Experimental multipartite entanglement and randomness certification of the W state in the quantum steering scenario

A Máttar, P Skrzypczyk, G H Aguilar, R V Nery, S P Walborn and D Cavalcanti

ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, E-08860 Castelldefels (Barcelona), Spain
H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol, BS8 1TL, United Kingdom
Instituto de Física, Universidade Federal do Rio de Janeiro, CP 68528, 21941-972, Rio de Janeiro, RJ, Brazil
Institute for Quantum Science and Technology, and Department of Physics and Astronomy, University of Calgary, Calgary, Alberta T2N 1N4, Canada
Departamento de Física, Universidade Federal de Santa Catarina, CEP 88040-900, Florianópolis, SC, Brazil

E-mail: alejandro.mattar@icfo.es

Keywords: entanglement, quantum steering, quantum correlations, quantum nonlocality, quantum information

Abstract
Recently, Cavalcanti et al (2015) proposed a method to certify the presence of entanglement in asymmetric networks, where some users do not have control over the measurements they are performing. Such asymmetry naturally emerges in realistic situations, such as in cryptographic protocols over quantum networks. Here we implement such ‘semi-device-independent’ techniques to experimentally witness all types of entanglement on a three-qubit photonic W state. Furthermore, we analyse the amount of genuine randomness that can be certified in this scenario from any bipartition of the three-qubit W state.

1. Introduction
In general, the certification of entanglement requires the performance of specific measurements on the quantum state one is willing to test. Experimentally, this is a delicate task, since mismatches between either the state or the measurements and their actual physical implementation may lead to false-positive conclusions about the presence of entanglement in the network. Although such mismatches can, in principle, be patched in experimental setups, the situation becomes dramatic when considering applications, where the devices used are not trusted as they could have been provided and controlled by some adversary. One solution to this problem is the use of device-independent techniques, for which no assumption is made on the devices that generate the state or perform the measurements. In this approach, the devices are seen as black boxes, accessed only with classical inputs (corresponding to the measurement choices) and providing classical outputs (corresponding to the measurement outcomes). Although such device-independent entanglement witnesses have been soundly considered in the past years, their physical implementation turns out to be very demanding, as it requires one to observe a Bell inequality violation without the presence of loopholes.

A midpoint among the aforementioned cases is the semi-device-independent approach based on the presence of quantum steering to certify entanglement in the network. This is an asymmetric situation in the sense that only some of the parties in the network use trusted devices while others do not. Once more, trust should be understood in terms of full knowledge or characterisation of the devices used. More precisely, whenever a party’s device is assumed untrusted, all the analysis employed will only be based on the statistics it produces, not on its internal working.

The steering approach is less demanding experimentally than the device-independent case, but it still presents practical interest for adversarial situations; for instance, one could think of a practical semi-device-independent network composed by a single central provider using well-characterised devices, while the remaining parties, the clients, hold untrusted, i.e. uncharacterised devices. For these reasons the study of quantum steering has increased substantively in recent years.
Methods to certify all kinds of multiparticle entanglement in semi-device-independent networks were presented—and experimentally demonstrated—very recently in [14]. These methods rely on semi-definite programming (SDP) techniques. They represent an important achievement for the certification of entanglement in quantum networks. In fact, these techniques certify entanglement in networks with amounts of noise that make them undetectable by the existing fully device-independent techniques [7].

Here, we apply such semi-device-independent entanglement certification techniques to the three-qubit W state. Crucially, this state displays both genuine multipartite entanglement (GME) and entanglement in all of its reduced states, being then a flexible resource for the implementation of quantum networks. This is not the case for the GHZ state implemented in [14], as its reduced state turns to be separable, therefore making it highly desirable to assess the certification of all types of entanglement from one single resource, like the W state. Moreover, we show that all types of entanglement of the W state can be certified in all tripartite steering scenarios in a scheme where each party applies the same set of measurements. In this way, each party can certify all types of entanglement without the need to rely on any characterisation of the measurement devices used by the others.

In this paper, we show that by sharing a W state, every party can detect all types of entanglement without the need of trusting the measurements that the other parties are performing. This puts the W state as a promising candidate to implement asymmetric cryptographic protocols. We demonstrate the feasibility of such aforementioned techniques for entanglement certification in a proof-of-principle photonic experiment. Additionally, we implement for the first time the recent methods for one-sided device-independent randomness certification presented in [16] to estimate the amount of randomness that can be obtained in bipartitions of the W state.

The paper is organised as follows. In section 2 we first provide a general overview on the construction of semi-device-independent witnesses required to certify all types of entanglement. Next, we present theoretical results for the values achieved by such witnesses when the three-qubit W state is considered. Then, in section 3 we describe the scenario and methods required for one-sided device-independent randomness certification, and we apply such framework to bipartitions of the three-qubit W state. In section 4 we present the photonic implementation and the corresponding experimental results. Finally, in section 5 conclusions are presented.

2. Entanglement detection

In this section we first recall the methods of [14] to construct multipartite semi-device-independent entanglement witnesses. The intuition is the following. Assuming that the quantum state (denoted by \( \rho \)) distributed in the network is separable according to some particular decomposition (e.g. fully separable, separable across any bipartition, etc), constraints are imposed on the collection of all possibly observable set of post-measured states that the untrusted measurements create for the the parties holding trusted devices. From these constraints, one can then determine if the original state \( \rho \) could have the considered decomposition with SDP techniques in an efficient way. This SDP also provides experimentally friendly entanglement witnesses.

2.1. Semi-device-independent scenarios

For illustrative purposes and simplicity, we narrow our focus to the distribution of \( \rho \) among three parties: A, B and C, but it is worth noting that the witness constructions that will be presented can indeed be generalised for a larger number of parties. Two semi-device-independent cases arise; namely, either one or two of the parties could be holding untrusted devices in the network. In the case where one party, say A, uses untrusted devices, it will be first interesting to analyse the reduced asymmetric network that stems between A and B when discarding the third party C (top left of figure 1). This corresponds to a bipartite steering scenario and the witness for such case will be derived in section 2.2. Note that the certification of entanglement in the reduced state shared by A and B guarantees the presence of entanglement across bipartitions A:BC and AC:B, regardless of whether C trusts his measurement device or not.

A slightly more complicated task is to certify tripartite entanglement when either one or two parties hold untrusted devices (top right and bottom of figure 1, respectively). Equivalently, this task requires one to decide whether the original state \( \rho \) is fully separable or not, and we will construct the witness necessary to answer this question in section 2.3. Next, the question will be extended for genuine multipartite entanglement (GME) in section 2.4 by asking if the state is biseparable.

2.2. Entanglement in bipartite reductions

We start by analysing the presence of entanglement in the reduced bipartite system left to A and B when C is disregarded (see top left in figure 1). In this case, A and B are left with the quantum state \( \rho_{AB} = \text{Tr}_C[\rho] \). The measurements performed by A on its share of \( \rho_{AB} \) are untrusted, and therefore they are described by unknown positive operators \( M_{a|x} \) summing to identity for each \( x \), where \( x \) labels the measurement chosen by A and \( a \) the
obtained outcome. On the other hand, B trusts the measurement device and can thus perform quantum
tomography on the system to observe an (unnormalised) conditional state:

$$\sigma^B_{a|x} = \text{Tr}_A [(M_{a|x} \otimes \mathbb{1}^B) \rho^{AB}], \quad \forall \ a, \ x.$$  \hspace{1cm} (1)

Note that the statistics observed by A can be recovered from the relation (Born rule) $p(a|x) = \text{Tr} [\sigma^B_{a|x}]$, and thus the collection $\{\sigma^B_{a|x}\}$, known as a quantum assemblage [13], contains all the information obtainable in this measurement scenario. If $\rho^{AB}$ is not entangled, it reads

$$\rho^{AB} = \sum_{\lambda} p_{\lambda} \rho^A_{\lambda} \otimes \rho^B_{\lambda},$$  \hspace{1cm} (2)

where $p_{\lambda}$ defines some probability distribution. In this case, the assemblage (1) takes the form

$$\sigma^B_{a|x} = \sum_{\lambda} p(a|x) \rho^B_{\lambda},$$  \hspace{1cm} (3)

with $p(a|x) = p_{\lambda} \text{Tr} [M_{a|x} \rho^A_{\lambda}]$. A decomposition for $\sigma^B_{a|x}$ of the form (3) is a typical instance of an assemblage admitting a local hidden state (LHS) model [13]. The collection of all such unnormalised assemblages admitting an LHS model for B forms a convex set which we denote $\Sigma^{B}_{A:B}$. Concretely,

$$\Sigma^{B}_{A:B} = \left\{ \sigma^B_{a|x} \mid \sigma^B_{a|x} = \sum_{\mu} D_\mu(a|x) \sigma^B_{\mu}, \sigma^B_{\mu} \geq 0 \right\},$$  \hspace{1cm} (4)

where we have used the fact that any probability distribution $p(a|x)$ can always be written as a convex combination of deterministic strategies $D_\mu(a|x)$. (Note that the constraints inside the brackets in equation (4) involve all values of $a$ and $x$; unless otherwise specified, all expressions with indices should be understood to hold for each value of the index.)

Crucially, imposing membership in $\Sigma^{B}_{A:B}$ involves a finite number of linear matrix inequalities and positive-semi-definite constraints for the variables $\sigma^B_{\mu}$ in (4), which are all valid constraints to formulate the problem as an SDP [17]. By introducing the maximally mixed assemblage for Bob, $\mathbb{1}^B_{a|x} = \frac{1}{d_B} \text{Tr}_A \left[ \frac{1}{d_A} \rho^A_{a|x} \right]$ where $o_A$ denotes the number outcomes of $A$ and $d_A$ and $d_B$ denote the dimension of $A$’s and $B$’s respective systems, we arrive at the following SDP test for bipartite entanglement with one party holding untrusted devices:

$$\min \ r \quad \text{s.t.} \quad (1 - r) \sigma^B_{a|x} + r \mathbb{1}^B_{a|x} \in \Sigma^{B}_{A:B} \quad \forall \ a, \ x,$$  \hspace{1cm} (5)

where $\sigma^B_{a|x}$ is the assemblage observed by B in this network. Since $\mathbb{1}^B_{a|x} \in \Sigma^{B}_{A:B}$, a sufficiently small value of $r$ will always solve the second line of (5), and hence this SDP is strictly feasible. The solution of (5), denoted by $r^*$, quantifies how much maximally mixed noise has to be added to the assemblage such that the mixture becomes LHS: if $r^* = 0$, then $\sigma^B_{a|x} \in \Sigma^{B}_{A:B}$ and no steering can be demonstrated. On the other hand, if $r^* > 0$, some amount of maximally mixed noise has to be added to the assemblage to make it LHS, so we certify entanglement in $\rho^{AB}$. 

---

Figure 1. Relevant semi-device-independent networks. Trusted (untrusted) devices are represented as white (black) boxes. Top left: C is discarded (crossed box) and the network consists of the reduction left to A and B. If A performs a measurement $x$ giving outcome $a$, B observes an unnormalised quantum state denoted $\sigma^B_{a|x}$. Top right: in this case, C is not discarded, and B and C observe a bipartite state $\sigma^B_{a|xy}$. Bottom: with two parties holding untrusted devices, C receives a state $\sigma^B_{a|xy}$ conditioned on the statistics observed both by A and B.
Furthermore, from the dual formulation of the primal problem (5), it is possible to define a set of operators \( \{ E_{a|x} \}_{a|x} \), which are such that the linear functional
\[
\hat{w} : \pi_{a|x} \mapsto \sum_{a|x} \text{Tr} \left[ E_{a|x} \pi_{a|x} \right]
\]  
(6)
provides a strictly positive value only if the assemblage \( \pi_{a|x} \) demonstrates steering. Thus, \( \hat{w} \) constitutes a witness for bipartite entanglement with one party holding untrusted devices. Moreover, since the primal problem is strictly feasible, strong duality holds, and the dual and primal solutions coincide [17]. That is, \( \hat{w} (\sigma_{a|x}^B) = r^* \), i.e. the value of the witness applied to the assemblage from which it was derived gives exactly the robustness \( r^* \) of this assemblage.

To conclude this section, note that the witness we constructed here certifies entanglement between A and B, whether C is holding a device that is trusted or untrusted. In other words, this witness also certifies the presence of entanglement across the bipartitions A:BC and B:AC, for any level of trust that C might have on his measurement device.

2.3. Entanglement in the full state

We now move on to the full tripartite network, for which we wish to certify the presence of entanglement in the whole state \( \rho \) distributed to A, B and C. The construction procedure is similar to the one from the previous section. If \( \rho \) is fully separable, then
\[
\rho = \sum_{\lambda} p_{\lambda} \rho^A_{\lambda} \otimes \rho^B_{\lambda} \otimes \rho^C_{\lambda}.
\]  
(7)

We treat first the case in which only A uses an untrusted device, while B and C’s devices remain trusted (see top right of figure 1). In this case, B and C are provided with the assemblage
\[
\sigma^B_{a|x} = \text{Tr}_A \left[ (M_{a|x} \otimes 1^B \otimes 1^C) \rho \right],
\]  
(8)
which, after using equation (7), takes the form
\[
\sigma^B_{a|x} = \sum_{\lambda} p(a|x|\lambda) \rho^B_{\lambda} \otimes \rho^C_{\lambda}.
\]  
(9)

A decomposition of \( \sigma^B_{a|x} \) of the form in equation (9) can readily be seen to be similar to the one in equation (3), with the only difference that now the bipartite states of B and C conditioned on a and x are separable. This last requirement (separability) cannot, in general, be translated to a finite number of linear matrix inequalities and positive constraints as before, because the set of separable states has a complicated structure. However, separability can be relaxed to positivity under partial transposition [2], which is now a valid SDP constraint and equivalent to separability whenever the product of the dimensions of B and C satisfies \( d_B \leq d_C \). Therefore, we define the relaxed set
\[
\Sigma^{BC}_{A:B:C} = \left\{ \sigma^B_{a|x}, \sigma^C_{a|y} = \sum_{\mu} D_\mu (a|x|\mu) \sigma^B_{\mu} \otimes \sigma^C_{\mu} \geq 0, (\sigma^B_{\mu})^{T_B} \geq 0 \right\},
\]  
(10)
where \( T_B \) denotes the partial transposition operation with respect to system B. In the same fashion as in section 2.2, with the help of the maximally mixed assemblage for B and C, namely \( \rho^B_{a|x} = \frac{1}{d_B} \text{Tr}_B \left[ (1_{d_B} \otimes 1_{d_C}) \right] \), we obtain the corresponding SDP test for tripartite entanglement with one party holding untrusted devices:
\[
\min r \text{ s.t.} \quad (1 - r) \sigma^B_{a|x} + r \rho^B_{a|x} \in \Sigma^{BC}_{A:B:C}.
\]  
(11)

Here again, duality theory allows one to retrieve operators \( \{ E_{a|x} \}_{a|x} \) defining a new witness \( \hat{w} \) with the exact same structure as in equation (6), such that \( \hat{w} (\sigma^B_{a|x}) < 0 \) guarantees that \( \rho \) is tripartite entangled. Finally, note that whenever \( d_B \leq d_C \), there exists entangled steerable states that remain undetected by our witness construction, since the set of unsteerable states does not coincide with \( \Sigma^{BC}_{A:B:C} \); in this case. But since \( \Sigma^{BC}_{A:B:C} \) does contain all separable states, a positive value of the witness guarantees that the state is, unequivocally, entangled.

In the case of two parties holding untrusted devices (say A and B, as shown at the bottom of figure 1), C observes the assemblage
\[
\sigma^C_{a|xy} = \text{Tr}_{AB} \left[ (M_{a|xy} \otimes M_{b|y} \otimes 1^C) \rho \right],
\]  
(12)
which, after replacing \( \rho \) with its separable form in equation (7), gives
\[
\sigma^C_{a|xy} = \sum_{\lambda} p(a|xy|\lambda) \rho^C_{\lambda},
\]  
(13)

\[^6\text{The only difference is that the witness now is a functional acting on the space of assemblages of B and C.}\]
Since $p(ab|x,y)$ arises from local measurements of a separable state, it must be local [5] and can therefore be written as a convex combination of products of deterministic strategies for A and B. Thus, the relevant set of unnormalised assemblages for tripartite entanglement with two parties using untrusted measurements is

$$\Sigma_{A:B:C} = \left\{ \sigma_{a|b|y}^{C} \mid \sigma_{a|b|y}^{C} = \sum_{\mu} D_{\mu}(a|x) D_{\mu}(b|y) \sigma_{\mu}^{C}, \sigma_{\mu}^{C} \geq 0 \right\}$$  \hspace{1cm} (14)

and since membership in $\Sigma_{A:B:C}$ involves valid SDP constraints, we obtain the corresponding SDP test:

$$\min r \text{ s.t. } (1 - r) \sigma_{a|b|y}^{C} + rI_{a|b|y}^{C} \in \Sigma_{A:B:C}^{C}$$  \hspace{1cm} (15)

where $I_{a|b|y}^{C} = \frac{1}{\alpha_{a|b}} \text{Tr}_{B} \left[ I_{a|b|y}^{BC} \right]$ is the maximally mixed assemblage for C. The set of dual variables $\{I_{a|b|y}^{C}\}_{a|b|y}$ of programme (15) enables the construction of the witness

$$\hat{w} : \pi_{a|b|y} \mapsto \sum_{a|b|y} \text{Tr}[I_{a|b|y}^{C} \pi_{a|b|y}],$$  \hspace{1cm} (16)

which provides a strictly positive value if—and only if—$\pi_{a|b|y}^{C}$ demonstrates steering. Once more, $\hat{w}(\pi_{a|b|y}^{C}) = r^*$.  

### 2.4. Genuine multipartite entanglement

In this section we move to the more delicate task of certifying genuine tripartite entanglement in the state $\rho$ shared by A, B and C. If $\rho$ is not genuinely tripartite entangled, it is biseparable and has the form

$$\rho = \sum_{\lambda} (p_{\lambda} \rho_{\lambda}^{A} \otimes \rho_{\lambda}^{BC} + q_{\lambda} \rho_{\lambda}^{A} \otimes \rho_{\lambda}^{AC} + r_{\lambda} \rho_{\lambda}^{C} \otimes \rho_{\lambda}^{AB}),$$  \hspace{1cm} (17)

where $p_{\lambda}, q_{\lambda}$ and $r_{\lambda}$ are unnormalised probability distributions. For the case of one party using an untrusted device (top right of figure 1), using equation (17) in equation (8) leads to

$$\sigma_{a|l|x}^{BC} = \sum_{\lambda} p_{\lambda} p(a|x\lambda) \rho_{\lambda}^{BC} + q_{\lambda} \rho_{\lambda}^{AC} \otimes \sigma_{a|l|x}^{C} + r_{\lambda} \rho_{\lambda}^{C} \otimes \rho_{\lambda}^{AB}.$$  \hspace{1cm} (18)

The first summation term in equation (18) has the same structure as the decomposition in equation (9), with the only difference that now $\rho_{\lambda}^{BC}$ may even be entangled. Thus, the relevant set defined for this first decomposition term is

$$\Sigma^{BC}_{A:B:C} = \left\{ \sigma_{a|l|x}^{BC} \mid \sum_{\mu} D_{\mu}(a|x) \sigma_{\mu}^{BC}, \sigma_{\mu}^{BC} \geq 0 \right\},$$  \hspace{1cm} (19)

which clearly involves valid SDP constraints only. The second summation term in equation (18) has two main features: (i) it does not demonstrate steering from A to B, which implies that tracing out C will leave B with an LHS assemblage with respect to A; and (ii) it is separable across B:C. The first feature, having an LHS model, is readily translated to SDP constraints, as we have seen in the previous sections. The second one, separability, has to be relaxed to positivity under partial transposition, as explained in section 2.3. Thus, the relaxed set $\Sigma^{BC}_{B:AC}$ corresponding to the second decomposition term is given by

$$\Sigma^{BC}_{B:AC} = \left\{ \sigma_{a|l|x}^{BC} \mid \text{Tr}_{C} \left[ \sigma_{a|l|x}^{BC} \right] = \sum_{\mu} D_{\mu}(a|x) \sigma_{\mu}^{B}, \sigma_{\mu}^{B} \geq 0, (\sigma_{a|l|x}^{BC})^{T} \geq 0 \right\},$$  \hspace{1cm} (20)

The third summation term of equation (18) is identical to the second term, except that the roles of B and C are interchanged. From the previous claims, we can now write explicitly the SDP test for genuine tripartite entanglement with one party holding untrusted devices:

$$\min r \text{ s.t. } (1 - r) \sigma_{a|l|x}^{BC} + rI_{a|l|x}^{BC} \in \Sigma^{BC}_{A:B:C}$$  \hspace{1cm} (21)

and the dual formulation of this problem provides a witness $\hat{w}$, defined as in equation (6), such that $\hat{w}(\sigma_{a|l|x}^{BC}) > 0$ certifies that $\rho$ is genuinely tripartite entangled.

For the case of two parties using untrusted devices (bottom right of figure 1), substituting equation (17) in equation (12) gives

$$\sigma_{a|b|y}^{C} = \sum_{\lambda} (p_{\lambda} p(a|x\lambda) \sigma_{b|y\lambda}^{C} + q_{\lambda} p(b|y\lambda) \sigma_{a|l|x\lambda}^{C} + r_{\lambda} p(ab|xy\lambda) \sigma_{\lambda}^{C}),$$  \hspace{1cm} (22)

The first summation term of the decomposition obtained in equation (22) has only one main feature, which is that it may contain steering from B to C, but never from A to C. Hence, it defines the set $\Sigma^{C}_{A:BC}$ as
and denotes the two-qubit maximally entangled state is obtained from duality theory and has the same structure as equation \( \Sigma^C_{k} \). The second summation term appearing in equation \( \Sigma^C_{k} \) is straightforwardly defined in the same manner as \( \Sigma^C_{k} \) in equation \( \Sigma^C_{k} \). The third term in equation \( \Sigma^C_{k} \), on the other hand, has two features: (i) it corresponds to an LHS assemblage and (ii) the probability distribution \( p(ab(xy)) \) is quantum, in the sense that it arises from local measurements performed on (possibly entangled) states \( \rho^A_{AB} \). Deciding if a probability distribution is quantum is not straightforward because of the existence of quantum correlations lying outside the local set \( \mathcal{NS} \). The SDP test for genuine tripartite entanglement where two parties use untrusted devices is therefore

\[
\min_{r} \text{ s.t. } (1 - r)\sigma^C_{ab|xy} + r1_{ab|xy} = \gamma^A_{ab|xy} + \gamma^B_{ab|xy} + \gamma^C_{ab|xy} \leq 1, \quad \gamma^A_{ab|xy} \in \Sigma^C_{A:BC}, \quad \gamma^B_{ab|xy} \in \Sigma^C_{B:AC}, \quad \gamma^C_{ab|xy} \in \Sigma^C_{C:AB}
\]

and the corresponding semi-device-independent witness \( \overline{w} \) is obtained from duality theory and has the same structure as equation \( \Sigma^C_{k} \).

### 2.5. Multipartite steering of the W state

Here we provide numerical values for the three-qubit W state

\[
|W\rangle = \frac{1}{\sqrt{2}} (|001\rangle + |010\rangle + |100\rangle)
\]

and discuss the fact that parties A, B, and C can check for all kinds of entanglement without trusting the devices of the others. In all that follows we consider that the measurements performed by all trusted boxes are Pauli observables, namely, \( X, Y \) and \( Z \). Our theoretical findings regarding the witness values \( r^* \) are summarised in Table 1.

Since the W state is symmetric, all reductions are equivalent regardless of the party that is discarded. Specifically, \( \rho^{\text{red}} = 2/3|\psi^+\rangle \langle \psi^+| + 1/3|00\rangle \langle 00| \), where \( |\psi^+\rangle \) denotes the two-qubit maximally entangled state \( |\psi^+\rangle = 1/\sqrt{2} (|01\rangle + |10\rangle) \). The reduced state turns out to be steerable with a theoretical violation of \( r^* = 0.11 \). This value is relatively small because of the detrimental contribution of the separable state \( |00\rangle \). Such violation not only guarantees the presence of entanglement in the reduced state, but it also certifies the presence of entanglement across any bipartition of the tripartite network, regardless of whether the third party (the discarded one) is using a trusted device or not, as explained in the first paragraph of section 2.1. We also notice

**Table 1.** Witness values \( r^* \) from the three-qubit W state. For each of the quantum information tasks appearing in the first column, the corresponding witness is constructed as explained in section 2 and in section 4.2. A strictly positive value of the semi-device-independent witness certifies the presence of: entanglement in the reduced state (first row), entanglement in the full tripartite state (second and third rows), genuine multipartite entanglement (fourth and fifth rows). See main text for details.

| Certification of: | Theory | Experiment |
|-------------------|--------|------------|
| Ent. in reductions | 0.1112 | 0.07 ± 0.01 |
| Ent. (1 untrusted) | 0.7297 | 0.77 ± 0.01 |
| Ent. (2 untrusted) | 0.5355 | 0.50 ± 0.008 |
| GME (1 untrusted)  | 0.4581 | 0.41 ± 0.01 |
| GME (2 untrusted)  | 0.3244 | 0.32 ± 0.01 |

\[
\Sigma^C_{A:BC} = \left\{ \sigma^C_{ab|xy} : \sigma^C_{ab|xy} = \sum_{\mu} \delta_\mu (a|x) \sigma_{\mu}^C, \quad \sigma_{\mu}^C \geq 0 \right\}.
\]

The second summation term appearing in equation \( \Sigma^C_{k} \) has the same structure as the first one, thus the set \( \Sigma^C_{B:AC} \) is straightforwardly defined in the same manner as \( \Sigma^C_{A:BC} \) in equation \( \Sigma^C_{k} \). The third term in equation \( \Sigma^C_{k} \), on the other hand, has two features: (i) it corresponds to an LHS assemblage and (ii) the probability distribution \( p(ab|xy) \) is quantum, in the sense that it arises from local measurements performed on (possibly entangled) states \( \rho^A_{AB} \). Deciding if a probability distribution is quantum is not straightforward because of the existence of quantum correlations lying outside the local set \( \mathcal{NS} \). The SDP test for genuine tripartite entanglement where two parties use untrusted devices is therefore

\[
\min_{r} \text{ s.t. } (1 - r)\sigma^C_{ab|xy} + r1_{ab|xy} = \gamma^A_{ab|xy} + \gamma^B_{ab|xy} + \gamma^C_{ab|xy} \leq 1, \quad \gamma^A_{ab|xy} \in \Sigma^C_{A:BC}, \quad \gamma^B_{ab|xy} \in \Sigma^C_{B:AC}, \quad \gamma^C_{ab|xy} \in \Sigma^C_{C:AB}
\]

and the corresponding semi-device-independent witness \( \overline{w} \) is obtained from duality theory and has the same structure as equation \( \Sigma^C_{k} \).
that it is still an open question whether the reduced state of the W state can violate any Bell inequality [20, 21],
while here we show that it does present steering.

For the tripartite W state, we observe the presence of entanglement and GME both in the ‘one untrusted’
scenario and in the ‘two untrusted’ scenario as well (see lines 2–5 of table 1). Note that the violations for the ‘one
untrusted’ scenario are always better than for the ‘two untrusted’ scenario, because in the former case there is
more useful information available (about the state) than in the latter case. The values for tripartite entanglement
are also always better than the values obtained for GME, as the presence of the latter implies the presence of
the former, but the converse is not true in general; that is, a state might be entangled without being GME.

3. One-sided device-independent randomness certification

3.1. Scenario and guessing probability

One of the most interesting applications following the semi-device-independent quantum information
approach is the semi-device-independent random number generation [16, 22]. To carry out this task, one must
bound the predictability of the outcomes of the black boxes (parties holding untrusted devices), only from the
observation of a certain assemblage by the parties holding trusted devices in the network. Just as in the previous
sections, the black boxes might be provided with any a priori unknown quantum state $\rho$, but now $\rho$ may even be
correlated with some other quantum system $\rho^{ABCE}$ in the possession of a malicious eavesdropper $E$, such that
$\rho = \text{Tr}_E [\rho^{ABCE}]$. Furthermore, semi-device-independent random number generation is appealing because it
enables a corresponding cryptographic task, namely, semi-device-independent quantum key distribution [23].

As an interesting example, here we implement the methods of [16] to certify the optimal amount of one-
sided randomness present in the string of outcomes of two black boxes, when the third one remains trusted.
Since these methods can only be applied on a bipartite scenario, we shall consider that the two black boxes are
held by a single party performing measurements labelled $m = (x, y)$ and obtaining outcomes labelled
$s = (a, b)$, as illustrated in figure 2.

The predictability of the outcome $s$ when a given measurement $m^* \in \mathcal{M}$ is chosen is quantified by the guessing probability $G_\epsilon (m^*)$: the probability that $E$ guesses correctly the value of $s$, optimised over all of $E$’s possible
strategies, and conditioned on the observation of the assemblage $\sigma_{s|m}^\epsilon$ by the party $C$ [16, 24]. Formally,
$$G_\epsilon (m^*) = \max \sum_\epsilon \text{Tr} [\sigma_{s=\epsilon|m}^\epsilon]$$

subject to \( \sum_\epsilon \sigma_{s=\epsilon|m} = \sigma \) \\forall \epsilon, m, m' \\text{and} \ \sum_\epsilon \sigma_{s=\epsilon|m} \geq 0 \ \forall \epsilon, m, \epsilon \),

where we used $\text{Tr} [\sigma_{s=\epsilon|m}^\epsilon] = p(\epsilon)p(s|\epsilon, m^*)$ to re-express the objective function in the first line of equation (27).

Intuitively, Eve may prepare any convex combination of the unnormalised assemblages $\{\sigma_{s=\epsilon|m}^\epsilon\}_k$, which are such
that, whenever Eve obtains the result $\epsilon = s$ after measuring her system, she then guesses that the outcome of the
black boxes was $s$. Thus, Eve needs as many preparations $\{\sigma_{s=\epsilon|m}^\epsilon\}_k$ as possible values that $s$ can take, and $\sigma_{s=\epsilon|m}$
would be the assemblage obtained if the information of Eve’s outcome $\epsilon$ were available. The first constraint in
equation (27) translates the fact that Eve has to reproduce on average the observed assemblage, since otherwise
her attack would be detected by the party holding the trusted device. The second and third constraints, non-
signalling and positivity respectively, guarantee that the assemblages prepared by Eve stem from quantum
theory. In fact, any bipartite non-signalling assemblage admits a quantum realisation [25, 26].

Once again, duality theory allows us here—from the dual formulation of equation (27)—to obtain a steering inequality (i.e. a linear functional $\tilde{\varphi}$) acting on the set of assemblages of $C$, having the same structure as
equation (16), such that $\tilde{\varphi} (\sigma) = G_\epsilon (m^*)$. Finally, assuming Independent and identically distributed (ID)
rounds in the experiment, the amount of genuine random bits certified is given by $R = -\log_2 (G_\epsilon (m^*))$, the

---

Figure 2. One-sided randomness certification scenario. A and B are thought as a single party holding two untrusted boxes, performing
at each round a measurement $m$ and obtaining some result $s$. This scenario allows us to analyse the amount of randomness of the result
$s$ when $\sigma_{s|m}$ is observed by $C$. 

---
min-entropy of the semi-device-independent guessing probability \[24\]. Note that, when \(G_e(m^*) = s\) no random bits can be certified \((R = 0)\), as \(E\) guesses with probability 1 the outcome of the boxes and thus there is no unpredictability. On the other hand, any value \(G_e(m^*) < s\), guarantees unpredictability and hence provides a strictly positive amount of randomness \(R > 0\).

### 3.2. One-sided device-independent randomness certification from bipartitions of the W state

We first analysed the reduced state \(\rho_{\text{red}}\) of the three-qubit W state. Though we found that the state is steerable (as shown in the first line of table 1), it is not possible to extract one-sided genuine randomness from such reduced state with the measurements considered here. On the other hand, one-sided randomness certification turns out to be appealing when bipartitions of the tripartite W state are considered. In fact, when two of the boxes are seen as a single untrusted measurement \(m = (x, y)\) performed on some unknown quantum state, while the other qubit, \(C\), uses trusted measurements (see figure 2), we manage to certify \(-\log_2(1/3) \approx 1.58\) random bits from the outcome \(s = 00, 01, 10, 11\) of the measurement \(m^*\) corresponding to the observables \(\hat{X}\) and \(\hat{Z}\) acting on the two-qubit subspace reduction of the W state.

The fact that no one-sided genuine randomness could be extracted from the reduced state of the three-qubit W state is unfortunate but interesting. This is analogous to a similar phenomenon, known as bound randomness \[27\], which arises in the fully device-independent scenario where the two parties hold untrusted devices. More precisely, in the fully device-independent scenario, bound randomness arises in non-local correlations for which a non-signalling eavesdropper can find out a posteriori the result of any implemented measurement. Thus, the fact that any reduction of the W state is steerable but does not allow for one-sided randomness certification, may tentatively be referred to as one-sided bound randomness, a form of steerable correlations for which an eavesdropper can predict the result of any of the measurements performed on the untrusted side.

### 4. Experimental results

#### 4.1. Setup

To demonstrate the practical utility of the theoretical results presented in sections 2 and 2.5, we produced a three-qubit W state using photon pairs produced by spontaneous parametric down conversion (SPDC). Figure 3 shows the experimental setup. Two 1 mm thick type-I non-linear BBO crystals with optical axes oriented perpendicularly were pumped with a 325 nm continuous-wave He-Cd laser, producing degenerate photon pairs centred around 650 nm. Using an additional half-wave plate in the path of photon 1, the crossed-crystal arrangement produces two polarisation-entangled photons in the target state \[28\]:

\[
|\psi\rangle = \cos \theta |VH\rangle_{12} + e^{i\phi} \sin \theta |HV\rangle_{12}.
\]

Qubits \(B\) and \(C\) were encoded in the polarisation of the photons 1 and 2, respectively. Qubit \(A\) was encoded in the path of photon 2. Initially, qubit \(A\) is in the state \(|0\rangle_A\). To produce the W state, we entangle the path and polarisation degrees of freedom (DOF) of photon 2 using a polarisation-dependent Mach-Zehnder
interferometer composed of two beam displacers (BDs) and several half-wave plates (HWPs), as described in more detail in [29, 30]. The angles of the HWPs are shown in figure 3. We label the input and output paths (0 and 1 in the figure) such that when the polarisation state is $|H\rangle_C$, the output state is $|0H\rangle_{AC}$. For input vertical polarisation, the interferometer implements the transformation

$$|0V\rangle_{AC} \rightarrow \frac{1}{\sqrt{2}}|0V\rangle_{AC} + \frac{1}{\sqrt{2}}|1H\rangle_{AC}. \quad (29)$$

By controlling the polarisation of the pump laser [28], the initial polarisation-entangled state was prepared with $\cos \theta = 1/\sqrt{3}$ and $\varphi = 0$. Renaming the polarisation state $|H\rangle \rightarrow |0\rangle$ and $|V\rangle \rightarrow |1\rangle$, our setup produces a three-qubit state that is ideally a $W$ state [29]. In the appendix we provide details on the stability of the setup, the characterisation of the $W$ state and of its reconstructed density matrix.

A set of 216 joint projective measurements in the $\hat{X}$, $\hat{Y}$ and $\hat{Z}$ Pauli basis was performed on all three qubits, which allowed us to evaluate the SDP tests developed above. To perform projective measurements on qubit $B$ (polarisation of photon 1), the usual system consisting of a quarter-wave plate (QWP), HWP and a polarising beam splitter (PBS) is used. For projective measurements on qubit $C$, a QWP, HWP and BD are used. This measurement system works in much the same way as that of qubit $B$; however, after the projection on a given polarisation state, the BD maps the state of the path DOF at its input into the polarisation DOF at its output. In this fashion, the state describing the path DOF, which is now encoded in the polarisation DOF, can be measured using the same arrangement as in photon 1. The photons were spectrally filtered with 3 nm full width at half maximum (FWHM) bandwidth filters centred at 650 nm (not shown in the figure), coupled into single-mode optical fibres using $10 \times$ microscope objectives and registered with single photon detectors and coincidence electronics (the ‘&’ box in figure 3).

4.2. Practical considerations

The methods described in section 2 were designed to detect entanglement and certify randomness from an observed physical assemblage $\sigma^{\text{phys}}$. However, due to the unavoidable problem of finite statistics in any experiment, the assemblage that is experimentally observed $\sigma^{\text{exp}}$ does not satisfy the non-signalling property. To overcome this problem, we took the following steps. First, we construct a physical assemblage that approximates the experimental data. This step is done with a least-squares optimisation, an SDP programme that minimises the distance from the experimental assemblage to the set of physical assemblages bounded by the non-signalling constraints. The second step consists of using the constructed physical assemblage to obtain the desired witness $\hat{w}^{\text{phys}}$, following the SDP techniques for entanglement detection. The last step is to apply the derived witness, which is simply a linear functional, to the experimental assemblage to show the presence of entanglement/ randomness in the network.

4.3. Experimental multipartite entanglement detection in the steering scenario

Our experimental results are summarised in table 1. The error bars were calculated by performing Monte Carlo simulation (494 rounds) assuming Poissonian coincidence counting statistics of our measurement results. Experimentally, the reduced state is not entirely symmetric because of imperfections in the optical setup, such as temporal and spatial mode mismatch in the interferometer. Thus, we analysed all reductions and found that the highest violation of $0.07 \pm 0.01$ is obtained when discarding party $B$, corresponding to the polarisation of photon 1. This is due to the fact that the entanglement that survives, between qubits $A$ and $C$, is encoded entirely in the polarisation and spatial qudits of photon 2.

As far as the experimental certification of tripartite entanglement and genuine multipartite entanglement (GME) are concerned, the corresponding observed witness values are shown in lines 2–3 and 4–5 of table 1, respectively. One obtains a strictly positive value (violation) for these two types of tripartite entanglement, both in the ‘one untrusted’ and in the ‘two untrusted’ scenarios. The experimental witness values are close to the theoretical ones, although these do not always fall within the error margins obtained. This is expected since the experimental state is not perfectly pure (see the appendix). The case where the measured value agrees with the theory within the error interval corresponds to the situation where the correlations between two internal degrees of freedom of the same photon (path and polarisation) are the most relevant. In this special case, the purity of the reduced state can be very high experimentally. Even with these small discrepancies between theory and experiment, we successfully certify the presence of entanglement and GME in the considered semi-device-independent networks. Please note that, for completeness, the reader may find the numerical values for all steering inequalities described in this work at the Git online repository: github.com/mattaron2tes/Steering.

4.4. Experimental one-sided device-independent randomness certification

The scenario presented in figure 2 turns out to be relevant and well suited for our experimental implementation of the photonic $W$ state (see section 4), as a physical bipartition of the state stems between the two photons
produced. In this sense, it is natural to consider the photon encoding both polarisation and path qubits as a single party, and analyse the amount of randomness of the outcomes \( s = (a, b) \) retrieved when untrusted measurements are performed on such physical part of the system.

First of all, we checked that the experimental data of each of the the reduced states does not reveal any amount of one-sided randomness, as predicted by the theory. Subsequently, we managed to certify 0.26 ± 0.04 bits from the bipartitions of the W state. This value falls far from the theoretical value of \(-\log_2(2/3) \approx 1.58\) bits. This discrepancy is due to the fact that the amount of randomness is extremely sensitive to the visibility of the pure W state with respect to white noise. For instance, we observe that for visibility of 0.994 the number of one-sided random bits that can be certified is already less than unity. The obtained theoretical results are nevertheless encouraging for the near future, as sources with better visibilities should allow to certify higher and higher amounts of genuine random bits.

5. Conclusion

In conclusion, we show that a recently introduced method for certification of entanglement when semi-device-independent measurements realised in a quantum network can be successfully employed to certify all types of entanglement from a three-qubit W state. Furthermore, such semi-DI entanglement certification is achieved in all tripartite steering scenarios, and without the need to consider different measurements among different scenarios. We study in detail the case of a tripartite configuration, even though the method is valid for larger networks. Entanglement is witnessed for a few illustrative combinations of trusted and untrusted measurements. We also present experimental results obtained with a proof-of-principle optical setup. We observe good qualitative agreement between theory and experimental results, and verify the strong dependence of the witnessed entanglement on the degree of purity of the initial state.

We further investigate the certification of genuine randomness. We observe that one-sided randomness cannot be certified. However, considering bipartitions of the tripartite W state and the bipartition with two elements untrusted, it is possible in principle to certify up to 1.58 random bits. Analysing the experimental implementation, 0.26 ± 0.04 random bits were certified. This in fact constitutes the first experimental demonstration of one-sided device-independent randomness certification. This discrepancy between the expected and measured values emphasises the critical dependence of the amount of random information certified on the purity of the initial state. Our results promote the W state as a key candidate for the implementation of device semi independent protocols, where some of the parties use untrusted devices.

Acknowledgements

We thank O Jimenez-Farias for discussions. This work was supported by the Mexican CONACyT graduate fellowship programme, the Ramon y Cajal fellowship, Spanish MINECO (Severo Ochoa grant SEV-2015-0522 and FoQus), the AXA Chair in Quantum Information Science, the Generalitat de Catalunya (SGR875), Fundacio Privada Cellex, ERC CoG QITBOX and the ERC AdG NLST. Financial support was also provided by Brazilian agencies FAPERJ, CNPq, CAPES and the National Institute of Science and Technology for Quantum Information.

Appendix. Experimental state

Using quantum state tomography, we reconstruct the experimental density matrix \( \rho_E \), shown in figure 4(a), to check the quality of the W state produced. We found that purity \( P = Tr(\rho_E^2) \) of the measured state is 0.88 ± 0.02 while its fidelity \( F_W = \langle W | \rho_E | W \rangle \) with respect to the ideal W state is 0.92 ± 0.01. The errors in \( P \) and \( F_W \) were calculated using Monte Carlo simulation assuming Poissonian coincidence counting statistics.

The degree of purity and the fidelity can be considered high for a tripartite system, when compared to other physical realisations of multipartite states. Even comparing with other photonic setups, our experiment produce better quality three-qubit states with larger count rates. For instance, in [31] the W state is achieved using four photons produced by SPDC. In that experiment the fidelities attained are up to 0.88 with rates of coincidences 1000 times smaller than in our experiment. These characteristics highlight the reliability of using two degrees of freedom of a pair of photons rather than three or four photons, as a platform to test theoretical strategies related to three and four-partite entangled states.

Concerning the purity of the experimental bipartite entangled states, which affects the visibility of the W states, we notice that considerably high purities in the range of 0.99 have been achieved for bipartite states. For increasing the number of parties, obtaining experimental entangled states with such high purity is increasingly
Figure 4. Full density matrix and examples of reconstructed conditional density matrices for ρ\_\text{AC} when party B uses untrusted measurements. The real and imaginary parts of the density matrices are shown in the left and right columns, respectively. Plots (a) and (b) show the full density matrix ρ\_\text{E}, (c) and (d) show ρ\_\text{AC} when B projects onto \(|0\rangle\), (e) and (f) show ρ\_\text{AC} when B projects onto \(|1\rangle\), (g) and (h) show ρ\_\text{AC} when B projects onto \(|R\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}\), (i) and (j) show ρ\_\text{AC} when B projects onto \(|R\rangle = (|0\rangle + |1\rangle)/\sqrt{2}\).
challenging, since the purity decreases exponentially with the number of parties in the presence of noise. The present realisation with purity and fidelity to the W state in the range 0.9 is enough to demonstrate some randomness certification and to highlight the sensitivity of this task to the visibility of the W state.

The discussed experimental imperfections also imply a discrepancy at the level of the steering witnesses, which are available online at: https://github.com/mattarcon2tes/Steering. More precisely, the differences which may be found on the experimental witnesses with respect to the theoretical ones—obtained from pure assemblages of the W state—is due to the non-unit purity and fidelity of the experimental state, but also is due to the signalling character of the experimental data, which forces one to consider a non-signalling assemblage to extract the inequality, as explained in section 4.2.

References

[1] Schrodinger E 1935 Naturwissenschaften 23 807
[2] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Rev. Mod. Phys. 81 865
[3] Guhne O and Toth G 2009 Phys. Rep. 474 1 ISSN 0370-1573
[4] Rosset D, Ferretti-Schöbitz R, Bancal J-D, Gisin N and Liang Y-C 2012 Phys. Rev. A 86 062325
[5] Brunner N, Cavalcanti D, Pironio S, Scarani V and Wehner S 2014 Rev. Mod. Phys. 86 419
[6] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 Phys. Rev. Lett. 98 230501
[7] Bancal J-D, Gisin N, Liang Y-C and Pironio S 2011 Phys. Rev. Lett. 106 250404
[8] Barreiro J T, Bancal J-D, Schindler P, Nigg D, Hennrich M, Montz T, Gisin N and Blatt R 2013 Nat. Phys. 9 559
[9] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kürtsiefer C and Makarov V 2011 Nat. Commun. 2 349
[10] Hensen B et al 2015 Nature 526 682
[11] Shalm L K et al 2015 Phys. Rev. Lett. 115 250402
[12] Giustina M et al 2015 Phys. Rev. Lett. 115 250401
[13] Wiseman H M, Jones S J and Doherty A C 2007 Phys. Rev. Lett. 98 140402
[14] Cavalcanti D, Szegedy A, Agular G H, Nery R V, Ribeiro P H S and Walborn S P 2015 Nat. Commun. 6 7941
[15] Cavalcanti D and Szegedy A 2017 Rep. Prog. Phys. 80 026401
[16] Passaro E, Cavalcanti D, Szegedy A and Acín A 2015 New J. Phys. 17 113010
[17] Boyd S and Vandenberghe L 2004 Convex Optimization (New York, NY, USA: Cambridge University Press) ISBN 0521833787
[18] Navascués M, Pironio S and Acín A 2007 Phys. Rev. Lett. 98 010401
[19] Navascués M, Pironio S and Acín A 2008 New J. Phys. 10 073013
[20] Sohbi A, Zaquine I, Diamanti E and Markham D 2015 Phys. Rev. A 91 022101
[21] Barnea T J, Pütz G, Brask J B, Brunner N, Gisin N and Liang Y-C 2015 Phys. Rev. A 91 032108
[22] Law Y Z, Thinh L P, Bancal J-D and Scarani V 2014 J. Phys. A: Math. Theor. 47 424028
[23] Branciard C, Cavalcanti E G, Walborn S P, Scarani V and Wiseman H M 2012 Phys. Rev. A 85 010301
[24] Nieto-Silleras O, Pironio S, Silman J, Nieto-Silleras O et al 2014 New J. Phys. 16 013035
[25] Hughston L P, Jozsa R and Wootters W K 1993 Phys. Lett. A 183 14 ISSN 0375-9601
[26] Sainz A B, Brunner N, Cavalcanti D, Skrzypczyk P and Vértesi T 2015 Phys. Rev. Lett. 115 190403
[27] Acín A, Cavalcanti D, Passaro E, Pironio S and Skrzypczyk P 2016 Phys. Rev. A 93 012319
[28] Kwiat P G, Waks E, White A G, Appelbaum I and Eberhard P H 1999 Phys. Rev. A 60 2373
[29] Farias O J, Aguilar G H, Valdés-Hernández A, Ribeiro P H S, Davidovich L and Walborn S P 2012 Phys. Rev. Lett. 109 150403
[30] Aguilar G H, Valdés-Hernández A, Davidovich L, Walborn S P and Ribeiro P H 2014 Phys. Rev. Lett. 113 240501
[31] Kiesel N, Schmid C, Törl G, Solano E and Weinfurter H 2007 Phys. Rev. Lett. 98 063604