Reliable and robust entanglement witness

Xiao Yuan, Quanxin Mei, Shan Zhou, and Xiongfeng Ma

Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China

Entanglement, a critical resource for quantum information processing, needs to be witnessed in many practical scenarios. Theoretically, witnessing entanglement is by measuring a special Hermitian observable, called an entanglement witness (EW), which has non-negative expected outcomes for all separable states but can have negative expectations for certain entangled states. In practice, an EW implementation may suffer from two problems. The first one is *reliability*. Due to unreliable realization devices, a separable state could be falsely identified as an entangled one. The second problem relates to *robustness*. A witness may not be optimal for a target state and fail to identify its entanglement. To overcome the reliability problem, we employ a recently proposed measurement-device-independent entanglement witness scheme, in which the correctness of the conclusion is independent of the implemented measurement devices. In order to overcome the robustness problem, we optimize the EW to draw a better conclusion given certain experimental data. With the proposed EW scheme, where only data postprocessing needs to be modified compared to the original measurement-device-independent scheme, one can efficiently take advantage of the measurement results to maximally draw reliable conclusions.

I. INTRODUCTION

Since the inception of quantum theory, entanglement has been recognized as one of the most distinctive quantum features. In a way, Einstein, Podolsky, and Rosen proposed a paradox [1] on entanglement, which was motivated to argue against the quantum theory, however, turned out to be an effective experimental (Bell) test [2] for ruling out classical theories. In the development of the quantum information field, entanglement becomes an essential resource for varieties of tasks [3]. Many quantum advantages can be revealed if there exists entanglement. Witnessing the existence of entanglement is thus an important and necessary step for quantum information processing. For instance, in quantum key distribution (QKD) [4,5], secret keys are ensured crucially by showing that entanglement can be preserved after the quantum channel [6].

In theory, as shown in Fig. 1, entanglement can be witnessed by measuring a Hermitian observable W, whose output expectation for any separable state σ is non-negative,

$$\mathrm{Tr}(W\sigma) \geqslant 0, \tag{1}$$

but can be negative for certain entangled state ρ,

$$\mathrm{Tr}(W\rho) < 0. \tag{2}$$

In this case, we call W an entanglement witness (EW) for ρ [7]. In general, W can be obtained by a linear combination of product observables, which can be measured locally on the subsystems. For a review of entanglement witness, one can refer to Refs. [8,9].

In reality, an EW implementation may suffer from two problems. The first one is *reliability*. That is, one might conclude unreliable results due to imperfect experimental devices. In this case, the validity of the EW result depends on how faithfully one can implement the measurements according to the witness W. If the realization devices are not well calibrated, see Fig. 1 as an example, the practically implemented observable W' may deviate from the original theoretical design W, which can even be not a witness. That is, there may exist

some separable states σ, such that $\mathrm{Tr}[\sigma W'] < 0 \leqslant \mathrm{Tr}[\sigma W]$. Practically, by exploiting device imperfections, an attack has been experimentally implemented for an entanglement witness procedure [10]. In cryptographic applications, such a problem is regarded as a loophole, where one mistakes separable states to be entangled ones. For instance, in QKD, this would indicate that an adversary successfully convinces the users Alice and Bob to share keys which they think are secure but are eavesdropped on. Such a problem is solved by the measurement-device-independent QKD scheme [11], inspired by the time-reversed entanglement-based scheme [12–14]. Branciard *et al.* applied a similar idea to an EW and proposed the measurement-device-independent entanglement witness (MDIEW) scheme [15], in which entanglement can be witnessed without assuming the realization devices. The MDIEW scheme is based on an important discovery that any entangled state can be witnessed in a nonlocal game with quantum inputs [16]. In the MDIEW scheme, it is shown that an arbitrary conventional EW can be converted to be an MDIEW, which has been experimentally tested [10].

The second problem lies with the *robustness* of the EW implementation. Since each (linear) EW can only identify a certain regime of entangled states, a given EW is likely to be ineffective in detecting entanglement existing in an unknown quantum state. While a failure of detecting entanglement is theoretically acceptable, in practice, such a failure may cause an experiment to be highly inefficient. In fact, a conventional EW can only be designed optimally when the quantum state has been well calibrated, which, on the other hand, generally requires one to run quantum state tomography. Practically, when the prepared state can be well modeled, one can indeed choose the optimal EW to detect its entanglement. Since a full tomography requires exponential resources regarding the number of parties, an EW plays an important role for detecting well modeled entanglement, which would generally fail for an arbitrary unknown state. In a way, this problem becomes more serious in the MDIEW scenario, where the measurement devices are assumed to be uncharacterized and even untrusted. In this case, the implemented witness, which may although
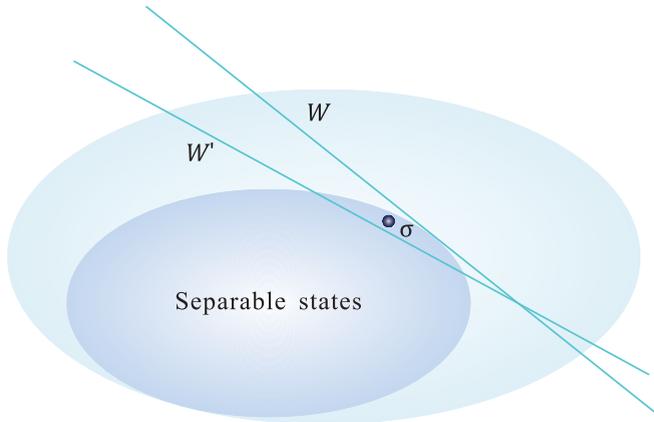
FIG. 1. Entanglement witness and the reliability problem.

be designed optimally in the first place, can become a bad one which merely detects no entanglement. However, the observed experimental data may still have enough information for detecting entanglement. Therefore, the key problem we are facing here is that given a set of observed experimental data, what is the best entanglement detection capability one can achieve.

In detecting quantum nonlocality, a similar problem is to find the optimal Bell inequality for the observed correlation, which can be solved efficiently with linear programming [17]. Regarding our problem, we essentially need to optimize over all entanglement witnesses to draw the best conclusion of entanglement with the same experiment data, as shown in Fig. 2(a). As the set of separable states is not a polytope, this problem cannot be solved by linear programming. Generally speaking, it is proved that the problem of accurately finding such an optimal witness is NP-hard [18]. However, if a certain failure probability is tolerable, we show in this work that this problem can be efficiently solved. That is, if we admit a probability less than ϵ to detect a separable state to be entangled, we show that the optimal entanglement witness can be efficiently found. As the optimization step can be effectively conducted as postprocessing, our scheme does not pose extra burdens on experiments compared to the original MDIEW

scheme. In this case, our result can be directly applied in practice.

The rest of the paper is organized as follows. In Sec. II, we review the MDIEW scheme, which solves the reliability problem. Then, we introduce our robust MDIEW scheme in Sec. III and give an explicit example in Sec. IV. In Sec. V, we summarize our results and discuss practical applications. We mainly focus our discussion on the bipartite scenario. However, our results can be naturally generalized to multipartite cases.

II. RELIABLE ENTANGLEMENT WITNESS

A. Nonlocal games

Before reviewing the MDIEW scheme, we first discuss nonlocal games with classical and quantum inputs as shown in Fig. 3. In a classical nonlocal game, classical random inputs x and y are given to two spacelikely separated users Alice and Bob, who each perform a measurement on a preshared entangled state ρ_{AB} and get outputs a and b, respectively. According to the probability distribution $p(a,b|x,y)$, a Bell inequality can be defined by

$$I = \sum_{a,b,x,y} \beta_{a,b}^{x,y} p(a,b|x,y) \geqslant I_C, \qquad (3)$$

where $\beta_{a,b}^{x,y}$ is the coefficient and I_C is a bound for all separable states σ_{AB}. A violation of the inequality can be considered as a witness for entanglement. As the Bell test does not assume measurement detail, witnessing entanglement by a Bell test is device independent. However, as the conclusion is so strong such that the implementation is self-testing, not all entangled states can be witnessed in such a way [19,20]. Furthermore, the requirement of a faithful Bell test is very high, which makes such a witnesses impractical. For instance, the minimum efficiency required is 2/3 for all Bell tests with binary inputs and outputs [21,22]. On the other hand, if we can trust the measurement, a Bell test essentially becomes an EW. Although such a method is able to detect all entangled states and is easy to realize, this scheme is not measurement-device-imperfection tolerant.

In the seminal work [16], Buscemi introduces the concepts of nonlocal games with quantum inputs. If one denotes the inputs of Alice and Bob by ω_x and τ_y, then an inequality
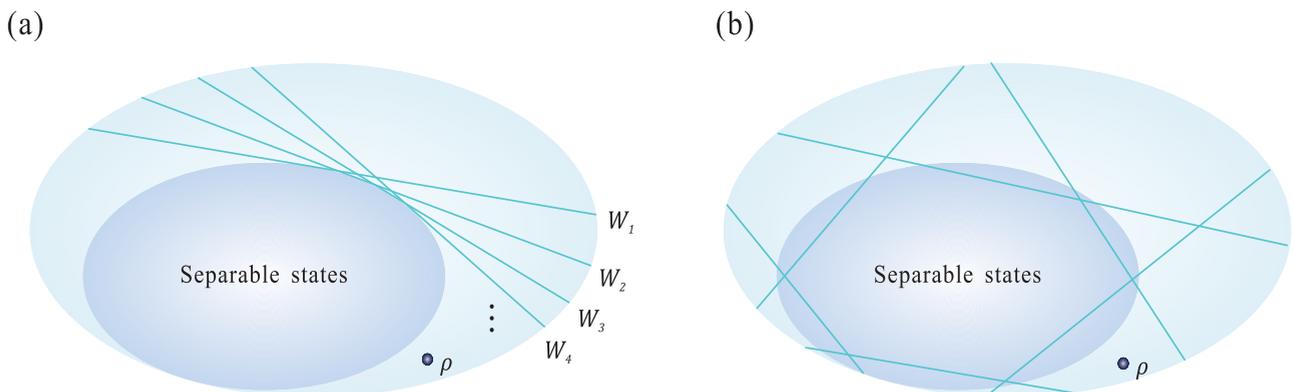
FIG. 2. Optimization of entanglement witnesses. (a) To get the optimal witness of an unknown entangled state ρ, one has to run over all possible witnesses. Intuitively, this is done by scanning over all witnesses that are *tangent* to the set of separable states. (b) The optimization can be efficiently done if a certain failure probability can be tolerated.
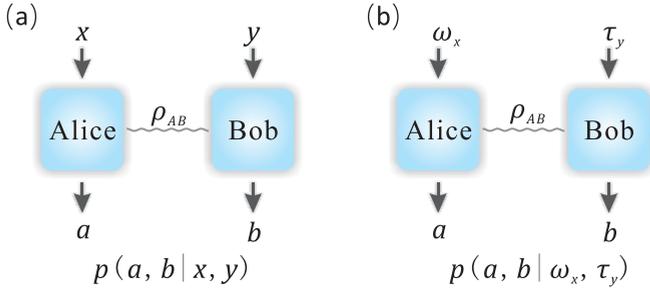
FIG. 3. Bipartite nonlocal game with classical and quantum inputs. (a) Nonlocal game with classical inputs. Based on the classical inputs x and y, Alice and Bob each perform a local measurement on the preshared entangled state ρ_{AB} and get classical outputs a and b, respectively. A linear combination of the probability distribution $p(a,b|x,y)$ defines a Bell inequality as shown in Eq. (3). (b) Nonlocal game with quantum inputs. The quantum inputs of Alice and Bob are, respectively, ω_x and τ_y. It is shown [16] that any entangled quantum states can be witnessed with a certain nonlocal game with quantum inputs. Equivalently, if we consider that Alice and Bob each prepares an ancillary state and a third party Eve performs the measurement, this setup also corresponds to the case of an MDIEW.

similar to a Bell inequality can be defined by

$$J = \sum_{a,b,x,y} \beta_{a,b}^{x,y} p(a,b|\omega_x,\tau_y) \geqslant J_C, \qquad (4)$$

where J_C is also the bound for all separable states ρ_{AB}. As the quantum inputs can be indistinguishable, it is proved that all entangled states can violate a certain inequality [16]. If we consider that the input states are faithfully prepared by Alice and Bob, then such a nonlocal game with quantum inputs can be considered as an MDIEW [15]. Moreover, as shown below, there is no detection efficiency limit for such a test.

B. MDIEW

The nonlocal game presented in Ref. [16] can be considered as a reliable entanglement witness method, which does not witness a separable state as entangled with an arbitrary implemented measurement. This nonlocal game is thus an MDIEW, i.e., $J \geqslant 0$ for all separable states and J can be negative if Alice and Bob share an entangled state. Furthermore, the statement that $J \geqslant 0$ for all separable states is independent of the implementation of the measurement. In Ref. [15], the authors put this statement into a more concrete and practical framework. They show that, for an arbitrary conventional EW, there is a corresponding MDIEW. Below, we will quickly show how to derive MDIEWs from conventional EWs.

Focus on the bipartite scenario with Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, with dimensions $\dim \mathcal{H}_A = d_A$ and $\dim \mathcal{H}_B = d_B$. For a bipartite entangled state ρ_{AB} defined on $\mathcal{H}_A \otimes \mathcal{H}_B$, we can always find a conventional entanglement witness W such that $\text{Tr}[W\rho_{AB}] < 0$ and $\text{Tr}[W\sigma_{AB}] \geqslant 0$ for any separable state σ_{AB}. Suppose $\{\omega_x^{\text{T}}\}$ and $\{\tau_y^{\text{T}}\}$ to be two bases for Hermitian operators on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Thus, we can decompose W on the basis $\{\omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\}$ by

$$W = \sum_{x,y} \beta^{x,y} \omega_x^{\text{T}} \otimes \tau_y^{\text{T}}, \qquad (5)$$

where $\beta^{x,y}$ are real coefficients and the transpose is for later convenience. Notice that, owing to the completeness of the set of density matrices, we further require $\{\omega_x\}$ and $\{\tau_y\}$ to be density matrices. In addition, the decomposition of Hermitian operators is not unique which varies with different $\{\omega_x\}$ and $\{\tau_y\}$.

With a conventional EW decomposed in Eq. (5), an MDIEW can be obtained by

$$J = \sum_{x,y} \beta_{1,1}^{x,y} p(1,1|\omega_x,\tau_y), \qquad (6)$$

where $\beta_{1,1}^{x,y} = \beta^{x,y}$ and $p(1,1|\omega_x,\tau_y)$ is the probability of outputting $(a=1,b=1)$ with input states (ω_x,τ_y). In the MDIEW design, Alice (Bob) performs Bell state measurement on ρ_A (ρ_B) and ω_x (τ_y). The probability distribution $p(1,1|\omega_x,\tau_y)$ is thus obtained by the probability of projecting onto the maximally entangled state $|\Phi_{AA}^+\rangle = 1/\sqrt{d_A} \sum_{i=1}^{d_A} |ii\rangle$ and $|\Phi_{BB}^+\rangle = 1/\sqrt{d_B} \sum_{j=1}^{d_B} |jj\rangle$.

As shown in Ref. [15] and also the Appendix, J is linearly proportional to the conventional witness with an ideal measurement,

$$J = \text{Tr}[W\rho_{AB}]/d_A d_B. \qquad (7)$$

Thus, J defined in Eq. (6) witnesses entanglement. Furthermore, it can be proved that such a witness is independent of the measurement devices. That is, even if the measurement devices are imperfect, J is always non-negative for all separable states and hence no separable state will be mistakenly witnessed to be entangled. We refer to Ref. [15] and also the Appendix for a rigorous proof.

Theoretically, the MDIEW scheme prevents identifying separable states as being entangled. Such a reliable MDIEW has been experimentally demonstrated lately [10]. In practice, however, such a scheme can be inefficient, meaning that it witnesses very few entangled states despite that the observed data could actually provide more information. This is because, in the MDIEW procedure, one first chooses a conventional EW and then realizes it in an MDI way. The conventional EW is chosen based on an empirical estimation of the to-be-witnessed state; thus it may not be able to witness the state for an ill estimation. Furthermore, even if the conventional EW is optimal in the first place, the measurement imperfection will make it suboptimal in practice. Especially, when the input states $\{\omega_x \otimes \tau_y\}$ are complete, a specific witness may not be able to detect entanglement. With complete information, a natural question is whether we can obtain maximal information about entanglement, i.e., get the optimal estimation of an MDIEW.

III. ROBUST MDIEW

Now, we present a method to optimize the MDIEW given fixed observed experiment data $p(1,1|\omega_x,\tau_y)$. Before digging into the details, we compare the problem to a similar one in nonlocality. In the nonlocality scenario, a Bell inequality is used as a witness for quantumness; see Eq. (3). In practice, the Bell inequality may not be optimal for the observed probability distribution $p(a,b|x,y)$. As the probability distribution of a classical correlation forms a polytope, one can run linear

programming to get an optimal Bell inequality for $p(a,b|x,y)$. While, in our case, the probability distribution $p(1,1|\omega_x,\tau_y)$ with separable states is only a convex set but no longer a polytope. Thus, our problem cannot be solved directly with linear programming.

A. Problem formulation

Let us start with formulating the optimization problem. Informally, our problem can be described as follows:

Problem (informal). Find an optimal witness for the observed probability distribution $p(1,1|\omega_x,\tau_y)$. ∎

According to Eq. (6), the witness value is defined by a linear combination of $p(1,1|\omega_x,\tau_y)$ with coefficient $\beta^{x,y}$. To witness entanglement, the coefficient $\beta^{x,y}$ must lead to a witness as defined in Eq. (5). In addition, as we can always assign $2\beta^{x,y}$ to double a violation, we require a trace normalization of the witness W by

$$\text{Tr}[W] = 1. \tag{8}$$

Under this normalization, the optimal entanglement witness W [23] for a given state ρ is defined by the solution to the minimization

$$\min \text{Tr}[W\rho]. \tag{9}$$

Generally speaking, the minimum value, i.e., maximum violation, of the entanglement witness makes the result more robust to experimental errors and statistical fluctuations. Furthermore, a larger violation of entanglement witness can also help for a larger estimation of entanglement measures [24].

Therefore, the problem can be expressed as

Problem (formal). For a given probability distribution $p(1,1|\omega_x,\tau_y)$, minimize

$$J(\beta^{x,y}) = \sum_{x,y} \beta^{x,y} p(1,1|\omega_x,\tau_y) \tag{10}$$

over all $\beta^{x,y}$ satisfying

$$\sum_{x,y} \beta^{x,y} \text{Tr}\big[\sigma_{AB}\big(\omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\big)\big] \geqslant 0, \tag{11}$$

for any separable state σ_{AB} and

$$\text{Tr}\bigg[\sum_{x,y} \beta^{x,y} \omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\bigg] = 1. \tag{12}$$

∎

Contrary to the optimization of the Bell inequality, we can see that this problem is much more complex. When the measurements are implemented faithfully, it is easy to verify that $p(1,1|\omega_x,\tau_y) = \text{Tr}[(\omega_x \otimes \tau_y)\rho_{AB}]/\sqrt{d_A d_B}$, where ρ_{AB} is the state measured. Therefore, finding the optimal $\beta^{x,y}$ is equivalent to finding the optimal entanglement witness $W = \sum_{x,y} \beta^{x,y} \omega_x^{\text{T}} \otimes \tau_y^{\text{T}}$ for state ρ_{AB}. A possible solution to this problem is to try all entanglement witnesses to find the optimal one; see Fig. 2. However, it is proved that the problem of accurately finding such an optimal witness is NP-hard [18]. Thus, our problem is also intractable for the most general case.

B. ϵ-level optimal EW

The key for the problem being intractable is that there is no efficient way to characterize an arbitrary entanglement witness. In the bipartite case, an operator is an witness if and only if

$$\text{Tr}[\sigma_{AB} W] \geqslant 0 \tag{13}$$

for any separable state σ_{AB}. As σ_{AB} can always be decomposed as a convex combination of separable states as $|\psi\rangle_A|\phi\rangle_B$, the condition can be equivalently expressed as

$$\langle\psi|_A\langle\phi|_B W|\psi\rangle_A|\phi\rangle_B \geqslant 0, \tag{14}$$

for any pure states $|\psi\rangle_A$ and $|\phi\rangle_B$. The constraints for a witness W are very difficult to describe in the most general case, which makes our problem hard.

However, this problem can be resolved if we allow certain failure errors. A Hermitian operator W_ϵ is defined as an ϵ-level entanglement witness, when

$$\text{Prob}\{\text{Tr}[\sigma W_\epsilon] < 0|\sigma \in S\} \leqslant \epsilon, \tag{15}$$

where S is the set of separable states. That is, the operator W_ϵ has a probability less than or equal to ϵ to detect a randomly selected separable quantum state to be entangled. Intuitively, ϵ can be regarded as a failure error probability. We refer to Ref. [25] for a rigorous definition. It is shown that the ϵ-level optimal EW can be found efficiently for any given entangled state ρ. In particular, constrained on $\text{Tr}[W_\epsilon] = 1$ and W_ϵ to be an ϵ-level EW, one can run a semidefinite programming (SDP) to minimize $\text{Tr}[W_\epsilon\rho]$.

C. Solution

Following the method proposed in Ref. [25], we can solve the minimization problem given in Eq. (10) by allowing a certain failure probability ϵ. First, we relax the constraint given in Eq. (11). Instead of requiring being non-negative for all separable states, we randomly generate N separable states $\{|\psi\rangle_A^i|\phi\rangle_B^i\}$ and require that

$$\sum_{x,y} \beta^{x,y} \langle\omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\rangle^i \geqslant 0, \forall i \in \{1,2,\ldots,N\}, \tag{16}$$

where $\langle\omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\rangle^i = \langle\psi|_A^i\langle\phi|_B^i \omega_x^{\text{T}} \otimes \tau_y^{\text{T}}|\psi\rangle_A^i|\phi\rangle_B^i$. Then the problem can be expressed as

Problem (*ϵ-level*). Given a probability distribution $p(1,1|\omega_x,\tau_y)$, minimize

$$J(\beta^{x,y}) = \sum_{x,y} \beta^{x,y} p(1,1|\omega_x,\tau_y) \tag{17}$$

over all $\beta^{x,y}$ satisfying

$$\sum_{x,y} \beta^{x,y} \langle\omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\rangle^i \geqslant 0, \forall i \in \{1,2,\ldots,N\}, \tag{18}$$

for N randomly generated separable states $\{|\psi\rangle_A^i|\phi\rangle_B^i\}$ and

$$\sum_{x,y} \beta^{x,y} \text{Tr}\big[\omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\big] = 1. \tag{19}$$

∎

This problem can be converted to an SDP solvable problem when we reexpress the inequality of numbers in Eq. (18) by an

inequality of matrices. To do so, we only need to notice that Eq. (14) is equivalent to require that

$$W_B = \langle\psi|_A W_\epsilon|\psi\rangle_A \geqslant 0, \forall|\psi\rangle_A, \qquad (20)$$

where $W_B \geqslant 0$ indicates that W_B has non-negative eigenvalues. Therefore, we only need to generate N states $|\psi\rangle_A^i$, for $i = 1, 2, \ldots, N$, and the problem is

Problem (ϵ-level, SDP). Given a probability distribution $p(1,1|\omega_x, \tau_y)$, minimize

$$J(\beta^{x,y}) = \sum_{x,y} \beta^{x,y} p(1,1|\omega_x, \tau_y) \qquad (21)$$

over all $\beta^{x,y}$ satisfying

$$\sum_{x,y} \beta^{x,y} \langle\psi|_A^i \omega_x^T|\psi\rangle_A^i \tau_y^T \geqslant 0, \forall i \in \{1,2,\ldots,N\}, \qquad (22)$$

for N randomly generated states $\{|\psi\rangle_A^i\}$ and

$$\sum_{x,y} \beta^{x,y} \mathrm{Tr}[\omega_x^T \otimes \tau_y^T] = 1. \qquad (23)$$

∎

In practice, we can run an SDP to solve this problem. According to Refs. [25,26], to get the ϵ-level witness with probability at least $1 - \beta$, the number of random states N should be at least $r/(\epsilon\beta) - 1$. Here r is the number of optimization variables, i.e., coefficients β, and β can be understood as the failure probability of the minimization program. It is worth to remark that the problem can be similarly solved in the multipartite case.

IV. EXAMPLE

In this section, we show explicit examples about how the witness becomes nonoptimal in the MDI scenario and how this problem can be resolved by running the optimizing program.

Suppose the to-be-witnessed state is a two-qubit Werner state [19]:

$$\rho_{AB}^v = v|\Psi^-\rangle\langle\Psi^-| + (1-v)I/4, \qquad (24)$$

where $v \in [0,1]$, $|\Psi^-\rangle = 1/\sqrt{2}(|01\rangle - |10\rangle)$, and I is the identity matrix. The designed entanglement witness for the Werner states is

$$W = \tfrac{1}{2}I - |\Psi^-\rangle\langle\Psi^-|. \qquad (25)$$

As $\mathrm{Tr}[W\rho_{AB}^v] = (1 - 3v)/4$, ρ_{AB}^v is entangled for $v > 1/3$ and separable otherwise.

As shown in Ref. [15], we can choose the input set by

$$\omega_x = \sigma_x \frac{I + \vec{n}\cdot\vec{\sigma}}{2}\sigma_x, \tau_y = \sigma_y \frac{I + \vec{n}\cdot\vec{\sigma}}{2}\sigma_y, x, y = 0, \ldots, 3, \qquad (26)$$

where $\vec{n} = (1,1,1)/\sqrt{3}$, $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ is the Pauli matrices, and $\sigma_0 = I$. According to Eq. (5), the witness can be decomposed on the basis of $\{\omega_x \otimes \tau_y\}$ with coefficient $\beta^{x,y}$ given by

$$\beta^{x,y} = \begin{cases} \frac{5}{8} & \text{if } x = y \\ -\frac{1}{8} & \text{if } x \neq y. \end{cases} \qquad (27)$$
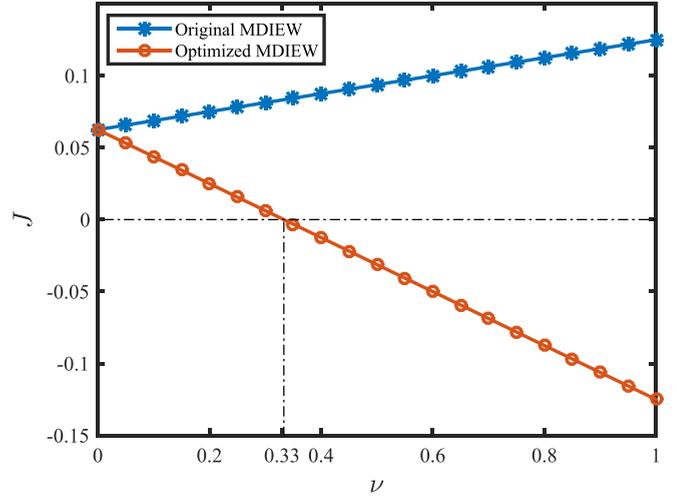
FIG. 4. Simulation results of the original and optimized MDIEW protocols. The to-be-witnessed state is the two-qubit Werner state defined in Eq. (24). Here, we consider that Alice projects onto $|\Phi_{AA}^+\rangle$ and Bob projects onto $|\Phi_{BB}^-\rangle$. In this case, the original MDIEW cannot detect entanglement, while the optimized MDIEW protocol detects all entangled Werner states.

And the MDIEW value is given by

$$J = \frac{5}{8}\sum_{x=y} p(1,1|\omega_x, \tau_y) - \frac{3}{8}\sum_{x\neq y} p(1,1|\omega_x, \tau_y). \qquad (28)$$

In the ideal case, the probability distribution $p(1,1|\omega_x, \tau_y)$ is obtained by projecting onto maximally entangled states, that is,

$$p(1,1|\omega_x, \tau_y) = \mathrm{Tr}[(M_A \otimes M_B) \times (\omega_x \otimes \rho_{AB} \otimes \tau_y)], \quad (29)$$

where $M_A = |\Phi_{AA}^+\rangle\langle\Phi_{AA}^+|$ and $M_B = |\Phi_{BB}^+\rangle\langle\Phi_{BB}^+|$. However, in practice, there may exist imperfection in a measurement. For instance, we consider that Alice's measurement is perfect while Bob's measurement is instead

$$M_B' = |\Phi_{BB}^-\rangle\langle\Phi_{BB}^-|, \qquad (30)$$

where $|\Phi_{BB}^-\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$. In the case of quantum key distribution, projecting onto $|\Phi_{BB}^-\rangle$ can be regarded as a phase error.

As shown in Fig. 4, we plot the original MDIEW and the optimized MDIEW results. For the original MDIEW result, as Bob's measurement is incorrect, no Werner state given in Eq. (24) can be witnessed to be entangled. Although, by optimizing over all possible entanglement witness, we show that ρ_{AB}^v is entangled as long as $v > 1/3$. In this case, the optimized MDIEW can detect all entangled Werner states. In our program, we set $N = 1000$ and we can see from Fig. 4 that no separable state is falsely identified as entangled.

V. DISCUSSION

In this work, we propose an optimized MDIEW scheme to solve the reliability and robustness problems at the same time in entanglement detection, which maximally exploits the measurement data to investigate the entanglement property

without trusting the measurement. By adopting an ϵ-level EW, we present an efficient way for the optimization procedure. As an explicit example, we show that the original MDIEW may not detect entanglement while our optimized MDIEW can. As our optimization can be regarded as a postprocessing of experimental data, our scheme can be easily applied in practice.

The optimization program finds the ϵ-level optimal EW W_ϵ, which as its name indicates, has a probability less than or equal to ϵ to detect a separable state to be entangled. To get a smaller ϵ, one can use a larger number N of random states. In this case, the ϵ can be regarded as the statistical fluctuation which is inversely related to the number of trials N. On the one hand, to efficiently get the optimal witness W_ϵ, one has to introduce a nonzero failure error ϵ; on the other hand, we can always add an extra term to the EW to eliminate ϵ, i.e.,

$$W = W_\epsilon + \alpha I, \tag{31}$$

where α is chosen to be the minimum value such that W is an entanglement witness. To efficiently find α, one can make use of the technique similar to Ref. [27], in which EW can be systematically constructed.

ACKNOWLEDGMENT

APPENDIX: PROOF OF MDIEW

Here, we review the properties of the MDIEW scheme and refer to Ref. [15] for further reference. First, when the measurement is to project onto the maximally entangled state, we show that

$$J = \text{Tr}[W\rho_{AB}]/d_A d_B. \tag{A1}$$

Proof. When Alice and Bob perform both projection measurements onto the maximally entangled state, the conditional probability distribution is

$$
\begin{aligned}
p(1,1|\omega_x, \tau_y) = \text{Tr}[(&|\Phi^+_{AA}\rangle\langle\Phi^+_{AA}| \\
&\otimes |\Phi^+_{BB}\rangle\langle\Phi^+_{BB}|)(\omega_x \otimes \rho_{AB} \otimes \tau_y)] \tag{A2}
\end{aligned}
$$

$$= \text{Tr}\left[\left(\omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\right)\rho_{AB}\right]/d_A d_B. \tag{A3}$$

In this case, the MDIEW value J is

$$J = \sum_{x,y} \beta^{x,y}\text{Tr}\left[\left(\omega_x^{\text{T}} \otimes \tau_y^{\text{T}}\right)\rho_{AB}\right]/d_A d_B \tag{A4}$$

$$= \text{Tr}[W\rho_{AB}]/d_A d_B. \tag{A5}$$

■

Second, we show that for an arbitrary measurement, the MDIEW value will be non-negative for any separable state σ.

Proof. Suppose Alice and Bob are asked to witness a separable state $\sigma_{AB} = \sum_i p_i \sigma_A^i \otimes \sigma_B^i$, where $p_i \geqslant 0, \sum_i p_i = 1$, and the measurements are general positive-operator valued measure elements M_A, M_B, respectively. Consequently, we can represent the conditional probability distribution as the following:

$$p(1,1|\omega_x, \tau_y) = \text{Tr}[(M_A \otimes M_B)(\omega_x \otimes \sigma_{AB} \otimes \tau_y)] \tag{A6}$$

$$= \sum_i p_i \text{Tr}[(A_1^i \otimes B_1^i)(\omega_x \otimes \tau_y)], \tag{A7}$$

where $A_1^i = \text{Tr}_A[M_A(I \otimes \sigma_A^i)]$ and $B_1^i = \text{Tr}_B[M_B(I \otimes \sigma_B^i)]$. Therefore, the MDIEW value J is

$$J = \sum_{x,y} \beta^{x,y} \sum_i p_i \text{Tr}[(A_1^i \otimes B_1^i)(\omega_x \otimes \tau_y)] \tag{A8}$$

$$= \text{Tr}\left[\left(\sum_i p_i A_1^i \otimes B_1^i\right)W^{\text{T}}\right] \tag{A9}$$

$$= \text{Tr}\left[\left(\sum_i p_i A_1^i \otimes B_1^i\right)^{\text{T}} W\right]. \tag{A10}$$

As W is an EW and $\left(\sum_i p_i A_1^i \otimes B_1^i\right)^{\text{T}}$ is a separable state, we can see that $J \geqslant 0$ for an arbitrary measurement and separable state σ_{AB}. ■

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] J. S. Bell, Physics **1**, 195 (1964); *Speakable and Unspeakable in Quantum Mechanics* (Cambridge University Press, Cambridge, 1987).

[3] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[4] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[5] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[6] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).

[7] B. M. Terhal, Linear Algebra Appl. **323**, 61 (2001).

[8] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).

[9] D. Chruściński and G. Sarbicki, J. Phys. A **47**, 483001 (2014).

[10] P. Xu, X. Yuan, L.-K. Chen, H. Lu, X.-C. Yao, X. Ma, Y.-A. Chen, and J.-W. Pan, Phys. Rev. Lett. **112**, 140506 (2014).

[11] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[12] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).

[13] H. Inamori, Algorithmica **34**, 340 (2002).

[14] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[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] S. Boyd and L. Vandenberghe, *Convex Optimization* (Cambridge University Press, Cambridge, 2004).

[18] A. Ben-Tal and A. Nemirovski, Math. Oper. Res. **23**, 769 (1998).

[19] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[20] J. Barrett, Phys. Rev. A **65**, 042302 (2002).

[21] S. Massar and S. Pironio, Phys. Rev. A **68**, 062109 (2003).

[22] J. Wilms, Y. Disser, G. Alber, and I. C. Percival, Phys. Rev. A **78**, 032116 (2008).

[23] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki, Phys. Rev. A **62**, 052310 (2000).

[24] J. Eisert, F. G. Brandão, and K. M. Audenaert, New J. Phys. **9**, 46 (2007).

[25] F. G. S. L. Brandão and R. O. Vianna, Phys. Rev. Lett. **93**, 220503 (2004).

[26] G. Calafiore and M. C. Campi, Math. Program. **102**, 25 (2005).

[27] J. Sperling and W. Vogel, Phys. Rev. Lett. **111**, 110503 (2013).