Randomness extraction from quantum systems with different levels of trust in the working of the devices

Yun Zhi Law, Jean-Daniel Bancal, and Valerio Scarani

Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore

Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore

(Dated: January 20, 2014)

The amount of intrinsic randomness that can be extracted from measurement on quantum systems depends on several factors: in this paper we compare various levels of trust in the working of the devices of the authorized partners. Many recent studies have focused the so-called “device-independent” level: by violating a Bell inequality, a lower bound on the amount of randomness present in the data can be certified without knowing any operational details about the devices. When on the contrary all the devices are trusted, specific measurements can be chosen in order to extract the maximal amount of randomness. This “tomographic” level of trust is well known (in a sense, it has been known since people noticed that there is randomness in quantum physics); but we present a systematic approach to quantifying the amount of extractable randomness. Finally, we introduce an intermediate level of trust, related to the task of “steering”, in which the device of one party is trusted but not the other’s.

I. INTRODUCTION

The quantum information community has always duly acknowledged Bell’s work as pioneering. Indeed, Bell’s discovery [1] that an apparently philosophical issue can actually be settled by experiment was a precursor to the approach of stopping complaining about quantum weirdness and putting it to practical use. In this novel approach, however, there seemed to be little scope left for Bell inequalities: the most senior of the present authors was told a few times that, Bell having done its job by showing that local variables don’t exist, “nowadays one should rather work on entanglement”. A few authors tried to find links between Bell inequalities and some useful tasks, but for some time the reported examples happened to be either artefacts of restrictive assumptions [2] or ad hoc constructions [3].

The practical role of Bell inequalities in quantum information was fully clarified by a “flash of the obvious” around the year 2007 (see [4] [5] for a review of those developments): the violation of Bell inequalities witnesses entanglement without any need to specify the dimensionality of the system under study or the measurements that are performed on it. This means that one can certify, and even more, quantify [6], the entanglement shared between two or more black boxes. This possibility, unique to Bell inequalities, was called device-independent certification. The first task to be studied this way was quantum key distribution [7]; it was followed by the task of generating certified randomness [8] [9].

Device-independent certification still requires some assumptions; notably, one must assume “measurement independence” (i.e. the fact that the state in the boxes is uncorrelated from the choice of measurements that are going to be performed on it) and guarantee that the devices are not exchanging signals. This is the minimal level of trust in the devices that is required to be able to certify some quantum behavior [10]. On the contrary, the bulk of the quantum information literature (the “work on entanglement” mentioned above) usually works under the assumption of complete trust in the quantum description of the system and the measurements — intriguingly, this is the case even in quantum cryptography: for instance, the unconditional security of the BB84 protocol relies on the trust that the systems used by Alice and Bob are qubits [11]. Between the two extremes, several semi-device-independent levels of trust can be relevant: for instance, one may want to trust only some devices [12], or assume an upper bound on the dimensionality of the systems under study [13]. It is clear that a tradeoff is expected: more trust means higher yield of the protocol (a longer secret key, a longer list of random numbers...), alongside however with higher risk that some of the trust may be unwarranted. A quantitative comparison for the yield of secret key in quantum key distribution can be found in the literature [7] [14]. In this paper, we compare the yield of randomness generation for various levels of trust.
many runs, Alice and Bob can reconstruct the statistics of two types: one accidental, due to ignorance of some details of the state or the device; the other intrinsic, due to the unpredictability of the outcome of quantum measurements. We are interested in quantifying the latter.

II. DEFINITIONS AND NOTATION

We focus on a bipartite scenario. Each of the two users Alice and Bob holds a device with $m_A$, respectively $m_B$ buttons as inputs, and binary outcomes $a, b \in \{-1, +1\}$. In the asymptotic limit of infinitely many runs, Alice and Bob can reconstruct the statistics

$$P(a, b|u, v), u \in \{1...m_A\}, v \in \{1...m_B\}.$$  

We work under the assumption that quantum physics correctly describes the devices. We call white box a device whose operation is trusted as fully characterized; black box a device whose operation is unknown.

We are going to consider three levels of trust: device-independent, in which both Alice’s and Bob’s devices are black boxes; tomography, in which both devices are white boxes; and semi-device-independent, in which Alice’s device is a black box and Bob’s device is a white box. In what follows, we shall study each of these levels of trust separately, then finally compare them. Before this, we introduce the basic notions to study randomness (cf. Ref. [15]).

The randomness that we consider is the initial ignorance of Alice and Bob about the outcome of a query of the box (a measurement, in the usual quantum language). The unpredictability of the outcomes can be of two types: one accidental, due to

A. Randomness from one pair of settings

If the state shared by Alice and Bob is pure, there is no accidental randomness: then, the randomness of the outcome pair $(a, b)$ obtained from measuring $(A_u, B_v)$ is quantified by the probability $G(|\psi\rangle, A_u, B_v)$ of guessing the outcomes correctly. Since the best strategy for guessing is to guess the most probable outcome, this guessing probability is

$$G(|\psi\rangle, A_u, B_v) = \max_{a, b} P(a, b|A_u, B_v, |\psi\rangle)$$  

This gives the global randomness, i.e. the randomness that can be extracted from both Alice and Bob’s outcomes. A similar definition holds for local randomness, where only either Alice or Bob’s outcomes are taken into account.

If the state shared by Alice and Bob is mixed, we have to separate the intrinsic randomness from the accidental one. For measurements $A_u$ and $B_v$, the average guessing probability that quantifies intrinsic randomness will be given by

$$G(\rho, A_u, B_v) = \max_{\{q_\lambda, \psi_\lambda\}} \sum_\lambda q_\lambda G(|\psi_\lambda\rangle, A_u, B_v)$$  

where $\rho = \sum_\lambda q_\lambda |\psi_\lambda\rangle \langle \psi_\lambda|$, and the maximization is taken over all possible such decompositions. This assumes that the guesser, Charlie, knows $|\psi_\lambda\rangle$ in each run and tries to guess each run independently. As explained in the next section, in this paper we do not consider the more extreme cases, in which Charlie holds a purification and is allowed to perform collective measurements, or even keep his systems without measuring for an arbitrary amount of time.

Finally, in the case of black boxes, the users know nothing at the start and only the observed probability distribution $P$ at the end. In such case, the guessing probability that quantifies intrinsic randomness is

$$G(P, u, v) = \max_{(\rho, M) \rightarrow P} G(\rho, A_u, B_v)$$  

where the maximization is taken over all quantum states $\rho$ and measurements $M$ compatible with the probability distribution $P$.

In all these cases, the number of random bits that can be extracted per run is quantified by the min-entropy

$$H_{\infty}(G) = -\log_2 G.$$  

FIG. 1. Three different levels of trust that we are considered. (top) In the case no device is trusted we are in the device-independent level of trust. Bell inequality are needed to certify the random number generated. (middle) If Bob’s device is trusted only, we are in a semi-device-independent level of trust. We use a linear steering inequality to certify random number generated. (bottom) If both devices are trusted, we are in the tomography level of trust. In principle one can perform a tomography to recover the state measured exactly.
B. Randomness from several settings

One may consider extracting randomness out of several pairs of settings, rather than a single one \((u, v)\) \[16\]. This is going to be advantageous for Alice and Bob only if the person who is supposed to guess, Charlie, is not allowed to hold a purification of their state. Let us explain this point in detail:

- If Charlie holds a purification of \(\rho\), upon learning which settings have been used in a given run, he can steer \(\rho\) to the decomposition that maximizes \[3\] for those settings. In such a situation, therefore, there is no advantage for Alice and Bob to use several pairs of settings: they should just stick to the \((u, v)\) that gives the largest \(G(\rho, A_u, B_v)\).

- If Charlie does not hold a purification, he should be at least allowed to have the best classical information about the boxes, i.e. he is allowed to know a pure quantum state that describes each run. Crucially now, this knowledge is prior to the choice of the settings: these pure states must be chosen as to maximize the average guessing probability, and as it turns out the result falls shorter than the independent maximization of each term. In other words, Alice and Bob will have more randomness.

If one does not trust the provider and the latter is supposed to have unbounded quantum equipment (as is usually assumed in cryptography), then Charlie must be allowed to hold a purification of \(\rho\). But the other scenario has its own relevance: if one trusts the provider (call them “experimentalists”), it is reasonable to assume that neither they nor anyone else has done all the effort needed to keep a purification of all necessary degrees of freedom in a quantum memory until the settings are revealed, which may well be at the end of the collection of the data.

In what follows, whenever we present randomness bounds for several settings, it is understood that they refer to Charlie not having a purification. The case in which Charlie has a purification and performs independent measurements on each run is covered by the single-setting results.

III. DEVICE-INDEPENDENT LEVEL OF TRUST: TWO BLACK BOXES

Device-independence is the minimal level of trust. In this context, both Alice and Bob’s devices are considered as black boxes: the only information available is the probability distribution \(P\). The violation of a Bell inequality is a necessary condition for certifying randomness in this setting.

For concreteness, we only consider here the use of few (two or three) measurement settings for each party. Since many more settings could in principle be used to further probe the system at hand, the bounds we can obtain in this way come with no claim of optimality with respect to the device-independent level of trust. Nevertheless, this restriction makes the scenario relatively simple, so we can try to study a Bell inequality whose maximal violation certifies a maximal amount of randomness. Since we are considering scenarios in which Alice’s and Bob’s output are binary, the maximal amount of randomness is \(H_\infty = 2\) bits per run.

The simplest and most widely used Bell inequality is the one by Clauser, Horne, Shimony and Holt (CHSH), which uses \(m_A = m_B = 2\) buttons on each box. Among its many properties, it is known that its maximal violation \(S = 2\sqrt{2}\) can be obtained only with two-qubit maximally entangled states \[17\]. Even in such a limiting case, however, only \(H_\infty(P, u, v) = 1.23\) bits of global randomness can be extracted, because all pairs of measurements exhibit correlated statistics \[8\]. Now, from binary measurements on a certified maximally entangled state, one would expect to be able to extract two bits of randomness. This can be achieved by introducing a third measurement \(B_3\) on Bob side \[18\]. If, in the ideal case, the outcomes of \(B_3\) are fully correlated to the outcomes of \(A_1\), then they should be completely uncorrelated from those of \(A_2\), therefore, yielding \(H_\infty(P, 2, 3) = -\log_2 \max_{a,b} P(a, b|2, 3) = 2\) bits of global randomness in the ideal case.

Motivated by this observation, we are going to work with the modified CHSH inequality

\[
S = \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle + \langle A_1 B_3 \rangle \leq 3
\]

The maximum value of this modified CHSH inequality in quantum formalism is given by \(2\sqrt{2} + 1\). Our goal is now to calculate the amount of randomness that can be extracted per run, for any value of the observed violation, that is, to compute \(G\).

\[
G(P, 2, 3) = \max_{(\rho, A_2, B_3) \rightarrow P} G(\rho, A_2, B_3)
= \max_{(\rho_\lambda, A_2, B_3) \rightarrow P} \sum \lambda G(\rho_\lambda, A_2, B_3)
= \max_{(\rho_\lambda, A_2, B_3) \rightarrow P} \sum \lambda \max_{ab} P^\lambda(a, b|2, 3)
\]
where $\rho = \sum \rho_\lambda$, and $P^\lambda(a, b|2, 3)$ is a probability distribution achievable by quantum system (the states $\rho_\lambda$ need not be normalized here).

The number of values that $\lambda$ can take is a priori unbounded; however, for this optimization it is enough to consider four values of $\lambda$. The argument is given in Ref. [16]. In a nutshell, the reason is that all $\lambda$’s for which the inner maximization is achieved by the same arguments $(a, b)$ can be grouped together into a unique $\lambda$. Hence, the maximization in (7) can be rewritten as

$$\max_{\{P^\lambda\}, \lambda = 4} \sum \lambda P^\lambda(a_\lambda, b_\lambda|2, 3) \quad (8)$$

Subject to,

$$S = \sum_{abuv} c_{abuv} P(a, b|u, v)$$

$$\sum_\lambda P^\lambda(a, b|u, v) = P(a, b|u, v)$$

$$\forall a, b, u, v$$

$$P^\lambda(a, b|u, v) \in \mathbb{Q}$$

where $\lambda = (a, b)$, we denote by $a_\lambda(b_\lambda)$ the outcome of Alice(Bob) corresponding to some $\lambda$, $c_{abuv}$ is the coefficients corresponding to the modified CHSH inequality in [4], the value of $S$ is taken from 3 to $2\sqrt{2}+1$, and $\mathbb{Q}$ is the set of probability distributions achievable by measuring quantum systems. The third constraint cannot be efficiently implemented, but can be relaxed to the hierarchy of semi-definite programs (SDP) by Navascués, Pironio, and Acín [19], thus yielding an upper bound on the guessing probability. We performed this optimization with Yalmip [20] and SeDuMi [21] in Matlab for the relaxation to the set $\mathbb{Q}^2$. The result is shown in Fig. 2.

The optimization confirms that 2 bits of randomness can be extracted in the case of maximal violation, thanks to the third measurement setting. Note that 2 bits of randomness were already demonstrated in [15], but that example required the use of very partially entangled states, whereas the 2 bits achieved here are with a maximally entangled state. Some amount of randomness remains present in the outcomes for all values of the violation, as expected, since any violation of a Bell inequality certifies the presence of some intrinsic randomness.

IV. TOMOGRAPHY LEVEL OF TRUST: TWO WHITE BOXES

We move now to the other extreme case, in which both Alice and Bob’s devices are white boxes: the dimensionality of the degrees of freedom under study is considered known, the measurement devices are fully characterized, and the source is trusted to produce always the same state in each run (i.i.d.). Only the state itself may be initially unknown and needs to be characterized by tomography; once this is done, the users can choose the measurements that lead to extracting the largest amount of randomness.

Before continuing, let us notice that in this level of trust, two boxes are actually not needed: one quantum system already provides intrinsic randomness. For instance, if a qubit is prepared in the state $|+\rangle$, in each run, a measurement of $\sigma_z$ provides a perfect random bit. In this paper, we present the two-boxes case for ease of comparison with the other levels of trust that do require bipartite systems, but all the tools can be directly translated to the single-box case.

A. Tools

Since the state can be reconstructed, the guessing probability associated to intrinsic randomness is given by Eq. (3). However, similarly to what happened in the previous section, it is unclear how many quantum states $|\psi_\lambda\rangle$ one should consider in the maximization. Fortunately, the same argument as the one used above from Ref. [10] can be transposed here and applied to mixtures of density matrices, i.e. write $\rho = \sum \lambda \rho_\lambda$. It is thus sufficient to maximize the following expression

$$G(\rho, A, B) = \max_{\{\rho_\lambda\}_{\lambda = 4}} \sum_\lambda \text{Tr} \left[ \rho_\lambda \frac{1 + a_\lambda A}{2} \otimes \frac{1 + b_\lambda B}{2} \right] \quad (9)$$

FIG. 2. Lower bound on the amount of random bits can be extracted from the violation of modified CHSH inequality [6], based on the relaxation $\mathbb{Q}^2$ for the quantum set. The maximum possible amount of 2 random bits is extracted when $S$ reaches its maximum value $2\sqrt{2} + 1$. Some intrinsic randomness can be certified down to the local bound $S = 3$, where device-independent certification ceases to be possible.
with \( \rho = \sum_{\lambda} \rho_\lambda, \rho_\lambda \geq 0, \lambda = (a, b), \) with \( a = \pm 1, b = \pm 1. \) Such maximization is again a SDP, though a different one from the one discussed in the previous section: here, the matrix that must be positive is the quantum state itself, not a matrix of momenta of the observed statistics. Moreover, this SDP solves the problem of interest directly rather than a relaxation thereof.

Further, for the tomography level of trust, Alice and Bob can choose to extract randomness from any measurements, and will choose those for which the guessing probability in \( \mathcal{F} \) is the lowest. Hence, the guessing probability of a given state \( \rho \) is

\[
G(\rho) = \min_{A,B} G(\rho, A, B) \tag{10}
\]

As we said in section \(|\underline{11}\underline{B}|\) instead of just extracting randomness from only one pair of measurement settings, if Charlie is not allowed to hold a purification of the state it may be advantageous to use more settings. Let us consider extracting randomness from two pairs of measurement settings, \((u, v) = (1, 1)\) and \((u, v) = (2, 2)\), chosen with equal probability. The maximization is then written as follows:

\[
G(\rho, A_1, B_1; A_2, B_2) = \max_{\rho_\lambda} \sum_{\lambda} \frac{1}{2} \left( \text{Tr}(\rho_\lambda M_1^{a\lambda} \otimes M_1^{b\lambda}) + \text{Tr}(\rho_\lambda M_2^{a\lambda} \otimes M_2^{b\lambda}) \right) \tag{11}
\]

where \( M_u^a \) and \( M_u^b \) are the projectors of measurements \( A_u, B_v, \) and the unnormalized states \( \rho_\lambda \) must be such that \( \rho = \sum_{\lambda} \rho_\lambda \), with \( \lambda = (a, b, a', b') \). In this case, therefore, sixteen \( \lambda \)'s are needed for the maximization.

B. An explicit example

Any explicit calculation will obviously depend on the actual state determined by tomography. In order to illustrate the method, we choose the theorists’ favorite family of two-qubit states, namely the Werner states

\[
W(\eta) = |\Psi^-\rangle \langle \Psi^-| + (1 - \eta) I \otimes 1/4
\]

For this state, it is easy to guess that an optimal choice of settings satisfying \(|\underline{10}|\) is \( A = \sigma_x \) and \( B = \sigma_z \). Then, we perform the maximization in \(|\underline{9}|\). The result obtained for extracting randomness from measurements \((A, B)\) are shown in Fig. 3. Note that randomness can be extracted for all values of \( \eta > 0. \) This is because both parties’ measurements are trusted, and we restrict the state between them as the Werner state, thus some correlations still exist as long as the state between them is not white noise.

For the case of extracting randomness from two pairs of settings, we choose where \( A_1 = \sigma_x, A_2 = \sigma_x, B_1 = \sigma_z, B_2 = \sigma_z \). The result for this optimization is shown in Fig. 3. Interestingly, non-zero randomness can be extracted even when the tomography reveals white noise (see Appendix \(|\underline{A}|\) for an analytical derivation of that limiting value). This is due to the fact that the two pairs of measurements are trusted not to be compatible — again, the same would happen for a single qubit: even if the effective state is \( 1/2 \), nobody who does not hold a purification can predict perfectly the outcomes of both \( \sigma_x \) and \( \sigma_z \).

V. SEMI-DEVICE INDEPENDENT LEVEL OF TRUST: ONE BLACK BOX AND ONE WHITE BOX

After considering the two extreme levels of trust, we consider the intermediate one, which consists of one black box on Alice’s side and one white box on Bob’s side. This semi-device-independent level of trust, to our knowledge, has never been considered before in the context of randomness.

The scenario is very similar to steering \(|\underline{22}|\underline{23}|\): the setup is actually the same, but the figure of merit is different. Indeed, instead of having Alice to convince Bob that she can steer his state, we just let them perform their measurements locally and ask whether randomness can be extracted from their outcomes. Once again, it is not our goal to provide a bound over all possible steering-like protocols (assuming it were possible at all): rather, we want
to illustrate how such a level of trust can be studied. We do this by considering a concrete example, which will later be used for comparison with the two extreme cases.

Explicitly, we consider that Bob’s system is a qubit and base ourselves on the linear steering inequalities proposed in Ref. [24] for n=2:

\[ S_2 = \frac{1}{2}((A_1 B_1) + (A_2 B_2)). \]  

(12)

Here \( A_1 \)'s are Alice’s measurements and Bob’s observables \( B_1 \) and \( B_2 \) correspond to qubit measurements \( \vec{b}_1 \cdot \vec{\sigma} \) and \( \vec{b}_2 \cdot \vec{\sigma} \). We choose \( \vec{b}_1 \perp \vec{b}_2 \). The maximum value that can be achieved by quantum formalism then is 1; non-steerable states can reach at most \( 1/\sqrt{2} \).

The amount of random bits extracted can be computed by solving the optimization in [14]

\[ G(P, A, B) = \min_B \max_{\rho, A} G(\rho, A, B) \]

\[ = \min_B \max_{\{q_x, \psi_x\}, A} \sum_{\lambda} q_{\lambda} G(|\psi_{\lambda}\rangle, A, B) \]

Such that

\[ S_2 = \sum_{\lambda} q_{\lambda} S_{2}^\lambda \text{ fixed value} \]

\[ \vec{b}_1 \perp \vec{b}_2 \]  

(13)

where \( \rho = \sum_{\lambda} q_{\lambda} |\psi_{\lambda}\rangle \langle \psi_{\lambda}| \). It is interesting to notice that one has to maximize over \( (\rho, A) \), while one can minimize over \( B \). Indeed, Bob has a white box, so he can choose the measurements that gives the minimum guessing probability; while \( (\rho, A) \) are unknown, so one has to consider the worst case. Without loss of generality we consider the anticommuting measurements of Bob to be \( \sigma_x \) and \( \sigma_z \).

We solve the optimization in [13] in two steps: first we bound the guessing probability under the assumption that the state is pure, that is, we find the concave function \( f \) such that

\[ \max_{\psi, A} G(|\psi\rangle, A, B) \leq f(S_2(\psi)). \]  

(14)

The second step consists in noticing that since \( f \) is concave, i.e. \( \sum_{\lambda} q_\lambda f(S_{2}^\lambda) \leq f(\sum_{\lambda} q_\lambda S_{2}^\lambda) \), then

\[ \max_{\rho, A} G(\rho, A, B) = \max_{\{q_x, \psi_x\}, A} \sum_{\lambda} q_{\lambda} G(|\psi_{\lambda}\rangle, A, B) \]

\[ \leq \max_{\{q_x, \psi_x\}, A} \sum_{\lambda} q_{\lambda} f(S_{2}^\lambda) \]

\[ \leq \max_{\{q_x, \psi_x\}, A} f(\sum_{\lambda} q_{\lambda} S_{2}^\lambda) \]

\[ = \max_{\rho, A} f(S_2) \]

where we have written \( S_{2}^\lambda \equiv S_2(|\psi_{\lambda}\rangle) \). Hence, the bound on the guessing probability \( \{14\} \) obtained for pure states will be actually valid for any state.

In order to compute the function in \( \{14\} \), we consider the Schmidt decomposition of \( |\psi\rangle \); since Bob’s system is trusted to be a qubit, Alice has an effective qubit. In this case, Alice’s measurement can be regarded as POVMs on a qubit space. Hence, \( \{14\} \) can be rewritten as

\[ \max_{\psi, A'} G(|\psi'\rangle, A', B) \leq f(S_2(\psi)) \]  

(15)

where \( |\psi'\rangle \) is a two qubit pure state, and \( A' \) is the POVM. We compute the the bound above numerically using optimization function in MATLAB, with the following parametrization,

\[ |\psi'\rangle = (1 \otimes U_B)(|\cos \theta |00\rangle + |\sin \theta |11\rangle) \]

\[ A_1 = a_1(1 + \vec{a}_1 \cdot \vec{\sigma}) \]

\[ B_1 = \sigma_x, \ B_2 = \sigma_z \]  

(16)

where \( U_B = e^{i \phi \vec{a}_1 \cdot \vec{\sigma}} \) is a local unitary acting on Bob’s space, which is needed because we have fixed Bob’s measurements, and the computational basis for Schmidt decomposition might not be the same as Bob’s measurements basis. Notice that, contrary to the previous optimizations, which were SDPs, this 12-variable optimization has to be performed with heuristic optimization algorithms. We performed it several times with independent random initial starting points to be confident that the global optimum was attained.

The result of the optimization, for randomness extracted out of \( A_1 \) and \( B_2 \), is shown in Fig. 3. The function \( f(S) \) being manifestly concave, by the argument given above this curve is actually the amount of randomness that can be extracted even when one drops the assumption that the state is pure.

This result has several features worth commenting after we notice that no randomness can be extracted when \( S_2 \leq 1/2 \); and below the steering bound \( S_2 \leq 1/\sqrt{2} \), one cannot extract any randomness from Alice. In the semi-device independent level of trust, Bob’s measurements are trusted, but not Alice’s. If the correlations between them are not steerable, then they can be written as

\[ P(a, b|u, v) = \sum_{\lambda} p_{\lambda} P(a|u, \lambda) P_Q(b|v, \lambda) \]  

(17)

where \( P_Q(b|v, \lambda) \equiv \text{Tr}(\rho_B M^\lambda_b) \) is quantum correlation with expected measurement operator \( M^\lambda_b \).
be achieved by LHS models is thus given by $S^{\text{incompatible}}$. The maximum value of $S^{\text{incompatible}}$ is therefore $1$ when $S^2 = 1$, while no randomness can be extracted when $S^2$ reaches $1/2$. However, Alice’s local random bits drop to $0$ when $S^2 = 1/\sqrt{2}$, which is the steering bound.

This constitutes a Local Hidden State (LHS) model, where Bob holds a local quantum state that is not entangled to Alice’s system. For this model, the steering inequality [12] becomes

$$S^2 = \frac{1}{2} \sum_{\lambda} p_{A_i} \left( \langle A_{1,\lambda} \rangle \langle B_{1,\lambda} \rangle + \langle A_{2,\lambda} \rangle \langle B_{2,\lambda} \rangle \right) \tag{18}$$

To maximize the value of $S^2$ with such model, one can choose to set $\langle A_{i,\lambda} \rangle = 1 \forall i, \lambda$, which gives

$$S^2 = \frac{1}{2} \sum_{\lambda} p_{A_i} \left( \langle B_{1,\lambda} \rangle + \langle B_{2,\lambda} \rangle \right) \tag{19}$$

We can’t do the same for Bob’s outcomes, however, as his measurements are quantum and maximally incompatible. The maximum value of $S^2$ that can be achieved by LHS models is thus given by

$$S^2 = \frac{1}{2} \sum_{\lambda} p_{A_i} \left( \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} \right) \leq \frac{1}{\sqrt{2}}, \tag{20}$$

i.e. the steering bound for $S^2$. Thus we see that it is possible to achieve the steering bound with deterministic outcomes for Alice, and so no randomness can be found here anymore.

On the other hand, if we are focusing on extracting randomness from measurements $A_1$ and $B_2$, choosing $\langle B_{1,\lambda} \rangle = 0, \langle B_{2,\lambda} \rangle = 1$, can yield $\max_{a,b} P(a,b|A_1B_2) = 1$, i.e. no randomness, whenever $S^2 \leq 1/2$. Again, this explains that no more joint randomness is found in this region. Note however that in the interval $S^2 \in [1/2, 1/\sqrt{2}]$, the steering inequality is not violated anymore, but randomness is still found in the joint outcomes $A_1, B_2$.

As we have done in tomography level of trust, by extracting randomness from two measurement settings that are not compatible to each other, one could also extract some randomness from the trusted system by using all its settings. Indeed, just like for the tomography case, one cannot guess both outcomes with certainty for measurements $\sigma_2$ and $\sigma_2$. For $S^2$, we choose two pairs of measurement settings, $(u, v) = (1, 2)$ and $(u, v) = (2, 1)$ with equal probability. The solid line represents the global randomness, dashed line represents the Alice’s local randomness, and dash-dotted line represents Bob’s local randomness. After $S^2$ reaches steering bound, only Bob’s local randomness contributes to global randomness.

We observed that one can always extract some randomness for any value of $S^2$ by using two pairs of measurement settings. Moreover, the global randomness is only contributed by Bob’s local randomness when $S^2$ reaches its steering bound, $1/\sqrt{2}$. It is because, as one can see in (19), $\langle B_1 \rangle$ and $\langle B_2 \rangle$ can not be equal to one at the same time, which implies that the outcomes can not be guessed with certainty simultaneously. Alice’s local randomness, however, reduces to zero when $S^2$ reaches steering bound, as one do not know or constrain her measurements and system.

### VI. COMPARISON OF THE THREE LEVELS OF TRUST

In order to compare the different level of trust, ideally we should analyze a unique setup in the three cases. However, the optimal measurements are not the same for the device-independent and semi-device-independent levels of trust: in other words,
if a vendor produces a box that is optimal for one level of trust, that same box will perform poorly in the other level of trust. But we can compare each with the tomography level of trust, and we can do it by assuming that the quantum state is always a Werner state of two qubits [12].

We first start off with the comparison between the device-independent and the tomography levels of trust. We let Alice’s system have two measurements, and Bob’s system three measurements, where

- \( A_1 = \sigma_x, A_2 = \sigma_z, B_1 = (\sigma_z + \sigma_x)/\sqrt{2}, \)
- \( B_2 = (\sigma_z - \sigma_x)/\sqrt{2}, B_3 = -\sigma_x. \)

In the device-independent case, we are only interested in the modified CHSH inequality in [6], where \( S' = (2\sqrt{2} + 1)\eta, \) and compute the guessing probability of pair of measurements \((u, v) = (2, 3)\). In tomography, we compute the guessing probability in [2] and [10] by using the pair of measurement settings \((u, v) = (2, 3)\) as well. The comparison of both levels of trust with Werner state is shown in Fig. 6.

Note that we can choose to extract randomness from two or more pairs of measurement settings in this case. However, there is no obvious choice of measurement settings other than \((u, v) = (2, 3)\), which gives 2 uncorrelated bits when \( \eta = 1. \) Moreover, for device-independent, there will be no randomness extracted when \( S' \) in [6] reaches its local bound.

Then, we continue our discussion by comparing the semi-device-independent and the tomography levels of trust. In this case, we let Alice and Bob’s system have two measurements, where \( A_1 = \sigma_x, A_2 = \sigma_z, B_1 = \sigma_x, B_2 = \sigma_z, \) and the pair of measurement settings \((u, v) = (1, 2)\) is used to extract the randomness. For the semi-device-independent case, the quantity that we are interested is \( S_2 \) value in [12], where \( S_2 = \eta \) if the state is a Werner state.

For tomography, we replace the pair of measurement settings in [10] with \((u, v) = (1, 2)\), and compute the maximization. The result is shown in Fig. 7.

In this comparison, it is useful for us to compare also the case in which two pairs of measurement settings, \((u, v) = (1, 2)\) and \((u, v) = (2, 1)\) are used to extract randomness. When both measurement settings are chosen with equal probability, the amount of randomness that can be extracted is as shown in the Fig. 8.

As shown in the figure, some amount of randomness can be extracted for all Werner state, including white noise. For semi-device independent, at least 0.228 bits can be extracted, which is contributed by Bob’s local randomness. In the case of tomography, at least 0.415 bits can be extracted, even if the state becomes white noise.
VII. CONCLUSION

In this work, we compared the randomness that can be extracted from a given quantum device with the device-independent, semi-device-independent, and tomographic level of trust. We have shown that one can extract up 2 bits of randomness in all levels of trust. Moreover, we also showed that the amount of random bits increased by relaxing one of the devices to white box in device independent level of trust. Furthermore, by using two pairs of measurement settings that are incompatible to each other to extract randomness, at least some amount of random bits can be extracted from white box.

ACKNOWLEDGMENT

This work is funded by the Singapore Ministry of Education (partly through the Academic Research Fund Tier 3 MOE2012-T3-1-009) and by the Singapore National Research Foundation.

[1] J. S. Bell, Physics (Long Island City, N.Y.) 1, 195 (1964).
[2] V. Scarani and N. Gisin, Physical Review A 65, 012311 (2002).
[3] C. Brukner, M. Zukowski, J. W. Pan, and A. Zeilinger, Physical Review Letters 92, 127901 (2004).
[4] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, arXiv preprint arXiv:1303.2849 (2013).
[5] V. Scarani, Acta Physica Slovaca 62, 247 (2012).
[6] T. Moroder, J.-D. Bancal, Y.-C. Liang, M. Hofmann, and O. Gühne, Phys. Rev. Lett. 111, 030501 (2013).
[7] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Physical Review Letters 98, 230501 (2007).
[8] S. Pironio, A. Acín, S. Massar, A. B. de La Guardia, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al., Nature 464, 1021 (2010).
[9] R. Colbeck and A. Kent, Journal of Physics A: Mathematical and Theoretical 44, 095305 (2011).
[10] In fact, several recent works have shown that quantum behaviour can still be certified if the amount of signaling, or of allowed measurement dependence, is duly limited. While certainly of great conceptual interest, there does not seem to be a natural way to justify a specific limit: if an adversary has inserted a radio in the devices, for instance, it is unclear why she would limit her transmission to less than one bit.
[11] A. Acín, N. Gisin, and L. Masanes, Physical Review Letters 97, 120405 (2006).
[12] H.-K. Lo, M. Curty, and B. Qi, Physical Review Letters 108, 130503 (2012).
[13] M. Pawłowski and N. Brunner, Physical Review A 84, 010203(R) (2011).
[14] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. Wiseman, Physical Review A 85, 010301(R) (2012).
[15] A. Acín, S. Massar, and S. Pironio, Physical Review Letters 108, 100402 (2012).
[16] J.-D. Bancal, L. Sheridan, and V. Scarani, arXiv preprint arXiv:1309.3894 (2013).
[17] S. Popescu and D. Rohrlich, Physics Letters A 169, 411 (1992).
[18] P. Mironowicz and M. Pawłowski, Physical Review A 88, 032319 (2013).
[19] M. Navascués, S. Pironio, and A. Acín, New J. Phys. 10, 073013 (2008).
[20] J. Lofberg, in Computer Aided Control Systems Design, 2004 IEEE International Symposium on (IEEE, 2004) pp. 284–289.
[21] J. Sturyn, Department of Econometrics, Tilburg University, The Netherlands 2003 (1998).
[22] S. J. Jones, H. M. Wiseman, and A. C. Doherty, Physical Review A 76, 052116 (2007).
[23] E. G. Cavalcanti, S. J. Jones, H. M. Wiseman, and M. Reid, Physical Review A 80, 032112 (2009).
[24] D. J. Saunders, S. J. Jones, H. M. Wiseman, and G. Pryde, Nature Physics 6, 845 (2010).

Appendix A: Randomness from white noise

We perform here the analytical optimization of (11) for $\eta = 0$ i.e. for the state $W(0) = I \otimes \frac{1}{4}$. The SDP algorithm provided the value $G(W(0), A_1, B_1, A_2, B_2) = 0.75$ up to numerical precision (which corresponds to $H_\infty \approx 0.415$, cf. Fig. 3).

Inserting into (11) the explicit form of the operators

$$M_1^a = \frac{1 + a\sigma_x}{2}, \quad M_2^a = \frac{1 + a'\sigma_z}{2},$$

$$M_1^b = \frac{1 + b\sigma_z}{2}, \quad M_2^b = \frac{1 + b'\sigma_x}{2},$$

(A1)
one has

\[ G(W(0), A_1, B_1, A_2, B_2) = \max_{\{\rho_\lambda\}} \sum_\lambda O(\lambda) \]  

(A3)

with

\[ O(\lambda) = \frac{1}{8} \left[ (1 + a\sigma_x) \otimes (1 + b\sigma_z) + (1 + a'\sigma_z) \otimes (1 + b'\sigma_x) \right]. \]  

(A4)

The maximum is to be taken over sets of sixteen non-normalized positive operators such that \( \sum_\lambda \rho_\lambda = W(0) \).

Now, the largest eigenvalue of each \( O(\lambda) \) is easily found to be \( \frac{3}{4} \); denoting \( |\psi_\lambda\rangle \) the corresponding eigenvector, one can verify that the choice \( \rho_\lambda = \frac{1}{16} |\psi_\lambda\rangle \langle \psi_\lambda| \) satisfy indeed \( \sum_\lambda \rho_\lambda = W(0) \). Consequently, \( G(W(0), A_1, B_1, A_2, B_2) = \frac{3}{4} \), as claimed.

The states \( |\psi_\lambda\rangle \) are entangled: for instance,

\[ |\psi_{++++}\rangle = \frac{2|00\rangle + |01\rangle + |10\rangle}{\sqrt{6}}. \]  

(A5)

This is pretty obvious from the structure of the operator; it is nevertheless intriguing, given the nature of the task. Recall what is the scenario: Charlie is allowed to put a state of his choice into the boxes, drawn from a mixture that looks maximally mixed to Alice and Bob. Since Alice and Bob are going to generate randomness by measuring either \( (\sigma_x, \sigma_z) \) or \( (\sigma_z, \sigma_x) \), Charlie has better chances to guess the outcomes by decomposing the maximally mixed state on entangled state. If Bob would restrict to product states, the probability of guessing would be \( \frac{1}{8}(3 + 2\sqrt{2}) \approx 0.73 \) with a corresponding min-entropy \( H_\infty \approx 0.46 \).