Witnessing arbitrary bipartite entanglement in a measurement-device-independent way

Arindam Mallick* and Sibasish Ghosh†

Optics and Quantum Information Group, The Institute of Mathematical Sciences, HBNI, C. I. T. Campus, Taramani, Chennai 600113, India

(Received 10 January 2017; published 16 November 2017)

Experimental detection of entanglement of an arbitrary state of a given bipartite system is crucial for exploring many areas of quantum information processing. But such a detection should be made in a device-independent way if the preparation process of the state is considered to be faithful, in order to avoid detection of a separable state as an entangled one. The recently developed scheme of detecting bipartite entanglement in a measurement-device-independent way [Phys. Rev. Lett. **110**, 060405 (2013)] does require information about the state. Here, by using Auguisiak *et al.*'s universal entanglement witness scheme for two-qubit states [Phys. Rev. A **77**, 030301 (2008)], we provide a universal entanglement detection scheme for two-qubit states in a measurement-device-independent way. We also provide a set of universal witness operators for detecting NPT-ness (negative under partial transpose) of two-qudit states in a measurement-device-independent way. We conjecture that no such universal entanglement witness scheme exists for PPT (positive under partial transpose) entangled states. We also analyze the robustness of some of the experimental schemes—for detecting entanglement in a measurement-device-independent way—under the influence of noise in the inputs (from the referee) as well as in the measurement operator.

DOI: 10.1103/PhysRevA.96.052323

I. INTRODUCTION

Entanglement is known to be a resource for quantum information processing, like quantum cryptography [1], teleportation [2], quantum metrology [3], channel capacity [4,5], etc. Moreover, it helps to speed up computation sometimes [6] over the existing classical algorithms. Also, understanding entanglement is necessary to reveal the various nonclassical nature of the physical world. Entanglement in quantum theory correlates two parties in such a way that at the individual levels, they loose their independent state vector descriptions. Mathematically, two systems $\mathcal{A}$ (the quantum system possessed by Alice) and $\mathcal{B}$ (the quantum system possessed by Bob) are separable iff their joint state ρ can be expressed as $\sum_j \alpha_j {\rho_{\mathcal{A}}}^{(j)} \otimes {\rho_{\mathcal{B}}}^{(j)}$ which acts on the Hilbert space $\mathcal{H}_{\mathcal{AB}} = \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, where $\sum_j \alpha_j = 1$ and $0 \leqslant \alpha_j \leqslant 1 \, \forall j$, ${\rho_{\mathcal{A}}}^{(j)}$ and ${\rho_{\mathcal{B}}}^{(j)}$ are density matrices acting on $\mathcal{H}_{\mathcal{A}}$ and $\mathcal{H}_{\mathcal{B}}$, respectively. If the joint state can't be written in the above form, we call them entangled [7].

Deciding whether an unknown state of a given bipartite quantum system is entangled or separable, remains a challenging problem [8–10] right from the initial stage of quantum information theory. People tried to see the presence of entanglement in a state experimentally through some Bell-inequality violation, but there are entangled states which do not violate any such inequality [11]. Given any entangled state $\rho_{\mathcal{AB}}$, it is (in principle) possible to find out an entanglement witness (EW) operator W, whose measurement can distinguish the given entangled state from all possible separable states of the system, and the measurement is, in principle, implementable experimentally, using local measurement settings, (possibly) supported by classical communication. It may be recalled that an entanglement witness is a Hermitian operator W: $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}} \to \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$ such that there exists at least one entangled state $\rho_{\mathcal{AB}}$ on $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$, for which $\mathrm{Tr}[W\rho_{\mathcal{AB}}] < 0$ while $\mathrm{Tr}[W\sigma_{\mathcal{AB}}] \geq 0$ for all separable states $\sigma_{\mathcal{AB}}$ on $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. So W witnesses the entanglement in the state $\rho_{\mathcal{AB}}$. But $\mathrm{Tr}[W\sigma_{\mathcal{AB}}] \geq 0$ does not necessarily imply that $\sigma_{\mathcal{AB}}$ is separable [12]. In general, W depends on the the form of entangled state $\rho_{\mathcal{AB}}$, and hence it does not have a universal character. Thus a state-independent witness operator is a desired one for most practical purposes.

The conventional entanglement detection strategies are based on local measurements to be performed on individual subsystems $\mathcal{A}$ and $\mathcal{B}$. In this case, both the local measuring apparatuses should be necessarily perfect. In fact, if some measurement results get lost or some overcounting occurs during the measurement, it may lead to an erroneous conclusion about entanglement of the state $\rho_{\mathcal{AB}}$. In Ref. [13], the time shift attack [14] has been used experimentally which causes identification of a separable state as an entangled one. Such a scenario can be avoided if one can witness entanglement in a measurement-device-independent way, described below.

Recently, Branciard *et al.* [15] demonstrated implementation of any entanglement witness operator in a measurement-device-independent (MDI) way using Buscemi's work on the semiquantum nonlocal game [16]. This scheme of Branciard *et al.* [15] guarantees that no separable state will get detected as an entangled one, irrespective of the kind of noise effects present during the measurement (see [17]). But their scheme depends on the form of the shared bipartite state, and hence, their scheme lacks universality, that is, it may not be able to detect entanglement in an *arbitrary* entangled state of the bipartite system even though *no* separable state (known or unknown) of the system will get detected as an entangled one in the MDI scheme of Branciard *et al.* [15].

Augusiak *et al.* [18] showed the existence of a universal entanglement witness operator that can detect entanglement in *any* two-qubit state, depending on the Peres-Horodecki PPT criteria [7,19]. But this does not address measurement-device-independent implementation of the witness operator, and, moreover, it is restricted to the two-qubit case only.

In this paper, we first show that this two-qubit universal entanglement witness operator of Augusiak *et al.* [18] can be

*marindam@imsc.res.in
†sibasish@imsc.res.in

implemented in a measurement-device-independent way (see also [19]). We then generalize this idea for higher dimensional bipartite NPT states and find out a set of finite numbers of universal witness operators for witnessing NPT-ness in an unknown state of any *given* bipartite system. We also argue here that resource-wise, our aforesaid NPT-ness witness scheme is better than using tomography to identify the state. We conjecture that no universal entanglement witness operator can exist to detect entanglement in an unknown PPT state of any given bipartite system of dimension greater than six. We also point out that, in the aforesaid scheme of Branciard *et al.*'s measurement-device-independent entanglement witness [15], if some general type of noise is added with the inputs or with the measurement operator, the referee will not face any problem in witnessing entanglement provided he knows the character of the noise (here we will provide analysis for a particular type of noise and general treatment is given in Appendix 2). In case the referee doesn't know the character of noise, we show how much robust the witnessing operation can be. Note that such a noise analysis is particularly important in the case of experimental verification of the measurement-device-independent entanglement witness (MDIEW) scheme [15].

Our article is organized as follows. In Secs. I A and I B, we, respectively, describe briefly the measurement-device-independent (MDI) scheme of the entanglement witness (EW) [15] and the witness operator for detecting entanglement in an arbitrary two-qubit state [18]. Section II is devoted to MDI implementation of the two-qubit universal EW of Auguisiak *et al.* [18]. Section III describes the universal witness for NPT-ness of two-qudit states. Section IV describes the conjecture about the impossibility of the existence of a universal witness operator for bipartite PPT-entangled states. In Sec. V, we analyze the possible noise effects in the experimental implementation scheme of Ref. [15]. We draw the conclusion of our work in Sec. VI.

A. Measurement-device-independent scheme of entanglement witness

This scheme starts as a cooperative game played between two parties Alice (possessing the quantum system $\mathcal{A}$) and Bob (possessing the quantum system $\mathcal{B}$), who receive states τ_s (of a quantum system $\mathcal{A}_0$) and ω_t (of a quantum system $\mathcal{B}_0$), respectively, as inputs from a referee, who then ask them to produce outputs a and b, respectively. Here $\dim(\mathcal{H}_{\mathcal{A}_0}) = \dim(\mathcal{H}_{\mathcal{A}}) = d_{\mathcal{A}}$ and $\dim(\mathcal{H}_{\mathcal{B}_0}) = \dim(\mathcal{H}_{\mathcal{B}}) = d_{\mathcal{B}}$, and for our analysis, we consider $d_{\mathcal{A}} = d_{\mathcal{B}} = d$. During the game, Alice and Bob aren't allowed to communicate anyway, but before starting the game, they have to decide upon their strategies where they may share *a priori* a bipartite state $\rho_{\mathcal{AB}}$. If the state $\rho_{\mathcal{AB}}$ is entangled they can always achieve an average pay-off which is more than the case when $\rho_{\mathcal{AB}}$ is a separable state. So, from the average pay-off values, the referee can conclude whether the corresponding shared state was entangled or separable (after knowing the maximum average payoff for all possible separable states). To produce outcomes of the game, each party has to perform local joint projective measurement on their individual inputs (from the referee) and their individual subsystems of the shared state (see Fig. 1 for details).

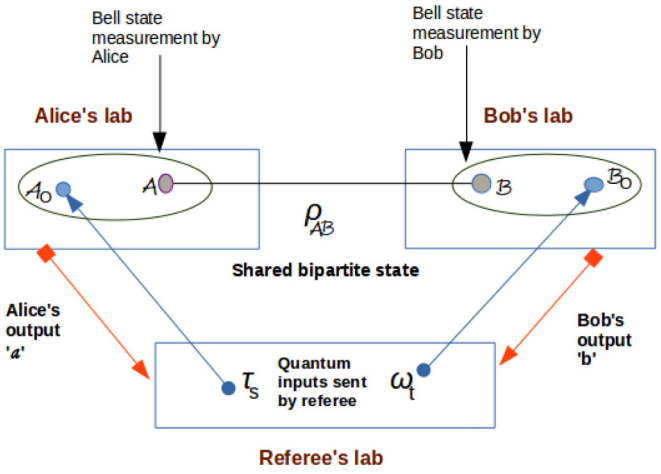

FIG. 1. Alice and Bob perform Bell state measurement on the states of the joint systems $\mathcal{A}_0\mathcal{A}$ and $\mathcal{B}\mathcal{B}_0$, respectively. Blue arrows are lossless quantum channels for sending input states to Alice and Bob. Red arrows correspond to the lossless classical channels for receiving the outputs. Green ellipses indicate joint Bell state measurement performed by the players.

The authors of [15] described the aforesaid projective measurement in the maximally entangled state,

$$|\Phi\rangle_{\mathcal{A}_0\mathcal{A}} = |\Phi\rangle_{\mathcal{B}\mathcal{B}_0} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d,$$

with probability of output $(a,b) = (1,1)$ for the given quantum input pair (τ_s,ω_t) being $P_{\rho_{\mathcal{AB}}}(1,1|s,t) = \mathrm{Tr}((|\Phi\rangle_{\mathcal{A}_0\mathcal{A}}\langle\Phi| \otimes |\Phi\rangle_{\mathcal{B}\mathcal{B}_0}\langle\Phi|)(\tau_s \otimes \rho_{\mathcal{AB}} \otimes \omega_t))$, and showed that if the average payoff function is $\Pi(\rho_{\mathcal{AB}}) = \sum_{s,t} \tilde{\beta}_{st} P_{\rho_{\mathcal{AB}}}(1,1|s,t)$ then

$$\begin{aligned} I(\rho_{\mathcal{AB}}) &:= \max\{\Pi(\sigma_{\mathcal{AB}})\} - \Pi(\rho_{\mathcal{AB}}) \\ &= \max_{\sigma_{\mathcal{AB}}} \left\{ \sum_{s,t} \tilde{\beta}_{st} P_{\sigma_{\mathcal{AB}}}(1,1|s,t) \right\} - \sum_{s,t} \tilde{\beta}_{st} P_{\rho_{\mathcal{AB}}}(1,1|s,t) \\ &= \sum_{s,t} \beta_{st} P_{\rho_{\mathcal{AB}}}(1,1|s,t), \end{aligned} \tag{1}$$

where the maximization is performed over all possible separable states $\sigma_{\mathcal{AB}}$ of the bipartite system, and β_{st} is the linear function of $\tilde{\beta}_{st}$ for all s,t. The outcome $(1,1)$ is nothing but the successful projection of the state $\tau_s \otimes \rho_{\mathcal{AB}} \otimes \omega_t$ on the operator $|\Phi\rangle_{\mathcal{A}_0\mathcal{A}}\langle\Phi| \otimes |\Phi\rangle_{\mathcal{B}\mathcal{B}_0}\langle\Phi|$, and β_{st} is the linear function of the pay-off value corresponding to the input state pair (τ_s,ω_t).

The aim here is to use the signature of $I(\rho_{\mathcal{AB}})$ for witnessing entanglement in $\rho_{\mathcal{AB}}$. In particular, Branciard *et al.* [15] showed $I(\rho_{\mathcal{AB}})$ to be proportional to $\mathrm{Tr}[W\rho_{\mathcal{AB}}]$ by expressing the witness operator W as

$$W = \sum_{s,t} \beta_{st} \tau_s^T \otimes \omega_t^T, \tag{2}$$

which, in principle, is possible in this case as the inputs τ_s (to Alice) and ω_t (to Bob)—supplied by the referee—are sufficient enough in number to span the linear space of all Hermitian operators on $\mathcal{H}_{\mathcal{AB}} \equiv \mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. The referee can determine

the values of the coefficients β_{st} accordingly prior to the game, and hence, he or she can identify whether the shared state is entangled or separable from the sign of $I(\rho_{\mathcal{AB}})$.

In this scenario, accuracy in preparation of the input states τ_s and ω_t as well as $\rho_{\mathcal{AB}}$ must be trusted. In Ref. [15], it is proved that no noise introduced in the local measurement operators can lower the bound $I(\rho_{\mathcal{AB}}) \geqslant 0$ for separable $\rho_{\mathcal{AB}}$, and hence, in this scheme, no separable state will ever be identified as an entangled one. In this sense the scheme of Ref. [15] is measurement-device independent. Thus, in the aforesaid MDIEW scheme, one *avoids* erroneous measurement settings for measuring the witness operator W by measuring just the maximally entangled state $|\Phi\rangle$. And even if this later measurement is erroneous, by the very construction of the MDIEW scheme of Branciard *et al.* [15], no separable state gets detected as entangled, although some entangled states will not get detected as entangled.

B. Detecting entanglement in an unknown two-qubit state

In this subsection, we briefly describe the universal entanglement witness scheme of Augusiak *et al.* [18] for witnessing entanglement in arbitrary two-qubit states.

In the case of witnessing entanglement in an unknown two-qubit state [18], instead of sharing a single copy of the state, the players need to share four identical copies of the state at a time. This is so because the signature of $\det(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}})$ (= product of eigenvalues of $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}} = \mathrm{Tr}[W\rho_{\mathcal{AB}}^{\otimes 4}] = \lambda_1\lambda_2\lambda_3\lambda_4$) completely determines whether the two-qubit state $\rho_{\mathcal{AB}}$ is entangled or separable. Here λ_i's are eigenvalues of $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$ and W is a fixed Hermitian operator acting on $\mathcal{H}_{\mathcal{A}}^{\otimes 4} \otimes \mathcal{H}_{\mathcal{B}}^{\otimes 4}$ (with $\dim\mathcal{H}_{\mathcal{A}} = \dim\mathcal{H}_{\mathcal{B}} = 2$). From the Newton-Girard formula [20], we have: $\lambda_1\lambda_2\lambda_3\lambda_4 =$

$$\frac{1}{24}\left(1 - 6\sum_{i=1}^{4}\lambda_i^4 + 8\sum_{i=1}^{4}\lambda_i^3 + 3\left(\sum_{i=1}^{4}\lambda_i^2\right)^2 - 6\sum_{i=1}^{4}\lambda_i^2\right).$$

To formulate this in terms of an operator, we first use the swap operator $V^{(k)}$, defined as

$$\begin{aligned} &V^{(k)}(|\varphi_1\rangle_{\mathcal{A}_1\mathcal{B}_1} \otimes |\varphi_2\rangle_{\mathcal{A}_2\mathcal{B}_2} \otimes \ldots . |\varphi_k\rangle_{\mathcal{A}_k\mathcal{B}_k}) \\ &\quad = |\varphi_k\rangle_{\mathcal{A}_1\mathcal{B}_1} \otimes |\varphi_1\rangle_{\mathcal{A}_2\mathcal{B}_2} \otimes \ldots . |\varphi_{(k-1)}\rangle_{\mathcal{A}_k\mathcal{B}_k}, \end{aligned} \tag{3}$$

and it has the property that $\mathrm{Tr}(V^{(k)}\rho^{\otimes k}) = \mathrm{Tr}(\rho^k)$ [18,21,22] for any Hermitian matrix ρ acting on $\mathcal{H}_{\mathcal{A}} \otimes \mathcal{H}_{\mathcal{B}}$. $V^{(k)}$ is not Hermitian except for $k = 2$. So, to make it an observable, in place of $V^{(k)}$, $\frac{1}{2}(V^{(k)} + V^{(k)\dagger})$ will be used for future analysis. $V^{(k)} : \mathcal{H}_{\mathcal{AB}}{}^{\otimes k} \to \mathcal{H}_{\mathcal{AB}}{}^{\otimes k}$ can be decomposed as a tensor product of two local operators $V^{(k)} = \tilde{V}^{(k)} \otimes \tilde{V}^{(k)}$ where $\tilde{V}^{(k)} : \mathcal{H}_{j_1} \otimes \mathcal{H}_{j_2} \otimes \ldots \otimes \mathcal{H}_{j_k} \to \mathcal{H}_{j_1} \otimes \mathcal{H}_{j_2} \otimes \ldots \otimes \mathcal{H}_{j_k}$ is given by

$$\begin{aligned} &\tilde{V}^{(k)}(|\varphi_1\rangle_{j_1} \otimes |\varphi_2\rangle_{j_2} \otimes \ldots\ldots \otimes |\varphi_k\rangle_{j_k}) \\ &\quad = |\varphi_k\rangle_{j_1} \otimes |\varphi_1\rangle_{j_2} \otimes \ldots\ldots \otimes |\varphi_{(k-1)}\rangle_{j_k}. \end{aligned} \tag{4}$$

Note here that $\mathcal{H}_{j_i} \equiv \mathcal{H}_j$ for all $i = 1,2,\ldots,k$ and $j = \mathcal{A},\mathcal{B}$. As the swap operator $V^{(k)}$ is a real matrix with respect to a fixed basis (for our case it is the computational basis), used for the whole analysis, we see that

$$\begin{aligned} &\mathrm{Tr}\left(\left(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}\right)^k\right) \\ &\quad = \sum_j (\lambda_j)^k = \mathrm{Tr}\left(V^{(k)}\left(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}\right)^{\otimes k}\right) \\ &\quad \text{is a real number.} \\ &\text{So, } \mathrm{Tr}\left(V^{(k)}\left(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}\right)^{\otimes k}\right) \\ &\quad = \mathrm{Tr}\left(V^{(k)\dagger}\left(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}\right)^{\otimes k}\right) \\ &\quad = \tfrac{1}{2}\mathrm{Tr}\left((V^{(k)} + V^{(k)\dagger})\left(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}\right)^{\otimes k}\right) \\ &\quad = \tfrac{1}{2}\mathrm{Tr}\left((V^{(k)} + V^{(k)\dagger})^{T_{\mathcal{B}}}\rho_{\mathcal{AB}}^{\otimes k}\right) \\ &\quad = \tfrac{1}{2}\mathrm{Tr}\left([\tilde{V}^{(k)} \otimes \tilde{V}^{(k)} + \tilde{V}^{(k)\dagger} \otimes \tilde{V}^{(k)\dagger}]^{T_{\mathcal{B}}}\rho_{\mathcal{AB}}^{\otimes k}\right) \\ &\quad = \tfrac{1}{2}\mathrm{Tr}\left([\tilde{V}^{(k)} \otimes \tilde{V}^{(k)T} + \tilde{V}^{(k)T} \otimes \tilde{V}^{(k)}]\rho_{\mathcal{AB}}^{\otimes k}\right), \end{aligned} \tag{5}$$

using the fact that $\tilde{V}^{(k)\dagger} = \tilde{V}^{(k)T}$, as $\tilde{V}^{(k)}$ is a real matrix with respect to the computational basis.

Then, the aforesaid Hermitian operator W, witnessing entanglement in an arbitrary two-qubit state, is given by

$$\begin{aligned} W^{\mathrm{univ}} = &\tfrac{1}{24}\mathbb{I}_{256\times 256} - \tfrac{1}{8}(\tilde{V}^{(4)} \otimes \tilde{V}^{(4)T} + \tilde{V}^{(4)T} \otimes \tilde{V}^{(4)}) \\ &+ \tfrac{1}{6}\mathbb{I}_{4\times 4} \otimes (\tilde{V}^{(3)} \otimes \tilde{V}^{(3)T} + \tilde{V}^{(3)T} \otimes \tilde{V}^{(3)}) \\ &+ \tfrac{1}{8}V^{(2)} \otimes V^{(2)} - \tfrac{1}{4}\mathbb{I}_{16\times 16} \otimes V^{(2)}, \end{aligned} \tag{6}$$

and our $I(\rho_{\mathcal{AB}})$ of Eq. (1) turns out to be proportional to $\mathrm{Tr}(W^{\mathrm{univ}}\rho_{\mathcal{AB}}^{\otimes 4}) = \det(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}})$ (see Sec. II for details).

The aforesaid operator W^{univ} doesn't depend on the two-qubit shared state, and hence, entanglement in an unknown two-qubit state $\rho_{\mathcal{AB}}$ can be detected by looking into the signature of $\mathrm{Tr}(W^{\mathrm{univ}}\rho_{\mathcal{AB}}^{\otimes 4})$. In this sense, it's a universal entanglement witness operator.

II. MDI IMPLEMENTATION OF TWO-QUBIT UNIVERSAL EW

Recent work by Bartkiewicz *et al.* in [23] demonstrated a physical implementation of the aforesaid universal entanglement witness operator (6), using two-photon polarized states. But that has not been done in a measurement-device-independent way. Authors of Refs. [24] and [25], address entanglement detection of *arbitrary* two-qubit states in the MDI way, but their approaches take care of error in Bell state measurement by optimizing the possible entanglement witness operators which can detect entanglement in the arbitrarily given state—by taking into account the erroneous measurement statistics themselves. The extra cost for this occurs due to measurements of one or both of the observables corresponding to the supplied states τ_s and ω_t in some known states of $\mathcal{A}$ or/and $\mathcal{B}$. In the following, although we are going to consider the partial Bell state measurements (BSM) $\{|\Phi^+\rangle\langle\Phi^+|, \mathbb{I} - |\Phi^+\rangle\langle\Phi^+|\}$ of both Alice and Bob to be perfect while witnessing entanglement in an arbitrary two-qubit state in an MDI way, one can, in principle, allow imperfection in BSM in our scheme and thereby calibrate (i.e., find out) exactly the corresponding noisy BSM using some known states (of Alice and Bob separately), and then

follow the same procedure as described below (see also Appendixes 2 and 3)—after (possibly) suitably modifying the supplied states τ_s and ω_t.

Our main result of this section can be stated as follows.

Theorem 1. Witnessing entanglement in an arbitrary two-qubit state, given four copies of the state at a time, can be realized in a measurement-device-independent way.

Proof. We consider the game described by Fig. 1 which starts with two inputs (one for Alice and one for Bob) and a single copy of a shared state $\rho_{\mathcal{AB}}$, while our universal measurement scheme for witnessing entanglement needs four identical copies of shared state $\rho_{\mathcal{AB}}$ at each run of the experiment, and the witness operator W^{univ} is a 256×256 matrix. Thus, the Hilbert space of the shared state is $[\mathbb{C}^2]^{\otimes 4} \otimes [\mathbb{C}^2]^{\otimes 4} \equiv \mathbb{C}^{16} \otimes \mathbb{C}^{16}$ instead of $\mathbb{C}^2 \otimes \mathbb{C}^2$. As a result of that, both τ_s and ω_t must be density matrices on $\mathbb{C}^{16}$.

We now take the witness operator W^{univ} of Eq. (6) in the form,

$$W^{\text{univ}} = \sum_{s,t} \beta_{st} \left(\tau_s^T \otimes \omega_t^T\right), \tag{7}$$

where the input states τ_s and ω_t are expandable in the appropriate Gell-Mann matrix basis as

$$\tau_s^T = \frac{\vec{\Lambda}.\text{Tr}\left(\tau_s^T \vec{\Lambda}\right)}{16} = \sum_i \Lambda_i p_i^{(s)},$$
$$\omega_t^T = \frac{\vec{\Lambda}.\text{Tr}\left(\omega_t^T \vec{\Lambda}\right)}{16} = \sum_j \Lambda_j q_j^{(t)}, \tag{8}$$

where $\vec{\Lambda}$ is the vector of all the 16×16 generalized Gell-Mann matrices Λ_i [26], the first component being the identity matrix. Also $p_i^{(s)}$ and $q_j^{(t)}$ are known real coefficients.

From the above relation (7) and using the actual form of the universal witness operator (6), the referee can calculate the quantities,

$$\text{Tr}(W^{\text{univ}}(\Lambda_i \otimes \Lambda_j)) = (16)^2 \sum_{s,t} \beta_{st} p_i^{(s)} q_j^{(t)}, \tag{9}$$

which will give rise to a set of $(256)^2$ numbers of linear equations for all i, j, from which the referee can calculate the coefficients β_{st} in Eq. (7). Also, instead of using a two-qubit Bell state projector $|\phi^+\rangle\langle\phi^+| = \frac{1}{2}\sum_{i,j=0}^{1} |ii\rangle\langle jj|$ or its local unitarily equivalent form as a measurement operator, each party should use a Bell state projector $|\Phi^+\rangle\langle\Phi^+| = \frac{1}{16}\sum_{i,j=0}^{15} |ii\rangle\langle jj|$ of two 16-dimensional systems as the measurement operator or its local unitarily equivalent form, for each party. Then the negativity of

$$\begin{aligned} I(\rho_{\mathcal{AB}}) &= \det\left(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}\right) \\ &= \text{Tr}[W^{\text{univ}}(\rho_{\mathcal{A}_1\mathcal{B}_1} \otimes \rho_{\mathcal{A}_2\mathcal{B}_2} \otimes \rho_{\mathcal{A}_3\mathcal{B}_3} \otimes \rho_{\mathcal{A}_4\mathcal{B}_4})] \\ &= \sum_{s,t} \beta_{st} \text{Tr}\Big[(|\Phi^+\rangle_{\mathcal{A}_0:\mathcal{A}_1\mathcal{A}_2\mathcal{A}_3\mathcal{A}_4}\langle\Phi^+| \otimes |\Phi^+\rangle_{\mathcal{B}_0:\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4}\langle\Phi^+|) \\ &\quad \times \left(\tau_s^{(\mathcal{A}_0)} \otimes \rho_{\mathcal{A}_1\mathcal{B}_1} \otimes \rho_{\mathcal{A}_2\mathcal{B}_2} \otimes \rho_{\mathcal{A}_3\mathcal{B}_3} \otimes \rho_{\mathcal{A}_4\mathcal{B}_4} \otimes \omega_t^{(\mathcal{B}_0)}\right)\Big] \end{aligned} \tag{10}$$

confirms the presence of entanglement of the shared state in an MDI way.

Now, in order to solve the set of $(256)^2$ linear equations given in (9), one needs to calculate the quantities $\text{Tr}[W^{\text{univ}}(\Lambda_i \otimes \Lambda_j)]$. By using the expression (6), this amounts to calculating the "local" quantities $\text{Tr}[\mathbb{I}_{16\times16}\Lambda_i]$, $\text{Tr}[\tilde{V}^{(4)}\Lambda_i]$, $\text{Tr}[\tilde{V}^{(4)T}\Lambda_i]$, $\text{Tr}[(\mathbb{I}_{2\times2} \otimes \tilde{V}^{(3)})\Lambda_i]$, $\text{Tr}[(\mathbb{I}_{2\times2} \otimes \tilde{V}^{(3)T})\Lambda_i]$, and the "global" quantity $\text{Tr}[V^{(2)}\Lambda_i]$, and thereby calculating the appropriate linear combination of their associated products—in respect to the right-hand-side expression of Eq. (6). For explicit expressions of the operators $\tilde{V}^{(4)}$, $\tilde{V}^{(3)}$, and $V^{(2)}$ in the computational basis, please see Appendix 1. ■

III. UNIVERSAL WITNESS FOR NPT-NESS OF TWO-QUDIT STATES IN MDI WAY

Any two-qudit density matrix $\rho_{\mathcal{AB}}$ whose partial transposition (denoted by $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$) has at least one negative eigenvalue, is called an NPT state. Any bipartite state having NPT is necessarily entangled [27]. Let us look at the characteristic equation for the matrix $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$:

$$\det\left(\rho_{\mathcal{AB}}^{T_{\mathcal{B}}} - \lambda \mathbb{I}_{d^2\times d^2}\right) = 0,$$
$$\text{which is of the form, } \sum_{i=0}^{d^2} (-1)^{d^2-i} a_{d^2-i} \lambda^i = 0, \tag{11}$$

where the coefficients $a_0, a_1, a_2, \ldots, a_{d^2}$ are given in terms of the eigenvalues $\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_{d^2}$ of $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$ as follows:

$$a_0 = 1, a_1 = \sum_{i=1}^{d^2} \lambda_i, a_2 = \sum_{i,j=1;i>j}^{d^2} \lambda_i \lambda_j,$$
$$a_3 = \sum_{i,j,k=1;i>j>k}^{d^2} \lambda_i \lambda_j \lambda_k, \ldots\ldots, a_{d^2} = \prod_{i=1}^{d^2} \lambda_i.$$

As $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$ is Hermitian, λ's are all real, and thereby a_i's are all real. If $a_i \geqslant 0$ for all i, we have $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}} \geqslant 0$. Otherwise, $\rho_{\mathcal{AB}}$ has NPT. Now, we determine whether the aforesaid characteristic equation has any negative root. We have written above each of the coefficients $a_0, a_1, a_2, \ldots, a_{d^2}$ as a polynomial in terms of the eigenvalues of $\rho_{\mathcal{AB}}^{T_{\mathcal{B}}}$ using the Newton-Girard formulas [20]. In fact, we have $a_1 = 1$ because partial transposition operation is trace preserving;

$$a_2 = \frac{1}{2}\left(1 - \sum_{i=1}^{d^2} \lambda_i^2\right) = \text{Tr}\left(W_2 \rho_{\mathcal{AB}}^{\otimes 2}\right), \quad \text{with}$$
$$W_2 = \frac{1}{2}[\mathbb{I}_{d^4\times d^4} - V^{(2)}]; \tag{12}$$
$$a_3 = \frac{1}{6}\left(1 - 3\sum_{i=1}^{d^2} \lambda_i^2 + 2\sum_{i=1}^{d^2} \lambda_i^3\right) = \text{Tr}\left(W_3 \rho_{\mathcal{AB}}^{\otimes 3}\right),$$
$$\text{with } W_3 = \frac{1}{6}[\mathbb{I}_{d^6\times d^6} - 3\mathbb{I}_{d^2\times d^2} \otimes V^{(2)} + \tilde{V}^{(3)} \otimes \tilde{V}^{(3)T} + \tilde{V}^{(3)T} \otimes \tilde{V}^{(3)}]; \tag{13}$$

$$a_4 = \frac{1}{24}\left(1 - 6\sum_{i=1}^{d^2}\lambda_i^2 + 3\left(\sum_{i=1}^{d^2}\lambda_i^2\right)^2 + 8\sum_{i=1}^{d^2}\lambda_i^3 - 6\sum_{i=1}^{d^2}\lambda_i^4\right) = \mathrm{Tr}\big(W_4\rho_{\mathcal{AB}}^{\otimes 4}\big), \tag{14}$$

where W_4 has a similar expression as that of W^{univ} in Eq. (6); so on and so forth.

We now argue about measurement-device-independent detection of NPT-ness of an unknown two-qudit state. Our argument starts from finding the signatures of the coefficients a_i for $i \geqslant 2$. In the most favorable case, a_2 may turn out to be negative and thereby $\rho_{\mathcal{AB}}$ has NPT. So, supply of two copies of the shared state $\rho_{\mathcal{AB}}$ at a time is enough to determine NPT-ness while both the inputs τ_s and ω_t are density matrices on the Hilbert space $(\mathbb{C}^d)^{\otimes 2}$. But, for the general case, the players have to share "i" number of copies of the state $\rho_{\mathcal{AB}}$ whenever the referee wants to know the sign of the coefficient a_i. Also, the dimension of the input states (τ_s and ω_t—to be supplied by the referee) should increase accordingly. In the worst case, we have to go up to the signature of the coefficient a_{d^2} for which we need d^2 copies of $\rho_{\mathcal{AB}}$, and τ_s and ω_t will be density matrices acting on the Hilbert space $(\mathbb{C}^d)^{\otimes d^2}$. As, for *any* PPT state $\rho_{\mathcal{AB}}$, all of $\lambda_1,\lambda_2,\lambda_3,\ldots,\lambda_{d^2}$ are non-negative, all the coefficients $a_2,a_3,\ldots,a_{d^2}$ are non-negative there. So, the operators, $W_2, W_3, \ldots, W_{d^2}$ indeed work as witnessing NPT-ness of the state $\rho_{\mathcal{AB}}$, and it gives rise to the following result.

Theorem 2. NPT-ness of an arbitrary two-qudit state can be witnessed by performing measurement on a finite number of copies of that state at a time in a measurement-device-independent way.

Proof. As none of the aforesaid witness operators $W_2, W_3, \ldots, W_{d^2}$ depend on the shared state $\rho_{\mathcal{AB}}$, we can use the scheme, similar to that described in Sec. II, to implement the measurement of these operators in a measurement-device-independent way. ■

A notable point is that, in the two-qubit case, under partial transposition, the shared density matrix can have only one negative eigenvalue and all other eigenvalues are positive definite, if the state is entangled [18]. Thus in the case of two qubits, the sign of the coefficient a_4 is enough to decide the NPT-ness, and thereby entanglement of the state—as done in Sec. II. We don't need to check the signs of the coefficients a_2,a_3. But for higher dimensions, that is not the case.

As discussed in the end of the first paragraph of Sec. II, Theorem 2 holds under the assumption that the BSM can be done perfectly. In case it is not possible, one can calibrate the noisy BSM by using it on some known states and thereby use this (calibrated) BSM—taking help of suitably chosen supplied states τ_s and ω_t.

A. Comparison between our MDI scheme and the conventional quantum state tomography

In recent works [28,29], it has been shown that, in the optimal scenario, the total number of different measurement settings required to check whether an arbitrary state of a given bipartite system is entangled or not matches with the total number of different measurement settings required for quantum state tomography—if the measurement settings are restricted to single usage of the state at a time. As, in our aforesaid discussion on universal witnessing in an MDI way, we have used measurements on multiple copies of the state, such a matching may not occur. In fact, in this section, we will argue that our method of universal MDI (i) entanglement witnessing scheme for two qubits, and (ii) NPT-ness witness scheme for two qudits are better—resource wise—compared to quantum state tomography (assuming that the BSM can be done perfectly).

In quantum state tomography, for a two-qudit system, we surely require $d^4 - 1$ number of different measurement settings, as the number of coefficients in any basis representation (like generalized Gell-Mann matrices Λ_n [30]) are $d^4 - 1$, in general:

$$\rho_{d^2\times d^2} = \frac{1}{d^2}\left[\mathbb{I}\otimes\mathbb{I} + \sum_{n=1}^{d^4-1} r_n\Lambda_n\right]. \tag{15}$$

The coefficients $r_n \in \mathbb{R}$, can be obtained from the expectation values of the observables $\Lambda_n : r_n = \mathrm{Tr}[\rho_{d^2\times d^2}\Lambda_n]$. Therefore, for each coefficient, a single copy of the state has to be used. In order to reconstruct the state, we need to know exact values of the coefficients; their signs only won't provide us sufficient information. The erroneous numerical values of these coefficients lead to an estimated state, generally different from $\rho_{d^2\times d^2}$. It may be noted here that it is possible to perform quantum state tomography of any two-qudit state $\rho_{\mathcal{AB}}$ in an MDI way by supplying one of a given set of (linearly independent) $d^4 - 1$ no. of two-qudit states $\sigma^{(1)}_{\mathcal{A}_1\mathcal{B}_1}, \sigma^{(2)}_{\mathcal{A}_1\mathcal{B}_1}, \ldots, \sigma^{(d^4-1)}_{\mathcal{A}_1\mathcal{B}_1}$, and thereby performing measurement of the projector $|\Phi^+\rangle_{\mathcal{AA}_1\mathcal{BB}_1}\langle\Phi^+|$ on one of the states $\sigma^{(1)}_{\mathcal{A}_1\mathcal{B}_1}\otimes\rho_{\mathcal{AB}}$, $\sigma^{(2)}_{\mathcal{A}_1\mathcal{B}_1}\otimes\rho_{\mathcal{AB}}$, ..., $\sigma^{(d^4-1)}_{\mathcal{A}_1\mathcal{B}_1}\otimes\rho_{\mathcal{AB}}$. Here $|\Phi^+\rangle_{\mathcal{AA}_1\mathcal{BB}_1} = \frac{1}{d}\sum_{i,j=1}^{d}|ij\rangle_{\mathcal{AA}_1}\otimes|ij\rangle_{\mathcal{BB}_1}$. In fact, it will also be possible to perform measurement in the maximally entangled states $|\Phi^+\rangle_{\mathcal{AA}_1}$ and $|\Phi^+\rangle_{\mathcal{BB}_1}$ separately. Once again, it is assumed here that measurement of $|\Phi^+\rangle$ can be done perfectly. In case that is not possible, one can calibrate the corresponding erroneous measurement by performing it on some known states, and thereby use the calibrated measurement for the MDI purpose—by suitably choosing the supplied states τ_s and ω_t. Even in this latter case, the required number of measurement settings is much less than the one required for the usual state tomography (see Appendix 4). ■

In case of tomography of two-qubit states we require measuring 15 parameters, so we need at least 15 measurement settings globally. But in our case (of witnessing entanglement universally), without going into any MDI scheme, to measure a_2 in Eq. (12), we have to measure the expectation value of a single observable $V^{(2)}$ only on two copies of $\rho_{\mathcal{AB}}$. For a_3 in Eq. (13), we need to measure expectation values of two observables $\mathbb{I}_{d^2\times d^2}\otimes V^{(2)}, \tilde{V}^{(3)}\otimes\tilde{V}^{(3)T} + \tilde{V}^{(3)T}\otimes\tilde{V}^{(3)}$ on three copies of $\rho_{\mathcal{AB}}$. Similarly for a_4, we have four observables to measure. But as for the two-qubit case the sign of a_4 is the deciding factor for entanglement, we need four measurement settings. So, we need here fewer numbers of measurement settings compared to the case of state tomography, at the cost

of using n copies of the state to determine the coefficient a_n (for $n = 2,3,4,\ldots$).

In the case of a two-qudit state tomography, we require at least $d^4 - 1$ measurement settings. But for our NPT-ness witness scheme in an MDI way, the required number of measurement settings is much less than that.

IV. WITNESSING ENTANGLEMENT IN AN ARBITRARY PPT STATE OF A GIVEN BIPARTITE SYSTEM

Existence of PPT entangled states $\rho_{\mathcal{AB}}$ (so-called PPT bound entangled states) is well known whenever $\dim(\mathcal{H}_\mathcal{A}) \times \dim(\mathcal{H}_\mathcal{B}) > 6$. Evidently our scheme of universal NPT-ness witness, as described in Sec. III, does not work here to detect entanglement of any such state. Below we try to argue that a universal entanglement witness operator cannot exist to single out entanglement in any PPT state of a given bipartite system, through some conjectures.

Conjecture I. If $\dim(\mathcal{H}_\mathcal{A}) \times \dim(\mathcal{H}_\mathcal{B}) > 6$, there cannot exist one (or a finitely many) universal entanglement witness operator(s) detecting entanglement in an arbitrary PPT state $\rho_{\mathcal{AB}}$, and which can be realized in an MDI way.

The reason behind this conjecture is another conjecture (following).

Conjecture II. There cannot exist a universal EW (or, a finitely many EW operators) for all PPT entangled states of any given bipartite system.

Let us try to provide some geometrical argument which potentially may give rise to Conjecture II.

Let $\mathcal{D}_{\mathcal{AB}}, \mathcal{S}_{\mathcal{AB}}, \mathcal{P}_{\mathcal{AB}}$, respectively, be the set of all density matrices, separable density matrices, and density matrices which are positive semidefinite under partial transposition (PPT) on $\mathcal{H}_{\mathcal{AB}}$; $\tilde{\mathcal{P}}_{\mathcal{AB}}$ be the set of all entangled density matrices (PPTE) in $\mathcal{P}_{\mathcal{AB}}$. $\mathcal{S}_{\mathcal{AB}}$ and $\mathcal{P}_{\mathcal{AB}}$ are both convex sets. It is obvious that, $\mathcal{S}_{\mathcal{AB}} \subset \mathcal{P}_{\mathcal{AB}} \subset \mathcal{D}_{\mathcal{AB}}$ and $\mathcal{P}_{\mathcal{AB}} - \mathcal{S}_{\mathcal{AB}} = \tilde{\mathcal{P}}_{\mathcal{AB}}$. Note that $\tilde{\mathcal{P}}_{\mathcal{AB}}$ is not convex. For $\max\{\dim(\mathcal{H}_\mathcal{A}),\dim(\mathcal{H}_\mathcal{B})\} = 3$ together with $\min\{\dim(\mathcal{H}_\mathcal{A}),\dim(\mathcal{H}_\mathcal{B})\} = 2$, $\mathcal{P}_{\mathcal{AB}} = \mathcal{S}_{\mathcal{AB}}$. Let $\tilde{\mathcal{P}}'_{\mathcal{AB}}$ be the set of all the states formed by the convex combination of states in $\tilde{\mathcal{P}}_{\mathcal{AB}}$.

Edge state. $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$ is an edge state iff the state $(\rho_{\mathcal{AB}} + p\sigma_{\mathcal{AB}})/(1+p) \in \mathcal{S}_{\mathcal{AB}}$ for all $p \in (0,1]$ and for all $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$. Edge states lie near the boundary of $\mathcal{S}_{\mathcal{AB}}$ and exist for $\dim(\mathcal{H}_\mathcal{A}),\dim(\mathcal{H}_\mathcal{B}) \geqslant 3$.

It is well known that [31,32] there always exist at least two edge states $\rho^{(\alpha)}_{\mathcal{AB}}, \rho^{(\beta)}_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$ such that their convex combination, $p\rho^{(\alpha)}_{\mathcal{AB}} + (1-p)\rho^{(\beta)}_{\mathcal{AB}} = \sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$ for $0 < p < 1$. Hence for, $\dim(\mathcal{H}_\mathcal{A}),\dim(\mathcal{H}_\mathcal{B}) \geqslant 3$, $\tilde{\mathcal{P}}'_{\mathcal{AB}} \cap \mathcal{S}_{\mathcal{AB}} \neq \phi$ (null set). This is the case when we consider only a single copy of the state. Figure 2 depicts existence of these edge states in region (II) near the common boundary of (II) and (III).

From Fig. 2 it is clear (at least pictorially) that there cannot exist a Hermitian operator $W : \mathbb{C}^d \otimes \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d$ such that $\mathrm{Tr}[W\rho_{\mathcal{AB}}] < 0$ for *all* $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$ while $\mathrm{Tr}[W\sigma_{\mathcal{AB}}] \geqslant 0$ for all $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$. So, in the single copy case, no such universal witness operator W exists to witness entanglement in all $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$.

Now, the question is—as in the case of qubits—is it possible to have a (or a finite number of) universal witness operator(s) W^{univ} which can detect entanglement in any PPT state $\rho_{\mathcal{AB}}$ of two qudits in case n copies of the state are supplied with $n \geqslant 2$?

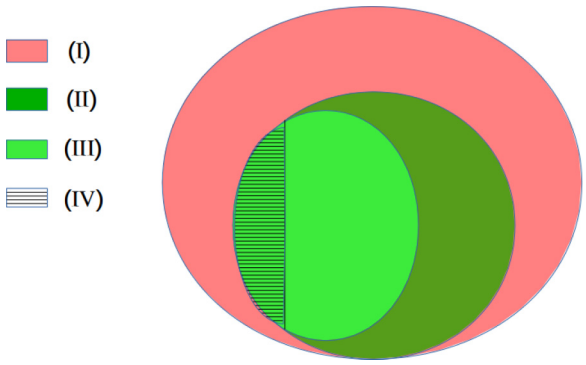

FIG. 2. Distribution of density matrix spaces acting on the Hilbert space $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$. [(I) + (II) + (III) + (IV)] $\equiv \mathcal{D}_{\mathcal{AB}}$, the set of all density matrices. (I) $\equiv \mathcal{D}_{\mathcal{AB}} - \mathcal{P}_{\mathcal{AB}}$ is the set of all NPT states, $\mathcal{P}_{\mathcal{AB}}$ is the set of all states having PPT. (II) $\equiv \tilde{\mathcal{P}}_{\mathcal{AB}}$, the set of all PPT entangled states, [(III) + (IV)] $\equiv \mathcal{S}_{\mathcal{AB}}$, is the set of all separable states, [(II) + (III)] $\equiv \tilde{\mathcal{P}}'_{\mathcal{AB}}$ is the set of a convex combination of PPT entangled states. Region (III) clearly depicts the non-empty-ness of $(\tilde{\mathcal{P}}'_{\mathcal{AB}} \bigcap \mathcal{S}_{\mathcal{AB}})$. This holds due to the fact that $\tilde{\mathcal{P}}_{\mathcal{AB}}$ is a nonconvex subset of the convex set $\mathcal{P}_{\mathcal{AB}}$.

We conjecture below that such a W^{univ} does not exist.

In this direction let's consider $\mathcal{D}_{\mathcal{A}_n\mathcal{B}_n}$ to be the set of all density matrices on ${\mathcal{H}_\mathcal{A}}^{\otimes n} \otimes {\mathcal{H}_\mathcal{B}}^{\otimes n}$. ${\mathcal{S}'_{\mathcal{AB}}}^{(n)}$ be the set formed by the convex combinations of the states $\sigma^{\otimes n}_{\mathcal{AB}}$, where $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$, and let ${\tilde{\mathcal{P}}'}^{(n)}_{\mathcal{AB}}$ be the set formed by the convex combinations of the states $\rho^{\otimes n}_{\mathcal{AB}}$, where $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$. If $\mathcal{S}_{\mathcal{A}_n\mathcal{B}_n}$ be the set of all separable states on ${\mathcal{H}_\mathcal{A}}^{\otimes n} \otimes {\mathcal{H}_\mathcal{B}}^{\otimes n}$, it is evident that ${\mathcal{S}'_{\mathcal{AB}}}^{(n)} \subseteq \mathcal{S}_{\mathcal{A}_n\mathcal{B}_n}$ and it is most likely that $\mathcal{S}_{\mathcal{A}_n\mathcal{B}_n} \cap {\tilde{\mathcal{P}}'}^{(n)}_{\mathcal{AB}} \neq \phi$ (null set) for all n with $\dim(\mathcal{H}_\mathcal{A}),\dim(\mathcal{H}_\mathcal{B}) \geqslant 3$, because of the existence of edge states on ${\mathcal{H}_\mathcal{A}}^{\otimes n} \otimes {\mathcal{H}_\mathcal{B}}^{\otimes n}$.

Conjecture III. ${\mathcal{S}'_{\mathcal{AB}}}^{(n)} \cap {\tilde{\mathcal{P}}'}^{(n)}_{\mathcal{AB}} \neq \phi$ for all n with $\dim(\mathcal{H}_\mathcal{A}),\dim(\mathcal{H}_\mathcal{B}) \geqslant 3$.

Figure 2 depicts Conjecture III to be true with $n = 1$.

Conjecture III implies that there always exist at least two states $\rho^{(\alpha)}_{\mathcal{AB}}, \rho^{(\beta)}_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$ such that a convex combination of their n number of copies belongs to ${\mathcal{S}'_{\mathcal{AB}}}^{(n)}$ for all $n \geqslant 1$ (see Fig. 3):

$$p\left(\rho^{(\alpha)}_{\mathcal{AB}}\right)^{\otimes n} + (1-p)\left(\rho^{(\beta)}_{\mathcal{AB}}\right)^{\otimes n} = \sum_r p_r \left(\sigma^{(r)}_{\mathcal{AB}}\right)^{\otimes n}. \tag{16}$$

Validity of Conjecture III implies nonexistence of any Hermitian operator,

$$W_{\mathcal{A}_n\mathcal{B}_n} : {\mathcal{H}_\mathcal{A}}^{\otimes n} \otimes {\mathcal{H}_\mathcal{B}}^{\otimes n} \to {\mathcal{H}_\mathcal{A}}^{\otimes n} \otimes {\mathcal{H}_\mathcal{B}}^{\otimes n},$$

for which $\mathrm{Tr}[W_{\mathcal{A}_n\mathcal{B}_n}(\rho_{\mathcal{AB}})^{\otimes n}] < 0$ for *some* $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$ together with $\mathrm{Tr}[W_{\mathcal{A}_n\mathcal{B}_n}(\sigma_{\mathcal{AB}})^{\otimes n}] \geqslant 0$ for *all* $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$—irrespective of the choice of n.

Thus, validity of Conjecture III implies that there cannot exist a universal EW (or finitely many EWs) which can detect entanglement in all the PPT entangled states of the bipartite system $\mathcal{A} + \mathcal{B}$ whenever $d \geqslant 3$.

This automatically implies the validity of Conjecture II. It appears to be quite difficult to verify Conjecture III directly. One may try to verify whether for some given states

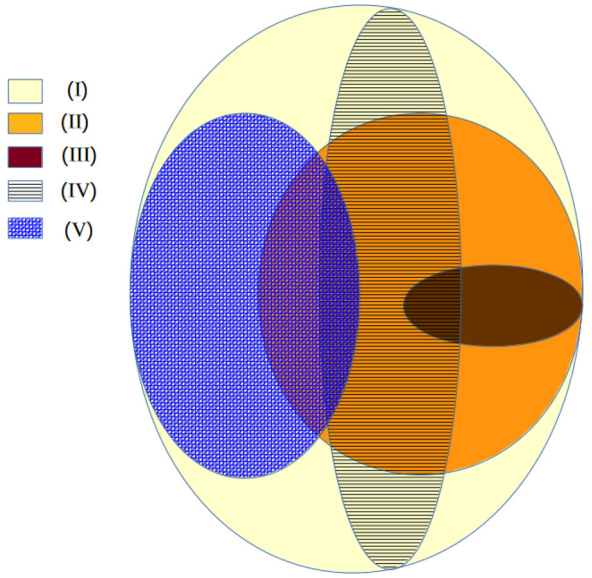

FIG. 3. Distribution of density matrix spaces acting on the Hilbert space $\mathcal{H}_{\mathcal{A}}{}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}{}^{\otimes n}$. [(I) $\bigcup$ (II) $\bigcup$ (III) $\bigcup$ (IV) $\bigcup$ (V)] $\equiv \mathcal{D}_{\mathcal{A}_n\mathcal{B}_n}$, the set of all density matrices. (II)$\equiv \mathcal{S}_{\mathcal{A}_n\mathcal{B}_n}$ be the set of all separable states, (III) $\equiv \mathcal{S}'_{\mathcal{AB}}{}^{(n)}$ is the set of convex combinations of all states like $\sigma_{\mathcal{AB}}^{\otimes n}$, where $\sigma_{\mathcal{AB}} \in \mathcal{S}_{\mathcal{AB}}$. (IV) $\equiv \tilde{\mathcal{P}}'_{\mathcal{AB}}{}^{(n)}$ be the convex combination of all the states like $\rho_{\mathcal{AB}}^{\otimes n}$, where $\rho_{\mathcal{AB}} \in \tilde{\mathcal{P}}_{\mathcal{AB}}$. (V) contains convex combination of all the states like $\rho_{\mathcal{AB}}^{\otimes n}$, where $\rho_{\mathcal{AB}} \in \mathcal{D}_{\mathcal{AB}} - \tilde{\mathcal{P}}_{\mathcal{AB}}$, the set of all NPT states at the single copy level. We conjecture about the non-empty-ness of the intersection (III) $\bigcap$ (IV), and the empty-ness of (III) $\bigcap$ (V).

$\rho_{\mathcal{AB}}^{\alpha} \in \tilde{P}_{\mathcal{AB}}$, there exists a separable state $\sigma_{\mathcal{AB}} \in \mathcal{H}_{\mathcal{A}}{}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}{}^{\otimes n}$ such that

$$\mathrm{Tr}\left[\mathcal{O}\sum_{\alpha} p_{\alpha}\left(\rho_{\mathcal{AB}}^{(\alpha)}\right)^{\otimes n}\right] = \mathrm{Tr}[\mathcal{O}\sigma_{\mathcal{AB}}],$$

for a complete set of linearly independent observables $\mathcal{O}$: $\mathcal{H}_{\mathcal{A}}{}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}{}^{\otimes n} \to \mathcal{H}_{\mathcal{A}}{}^{\otimes n} \otimes \mathcal{H}_{\mathcal{B}}{}^{\otimes n}$. Even verification of this one may turn out to be difficult.

This difficulty seems to arise from the well-known fact that the separability problem (that is, to find out whether an *arbitrary* state of a given bipartite quantum system is entangled or separable) is NP-hard [33,34]. See also [35].

V. NOISE ANALYSIS FOR REAL EXPERIMENTS

Recently, a few experimental works [13,36] have been done to implement the aforesaid MDI protocol to witness the entanglement in two particular classes of two-qubit states.

We now analyze the effect of possible noises in the Bell-state-measurement (BSM) part of both the aforesaid experimental setups. Here we introduce three kinds of possible noise (see Fig. 4).

(1) Photon loss in polarizing beam splitter (PBS). We model here the photon loss in a PBS through the action of a white noise—as described below.

(2) Error in the angle of rotation in half wave plate (HWP). HWP rotates the polarization axis of the light vector (which carries the information about the projected state by the measurement operator) with respect to its direction of the propagation of light ray by the angle equals two times of the angle (θ) between the fast axis of HWP and the polarization axis. So, if the angle of rotation is improper, we can take it as $2\theta + \eta$, where η is the error in BSM.

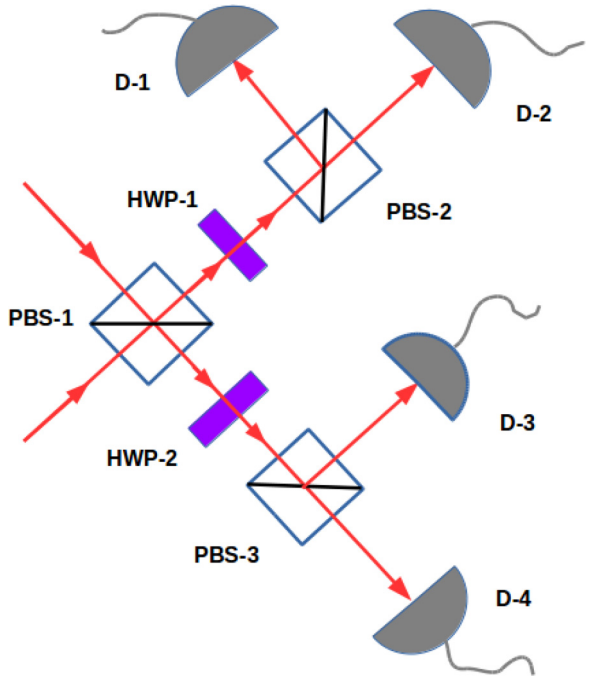

FIG. 4. Bell-state projection $\frac{1}{2}(|HH\rangle + VV)(\langle HH| + \langle VV|)$ measurement via coincidence counts. Photon propagations are denoted by red arrows. PBS, polarizing beam splitter; HWP, half wave plate; D, single-photon detector.

(3) Detection inefficiencies in diode photon-detector parts. For detection inefficiency, the probability of detection gets reduced by a factor $\xi_{\mathcal{A}}$ in Alice's side and a factor $\xi_{\mathcal{B}}$ in Bob's side such that $0 \leqslant \xi_{\mathcal{A}}, \xi_{\mathcal{B}} \leqslant 1$ and the probability of detection in BSM becomes $\xi P(1,1|\tau_s,\omega_t)$, where $\xi = \xi_{\mathcal{A}}\xi_{\mathcal{B}}$.

For our discussion, we choose the Bell state projector $|\Phi^+\rangle\langle\Phi^+|$ as the measurement operator (in BSM), where $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$ with the consideration that the horizontally polarized state is $|H\rangle = (1\ 0)^T \equiv |0\rangle$ and vertically polarized state is $|V\rangle = (0\ 1)^T \equiv |1\rangle$.

Under additive white noise (a special case), our actual measurement operator will be $\mu\,|\Phi^+\rangle\langle\Phi^+| + \frac{1-\mu}{4}\mathbb{I}$, where μ is the corresponding visibility.

We assume the direction of propagation of photon to be along the y axis (denoted by red rays in Figs. 4 and 5), where the reference coordinate frames are fixed at every HWP. Thus, if the angle of rotation for the polarization axis (shown in Fig. 5) of one player and that coming from the referee are, respectively, $2g_1$ and $2g_2$ then, the *rotated* Bell state is given by

$$e^{-ig_1\sigma_y} \otimes e^{-ig_2\sigma_y}\,|\Phi^+\rangle = \cos(g_2 - g_1)\,|\Phi^+\rangle + \sin(g_2 - g_1)\,|\Psi^-\rangle\,, \qquad (17)$$

where $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$. So, if $g_2 - g_1 \in \{0, \pm\pi, \pm 2\pi, \pm 3\pi, \pm 4\pi\}$ then $|\Phi^+\rangle\langle\Phi^+|$ will remain the same

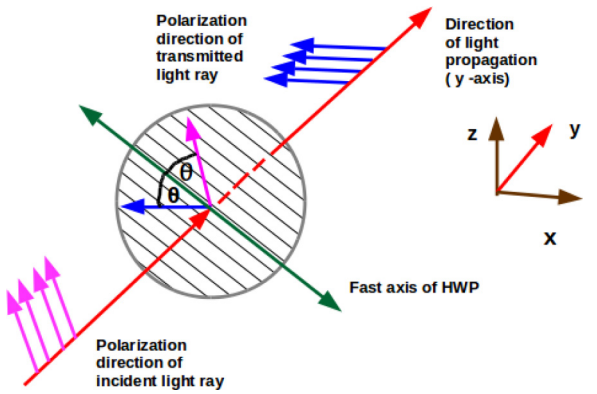

FIG. 5. Light ray passing through the half wave plate. The polarization axis, rotates by angle 2θ with respect to the direction of propagation. θ is the angle between the polarization axis of the incident ray and the fast axis of the HWP. The fast axis of the HWP lies in the xz plane.

and there is no error in the HWP. Therefore, after passing through the noisy PBS and HWP, our noisy Bell state projector $|\Phi^+\rangle\langle\Phi^+|$ will become the following noisy one:

$$\begin{aligned} P &= \mu\cos^2(g_2-g_1)\,|\Phi^+\rangle\langle\Phi^+| \\ &\quad + \mu\cos(g_2-g_1)\sin(g_2-g_1)(|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \\ &\quad + \mu\sin^2(g_2-g_1)\,|\Psi^-\rangle\langle\Psi^-| + \frac{1-\mu}{4}\mathbb{I}. \end{aligned} \tag{18}$$

Let's take $g_2 - g_1 = \Delta$. Then the noisy projection operator shared between $\mathcal{A}$ and a part coming from the referee $\mathcal{A}_0$ is given by

$$\begin{aligned} P_{\mathcal{A}_0\mathcal{A}} &= \mu_1\cos^2(\Delta_1)\,|\Phi^+\rangle\langle\Phi^+| \\ &\quad + \mu_1\cos(\Delta_1)\sin(\Delta_1)(|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \\ &\quad + \mu_1\sin^2(\Delta_1)\,|\Psi^-\rangle\langle\Psi^-| + \frac{1-\mu_1}{4}\mathbb{I}. \end{aligned} \tag{19}$$

Similarly for $\mathcal{B}$ and $\mathcal{B}_0$ we have

$$\begin{aligned} P_{\mathcal{B}\mathcal{B}_0} &= \mu_2\cos^2(\Delta_2)\,|\Phi^+\rangle\langle\Phi^+| \\ &\quad + \mu_2\cos(\Delta_2)\sin(\Delta_2)(|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \\ &\quad + \mu_2\sin^2(\Delta_2)\,|\Psi^-\rangle\langle\Psi^-| + \frac{1-\mu_2}{4}\mathbb{I}. \end{aligned} \tag{20}$$

Here, μ_1 and μ_2 are the visibilities of the PBS's of the $\mathcal{A}$ side and $\mathcal{B}$ side, respectively, in the noisy measurement of $|\Phi^+\rangle$, Δ_1, and Δ_2 are the corresponding errors in the rotational angle in HWP in the $\mathcal{A}$ side and $\mathcal{B}$ side, respectively.

So, our desired (modified) quantity will be

$$\begin{aligned} &I_{\text{mod}}(\rho_{\mathcal{A}\mathcal{B}}) \\ &= \sum_{s,t}\beta_{st}\xi\,\text{Tr}\big[\big(P_{\mathcal{A}_0\mathcal{A}}\otimes P_{\mathcal{B}\mathcal{B}_0}\big)(\tau_s\otimes\rho_{\mathcal{A}\mathcal{B}}\otimes\omega_t)\big] \\ &= \xi\Bigg[\mu_1\mu_2\cos^2(\Delta_1)\cos^2(\Delta_2) + \frac{\mu_1(1-\mu_2)}{4}\cos^2(\Delta_1) \\ &\quad + \frac{\mu_2(1-\mu_1)}{4}\cos^2(\Delta_2) + \frac{(1-\mu_1)(1-\mu_2)}{16}\Bigg] \\ &\quad \times I(\rho_{\mathcal{A}\mathcal{B}}) + \text{additional term}. \end{aligned} \tag{21}$$

TABLE I. Input states used in Ref. [36] for Alice's and Bob's sides and their corresponding Bloch vectors.

Input states τ_s,ω_t	Bloch vectors $\vec{r}_s,\vec{R}_t$
$\tau_1=\omega_1=\lvert H\rangle\langle H\rvert$	$\vec{r}_1=\vec{R}_1=(0,0,1)$
$\tau_2=\omega_2=\lvert V\rangle\langle V\rvert$	$\vec{r}_2=\vec{R}_2=(0,0,-1)$
$\tau_3=\omega_3=\lvert D\rangle\langle D\rvert$	$\vec{r}_3=\vec{R}_3=(1,0,0)$
$\tau_4=\omega_4=\lvert \bar{D}\rangle\langle \bar{D}\rvert$	$\vec{r}_4=\vec{R}_4=(-1,0,0)$
$\tau_5=\omega_5=\lvert L\rangle\langle L\rvert$	$\vec{r}_5=\vec{R}_5=(0,1,0)$
$\tau_6=\omega_6=\lvert R\rangle\langle R\rvert$	$\vec{r}_6=\vec{R}_6=(0,-1,0)$

The additional term is given in Eqs. (A13) and (A15) of Appendix 3.

Now, for simplicity, let us assume that $\mu_1=\mu_2=\mu$ and $\Delta_1=\Delta_2=\Delta$.

In the case of a two-qubit shared state $\rho_{\mathcal{A}\mathcal{B}}$, the input states τ_s and ω_t take the forms,

$$\begin{aligned} \tau_s &= \frac{\mathbb{I}+\vec{r}_s.\vec{\sigma}}{2}, \quad \omega_t = \frac{\mathbb{I}+\vec{R}_t.\vec{\sigma}}{2}, \\ \rho_{\mathcal{A}\mathcal{B}} &= \frac{1}{4}\Bigg(\mathbb{I}\otimes\mathbb{I} + \sum_{i=1}^{3}a_i\,\mathbb{I}\otimes\sigma_i \\ &\quad + \sum_{i=1}^{3}b_i\,\sigma_i\otimes\mathbb{I} + \sum_{i,j=1}^{3}c_{ij}\,\sigma_i\otimes\sigma_j\Bigg), \\ &\text{with } \vec{r}_s=(x_s,y_s,z_s) \text{ and } \vec{R}_t=(x_t,y_t,z_t)\in\mathbb{R}^3, |\vec{r}_s|,|\vec{R}_t| \\ &\leqslant 1, (a_1,a_2,a_3)\in\mathbb{R}^3, (b_1,b_2,b_3)\in\mathbb{R}^3; \\ &\quad (c_{ij})_{i,j=1}^3 \text{is a real } 3\times 3 \text{ matrix}. \end{aligned} \tag{22}$$

The corresponding form of $I_{\text{mod}}(\rho_{\mathcal{A}\mathcal{B}})$ is given in Eq. (A16) of Appendix 3.

According to Ref. [36], the input states (τ_s's and ω_t's) are given in Table I.

The corresponding payoffs (associated to Table I) are:

$$\begin{aligned} &\beta_{11}=\beta_{22}=\beta_{33}=\beta_{44}=\beta_{55}=\beta_{66}=\tfrac{1}{3}, \\ &\beta_{12}=\beta_{21}=\beta_{34}=\beta_{43}=\beta_{56}=\beta_{65}=-\tfrac{1}{6}. \end{aligned} \tag{23}$$

Other β_{st} are equal to zero.

The shared state is here $\rho_{\mathcal{A}\mathcal{B}} = p\,|\Psi^-\rangle\langle\Psi^-| + \frac{1-p}{4}\mathbb{I}$ which is separable iff $0\leqslant p\leqslant\frac{1}{3}$. Thus, in Eq. (22), $c_{11}=c_{22}=c_{33}=-p$, and $c_{kl}=0$ when $k\neq l$; $a_k=b_k=0\,\forall k,l\in\{1,2,3\}$.

Using Eq. (23) and Table I we have

$$\begin{aligned} &\sum_{s,t}\beta_{st}=1, \\ &\sum_{s,t}\beta_{st}x_sx_t=\sum_{s,t}\beta_{st}y_sy_t=\sum_{s,t}\beta_{st}z_sz_t=1, \\ &\sum_{s,t}\beta_{st}x_sy_t=\sum_{s,t}\beta_{st}x_sz_t=\sum_{s,t}\beta_{st}y_sx_t \\ &\qquad =\sum_{s,t}\beta_{st}y_sz_t=\sum_{s,t}\beta_{st}z_sx_t=\sum_{s,t}\beta_{st}z_sy_t=0. \end{aligned} \tag{24}$$

Therefore, according to Eq. (21) [see Eq. (A16) in Appendix 3 for details], we have

$$I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) = \frac{\xi}{4}[1 - p\mu^2 - 2p\mu^2\cos(4\Delta)]. \quad (25)$$

For the allowed values of the noise parameters ξ,μ,Δ, we have $0 \leqslant I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) \leqslant \frac{1}{3}$. Hence, for these kinds of errors, no separable state will ever be detected as an entangled one.

Reference [13] deals with the entangled state $\rho = (1-r)\,|\Psi^-\rangle\langle\Psi^-| + \frac{r}{2}(|HH\rangle\langle HH| + |VV\rangle\langle VV|)$ with $0 \leqslant r \leqslant 1$. $\rho_{\mathcal{AB}}$ is separable iff $\frac{1}{2} \leqslant r \leqslant 1$. Here, for this case, $c_{11} = c_{22} = (r-1)$ and $c_{33} = 2r-1$. $c_{kl} = 0$ when $k \neq l$; $a_k = b_k = 0, \forall k,l \in \{1,2,3\}$.

Here we are going to use the data of Table II in the Supplemental Material of Ref. [13]. In this case,

$$\begin{aligned}
&\sum_{s,t}\beta_{st} = 1,\\
&\sum_{s,t}\beta_{st}x_s x_t = \sum_{s,t}\beta_{st}y_s y_t = 1, \sum_{s,t}\beta_{st}z_s z_t = 1,\\
&\sum_{s,t}\beta_{st}z_s x_t = \sum_{s,t}\beta_{st}z_s y_t = \sum_{s,t}\beta_{st}x_s y_t\\
&\qquad = \sum_{s,t}\beta_{st}x_s z_t = \sum_{s,t}\beta_{st}y_s x_t = \sum_{s,t}\beta_{st}y_s z_t = 0.
\end{aligned} \quad (26)$$

Therefore, according to Eq. (21) [see Eq. (A16) in Appendix 3 for the details],

$$I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) = \frac{\xi}{4}[(3r-2)\mu^2\cos(4\Delta) + \mu^2(r-1) + 1]. \quad (27)$$

For $\frac{1}{2} \leqslant r \leqslant 1$ and for allowed values of noise parameters ξ,μ,Δ, we have $0 \leqslant I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) \leqslant \frac{1}{2}$. So, as in the case of Ref. [36], separable states will never get detected as entangled. Thus we see the Bell state measurement in both the experiments, reported in Refs. [13] and [36], does give rise to MDIEW for the respective classes of states even if we consider some *specific* form of noise in the measurement setups—as should be the case for any MDIEW scheme.

VI. CONCLUSION

Using the prescription of Auguisiak *et al.* [18] for witnessing entanglement in an unknown state of two qubits, we have extended here the measurement-device-independent entanglement witness scheme of Branciard *et al.* [15] to a universal measurement-device-independent entanglement witness scheme for two-qubit states, the caveat being that we need four copies of the state at a time and the referee should supply the input states from 16-dimensional Hilbert spaces of Alice and Bob separately. In an aim to extend this result to higher dimension, we provided here a measurement-device-independent scheme for universally witnessing NPT-ness of an unknown state of any given bipartite system—provided many copies of the state are being supplied at a time. Of course, this number of copies (as well as the number of different measurement settings required) is much less than what is required for state tomography. We conjectured that, there doesn't exist a single or a finitely many universal witness operators for witnessing entanglement in an arbitrary PPT state of a given bipartite system, a support for which comes from the well-known result that the separability problem is NP-hard [33,34]. Our noise analysis of the Bell state measurement scenario in both the experimental demonstrations of MDIEW [13,36] are in conformity with the MDI of EW of Branciard *et al.* [15].

ACKNOWLEDGMENT

The authors would like to thank Sandeep K. Goyal and Manik Banik for useful discussion on the present work.

APPENDIX

1. The explicit form of the operators appeared in Eq. (6)

By looking at the action of $\tilde{V}^{(4)}$ on an arbitrary state $|\psi_{\mathcal{A}}\rangle = (\alpha\,|0\rangle_1 + \beta_1\,|1\rangle)_{\mathcal{A}_1} \otimes (\alpha_2\,|0\rangle + \beta_2\,|1\rangle)_{\mathcal{A}_2}$
$\otimes(\alpha_3\,|0\rangle + \beta_3\,|1\rangle)_{\mathcal{A}_3} \otimes (\alpha_4\,|0\rangle + \beta_4\,|1\rangle)_{\mathcal{A}_4}$, one can figure out that $\tilde{V}^{(4)}$ acts on $\mathcal{H}_{\mathcal{A}_1} \otimes \mathcal{H}_{\mathcal{A}_2} \otimes \mathcal{H}_{\mathcal{A}_3} \otimes \mathcal{H}_{\mathcal{A}_4}$ as

$$\tilde{V}^{(4)} = \sum_{i,j,k,l=0}^{1} |l,i,j,k\rangle\langle i,j,k,l|\,. \quad (A1)$$

On the other hand, by taking action of $\tilde{V}^{(3)}$ on $|\psi_{\mathcal{A}}\rangle$, we get

$$\tilde{V}^{(3)} = \sum_{i,j,k=0}^{1} |k,i,j\rangle\langle i,j,k|\,, \quad (A2)$$

which acts on $\mathcal{H}_{\mathcal{A}_{i_1}} \otimes \mathcal{H}_{\mathcal{A}_{i_2}} \otimes \mathcal{H}_{\mathcal{A}_{i_3}}$ with i_1,i_2,i_3 being three distinct elements of $\{1,2,3,4\}$.

Similar expressions are valid for the corresponding operators acting on $\mathcal{H}_{\mathcal{B}}{}^{\otimes n}$where, $n = 3,4$.

Taking the action of $V^{(2)} \otimes V^{(2)}$ on a general state,

$$\begin{aligned}
|\psi_{\mathcal{AB}}\rangle = &(\alpha_1\,|0\rangle + \beta_1\,|1\rangle)_{\mathcal{A}_1} \otimes (\alpha_1'\,|0\rangle + \beta_1'\,|1\rangle)_{\mathcal{B}_1}\\
&\otimes(\alpha_2\,|0\rangle + \beta_2\,|1\rangle)_{\mathcal{A}_2} \otimes (\alpha_2'\,|0\rangle + \beta_2'\,|1\rangle)_{\mathcal{B}_2}\\
&\otimes(\alpha_3\,|0\rangle + \beta_3\,|1\rangle)_{\mathcal{A}_3} \otimes (\alpha_3'\,|0\rangle + \beta_3'\,|1\rangle)_{\mathcal{B}_3}\\
&\otimes(\alpha_4\,|0\rangle + \beta_4\,|1\rangle)_{\mathcal{A}_4} \otimes (\alpha_4'\,|0\rangle + \beta_4'\,|1\rangle)_{\mathcal{B}_4},
\end{aligned}$$

we get

$$V^{(2)} = \sum_{i,j,k,l=0}^{1} |kl,ij\rangle\langle ij,kl|\,, \quad (A3)$$

which acts on $\mathcal{H}_{\mathcal{A}_i\mathcal{B}_i} \otimes \mathcal{H}_{\mathcal{A}_j\mathcal{B}_j}$ for any two different elements i and j from $\{1,2,3,4\}$.

2. Inputs and measurement operators are noisy

Any apparatus is generally influenced by the ambient noise. In Ref. [15], the players and the referee trust the preparation of the input states τ_s's and ω_t's. So, the noise in τ_s and ω_t (if any), is supposed to be known by the referee (or, even by the players). Some noise may affect the actual shared state $\rho_{\mathcal{AB}}$, but as our method works universally, we will consider the noise-induced shared state as the actual state $\rho_{\mathcal{AB}}$; entanglement of such a

noise-induced state needs to be detected. Note that so far as the set $\mathcal{L}_{\mathcal{AB}}$ (say) of input joint states $\eta_{\mathcal{A}_0\mathcal{B}_0}$ (say) of $\mathcal{A}_0$ and $\mathcal{B}_0$—to be supplied by the referee to Alice and Bob—is known *a priori*, the MDIEW will work equally well—irrespective of whether $\eta_{\mathcal{A}_0\mathcal{B}_0}$ has entanglement or not. Thus the knowledge of the set $\mathcal{L}_{\mathcal{AB}}$ and authenticity of the supplied states $\eta_{\mathcal{A}_0\mathcal{B}_0}$ from $\mathcal{L}_{\mathcal{AB}}$ are assumed to be guaranteed *a priori* for the aforesaid MDIEW scheme of Branciard *et al.* [15].

Even though both the players as well as the referee have trust in the preparation of the input states τ_s and ω_t, for experimental purpose, these states may get affected by some unwanted noise on which the experimenter may not have any control. In this scenario, it is important to know how robust the MDIEW scheme is in the presence of such a noise. In this direction, a general d dimensional noise can be expressed as $\frac{1}{d}\vec{n}.\vec{\Lambda}_{d\times d}$ where n^i and Λ^i are the i^{th} components of generalized Bloch vector and Gell-Mann matrix in the d dimension, respectively, $\Lambda^0 = \mathbb{I}_{d\times d}$ [30]. If the visibility μ of the actual input state is the same for all input states, and assume the visibility remains constant throughout the experiment, then the players (Alice and Bob) would receive the input states as

$$\begin{aligned}\tau_s' &= \mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1\cdot\vec{\Lambda}_{d\times d}\\ &= \left[\frac{(1-\mu)}{d}\vec{n}_1 + \frac{\mu}{d}\mathrm{Tr}(\tau_s\vec{\Lambda}_{d\times d})\right]\cdot\vec{\Lambda}_{d\times d}, \quad \text{and } \omega_t'\\ &= \left[\frac{(1-\mu)}{d}\vec{n}_2 + \frac{\mu}{d}\mathrm{Tr}(\omega_t\vec{\Lambda}_{d\times d})\right]\cdot\vec{\Lambda}_{d\times d},\end{aligned}$$

instead of τ_s and ω_t, respectively. If the referee is not aware about the noise mixed with the inputs, there will be mismatch of the value of $I(\rho_{\mathcal{AB}})$ from its actual value—the case when the referee has information about the noise characteristics.

In the game, the form of W is known to the referee; he calculates the payoff functions, β_{st} according to the inputs from the relation (2). If the referee uses τ_s' and ω_t' as the inputs instead of τ_s and ω_t, his calculated value β_{st} will be different compared to the actual one that will give rise to the actual value of $I(\rho_{\mathcal{AB}})$.

The modified witness operator looks like

$$W' = \sum_{s,t}\beta_{st}\tau_s'^T\otimes\omega_t'^T = \frac{\mu^2}{d^2}\sum_{s,t}\beta_{st}\tau_s^T\otimes\omega_t^T + \text{additional noise terms.} \tag{A4}$$

So, by knowing the amount of noise induced in the input states, the referee can calculate the modified value of β_{st}, which comes from the linear equation generated by $\mathrm{Tr}[W'(\tau_s'^T\otimes\omega_t'^T)]$, for all s,t.

So, we can claim that if the referee knows about the character of the noise in inputs, entanglement determination shouldn't be erroneous.

In general, the measurement operators can also be noisy, and the character of the noise is not supposed to be known by the referee nor by the players. But that noise can obviously affect the final decision based on the value of $I(\rho_{\mathcal{AB}})$. If a general additive noise, $\frac{1}{d^2}\vec{m}\cdot\vec{\Lambda}_{d^2\times d^2}$ is added with the maximally entangled projector $\frac{1}{d}\sum_{i,j=1}^{d}|ii\rangle\langle jj|$, then with the visibility ν of the original measurement operator, the actual measurement operator appears as

$$\frac{\nu}{d}\sum_{i,j}|ii\rangle\langle jj| + \frac{(1-\nu)}{d^2}\vec{m}\cdot\vec{\Lambda}_{d^2\times d^2},$$

provided this is a positive operator, that is, for all $|\chi\rangle$ we have

$$\langle\chi|\left(\frac{\nu}{d}\sum_{i,j}|ii\rangle\langle jj| + \frac{(1-\nu)}{d^2}\vec{m}\cdot\vec{\Lambda}_{d^2\times d^2}\right)|\chi\rangle \geqslant 0.$$

In the standard product basis $\{|i,j\rangle\}$ of $\mathbb{C}^d\otimes\mathbb{C}^d$, we can write

$$\vec{\Lambda}_{d^2\times d^2} = \sum_{a,b,p,q}\langle a,b|\vec{\Lambda}|p,q\rangle|a,b\rangle\langle p,q|$$

For notational convenience, in place of $\rho_{\mathcal{AB}}$, we will be using ρ here and also Λ for $\Lambda_{d^2\times d^2}$. Then

$$\begin{aligned}P_\rho(1,1|s,t) &= \mathrm{Tr}\left[\left\{\left(\frac{\nu}{d}\sum_{i,j}|ii\rangle\langle jj| + \frac{(1-\nu)}{d^2}\vec{m}_1\cdot\vec{\Lambda}\right)\otimes\left(\frac{\nu}{d}\sum_{u,v}|uu\rangle\langle vv| + \frac{(1-\nu)}{d^2}\vec{m}_2\cdot\vec{\Lambda}\right)\right\}\left(\tau_s\otimes\rho\otimes\omega_t\right)\right]\\ &= \frac{\nu^2}{d^2}\mathrm{Tr}\left[\left(\tau_s^T\otimes\omega_t^T\right)\rho\right] + \frac{\nu(1-\nu)}{d^3}\mathrm{Tr}\left[\left(\tau_s^T\otimes\mathrm{Tr}_{\mathcal{B}_i}[(\vec{m}_2\cdot\vec{\Lambda})(\mathbb{I}\otimes\omega_t)]\right)\rho\right]\\ &\quad + \frac{\nu(1-\nu)}{d^3}\mathrm{Tr}\left[\left(\mathrm{Tr}_{\mathcal{A}_i}[(\tau_s\otimes\mathbb{I})(\vec{m}_1\cdot\overrightarrow{\Lambda})]\otimes\omega_t^T\right)\rho\right] + \frac{(1-\nu)^2}{d^4}\mathrm{Tr}\left[\left(\mathrm{Tr}_{\mathcal{A}_i}[(\tau_s\otimes\mathbb{I})\vec{m}_1\cdot\vec{\Lambda}]\otimes\mathrm{Tr}_{\mathcal{B}_i}[\vec{m}_2\cdot\vec{\Lambda}(\mathbb{I}\otimes\omega_t)]\right)\rho\right]\\ &\equiv \frac{1}{d^2}\mathrm{Tr}\left[\left(\tau_s''^T\otimes\omega_t''^T\right)\rho\right].\end{aligned} \tag{A5}$$

If in (A5), $\vec{m}_1\cdot\vec{\Lambda} = \vec{m}_2\cdot\vec{\Lambda} = \mathbb{I}_{d^2\times d^2}\otimes\mathbb{I}_{d^2\times d^2}$ (which will be denoted here as $\mathbb{I}\otimes\mathbb{I}$), and if we define $\vec{\Lambda} = (\mathbb{I},\vec{\Gamma})$, then

$$\begin{aligned}\tau_s''^T\otimes\omega_t''^T &= \frac{\nu^2}{d^2}\tau_s^T\otimes\omega_t^T + \frac{\nu(1-\nu)}{d^3}\tau_s^T\otimes tr_{\mathcal{B}_0}[(\mathbb{I}\otimes\mathbb{I})(\mathbb{I}\otimes\omega_t)]\\ &\quad + \frac{\nu(1-\nu)}{d^3}tr_{\mathcal{A}_0}[(\tau_s\otimes\mathbb{I})(\mathbb{I}\otimes\mathbb{I})]\otimes\omega_t^T + \frac{(1-\nu)^2}{d^4}tr_{\mathcal{A}_0}[(\tau_s\otimes\mathbb{I})\mathbb{I}\otimes\mathbb{I}]\otimes\mathrm{Tr}_{\mathcal{B}_0}[\mathbb{I}\otimes\mathbb{I}(\mathbb{I}\otimes\omega_t)]\end{aligned}$$

$$= \frac{\nu^2}{d^2}\tau_s^T \otimes \omega_t^T + \frac{\nu(1-\nu)}{d^3}\tau_s^T \otimes \mathbb{I} + \frac{\nu(1-\nu)}{d^3}\mathbb{I} \otimes \omega_t^T + \frac{(1-\nu)^2}{d^4}\mathbb{I} \otimes \mathbb{I}$$
$$= \frac{1}{d^4}\mathbb{I} \otimes \mathbb{I} + \frac{\nu}{d^4}(\mathbb{I} \otimes \vec{\Gamma}) \cdot tr\left(\vec{\Gamma}\omega_t^T\right) + \frac{\nu}{d^4}(\vec{\Gamma} \otimes \mathbb{I}) \cdot tr\left(\vec{\Gamma}\tau_s^T\right) + \frac{\nu^2}{d^4}\left(\vec{\Gamma} \cdot tr\left(\vec{\Gamma}\tau_s^T\right)\right) \otimes \left(\vec{\Gamma} \cdot tr\left(\vec{\Gamma}\omega_t^T\right)\right)$$
$$= \frac{1}{d^4}\left(\mathbb{I} + \nu\vec{\Gamma} \cdot tr\left(\vec{\Gamma}\tau_s^T\right)\right)\left(\mathbb{I} + \nu\vec{\Gamma} \cdot tr\left(\vec{\Gamma}\omega_t^T\right)\right). \tag{A6}$$

Thus this is just a shrinking operation of the generalized Bloch vector $\vec{\Gamma}$.

If the referee is unaware about the noise, then, there is deviation from the actual results. So, the referee will use the coefficients β_{st} to be the same as that obtained without any noise. In the presence of noise in inputs and the measurement operator, the witness operator form becomes

$$\sum_{s,t}\beta_{st}\Bigg[\frac{\nu^2}{d^2}\left(\mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1 \cdot \vec{\Lambda}_{d\times d}\right)^T \otimes \left(\mu\omega_t + \frac{(1-\mu)}{d}\vec{n}_2 \cdot \vec{\Lambda}_{d\times d}\right)^T$$
$$+ \frac{\nu(1-\nu)}{d^3}\left(\mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1 \cdot \vec{\Lambda}_{d\times d}\right)^T \otimes tr_{\mathcal{B}_0}\left[(\vec{m}_2 \cdot \vec{\Lambda})\left(\mathbb{I} \otimes \left(\mu\omega_t + \frac{(1-\mu)}{d}\vec{n}_2 \cdot \vec{\Lambda}_{d\times d}\right)\right)\right]$$
$$+ \frac{\nu(1-\nu)}{d^3}tr_{\mathcal{A}_0}\left[\left(\left(\mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1 \cdot \vec{\Lambda}_{d\times d}\right) \otimes \mathbb{I}\right)(\vec{m}_1 \cdot \vec{\Lambda})\right] \otimes \left(\mu\omega_t + \frac{(1-\mu)}{d}\vec{n}_2 \cdot \vec{\Lambda}_{d\times d}\right)^T$$
$$+ \frac{(1-\nu)^2}{d^4}\left\{tr_{\mathcal{A}_0}\left[\left(\left(\mu\tau_s + \frac{(1-\mu)}{d}\vec{n}_1 \cdot \vec{\Lambda}_{d\times d}\right) \otimes \mathbb{I}\right)\vec{m}_1 \cdot \vec{\Lambda}\right] \otimes tr_{\mathcal{B}_0}\left[\vec{m}_2 \cdot \vec{\Lambda}\left(\mathbb{I} \otimes \left(\mu\omega_t + \frac{(1-\mu)}{d}\vec{n}_2 \cdot \vec{\Lambda}_{d\times d}\right)\right)\right]\right\}\Bigg]$$
$$\equiv W''(\text{say}). \tag{A7}$$

Therefore, to get the correct result, in the expression of W, given by Eq. (2), instead of $\tau_s^T \otimes \omega_t^T$, the referee should use

$$\tau_s^{''T} \otimes \omega_t^{''T} = \frac{\nu^2}{d^2}\tau_s^T \otimes \omega_t^T + \frac{\nu(1-\nu)}{d^3}\tau_s^T \otimes \mathrm{Tr}_{\mathcal{B}_0}[(\vec{m}_2 \cdot \vec{\Lambda})(\mathbb{I} \otimes \omega_t)]$$
$$+ \frac{\nu(1-\nu)}{d^3}\mathrm{Tr}_{\mathcal{A}_0}[(\tau_s \otimes \mathbb{I})(\vec{m}_1 \cdot \vec{\Lambda})] \otimes \omega_t^T + \frac{(1-\nu)^2}{d^4}\mathrm{Tr}_{\mathcal{A}_0}[(\tau_s \otimes \mathbb{I})\vec{m}_1 \cdot \vec{\Lambda}] \otimes \mathrm{Tr}_{\mathcal{B}_0}[\vec{m}_2 \cdot \vec{\Lambda}(\mathbb{I} \otimes \omega_t)]. \tag{A8}$$

By knowing the character of the noise mixed with the measurement operator, the referee can change the β_{st} values and in this way $I(\rho)$ remains proportional to $\mathrm{Tr}(W\rho)$. If he doesn't know that, then the error will be proportional to $\mathrm{Tr}[(W'' - W)\rho]$, where

$$W'' - W = \sum_{s,t}\beta_{st}\left[\tau_s^{''T} \otimes \omega_t^{''T} - \tau_s^T \otimes \omega_t^T\right], \tag{A9}$$

and β_{st} are calculated according to the Eq. (2).

With noisy input states and measurement operator, we have

$$I(\rho) = I(\nu,\mu,\vec{m}_1,\vec{m}_2,\vec{n}_1,\vec{n}_2,\rho) = I(1,1,\vec{0},\vec{0},\vec{0},\vec{0},\rho) + \mathrm{Tr}\left[\rho\left(W'' - \sum_{s,t,a,b}\beta_{st}^{ab}\tau_s^T \otimes \omega_t^T\right)\right]. \tag{A10}$$

So noise (both in preparation as well as measurement) can, in principle, *degrade* the quality of measurement-device-independent implementation of the entanglement witness operator. Based upon reliability of the state preparations, noise in the BSM can, in principle, be detected and thereby using the complete knowledge of such a noisy BSM, MDIEW is possible.

3. Expression for $I_{\mathrm{mod}}(\rho_{\mathcal{AB}})$

Our original witnessing function was

$$I(\rho_{\mathcal{AB}}) = \sum_{s,t}\beta_{st}\mathrm{Tr}[(|\Phi^+\rangle\langle\Phi^+| \otimes |\Phi^+\rangle\langle\Phi^+|)(\tau_s \otimes \rho_{\mathcal{AB}} \otimes \omega_t)], \tag{A11}$$

while the modified form of that is (due to noise in BSM)

$$I_{\mathrm{mod}}(\rho_{\mathcal{AB}}) = \sum_{s,t}\beta_{st}\xi\ \mathrm{Tr}\left[\left(P_{\mathcal{A}_0\mathcal{A}} \otimes P_{\mathcal{B}\mathcal{B}_0}\right)(\tau_s \otimes \rho_{\mathcal{AB}} \otimes \omega_t)\right], \tag{A12}$$

where the modified measurement operator is given by

$$
\begin{aligned}
P_{\mathcal{A}_0\mathcal{A}} \otimes P_{\mathcal{B}\mathcal{B}_0} &= \mu_1\mu_2 \cos^2(\Delta_1)\cos^2(\Delta_2)\,|\Phi^+\rangle\langle\Phi^+| \otimes |\Phi^+\rangle\langle\Phi^+| \\
&+ \mu_1\mu_2 \cos^2(\Delta_1)\cos(\Delta_2)\sin(\Delta_2)\,|\Phi^+\rangle\langle\Phi^+| \otimes (|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \\
&+ \mu_1\mu_2 \cos^2(\Delta_1)\sin^2(\Delta_2)\,|\Phi^+\rangle\langle\Phi^+| \otimes |\Psi^-\rangle\langle\Psi^-| + \frac{\mu_1(1-\mu_2)}{4}\cos^2(\Delta_1)\,|\Phi^+\rangle\langle\Phi^+| \otimes \mathbb{I} \\
&+ \mu_1\mu_2 \cos(\Delta_1)\sin(\Delta_1)\cos^2(\Delta_2)(|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \otimes |\Phi^+\rangle\langle\Phi^+| + \mu_1\mu_2 \cos(\Delta_1)\sin(\Delta_1)\cos(\Delta_2) \\
&\times \sin(\Delta_2)(|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \otimes (|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \\
&+ \mu_1\mu_2 \cos(\Delta_1)\sin(\Delta_1)\sin^2(\Delta_2)(|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \otimes |\Psi^-\rangle\langle\Psi^-| \\
&+ \frac{\mu_1(1-\mu_2)}{4}\cos(\Delta_1)\sin(\Delta_1)(|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \otimes \mathbb{I} \\
&+ \mu_1\mu_2 \sin^2(\Delta_1)\cos^2(\Delta_2)\,|\Psi^-\rangle\langle\Psi^-| \otimes |\Phi^+\rangle\langle\Phi^+| \\
&+ \mu_1\mu_2 \sin^2(\Delta_1)\cos(\Delta_2)\sin(\Delta_2)\,|\Psi^-\rangle\langle\Psi^-| \otimes (|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \\
&+ \mu_1\mu_2 \sin^2(\Delta_1)\sin^2(\Delta_2)\,|\Psi^-\rangle\langle\Psi^-| \otimes |\Psi^-\rangle\langle\Psi^-| \\
&+ \frac{\mu_1(1-\mu_2)}{4}\sin^2(\Delta_1)\,|\Psi^-\rangle\langle\Psi^-| \otimes \mathbb{I} + \frac{(1-\mu_1)\mu_2}{4}\cos^2(\Delta_2)\mathbb{I} \otimes |\Phi^+\rangle\langle\Phi^+| \\
&+ \frac{(1-\mu_1)\mu_2}{4}\cos(\Delta_2)\sin(\Delta_2)\mathbb{I} \otimes (|\Psi^-\rangle\langle\Phi^+| + |\Phi^+\rangle\langle\Psi^-|) \\
&+ \frac{(1-\mu_1)\mu_2}{4}\sin^2(\Delta_2)\mathbb{I} \otimes |\Psi^-\rangle\langle\Psi^-| + \frac{(1-\mu_1)(1-\mu_2)}{16}\mathbb{I} \otimes \mathbb{I}. \qquad \text{(A13)}
\end{aligned}
$$

In right-hand side of Eq. (A13), only four terms—first, fourth, thirteenth, and sixteenth summands—will contribute to the projector $|\Phi^+\rangle\langle\Phi^+| \otimes |\Phi^+\rangle\langle\Phi^+|$. These terms are as follows:

$$
\begin{aligned}
&\mu_1\mu_2 \cos^2(\Delta_1)\cos^2(\Delta_2)\,|\Phi^+\rangle\langle\Phi^+| \otimes |\Phi^+\rangle\langle\Phi^+|, \\
&\frac{\mu_1(1-\mu_2)}{4}\cos^2(\Delta_1)\,|\Phi^+\rangle\langle\Phi^+| \otimes \mathbb{I}, \frac{(1-\mu_1)\mu_2}{4}\cos^2(\Delta_2)\mathbb{I} \otimes |\Phi^+\rangle\langle\Phi^+|, \quad \text{and} \qquad \text{(A14)} \\
&\frac{(1-\mu_1)(1-\mu_2)}{16}\mathbb{I} \otimes \mathbb{I},
\end{aligned}
$$

because $\mathbb{I}$ is mixture of four Bell states,

$$\mathbb{I} = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|.$$

Therefore, from Eqs. (A11)–(A13) we have

$$
\begin{aligned}
I_{\text{mod}}(\rho_{\mathcal{A}\mathcal{B}}) = \xi\Bigg[&\mu_1\mu_2 \cos^2(\Delta_1)\cos^2(\Delta_2) + \frac{\mu_1(1-\mu_2)}{4}\cos^2(\Delta_1) \\
&+ \frac{\mu_2(1-\mu_1)}{4}\cos^2(\Delta_2) + \frac{(1-\mu_1)(1-\mu_2)}{16}\Bigg] I(\rho_{\mathcal{A}\mathcal{B}}) + \text{additional term.} \qquad \text{(A15)}
\end{aligned}
$$

This additional term comes from all the terms in the right-hand side of Eq. (A13) except the above-mentioned four terms in (A14).

Thus, both multiplicative and additive noises are present in the system.

Now, using Eqs. (22) and (A15), we have [for the choice $\mu_1 = \mu_2 = \mu$ and $\Delta_1 = \Delta_2 = \Delta$,],

$$
\begin{aligned}
I_{\text{mod}}(\rho_{\mathcal{A}\mathcal{B}}) = \frac{\xi}{8}\sum_{s,t}\beta_{st}[&2a_3\mu \sin(2\Delta)x_t + 2a_1\mu\cos(2\Delta)x_t - 2a_2\mu y_t - 2a_1\mu\sin(2\Delta)z_t \\
&+ 2a_3\mu\cos(2\Delta)z_t + 2b_1\mu(\cos(2\Delta)x_s + \sin(2\Delta)z_s) - 2b_3\mu(\sin(2\Delta)x_s - \cos(2\Delta)z_s) \\
&- 2b_2\mu y_s - 2c_{33}\mu^2\sin^2(2\Delta)x_s x_t + c_{13}\mu^2\sin(4\Delta)x_s x_t - c_{31}\mu^2\sin(4\Delta)x_s x_t \\
&+ 2c_{11}\mu^2\cos^2(2\Delta)x_s x_t - 2c_{23}\mu^2\sin(2\Delta)y_s x_t + 2c_{32}\mu^2\sin(2\Delta)x_s y_t \\
&- 2c_{21}\mu^2\cos(2\Delta)y_s x_t - 2c_{12}\mu^2\cos(2\Delta)x_s y_t + 2c_{13}\mu^2\sin^2(2\Delta)z_s x_t \\
&+ 2c_{31}\mu^2\sin^2(2\Delta)x_s z_t + c_{11}\mu^2\sin(4\Delta)z_s x_t + c_{33}\mu^2\sin(4\Delta)z_s x_t - c_{11}\mu^2\sin(4\Delta)x_s z_t \\
&- c_{33}\mu^2\sin(4\Delta)x_s z_t + 2c_{31}\mu^2\cos^2(2\Delta)z_s x_t + 2c_{13}\mu^2\cos^2(2\Delta)x_s z_t + 2c_{22}\mu^2 y_s y_t \\
&- 2c_{12}\mu^2\sin(2\Delta)z_s y_t + 2c_{21}\mu^2\sin(2\Delta)y_s z_t - 2c_{32}\mu^2\cos(2\Delta)z_s y_t - 2c_{23}\mu^2\cos(2\Delta)y_s z_t \\
&- 2c_{11}\mu^2\sin^2(2\Delta)z_s z_t + c_{13}\mu^2\sin(4\Delta)z_s z_t - c_{31}\mu^2\sin(4\Delta)z_s z_t + 2c_{33}\mu^2\cos^2(2\Delta)z_s z_t + 2]. \qquad \text{(A16)}
\end{aligned}
$$

4. Noisy Bell state measurement for MDI tomography

Assume that the two-qubit BSM $\{|\Phi^+\rangle\langle\Phi^+|, \mathbb{I}_{4\times4} - |\Phi^+\rangle\langle\Phi^+|\}$ is noisy and it is of the form $\{(1-\zeta)|\Phi^+\rangle\langle\Phi^+| + (1-\zeta)\mathbb{I}_{4\times4}, (1-\zeta)(\mathbb{I}_{4\times4} - |\Phi^+\rangle\langle\Phi^+|) + \zeta|\Phi^+\rangle\langle\Phi^+|\}$ with unknown $\zeta \in [0,1]$. Now, for the referee's input state $\tau_s = \frac{1}{2}(\mathbb{I}_{2\times2} + \vec{r}_s\cdot\vec{\sigma})$ to Alice and a fixed state $\Upsilon = \frac{1}{2}(\mathbb{I}_{2\times2} + \vec{r}\cdot\vec{\sigma})$ of Alice (with $\vec{r}_s, \vec{r} \in \mathbb{R}^3$ and $|\vec{r}_s|, |\vec{r}| \leqslant 1$), from the observed value $\Xi := \mathrm{Tr}[\{(1-\zeta)|\Phi^+\rangle\langle\Phi^+| + (1-\zeta)\mathbb{I}_{4\times4}\} \times \{\tau_s \otimes \Upsilon\}]$, one gets

$$\zeta = \frac{4\Xi - (1 + r_{sx}r_x - r_{sy}r_y + r_{sz}r_z)}{3 - (r_{sx}r_x - r_{sy}r_y + r_{sz}r_z)}.$$

Knowledge of ζ can now be used to get measurement statistics after performing the aforesaid noisy measurement.

[1] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[2] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, (London) Nature **390**, 575 (1997).
[3] L. Maccone, Phys. Rev. A **88**, 042109 (2013).
[4] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett. **83**, 3081 (1999).
[5] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[6] R. Jozsa, arXiv:quant-ph/9707034v1.
[7] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[8] R. Horodecki and M. Horodecki, Phys. Rev. A **54**, 1838 (1996).
[9] L. M. Ioannou, B. C. Travaglione, D. C. Cheung, and A. K. Ekert, Phys. Rev. A **70**, 060303(R) (2004).
[10] L. M. Ioannou and B. C. Travaglione, Phys. Rev. A **73**, 052314 (2006).
[11] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).
[12] R. Augusiak, J. Bae, J. Tura, and M. Lewenstein, J. Phys. A **47**, 065301 (2014).
[13] P. Xu, X. Yuan, L. K. Chen, He Lu, X. C. Yao, X. Ma, Y.-A. Chen, and J. W. Pan, Phys. Rev. Lett. **112**, 140506 (2014).
[14] V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A **74**, 022313 (2006).
[15] C. Branciard, D. Rosset, Y. C. Liang, and N. Gisin, Phys. Rev. Lett. **110**, 060405 (2013).
[16] F. Buscemi, Phys. Rev. Lett. **108**, 200401 (2012).
[17] Reference [15] works in case one can implement measurement in the two-qubit Bell state $|\Phi^+\rangle$ perfectly. See the discussions at the beginning of Sec. II of the present article regarding the scenario when the aforesaid measurement cannot be done perfectly.
[18] R. Augusiak, M. Demianowicz, and P. Horodecki, Phys. Rev. A **77**, 030301 (2008).
[19] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[20] D. G. Mead, Am. Math. Mon. **99**, 749 (1992).
[21] P. Horodecki, Phys. Rev. A **68**, 052101 (2003).
[22] A. K. Ekert, C. M. Alves, D. K. L. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek, Phys. Rev. Lett. **88**, 217901 (2002).
[23] K. Bartkiewicz, P. Horodecki, K. Lemr, A. Miranowicz, and K. Zyczkowski, Phys. Rev. A **91**, 032315 (2015).
[24] X. Yuan, Q. Mei, S. Zhou, and X. Ma, Phys. Rev. A **93**, 042317 (2016).
[25] E. Verbanis, A. Martin, D. Rosset, C. C. W. Lim, R. T. Thew, and H. Zbinden, Phys. Rev. Lett. **116**, 190501 (2016).
[26] G. Kimura, Phys. Lett. A **314**, 339 (2003).
[27] P. Horodecki and A. Ekert, Phys. Rev. Lett. **89**, 127902 (2002).
[28] C. Carmeli, T. Heinosaari, A. Karlsson, J. Schultz, and A. Toigo, Phys. Rev. Lett. **116**, 230403 (2016).
[29] D. Lu, T. Xin, N. Yu, Z. Ji, J. Chen, G. Long, J. Baugh, X. Peng, B. Zeng, and R. Laflamme, Phys. Rev. Lett. **116**, 230501 (2016).
[30] R. A. Bertlmann and P. Krammer, J. Phys. A **41**, 235303 (2008).
[31] S. Bandyopadhyay, S. Ghosh, and V. Roychowdhury, Phys. Rev. A **77**, 032318 (2008).
[32] R. Augusiak, J. Grabowski, M. Kus, and M. Lewenstein, Opt. Commun. **283**, 805 (2010).
[33] L. Gurvits, J. Comput. Syst. Sci. **69**, 448 (2004).
[34] S. Gharibian, Quant. Inf. Comp. **10**, 343 (2010).
[35] Even though we intend to connect the potential validity of the conjectures, made in Sec. IV, with the NP-hardness of the separability problem [33,34], validity of these conjectures may not directly imply that universal witness of entanglement in an arbitrary state of a two-qudit system in an MDI way is impossible, as we rely here on a *specific* way of choosing the universal entanglement witness operators. In fact, in Ref. [25], the authors claimed to have provided a scheme—via semidefinite programming—for universal witnessing of bipartite entanglement in an MDI way, even though, in our opinion, the total number of measurement settings used in Ref. [25] does not seem to beat much that required for the usual quantum state tomography. In fact, our discussion in Sec. III shows that detecting NPT-ness of an arbitrary state of a given bipartite system requires a polynomial (in subsystem dimension) number of different measurement settings—irrespective of whether we want it to be in MDI way or not. Hardness of the problem arises while universally detecting entanglement in PPT states, which, in the worst case, may require a huge number of measurement settings.
[36] M. Nawareg, S. Muhammad, E. Amselem, and M. Bourennane, Sci. Rep. **5**, 8048 (2015).