Bounds on semi-device-independent quantum random-number expansion capabilities

Vaisakh Mannalath [*] and Anirban Pathak [†]
Jaypee Institute of Information Technology, A-10, Sector 62, Noida UP 201309, India

(Received 2 December 2021; accepted 4 February 2022; published 23 February 2022)

The randomness expansion capabilities of semi-device-independent (SDI) prepare and measure protocols are analyzed under the sole assumption that the Hilbert state dimension is known. It is explicitly proved that the maximum certifiable entropy that can be obtained through this set of protocols is $-\log_2[\frac{1}{2}(1+\frac{1}{\sqrt{3}})]$ and the same is independent of the dimension witnesses used to certify the protocol. The minimum number of preparation and measurement settings required to achieve this entropy is also proven. An SDI protocol that generates the maximum output entropy with the least amount of input setting is provided. An analytical relationship between the entropy generated and the witness value is obtained. It is also established that certifiable entropy can be generated as soon as the dimension witness crosses the classical bound, making the protocol noise-robust and useful in practical applications.

DOI: 10.1103/PhysRevA.105.022435

I. INTRODUCTION

Randomness plays an important role in simulation algorithms [1–3], cryptography [4–6], fundamental sciences [7–9], and much research has been devoted to the generation of random numbers [10]. Deterministic algorithms can at best create "pseudorandom numbers" that mimic the statistics of "true" random numbers [11]. One needs access to unpredictable physical processes in order to generate truly random numbers [10,12]. Quantum theory provides well-defined theoretical models which are inherently probabilistic and serve us with good entropy sources to extract randomness [13]. Generating randomness from quantum systems is a matured field [14]. There are now even commercially available quantum random-number generators (QRNGs) [15–17]. These devices are based on methods that are only applicable to their specific experimental setup and corresponding entropy estimates of the output randomness depend on a number of assumptions. Ultimately, these devices require a level of trust in the manufacturer which is not ideal for a number of reasons [10].

For the above-mentioned reasons, it is highly advantageous to have a setup that provides certifiable entropy while making minimal assumptions about its working. Device-independent QRNGs (DI-QRNGs) [18,19] provide a solution to this problem. By consuming input randomness and using nonlocality of quantum theory it can, theoretically, certify the output randomness without characterizing the inner workings of the setup. There has also been numerous experimental demonstrations of this approach [20–23]. However, protocols for DI-QRNG suffer from practical issues which make them hard to implement outside of a laboratory setup compared to one-way protocols commonly used in commercial devices.

A more practical approach to random-number generation is provided by the so-called semi-device-independent QRNGs (SDI-QRNGs) [24–29]. Unlike DI-QRNG, complete knowledge of a part of the setup used for random-number generation is allowed in SDI-QRNGs. Even though this incurs a weaker form of security compared to the device-independent counterpart, it is much more practical. Realistically, there might be parts of the device that are more error prone than others. The SDI approach lets you design protocols that can still generate certifiable randomness while leaving such parts uncharacterized [30–33]. These protocols are also easier to implement since nonlocal sources are not required and is thus more consumer friendly. Hence the entropy generation capabilities of the SDI protocols are of particular interest to cryptographers and others who use random numbers for various practical purposes.

In this paper, we derive a general upper bound on the amount of entropy generated by a class of SDI protocols. Specifically, we consider prepare and measure protocols of two-dimensional systems and two-outcome measurements. Even though various protocols belonging to this class have been studied previously [24,25], their analysis has been restricted to some particular dimension witnesses which are used to distinguish quantum processes from classical processes. Our results, however, are independent of dimensional witnesses. We prove that the maximum amount of entropy which could be generated by any protocol of this class is equal to $-\log_2[\frac{1}{2}(1+\frac{1}{\sqrt{3}})]$. The 3 → 1 quantum random access code (QRAC) was shown to certify the same amount of entropy and it was conjectured to be the maximum among $n \to 1$ QRAC protocols [25]. The results we obtain confirm this and also prove that 3 → 1 QRAC generates maximal randomness among general SDI protocols with binary outcome measurements. Moreover, the minimum number of preparation and measurement settings to certify the maximum amount of entropy is also proven. We give an explicit example of a unique protocol that matches these bounds, proving them to be tight.

[*] vaisakhmannalath@gmail.com
[†] anirban.pathak@jiit.ac.in

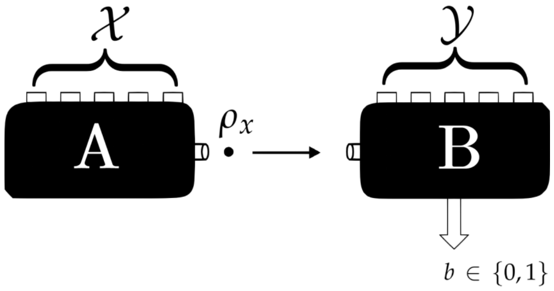

FIG. 1. We consider the prepare and measure scenario of two-dimensional systems ρ_x. The protocol features two black boxes A and B, for preparation and measurement, respectively. A has $\mathcal{X}$ input settings and B has $\mathcal{Y}$ input settings. Based on the input, A will output a state ρ_x and B will output $b \in \{0, 1\}$ based on its input and the state sent by A.

Furthermore, we derive an analytical relationship between the witness values and the entropy generated with this protocol.

The rest of the paper is organized as follows. In Sec. II, we briefly describe the SDI model and state some definitions that we use in the subsequent sections. Section III contains results on the limits of output/input randomness. We report an explicit protocol matching these limits and its subsequent analysis in Sec. IV. In Sec. V, we present a brief discussion along with some relevant open questions for further research.

II. SEMI-DEVICE-INDEPENDENT MODEL

We first illustrate the general structure of the SDI-QRNG protocol that we have considered here. It involves two black boxes shielded from the outside world (see Fig. 1). One of the devices (boxes) is used for state preparation while the other one is used for the measurement. The preparation black box A has $\mathcal{X}$ settings, and the measurement black box B has $\mathcal{Y}$ settings: $\mathcal{X}, \mathcal{Y} \geqslant 2$. Depending on the randomly chosen setting among $\mathcal{X}$, A outputs a quantum system ρ_x, $x \in [\mathcal{X}]$ (we use $[N]$ to denote a set of cardinality N), which will then be sent to the second black box B for measurement. We assume that the state $\rho_x \in \mathbb{C}^2$ is a two-dimensional system. The measurement device takes ρ_x as input and measures it in one of the randomly chosen settings $\mathcal{Y}$ and outputs $b \in \{0, 1\}$. This forms one round of the prepare and measure protocol. We can repeat this procedure multiple times to get a probability distribution given by

$$p(b|x, y) = \mathrm{Tr}\left(\rho_x M_y^b\right), \tag{1}$$

where M_y^b is the measurement operator acting on ρ_x with input parameter $y \in [\mathcal{Y}]$ and output b.

In order to identify whether the probability distributions truly have a quantum origin or not, dimension witnesses of the form

$$W \equiv \sum_{x,y} w_{x,y} E_{x,y} \tag{2}$$

are usually used, where $w_{x,y}$ are real coefficients and

$$E_{x,y} = P(b = 0|x, y).$$

Under such dimension witnesses, an SDI protocol does not demand any restriction on preshared classical correlations between the preparation and measurement devices [34]. Although we do assume that they do not share any quantum correlations. If we denote by W_c and W_Q the classical and quantum upper bounds of the witness value using two-dimensional systems, whenever

$$W_c < W \leqslant W_Q, \tag{3}$$

we can be certain that the protocol has no classical description [24,34]. Hence the output b of B is truly probabilistic in nature and can be used to extract randomness [35,36].

The entropy in the output b can be quantified by the following min-entropy function [37]

$$H_\infty(B|\mathcal{X}, \mathcal{Y}) = -\log_2\Big[\max_{b,x,y} p(b|x, y)\Big]. \tag{4}$$

This entropy is considered to be "certifiable" if the corresponding probability distribution satisfies the constraint Eq. (3).

Since our witnesses defined by Eq. (2) are linear in probabilities, we just need to consider pure states for our analysis as any arbitrary mixed state can be written as a convex combination of pure states [34]. It has also been proven that positive-operator valued measures (POVMs) can be depicted as a convex combinations of projective measurements in the case of two-measurement outcomes [38,39]. Furthermore, it is known that projective measurements on two-dimensional systems can be represented as antipodal unit vectors on the Bloch sphere. In general, the basis elements can be expressed as

$$M_y^0 = \tfrac{1}{2}(\mathbb{I} + \vec{t}_y \cdot \sigma), \quad M_y^1 = \tfrac{1}{2}(\mathbb{I} - \vec{t}_y \cdot \sigma), \tag{5}$$

where $\vec{t}_y$ is a unit vector on the Bloch sphere and $\sigma = (\sigma_x, \sigma_y, \sigma_z)$, the Pauli matrices. For preparations, it is enough to consider pure states represented using unit vectors $\vec{s}_x$ as

$$\rho_x = \tfrac{1}{2}(\mathbb{I} + \vec{s}_x \cdot \sigma). \tag{6}$$

Under this representation, the probability distribution $p(b|x, y)$ can be expressed as

$$p(b|x, y) = \mathrm{Tr}\left(\rho_x M_y^b\right) = \tfrac{1}{2}(1 + \vec{s}_x \cdot \vec{t}_y). \tag{7}$$

We may now proceed to prove some general results related to the capabilities of SDI-QRNGs using the definitions and notations introduced in this section.

III. RESULTS: BOUNDS ON CERTIFIABLE ENTROPY

Theorem 1. A prepare and measure protocol of two-dimensional systems and two-outcome measurements can generate at most $-\log_2[\frac{1}{2}(1 + \frac{1}{\sqrt{3}})]$ bits of certifiable entropy.

Proof. Maximizing the entropy in Eq. (4) amounts to minimizing the quantity $\max_{b,x,y} p(b|x, y)$ over all prepare and measure protocols. We shall achieve this by first defining a lower bound for the quantity to be minimized and then deriving the lowest possible value for the lower bound.

Consider the quantity

$$p_{lb} = \max_x \frac{1}{\mathcal{Y}} \sum_y \max_b p(b|x, y),$$

where the average is taken over all the measurement settings. Since the mean over a set is lower than the maximum of a set,

p_{lb} forms a lower bound to $\max_{b,x,y} p(b|x,y)$. We may now derive an expression for p_{lb}.

Let us represent the measurement basis for $\mathcal{Y}$ measurement settings as

$$\mathcal{T}_{\mathcal{Y}} = \{\{\vec{t}_1, -\vec{t}_1\}, \{\vec{t}_2, -\vec{t}_2\}, \dots, \{\vec{t}_{\mathcal{Y}}, -\vec{t}_{\mathcal{Y}}\}\}.$$

Each of these measurement bases can be represented by a diameter of the Bloch sphere with the basis elements as its endpoints. For example, the basis $\{\vec{t}_1, -\vec{t}_1\}$ represents a diameter with $\vec{t}_1$ and $-\vec{t}_1$ as its endpoints. It is trivial to see that given any two nonperpendicular diameters of a sphere in $\mathbb{R}^3$ the smallest angle between them would be less than or equal to $\pi/2$. To further illustrate our point, let us consider the bases $\{\vec{t}_i, -\vec{t}_i\}$ and $\{\vec{t}_j, -\vec{t}_j\}$. If the angle between the vectors $\vec{t}_i$ and $-\vec{t}_j$ is greater than $\pi/2$, then the angle between $\vec{t}_i$ and $\vec{t}_j$ will definitely be less than $\pi/2$, for any $i, j \in [\mathcal{Y}]$.

Keeping the above arguments in mind, consider a particular case, $\mathcal{Y} = 2$, with measurement bases as $\{\vec{t}_1, -\vec{t}_1\}$ and $\{\vec{t}_2, -\vec{t}_2\}$. If we consider the angle between $\vec{t}_1$ and $\vec{t}_2$ to be less than or equal to $\pi/2$, then the state ρ_x with $\vec{s}_x = \frac{\vec{t}_1+\vec{t}_2}{|\vec{t}_1+\vec{t}_2|}$ maximizes $\frac{1}{\mathcal{Y}} \sum_y \max_b p(b|x,y)$, yielding p_{lb}. It is easy to see that p_{lb} is minimum when $\vec{t}_1$ and $\vec{t}_2$ are perpendicular to each other.

For now, let us assume that $0 \leqslant \theta_{i,j} \leqslant \pi/2$, where $\theta_{i,j}$ is the angle between the measurement vectors $\vec{t}_i$ and $\vec{t}_j$ for $i, j \in [\mathcal{Y}]$. This is in general not true for $\mathcal{Y} \geqslant 3$. but we will give an argument at the end of the proof as to why this assumption is valid enough to find out the minimum value of p_{lb}.

Given this setup, consider ρ_x with $\vec{s}_x = \frac{\vec{t}_1+\vec{t}_2+\cdots+\vec{t}_{\mathcal{Y}}}{|\vec{t}_1+\vec{t}_1+\cdots+\vec{t}_{\mathcal{Y}}|}$. Note that given the choice of measurement vectors $\{\vec{t}_1, \vec{t}_2, \dots, \vec{t}_{\mathcal{Y}}\}$, this state maximizes $\frac{1}{\mathcal{Y}} \sum_y \max_b p(b|x,y)$ since it lies along the average direction of the measurement vectors. Simplification yields

$$p_{lb} = \frac{1}{2}\left(1 + \frac{|\vec{t}_1 + \vec{t}_2 + \cdots + \vec{t}_{\mathcal{Y}}|}{\mathcal{Y}}\right). \tag{8}$$

We can represent Eq. (8) as

$$p_{lb} = \frac{1}{2}\left(1 + \frac{\sqrt{\mathcal{Y} + 2(\cos\theta_{1,2} + \cdots + \cos\theta_{\mathcal{Y}-1,\mathcal{Y}})}}{\mathcal{Y}}\right). \tag{9}$$

Lemma 1. For $\mathcal{Y}$ unit vectors that lie in an octant of a sphere in $\mathbb{R}^3$, the minimum of the sum of cosines of the angles formed between them is equal to $\frac{3}{2}\mu(\mu-1) + r\mu$, where $\mathcal{Y} = 3\mu + r$ for positive integers μ and $r \in \{0, 1, 2\}$.

Proof. Consider $\mathcal{Y}$ vectors $\{\vec{t}_1, \dots, \vec{t}_{\mathcal{Y}}\}$. The sum to be minimized is

$$\cos\theta_{1,2} + \cos\theta_{1,3} + \cdots + \cos\theta_{\mathcal{Y}-1,\mathcal{Y}}.$$

We can rewrite it as

$$(\cos\theta_{1,2} + \cos\theta_{1,3} + \cdots + \cos\theta_{1,\mathcal{Y}}) + \cdots + \cos\theta_{\mathcal{Y}-1,\mathcal{Y}}.$$

The terms in the parentheses are equal to

$$\vec{t}_1 \cdot (\vec{t}_2 + \cdots + \vec{t}_{\mathcal{Y}}).$$

Since every vector lies in the same octant, the dot product is minimized when $\vec{t}_1$ is along one of the axes. We can repeat the same process for every other vector until all of them line up with one of the three axes. We have three scenarios based on the value of $r \in \{0, 1, 2\}$.

(1) $\mathcal{Y} = 3\mu$: It is trivial to see that the sum is minimum when the vectors are equally distributed among the axes—μ vectors along each axis. The sum of cosines is equal to $3\,{}^{\mu}C_2$. The symbol "${}^{n}C_k$" is the coefficient of the term x^k in the polynomial expansion of the $(1+x)^n$. It is given by the formula

$${}^{n}C_k = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1},$$

where $0 \leqslant k \leqslant n$.

(2) $\mathcal{Y} = 3\mu + 1$: An additional vector along any one of the axes, say x axis. The sum becomes $2\,{}^{\mu}C_2 + {}^{\mu+1}C_2$.

(3) $\mathcal{Y} = 3\mu + 2$: Consider the sum of vectors

$$\vec{t}_1 + \cdots + \vec{t}_{3\mu+1}.$$

Since they have an arrangement dictated by the previous case, the vector $\vec{t}_{3\mu+2}$ should end up at the y or z axis. The sum becomes ${}^{\mu}C_2 + 2\,{}^{\mu+1}C_2$.

Putting it all together, we have the sum as

$$(3-r)\,{}^{\mu}C_2 + r\,{}^{\mu+1}C_2.$$

Simplifying it we obtain

$$\tfrac{3}{2}\mu(\mu-1) + r\mu. \qquad \blacksquare$$

Since our measurement vectors $\{\vec{t}_1, \vec{t}_2, \dots, \vec{t}_{\mathcal{Y}}\}$ are at most $\pi/2$ away from each other, we can consider them to lie in the same octant. Applying Lemma 1, Eq. (9) becomes

$$p_{lb} = \frac{1}{2}\left(1 + \frac{\sqrt{\mathcal{Y} + 3\mu(\mu-1) + 2r\mu}}{\mathcal{Y}}\right). \tag{10}$$

Substituting $\mathcal{Y} = 3\mu + r$ we obtain

$$p_{lb} = \frac{1}{2}\left(1 + \frac{\sqrt{3\mu^2 + r(2\mu+1)}}{3\mu + r}\right). \tag{11}$$

Thus, for $r = 0$, we have

$$p_{lb} = \frac{1}{2}\left(1 + \frac{\sqrt{3\mu^2}}{3\mu}\right) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right). \tag{12}$$

For $r \in \{1, 2\}$, $p_{lb} > \frac{1}{2}(1 + \frac{1}{\sqrt{3}})$ and $p_{lb} \to \frac{1}{2}(1 + \frac{1}{\sqrt{3}})$ as $\mu \to \infty$. Thus, in general,

$$p_{lb} \geqslant \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right). \qquad \blacksquare$$

Note that our assumption that $0 \leqslant \theta_{i,j} \leqslant \pi/2$ for $i, j \in [\mathcal{Y}]$ is valid enough since the minimum value for p_{lb} is obtained when the measurement vectors are along the three-dimensional (3D) axes. This implies that by induction, using $\mathcal{Y} = 2$ as the initial step and the freedom to relabel any measurement basis, we can take any $\mathcal{Y}$ measurement vectors to lie in the same octant.

Theorem 2. A prepare and measure protocol of two-dimensional systems needs at least four preparation settings and three measurement settings to generate the maximum amount of entropy.

Proof. From Theorem 1, the maximum entropy is generated when $\mathcal{Y} = 3\mu$. For $\mu = 1$, we have the minimum number of measurement settings, $\mathcal{Y}=3$. We will now try to minimize the number of preparation settings when $\mathcal{Y}=3$.

As for the number of preparation settings $\mathcal{X}$, note that it cannot be two since the states will be perfectly distinguishable; there is no entropy in the output. When $\mathcal{X}=3$ and $\mathcal{Y}=3$, a general dimension witness defined by Eq. (2) can be expressed as

$$\begin{aligned}W &= w_{1,1}E_{1,1}+w_{1,2}E_{1,2}+w_{1,3}E_{1,3}+w_{2,1}E_{2,1}+w_{2,2}E_{2,2}\\ &\quad +w_{2,3}E_{2,3}+w_{3,1}E_{3,1}+w_{3,2}E_{3,2}+w_{3,3}E_{3,3}. \qquad (13)\end{aligned}$$

From Theorem 1, maximum entropy generation needs at least three measurement settings. Since maximization is over the entire probability distribution, this holds for every preparation setting. Hence, none of the coefficients $w_{x,y}$ can be 0 for a witness which achieves the maximum entropy. For example, suppose $w_{3,3}$ is 0. This implies that the state ρ_3 depends only on the measurement bases M_1 and M_2; ρ_3 lies in the plane defined by M_1 and M_2. Subsequently, for a given witness value, $\max_{b,x,y} p(b|x,y) \geqslant \frac{1}{2}(1+\frac{1}{\sqrt{2}}) > \frac{1}{2}(1+\frac{1}{\sqrt{3}})$.

Now that we have established that all coefficients in Eq. (13) are nonzero, we can model it as an QRAC-like protocol where preparation states correspond to 3-bit strings and measurement settings determine which bit to guess. Positive coefficients are mapped to bit 0 and negative coefficients to bit 1. For example, consider

$$\begin{aligned}R_{3,3} \equiv\; & E_{1,1}+E_{1,2}+E_{1,3}+E_{2,1}-E_{2,2}\\ & -E_{2,3}-E_{3,1}+E_{3,2}-E_{3,3}. \qquad (14)\end{aligned}$$

Based on our construction, $R_{3,3}$ can be defined as the average success probability of an QRAC protocol where preparation states are represented as $x \in \{000, 011, 101\}$ and measurement settings dictate which one of the three bits to guess.

For any such task we can construct a protocol based on the $2 \rightarrow 1$ QRAC (cf. Fig. 2) whose average probability would be greater than $\frac{1}{2}(1+\frac{1}{\sqrt{3}})$, implying the entropy generated will be lesser than $-\log_2[\frac{1}{2}(1+\frac{1}{\sqrt{3}})]$ [since $\max_{b,x,y} p(b|x,y) \geqslant \sum_{x,y} p(b=x_y|x,y)$: x represents any of the 3-bit strings and x_y denotes the yth bit of that string].

The protocol is represented using Fig. 2. A 3-bit string can be written as x where $x \in \{00x_3, 01x_3, 10x_3, 11x_3\}$ and x_3 is the third bit (which could be different for different strings). The task is then straightforward: Encode the strings on any three of the four possible states using $2 \rightarrow 1$ QRAC, where the encoding can be represented as

$$\text{Encoding}\begin{cases} 00 \rightarrow \frac{1}{2}\big(\mathbb{I}+\frac{1}{\sqrt{2}}\sigma_x+\frac{1}{\sqrt{2}}\sigma_y\big),\\ 01 \rightarrow \frac{1}{2}\big(\mathbb{I}+\frac{1}{\sqrt{2}}\sigma_x-\frac{1}{\sqrt{2}}\sigma_y\big),\\ 10 \rightarrow \frac{1}{2}\big(\mathbb{I}-\frac{1}{\sqrt{2}}\sigma_x+\frac{1}{\sqrt{2}}\sigma_y\big),\\ 11 \rightarrow \frac{1}{2}\big(\mathbb{I}-\frac{1}{\sqrt{2}}\sigma_x-\frac{1}{\sqrt{2}}\sigma_y\big).\end{cases}$$

Decode the first two bits using the measurement bases given by

$$M_y \equiv \big\{\tfrac{1}{2}(\mathbb{I}+\vec{t}_y\cdot\sigma), \tfrac{1}{2}(\mathbb{I}-\vec{t}_y\cdot\sigma)\big\}$$

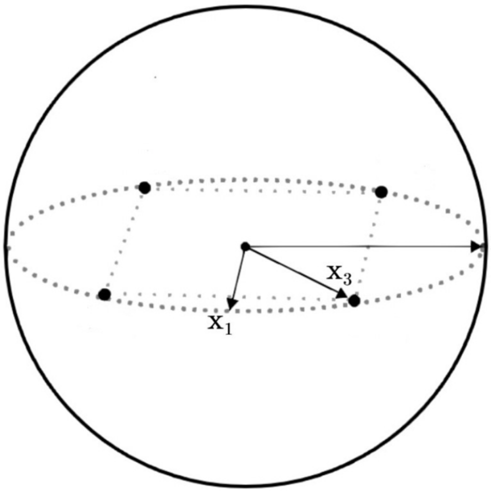

FIG. 2. Bloch sphere diagram of a SDI protocol with three preparation setting and three measurement settings. The arrows denote the "up" direction of the measurement basis and the black dots indicate the encoded states for a particular choice of setting or equivalently, a string of bits. The three strings are to be encoded in any of the four vertices. The encoded states of this protocol form a subset of the encoded states in the $2 \rightarrow 1$ QRAC, which forms a square on the equatorial plane of the Bloch sphere, denoted in this figure using dotted lines.

and their corresponding Bloch vectors

$$\text{Decoding}\begin{cases} x_1 \rightarrow \vec{t}_i \equiv (1,0,0),\\ x_2 \rightarrow \vec{t}_i \equiv (0,1,0).\end{cases}$$

Decode the third bit using

$$x_3 \rightarrow \vec{t}_3 \equiv \frac{1}{\sqrt{2}}(1,1,0).$$

Given the choice of measurement bases and prepared states the average probability is found to be at least

$$\frac{6\big[\frac{1}{2}\big(1+\frac{1}{\sqrt{2}}\big)\big]+2}{9} \approx 0.791\,25.$$

Hence for such a protocol we have an average probability greater than ~0.791 25 which is greater than $\frac{1}{2}(1+\frac{1}{\sqrt{3}}) \approx 0.788\,67$. ■

IV. A SPECIFIC PROTOCOL

An explicit protocol to achieve $H_\infty = -\log_2[\frac{1}{2}(1+\frac{1}{\sqrt{3}})] \approx 0.342\,49$ using four preparation settings and three measurement settings is given here. It corresponds to a QRAC-like protocol in which the preparation party A encodes one of the strings $x \in \{000, 011, 101, 110\}$ to a single qubit and the measurement party B attempts to decode $x_y \in \{x_1, x_2, x_3\}$ by suitable measurements (cf. Fig. 3). Using arguments similar to those used for proving Theorem 2, this protocol can be proven to be unique up to some relabeling of the measurement bases. A suitable dimension witness is provided by

$$\begin{aligned}R_{4,3} \equiv\; & E_{000,1}+E_{000,2}+E_{000,3}+E_{011,1}\\ & -E_{011,2}-E_{011,3}-E_{101,1}+E_{101,2}\\ & -E_{101,3}-E_{110,1}-E_{110,2}+E_{110,3}, \qquad (15)\end{aligned}$$

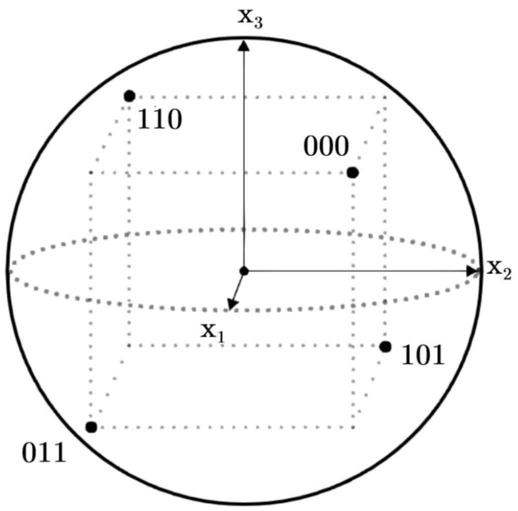

FIG. 3. Bloch sphere diagram of a SDI protocol with four preparation settings and three measurement settings. The measurement bases are mutually unbiased, similar to the 3 → 1 QRAC protocol. The arrows denote the “up” direction of the measurement basis and the black dots indicate the encoded states for a particular choice of string/setting. The encoded states form a tetrahedron inside the Bloch sphere. They also form a subset of the encoded states in the 3 → 1 QRAC, which forms a cube, denoted in this figure using dotted lines.

and whenever

$$3 < R_{4,3} \leqslant 2\sqrt{3}, \tag{16}$$

the protocol has no classical description. Equation (16) was derived from the results provided in Ref. [40]. They have treated the protocol as a generalized version of the 2 → 1 QRAC protocol where B attempts to decode, in addition to the bits encoded by A, the parity of the bits as well. The average success probability of this particular protocol has previously found applications in the SDI security of quantum key distribution (QKD) protocols [41]. The corresponding dimension witness has also been applied previously in the self-testing of POVMs [42,43] and in the reduction of symmetric dimension witnesses [44]. In order to achieve the maximal quantum value $2\sqrt{3}$, we may encode the bits using the states given by

$$\text{Encoding}\begin{cases} 000 \mapsto \frac{1}{2}\big(\mathbb{I} + \frac{1}{\sqrt{3}}\sigma_x + \frac{1}{\sqrt{3}}\sigma_y + \frac{1}{\sqrt{3}}\sigma_z\big), \\ 011 \mapsto \frac{1}{2}\big(\mathbb{I} + \frac{1}{\sqrt{3}}\sigma_x - \frac{1}{\sqrt{3}}\sigma_y - \frac{1}{\sqrt{3}}\sigma_z\big), \\ 101 \mapsto \frac{1}{2}\big(\mathbb{I} - \frac{1}{\sqrt{3}}\sigma_x + \frac{1}{\sqrt{3}}\sigma_y - \frac{1}{\sqrt{3}}\sigma_z\big), \\ 110 \mapsto \frac{1}{2}\big(\mathbb{I} - \frac{1}{\sqrt{3}}\sigma_x - \frac{1}{\sqrt{3}}\sigma_y + \frac{1}{\sqrt{3}}\sigma_z\big), \end{cases}$$

and decode the bits using the measurement bases given by

$$M_y \equiv \big\{\tfrac{1}{2}(\mathbb{I} + \vec{t}_y \cdot \sigma), \tfrac{1}{2}(\mathbb{I} - \vec{t}_y \cdot \sigma)\big\}$$

with the corresponding Bloch vectors

$$\text{Decoding}\begin{cases} x_1 \to \vec{t}_1 \equiv (1, 0, 0), \\ x_2 \to \vec{t}_2 \equiv (0, 1, 0), \\ x_3 \to \vec{t}_3 \equiv (0, 0, 1). \end{cases}$$

Note that a general two-dimensional witness for four preparation settings and three measurement settings may not be able to produce the maximum amount of randomness. For example, consider the well-known dimension witness I_4 [34,45], defined as

$$\begin{aligned} I_4 \equiv {} & E_{1,1} + E_{1,2} + E_{1,3} + E_{2,1} + E_{2,2} - E_{2,3} \\ & + E_{3,1} - E_{3,2} - E_{4,1}. \end{aligned}$$

Since the choice of the fourth state solely depends on the first measurement basis, one can always take $E_{4,1}$ to be 0. This implies that $p(b = 1|4, 1) = 1$; no entropy is generated in this case. The choice of dimension witness is special in that regard and warrants further analysis. We will now derive an analytical bound on the min-entropy based on the value of the dimension witness. The analysis and methods used is similar to what have been done in Refs. [46,47].

Using Eqs. (5) and (6), Eq. (15) can be written as

$$\begin{aligned} R_{4,3} \equiv {} & E_{000,1} + E_{000,2} + E_{000,3} + E_{011,1} - E_{011,2} - E_{011,3} - E_{101,1} + E_{101,2} - E_{101,3} - E_{110,1} - E_{110,2} + E_{110,3} \\ = {} & \mathrm{Tr}\big[\rho_{000}\big(M_1^0 + M_2^0 + M_3^0\big)\big] + \mathrm{Tr}\big[\rho_{011}\big(M_1^0 - M_2^0 - M_3^0\big)\big] \\ & + \mathrm{Tr}\big[\rho_{101}\big(-M_1^0 + M_2^0 - M_3^0\big)\big] + \mathrm{Tr}\big[\rho_{110}\big(-M_1^0 - M_2^0 + M_3^0\big)\big] \\ = {} & \tfrac{1}{2}[\vec{s}_{000} \cdot (\vec{t}_1 + \vec{t}_2 + \vec{t}_3) + \vec{s}_{011} \cdot (\vec{t}_1 - \vec{t}_2 - \vec{t}_3) + \vec{s}_{101} \cdot (-\vec{t}_1 + \vec{t}_2 - \vec{t}_3) + \vec{s}_{110} \cdot (-\vec{t}_1 - \vec{t}_2 + \vec{t}_3)] \\ \leqslant {} & \tfrac{1}{2}\,(|\vec{t}_1 + \vec{t}_2 + \vec{t}_3| + |\vec{t}_1 - \vec{t}_2 - \vec{t}_3| + |\vec{t}_1 - \vec{t}_2 + \vec{t}_3| + |\vec{t}_1 + \vec{t}_2 - \vec{t}_3|) \\ \leqslant {} & \tfrac{1}{2}(\sqrt{3 + 2[\cos{(\theta_{1,2})} + \cos{(\theta_{1,3})} + \cos{(\theta_{2,3})}]} + \sqrt{3 + 2[\cos{(\theta_{1,2})} - \cos{(\theta_{1,3})} + \cos{(\theta_{2,3})}]} \\ & + \sqrt{3 + 2[\cos{(\theta_{1,2})} + \cos{(\theta_{1,3})} - \cos{(\theta_{2,3})}]} + \sqrt{3 + 2[\cos{(\theta_{1,2})} - \cos{(\theta_{1,3})} - \cos{(\theta_{2,3})}]}), \end{aligned} \tag{17}$$

where the first inequality follows from $|\vec{s}_x| < 1$. Using Eq. (9) we can write p_{lb} for our example as

$$p_{lb} = \frac{1}{2}\left(1 + \frac{\sqrt{3 + 2[\cos{(\theta_{1,2})} + \cos{(\theta_{1,3})} + \cos{(\theta_{2,3})}]}}{3}\right). \tag{18}$$

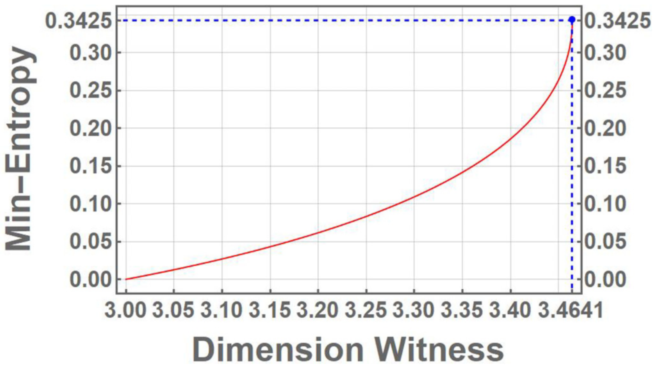

FIG. 4. Relationship between dimension witness value and upper bound on the entropy created by the protocol discussed in Sec. IV.

In order to obtain a bounded value of $R_{4,3}$ as a function of p_{lb} we will use the extreme value problem of a multivariable function. Changing variables as

$$\mathcal{P} = \frac{[3(2p_{lb}-1)]^2-3}{2}, \quad a = \cos\theta_{1,3}, \quad b = \cos\theta_{2,3},$$

and applying it to Eq. (17), we obtain

$$R_{4,3} \leqslant \max_{\{(q,r)\}} \Big\{\tfrac{1}{2}\big(\sqrt{3+2\mathcal{P}} + \sqrt{3+2(2q-\mathcal{P})} + \sqrt{3+2(2r-\mathcal{P})} + \sqrt{3+2[\mathcal{P}-(2q+2r)]}\big)\Big\}, \tag{19}$$

where (q, r) is one of the real roots of equation set with variables (a, b) given by

$$\frac{1}{2}\left(\frac{2}{\sqrt{2(2a-\mathcal{P})+3}} - \frac{2}{\sqrt{2(\mathcal{P}-2a-2b)+3}}\right) = 0,$$
$$\frac{1}{2}\left(\frac{2}{\sqrt{2(2b-\mathcal{P})+3}} - \frac{2}{\sqrt{2(\mathcal{P}-2b-2a)+3}}\right) = 0. \tag{20}$$

The equation set provided above is obtained by taking the derivatives of Eq. (17) with respect to a and b. It turns out that the solutions of Eq. (20) should satisfy the condition

$$a = b = \mathcal{P}/3 \Rightarrow \cos\theta_{1,2} = \cos\theta_{1,3} = \cos\theta_{2,3}. \tag{21}$$

Since p_{lb} is defined as $\max_x \frac{1}{y}\sum_y \max_b p(b|x,y)$, by Eq. (21) all the terms in the summation are equal. This means that when $R_{4,3}$ is maximized, p_{lb} is equivalent to $\max_{b,x,y} p(b|x,y)$. Hence the maximization will yield a tight upper bound on the randomness generated by this protocol. Also, Eq. (21) reduces our problem to a single variable one.

Substituting Eq. (21) in Eqs. (17) and (18), we get

$$R_{4,3} \leqslant \tfrac{1}{2}(3\sqrt{3-2a} + \sqrt{6a+3}),$$
$$p_{lb} = \tfrac{1}{2}\big(\tfrac{1}{3}\sqrt{6a+3} + 1\big). \tag{22}$$

Solving Eq. (22) we obtain

$$p_{lb} \leqslant \tfrac{1}{12}\Big[R_{4,3} + 6 + \sqrt{3\big(12 - R_{4,3}^2\big)}\Big]. \tag{23}$$

This forms a min-entropy bound for the particular protocol as shown in Fig. 4. Since the choice of angles is unique when $R_{4,3} = 2\sqrt{3}$, i.e.,

$$\theta_{1,2} = \theta_{1,3} = \theta_{2,3} = \pi/2,$$

it yields the maximum amount of certifiable randomness, $H_\infty \approx 0.342\,49$. Also note that since p_{lb} forms an upper bound to the average success probability of the protocol, Eq. (23) implies that certifiable randomness can be generated as soon as one violates the classical bound on witness. This is particularly relevant in practical setups, which might not be able to achieve the maximum possible quantum violation. The protocol is thus noise robust, and has immediate applications in practical SDI-QRNG setups.

Since we assume that devices are shielded from the outside world, the randomness used to choose the input settings in each round can be used for other purposes. Hence the total output randomness from each round is more than what is being used to start the process. In order to increase randomness expansion even further, one can consider using a fixed subset of the input setting for randomness generation for most rounds and a randomly chosen input setting for the rest of the rounds [46,48,49]. If the number of rounds is large enough, one can use the subset of rounds wherein the input settings were randomly chosen in order to estimate the witness value [20].

V. DISCUSSIONS AND OUTLOOK

A tight bound on the entropy generation rate is derived for SDI prepare and measure protocols for two-dimensional systems and two-outcome measurements solely from geometrical arguments. The maximum entropy generated from such a class of protocols is found to be equal to $-\log_2[\frac{1}{2}(1+\frac{1}{\sqrt{3}})]$. Here it will be apt to note the results of a previous work [50] which suggests an upper bound on the certifiable randomness from a quantum black box as $-\log_2[\min\{l, k+1\}]$, where l is the number of outputs for a measurement (2 in our case) and k is the number of preparation settings. For the particular class of protocols that we are considering, this result forms a trivial bound of 1 bit of certifiable entropy. Our results are much more strict in that regard. It was also conjectured in Ref. [25] that 3 → 1 QRAC generates the maximum amount of randomness among $n \to 1$ QRAC protocols. We have proved that this is indeed the case. Our results are more general than QRAC protocols and also independent of any dimension witness. We have also provided an explicit protocol generating the maximum amount of entropy while having the least amount of input settings. The protocol generates as much entropy as the 3 → 1 QRAC protocol does, however, it requires lesser input settings. Note that even though the protocol generates maximum entropy when $W = W_Q$, it still remains an open question if one can extract more randomness than what is given in Fig. 4 when $W < W_Q$. Since Eq. (23) is tied to a specific dimension witness, i.e., $R_{4,3}$, it would be worthwhile to investigate whether the methods by Wang *et al.* [51] would be able to extract more randomness when $3 < R_{4,3} < 2\sqrt{3}$. Inspired by the device-independent approach used in Refs. [49,52], they used the full observed statistics to certify randomness rather than restricting to a particular inequality.

The results reported here open up possibilities for a set of interesting investigations. An immediate generalization of the presented work would be to consider the limits on entropy generation for l-outcome measurements on d-dimensional systems, $l, d > 2$. It would also be interesting to investigate the randomness expansion capabilities of such protocols with partially free random sources as the input seed [53,54]. Given the advantage of our protocol over the $3 \rightarrow 1$ QRAC with perfect random sources, it would be interesting to see a comparison with partially free sources [55]. Another possible avenue for research would be to consider the randomness generation ability for multiple users as discussed in Ref. [56].

ACKNOWLEDGMENTS

The authors acknowledge the support from the QUEST scheme of Interdisciplinary Cyber Physical Systems (ICPS) program of the Department of Science and Technology (DST), India [Grant No. DST/ICPS/QuST/Theme-1/2019/14 (Q80)]. They also thank Manik Banik, Ram Krishna Patra, Sandeep Mishra, R. Srikanth, H. S. Karthik, H. Akshata Shenoy, and Kishore Thapliyal for their interest and feedback on the work.

[1] N. Metropolis and S. Ulam, J. Am. Stat. Assoc. **44**, 335 (1949).
[2] R. M. Karp, Discrete Appl. Math. **34**, 165 (1991).
[3] R. Motwani and P. Raghavan, ACM Comput. Surv. **28**, 33 (1996).
[4] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).
[5] R. Gennaro, IEEE Secur. Priv. **4**, 64 (2006).
[6] J. Bouda, M. Pivoluska, M. Plesch, and C. Wilmott, Phys. Rev. A **86**, 062308 (2012).
[7] J. S. Bell, Phys. Phys. Fiz. **1**, 195 (1964).
[8] J. A. Wheeler, in *Mathematical Foundations of Quantum Theory* (Academic Press, New York, 1978), pp. 9–48.
[9] P. Shadbolt, J. C. F. Mathews, A. Laing, and J. L. O'Brien, Nat. Phys. **10**, 278 (2014).
[10] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).
[11] P. L'Ecuyer, in *Handbook of Computational Statistics*, edited by J. Gentle, W. Härdle, and Y. Mori (Springer, Berlin, 2012), p. 35.
[12] C. S. Calude, in *Indeterminism and randomness*, edited by M. Gheorghe, I. Petre, M. J. Pérez-Jiménez, G. Rozenberg, and A. Salomaa, Multidisciplinary Creativity (Spandugino Publ. House, Bucharest, 2015), pp. 207–212.
[13] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).
[14] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Inf. **2**, 16021 (2016).
[15] Quantum random number generation (QRNG) - ID Quantique, https://www.idquantique.com/random-number-generation/overview/ (accessed on 11/21/2021).
[16] M. M. Jacak, P. Jóźwiak, J. Niemczuk, and J. E. Jacak, Sci. Rep. **11**, 16108 (2021).
[17] L. Huang, H. Zhou, K. Feng, and C. Xie, npj Quantum Inf. **7**, 107 (2021).
[18] R. Colbeck, Ph.D. thesis, University of Cambridge, 2006, arXiv:0911.3814.
[19] R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2010).
[20] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).
[21] S. Pironio and S. Massar, Phys. Rev. A **87**, 012336 (2013).
[22] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Nature (London) **562**, 548 (2018).
[23] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, Nat. Phys. **17**, 448 (2021).
[24] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).
[25] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).
[26] D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, Phys. Rev. A **100**, 062338 (2019).
[27] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Phys. Rev. A **94**, 060301(R) (2016).
[28] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Phys. Rev. X **6**, 011020 (2016).
[29] A. Tavakoli, Phys. Rev. Lett. **126**, 210503 (2021).
[30] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).
[31] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. Appl. **7**, 054018 (2017).
[32] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Phys. Rev. Appl. **15**, 034034 (2021).
[33] M. Pivoluska, M. Plesch, M. Farkas, N. Ružičková, C. Flegel, N. H. Valencia, W. McCutcheon, M. Malik, and E. A. Aguilar, npj Quantum Inf. **7**, 50 (2021).
[34] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Phys. Rev. Lett. **105**, 230501 (2010).
[35] L. Trevisan, J. ACM **48**, 860 (2001).
[36] J. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).
[37] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[38] L. Masanes, arXiv:quant-ph/0512100.
[39] M. Tomamichel and E. Hänggi, J. Phys. A: Math. Theor. **46**, 055301 (2013).
[40] Vaisakh M, R. K. Patra, M. Janpandit, S. Sen, M. Banik, and A. Chaturvedi, Phys. Rev. A **104**, 012420 (2021).
[41] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).
[42] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Sci. Adv. **6**, eaaw6664 (2020).
[43] P. Mironowicz and M. Pawłowski, Phys. Rev. A **100**, 030301(R) (2019).
[44] P. Mironowicz, H.-W. Li, and M. Pawłowski, Phys. Rev. A **90**, 022322 (2014).
[45] M. Hendrych, R. Gallego, M. Mičuda, N. Brunner, A. Acín, and J. P. Torres, Nat. Phys. **8**, 588 (2012).
[46] H.-W. Li, Z.-Q. Yin, M. Pawłowski, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **91**, 032305 (2015).
[47] D.-D. Li, Q.-Y. Wen, Y.-K. Wang, Y.-Q. Zhou, and F. Gao, Sci. Rep. **5**, 15543 (2015).

[48] P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, M. Pawłowski, and M. Bourennane, New J. Phys. **18**, 065004 (2016).

[49] J.-D. Bancal, L. Sheridan, and V. Scarani, New J. Phys. **16**, 033011 (2014).

[50] M. Ioannou, J. B. Brask, and N. Brunner, Phys. Rev. A **99**, 052338 (2019).

[51] Y.-K. Wang, S.-J. Qin, X. Wu, F. Gao, and Q.-Y. Wen, Phys. Rev. A **92**, 052321 (2015).

[52] O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).

[53] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).

[54] Y.-Q. Zhou, H.-W. Li, Y.-K. Wang, D.-D. Li, F. Gao, and Q.-Y. Wen, Phys. Rev. A **92**, 022331 (2015).

[55] Y.-Q. Zhou, F. Gao, D.-D. Li, X.-H. Li, and Q.-Y. Wen, Phys. Rev. A **94**, 032318 (2016).

[56] X. Wang, J. Yuan, Y. Zhou, Y. Liu, and L. Fan, Quantum Inf. Process. **20**, 346 (2021).