Randomness-Free Test of Nonclassicality: A Proof of Concept

Zhonghua Ma,[1] Markus Rambach,[1] Kaumudibikash Goswami,[1,2,*] Some Sankar Bhattacharya,[3,†]
Manik Banik,[4] and Jacquiline Romero[1,‡]

[1]*Australian Research Council Centre of Excellence for Engineered Quantum Systems and School of Mathematics and Physics, University of Queensland, Queensland 4072, Australia*

[2]*Department of Computer Science, QICI Quantum Information and Computation Initiative, The University of Hong Kong, Pokfulam Road, Hong Kong*

[3]*International Centre for Theory of Quantum Technologies, University of Gdansk, Wita Stwosza 63, 80-308 Gdansk, Poland*

[4]*Department of Physics of Complex Systems, S.N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700106, India*

(Received 25 May 2023; accepted 5 September 2023; published 25 September 2023)

Quantum correlations and nonprojective measurements underlie a plethora of information-theoretic tasks, otherwise impossible in the classical world. Existing schemes to certify such nonclassical resources in a *device-independent* manner require seed randomness—which is often costly and vulnerable to loopholes—for choosing the local measurements performed on different parts of a multipartite quantum system. In this Letter, we propose and experimentally implement a semi-device-independent certification technique for both quantum correlations and nonprojective measurements without seed randomness. Our test is semi–device independent in the sense that it requires only prior knowledge of the dimension of the parts. We experimentally show a novel quantum advantage in correlated coin tossing by producing specific correlated coins from pairs of photons entangled in their transverse spatial modes. We establish the advantage by showing that the correlated coin obtained from the entangled photons cannot be obtained from two two-level classical correlated coins. The quantum advantage requires performing qubit trine positive operator-valued measures (POVMs) on each part of the entangled pair, thus also certifying such POVMs in a semi-device-independent manner. This proof of concept firmly establishes a new cost-effective certification technique for both generating nonclassical shared randomness and implementing nonclassical measurements, which will be important for future multiparty quantum communications.

DOI: 10.1103/PhysRevLett.131.130201

Introduction.—Correlations play an integral role in information processing be it classical or quantum. Nature presents us with composite systems consisting of correlations among multiple subsystems, that cannot be explained if the subsystems are separable [1–6]. Characterizing such nonclassical correlations has been central to quantum theory. Aside from testing Bell inequalities, recent developments in quantum technology provide us with the tools to detect nonclassicality of correlations either as a pseudotelepathy game [7,8] or in a communication task assisted by those correlations [9,10]. Both cases involve randomizing over the choice of inputs (measurement settings in the first case and preparation and measurement in the second case). In this work, we implement a new technique of detecting nonclassical correlations, which does not require costly seed randomness for inputs. As a trade-off the experimenter is required to know only an upper bound to the dimension of the subsystems in use, hence the technique is semi–device independent. Besides foundational interest, this new tool paves the way for a cost-effective characterization of nonclassical resources in quantum information and computation.

We follow an operational approach by considering the task of generating shared randomness between two distant parties. Shared randomness (SR), also known as public or correlated randomness (as opposed to private randomness [11]), can be thought of as a joint probability distribution over random variables shared between two distant parties, that cannot be factorized. Mutual information is a well-known quantifier of such correlations and is a bona fide measure for the distant parties agreeing on a string of measurement outcomes, given a common source [12–14]. Based on mutual information, shared randomness has been established as a useful resource in a number of tasks: privacy amplification, simultaneous message passing, simulation of noisy classical and quantum channels, secret sharing, simulation of quantum correlations, and Bayesian game theory, to name a few [15–28]. Therefore, the generation of shared randomness from some physical system is a question of utmost practical relevance. In an operational theory, SR between two distant parties can be obtained from a bipartite system prepared in some correlated state. In practice, the two parties could each be given a part of a correlated pair of classical or quantum coins which they could use for "coin tossing." Each party performs a local operation on their respective parts of the composite system which results in correlated outcomes and hence SR.

Here, we demonstrate an experimental quantum advantage in generating SR between two parties. Particularly, we show that a two-qubit system prepared in a maximally entangled state can yield some desired SR, that otherwise is unobtainable from the corresponding classical system—two two-level correlated classical coins which we call two-2-coin. This in turn establishes a nonclassical feature of the two-qubit system which distinguishes it from its classical counterpart. Importantly, in our case, a single measurement—positive operator value measure (POVM)—is performed on each part of the entangled pair. Therefore, unlike Bell tests (see [29–31]), no randomization over the choice of local measurements is required for establishing this nonclassicality. In the experiment, we use transverse-mode entangled photon pairs produced via degenerate spontaneous parametric down-conversion as the two-qubit system. The advantage is established through a payoff (different from mutual information) in a game played between two distant parties [32]. The payoff is upper bounded by a threshold value when the parties share a two-2-coin state, whereas a better payoff can be obtained from a two-qubit singlet state even when the state is noisy. The resulting quantum advantage requires generalized measurements, viz. POVMs [33,34] on the local parts of the shared entangled state. The advantage cannot be obtained from local projective measurements, also known as von Neumann measurements [35] and subsequent postprocessing of the outcome statistics. Payoff exceeding the classical threshold value ensures that the measurements are not projective, and thus establishes a semi-device-independent test of generalized measurement.

Correlated coin tossing.—The operational utility of SR can be understood within the framework of resource theory [36]. Sources of two random variables X and Y held by two distant parties, Alice and Bob, will not yield any SR whenever the joint probability distribution is in the product form, i.e., $P(X,Y) = P(X)P(Y)$; here, $P(Z) \equiv \{p(z) | p(z) \geq 0 \text{ and } \sum_{z\in Z} p(z) = 1\}$ denotes a probability distribution on Z. On the other hand, the joint source produces a nonzero amount of shared randomness when the distribution cannot be written as a product. The amount of SR can be quantified by the entropic function called mutual information, $I(X:Y) \coloneqq H(X) + H(Y) - H(X,Y)$; where $H(Z) \coloneqq -\sum p(z)\log_2 p(z)$ denotes the Shannon entropy associated with the source $P(Z)$ [37]. A source $P(Z)$ can be converted into a different one $P'(Z')$ by a stochastic map $S^{Z\to Z'}$, represented by a $|Z'| \times |Z|$ matrix having nonnegative real elements with the entries in each column adding up to unity [38]. While constructing the resource theory of SR, the free operations on a bipartite source $P(X,Y)$ are given by the product of stochastic maps applied on the individual parts, i.e., instead of a general stochastic matrix of the form $S^{XY\to X'Y'}$ only product of local stochastic matrices $S^{X\to X'}$ and $S^{Y\to Y'}$ are allowed as free. For convenience, the free operations can be represented as a tensor product, $S^{X\to X'} \otimes S^{Y\to Y'}$ [32].

Physically, SR can be obtained from a composite system prepared in some correlated state which is shared between distant parties. Alice and Bob perform local operations on their respective parts of the composite state resulting in random but correlated outcomes. Within the framework of generalized probability theory, the state space of such a bipartite system is described by $\Omega_A \otimes \Omega_B$, where Ω_K denotes the marginal state space [39]. For instance, the state space of d-level classical system is the d simplex, a convex set embedded in $\mathbb{R}^{d-1}$ having d number of extremal points. The state space of a two-d-coin, shared between two parties Alice and Bob, is defined as, $\mathbf{C}(d) \equiv \{[p(11), p(12), \ldots, p(dd)]^{\mathrm{T}} | p(ij) \geq 0, \quad \forall\, i,j \in \{1,\ldots,d\}, \quad \text{and} \sum_{i,j} p(ij) = 1\}$ (also see [40]). The quantum analog of two-d-coin is a two-qudit system associated with the Hilbert space $\mathbb{C}_A^d \otimes \mathbb{C}_B^d$, and the corresponding state space is given by $\mathcal{D}(\mathbb{C}_A^d \otimes \mathbb{C}_B^d)$; where $\mathcal{D}(\mathbb{H})$ denotes the set of density operators acting on the Hilbert space $\mathbb{H}$. From a quantum state, $\rho_{AB} \in \mathcal{D}(\mathbb{C}_A^d \otimes \mathbb{C}_B^d)$, Alice and Bob can generate shared randomness (classically correlated coin) by performing local measurements on their respective parts (see Fig. 1). By $\mathbf{C}(k \to d)$, with $k \leq d$, we denote the set of two-d-coin states that can be obtained from the set of two-k-coin states $\mathbf{C}(k)$ by applying free local stochastic maps $S_{A/B}^{k\to d}$ on Alice's and Bob's part of the states. Similarly, $\mathbf{Q}(k \to d)$ denotes the set of two-d-coin states obtained by performing d-outcome local measurements on Alice's and Bob's parts of the bipartite quantum states $\mathcal{D}(\mathbb{C}_A^k \otimes \mathbb{C}_B^k)$. We are now in a position to present our first result as stated in the following proposition (see Appendix A in Supplemental Material [41] for proof).

Proposition 1.—For every $d \geq 3$, $\mathbf{C}(2\to d) \subseteq \mathbf{Q}(2\to d) \subsetneq \mathbf{C}(d)$, whereas $\mathbf{Q}(2 \to 2) = \mathbf{C}(2) = \mathbf{C}(2 \to 2)$.

As evident from this proposition, a quantum advantage in SR generation is possible if we consider the generation of

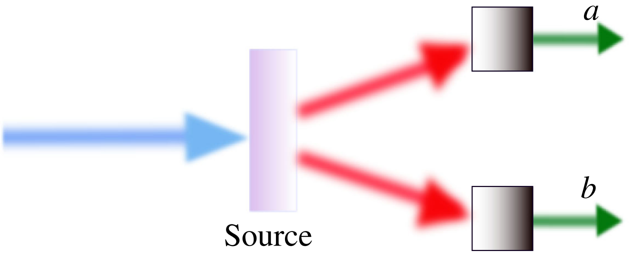

FIG. 1. A trusted source is emitting bipartite correlated systems of local dimension 2, which are then being measured by spatially separated black box devices, which outputs $a \in \{1,\ldots,d\}$ and $b \in \{1,\ldots,d\}$. The sets of observed joint probability distributions $P(a,b)$ for $d > 2$, are different for classical and quantum sources.

a higher dimensional correlated coin state starting from a lower dimensional correlated coin state. More precisely, a proper set inclusion relation $\mathbf{C}(2\to d) \subsetneq \mathbf{Q}(2\to d)$ for some $d \geq 3$ establishes a quantum advantage in correlated coin state generation, which is experimentally testable through the game introduced in [32].

Quantum advantage in correlated coin tossing.—Consider a game $\mathbb{G}(n)$ involving Alice and Bob working in an organization. They buy their lunch from one of the n restaurants $\{r_1, \ldots, r_n\}$. The reimbursement policy of the organization ensures the maximum reimbursement of the lunch bill when (1) Alice and Bob do not end up in the same restaurants on the same day, and (2) their probability of visiting different restaurants should be identical in the long run (see Appendix B in [41] for details). Achieving the maximum reimbursement requires Alice and Bob to share some classical shared randomness which they use to decide which restaurants to go in a particular day. Satisfying (1) and (2) (perfect success) of the game $\mathbb{G}(3)$ requires Alice and Bob to share a coin $\mathcal{C}_{ac}(3) := \frac{1}{6}(0, 1, 1, 1, 0, 1, 1, 1, 0)^{\mathrm{T}} \in \mathbf{C}(3)$. As it turns out, this particular coin cannot be generated from any of the coin states in $\mathbf{C}(2)$ by applying free operations. The optimal payoff Alice and Bob can have with a $\mathbf{C}(2)$ coin is $\mathcal{R}^{\mathbf{C}(2)}_{\max}(3) = 1/8 < 1/6 = \mathcal{R}_{\max}(3)$ (see Supplemental Material [41]). In the quantum case, Alice and Bob, however, can start their protocol by sharing a noisy singlet state

$$\mathcal{W}_p := p|\psi^-\rangle\langle\psi^-| + (1-p)\frac{\mathbf{I}_2}{2}\otimes\frac{\mathbf{I}_2}{2}, \qquad p\in[0,1]; \quad (1)$$

where $|\psi^-\rangle := (1/\sqrt{2})(|0\rangle\otimes|1\rangle - |1\rangle\otimes|0\rangle)$ with $\{|0\rangle, |1\rangle\}$ denoting the eigenstates of Pauli σ_z operator. Both of them perform the *trine* POVM

$$\mathcal{M} \equiv \left\{e_i := \frac{1}{3}(\mathbf{I}_2 + \hat{n}_i.\sigma)\right\}: \hat{n}_i := (\sin\theta_i, 0, \cos\theta_i)^{\mathrm{T}},$$
$$\text{where } \theta_1 = 0, \qquad \theta_2 = 2\pi/3, \qquad \theta_3 = 4\pi/3, \qquad (2)$$

on their respective qubits. This results in a shared coin state $\mathcal{C}_p(3) := (f_p, s_p, s_p, s_p, f_p, s_p, s_p, s_p, f_p)^{\mathrm{T}} \in \mathbf{C}(3)$, with $f_p := (1-p)/9$, $s_p := (2+p)/18$. This manifests in the payoff

$$\mathcal{R}_p(3) := \min_{i\neq j} P(ij) = (2+p)/18, \qquad (3)$$

if Alice and Bob visit the ith restaurant when the ith outcome clicks in their respective measurements. A quantum advantage is demonstrated whenever $\mathcal{R}_p(3) > 1/8$. Quantum states $\mathcal{W}_p \in \mathcal{D}(\mathbb{C}^2\otimes\mathbb{C}^2)$ become advantageous over the classical two-2-coin states $\mathbf{C}(2)$ in playing the $\mathbb{G}(3)$ game whenever $p > 1/4$, with maximally entangled states yielding the highest payoff [32].

Randomness-free test of nonclassicality.—A POVM represents the most general quantum measurement. A POVM is a collection of positive semidefinite operators $\{e_i\}_{i=1}^k$, with $\sum_i e_i = \mathbf{I}_d$, where $\mathbf{I}_d$ is the identity operator acting on the Hilbert space $\mathbb{C}^d$ associated with the system [33,44]. Projective measurements are special cases, where the coefficients e_i correspond to mutually orthogonal projectors π_i. For a qubit, such a measurement can have only two outcomes: $\{\pi_i := |\psi_i\rangle\langle\psi_i| | \langle\psi_i|\psi_j\rangle = \delta_{ij}$ for $i, j = 0, 1\}$. A k-outcome POVM $\{e_i\}_{i=1}^k$ will be called projective simulable if the outcome probabilities of the POVM elements can be obtained by coarse graining the outcome probabilities of some d-outcome projective measurement for any $d < k$, i.e., $\forall\ i\in[1,k]$, $e_i = \sum_j P_{ij}\pi_j$, with $\{\pi_j\}_{j\in[1,d]}$ being a d-outcome projective measurement and $\{P_{ij}\}_i$ denoting probability distributions. For instance, the unsharp qubit measurement $\sigma_{\hat{n}}(\lambda) \equiv \{\frac{1}{2}(\mathbf{I}_2 \pm \lambda\hat{n}.\sigma) | \lambda\in(0,1)\}$ can be simulated through the projective measurement $\sigma_{\hat{n}} \equiv \{\frac{1}{2}(\mathbf{I}_2 \pm \hat{n}.\sigma)\}$, since $\frac{1}{2}(\mathbf{I}_2 \pm \lambda\hat{n}.\sigma) = [(1+\lambda)/4](\mathbf{I}_2 \pm \hat{n}.\sigma) + [(1-\lambda)/4](\mathbf{I}_2 \mp \hat{n}.\sigma)$ [34,45]. Not all POVMs are projective simulable and such measurements are known to be useful for a number of information-theoretic tasks [46–50]. Our game $\mathbb{G}(3)$ provides a semi-device-independent certification of such qubit measurements. Denoting the set of all qubit projective simulable measurements as $\mathbf{PS}(2)$, the result is formally stated as the following proposition.

Proposition 2.—The maximum payoff $\mathcal{R}^{\mathbf{PS}(2)}_{\max}(3)$ of the game $\mathbb{G}(3)$, achievable when the players are restricted to perform measurement from the set $\mathbf{PS}(2)$, is upper bounded by $\mathcal{R}^{\mathbf{C}(2)}_{\max}(3)$.

The claim of Proposition 2 follows from the fact that given dimension d of the local subsystems, the joint outcome probabilities obtained from any arbitrary quantum state and projective measurement are the diagonal elements of the density matrix (the state) when written in the same basis as the projective measurement. Thus, the same statistics can also be obtained from a classically correlated (diagonal) state and measurement on the computational basis.

A payoff higher than the maximum classical payoff, therefore, certifies that the qubit measurements performed by the players are not projective simulable [51]. We highlight that this certification technique is semi–device independent, with the experimenter requiring only the knowledge of the local dimension (in this case $d = 2$) of the state shared between parties. As shown in [52], certification of POVM is possible even in a device-independent manner. However, such a device-independent certification requires violation of a suitably designed Bell-type inequality and hence requires each of the parties involved in the Bell test to randomly perform incompatible measurements on their part of the shared system. Note that the technique of [52] is a detection of nonprojective measurement only if subsystem dimension $d = 2$, which is further guaranteed by a violation of Clauser, Horne,

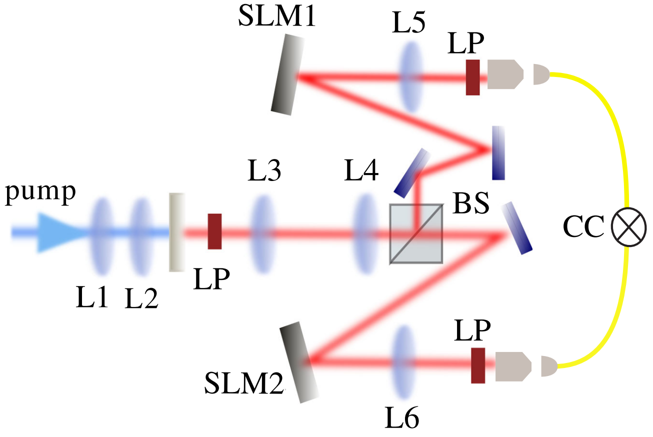

FIG. 2. Experimental setup. A 405-nm pump laser (pump) goes through a nonlinear crystal (BBO) producing pairs of entangled photons at 810 nm. A long-pass filter (LP) separates the pump from the single photons, which are then split probabilistically by a 50/50 beam splitter (BS) between the signal and idler arms representing Alice's and Bob's shares. The combination of the spatial light modulators (SLM1 and SLM2), single mode fibers (yellow curves), and single photon detectors (not shown) correspond to measurements of the transverse mode of the single photons. The output of the single photon detectors is fed to a coincidence circuit (CC) to record the correlations. Lenses (Ls) are placed along the optical path to optimize mode matching.

Shimony, Holt (CHSH)inequality. In contrast, our semi-device-independent scheme requires a single measurement device for each of the parties, getting rid of the seed randomness in inputs to the measurement devices.

Experimental results.—The quantum coin used in the experiment is a pair of photons entangled in their transverse spatial modes produced via degenerate spontaneous parametric down-conversion (SPDC) [42]. We show our experimental schematic in Fig. 2 (see Appendix E in [41]). We implement each element e_i of the trine POVM of Eq. (2) by programming an appropriate hologram onto the spatial light modulators (SLMs E-Series, Meadowlark Optics). The photons reflected from the SLM are coupled to single-mode fibers via lenses L5 and L6. The single-mode fibers are then connected to superconducting nanowire single-photon detectors (superconducting nanowire single-photon detector, Opus One, Quantum Opus). The probability of a party going to a particular restaurant is proportional to the probability of the outcomes of the POVM which can then be obtained from photon counts. To get the joint probability, we record the coincidence count (C_{ij}) between Alice's ith and Bob's jth measurement outcome. This is done via a time-tagging module (TT20, Swabian Instruments) by integrating for 3600 s per data point. We normalize the coincidence counts to evaluate the joint probability $P(ij)$ for Alice and Bob going to the ith and jth restaurant, i.e., $P(ij) = C_{ij}/\sum_{i,j} C_{ij}$ and evaluate the payoff of Eq. (3).

The entangled photons produced by SPDC are in the state $|\psi^+\rangle$, which transforms to the $|\psi^-\rangle$ state when a σ_z rotation is applied to one of the photons. Alternatively, we program the hologram for measuring $\sigma_z e_i \sigma_z$ for one of the photons, where e_i is a POVM element as defined in Eq. (2). In the same manner, for the noisy case where the quantum coin is in the noisy state of Eq. (1), instead of generating $\mathcal{W}_p$, we add the noise to the measurements. The state $\mathcal{W}_p$ signifies that one of the subsystems of the singlet state $|\psi^-\rangle$ undergoes a depolarizing channel of strength p, i.e., the state remains unchanged with a probability $(1+3p)/4$ or undergoes any of the three Pauli rotations, each with a probability $(1-p)/4$. In our experiment, we introduce this depolarizing channel in the measurement settings by implementing the POVM element e_i affected by the noise. This can be done by measuring $\{e_i\}$ with a probability of $(1+3p)/4$ and measuring $\{\sigma_j e_i \sigma_j\}$ with a probability of $(1-p)/4$, where $\{\sigma_j\}$ represent the Pauli operations. Experimentally, we implement this noisy POVM by performing a weighted time average on the relevant measurements. For a total acquisition time of T, we measure $\{e_i\}$ for a time duration of $T(1+3p)/4$ and measure $\{\sigma_j e_i \sigma_j\}$ for a time duration of $T(1-p)/4$ each. Thus, the temporal degree of freedom is used as pointers for the Kraus-operators of the depolarizing channel, and time averaging erases this pointer information leading to a statistical mixture of the Kraus operators [43].

Results obtained in the experiment are depicted in Fig. 3. The payoffs from the probabilities obtained from our experiment are all above the classical limit of 0.125 (dashed green line) for $p > 0.6$, with the highest value being 0.150 ± 0.003 obtained for the noiseless case. The experimental payoffs as a function of the noise (denoted by the depolarization strength p) are given by the blue dots. The ideal payoffs are given by the dash-dotted orange line (i.e., if we have a perfect maximally entangled state for the correlated coins and perfect POVMs). The discrepancies

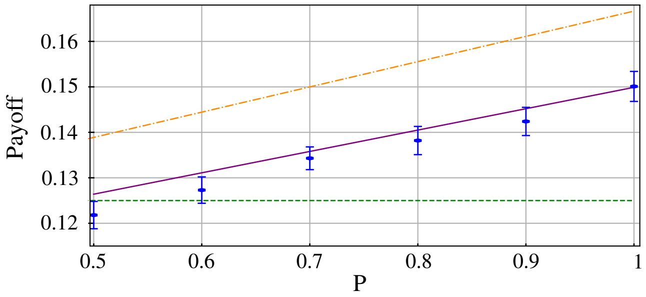

FIG. 3. Payoff of classical optimum strategy vs quantum strategy. The optimal classical payoff of 0.125 is shown as the dashed green line. Ideal quantum payoff following Eq. (3) is plotted in a dash-dotted orange line. Theoretically expected payoffs considering the imperfect entangled state are shown in the solid purple line. Payoffs obtained in experiments are shown in blue dots (along with error bars) and they are all above the classical limit for $p > 0.6$.

between the experiment and the ideal case can be accounted for by our imperfect entangled state. The purple solid line is the expected payoff given the entangled state that we obtained via quantum state tomography using an overcomplete set of 36 measurements (97.0% fidelity to $|\psi^+\rangle$ and purity of 95.2%). Nevertheless, our experiment firmly establishes a quantum advantage in correlated coin tossing even with a significant amount of noise. Apart from establishing the advantage in generating shared randomness our experiment also has another interesting implication as it constitutes a semi-device-independent certification of nonprojective measurement.

Discussions.—Tests of the quantum nature of physical systems are complicated by the requirement of randomness in the inputs to such tests. For example, the true randomness that quantum systems are known to exhibit can only be certified in a device-independent manner using Bell's theorem [53], which in turn needs true randomness (however small) in the inputs [54]—at least qualitatively the argument is circular. The quantum advantage for shared randomness processing that we experimentally demonstrate in this Letter is important as it provides a way to test nonclassical correlations without the need for true randomness—the only test of this kind. Our method certifying both nonclassical correlations and generalized measurements is semi–device independent, requiring only knowledge of the dimensionality of the subsystem. We show that a two-qubit system prepared in a maximally entangled state leads to a higher payoff in our two-party game by yielding some desired correlated coin state, which is impossible to obtain from any two two-level correlated classical coins. In contrast to the advantage in randomness processing demonstrated in [55,56] which involves the probability distribution of one random variable, our work focuses on a new kind of quantum advantage in generating *shared* randomness between two distant parties, involving two random variables and their joint probability distributions. This latter quantum advantage will find use in distributed computational tasks, as in the example of the game we show here. Our work sets the stage for further studies of quantum advantage in multiparty shared randomness processing for qubits or even higher-dimensional systems. Given that randomness processing is an important computational primitive, we envision our work will be useful for information processing in quantum networks.

We thank Valerio Scarani for helpful discussions. S. S. B. acknowledges support from the Foundation for Polish Science (IRAP project, ICTQT, Contract No. MAB/2018/5, cofinanced by EU within Smart Growth Operational Programme). This research was supported by the Australian Research Council Centre of Excellence for Engineered Quantum Systems (EQUS, CE170100009) and Discovery Project (DP200102273). M. B. acknowledges funding from the National Mission in Interdisciplinary Cyber-Physical systems from the Department of Science and Technology through the I-HUB Quantum Technology Foundation (Grant No. I-HUB/PDF/2021-22/008), support through the research grant of INSPIRE Faculty fellowship from the Department of Science and Technology, Government of India, and the start-up research grant from SERB, Department of Science and Technology (Grant No. SRG/2021/000267). J. R. is supported by a Westpac Bicentennial Foundation Research Fellowship.

[*] goswami.kaumudibikash@gmail.com
[†] somesankar@gmail.com
[‡] m.romero@uq.edu.au

[1] A. Einstein, B. Podolsky, and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, Phys. Rev. **47**, 777 (1935).

[2] E. Schrödinger, Probability relations between separated systems, Math. Proc. Cambridge Philos. Soc. **32**, 446 (1936).

[3] J. S. Bell, On the problem of hidden variables in quantum mechanics, Rev. Mod. Phys. **38**, 447 (1966).

[4] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett. **23**, 880 (1969).

[5] A. Aspect, J. Dalibard, and G. Roger, Experimental Test of Bell's Inequalities Using Time-Varying Analyzers, Phys. Rev. Lett. **49**, 1804 (1982).

[6] J-W Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Experimental Entanglement Swapping: Entangling Photons That Never Interacted, Phys. Rev. Lett. **80**, 3891 (1998).

[7] G. Brassard, R. Cleve, and A. Tapp, Cost of Exactly Simulating Quantum Entanglement with Classical Communication, Phys. Rev. Lett. **83**, 1874 (1999).

[8] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86**, 419 (2014).

[9] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Information causality as a physical principle, Nature (London) **461**, 1101 (2009).

[10] M. Pawłowski and M. Żukowski, Entanglement-assisted random access codes, Phys. Rev. A **81**, 042326 (2010).

[11] O. Fischer, R. Oshman, and U. Zwick, Public vs private randomness in simultaneous multi-party communication complexity, Theor. Comput. Sci. **810**, 72 (2020).

[12] A. Bogdanov and E. Mossel, On extracting common random bits from correlated sources, IEEE Trans. Inf. Theory **57**, 6351 (2011).

[13] Badih Ghazi and T. S. Jayram, Resource-efficient common randomness and secret-key schemes, *Proceedings of the 2018 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)* (2018), pp. 1834–1853, 10.1137/1.9781611975031.120.

[14] U. M. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory **39**, 733 (1993).

[15] C. H. Bennett, G. Brassard, and J. Robert, Privacy amplification by public discussion, SIAM J. Comput. **17**, 210 (1988).

[16] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, Generalized privacy amplification, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[17] I. Newman and M. Szegedy, Public vs private coin flips in one round communication games (extended abstract), *STOC '96: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing* (1996), pp. 561–570, 10.1145/237814.238004.

[18] L. Babai and P. G. Kimmel, Randomized simultaneous messages: Solution of a problem of Yao in communication complexity, *Proceedings of Computational Complexity, 20th Annual IEEE Conference* (1997), pp. 239–246, 10.1109/CCC.1997.612319.

[19] R. Ahlswede and I. Csiszar, Common randomness in information theory and cryptography. I. Secret sharing, IEEE Trans. Inf. Theory **39**, 1121 (1993).

[20] B. F. Toner and D. Bacon, Communication Cost of Simulating Bell Correlations, Phys. Rev. Lett. **91**, 187904 (2003).

[21] R. J. Aumann, Correlated equilibrium as an expression of Bayesian rationality, Econometrica **55**, 1 (1987).

[22] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, Zero-error channel capacity and simulation assisted by non-local correlations, IEEE Trans. Inf. Theory **57**, 5509 (2011).

[23] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, Quantum reverse Shannon theorem, IEEE Trans. Inf. Theory **60**, 2926 (2014).

[24] N. Brunner and N. Linden, Connection between Bell nonlocality and Bayesian game theory, Nat. Commun. **4**, 2057 (2013).

[25] A. Roy, A. Mukherjee, T. Guha, S. Ghosh, S. S. Bhattacharya, and M. Banik, Nonlocal correlations: Fair and unfair strategies in Bayesian games, Phys. Rev. A **94**, 032120 (2016).

[26] M. Banik, S. S. Bhattacharya, N. Ganguly, T. Guha, A. Mukherjee, A. Rai, and A. Roy, Two-qubit pure entanglement as optimal social welfare resource in Bayesian game, Quantum **3**, 185 (2019).

[27] C. L. Canonne, V. Guruswami, R. Meka, and M. Sudan, Communication with imperfectly shared randomness, IEEE Trans. Inf. Theory **63**, 6799 (2017).

[28] R. K. Patra, S. Gopalkrishna Naik, E. P. Lobo, S. Sen, T. Guha, S. S. Bhattacharya, M. Alimuddin, and M. Banik, Classical superdense coding and communication advantage of a single quantum, arXiv:2202.06796.

[29] M. J. W. Hall, Local Deterministic Model of Singlet State Correlations Based on Relaxing Measurement Independence, Phys. Rev. Lett. **105**, 250404 (2010).

[30] J. Barrett and N. Gisin, How Much Measurement Independence Is Needed to Demonstrate Nonlocality?, Phys. Rev. Lett. **106**, 100406 (2011).

[31] M. Banik, Lack of measurement independence can simulate quantum correlations even when signaling can not, Phys. Rev. A **88**, 032118 (2013).

[32] T. Guha, M. Alimuddin, S. Rout, A. Mukherjee, S. S. Bhattacharya, and M. Banik, Quantum advantage for shared randomness generation, Quantum **5**, 569 (2021).

[33] K. Kraus, *States, Effects, and Operations Fundamental Notions of Quantum Theory*, edited by K. Kraus, A. Böhm, J. D. Dollard, and W. H. Wootters (Springer, Berlin, Heidelberg, 1983).

[34] P. Busch, Unsharp reality and joint measurements for spin observables, Phys. Rev. D **33**, 2253 (1986).

[35] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, New York, Boston, Dordrecht, 1995), ISBN: 0-7923-2549-4.

[36] E. Chitambar and G. Gour, Quantum resource theories, Rev. Mod. Phys. **91**, 025001 (2019).

[37] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. (Wiley, New York, 2006).

[38] Markov Chains, *Applied Probability and Queues*, Stochastic Modelling and Applied Probability, Vol. 51 (Springer, New York, 2003).

[39] J. Barrett, Information processing in generalized probabilistic theories, Phys. Rev. A **75**, 032304 (2007).

[40] A normal coin-tossing experiment corresponds to the case $d = 2$, and leads to the state space $\mathbf{C}^2 \equiv \{[p(h), p(t)]^\mathrm{T} | p(h), p(t) \geq 0$ and $p(h) + p(t) = 1\}$; $p(h)$ and $p(t)$, respectively, denote the probability of obtaining outcome "head" and "tail." The state space $\mathbf{C}(2) \equiv \mathbf{C}_A^2 \otimes \mathbf{C}_B^2$ of two-2-coin shared between Alice and Bob is given by $\mathbf{C}(2) \equiv \{[p(hh), p(ht), p(th), p(tt)]^\mathrm{T} | p(ij) \geq 0, \quad \forall\, i, j \in \{h, t\}$, and $\sum_{i,j} p(ij) = 1\}$.

[41] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.130201 for proof of Proposition 1 and additional theoretical and experimental details.

[42] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Entanglement of the orbital angular momentum states of photons, Nature (London) **412**, 313 (2001).

[43] A. Shaham and H. S. Eisenberg, Realizing controllable depolarization in photonic quantum-information channels, Phys. Rev. A **83**, 022303 (2011).

[44] P. Busch, M. Grabowski, and P. J. Lahti, *Operational Quantum Physics* (Springer, Berlin, 1995); P. Busch, P. J. Lahti, and P. Mittelstaedt, *The Quantum Theory of Measurement: 2*, Lecture Notes in Physics Monographs Berlin, Heidelberg, (2013).

[45] M. Banik, Md. R. Gazi, S. Ghosh, and G. Kar, Degree of complementarity determines the nonlocality in quantum mechanics, Phys. Rev. A **87**, 052125 (2013).

[46] I. D. Ivanovic, How to differentiate between nonorthogonal states, Phys. Lett. A **123**, 257 (1987).

[47] A. Peres, How to differentiate between nonorthogonal states, Phys. Lett. A **128**, 19 (1988).

[48] T. Vértesi and E. Bene, Two-qubit Bell inequality for which positive operator-valued measurements are relevant, Phys. Rev. A **82**, 062115 (2010).

[49] A. Acín, S. Pironio, T. Vértesi, and P. Wittek, Optimal randomness certification from one entangled bit, Phys. Rev. A **93**, 040102(R) (2016).

[50] M. T. DiMario and F. E. Becerra, Demonstration of optimal non-projective measurement of binary coherent states with photon counting, npj Quantum Inf. **8**, 84 (2022).

[51] S. S. Bhattacharya, S. Rout, and P Horodecki (to be published).

[52] E. S. Gómez, S. Gómez, P. González, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi, and G. Lima, Device-Independent Certification of a Nonprojective Qubit Measurement, Phys. Rev. Lett. **117**, 260401 (2016).

[53] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes,

L. Luo, T. A. Manning, and C. Monroe, Random numbers certified by Bell's theorem, Nature (London) **464**, 1021 (2010).

[54] Gilles Pütz, Denis Rosset, Tomer Jack Barnea, Yeong-Cherng Liang, and Nicolas Gisin, Arbitrarily Small Amount of Measurement Independence Is Sufficient to Manifest Quantum Nonlocality, Phys. Rev. Lett. **113**, 190402 (2014).

[55] H. Dale, D. Jennings, and T. Rudolph, Provable quantum advantage in randomness processing, Nat. Commun. **6**, 8203 (2015).

[56] R. B. Patel, T. Rudolph, and G. J. Pryde, An experimental quantum Bernoulli factory, Sci. Adv. **5**, eaau6668 (2019).