rho\,\boldsymbol{\pi}\}$ and the vector $\boldsymbol{\pi}$ is constrained by (6). Admittedly, we have not solved this problem. Instead, we present and implement an iterative algorithm in Algorithm 1 that converges to a local maximum of $D[p(\boldsymbol{\pi})]$.

Algorithm 1 Proposed algorithm.

Input: input states ρ, initial positive operator-valued measure (POVM) $\boldsymbol{\pi}_0$, and stopping criteria ϵ
1: Initialize guessing probability $g_1 = 1$ and POVM $\boldsymbol{\pi}_1 = \boldsymbol{\pi}_0$
2: **repeat**
3: Update $\boldsymbol{\pi}_0 = \boldsymbol{\pi}_1$ and $g_0 = g_1$
4: Compute $\mathbf{p} = p(\boldsymbol{\pi}_0)$
5: Compute $D[\mathbf{p}]$ and corresponding $\mathbf{f}$ by solving the relaxed version of (4)
6: Compute the minimum of $g_1(\boldsymbol{\pi}) = \mathbf{f}\cdot p(\boldsymbol{\pi}_1)$ and corresponding $\boldsymbol{\pi}_1$
7: **until** $g_0 - g_1 \leqslant \epsilon$
Output: $\boldsymbol{\pi}_1$

The tolerance ϵ sets the stopping condition for the algorithm. In step 6, we compute the minimum of guessing

probability $\mathbf{f}\cdot p(\boldsymbol{\pi})$ which corresponds to finding the measurement settings that maximizes the Bell value for a given Bell expression $\mathbf{f}$. The guessing probability $\mathbf{f}\cdot p(\boldsymbol{\pi}) = \mathrm{Tr}\{\rho\,\mathbf{f}\cdot\boldsymbol{\pi}\}$ is a quadratic function of π_x^a and π_y^b with the quadratic constraints (6). We can use the Lagrange multiplier method to find the minimum.

While the algorithm might not find the global maximum $H[\rho]$, it usually finds measurement settings that yield more DI randomness than a randomly chosen measurement setting. In our implementation, we use several initial settings $\boldsymbol{\pi}_0$ in an attempt to find the global maximum. All SDP calculations were performed using the CVX package for MATLAB [17,18].

IV. RESULTS

We apply our algorithm to the family of states

$$\rho(v,\theta) = v|\Psi_\theta\rangle\langle\Psi_\theta| + (1-v)\tfrac{1}{4}, \tag{9}$$

where $|\Psi_\theta\rangle = |00\rangle\cos\theta + |11\rangle\sin\theta$ and visibility $0 \leqslant v \leqslant 1$ gives the fraction of the state $|\Psi_\theta\rangle$. In the noiseless limit of $v = 1$, arbitrarily close to two bits of DI randomness can be attained in the maximally entangled case when $\theta = \pi/4$ with $M_x = M_y = 2$ measurement settings [19]. Two bits of DI randomness are also achievable when θ is arbitrarily close to zero with $M_x = M_y = 4$ measurement settings [19].

We first consider the case where $M_x = M_y = 2$ and the visibility is fixed at $v = 0.99$. In Fig. 1, we compare the DI randomness from the optimized measurement setting to a bound obtained using a fixed measurement setting as reported in [9]. We see a significant improvement in the certifiable randomness using the optimized measurement settings. For

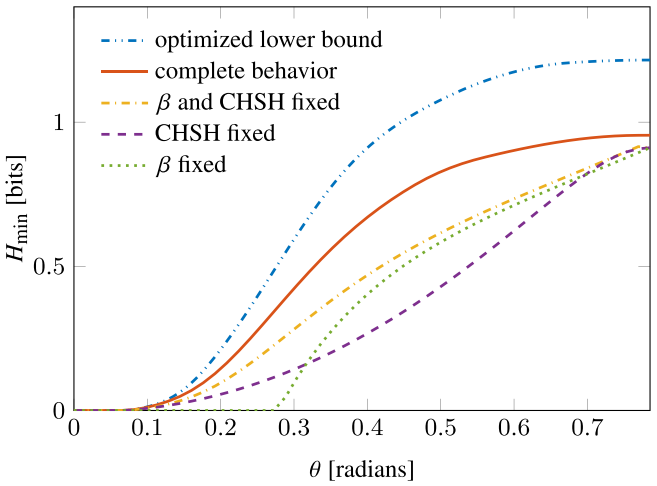

FIG. 1. Comparison of lower bounds on DI randomness for $v = 0.99$. The green dotted and purple dashed lines show the DI randomness obtained when constrained by the Bell operators (11) and (10) with a fixed measurement direction [9]. Using both operators together gives a higher randomness, depicted by the yellow dash-dotted line. Constraining Eve to the complete behavior gives the most randomness from the fixed behavior generated from the measurement direction depicted by the solid orange line [9]. The top line denotes the randomness bound for an optimized measurement direction. These curves were obtained with a third-order relaxation of the SDP hierarchy [13,14].

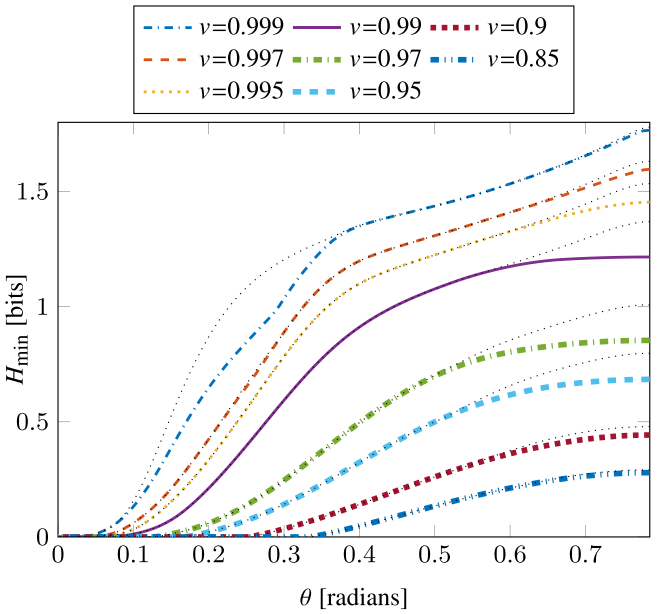

FIG. 2. Optimized lower bounds on DI randomness for various visibilities with two measurement settings for each side. The black dots have four measurement settings for each side. These curves were obtained with a second-order relaxation of the SDP hierarchy.

completeness, we also include the certifiable randomness constrained using two specific Bell operators,

$$I_{\mathrm{CHSH}} = \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle, \tag{10}$$

$$I^\beta = I_{\mathrm{CHSH}} + \beta\langle A_1\rangle, \tag{11}$$

and also constrained by both operators together [9] using a fixed measurement setting where $\beta = 2\cos 2\theta/\sqrt{1+\sin^2 2\theta}$, $\langle A_xB_y\rangle = \sum_{ab} ab\,p(a,b|x,y)$, and $\langle A_x\rangle = \sum_a a\,p(a|x)$. The DI randomness bounds using specific operators are always lower than using the complete measurement statistics.

Next, we plot the DI randomness bound as a function of θ for various visibilities in Fig. 2 for $M_x = M_y = 2$. We also plotted the DI randomness when $M_x = M_y = 4$ in the same figure. In most cases, the improvement obtained from using four measurement settings is not very significant. In Fig. 3, we plot the DI randomness as a function of nonlocality as measured by the CHSH value I_{CHSH}. Relying on the CHSH value alone gives a much lower DI randomness, especially when the state has a high visibility. Even with a maximally entangled two-qubit state, a CHSH value of $2\sqrt{2}$ can only certify 1.22845 bits of randomness.

In Fig. 4, we fix the input state to have $\theta = \pi/4$ and plot the DI randomness as a function of visibility for $M_x = M_y = 2$ and $M_x = M_y = 4$. There is only a slight increase in the DI randomness bound when going to four measurement settings. The DI randomness increases monotonically with v as one would expect. This is because from a high-visibility state, one can always introduce noise to get to a state with lower visibility and attain at least the same DI randomness.

Finally, in the limit when the number of settings becomes large, the DI randomness will be upper bounded by the setup

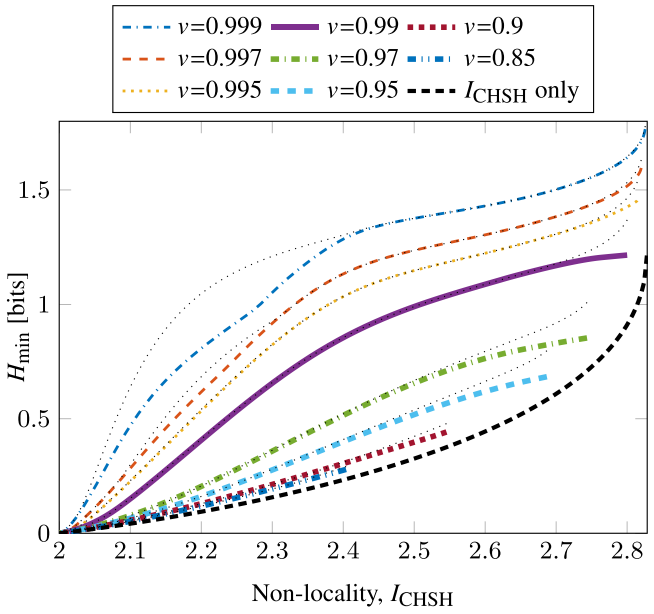

FIG. 3. Optimized lower bounds on DI randomness as a function of nonlocality, with a different amount of randomness from the same amount of CHSH violation with two measurement settings for each side. Black dots have four measurement settings for each side. The lowest dashed line shows the DI randomness bound obtained from using the CHSH value alone. These curves were obtained with a second-order relaxation of the SDP hierarchy.

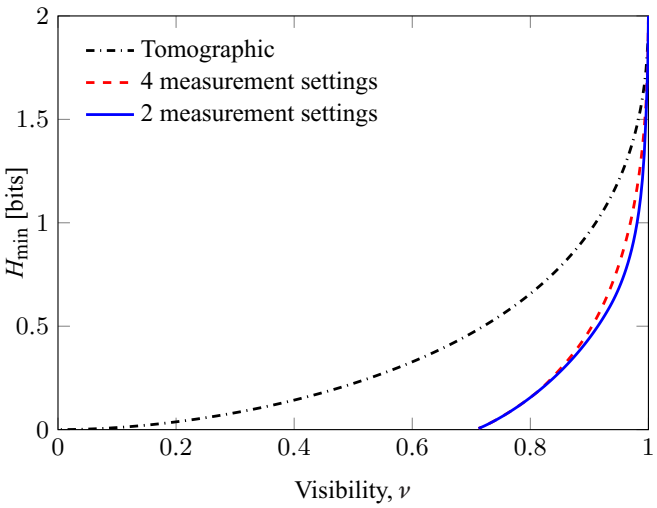

FIG. 4. Optimized lower bounds on DI randomness as a function of visibility from a mixture of a maximally entangled state and white noise. The DI randomness goes to zero when $v < 1/\sqrt{2}$ for two (solid line) and four (dashed line) measurement settings on each side. The four-measurement-setting randomness bound that we report here is slightly higher than the results reported in [20], where there are two fixed settings for one side and four fixed settings for the other side. We computed the fixed settings using both the second- and third-level relaxations of the SDP hierarchy, but they might turn out to be identical when a tighter constraint is used. We find no improvement in the tomographic result (dash-dotted line) compared to the results using a fixed measurement setting reported in [20]. The two-setting and four-setting curves were obtained using a second-order relaxation of the SDP hierarchy.

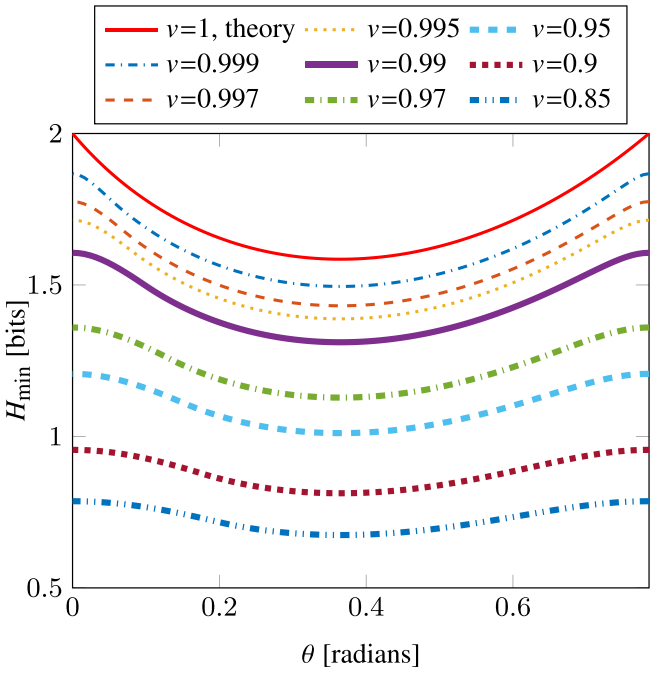

FIG. 5. Optimized randomness with complete tomography. With complete tomography, the randomness generation rate is not zero even when the two-qubit state is separable at $\theta = 0$. For a fixed visibility, the randomness rate is not a monotonic function of θ. It is maximum when $\theta = 0$ and $\theta = \pi/4$.

where the user can perform a complete tomography [20]. In this case, the constraint (2) is replaced by a constraint on the quantum states ρ_{ab} with $\sum_{ab} q_{ab}\rho_{ab} = \rho$. The constraints that ρ_{ab} is positive mean that programs (1) and (4) are already SDPs. We plot the tomographic randomness rate in Fig. 5. For a fixed θ, the tomographic randomness rates decrease with v. However, the tomographic randomness rates are not monotonic in θ for a fixed v. For the same v, starting with a state with small entanglement (low θ) can still yield the same amount of randomness as a state with large entanglement (θ near $\pi/4$). The dip in the randomness rates when $\theta = \pi/8$ is unlikely due to the algorithm being stuck in a local maximum. We check this numerically by scanning the whole parameter space. For the case of a qubit pair input that we are considering, the measurement directions that the user uses to generate the tomographic randomness can be parametrized by the Bloch vector angles α_1 and β_1. Some typical tomographic randomness rates are shown in Fig. 6 as a function of the two Bloch vectors.

In Fig. 4, we plot the randomness from a tomographic measurement when $\theta = \pi/4$ as a function of v. We find no improvement compared to the results reported in [20]. The measurement used there,

$$\alpha_1^{\pm 1} = (0,\pi), \quad \beta_1^{\pm 1} = \left(\frac{\pi}{2}, -\frac{\pi}{2}\right), \tag{12}$$

indeed attains the maximum randomness we found.

When the visibility is exactly unity, the quantum state that the user has is a pure state. For this, Eve's guessing probability can be calculated exactly and then maximized over the user's

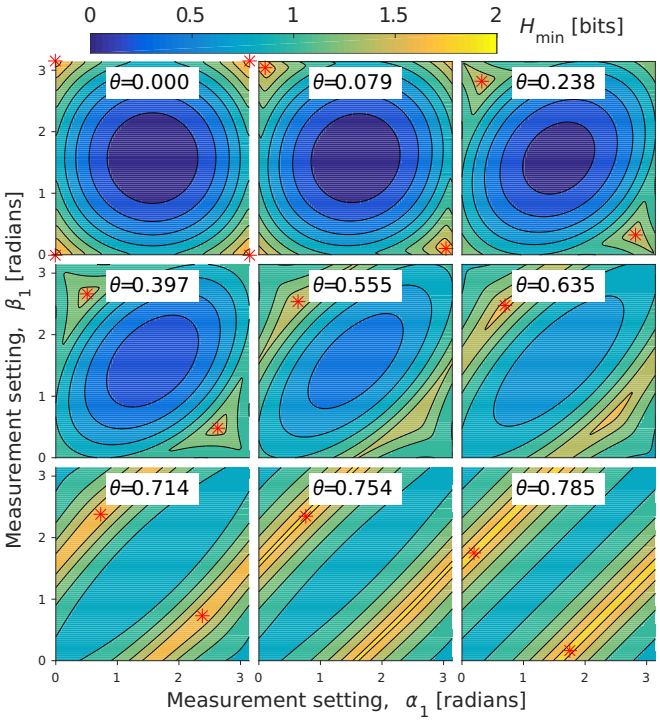

FIG. 6. Randomness with complete tomography as a function of measurement angles. $H_{\min}$ as a function of the measurement settings for different input states parametrized by θ from 0 to $\pi/4$ with $v = 0.999$. The x axis corresponds to the angle α_1 of the Bloch vector $(\sin\alpha_1, 0, \cos\alpha_1)$ of the measurement setting for the first side, and the y axis corresponds to the angle β_1 of the Bloch vector $(\sin\beta_1, 0, \cos\beta_1)$ of the measurement setting for the second side. The red asterisk denotes the maximum $H_{\min}$ value for each θ.

measurements. The final result is

$$G = \tfrac{1}{4}(1 + \sin 2\theta)\cos^2\alpha, \tag{13}$$

where α characterizes the measurement direction and is given by solving

$$\sin\alpha = \frac{-\cos 2\theta + \sqrt{\cos^2 2\theta + 4\sin 2\theta(1+\sin 2\theta)}}{2(1+\sin 2\theta)}. \tag{14}$$

The min-entropy from this guessing probability is plotted as the top line in Fig. 5. We see that two bits of randomness are achievable only when the state is maximally entangled or when it is separable.

V. CONCLUSIONS

The amount of randomness generated from a DIQRNG can be improved by optimizing the measurement setting. However, for the two-qubit state considered, the additional improvement achieved by using four measurement settings on each side is, in most cases, not significant. There is a disadvantage in having more measurement settings: the experimental setup is more complicated, and more data are needed to characterize the measurements. This is not justified by the minimal increase in the randomness generation rates.

ACKNOWLEDGMENTS

We acknowledge the support of the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Project No. CE110001027).

[1] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature (London) **526**, 682 (2015).

[2] L. K. Shalm *et al.*, Strong Loophole-Free Test of Local Realism, Phys. Rev. Lett. **115**, 250402 (2015).

[3] M. Giustina *et al.*, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Phys. Rev. Lett. **115**, 250401 (2015).

[4] We assume that the laboratory is secure.

[5] 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 *et al.*, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[6] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam *et al.*, Detection-Loophole-Free Test of Quantum Nonlocality, and Applications, Phys. Rev. Lett. **111**, 130406 (2013).

[7] 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 (1969).

[8] P. Mironowicz and M. Pawlowski, Robustness of quantum-randomness expansion protocols in the presence of noise, Phys. Rev. A **88**, 032319 (2013).

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

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

[11] A. Mattar, P. Skrzypczyk, J. B. Brask, D. Cavalcanti, and A. Acin, Optimal randomness generation from optical Bell experiments, New J. Phys. **17**, 022003 (2015).

[12] E. Passaro, D. Cavalcanti, P. Skrzypczyk, and A. Acín, Optimal randomness certification in the quantum steering and prepare-and-measure scenarios, New J. Phys. **17**, 113010 (2015).

[13] M. Navascués, S. Pironio, and A. Acín, Bounding the Set of Quantum Correlations, Phys. Rev. Lett. **98**, 010401 (2007).

[14] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, New J. Phys. **10**, 073013 (2008).

[15] C. Dhara, G. Prettico, and A. Acín, Maximal quantum randomness in Bell tests, Phys. Rev. A **88**, 052116 (2013).

[16] If some outcome symbols (a,b) given (x^*,y^*) are more unpredictable than others, then more randomness can potentially

be extracted by postselecting a subset of the symbols (a,b). Although the postselection reduces the number of data points available for randomness extraction, the postselected data might be more random, which makes it harder for Eve to guess correctly. The net result can be an increase in the final randomness generation rate [21].

[17] M. Grant and S. Boyd, Graph implementations for nonsmooth convex programs, in *Recent Advances in Learning and Control*, edited by V. Blondel, S. Boyd, and H. Kimura, Lecture Notes in Control and Information Sciences (Springer-Verlag, London, 2008), pp. 95–110.

[18] M. Grant and S. Boyd, CVX: MATLAB software for disciplined convex programming, version 2.1, http://cvxr.com/cvx.

[19] A. Acín, S. Massar, and S. Pironio, Randomness Versus Nonlocality and Entanglement, Phys. Rev. Lett. **108**, 100402 (2012).

[20] Y. Z. Law, L. P. Thinh, J.-D. Bancal, and V. Scarani, Quantum randomness extraction for various levels of characterization of the devices, J. Phys. A **47**, 424028 (2014).

[21] L. P. Thinh, G. de la Torre, J.-D. Bancal, S. Pironio, and V. Scarani, Randomness in post-selected events, New J. Phys. **18**, 035007 (2016).