
Peer reviewed version

License (if available): Unspecified

Link to published version (if available): 10.1103/PhysRevA.95.042340

Link to publication record in Explore Bristol Research

PDF-document

This is the author accepted manuscript (AAM). The final published version (version of record) is available online via APS at https://journals.aps.org/pra/abstract/10.1103/PhysRevA.95.042340. Please refer to any applicable terms of use of the publisher.

University of Bristol - Explore Bristol Research

General rights

This document is made available in accordance with publisher policies. Please cite only the published version using the reference above. Full terms of use are available: http://www.bristol.ac.uk/red/research-policy/pure/user-guides/ebr-terms/
Measurement-device-independent entanglement and randomness estimation in quantum networks

Ivan Šupić,1 Paul Skrzypczyk,2 and Daniel Cavalcanti1

1ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain
2H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, United Kingdom

(Dated: March 16, 2017)

Detection of entanglement in quantum networks consisting of many parties is one of the important steps towards building quantum communication and computation networks. We consider a scenario where the measurement devices used for this certification are uncharacterised. In this case, it is well known that by using quantum states as inputs for the measurement devices it is possible to detect any entangled state (a situation known as measurement device-independent entanglement witnessing). Here we go beyond entanglement detection and provide methods to estimate the amount of entanglement in a quantum network. We also consider the task of randomness certification and show that randomness can be certified in a variety of cases, including single-partite experiments or setups using only separable states.

I. INTRODUCTION

Quantum entanglement is one of the most intriguing aspects of quantum theory [2]. Implications of its existence on the foundations of quantum theory were already emphasized in the seminal work of Einstein, Podolsky, and Rosen [1]. In the last few decades entanglement has been at the core of the power of quantum theory for different information processing tasks [2]. Moreover, it allows quantum systems to display nonlocal correlations, which can be certified by the violation of Bell inequalities [3, 4]. Thus, whenever a Bell inequality violation is observed one certifies that the underlying quantum system is entangled. Importantly, this certification is done without the need to know which measurements are being performed (in contrast to the case of entanglement witnesses [2]). We can thus say that the observation of nonlocal correlations certifies entanglement in a device-independent way [4].

The relation between Bell nonlocality and entanglement is one of the open questions in the foundations of quantum theory. While nonlocal correlations can only be obtained by performing local measurements on an entangled state, not every entangled state can lead to nonlocality. As it was first shown by Werner [5] the probability distributions obtained by local measurements applied to certain entangled quantum states can be simulated by a purely classical model called a local-hidden-variable model. Werner’s result was latter generalised in many ways [6–17].

Since the standard Bell scenario exposes a gap between nonlocality and entanglement, one may ask if it is possible to come up with some alternative scenario in which every entangled state will exhibit nonlocal correlations. One possibility is to make use of many copies of the shared entangled state. It has been proven that some entangled states which are not nonlocal in the standard Bell scenario can violate a Bell inequality in this scenario [18, 19], a phenomenon known as super-activation. Whether every entangled state can be super-activated in this way is again an open problem. Another possibility is to consider a quantum network consisting of many copies of the same state shared among many parties [20–22]. Similarly to superactivation, some states that are local in the standard Bell scenario become nonlocal in the network scenario. However, the general relation between entanglement and nonlocality is also unknown in this case. Another alternative Bell scenario, historically preceding the others, was suggested in [23] (see also [11]) and is known as the hidden nonlocality scenario. In it the parties are allowed to perform pre-processing on their shared state before applying their measurements. Even though some local entangled states can become nonlocal in this new scenario it has recently been shown that there are entangled states which can never exhibit hidden nonlocality, i.e. they remain nonlocal after arbitrary pre-processing [24]. Finally, it is possible to combine all the non-standard Bell scenarios, but still there is no conclusive statement about the relation between entanglement and nonlocality in what would be called multy-copy with pre-processing scenario.

There is however one modification of the standard Bell scenario that can reveal nonlocal correlations from every entangled state. It consists of using measurement devices that receive quantum systems as inputs [25] (See also [26, 28, 29, 59] for further developments and [30, 31, 33] for experimental demonstrations). The observation of nonlocal correlations in this scenario can be seen as an entanglement test with uncharacterised measurements, which motivated the name of measurement-device-independent nonlocality.

The aim of this paper is to shed new light on some aspects of this new scenario with quantum inputs, explore its power for entanglement detection and quantification in quantum networks, and finally to study randomness certification in this scenario.

II. MEASUREMENT-DEVICE-INDEPENDENT ENTANGLEMENT CERTIFICATION

We start by reviewing some of the main results on entanglement certification in Bell scenario with quantum inputs, and

* ivan.supic@icfo.eu
by proposing some improvements on this task. We consider two separated parties, Alice and Bob, sharing a bipartite system in an unknown state \( \rho_{AB} \in \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B) \). They want to certify if their system is entangled, but do not know how their measurement devices work. Buscemi proposed a solution to this problem [25]: at each round of the experiment Alice and Bob encode their measurement choices in quantum states \( \psi_A \in \mathcal{L}(\mathcal{H}_A) \) and \( \psi_B \in \mathcal{L}(\mathcal{H}_B) \), respectively, which they use as inputs for their measurement devices. After receiving the quantum inputs the measurement devices provide classical outputs \( a \) and \( b \) according to the probability distributions

\[
p(a,b|\psi_A, \psi_B) = \text{Tr}([M_a^{AB} \otimes M_b^{B\!\!B\!\!B}] (\psi_X^A \otimes \rho_{AB} \otimes \psi_Y^B)), \tag{1}
\]

where \( M_a^{AB} \) and \( M_b^{B\!\!B\!\!B} \) are the measurement operators applied by the measurement devices on the corresponding input systems and their shares of state \( \rho_{AB} \). Buscemi proved that if \( \{\psi_A(x)/\psi_B(y)\} \) correspond to tomographically complete sets of input states \(^1\) in \( \mathcal{A}_A \mathcal{B}_B \), and each box performs a Bell state measurement, then every entangled state \( \rho_{AB} \) produces a set of probability distributions \( \{p(a,b|\psi_A, \psi_B)\}_{a,b,x,y} \) that cannot be reproduced with any separable state.

Building on Buscemi’s result, the authors of [26] provided a method of constructing Bell tests with quantum inputs from every entanglement witness, and named them measurement-device-independent entanglement witnesses (MDIEW). However, when it comes to practical entanglement detection, MDIEW are useful only when one has a good guess on which entangled state should be detected, and can thus start from an entanglement witness which is able to detect its entanglement. This problem was first addressed in [32], where it was shown that given multiple copies of the state then a universal witness can be found. More recently, in [33] solution at the single copy level was given, by showing that the quantum inputs scenario can be cast as a semidefinite programming (SDP) optimization problem [34], readily solvable with available software. We present here the said SDP in a slightly different form.

The starting point is the fact that the joint outcome probability distribution can be written in the following way

\[
p(a,b|\psi_A, \psi_B) = \text{Tr}([M_a^{AB} \otimes M_b^{B\!\!B\!\!B}] (\psi_X^A \otimes \rho_{AB} \otimes \psi_Y^B)), \tag{2}
\]

where \( M_{a,b} \) is an effective POVM operator defined by

\[
\tilde{M}_{a,b} = \text{Tr}_{AB}([M_a^{AB} \otimes M_b^{B\!\!B\!\!B}] (I_A^B \otimes \rho_{AB} \otimes I_B^B)), \tag{3}
\]

By construction, the effective POVM \( \tilde{M}_{a,b} \) satisfies a number of conditions, which can be thought of as playing the role of ‘no-signalling’ conditions. In particular,

\[
\begin{align*}
\sum_a \tilde{M}_{a,b} &= I^B \otimes \tilde{M}_b^B, \\
\sum_b \tilde{M}_{a,b} &= M_a^{AB} \otimes I^B
\end{align*}
\tag{4}
\]

where \( \tilde{M}_b^B = \text{Tr}_{AB}[[M_b^{B\!\!B\!\!B} (I^B \otimes \rho_{AB}^A)] \geq 0 \) and \( \tilde{M}_a^{AB} = \text{Tr}_{B}[[M_a^{AB} (I^B \otimes \rho_{AB}^A)] \geq 0 \) are effective local POVMs for Alice and Bob (i.e. such that \( \sum_a \tilde{M}_{a}^{AB} = I^A \) and \( \sum_b \tilde{M}_{b}^B = I^B \). We will write \( \{\tilde{M}_{a,b} \}_{a,b} \in \mathcal{M} \) to denote the fact that the effective POVM satisfies these conditions, i.e.

\[
\mathcal{M} = \left\{ \{\tilde{M}_{a,b}\}_{a,b} | \tilde{M}_{a,b} : \sum_a \tilde{M}_{a,b} = I^A \otimes \tilde{M}_b^B, \sum_b \tilde{M}_{a,b} = M_a^{AB} \otimes I^B \right\} \tag{5}
\]

Now, if the shared state \( \rho_{AB} \) is separable, i.e. \( \rho_{AB} = \Sigma_\lambda p_\lambda \rho_\lambda^A \otimes \rho_\lambda^B \), then (3) becomes

\[
\tilde{M}_{a,b} = \sum_\lambda \rho_\lambda \text{Tr}_A [M_a^{AB} (I_B^B \otimes \rho_\lambda^A)] \otimes \text{Tr}_B [M_b^{B\!\!B\!\!B} (\rho_\lambda^B \otimes I^B)]
\]

where \( \tilde{M}_a^{AB} \) and \( \tilde{M}_b^B \) are effective local POVMs for Alice and Bob. Consequently, the fact that \( \rho_{AB} \) is separable, implies that the operator \( \tilde{M}_{a,b} \) is a separable operator for all \( a \) and \( b \).

Alice and Bob can thus check the separability of \( \rho_{AB} \) by solving the following feasibility problem:

\[
\text{given } \left\{ p(a,b|\psi_A, \psi_B) \right\}_{a,b,x,y} \quad \text{find } \left\{ \tilde{M}_{a,b} \right\}_{a,b} \tag{7}
\]

s.t. \( p(a,b|\psi_A, \psi_B) = \text{Tr}([\tilde{M}_{a,b} (\psi_X^A \otimes \psi_Y^B)] \quad \forall a,b,x,y, \{\tilde{M}_{a,b} \}_{a,b} \in \mathcal{J} \)

where \( \mathcal{J} \) denotes the subset of \( \mathcal{M} \) which are separable operators, i.e.

\[
\mathcal{J} = \left\{ \left\{ \tilde{M}_{a,b} \right\}_{a,b} | \tilde{M}_{a,b} : \sum_\lambda \tau_\lambda \otimes \chi_\lambda \geq 0, \tau_\lambda \geq 0 \right\} \tag{8}
\]

This problem is in principle hard to solve, due to the lack of the efficient characterization of the set of separable operators. However one can relax the constraint of separability, and impose instead that each operator \( \tilde{M}_{a,b} \) is positive under partial transpose (PPT). In the feasibility problem above this amounts to replacing the condition \( \sum_\lambda \tau_\lambda \otimes \chi_\lambda \geq 0, \tau_\lambda \geq 0 \) by \( (\tilde{M}_a^{AB} \tau_{0}^A) \tau_{0}^B \geq 0 \forall a,b \). With this replacement, the problem

\(^1\) By a tomographically complete set of input states we mean that the set is sufficient to perform quantum process tomography.
becomes a feasibility SDP optimisation problem, which can then be solved efficiently.

Notice however that this relaxation is not able to detect PPT entangled states. A second, more stringent, relaxation of the set of separable operators is the set of the operators having a $k$-symmetric extension [35]. Imposing that the operators $\tilde{M}_{a,b}^{k}$ have a $k$ symmetric extension amounts to demanding that there exist a $(k+1)$-partite operator $\tilde{N}_{a,b}^{k} = 0$ such that $\tilde{N}_{a,b}^{k} = M_{a,b}^{k}$ $\forall$ $i$. For every fixed $k$, the above feasibility optimisation problem with this replacement is again a SDP feasibility problem, which now can also detect PPT entangled states [36]. Finally, we note that by increasing the order $k$ of the extension, we obtain stronger SDP tests that converge to the separability test above in the limit of $k \to \infty$.

Finally, it is an important fact that once the sets of quantum inputs used are tomographically complete, then the probabilities $p(a,b|\psi_x,\psi_y)$ allow for an exact reconstruction of the effective POVM elements $\tilde{M}_{a,b}^{k}$, using quantum process tomography. In this special case, any available entanglement criterion, not just those that can be checked via SDP, can be used to determine if it is a separable operator or not, leading directly to a conclusion of whether or not the shared state was entangled.

### III. MEASUREMENT-DEVICE-INDEPENDENT ENTANGLEMENT ESTIMATION

One step beyond certifying the presence of entanglement in a system is to estimate how much entanglement it contains. There are many different entanglement measures, but they are in general not easy to compute even if one knows the full state of the system (for more details on entanglement measures see [37]). In fact the problem of deciding if a given quantum state is entangled is NP-hard, which implies hardness of computing entanglement measures [38]. Quantification of entanglement in a measurement-device-independent scenario was the subject of [39] where the authors define the best possible pay-off in a semiquantum games that a state can achieve as an entanglement measure. In what follows we show how to place measurement-device-independent bounds on two well-known entanglement quantifiers, the robustness [40] and the negativity [41].

#### A. MDI lower bound on the robustness of entanglement

A physically well motivated way of quantifying entanglement is through its robustness to noise [40], defined as the amount of noise one can add to an entangled state before it becomes separable. In mathematical terms, the generalised robustness $r_g$ of a state $\rho$ is given by

$$r_g(\rho^{AB}) = \min_{\sigma^{AB}} \frac{\rho^{AB}}{1 + r_g^{\rho^{AB}}}$$

where $S$ is a subset of quantum states, which defines the type of robustness, and $SEP$ denotes the set of separable states. Typical choices for $S$ include the set of all quantum states (generalised robustness), the set of separable states (robustness) or the maximally mixed state (random robustness).

In a similar way we define the robustness of MDI-nonlocality $r_S^{MDI}$ as the minimum amount of noise that has to be added to the set of probability distributions $\{p(a,b|\psi_x,\psi_y)\}_{a,b,x,y}$ before it can be reproduced by a separable state, where the noise comes from the set $S$. Formally, the MDI-nonlocality robustness is the solution of the following optimization problem

$$r_S^{MDI} [p(a,b|\psi_x,\psi_y)] = \min_{\{\tilde{M}_{a,b}^{k}\}_{a,b}} r_S$$

subject to

$$p(a,b|\psi_x,\psi_y) + r \pi(a,b|\psi_x,\psi_y)$$

where $\pi_S$ is the set of effective POVMs associated to the noise $S$. For example, for the generalised robustness, when $S = \{I/\rho\}$, then $\pi_S = \{I\}$. Similarly, for the robustness, when $S = \{I/\rho\}$, then $\pi_S = \{I/\rho\}$.

We now show that $r_S^{MDI}$ is a lower bound to the robustness of entanglement $r_S$ of the underlining state being measured. To see this consider that the robustness of the state $\rho^{AB}$ is given by $r_S^{\rho^{AB}}$. This means that there exist a state $\sigma^{AB} \in S$ for which the state $(\rho + r_S^{\rho^{AB}}/1 + r_S^{\rho^{AB}})$ is separable. Thus for any POVMs $\{M_{a}^{A}\}_{a}$ and $\{M_{b}^{B}\}_{b}$ satisfying (1),

$$\tilde{M}_{a,b}^{k} = \text{Tr}_{AB} \left[ \left( M^{A}_{a} \otimes M^{B}_{b} \right) \left( \rho \otimes \frac{\sigma^{AB} + r_S^{\rho^{AB}}}{1 + r_S^{\rho^{AB}}} \otimes I \right) \right]$$

and

$$\tilde{N}_{a,b}^{k} = \text{Tr}_{AB} \left[ \left( M^{A}_{a} \otimes M^{B}_{b} \right) \left( \rho \otimes \sigma^{AB} \otimes I \right) \right],$$

are feasible for the problem (11) (i.e. satisfy all the constraints) and achieve the value $r = r_S^{\rho^{AB}}$, as can be verified by direct substitution. Since $\{\tilde{N}_{a,b}^{k}\}_{a,b}$ and $\{\tilde{N}_{a,b}^{k}\}_{a,b}$ given by (12) and (13) do not necessarily provide an optimal solution to the problem (11), then

$$r_S^{MDI} [p(a,b|\psi_x,\psi_y)] \leq r_S^{\rho^{AB}}.$$

(14)
This bound can be easily interpreted. If the measured state has no entanglement, i.e. \( r_\perp(\rho^{AB}) = 0 \), then the probability distribution obtained by measuring it trivially has a separable realisation, so \( p^{MDI}_0[p(a,b)|\psi_x,\psi_y] = 0 \). On the other hand, if Alice and Bob detect that \( p^{MDI}_0[p(a,b)|\psi_x,\psi_y] > 0 \), then they immediately conclude that the underlining state is entangled, and moreover can place a lower bound on the amount of entanglement, as measured by the robustness (with respect to \( S \)), that is necessary to explain the data.

### B. MDI lower bound on the negativity

Another widely used entanglement measure of entanglement is the negativity [41]. Analogously to the device-independent estimation of negativity [42] it is possible to put lower bound on the negativity in a measurement-device-independent way. The negativity \( \mathcal{N} \) of some state \( \rho^{AB} \) is defined as the sum of the absolute values of the non-positive eigenvalues of the partially transposed state \( \rho_T^A \). It has been shown in [41] that it admits the following representation

\[
\mathcal{N}(\rho^{AB}) = \min_{\rho_+ - \rho_-} \text{Tr}[\rho_-], \quad \text{s.t.} \quad \rho^{AB}_T = \rho_+ - \rho_- \geq 0.
\]  

(15)

Having in mind the decomposition \( \rho^{AB} = \rho_+ - \rho_- \) it is possible to write the observed probabilities from the quantum inputs scenario in the following way

\[
p(a,b|\psi_x,\psi_y) = \text{Tr} \left[ (M_a^{A0} \otimes M_b^{B0}) (\psi_x^{A0} \otimes \rho^{AB}_T \otimes \psi_y^{B0}) \right] = q_+(a,b|\psi_x,\psi_y) - q_-(a,b|\psi_x,\psi_y),
\]

where

\[
q_+(a,b|\psi_x,\psi_y) = \text{Tr} \left[ (M_a^{A0} \otimes M_b^{B0}) (\psi_x^{A0} \otimes \rho_+ \otimes \psi_y^{B0}) \right],
\]

\[
q_-(a,b|\psi_x,\psi_y) = \text{Tr} \left[ (M_a^{A0} \otimes M_b^{B0}) (\psi_x^{A0} \otimes \rho_- \otimes \psi_y^{B0}) \right].
\]

According to (15) the negativity can be obtained by minimizing \( \text{Tr}[\rho_-] \), which can be written as

\[
\sum_{a,b} q_-(a,b|\psi_x,\psi_y) = \text{Tr} \left[ \left( \sum_a M_a^{A0} \otimes \sum_b M_b^{B0} \right) (\psi_x^{A0} \otimes \rho_- \otimes \psi_y^{B0}) \right] = \text{Tr}[\rho_-].
\]  

(16)

In order to estimate the negativity by an SDP optimization it is necessary to understand the form an effective POVM \( \hat{M}_{a,b} \) corresponding to a PPT state. We recall that for an arbitrary state an effective POVM must be positive and satisfy no-signalling principle, as encoded in (5), and for a separable state it also has to be a separable operator, as encoded in (8). An effective POVM corresponding to a PPT state, besides satisfying the no-signalling constraints, must also be a PPT operator. To see this consider partial transpose of an effective POVM

\[
\left( \hat{M}_{a,b}^{A0} \right)^{T_0} = \text{Tr}_{AB} \left( \left( M_a^{A0} \otimes M_b^{B0} \right) (\hat{S}^{A0} \otimes \rho^{AB}_T \otimes \hat{S}^{B0}) \right) = \text{Tr}_{AB} \left( \left( M_a^{A0} \otimes M_b^{B0} \right) \left( \tilde{S}^{A0} \otimes (\rho^{AB}_T)^{T} \otimes \hat{S}^{B0} \right) \right) .
\]

The second equality follows from the fact that \( \text{Tr}[A^T B] = \text{Tr}[B A^T] \). Since the full transpose is a CPTP map, \( \left( M_a^{A0} \right)^{T} \) is a positive operator and thus \( \left( \hat{M}_{a,b}^{A0} \right)^{T_0} \) is positive if the state \( \rho^{AB} \) is PPT, which is exactly the claim we wanted to prove. We will denote by \( \mathcal{P} \) the set of effective POVMs that are also PPT, i.e.

\[
\mathcal{P} = \{ \left\{ \hat{M}_{a,b}^{A0} \right\}_{a,b} \mid \left\{ \hat{M}_{a,b}^{A0} \right\}_{a,b} \in \mathcal{M}, \left( \hat{M}_{a,b}^{A0} \right)^{T_0} \geq 0 \}.
\]  

(17)

Now we have all the ingredients for the formulation of the SDP whose solution lower bounds the negativity of a state compatible with some observed probability distribution \( p(a,b|\psi_x,\psi_y) \) in the quantum inputs scenario:

\[
A^{MDI}[p(a,b|\psi_x,\psi_y)] = \min_{\{M_{a,b}^{A0}\}_{a,b} \in \mathcal{P}} \sum_{a,b} q_-(a,b|\psi_x,\psi_y),
\]

\[
\text{s.t.} \quad p(a,b|\psi_x,\psi_y) = q_+(a,b|\psi_x,\psi_y) - q_-(a,b|\psi_x,\psi_y),
\]

\[
q_+(a,b|\psi_x,\psi_y) = \text{Tr} \left[ \left( M_a^{A0} \otimes M_b^{B0} \right) (\psi_x^{A0} \otimes \rho_- \otimes \psi_y^{B0}) \right],
\]

\[
\forall a,b \quad \left\{ M_{a,b}^{A0} \right\}_{a,b} \in \mathcal{P}.
\]

### IV. MULTIPARTITE CASE

In this section we will generalize the previous entanglement detection and quantification techniques to the multipartite scenario. In [43] there is an outline of the proof that all multipartite entangled states exhibit some kind of nonlocality when queried with quantum inputs. Moreover, the approach via entanglement witnesses is also explained in [26] but in the bipartite case the witness is tailored for a specific state. Here, as before, we are interested in the detection of multipartite entanglement without a priori knowledge of the system under study.

In the bipartite case we saw that the problem reduces to finding a separable effective POVM that returns the observed data when applied to the chosen set of inputs. This generalises to the multipartite case as follows: given a certain type of separability, we want to find the properties of the effective POVM which by acting on the given set of quantum inputs returns the observed probability distribution. As expected, we will show that the effective POVM should have the same type...
of separability properties as the underlying state. For the sake of simplicity we will consider the tripartite scenario, with the generalization to more parties straightforward.

The scenario involves three parties, Alice, Bob and Charlie, each of whom can input quantum systems in the states $\psi_x$, $\psi_y$, and $\psi_z$, respectively in their measuring devices, that subsequently provide classical outputs $a$, $b$ and $c$. The experiment is characterized by the set of joint probabilities of the form

$$p(a, b, c | \psi_x, \psi_y, \psi_z) = \text{Tr} \left[ \left( M^{A}_{ab} \otimes M^{B}_{b} \otimes M^{C}_{c} \right) \rho^{ABC} \otimes \mathbb{I}_{a | b | c} \right],$$

where $M^{A}_{a}$ is a POVM Alice applies to the input $\psi_x$, and her share of the state $\rho^{ABC}$, and analogous for $M^{B}_{b}$ and $M^{C}_{c}$. In the same way as in the bipartite scenario it is useful to define an effective POVM

$$\tilde{M}^{A}_{a,b,c} = \text{Tr}_{ABC} \left[ \left( M^{A}_{a} \otimes M^{B}_{b} \otimes M^{C}_{c} \right) \rho^{ABC} \otimes \mathbb{I}_{a | b | c} \right],$$

which allows one to write

$$p(a, b, c | \psi_x, \psi_y, \psi_z) = \text{Tr} \left[ \tilde{M}^{A}_{a,b,c} \left( \rho^{A}_{a} \otimes \rho^{B}_{b} \otimes \rho^{C}_{c} \right) \right].$$

As in the bipartite case, the effective POVM elements satisfy a number of constraints by construction, which play the role of no-signalling conditions. For example

$$\sum_{a} M^{A}_{a,b,c} = \mathbb{I}_{a} \otimes M^{B}_{b} \otimes M^{C}_{c},$$

with $M^{B}_{b} \otimes M^{C}_{c}$ another effective POVM for Bob and Charlie. We will denote the set of effective POVMs which satisfy all such conditions in the tripartite case by $\mathcal{A}^{ABC}$.

In what follows we will show that the entanglement properties of the effective POVM elements (20) are the same as entanglement properties of the shared state $\rho^{ABC}$.

Fully separable states can be written in the form $\rho^{ABC} = \sum_{\lambda} \rho_{\lambda}^{A} \otimes \rho_{\lambda}^{B} \otimes \rho_{\lambda}^{C}$ and if Alice, Bob and Charlie share such a state the corresponding effective POVM elements (20) will also be fully separable operators

$$\tilde{M}^{A}_{a,b,c} = \sum_{\lambda} \rho_{\lambda}^{A} M^{A}_{a | \lambda} \otimes M_{b | \lambda}^{B} \otimes M_{c | \lambda}^{C},$$

where $M^{A}_{a | \lambda} = \text{Tr}_{B} \left[ M^{A}_{a} \left( \rho_{\lambda}^{A} \otimes \rho_{\lambda}^{B} \right) \right]$ is an effective POVM, and analogously for $M^{B}_{b | \lambda}$ and $M^{C}_{c | \lambda}$. Analogously to the bipartite case, we define a subset $\mathcal{A}^{ABC}$ of all effective tripartite POVMs $\mathcal{A}^{ABC}$, which are also fully separable, $\mathcal{A}^{ABC} = \left\{ \tilde{M}^{A}_{a,b,c}, a,b,c \right\}$, $\mathcal{A}^{ABC} \subseteq \mathcal{A}^{ABC}$, $\tilde{M}^{A}_{a,b,c} = \sum_{\lambda} \tau_{a | \lambda} \otimes \chi_{b | \lambda} \otimes \omega_{c | \lambda} \geq 0$, and analogously for all other operators. Thus, the fact that the state $\rho^{ABC}$ is biseparable implies that the operators (26) are also biseparable.

In the similar way as in the bipartite scenario, it is necessary to choose an appropriate relaxation of the set of fully separable tripartite operators in order to turn this feasibility problem into an SDP. The set of operators which are PPT across all bipartitions is one choice. A second option is to use the multipartite generalisation of the $k$-shareability hierarchy of SDPs [44].

Tripartite states have a richer entanglement structure than bipartite states, such that even if the problem (24) confirms that there is some entanglement in the system, a full entanglement characterization is not yet complete. It can happen, for example, that the entanglement is shared only between two parties. States which have such entanglement structure are called separable across a certain bipartition. For example the state $\rho^{ABC} = \sum_{\lambda} \rho_{\lambda}^{A} \otimes \rho_{\lambda}^{B} \otimes \rho_{\lambda}^{C}$ is separable with respect to the bipartition $AB | C$. A state is biseparable if it can be written as a convex combination of the states that are separable with respect to different bipartitions:

$$\rho^{ABC} = \sum_{\lambda} p^{A}_{\lambda} \rho^{A}_{\lambda} \otimes \rho^{B}_{\lambda} \otimes \rho^{C}_{\lambda}$$

The strongest form of entanglement that can be present in a tripartite system is genuine multipartite entanglement (GME). A state $\rho^{ABC}$ is genuinely multipartite entangled if it is not biseparable.

Let us assume that the state shared between Alice, Bob and Charlie is biseparable (25). In that case the effective POVM reads

$$\tilde{M}^{A}_{a,b,c} = \sum_{\lambda} p^{A}_{\lambda} M^{A}_{a | \lambda} \otimes M^{B}_{b | \lambda} \otimes M^{C}_{c | \lambda}$$

where

$$M^{A}_{a | \lambda} = \text{Tr}_{B} \left[ M^{A}_{a} \left( \rho_{\lambda}^{A} \otimes \rho_{\lambda}^{B} \right) \right].$$

and analogously for all other operators.
With this structure in mind it is possible to construct a feasibility problem to test whether an observed probability distribution in the quantum input scenario can be obtained with a bipartite state.

given \( \{ p(a,b,c) | \psi_x, \psi_y, \psi_z \} \) \( a,b,c \in \mathbb{X} \),

find \( \{ M_{a,b,c}^A | R_{a,b,c}^B, M_{a,b,c}^C \} \) \( a,b,c \in \mathbb{X} \) \( (27) \)

\[ \begin{align*}
\text{s.t.} & \quad p(a,b,c) = \text{Tr}\left[ M_{a,b,c}^A (\psi_x \otimes \psi_y \otimes \psi_z) \right] \\
& \quad \forall a,b,c
\end{align*} \]

\[ \begin{align*}
M_{a,b,c}^A & = M_{a,b,c}^A + M_{a,b,c}^B + M_{a,b,c}^C \\
M_{a,b,c}^A & \in \mathcal{A}, \quad M_{a,b,c}^B \in \mathcal{B}, \quad M_{a,b,c}^C \in \mathcal{C}
\end{align*} \]

where \( \mathcal{A} \) denotes the set of effective tripartite POVMs \( \mathcal{A}ABC \) that are also separable across the bipartition \( A,B,C \) and analogously for \( \mathcal{B} \) and \( \mathcal{C} \). Once more, by replacing the sets \( \mathcal{A} \) by the set of PPT operators or operators having \( k \)-symmetric extension the above problem becomes an instance of a SDP.

Quantification of multipartite entanglement can be performed in a similar manner as in the bipartite scenario. Namely, one can lower bound the robustness of genuine multipartite entanglement, or simply robustness of multipartite entanglement, by defining MDI multipartite nonlocality robustness analogously to (11).

V. RANDOMNESS FROM QUANTUM INPUTS

Nonlocal correlations, as proven by Bell’s theorem [3], cannot be explained by any classical, deterministic model or a convex combinations of such models. Consequently, a violation of a Bell inequality can be used to certify that the data generated is intrinsically random. This reasoning led to the development of the protocols for so-called device-independent randomness certification [45–48]. In these protocols the amount of (global) randomness stemming from some Bell experiment is characterized by the guessing probability \( G_{x^*,y^*} \) with which an external eavesdropper can guess a pair of outcomes observed by Alice and Bob when they make measurements \( x \) and \( y \). A lower bound on the guessing probability is

\[ \begin{align*}
G_{x^*,y^*} & = \max_{a,b} p(a,b | x^*, y^*)
\end{align*} \]

and this is the best that an external observer uncorrelated with Alice and Bob can guess. However, an eavesdropper, usually named Eve, can have side-information – a system that is correlated (or even entangled) with the state of Alice and Bob. In principle she could have even provided all the measuring devices, and can possibly achieve much better guessing probability than the lower bound (28). Thus the aim of a device-independent randomness estimation protocol is to quantify the randomness of Alice’s (and/or Bob’s) measurement outcomes by optimizing over all possible eavesdropping strategies of Eve compatible with the obtained Bell inequality violation. The scenario assumes that by sharing a tripartite state, and performing some measurement on her share, Eve steers the state of Alice and Bob. Her strategy is to perform a measurement such that her outcome, denoted by \( e \), will give her the highest probability to guess the pair of outcomes for one particular choice of measurements for Alice and Bob. In such a scenario calculating Eve’s guessing probability, if the obtained value of a Bell expression \( \sum_{a,b,x,y} I_{a,b,x,y} p(a,b | x,y) \) is equal to \( \beta \) can be cast as the following optimisation problem

\[ \begin{align*}
G_{x^*,y^*} & = \max_{\{p(a,b,e | x,y)\} \in \mathcal{D}} \sum_{a,b,e} p(a,b,e | x^*, y^*) \\
\text{s.t.} & \quad \sum_{a,b,e} I_{a,b,x,y} p(a,b,e | x^*, y^*) = \beta \\
& \quad \{p(a,b,e | x,y)\} \in \mathcal{D}
\end{align*} \]

where \( \mathcal{D} \) denotes the set of quantum behaviours, i.e. the set of all \( \{p(a,b,e | x,y)\} \) that can arise by performing local measurements on a tripartite quantum state. This program gives the highest probability with which Eve’s outcome \( e \) is the same as Alice’s and Bob’s outcomes, \( a \) and \( b \), for some specific pair of inputs \( x^* \) and \( y^* \), with the constraints that the overall probabilities must be compatible with quantum mechanics and the observed violation of a Bell inequality. In general this problem cannot be solved exactly, due to the set \( \mathcal{D} \) having no known simple characterisation (in particular since it implicitly contains all behaviours compatible with any quantum state and measurements in a Hilbert space of any dimension) however by using the Navascues-Pironio-Acin (NPA) hierarchy of SDP relaxations of the quantum set of behaviours [49], computable upper bounds can be placed on the guessing probability.

One generalization of this protocol to the quantum-input scenario under the name measurement-device-independent randomness certification has been introduced in [50]. Analogously to the ability to detect entanglement of all entangled states, even those that do not violate any Bell inequality, the authors of [50] prove that it is possible to extract randomness from local entangled states in a measurement-device-independent way. They use the analogue of the program (29) with the constraint that the probabilities \( p(a,b | \psi_x, \psi_y) \) violate the inequality corresponding to a specific MDIEW. As already noted in the previous text, a MDIEW is usually constructed with respect to a specific entangled state. It can nevertheless be used to check if some other entangled state in principle can be useful for randomness extraction. However, as the source providing Alice’s and Bob’s shared state is uncharacterised it may not be clear which witness should be used, and therefore it is desirable to have a method to certify randomness that does not rely on a specific MDIEW. Another way to certify randomness in the quantum input scenario is the subject of [51]. In this approach the source has to prepare a tomographically complete set of inputs which are used to perform quantum process tomography of the measurement device. Randomness is generated by measuring one of the prepared quantum inputs by the characterized
POVM. A method do quantify the amount of randomness is presented for two-outcome POVMs. This approach was used to experimentally generate randomness in a measurement-device-independent manner [52].

In the following we will show the way to quantify the amount of randomness resulting from an experiment with quantum inputs without assuming the underlying state. This can be seen as the generalisation of the approach of [53, 54] from the standard Bell scenario to the quantum inputs scenario. The protocol works for measurements with arbitrary number of outputs and the set of quantum inputs does not have to be tomographically complete, which makes it more general than [51].

Before presenting the more general approach to randomness estimation in the quantum inputs scenario, let us consider in more detail the essential novelty of this scenario, which is the fact that before guessing the measurement outcome Eve has to guess the input state. Due to this it is not only possible to extract randomness from local entangled states as observed in [50], but also from a single black-box, i.e. without the use of entanglement.

This leads us to the change of scenario: now we have only one party, Alice, who has a characterised device which prepares quantum input states $|\psi_x\rangle$. Alice measures the states using an uncharacterised black box, modelled by POVM $\{M_a\}_a$, and obtains some outcomes $a$. By repeating the process she can calculate the set of probabilities $p(a|x)$, to get an outcome $a$ when the quantum input is $|\psi_x\rangle$. The question is how random Alice’s outputs are for Eve. In some cases Alice can be sure that her outcomes are genuinely random. If the set of quantum inputs is tomographically complete Alice can perform process tomography and exactly learn which POVM her black-box is applying. In the special case when the obtained POVM is extremal Eve cannot be correlated with Alice’s experiment because extremal POVMs cannot be decomposed as a convex combination of other POVMs. Therefore Eve’s guessing probability is obtained simply from (28) (restricted to a single party Alice, instead of Alice and Bob). An extremal $d$-dimensional POVMs cannot have more than $d^2$ outcomes [55], which means that when preparing qubit quantum inputs Alice at best can get 2 bits of randomness. One example is the case when Alice prepares the following informationally complete set of quantum inputs $\{|\psi_x\rangle \in \{|0\rangle, |0\rangle + |1\rangle \rangle, |0\rangle + |1\rangle \rangle, |0\rangle - |1\rangle \rangle\}$ and observes the probability distribution which corresponds to measuring these inputs with an extremal four-outcome tetrahedral POVM. The probabilities to get any of the four outcomes when measuring the input which is in the maximally mixed state $\rho = I_2$ is equal to 0.25, which corresponds to 2 bits of randomness.

In the general case, when the set of quantum inputs is not tomographically complete, or the applied POVM is not extremal it is still possible to construct an SDP-based estimation of randomness analogous to (29). Since the measuring device is uncharacterised it has to be assumed that it was possibly prepared by Eve. In that case Eve can be quantumly correlated with the box. That is, she can prepare an ancillary entangled pair of particles $\rho_{AE}$, and place half inside the box, while keeping the other half. In each round Alice’s box then performs a joint measurement $M_{a|x}$, where $a$ corresponds to Alice’s outcome, and Eve performs a measurement $N_e$, with outcome $e$. Thus, the probability for Alice to get outcome $a$ and Eve to get $e$, when the quantum input is $|\psi_x\rangle$ is

$$p(a,e|\psi_x) = \text{Tr} \left[ (M_{a|x} \otimes N_e) (\psi_x \otimes \rho_A) \right] = \text{Tr} (M_{a|x} \rho_x)$$

where $M_{a|x}$ is an effective POVM which satisfies the relation

$$M_{a|x} = \text{Tr}_{AE} \left[ (M_{a|x} \otimes N_e) (\rho_A \otimes \rho_{AE}) \right].$$

From this relation, it follows that the effective POVM satisfies the relation

$$\sum_a M_{a|x}^{e} = p(e)I_A,$$

where $p(e) \geq 0$. As in the above, this can be seen as the no-signalling constraint from Alice to Eve.

With the above in place, the optimisation problem which bounds the guessing probability of Eve is

$$G_e = \max_{\{M_{a|x}\}_{a,e}} \frac{\text{Tr} \sum_a M_{a|x}^{e} \psi_x^{a}}{\text{Tr} \sum_a M_{a|x}^{e} \psi_x^{a}},$$

subject to

$$\text{Tr} \sum_a M_{a|x}^{e} \psi_x^{a} = p(a|x), \quad \forall x, a;$$

$$\sum_a M_{a|x}^{e} = p(e)I_A, \quad \sum_e p(e) = 1, \quad \forall e.$$
on the outcome $e$, she prepares an subnormalized state $\rho_{e}^{AB}$, whose norm is equal to the probability for Eve to obtain the outcome $\text{Tr} \rho_{e}^{AB} = p(e)$. The full joint probability is given by

$$p(a, b, e | \psi_x, \psi_y) = \text{Tr} \left[ \left( M_{a}^{A} \otimes M_{b}^{B} \right) \left( \psi_{x}^{A} \otimes \rho_{e}^{AB} \otimes \psi_{y}^{B} \right) \right]$$

$$= \text{Tr} \left[ M_{a, b, e}^{A0B0} \left( \psi_{x}^{A} \otimes \psi_{y}^{B} \right) \right]$$

(34)

where $M_{a, b, e}$ is an effective POVM defined by

$$M_{a, b, e}^{A0B0} = \text{Tr}_{AB} \left[ \left( M_{a}^{A} \otimes M_{b}^{B} \right) \left( \Pi_{0} \otimes \rho_{e}^{AB} \otimes \Pi_{0} \right) \right].$$

(35)

These effective POVMs, apart from satisfying the completeness relation $\sum_{a, b, e} M_{a, b, e}^{A0B0} = \Pi_{0}$, also satisfy the no-signalling constraints

$$\sum_{a} M_{a, b, e}^{A0B0} = \Pi_{0} \otimes M_{b, e}^{B0},$$

$$\sum_{b} M_{a, b, e}^{A0B0} = M_{a, e}^{A0} \otimes \Pi_{0},$$

where $\{M_{b, e}^{B0}\}_{b}$ and $\{M_{a, e}^{A0}\}_{a}$ are sub-normalised POVMs (for Bob and Alice respectively), for all values of $e$, with the same normalisation for each $e$, i.e. $\sum_{b} M_{a, b, e}^{B0} = p(e) \Pi_{0}$ and $\sum_{b} M_{a, b, e}^{A0} = p(e) \Pi_{0}$.

Eve’s optimal guessing probability is then the solution of the following SDP

$$G_{x, y}^{MDI} = \max_{\{M_{a, b, e}^{A0B0}\}_{a, b, e}} \text{Tr} \sum_{e} \sum_{a, b} M_{a, b, e}^{A0B0} \left( \psi_{x}^{A} \otimes \psi_{y}^{B} \right),$$

(37)

s.t. $\text{Tr} \sum_{e} \sum_{a, b} M_{a, b, e}^{A0B0} \left( \psi_{x}^{A} \otimes \psi_{y}^{B} \right) = p(a, b | \psi_{x}, \psi_{y}), \forall x, y, a, b,$

$M_{a, b, e}^{A0B0} \geq 0$ \quad $\forall a, b, e,$

$\sum_{a} M_{a, b, e}^{A0B0} = \Pi_{0} \otimes M_{b, e}^{B0} \quad \forall b, e,$

$\sum_{b} M_{a, b, e}^{A0B0} = M_{a, e}^{A0} \otimes \Pi_{0} \quad \forall a, e,$

$\sum_{b} M_{a, b, e}^{B0} = p(e) \Pi_{0} \quad \forall e,$

$\sum_{a} M_{a, b, e}^{A0} = p(e) \Pi_{0} \quad \forall e,$

$p(e) = 1.$

The objective function is the total probability for Eve to guess Alice’s and Bob’s outputs for some specific pair of quantum inputs $\psi_{x}^{A0}$ and $\psi_{y}^{B0}$. The first constraint imposes consistency with the observed behaviour in the experiment, while the remaining constraints ensure an valid effective POVM (which is normalised and no-signalling).

As an example this program can be used to obtain the optimal guessing probability compatible with the probability distribution which arises by Alice and Bob performing Bell state measurements on a shared Werner state $|\Psi\rangle = w |\Phi^{+}\rangle + (1-w) |I\rangle$ and with quantum inputs corresponding to the vertices of tetrahedron on the Bloch sphere. The resulting guessing probability in terms of parameter $w$ is given presented in Fig. 1.

The correlations obtained on the maximally entangled state ($w = 1$) allow to extract four bits of randomness, because the guessing probability is $\frac{1}{\sqrt{2}}$. As in [50] some randomness can be observed from all entangled Werner states, even those admitting a local model. What may be particularly surprising is that actually all Werner states except for the maximally mixed state manifest some randomness. As commented earlier, intuitively this can be explained by the fact that Eve cannot with certainty guess which quantum input was used, which makes the probability distribution random even when there is no non-locality at all.

VI. DISCUSSION

In this work we have provided new insights into entanglement and randomness detection and quantification in the measurement-device-independent scenario. As explained, this scenario differs from the well-known device-independent scenario by the fact that parties possess a characterised device that can prepare quantum system in some defined quantum states. The scenario in which some parties do not trust their sources and measurements but have a characterised preparation device is not so uncommon in quantum information processing and has been used for constructing protocols for
universal blind quantum computation [58]. In particular, we showed how one can estimate the values of two widely used entanglement measures, robustness-based quantifiers of entanglement, and entanglement negativity. Furthermore we showed how entanglement detection and quantification can be performed in quantum networks (i.e. in situations involving multiple parties, not just two).

On the other hand we showed how possessing a characterised preparation device can decrease adversarial power in guessing measurement outputs. Already a single party which can prepare specific states and measure them with a black box can extract two bits of randomness. Two parties sharing some quantum state can extract randomness even when they do not share any entanglement.

There are a number of interesting directions for future work. First is to study whether the results presented here for the measurement-device-independent scenario can be adapted to other device-independent scenarios. A second interesting avenue is to explore the prospects with regard to full quantum state recovery. A third direction is to focus on mixed quantum inputs – in which can one can imagine that the Eavesdropper holds a purification. It is interesting to ask how this affects entanglement detection, and randomness estimation.

Note added: After finishing this work we learnt about independent work of Rosset et al. [59] also dealing with measurement-device-independent entanglement quantification.

VII. ACKNOWLEDGEMENTS

This work was supported by the Ramón y Cajal fellowship, Spanish MINECO (QIBEQI FIS2016-80773-P and Severo Ochoa SEV-2015-0522), the AXA Chair in Quantum Information Science, Generalitat de Catalunya (SGR875 and CERCA Programme), Fundació Privada Cellex and ERC CoG QITBOX, and a Royal Society University Research Fellowship.