Randomness Amplification under Simulated $\mathcal{PT}$-symmetric Evolution

Leela Ganesh Chandra Lakkaraju[1], Shiladitya Mal[1,2], Aditi Sen(De)[1]
[1] *Harish-Chandra Research Institute and HBNI, Chhatnag Road, Jhunsi, Allahabad - 211019, India*
[2] *Department of Physics and Center for Quantum Frontiers of Research and Technology (QFort), National Cheng Kung University, Tainan 701, Taiwan*

$\mathcal{PT}$-symmetric quantum theory does not require the Hermiticity property of observables and hence allows a rich class of dynamics. Based on $\mathcal{PT}$-symmetric quantum theory, various counter-intuitive phenomena like faster evolution than that allowed in standard quantum mechanics, single-shot discrimination of nonorthogonal states has been reported invoking Gedanken experiments. By exploiting open-system experimental set-up as well as by computing the probability of distinguishing two states, we prove here that if a source produces an entangled state shared between two parties, Alice and Bob, situated in a far-apart location, the information about the operations performed by Alice whose subsystem evolves according to $\mathcal{PT}$-symmetric Hamiltonian can be gathered by Bob, if the density matrix is in complex Hilbert space. Employing quantum simulation of $\mathcal{PT}$-symmetric evolution, feasible with currently available technologies, we also propose a scheme of sharing quantum random bit-string between two parties when one of them has access to a source generating pseudo-random numbers. We find evidences that the task becomes more efficient with the increase of dimension.

I. INTRODUCTION

Among the postulates of quantum mechanics, the requirement of the Hermiticity property for the observables has the least support from the perspective of physical considerations. It was pointed out that a condition dictated by the fundamental discrete symmetry of the world, i.e., space-time reflection symmetry may lead to a new kind of quantum theory [1, 2] which is commonly known as parity-time-symmetric or $\mathcal{PT}$- symmetric quantum theory. A Hamiltonian in this theory has real eigenvalues in the symmetry unbroken phase and pairwise complex eigenvalues in the symmetry broken phase while in between at the exceptional point, a new type of critical behavior emerges [3–10]. This complex extension of quantum theory not only solves a long-standing problem of negative norm 'ghost' state of renormalized Lee model in quantum field theory [11] but also enlarges the scope of allowed dynamics, thereby culminating in the exploration of varieties of rich phenomena. Throughout the past decade, $\mathcal{PT}$-symmetric Hamiltonian has been realized in classical system like electronic circuit [12], waveguide [13, 14], microcavity [15, 16] and in photonics, capitalzsing on the fundamental structure of balanced loss and gain, it creates almost a new paradigm of devices, eg., synthetic photonic lattices [17], single-mode laser [18, 19], high-sensitivity sensors [20], wireless power transfer [21] to name a few.

In a quantum domain, qualitatively distinct from classical behaviors has been discovered, such as wormhole like behavior in quantum brachistochrone problem [22], single-shot discrimination of non-orthogonal states [23]. Several no-go theorems, valid in standard quantum mechanics, shown to be disturbed in $\mathcal{PT}$-symmetric quantum theory [24–26]. More prominently, the most weaker condition, no-signaling, which is desired to be satisfied in any physical theory, has been shown to be violated in the Gedanken experimental set-up [27]. Violation of these fundamentally significant no-go theorems have deep consequences in the verification of the viability of quantum theory. The contradictions of $\mathcal{PT}$-symmetric quantum theory has been shown to be apparent in two different ways – firstly, by taking care of the proper inner product of the theory, these conflicts evaporates [28–30], while in the second approach, $\mathcal{PT}$-symmetric Hamiltonian was shown to be Hermitian in higher-dimensional space by employing Naimark dilation [31], which opens up the possibility of experimental simulation of the dynamics. In a recent novel experiment, a pair of spatially separated entangled photons is employed to address the problem of apparent signaling [32] in which one of the two photons is evolved according to $\mathcal{PT}$-symmetric evolution which is effectively simulated by a joint unitary operation on the system and an auxiliary system and by performing a measurement on auxiliary subsystem whereas the other spatially seperated photon is governed by the standard quantum theory. In this process, depending upon a particular post-selection on the auxiliary system, $\mathcal{PT}$-symmetric evolution happens on Alice's part of the entangled photons half of the time. In another work reported very recently, state distinguishability has been experimentally verified by structuring $\mathcal{PT}$-symmetric quantum simulator [33] – in the symmetry unbroken phase, the distinguishability quantifier, the trace distance between states oscillates while in the broken phase, it monotonically decreases and hence $\mathcal{PT}$-symmetric dynamics which is different from non-Markovian evolution, allows to completely retrieve information in the unbroken phase [34]. It was also argued in the past that exact $\mathcal{PT}$-symmetric quantum theory is equivalent to standard quantum theory [35, 36] and thus no new physics would be possible [37]. Therefore, to resolve the controversial issues completely in the quantum regime, and to probe the advantage of

$\mathcal{PT}$-symmetric quantum theory over the standard one, applications in the field of information processing tasks are most desirable, which is missing in the literature.

Towards filling the gap, in the present work, we consider $\mathcal{PT}$-symmetric quantum simulation in the open quantum system framework [32] and show that Bob cannot have any input information from Alice's side, if the underlying Hilbert space is real. This discovery has two immediate consequences. Firstly, it was known from the beginning era of quantum theory that system is associated with Hilbert space over complex field, although it was argued whether real Hilbert space is sufficient [38–42]. This line of study has a long history and it is recently proved that complex Hilbert space is inevitable. Therefore, our results along with the recent results on complex Hilbert space [42] indicate that an isolated subsystem may not evolve according to $\mathcal{PT}$-symmetric dynamics, in general. The second one is a direct application in devising cryptographic primitives, randomness amplification [43–45], where genuine randomness can be generated from an weak source of randomness generator (RNG). Pseudo RNG have many applications in biology, economics, statistics but for gambling and cryptographic purposes, genuine RNG is most wanted apart from the foundational application in Bell test [46]. We show a pseudo-random bit string generated from a source provided by a supplier who may be eavesdropper, can be transformed into a genuinely random bit string of a half-length of the initial in an ideal scenario only when $\mathcal{PT}$-symmetric evolution occurs on the underlying complex Hilbert space. The novel application may lead to a better understanding of $\mathcal{PT}$-symmetric quantum system in the context of very fruitful test bed of information processing tasks and devising new quantum technologies. We further show that increasing dimension can lead to some advantages in the distinguishability process of quantum states [47–49].

The paper is organized as follows. In Sec. II, we describe the prerequisites that are required to present the results. The effects of $\mathcal{PT}$-symmetric is more pronounced in the case of complex Hilbert space, shown in Sec. III while the consequence on Bob's reduced state due to local $\mathcal{PT}$-symmetric operation on Alice's end is illustrated in Appendix. Before concluding in Sec. VI, the application of the $\mathcal{PT}$-symmetric dynamics towards quantum randomness generation is presented in Sec. IV and the effects of $\mathcal{PT}$-symmetric dynamics of higher dimensional states are studied in Sec. V.

II. $\mathcal{PT}$-SYMMETRIC DYNAMICS AND ITS QUANTUM SIMULATION

Let us begin with a short discussion on a few preliminary notions relevant for the subsequent sections.

$\mathcal{PT}$-symmetric dynamics. In the $\mathcal{PT}$-symmetric evolution, the Hamiltonian satisfies $H = H^{\mathcal{PT}}$, i.e., the Hamiltonian commutes with parity and time reversal operators (i.e., for a parity operator, $\mathcal{P}H\mathcal{P} = H$ and for complex conjugation, $\mathcal{T}H\mathcal{T} = H$). An example of a two-dimensional non-Hermitian $\mathcal{PT}$-symmetric Hamiltonian is given by [27]

$$H = s\begin{pmatrix} i\sin\alpha & 1 \\ 1 & -i\sin\alpha \end{pmatrix}, \tag{1}$$

where s is the scale factor and α is the non-Hermiticity parameter, such that when $\alpha = n\pi$, H is σ_x Pauli matrix and hence Hermitian. Depending upon the value of α, the distinct three regions exists – (i) $0 < \alpha < \pi/2$ is symmetry unbroken phase, (ii) $\alpha = \pi/2$ is exceptional point where it crosses from unbroken phase to a broken one and (iii) $\alpha > \pi/2$ is symmetry broken phase. The initial state of the system, $\rho(0)$, is evolved to a final state, $\rho(t) = \frac{\exp(-iHt)\rho(0)\exp(iHt)}{Tr[\exp(-iHt)\rho(0)\exp(iHt)]}$.

Let us now describe the experimental set-up proposed in Ref. [32] for simulating the effective $\mathcal{PT}$-symmetric Hamiltonian in the open-system framework. A pair of space-like separated photons are generated by the parametric down conversion which are then sent to two different protagonist say, Alice and Bob via two different channels. After Alice encodes a single bit of information on her photon by randomly choosing between two operations ($A_\pm$), it is evolved according to the $\mathcal{PT}$-symmetric Hamiltonian. It is implemented by evolving the photon together with an auxiliary system via conventional quantum gate operation and subsequently, performing a measurement on the auxiliary system. Depending upon a particular post selection of the auxiliary system, Alice's photon evolved according to $\mathcal{PT}$-symmetric Hamiltonian. It is to be noted here that the entire protocol follows the standard quantum theory and no genuine $\mathcal{PT}$-symmetric Hamiltonian is realised although it can be simulated. On the other hand, Bob's photon is evolved according to the identity channel. Finally, Alice and Bob measure locally on their subsystems simultaneously and record some outcomes.

No-signaling condition. As a consequence of relativistic causality, each spatially separated parties cannot predict the measurement choice of others looking at its own measurement statistics. Mathematically, it is defined as $\sum_a P(a,b \mid A,B) = \sum_a P(a,b \mid A',B)\,\forall b,B$, where A, A' and B are measurements performed by Alice and Bob respectively. Similar condition also holds for interchanging Alice and Bob. In an equivalent formulation, satisfaction of no-signaling principle implies that Bob's reduced system cannot be affected by space-like separated Alice's operation and vice-versa [50]. For two-qubit maximally entangled shared state, by taking $A_\pm$ as $\mathbb{I}$ and σ_x and by permorning measurement by Alice and Bob in σ_y on their respective subsystems [27], a figure of merit for the violation of no-signaling condition can be represented as

$$P_+ - P_- = \sum_a P(a,b \mid A_+,B) - \sum_a P(a,b \mid A_-,B), \tag{2}$$

where $P(a, b \mid A_{\pm}, B)$ is the joint probability of getting outcome a by Alice and b by Bob measuring σ_y according to whether Alice applies A_+ or A_-. In all the previous work [27, 32], violation of no-signaling was shown for the maximally entangled shared two-qubit state in Gedanken experimental set-up. We go beyond such restrictions on shared states and local measurements performed by both the parties and show that it may help to address an important question of differentiating quantum mechanics in real Hilbert space from that in complex ones.

III. $\mathcal{PT}$-SYMMETRIC HAMILTONIAN SINGLES OUT THE REAL HILBERT SPACE

Going beyond maximally entangled shared states, let us consider (i) non-maximally entangled pure state, (ii) the Werner state [51], given by $\rho = p|\psi^+\rangle\langle\psi^+| + \frac{1-p}{4} I_4$, with $|\psi^+\rangle$ and I being the maximally entangled state and white noise respectively and (iii) arbitrary two-qubit density matrix. Such a consideration is also important due to the fact that if it turns out that violation of no-signaling condition at the subsystem level only happens for maximally entangled state, it will never be observed since in a practical scenario, one can have only state close to a maximally entangled state and violation of no-signaling under $\mathcal{PT}$-symmetric evolution becomes pathological. Interestingly, such a general framework provides us a necessary condition for the peaceful coexistence of the genuine $\mathcal{PT}$-symmetric dynamics and no-signaling principle, i.e., we find that the allowed states and observables have to be defined over real Hilbert space to avoid the information gain of Bob about Alice's random operation.

Before presenting the main results for arbitrary two-qubit states with arbitrary measurement, let us illustrate our findings with shared non-maximally entangled, Werner, and two-qubit states by performing the local projective measurement in the y-direction, i.e. in the basis $|\pm_y\rangle = \frac{|0\rangle \pm i|1\rangle}{\sqrt{2}}$ as described in Ref. [27].

Non-maximally entangled and Werner states under $\mathcal{PT}$-symmetric local evolution. Suppose Alice and Bob initially share the state, $|\psi^+\rangle = \frac{\beta|++\rangle + \gamma|--\rangle}{\sqrt{\beta^2+\gamma^2}}$, where $|\pm\rangle$ are eigenstates of σ_x. Depending upon her random information, Alice applies either $A_+ = I$ or $A_- = \sigma_x$ which is followed by the non-unitary evolution $U(t)$, generated by the non-Hermitian Hamiltonian in Eq. (1), $U(t) \equiv e^{-itH} = \frac{1}{\cos\alpha}\begin{pmatrix} \cos(t'-\alpha) & -i\sin t' \\ -i\sin t' & \cos(t'+\alpha) \end{pmatrix}$. Putting $t' = \frac{\Delta E}{2} t$, $t = \frac{\pi}{\delta} E$ where $\delta E = E_+ - E-$, we consequently get $U(t') = \begin{pmatrix} \sin\alpha & -i \\ -i & -\sin\alpha \end{pmatrix}$. After the $\mathcal{PT}$-symmetric evolution, the normalised joint state becomes $\left|\psi_f^{\pm}\right\rangle = [U(\tau) A_{\pm} \otimes e^{-iIt} I] \, |\psi\rangle$. It is to be noted again that here we follow the conventional inner product as in open system quantum simulation, everything follows according to standard quantum theory. After Alice and Bob measure in the $|\pm_y\rangle$ basis, we obtain $P_+ - P_- = \frac{8\beta\gamma\sin\alpha}{(\beta^2+\gamma^2)(-3+\cos 2\alpha)}$. Here we observe that the difference vanishes when either $\alpha = n\pi$, or when $\beta = 0$ or $\gamma = 0$. It implies that when the state is a product state, even with $\alpha \neq n\pi$, the non-Hermitian Hamiltonian does not lead to signaling or as we know, when the evolution is unitary, Bob cannot get the information about Alice's operation even if the shared state is entangled. In case of Werner state [51], following the same prescription as before, the information about Alice's subsystem f can be protected from Bob when $P_+ - P_- = \frac{4p\sin\alpha}{-3+\cos 2\alpha}$ vanishes, i.e. even when $\alpha \neq n\pi$ but $p = 0$, implying the shared state is a maximally mixed state.

Condition for arbitrary two-qubit states. The canonical form of an arbitrary two-qubit state can be written as

$$\rho(m_i, m_i^{'}, C_{ii}) = \frac{1}{4}(I_4 + \sum_{i=x,y,z} [m_i(\sigma_i \otimes I_2) + m_i^{'}(I_2 \otimes \sigma_i) + C_{ii}(\sigma_i \otimes \sigma_i)]), \tag{3}$$

where $m_i(m_i^{'}) = \mathrm{tr}(\sigma_i \otimes I\rho)$ $(\mathrm{tr}(I \otimes \sigma_i\rho))$ and $C_{ii} = \mathrm{tr}(\sigma_i \otimes \sigma_i\rho)$ denote the magnetizations and classical correlators respectively. Following the similar procedure, we obtain that when $C_{yy} = m_y m_y^{'}$ or when $C_{yy} = m_y = 0$, the difference $P_+ - P_- = \frac{2(C_{yy} - m_y m_y^{'})(-3+\cos 2\alpha)\sin\alpha}{(-3+\cos 2\alpha + 4m_y\sin\alpha)(1+2m_y\sin\alpha + \sin^2\alpha)}$ vanishes even when the $\mathcal{PT}$-symmetric evolution occurs at Alice's port. It indicates that the probabilities exclusively depend on state variables in the y direction such as $m_y, m_y^{'}$ and C_{yy}. This is due to the fact that the measurement is performed in the direction of $|\pm_y\rangle\langle\pm_y|$. Only the σ_y component is contracting with the measurement setting, hence the corresponding variables are visible in the probabilities.

Removing such biases, i.e., by performing arbitrary rank-1 projective measurements, we can arrive to the result that if the shared state has elements from complex Hilbert space, Bob can distinguish the information of Alice's random operation.

Theorem 1. *Random input information about Alice's operation can be predicted by Bob with a finite probability when Alice's subsystem is governed by $\mathcal{PT}$-symmetric Hamiltonian successfully and when the underlying Hilbert space corresponds to the state is in complex Hilbert space.*

Proof. By considering an arbitrary two-qubit state, $\rho(m_i, m_i^{'}, C_{ii})$, Alice applies I and σ_x (without loss of generality, we can choose such a fixed operation, since at the end, Alice performs arbitrary measurements), followed by an application of local $\mathcal{PT}$-symmetry operation at Alice's node. Finally, Alice locally performs measurements in the basis $\{|\phi\rangle\langle\phi|, |\phi^{\perp}\rangle\langle\phi^{\perp}|\}$ with

$|\phi\rangle = \cos\frac{y}{2}|0\rangle + e^{iv}\sin(\frac{y}{2})|1\rangle$ and $|\phi^{\perp}\rangle = \sin\frac{y}{2}|0\rangle - e^{-iv}\cos\frac{y}{2}|1\rangle$ while Bob measures $\{|\varphi\rangle\langle\varphi|, |\varphi^{\perp}\rangle\langle\varphi^{\perp}|\}$ with $|\varphi\rangle = \cos\frac{z}{2}|0\rangle + e^{iu}\sin\frac{z}{2}|1\rangle$. The difference between the probability of obtaining $|\varphi\rangle$ at Bob's end, reads

$$\begin{aligned} P^a_+ - P^a_- =& -2(7\sin\alpha - \sin 3\alpha)[m_y m'_x \cos u \sin z \\ &+ \sin u \sin z(-C_{yy} + m_y m'_y) + m_y m'_z \cos z] \\ &/((-3+\cos 2\alpha)^2 - 16 m_y^2 \sin^2\alpha), \end{aligned} \tag{4}$$

where superscript, "a", is used to indicate arbitrary measurements. We observe that the numerator vanishes when $7\sin\alpha - \sin 3\alpha = 0$, which is when $\alpha = n\pi$ and also when $\alpha = 2\pi n \pm 2i\tanh^{-1}(\sqrt{3\pm 2\sqrt{2}})$, $n \in \mathbb{Z}$ or when all the y components of Alice, i.e., m_y and C_{yy} vanish which gives the proof.

□

Remark. Since the time evolution operator at the given specific time can be written as $U = \sin(\alpha)\sigma_z - i\sigma_x$, we find that in $P^a_+ - P^a_-$, m_x, m_z, C_{xx} and C_{zz} are not present.

Corollary 1. *For maximally entangled state and for the Werner state, arbitrary measurements at Bob's end is required to be complex for gathering information about Alice's operation by Bob.*

Proof. When $|\varphi\rangle$ at Bob's side clicks, the condition for the non-maximally entangled state is $P^a_+ - P^a_- = \frac{8\beta\gamma\sin u \sin z \sin\alpha}{(\beta^2+\gamma^2)(-3+\cos 2\alpha)}$ while for the Werner state, it can be given by $P^a_+ - P^a_- = \frac{4p\sin u \sin z \sin\alpha}{-3+\cos 2\alpha}$ (in Eq. (4), putting m_y =0, and $C_{yy} = -p$). Clearly, Alice's information cannot be obtained by Bob if the measurement at Bob's side is real, i.e., $u = 0$ or measurement is along the z-direction or $\alpha = n\pi$.

For pure states, we also get the condition that when the state is product, signaling cannot occur while for Werner states, the condition gives the state to be maximally mixed states. Interestingly, note that the information gain at Bob's end is not related to entanglement for mixed shared states since the Werner state is entangled with $p > 1/3$ (see Appendix and Fig. 3).

□

Distinguishing Bob's states via Trace distance after PT-symmetric evolution at Alice's node. To exhibit the results further, let us find the distance between the Bob's state corresponding to Alice's action of I or σ_x on the shared state. It was shown that for maximally entangled state $|\psi^+\rangle$, at $\alpha = \frac{\pi}{2}$, Bob's state is $|\pm_y\rangle\langle\pm_y|$ corresponding to either I or σ_x operation on Alice's side [27], which indicates that Bob can distinguish his own subsystem perfectly, thereby distinguishing Alice's operation with unit probability. Here notice that the probability of success in distinguishing Alice's operation also depends on the probability involved in post-selection. In general, Bob's state may not always be perfectly distinguishable, it can only be discriminated probabilistically and hence with a nonvanishing probability, Bob can gain information about Alice's randomly chosen operation.

The trace distance between two density matrices, ρ and σ can quantify the maximum probability of minimum error discrimination between the states by the best quantum measurement strategy [52] and is defined as $T(\rho,\sigma) = \frac{1}{2}\mathrm{Tr}\left[\sqrt{(\rho-\sigma)^2}\right] = \frac{1}{2}\sum_i |\lambda_i|$, where λ_is are the eigenvalues of the operator $\sqrt{(\rho-\sigma)^2}$. In this situation, ρ and σ represent the state of Bob when I is applied by Alice, and when σ_x is applied respectively. For arbitrary two-qubit density matrix, it reduces to

$$\begin{aligned} T =& \left|\frac{\sqrt{C_{yy}^2 + m_x'^2 m_y^2 - 2C_{yy}m_y m'_y + m_y^2 m_y'^2 + m_y^2 m_z'^2}}{(-1+2m_y\sin\alpha - \sin^2\alpha)\,(1+2m_y\sin\alpha + \sin^2\alpha)}\right| \\ &\times|(\sin\alpha + \sin^3\alpha)|, \end{aligned} \tag{5}$$

which again shows that if both C_{yy} and m_y vanish, the distance vanishes. It also implies that if the shared state has no imaginary component, the information about Alice's operations cannot be gathered by Bob, even probabilistically, thereby confirming Theorem 1.

IV. RANDOMNESS AMPLIFICATION VIA $\mathcal{PT}$-SYMMETRIC EVOLUTION

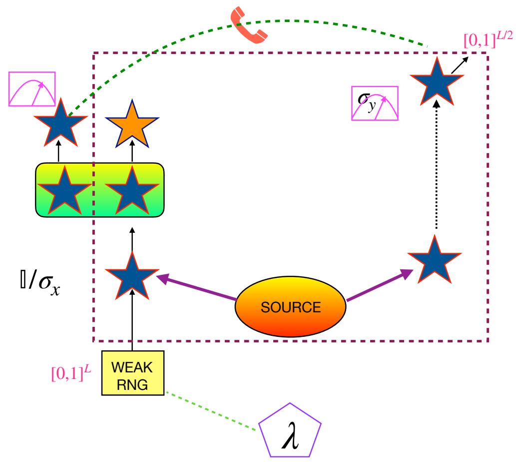

FIG. 1. Schematic diagram of randomness amplification with $\mathcal{PT}$-symmetric evolution. The source produces a two-party state shared between Alice (A) and Bob (B). Alice possess a weak random number generator, and accordingly, operates σ_x or nothing randomly. After that, by using the auxiliary system followed by the measurement and classical information transmission from A to B, Alice's subsystem evolves according to $\mathcal{PT}$-symmetric Hamiltonian. If the initial shared density matrix is in complex Hilbert space, Bob can always create a smaller string of genuine randomness with a finite probability which is dictated by the minimum error discrimination bound.

Let us now describe how the above result enables us to devise novel applications of $\mathcal{PT}$-symmetric dynamics in quantum information processing task, specifically, in the quantum cryptographic domain. It is known that in the classical regime, only pseudo-random number can be obtained while in the quantum domain, genuine randomness can be certified by using quantum no-go theorems [53, 54]. In randomness amplification, a shorter genuine random bit-string is generated from a pseudo-long random string [43]. Towards executing the protocol in our set-up, we replace the short-delay quantum random pulse generator employed in the original protocol [32] by an weak random number generator (WRNG) like Santha-Vazirani source [43, 55]. The choice is due to the fact that we want to show amplification of random number generation (RNG), thereby showing perfect quantum random number source and hence initially if parties have quantum random number generator in their possession, the protocol does not make sense. Here we also assume that this source provided by a supplier may be an eavesdropper.

Let us first give the protocol (in Fig. 1) for maximally entangled shared state and then we go for an arbitrary shared two-qubit states. Before starting the protocol, we assume that Alice and Bob's actions are predecided. Alice encodes one bit of information obtained from WRNG on her subsystem of the shared of maximally entangled photon via applying σ_x when she gets 0 and do nothing when she has 1. Using the open system approach, she jointly evolves her photon together with the auxiliary system by appropriate unitary followed by postselection on auxiliary subsystem (for detailed see [32]). After a short delay, Bob measures σ_y on his part and record his outcome. After that he receives a phone call from Alice and learns the incidence when she succeeds in post selection to obtain a particular outcome. Bob can keep only those outcomes and discard all others. As on average half of the times Alice succeeds about the simulation of $\mathcal{PT}$-symmetric evolution, at the end of the protocol, Bob has a genuine random bit string which has length half of the initial string which Alice obtained from some WRNG. Thus generated randomness is genuine as we do not allow any interference in the lab of two trusted parties, Alice and Bob, including source of entanglement.

The above scheme can lead to several directions depending upon how we run the protocol. For example, one can also think that at the end of protocol, Alice and Bob share a random string of bits which can not be predicted by the outsider, thereby manifesting a QKD protocol. On the other hand, we can employ this model to certify entanglement of the source instead of key generation protocol. If Alice and Bob verifies their random bit string to be equal, they can confirm about the source producing maximally entangled state and otherwise, the source is unable to create. In the ideal scenario, this protocol succeeds in the asymptotic limit of non-Hermiticity parameter to the exceptional point. It is an interesting further study how to make this protocol secure even when entangled photon source is provided by an eavesdropper.

Instead of maximally entangled state, if Alice and Bob share an arbitrary two-qubit density matrix, ρ, such random number amplification is successful probabilistically, and Bob can have a smaller length of bit string than half, provided the classical correlator and magnetization in the y-direction, i.e., C_{yy}, m_y are nonvanishing. The length of the genuine random bit string is related to the distinguishability of states as measured in the previous section.

V. $\mathcal{PT}$ SYMMETRY IN HIGHER DIMENSION

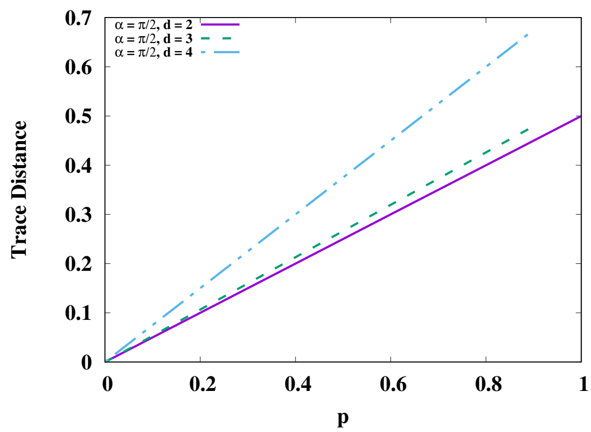

FIG. 2. Trace distance between the initial states and the state after $\mathcal{PT}$-symmetric evolution (vertical axis)) against p (horizontal axis) of the Werner state, given by $\rho^W = p|\psi^+\rangle\langle\psi^+ + (1-p)I$ where $|\psi^+\rangle$ is the maximally entangled state for a given dimension while I denotes the identity operator of that dimension. We choose different α values for demonstration. Both the axis is dimensionless.

Upto now, we consider the shared states to be two-qubits. Let us now move to a higher dimensional situation. The $\mathcal{PT}$-symmetric Hamiltonian, with spin-1 matrices, takes the form as [56] $H = \frac{1}{\sqrt{2}}\begin{pmatrix} i\sin\alpha & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & -i\sin\alpha \end{pmatrix}$. Suppose Alice and Bob share a two-qutrit density matrix, $\rho^3 = \frac{1}{9}(I_9 + \sum_{i=x,y,z} m_i S_i \otimes I + m_i' I \otimes S_i + C_{ii} S_i \otimes S_i)$, where S_i denotes the spin-1 matrices, and m_i, m_i', C_{ii} are correspondingly local and global correlators defined in terms of spin operator, S_i. If we now compare the Bob's state before and after applying $\mathcal{PT}$-symmetric evolution on Alice's side, we find that they coincide when m_y and C_{yy} are vanishing even with $\alpha \neq n\pi$ which is similar to the qubit case as shown in Appendix. However, unlike the qubit case, we also require m_z and C_{zz} to be zero in order to avoid signaling.

Let us now analyze the effects of dimensionality on distinguishability i.e., with the increase of dimension, we compute the trace distance between states before and after $\mathcal{PT}$-symmetric evolution, for different α values when the shared state is the Werner-like state in the respective dimension. We observe that the difference increases with the increase of the dimension as depicted in Fig. 2, when α is chosen to be close to $\pi/2$.

VI. CONCLUSION

In a quantum world, evolution of the system according to parity-time aka $\mathcal{PT}$ symmetry theory reveals several intriguing features ranging from minimum evolution time in quantum brachistochrone problem, spontaneous oscillations in the distinguishability of quantum states to the no-signaling condition. It was also shown that if two observers share a quantum state, an observer can predict the operations occurred at the other end evolved by the $\mathcal{PT}$-symmetric Hamiltonian – such a consequence can never occur when one adopts the proper inner product or simulates such systems in open quantum system framework.

We proved that for arbitrary two-qubit shared states, information about randomly chosen operations performed by a subsystem on which $\mathcal{PT}$-symmetric evolution takes place can be gathered by another subsystem provided the density matrix is defined in complex Hilbert space. For example, considering the maximally entangled state and Werner state, we demonstrated that information about operations can be obtained when either the state is a product or the measurement has a complex component. We then showed that such a consideration has a direct connection in designing quantum random number generator from a pseudo random bit-string. In particular, we showed that systems under $\mathcal{PT}$-symmetric evolution can indeed amplify the shared randomness which has direct implications in quantum state certification as well as quantum cryptographic protocols. Finally, we indicated that such a condition for obtaining information about the operation performed by a spatially separated party holds even in higher-dimensional systems.

ACKNOWLEDGEMENT

We acknowledge the support from the Interdisciplinary Cyber Physical Systems (ICPS) program of the Department of Science and Technology (DST), India, Grant No.: DST/ICPS/QuST/Theme- 1/2019/23 and SM acknowledges Ministry of Science and Technology in Taiwan (Grant no. 110-2811-M-006 -501).

APPENDIX: EFFECTS OF ALICE'S OPERATIONS ON BOB'S REDUCED STATE

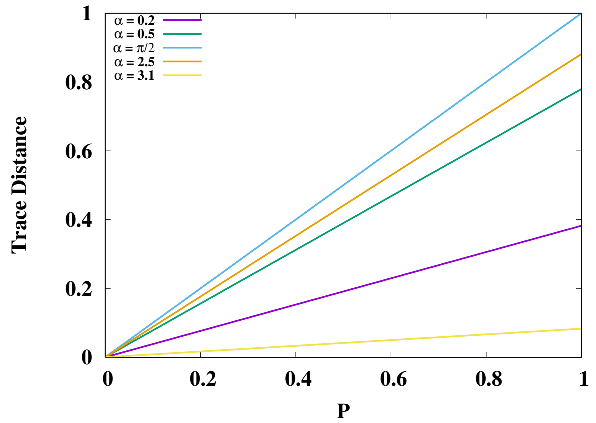

FIG. 3. Trace distance between Bob's state before and after $\mathcal{PT}$-symmetric dynamics (ordinate) vs. p (abscissa) of the two-qubit Werner state. Different α of $\mathcal{PT}$-symmetric evolution are chosen. Both the axes are dimensionless.

There is a straight forward way to check whether the Bob can draw information about Alice's operation, i.e., signaling happens or not by comparing Bob's state before and after local $\mathcal{PT}$-symmetric Hamiltonian as also shown in Sec. V.

Case 1. Non-maximally entangled states. When the shared state is non-maximally entangled, Bob's state (ρ_B) is initially

$$\rho_B = \begin{pmatrix} \frac{1}{2} & 1 - \frac{2\beta^2}{\beta^2+\gamma^2} \\ 1 - \frac{2\beta^2}{\beta^2+\gamma^2} & \frac{1}{2} \end{pmatrix} \tag{6}$$

while after the application of local $\mathcal{PT}$-symmetric Hamiltonian on Alice's subsystem, Bob's state becomes

$$\rho_B' = \begin{pmatrix} \frac{1}{2} & U^{nm} \\ \bar{U}^{nm} & \frac{1}{2} \end{pmatrix}, \tag{7}$$

where $U^{nm} = \frac{(\beta^2-\gamma^2)(-3+\cos(2\alpha))+8i\beta\gamma\sin(\alpha)}{4(\beta^2+\gamma^2)(1+\sin(\alpha)^2)}$ The condition that $\rho_B' = \rho_B$ leads to the condition $\gamma = 0$ even when $\alpha \neq n\pi$, which is similar to the condition reached in Sec. III.

Case 2. Mixed states. For Werner state, Bob's state after $\mathcal{PT}$-symmetry dynamics reads

$$\begin{pmatrix} \frac{1}{2} & \frac{\text{i p Sin }(\alpha)}{1+\sin(\alpha)^2} \\ \frac{2\text{ i }p\sin(\alpha)}{-3+\cos(2\alpha)} & \frac{1}{2} \end{pmatrix}. \tag{8}$$

from its initially maximally mixed subsystem. We plot the trace distance between these two states and find that it vanishes only when $p = 0$ and the maximum distance is achieved when $\alpha = n\pi/2$ (see Fig. 3).

Interestingly, we find the similar condition obtained in Eq. (4) if we compare Bob's state before the dynamics,

$$\rho_B = \begin{pmatrix} \frac{1}{2} + \frac{m_z'}{2} & \frac{m_x'}{2} - \frac{im_y'}{2} \\ \frac{m_x'}{2} + \frac{im_y'}{2} & \frac{1}{2} - \frac{m_z'}{2} \end{pmatrix} \tag{9}$$

and after Alice applies local $\mathcal{PT}$-symmetric operation,

$$\rho_B' = \begin{pmatrix} R_+ & U \\ \bar{U} & R_- \end{pmatrix} \tag{10}$$

with $R_\pm = \frac{1}{2}\left(1 + \frac{(1 \pm \sin(\alpha)^2) m_z{}'}{1+2m_y\sin(\alpha)+\sin(\alpha)^2}\right)$ and $U = \frac{(1+\sin(\alpha)^2)m_x{}' - i(2C_{yy}\sin\alpha + (1+\sin(\alpha)^2)m_y{}')}{2(1+2m_y\sin\alpha+\sin^2\alpha)}$. Comparing each element of the matrix, we find that $R_\pm$ reduces to $\frac{1}{2} \pm \frac{m_z'}{2}$ when m_y vanishes while if both C_{yy} and m_y are vanishing, U reduces to the off-diagonal term of ρ_B, thereby arriving to the same condition as obtained in Theorem 1.

[1] C. M. Bender and S. Boettcher, Phys. Rev. Lett. **80**, 5243 (1998).
[2] C. M. Bender, D. C. Brody, and H. F. Jones, Phys. Rev. Lett. **89**, 270401 (2002).
[3] C. M. Bender, S. Boettcher, and P. N. Meisinger, J. Math. Phys. **40**, 2201 (1999).
[4] P. E. Dorey, C. Dunning, and R. Tateo, J. Phys. A: Math. Gen. **34**, 5679 (2001).
[5] P. E. Dorey, C. Dunning, and R. Tateo, J. Phys. A: Math. Theor. **40**, R205 (2007).
[6] C. M. Bender and T. T. Wu, Phys. Rev. Lett. 21, 406 (1968).
[7] C. M. Bender and T. T. Wu, Phys. Rev. 184, 1231 (1969).
[8] W. D. Heiss, J. Phys. A: Math. Theor. 45, 444016 (2012).
[9] C. M. Bender, N. Hassanpour, D. W. Hook, S. P. Klevansky, C. Sünderhauf, and Z. Wen, Phys. Rev. A **95**, 052113 (2017).
[10] Y. Ashida, S. Furukawa and M. Ueda, Nat. Comm. **8**, 15791 (2017).
[11] C. M. Bender, Rep. Prog. Phys. **70**, 947 (2007).
[12] N. Bender, S. Factor, J. D. Bodyfelt, H. Ramezani, D. N. Christodoulides, F. M. Ellis, and T. Kottos, Phys. Rev. Lett. **110**, 234101 (2013).
[13] A. Guo, G. J. Salamo, D. Duchesne, R. Morandotti, M. Volatier-Ravat, V. Aimez, G. A. Siviloglou, and D. N. Christodoulides, Phys. Rev. Lett. **103**, 093902 (2009).
[14] J. Doppler, A. A. Mailybaev, J. Böhm, U. Kuhl, A. Girschik, F. Libisch, T. J. Milburn, P. Rabl, N. Moiseyev, and S. Rotter, Nature (London) **537**, 76 (2016).
[15] B. Peng, Ş. K. Ozdemir, F. Lei, F. Monifi, M. Gianfreda, G. Lu Long, S. Fan, F. Nori, C. M. Bender, and L. Yang, Nat. Phys. **10**, 394 (2014).
[16] L. Chang, X. Jiang, S. Hua, C. Yang, J. Wen, L. Jiang, G. Li, G. Wang, and M. Xiao, Nat. Photonics **8**, 524 (2014).
[17] A. Regensburger, *et. al.*, Nature **488**, 167–171 (2012).
[18] L. Feng, Z. J. Wong, R.-M. Ma, Y. Wang, and X. Zhang, Science **346**, 972 (2014).
[19] P. Miao, Z. Zhang, J. Sun, W. Walasik, S. Longhi, N. M. Litchinitser, and L. Feng, Science **353**, 464 (2016).
[20] W. Chen, S. K. Ozdemir, G. Zhao, J. Wiersig, and L. Yang, Nature (London) **548**, 192 (2017).
[21] S. Assawaworrarit, X. Yu, and S. Fan, Nature (London) **546**, 387 (2017).
[22] C. M. Bender, D. C. Brody, H. F. Jones, and B. K. Meister, Phys. Rev. Lett. **98**, 040403 (2007).
[23] C. M. Bender, D. C. Brody, J. Caldeira, U. Gunther, B. K. Meister, and B. F. Samsonov, Phil. Trans. R. Soc. A **01**, 371 (2013).
[24] S.-L. Chen, G.-Y. Chen, and Y.-N. Chen, Phys. Rev. A **90**, 054301 (2014).
[25] A. K. Pati, arXiv:1404.6166 (2014).
[26] M. Znojil, Acta Polytechnica (Prague) **56**, 254 (2016).
[27] Y.-C. Lee, M.-H. Hsieh, S. T. Flammia, and R.-K. Lee, Phys. Rev. Lett. **112**, 130404 (2014).
[28] D. C. Brody, J. Phys. A: Math. Theor. 49, 10LT03 (2016).
[29] G. Japaridze, D. Pokhrel, X-Q Wang, J. Phys. A: Math. Theor. **50**, 18503 (2017).
[30] Chia-Yi Ju, Adam Miranowicz, Guang-Yin Chen, and Franco Nori, Phys. Rev. A **100**, 062118 (2019).
[31] U. Gunther, and B. F. Samsonov, Phys. Rev. Lett. **101**, 230404 (2008).
[32] J.-S. Tang, *et al.*, Nat. Photonics **10**, 642 (2016).
[33] Y.-T. Wang *et al.*, Phys. Rev. Lett. **124**, 230402 (2020).
[34] K. Kawabata, Y. Ashida, M. Ueda, Phys. Rev. Lett. **119** 190401 (2017).
[35] A. Mostafazadeh, J. Math. Phys. **43**, 205 (2001).
[36] A. Mostafazadeh, Phys. Rev. Lett. **99**, 130502 (2007).
[37] S. Croke, Phys. Rev. A **91**, 052113 (2015).
[38] E. C. G. Stueckelberg, Quantum Theory in Real Hilbert Space. Helvetica Physica Acta **33**, 727 (1960).
[39] M. McKague, M. Mosca, and N. Gisin, Phys. Rev. Lett. **102**, 020505 (2009).
[40] L. Hardy and W. K. Wootters, Found. Phys. **42**, 454 (2012).
[41] A. Aleksandrova, V. Borish, and W. K. Wootters, Phys. Rev. A **87**, 052106 (2013).
[42] M.-O. Renou, D. Trillo, M. Weilenmann, Le P. Thinh, A. Tavakoli, N. Gisin, A. Acin, and M. Navascues, arXiv:2101.10873.
[43] R. Colbeck and R. Renner, Nat. Phys. **8**, 450 (2012).
[44] M.-H. Li, *et. al.*, Phys. Rev. Lett. **126**, 050503 (2021).
[45] R. Ramanathan, *et. al.*, arXiv:1810.11648.
[46] J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, (Cambridge University Press, New York, 1987).
[47] D. Kaszlikowski, P. Gnacinski, M. Zukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).
[48] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).
[49] S. Roy, A. Kumari, S. Mal, and A. Sen (De), arXiv: 2012.12200.
[50] A. Kumari, and U. Sen, arXiv:2007.13461.
[51] R.F. Werner, Phys. Rev. A **40**, 4277 (1989).
[52] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).

[53] S. Pironio, *et. al.*, Nature **464**, 1021 (2010).
[54] S. Mal, M. Banik and S. K. Choudhary, Quant. Inf. Proc. **15**, 2993 (2016).
[55] M. Santha and U. Vazirani, Journal of Computer and System Sciences **33**, 75 (1986).
[56] Z. Bian, *et. al.*, Phys. Rev. A **102**, 030201(R) (2020) and references therein.