Weak entanglement improves quantum communication using only product measurements

Amélie Piveteau, Alastair A. Abbott, Sadiq Muhammad, Mohamed Bourennane, Armin Tavakoli

Weak entanglement improves quantum communication using only passive linear optics

Amélie Piveteau,[1] Alastair A. Abbott,[2] Sadiq Muhammad,[1] Mohamed Bourennane,[1] and Armin Tavakoli[3]

[1]*Department of Physics, Stockholm University, S-10691 Stockholm, Sweden*
[2]*Univ. Grenoble Alpes, Inria, 38000 Grenoble, France*
[3]*Physics Department, Lund University, Box 118, 22100 Lund, Sweden*

We show that noisy entangled states, that cannot violate any Bell inequality, can be used to improve quantum communication when measurements are limited to being compatible with standard, ancilla-free, linear optics. We introduce a communication task inspired by the cryptographic primitive known as secret sharing and show that entanglement that is too weak to permit possible Einstein-Podolsky-Rosen steering can still enhance the success rate when using only standard partial Bell state analysers for decoding. We then go further and show that even the simplest type of decoding, namely product measurements, which require no optical interference at all, can still lead to an advantage when the entanglement is steerable but still Bell-local. We demonstrate the former advantage by preparing polarisation qubits in an unsteerable entangled state and by using only beam-splitters and phase-shifters observing a boost in the success rate of beyond the best entanglement-unassisted qubit protocol.

Introduction.—Entanglement is well-known to be the crucial resource for a wide variety of quantum information applications. A major domain of application is in quantum communication where it can, e.g., increase the classical capacity of a quantum channel [1] or reduce classical communication complexity [2]. However, not all forms of entanglement are evidently useful. For instance, while entanglement that is strong enough to generate nonlocality has been found to improve noiseless classical communication beyond its conventional limitations (see, e.g., [3–8]), weaker entangled states that cannot violate any Bell inequality do not have that ability [9]. However, if the system communicated is itself quantum, e.g. a qubit instead of a bit, then some weaker forms of entanglement also become useful. This can be seen in the celebrated dense coding protocol [10] where a maximally entangled state, $|\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, is exploited to allow a qubit message to transmit two bits instead of one bit. Then, if the maximally entangled state is replaced with an isotropic state

$$\rho_v = v|\phi^+\rangle\langle\phi^+| + \frac{1-v}{4}\mathbb{1}, \tag{1}$$

for some visibility $v \in [0,1]$, then an advantage over an unassisted qubit message exists whenever $v > \frac{1}{3}$ [11, 12]. This coincides with the visibility at which the state becomes separable, $v_{\text{sep}} = \frac{1}{3}$, and is considerably lower than the critical visibility for Einstein-Podolsky-Rosen steering under general projective measurements, $v_{\text{unsteer}} = \frac{1}{2}$ [13]. Moreover, it is even further below the largest known visibility at which the isotropic state (1) cannot violate any Bell inequality, $v_{\text{local}} \approx 0.6875$ [14].

However, to harness the dense coding advantage one must measure in the Bell basis $\{\Phi^+, \Phi^-, \Psi^+, \Psi^-\}$, where $\Phi^\pm = |\phi^\pm\rangle\langle\phi^\pm|$ and $\Psi^\pm = |\psi^\pm\rangle\langle\psi^\pm|$ are the projectors onto the states $|\phi^\pm\rangle = \frac{|00\rangle\pm|11\rangle}{\sqrt{2}}$ and $|\psi^\pm\rangle = \frac{|01\rangle\pm|10\rangle}{\sqrt{2}}$. In optical systems, which are the most relevant for quantum communication, it is impossible to implement a linear optics Bell basis measurement on separate photons without the use of auxiliary photons [15]. While dense coding experiments have been reported [16–20], implementation of the Bell basis is not expected to be scalable in optical systems in the near future. Nevertheless, it has recently been found that entanglement can yield advantages in one-shot quantum communication scenarios by using much more limited, yet much less experimentally demanding, optical measurements that are compatible with passive linear optics [21]. However, the schemes considered thus far come with greater requirements on the quality of entanglement, in particular demanding states that can be used to violate a Bell inequality.

Here, we show that when restricting to simple optical measurements, compatible with ancilla-free linear optics, weak forms of entanglement still constitute a resource for enhancing communication. To this end, we introduce a communication task which can be interpreted as a stochastic version of the cryptographic primitive known as secret sharing. In secret sharing a secret is distributed between two parties in such a way that they must cooperate to reconstruct it [22, 23]. This task is of considerable interest for quantum cryptography, and has consequently received much attention (see e.g. [24–28]). We prove that for our task there exist entangled but unsteerable isotropic states which enable an advantage over unassisted qubits using only conventional optical partial Bell state analysers [29, 30]. Using polarisation qubits generated via spontaneous parametric down-conversion, we use both a maximally entangled state to experimentally demonstrate an optimal stochastic secret sharing protocol, and an unsteerable isotropic state to outperform the best possible entanglement-unassisted qubit protocol for the task. We also consider whether an advantage could be obtained using the simplest type of measurements, namely product measurements of separate photons that require no two-photon interference in the decoding procedure. Even with such measurements, we find that some isotropic states that are steerable but cannot violate any Bell inequality still enable an advantage over unassisted qubit communication.

Stochastic secret sharing.—Suppose that Alice wishes to generate a random secret bit $a \in \{0,1\}$ that is shared with Bob and Charlie in such a way that they individually have no knowledge of a but can learn its value if they cooperate. To this end, we consider the scenario illustrated in Fig 1.

In this scenario, Bob and Charlie each privately select two uniformly random bits $x \equiv (x_0, x_1) \in \{0,1\}^2$ and $y \equiv (y_0, y_1) \in \{0,1\}^2$, respectively. Given their respective inputs, Bob and Charlie each communicate a message

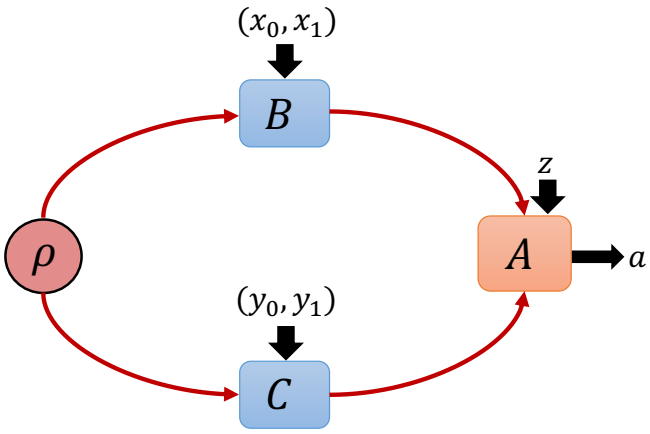

FIG. 1. The secret scharing scenario: Bob and Charlie select private inputs and perform separate transformations on a shared two-qubit entangled state. They relay their respective output qubits to Alice. Alice selects an input z and performs a corresponding measurement with outcome a. Depending on the value of her outcome, the round counts either towards secret sharing or towards a re-initialisation of the experiment which in itself serves as a control parameter for the advantages of entanglement.

to Alice. Alice privately selects a binary input $z \in \{0,1\}$ and accordingly decodes the two incoming messages. The decoding yields one of three possible values $a \in \{0,1,\perp\}$. The values $a \in \{0,1\}$ are interpreted as Alice's secret bit, whereas the value $a = \perp$ is associated to rejecting and discarding the round of the secret sharing protocol (after which it can be re-initiated). Specifically, the conditions for successfully completing the task are as follows. When Alice selects input z, the binary value of $x_z \oplus y_z$ determines whether the round contributes to the secret sharing or is a "discarding round". If it is a discarding round ($x_z \oplus y_z = 0$), then the round is deemed successful if $a = \perp$. Otherwise, if it is a secret sharing round ($x_z \oplus y_z = 1$), then it is successful if Bob and Charlie can reconstruct Alice's output through the relation $a = x_{\bar{z}} \oplus y_{\bar{z}}$, where $\bar{z} = z \oplus 1$. Thus, by announcing z, Alice informs Bob and Charlie which of their bits hold the shared secret. The average success probabilities in the discarding rounds and the secret sharing rounds, respectively, becomes

$$\begin{aligned} \mathcal{S}_{\text{discard}} &= \frac{1}{16}\sum_{z}\sum_{\substack{x,y:\\ x_z\oplus y_z=0}} p(a=\perp|x,y,z), \\ \mathcal{S}_{\text{secret}} &= \frac{1}{16}\sum_{z}\sum_{\substack{x,y:\\ x_z\oplus y_z=1}} p(a=x_{\bar{z}}\oplus y_{\bar{z}}|x,y,z). \end{aligned} \tag{2}$$

Note that this task could be equally well formulated using only the secret sharing rounds, i.e., by removing the outcome $a = \perp$. However, including $\mathcal{S}_{\text{discard}}$ in the analysis turns out to allow advantages to be obtained from even more weakly entangled states, while still admitting a simple interpretation. One may think of $\mathcal{S}_{\text{discard}}$ as a control parameter which certifies the nonclassical nature of the secret sharing correlations. While we may consider the pair $(\mathcal{S}_{\text{discard}}, \mathcal{S}_{\text{secret}})$, it is both simpler and sufficient for our purposes to instead consider the single success metric obtained by averaging the two,

$$\mathcal{S} = \frac{1}{2}\left(\mathcal{S}_{\text{discard}} + \mathcal{S}_{\text{secret}}\right). \tag{3}$$

Naturally, in order to draw meaningful conclusions, the parties must have some physical limitations. On the one hand, we are interested in the situation in which Bob and Charlie share no prior entanglement and simply send messages encoded in qubit states β_x and γ_y, respectively, while Alice can decode using a general quantum measurement $\{M_{a|z}\}_a$. The observed correlations are then given by

$$p_{\text{qubit}}(a|x,y,z) = \text{tr}\left[(\beta_x \otimes \gamma_y) M_{a|z}\right], \tag{4}$$

where $\{M_{a|z}\}_a$ are positive operator-valued measures for each z. On the other hand, we also consider the situation illustrated in Fig. 1, where Bob and Charlie may additionally share a two-qubit entangled state ρ and then encode their qubit messages through local quantum channels Λ_x^B and Λ_y^C, respectively. In this entanglement assisted case, the correlations are given by

$$p_{\text{EAqubit}}(a|x,y,z) = \text{tr}\left[\left(\Lambda_x^B \otimes \Lambda_y^C(\rho)\right) M_{a|z}\right]. \tag{5}$$

We now show that there exists an entanglement-assisted quantum protocol that simultaneously achieves a perfect discarding rate and a perfect secret sharing rate, while requiring no more sophisticated measurements than those compatible with standard linear optics.

Ideal entanglement-assisted and unassisted protocols.— Consider a maximally entangled state $\rho = |\phi^+\rangle\langle\phi^+|$ and let Bob's and Charlie's local channels correspond to implementing the four unitaries $U_x^B = \sigma_X^{x_0}\sigma_Z^{x_1}$ and $U_y^C = \sigma_X^{y_0}\sigma_Z^{y_1}$ respectively, where σ_X and σ_Z are the Pauli bit-flip and phase-flip operators. This means that the two-qubit state arriving to Alice is one of the four Bell states. When $z = 0$, Alice performs a three-outcome measurement corresponding to a projection onto $\{\Psi^+, \Psi^-, \Phi^+ + \Phi^-\}$, i.e., she discriminates the states $\Psi^\pm$. When $z = 1$, she instead discriminates the states Φ^- and Ψ^- by projecting the two qubits onto $\{\Phi^-, \Psi^-, \Phi^+ + \Psi^+\}$. A direct calculation then shows that $\mathcal{S}_{\text{discard}} = \mathcal{S}_{\text{secret}} = 1$ and hence $\mathcal{S}_{\text{EAqubit}} = 1$. Importantly, the employed measurements may be seen as partial Bell state analysers and it is known that passive linear optics can discriminate no more than two of the four Bell states [31]. This is indeed the case in our quantum protocol.

In contrast, in the scenario when entanglement is absent, it is no longer possible to succeed deterministically. Indeed, we were able to determine the maximum value of $\mathcal{S}$ achievable with entanglement-unassisted qubits and general projective measurements for Alice. To this end, we used a straightforward modification of a hierarchy of semidefinite programs for bounding dimensionally-restricted quantum correlation [32]. In order to obtain sufficiently tight upper bounds on $\mathcal{S}$ by solving numerically the semidefinite programs, we needed to consider terms appears in the first three levels of this hierarchy (the full third level being too computationally difficult to implement) [33]. To render these intensive calculations more readily tractable on a standard desktop computer, we

employed recently developed symmetrisation techniques [34]. The symmetrisation is based on the observation that the objective function $\mathcal{S}$ remains invariant under i) simultaneous bit-flip of x_0 and y_0, ii) simultaneous bit-flips of x_1 and y_1 and iii) simultaneous swaps $x_0 \leftrightarrow x_1$ and $y_0 \leftrightarrow y_1$. Up to solver precision, we determine the upper bound $\mathcal{S}_{\text{qubit}} \leq \frac{5}{8}$. This bound in fact holds even if all three parties share some pre-agreed classical randomness.

Although the approach described provides only an upper bound on $\mathcal{S}_{\text{qubit}}$, we demonstrate its tightness by exhibiting a strategy—in fact, an entirely classical one—which saturates it, thereby showing that there exists no quantum-over-classical advantage without using entanglement. To this end, consider the strategy in which Bob and Charlie relay the bits x_0 and y_0, respectively, to Alice. Alice then outputs $a = \perp$ unless $z = 0$ and she receives $(0,1)$ or $(1,0)$, in which case she simply outputs $a = 0$. A direct calculation gives $\mathcal{S}_{\text{discard}} = \frac{1}{2}$ and $\mathcal{S}_{\text{discard}} = \frac{1}{8}$, giving an overall winning probability of $\mathcal{S}_{\text{classical}} = \frac{5}{8}$. We conclude that any value in the range $\frac{5}{8} < \mathcal{S} \leq 1$ implies an advantage over both the best classical and the best entanglement-unassisted quantum model, and hence is powered by the consumption of entanglement.

Advantage from unsteerable states.—If, in the above ideal entanglement-assisted protocol, we substitute the maximally entangled state for the isotropic state (1), we find that $\mathcal{S} = \frac{3+5v}{8}$ Thus, we observe an advantage ascribed to entanglement whenever $\mathcal{S} > \mathcal{S}_{\text{qubit}}$, which occurs whenever $v > \frac{2}{5}$. Consequently, when $v \in \left(\frac{2}{5}, \frac{1}{2}\right]$, the isotropic state is both unsteerable and a communication resource with the employed decoding resources.

Bell-local state and product measurements.—While the partial Bell state measurements used above are compatible with passive linear optics, they still require Alice to perform precise two-photon interferences. This can become costly to scale to many qubits. It motivates the question of whether the simplest conceivable joint measurements can also reveal entanglement-assisted advantages [21]. This entails separately measuring each of the two qubits and then post-processing the two separate outcomes into the final output a. As we now show, such simple measurements can nonetheless still lead to an advantage from a relatively weak form of entanglement, namely that which is too weak to violate any Bell inequality but still strong enough to manifest Einstein-Podolsky-Rosen steering.

To this end, consider once more the isotropic state (1) and the unitaries U_x^B and U_y^C for Bob and Charlie. Now, let Alice perform product measurements $\sigma_Z \otimes \sigma_Z$ for $z = 0$ and $\sigma_X \otimes \sigma_X$ for $z = 1$. The individual qubit measurements yield binary outcomes $b_B, b_C \in \{0,1\}$. Alice then decides her final outcome by a classical post-processing where she assigns $(b_B, b_C) \in \{(0,0),(1,1)\}$ to $a = \perp$ and $(b_B, b_C) \in \{(0,1),(1,0)\}$ to $a = 1$. Evaluating this strategy gives $\mathcal{S}_{\text{prod}} = \frac{3(1+v)}{8}$ which outperforms the unassisted qubit limit whenever $v > \frac{2}{3}$. Hence, when $v \in \left(\frac{2}{3}, 0.6875\right]$, the isotropic state is both Bell-local and a communication resource even when using only such minimal decoding resources.

Experimental realisation.—We report here on an experimental implementation of the entanglement-assisted communication advantage in stochastic secret sharing developed in this letter. We give a proof-of-principle demonstration of both the ideal quantum protocol using maximally entangled states encoded in the polarisation of photos, and an advantage from a weakly entangled, unsteerable, state.

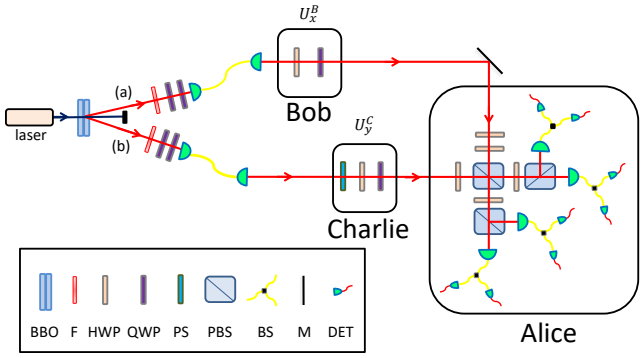

FIG. 2. Experimental setup. Entangled photon pairs in spatial modes (a) and (b) are generated through the SPDC process. Isotropic states are prepared by randomly transforming the maximally entangled $|\phi^+\rangle$ state into one of the other Bell states using quarter wave plates (QWP). The unitaries of Bob and Charlie are implemented using a combination of quarter wave plate (QWP), half wave plates (HWP) and phase shifters (PS). Alice's partial Bell state measurements are implemented using HWP, polarising beam splitters (PBS), beam splitters (BS) and then detected by single photon detectors (DET). See main text for further details.

To generate the entangled states, ultraviolet light centered at a wavelength of 390 nm is focused onto two 2 mm thick β barium borate (BBO) nonlinear crystals placed in an interferometric configuration to produce photon pairs emitted into two spatial modes through the second order degenerate type-I spontaneous parametric down-conversion process (SPDC). The spectral, and temporal distinguishability between the down-converted photons is carefully removed by passing through narrow-bandwidth interference filters and quartz wedges respectively (see Fig. 2).

To prepare the desired states for the secret sharing protocol, we first prepared the polarisation entangled pairs of photons in the state $|\phi^+\rangle = \frac{|HH\rangle+|VV\rangle}{\sqrt{2}}$, where H and V are, respectively, the horizontal and vertical photonic polarisation modes. By taking the standard encoding of $|0\rangle := |H\rangle$ and $|1\rangle := |V\rangle$, we recover the desired maximally entangled state. In order to prepare an isotropic state, ρ_v, $|\phi^+\rangle$ must be mixed with white noise. We achieve this by, with probability $1-v$, randomly transforming $|\phi^+\rangle$ into one of the four Bell states $|\phi^\pm\rangle, |\psi^\pm\rangle$. These transformations were experimentally realised by a motorised rotation of two quarter wave plates (QWP) placed in each of the modes (a) and (b) (see Fig. 2 and Supplemental Material for the QWP settings).

The polarisation measurements are performed using half wave plates (HWP) and polarising beam splitters (PBS), beam splitters (BS) placed at the two output modes of the PBS, and then by single photon detectors (actively quenched Si-avalanche photodiodes). The partial Bell analyser is implemented through two-photon interference, using PBS and

HWPs set at 22.5°. The two-photon Hong–Ou–Mandel dip visibility is $99\% \pm 4$, where the substantial statistical error is due to the low two-photon coincidence rate used in the experiment (one per second) and a measurement time of 2400 seconds per point (see Supplemental Material). To switch from a Bell measurement discriminating between $\{\Psi^+, \Psi^-, \Phi^+ + \Phi^-\}$ to $\{\Phi^-, \Psi^-, \Phi^+ + \Psi^+\}$, Alice uses three HWPs placed before the first PBS (see Supplemental Material the HWP settings). All single-detection events were registered using a VHDL-programmed multichannel coincidence logic unit, with a time coincidence window of 1.7 ns.

Bob's and Charlie's transformations U_x^B and U_y^C, respectively, are performed using two quarter wave plates (QWP), two half wave plates (HWP) and a phase shifter (PS) to change the relative phase between the two modes (a) and (b). Since they have a total of 16 settings but only four qualitatively different global operations on the states we consider, we have considered a simplified setting in which only the latter cases are realised (see Supplemental Material for details and HWP and PS settings).

To perform state tomography of isotropic states ρ_v for different v, we performed tomography of the four Bell states generated in the randomisation procedure. Measurements were made at a rate of one two-coincidence per second over 1400 seconds for each of the nine settings needed to perform the state tomography for each Bell state. These results were then recombined *a posteriori* at different ratios to establish the density matrices ρ_v. We considered the reconstructed states ρ_v for $v = 0.4$ to $v = 0.5$, with a step-size of 0.01, corresponding to the resourceful but unsteerable range. Naturally, the reconstructed density matrices are not exactly isotropic states. To ensure the unsteerability of the experimentally realised states, we used the linear programming method of Ref. [35] which allows one to obtain a certificate of unsteerability for an arbitrary two-qubit state. We chose to proceed during the experiment with $v = 0.47$, as this represented a good balance between being below the steering threshold of $v_{\text{unsteer}} = \frac{1}{2}$ while allowing for good enough statistics to show a significant quantum advantage. The fidelity of the reconstructed state with the target isotropic state for $v = 0.47$ is 0.9983 ± 0.0004. Detailed tomography results for the density matrices, the state fidelities, and the certificates of unsteerability are presented in the Supplemental Material.

The protocol was then carried out with the isotropic state at $v = 0.47$ with the noise added by randomly changing the Bell state between each two-photon coincidence while maintaining the necessary ratio between these states. To obtain at most one event per change of Bell state and thus ensure the randomness and therefore unpredictability of each event, we chose to work at a rate one two-photon detection coincidence per second. The effective measurement time per setting was 2.8 hours. We obtained a success probability of $\mathcal{S} = 0.655 \pm 0.003$ which significantly goes beyond the theoretical entanglement-unassisted limit of $\mathcal{S}_{\text{qubit}} \leq \frac{5}{8}$, hence showing an advantage from unsteerable states.

The same experiment was also performed for a maximally entangled state to realise the ideal protocol and show that Bob's and Charlie's unit rotations coupled with Alice's measurements give the expected results. This amounts to effectively setting $v = 1$ and thus no randomisation over Bell states was required. This allowed the experiment to be performed at an average rate of 800 two-photon detection coincidences per second and a measurement time per setting of 2 hours. The fidelity of the prepared state and the maximally entangled state $|\phi^+\rangle$ was measured to be 0.9947 ± 0.0009. We observed a success probability of $\mathcal{S} = 0.9748 \pm 0.0001$ in the secret sharing protocol, close to the ideal maximum value of $\mathcal{S} = 1$ and showing a large advantage due to entanglement.

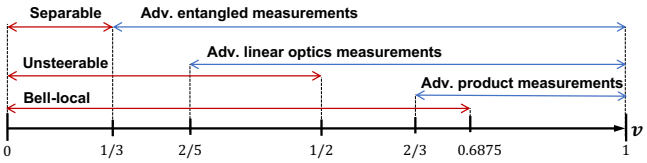

FIG. 3. Nonlocal properties (red) and quantum communication advantages (blue) of the two-qubit isotropic state (1). The ranges for separability and unsteerability are tight, whereas the limit for Bell-local models is a lower bound [14]. The range for quantum communication advantages from general entangled measurements follows from dense coding-like protocols [11, 12] and coincides with the range in which the state is entangled. The ranges shown for quantum communication advantages with passive linear optics measurements and product measurements are established in this work and are (potentially sub-optimal) upper bounds on the critical visibilities.

Discussion.— In this letter we demonstrated theoretically, and confirmed experimentally, that one can obtain quantum communication advantages using weakly entangled unsteerable states in a quantum secret sharing task. The advantage is rendered experimentally accessible by its achievability with passive linear optics, notably exploiting a Bell state analyser. Figure 3 summarises the ranges of noise v for which quantum communication advantages are achievable with two-qubit isotropic states and the relation to the nonlocal properties of the isotropic states. By focusing on easily realisable measurements, we showed that advantages can be obtained using partial Bell state measurements when $v \geq 2/5$ and hence for some unsteerable isotropic states, and even using the simplest product measurements when $v \geq 2/3$, a range that still includes some Bell-local states. It remains an open question whether advantages can be obtained in both these cases for smaller visibilities. In the former case, our bound is tight for the task at hand so an advantage would require a different task, whereas in the latter case it remains open whether $v = 2/3$ is tight for product measurements. Of particular relevance is to investigate whether product measurements also can generate advantages from highly noisy multi-qubit states, as this would pave the way for experiments that go beyond proof-of-principle demonstrations.

We finish by noting that, while we focused on the communication advantage itself, obtaining a sufficiently high success probability in the task can also be interpreted as a semi-device-independent certification of the entanglement in the shared resource state in the spirit of [11]. Moreover, if there is a strict separation between the critical visibilities for product

and more general measurements in this task, a sufficiently high success probability in the task would also certify the succesful implementation of an entangled measurement in a semi-device-independent manner.

ACKNOWLEDGMENTS

A.A.A. and A.T. thank Anthony Martin and Alek Lagarrigue for discussions on an early iteration of the task presented here. This work supported by the Swedish research council, the Wenner-Gren Foundation and by the Knut and Alice Wallenberg Foundation through the Wallenberg Center for Quantum Technology (WACQT).

[1] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Entanglement-assisted classical capacity of noisy quantum channels, Phys. Rev. Lett. **83**, 3081 (1999), arXiv:quant-ph/9904023.
[2] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Nonlocality and communication complexity, Rev. Mod. Phys. **82**, 665 (2010), arXiv:0907.3584 [quant-ph].
[3] R. Cleve and H. Buhrman, Substituting quantum entanglement for communication, Phys. Rev. A **56**, 1201 (1997), arXiv:quant-ph/9704026.
[4] Č. Brukner, M. Żukowski, J.-W. Pan, and A. Zeilinger, Bell's inequalities and quantum communication complexity, Phys. Rev. Lett. **92**, 127901 (2004), arXiv:quant-ph/0210114.
[5] T. S. Cubitt, D. Leung, W. Matthews, and A. Winter, Improving zero-error classical communication with entanglement, Phys. Rev. Lett. **104**, 230503 (2010), arXiv:arXiv:0911.5300 [quant-ph].
[6] N. Brunner and N. Linden, Connection between Bell nonlocality and Bayesian game theory, Nat Commun **4**, 2057 (2013), arXiv:1210.1173 [quant-ph].
[7] A. Tavakoli and M. Żukowski, Higher-dimensional communication complexity problems: Classical protocols versus quantum ones based on Bell's theorem or prepare-transmit-measure schemes, Phys. Rev. A **95**, 042305 (2017), arXiv:1611.00977 [quant-ph].
[8] A. Tavakoli, M. Żukowski, and Č. Brukner, Does violation of a Bell inequality always imply quantum advantage in a communication complexity problem?, Quantum **4**, 316 (2020), arXiv:1907.01322 [quant-ph].
[9] J. Pauwels, S. Pironio, E. Z. Cruzeiro, and A. Tavakoli, Adaptive advantage in entanglement-assisted communications, Phys. Rev. Lett. **129**, 120504 (2022), arXiv:2203.05372 [quant-ph].
[10] C. H. Bennett and S. J. Wiesner, Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, Phys. Rev. Lett. **69**, 2881 (1992).
[11] A. Tavakoli, A. A. Abbott, M.-O. Renou, N. Gisin, and N. Brunner, Semi-device-independent characterisation of multipartite entangled states and measurements, Phys. Rev. A **98**, 052333 (2018), arXiv:1805.00377 [quant-ph].
[12] G. Moreno, R. Nery, C. de Gois, R. Rabelo, and R. Chaves, Semi-device-independent certification of entanglement in superdense coding, Phys. Rev. A **103**, 022426 (2021), arXiv:2102.02709 [quant-ph].
[13] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox, Phys. Rev. Lett. **98**, 140402 (2007), arXiv:quant-ph/0612147.
[14] S. Designolle, G. Iommazzo, M. Besançon, S. Knebel, P. Gelß, and S. Pokutta, Improved local models and new Bell inequalities via Frank-Wolfe algorithms, arXiv:2302.04721 [quant-ph] (2023).
[15] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, Bell measurements for teleportation, Phys. Rev. A **59**, 3295 (1999), arXiv:quant-ph/9809063.
[16] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, Dense coding in experimental quantum communication, Phys. Rev. Lett. **76**, 4656 (1996).
[17] X. Li, Q. Pan, J. Jing, J. Zhang, C. Xie, and K. Peng, Quantum dense coding exploiting a bright Einstein-Podolsky-Rosen beam, Phys. Rev. Lett. **88**, 047904 (2002), arXiv:quant-ph/0107068.
[18] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, Beating the channel capacity limit for linear photonic superdense coding, Nature Phys. **4**, 282 (2008), arXiv:1009.5128 [quant-ph].
[19] B. P. Williams, R. J. Sadlier, and T. S. Humble, Superdense coding over optical fiber links with complete Bell-state measurements, Phys. Rev. Lett. **118**, 050501 (2017), arXiv:1609.00713 [quant-ph].
[20] X.-M. Hu, Y. Guo, B.-H. Liu, Y.-F. Huang, C.-F. Li, and G.-C. Guo, Beating the channel capacity limit for superdense coding with entangled ququarts, Science Advances **4**, eaat9304 (2018), arXiv:1807.10452 [quant-ph].
[21] A. Piveteau, J. Pauwels, E. Håkansson, S. Muhammad, M. Bourennane, and A. Tavakoli, Entanglement-assisted quantum communication with simple measurements, Nature Commun. **13**, 7878 (2022), arXiv:2205.09602 [quant-ph].
[22] G. R. Blakley, Safeguarding cryptographic keys, in *Proceedings of the 1979 AFIPS National Computer Conference* (AFIPS Press, Monval, NJ, USA, 1979) pp. 313–317.
[23] A. Shamir, How to share a secret, Commun. ACM **22**, 612 (1979).
[24] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999), arXiv:quant-ph/9806063.
[25] A. Karlsson, M. Koashi, and N. Imoto, Quantum entanglement for secret sharing and secret splitting, Phys. Rev. A **59**, 162 (1999).
[26] G.-P. Guo and G.-C. Guo, Quantum secret sharing without entanglement, Phys. Lett. A **310**, 247 (2003), arXiv:quant-ph/0212056.
[27] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane, Secret sharing with a single d-level quantum system, Phys. Rev. A **92**, 030302 (2015), arXiv:1501.05582 [quant-ph].
[28] V. Karimipour and M. Asoudeh, Quantum secret sharing and random hopping: Using single states instead of entanglement, Phys. Rev. A **92**, 030301 (2015), arXiv:1506.02966 [quant-ph].
[29] H. Weinfurter, Experimental Bell-state analysis, Europhys. Lett. **25**, 559 (1994).
[30] S. L. Braunstein and A. Mann, Measurement of the Bell operator and quantum teleportation, Phys. Rev. A **51**, R1727 (1995).
[31] J. Calsamiglia and N. Lütkenhaus, Maximum efficiency of a linear-optical Bell-state analyzer, Appl. Phys. B **72**, 67 (2001), arXiv:quant-ph/0007058.
[32] M. Navascués and T. Vértesi, Bounding the set of finite di-

mensional quantum correlations, Phys. Rev. Lett. **115**, 020501 (2015), arXiv:1412.0924 [quant-ph].
[33] Specifically, we used what would, in standard terminology, be called the "1+AB+AC+ABC" level, leading to a moment matrix of size 159.
[34] A. Tavakoli, D. Rosset, and M.-O. Renou, Enabling computation of correlation bounds for finite-dimensional quantum systems via symmetrization, Phys. Rev. Lett. **122**, 070501 (2019), arXiv:1808.02412 [quant-ph].
[35] H. C. Nguyen, H.-V. Nguyen, and O. Gühne, Geometry of Einstein-Podolsky-Rosen correlations, Phys. Rev. Lett. **122**, 240401 (2019), arXiv:1808.09349 [quant-ph].
[36] H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, Experimental characterization of unsharp qubit observables and sequential measurement incompatibility via quantum random access codes, Phys. Rev. Lett. **125**, 080403 (2020), arXiv:2001.04768 [quant-ph].
[37] C. K. Hong, Z. Y. Ou, and L. Mandel, Measurement of subpicosecond time intervals between two photons by interference, Phys. Rev. Lett. **59**, 2044 (1987).

SUPPLEMENTARY NOTE 1: UNSTEERABILITY OF EXPERIMENTAL ISOTROPIC STATES

Recall that the isotropic state ρ_v is defined as

$$\rho_v = v\Phi^+ + \frac{(1-v)}{4}\mathbb{1}, \tag{6}$$

where $\Phi^+ = |\phi^+\rangle\langle\phi^+|$. It is well known that ρ_v is unsteerable for $v \leq \frac{1}{2}$ and entangled for $v > \frac{1}{3}$ [13]. The states prepared experimentally, however, are necessarily not exactly the isotropic states. To exhibit an advantage in the stochastic secret sharing task from entangled but unsteerable states, it is necessary to verify that the experimentally prepared states, as reconstructed via state tomography, is indeed unsteerable.

While two-qubit entanglement can easily be verified by calculating its negativity, verifying unsteerability is more challenging. Here, we use a recently developed method [35] that allows one to obtain certificates of unsteerability via linear programming.

In particular, the approach of Ref. [35] computes, for an arbitrary two-qubit state and a given direction of steering (say, from Bob to Charlie or Charlie to Bob), both upper and lower bounds, $r_{\text{crit}}^{\text{upper}}$ and $r_{\text{crit}}^{\text{lower}}$, respectively, on a "critical radius" r_{crit} satisfying $r_{\text{crit}}^{\text{lower}} < r_{\text{crit}} < r_{\text{crit}}^{\text{upper}}$. They show that a two-qubit state ρ is steerable (in a given direction) if and only if $r_{\text{crit}} < 1$. Thus, by finding $r_{\text{crit}}^{\text{lower}} \geq 1$ for both possible directions of steering, we are guaranteed a state is unsteerable.

The precision of the upper and lower bounds can be increased at the cost of computational time and memory. On a standard desktop computer, using the CPLEX packaged provided by Ref. [35], we were typically able to obtain, for the experimental states approximating ρ_v, a gap $r_{\text{crit}}^{\text{upper}} - r_{\text{crit}}^{\text{lower}} \approx 0.02$ with a few minutes of computation. This can be reduced by an order of magnitude by allocating somewhat more computational time.

For the tomographically reconstructed density matrices $\tilde{\rho}_v$, for $v = 0.4$ to $v = 0.5$ (with a step size of 0.1), we computed $r_{\text{crit}}^{\text{lower}}$ and found the states to be unsteerable for all values except $v = 0.5$. However, to ensure that this result is robust (recalling, of course, the experimental error in the description of $\tilde{\rho}_v$) and ensure we choose a state providing a large enough quantum advantage (which diminishes as v decreases), we chose to perform the experiment with $v = 0.47$.

For this state, we performed a finer analysis of the unsteerability of $\tilde{\rho}_{0.47}$, taking into account the errors in each term of the density matrix. Adopting a conservative approach, we applied the worst case errors to all subsets of density matrix elements (up to Hermiticity) before calculating $r_{\text{crit}}^{\text{lower}}$ for the (renormalised) perturbed density matrix. We found that, in all cases, $r_{\text{crit}}^{\text{lower}} \gtrsim 1.031$ (while for the reconstructed state $\tilde{\rho}_{0.47}$ we found $r_{\text{crit}}^{\text{lower}} \approx 1.055$), showing that the prepared state is clearly unsteerable, even when errors are taken into account.

SUPPLEMENTARY NOTE 2: STATE PREPARATION, TRANSFORMATIONS AND MEASUREMENTS

1. State implementation

The setup used generates an entangled Φ^+ state with a visibility close to 100%. In order to generate an isotropic state ρ_v (6), this state needs to be mixed with probability $(1-v)$ with the maximally mixed state $\frac{\mathbb{1}}{4}$. We implement the maximally mixed state by randomly switching between the four Bell states, $\Phi^{\pm}, \Psi^{\pm}$, exploiting the fact that $\frac{\mathbb{1}}{4} = \frac{1}{4}(\Phi^+ + \Phi^- + \Psi^+ + \Psi^-)$. We can thereby generate ρ_v for any v by choosing correctly the weights with which we randomly change Φ^+ to one of the other Bell states.

The switching between these different states is done with the help of four quarter-wave plates and a phase plate (which is not necessary in theory, but which we use to compensate for the phase that rotating QWPs can bring); see Fig. 2 of the main text. These plates are distributed so that two are placed on the path going to Bob (mode (a)), $\frac{\lambda_{(a)}}{4}$ and $\frac{\lambda'_{(a)}}{4}$, and two on the path going to Charlie (mode (b)), $\frac{\lambda_{(b)}}{4}$ and $\frac{\lambda'_{(b)}}{4}$. These plates are motorised and switched randomly (with the desired probability) from one state to another every second. The number of coincidences being less than one per second, the result is to switch from one Bell

state to another randomly and independently between each pair of successive coincidences. The values of the angles allowing one to pass from one state to another are given in Table I.

TABLE I. Quarter wave plate rotation angles (in °) for the the four plates used to prepare the different Bell states.

State	$\frac{\lambda_{(a)}}{4}$	$\frac{\lambda'_{(a)}}{4}$	$\frac{\lambda_{(b)}}{4}$	$\frac{\lambda'_{(b)}}{4}$
Φ^+	0	90	0	90
Φ^-	0	90	0	0
Ψ^+	0	90	45	45
Ψ^-	0	0	45	45

2. Bob's and Charlie's rotations

As described in the main text, on inputs $x = (x_0, x_1) \in \{0,1\}^2$ and $y = (y_0, y_1) \in \{0,1\}^2$, Bob and Charlie apply the unitaries $U_x^B = \sigma_X^{y_0}\sigma_Z^{y_1}$ and $U_y^C = \sigma_X^{y_0}\sigma_Z^{y_1}$, respectively. Table II summarises explicitly the operations that Bob and Charlie must perform in inputs x and y, as well as the Bell state expected to be received by Alice in the ideal case (assuming Bob and Charlie share a Φ^+ state). The settings to be applied to achieve each of the four different possible rotations are given in Table III

TABLE II. Transformation table: the operations $\sigma_X^{x_0}\sigma_Z^{x_1}$ and $\sigma_X^{y_0}\sigma_Z^{y_1}$ that need to be performed by Bob and Charlie, respectively. The expected Bell state that Alice will receive in the ideal case that Bob and Charlie share a noiseless maximally entangled state is shown in the final column.

x_0	x_1	y_0	y_1	Bob	Charlie	Alice's expected state
0	0	0	0	$\mathbb{1}$	$\mathbb{1}$	Φ^+
0	0	1	0	$\mathbb{1}$	σ_X	Ψ^+
0	0	1	1	$\mathbb{1}$	$-i\sigma_Y$	Ψ^-
0	0	0	1	$\mathbb{1}$	σ_Z	Ψ^-
1	0	0	0	σ_X	$\mathbb{1}$	Ψ^-
1	0	1	0	σ_X	σ_X	Φ^+
1	0	1	1	σ_X	$-i\sigma_Y$	Φ^-
1	0	0	1	σ_X	σ_Z	Ψ^-
1	1	0	0	$-i\sigma_Y$	$\mathbb{1}$	Ψ^-
1	1	1	0	$-i\sigma_Y$	σ_X	Ψ^+
1	1	1	1	$-i\sigma_Y$	$-i\sigma_Y$	Φ^+
1	1	0	1	$-i\sigma_Y$	σ_Z	Ψ_+
0	1	0	0	σ_Z	$\mathbb{1}$	Φ^-
0	1	1	0	σ_Z	σ_X	Ψ_-
0	1	1	1	σ_Z	$-i\sigma_Y$	Ψ_+
0	1	0	1	σ_Z	σ_Z	Φ_+

TABLE III. Rotation angles (in °) for the unitaries for Bob's and Charlie's operations.

Unitary	Phase plate	HWP	QWP
$\mathbb{1}$	90	0	0
σ_X	-90	45	90
$-i\sigma_Y$	90	45	90
σ_Z	-90	0	0

Experimentally, the phase of a single photon cannot be determined, and only the relative phase between two photons can be measured. Moreover, as a QWP at 90° is equivalent to a QWP at 0° plus a phase, we have chosen to keep them at 0° in order to limit the number of rotations and therefore the systematic error and to compensate with the phase plate. In addition, to limit motor problems due to fast setting changes (once per second), we decided to limit rotations as much as possible and therefore to apply the equivalent global operations. The rotations actually performed by the two HWPs, the two QWPs and a phase shifter, as described in the main text (see Fig. 2 therein), are given in Table IV.

TABLE IV. Experimental rotations: For each initial Bell state that was prepared, the table gives the actual equivalent rotation that was (locally) performed so as to implement the global operations equivalent to the transformations specified in Table II.

State prepared	Equivalent rotation	$\frac{\lambda_B}{2}$	$\frac{\lambda_B}{4}$	$\frac{\lambda_C}{2}$	$\frac{\lambda_C}{4}$	Phase
Φ^+	$\mathbb{1}$	0	0	0	0	+
Φ^+	σ_Z	0	0	0	0	−
Φ^+	σ_X	0	0	45	0	+
Φ^+	$-i\sigma_Y$	0	0	45	0	−
Φ^-	$\mathbb{1}$	0	0	0	0	−
Φ^-	σ_Z	0	0	0	0	+
Φ^-	σ_X	0	0	45	0	−
Φ^-	$-i\sigma_Y$	0	0	45	0	+
Ψ^+	$\mathbb{1}$	0	0	0	0	+
Ψ^+	σ_Z	0	0	0	0	−
Ψ^+	σ_X	0	0	45	0	+
Ψ^+	$-i\sigma_Y$	0	0	45	0	−
Ψ^-	$\mathbb{1}$	0	0	0	0	−
Ψ^-	σ_Z	0	0	0	0	+
Ψ^-	σ_X	0	0	45	0	−
Ψ^-	$-i\sigma_Y$	0	0	45	0	+

3. Alice's measurements

Depending of her setting $z \in \{0, 1\}$, Alice performs one of the three-outcome partial Bell measurement $\{\Psi^+, \Psi^-, \Phi^+ + \Phi^-\}$ or $\{\Phi^-, \Psi^-, \Phi^+ + \Psi^+\}$ and obtains an outcome $c \in \{0, 1, \perp\}$. To make these measurements, she uses three HWPs $\frac{\lambda_{A1}}{2}$, $\frac{\lambda_{A2}}{2}$ and $\frac{\lambda_{A3}}{2}$, with the first two ($A1$ and $A2$) placed before one of the input ports of the PBS, and last one ($A3$) placed before the other input port (see Fig. 2 of the main text). The values of the angles of these HWPs are given in Table V.

TABLE V. Rotation angles for the HWPs used to implement Alice's partial Bell state measurements, for $z = 0$ and $z = 1$.

z	$\frac{\lambda_{A1}}{2}$	$\frac{\lambda_{A2}}{2}$	$\frac{\lambda_{A1}}{2}$
0	0	45	0
1	0	22.5	22.5

SUPPLEMENTARY NOTE 4: EXPERIMENTAL RESULTS AND ERROR ESTIMATION FOR THE ISOTROPIC STATES ρ_v

Tables VI and VII list our experimental results alongside the theoretical success probabilities $\mathcal{S}$ with the related errors for each combination of inputs (x, y, z).

TABLE VI. Theoretical and experimental success probabilities for the maximally entangled state Φ^+, conditioned on z and then averaged to give the overall success probability $\mathcal{S}$.

Parameter	Theoretical	Experimental	error
$S_{\text{discard}}^{[z=0]}$	1	0.9900	0.0002
$S_{\text{secret}}^{[z=0]}$	1	0.9811	0.0003
$S_{\text{discard}}^{[z=1]}$	1	0.9795	0.0002
$S_{\text{secret}}^{[z=1]}$	1	0.9485	0.0003
$\mathcal{S}$	1	0.9748	0.0001

To calculate these errors, following [36] we consider errors originating from the measurement side only. To reduce experimental errors in the measurements, we used computer controlled high precision motorised rotation stages, for Bob, Charlie and the

TABLE VII. Theoretical and experimental success probabilities for the isotropic state ρ_v with $v = 0.47$, conditioned on z and then averaged to give the overall success probability $\mathcal{S}$.

Parameter	Theoretical	Experimental	error
$S_{\text{discard}}^{[z=0]}$	0.735	0.743	0.005
$S_{\text{secret}}^{[z=0]}$	0.6025	0.591	0.006
$S_{\text{discard}}^{[z=1]}$	0.735	0.712	0.005
$S_{\text{secret}}^{[z=1]}$	0.6025	0.576	0.006
$\mathcal{S}$	0.66875	0.655	0.003

generation of Werner states, to set the orientation of the wave-plates with a repeatably high precision of $0.02°$. The use of different settings (x, y) induces a systematic error, which we estimate using Monte Carlo simulation. We assume that the wave plates' setting errors are normally distributed with a standard deviation of $0.02°$. Alice's wave plates are not motorised. In order to reduce systematic errors in the angle settings, all settings for $z = 0$ are measured, then all settings for $z = 1$, so the results are initially presented separately for each case. We estimate the accuracy of the angles of these WPs to be half a degree. This, together with the Poissonian error in photon counting statistics, comprises the final error reported here. Due to inefficiency in the single photon detectors, the photons are detected randomly and their counting is Poissonian. To decrease Poissonian counting error, we have chosen for $v = 1$ a measurement time of two hours for every setting and collected approximately 93 million events. To guarantee that both parties receive single qubits, we worked at a low rate (≈ 800 coincidence per sec) to suppress higher order coincidences to almost 0.9 per sec. For $v = 0.47$, we have collected around one hundred thousand two-photon coincidences and the low rate renders the higher order coincidences completely negligible.

SUPPLEMENTARY NOTE 6: TWO-FOLD HONG-OU-MANDEL DIP VISIBILITY

Bell state measurements are implemented through two-photon interference, using PBS and HWP plates set at 22.5°. The photons are detected by Si avalanche photodiodes and the coincidences are registered with an eight channel multifold coincidence counting unit. This Bell analyser consists of coherent interference at a polarising beam splitter (PBS). To achieve the necessary indistinguishability of the photons, due to their arrival times, we adjusted the path length of one of the photons using a delay line [37]. In Figure 4, the coincidences between the detectors versus the delay path length is shown. The zero delay corresponds to a maximal overlap (maximum indistinguishability). The interfering photons bunch (i.e., they both exit in the same output arm of the PBS) causing the coincidences to vanish. The measured visibility of the two-fold Hong-Ou-Mandel dip is $99\% \pm 4$, with a coincidence rate outside the dip around 0.9224 coincidences per second, identical to the rate at which we performed the experiment for $v = 0.47$.

SUPPLEMENTARY NOTE 7: DENSITY MATRIX TOMOGRAPHY

To ensure that the prepared state is the desired one, a tomography measurement is performed for a perfect Φ^+ state and for isotropic states ρ_v with a visibility between $v = 0.4$ and $v = 0.5$. The reconstructed density matrices obtained for the cases of $v = 1$ (i.e., the ideal case of $\rho_1 = \Phi^+$) and $v = 0.47$, which are the two states for which the experimental demonstration of the protocol was carried out, are presented in Figures 5 and 6, respectively.

The fidelity of each state obtained during the tomography with the ideal isotropic state ρ_v was found to be between 0.9947 and 0.9983. Table VIII gives the fidelity for each of these states.

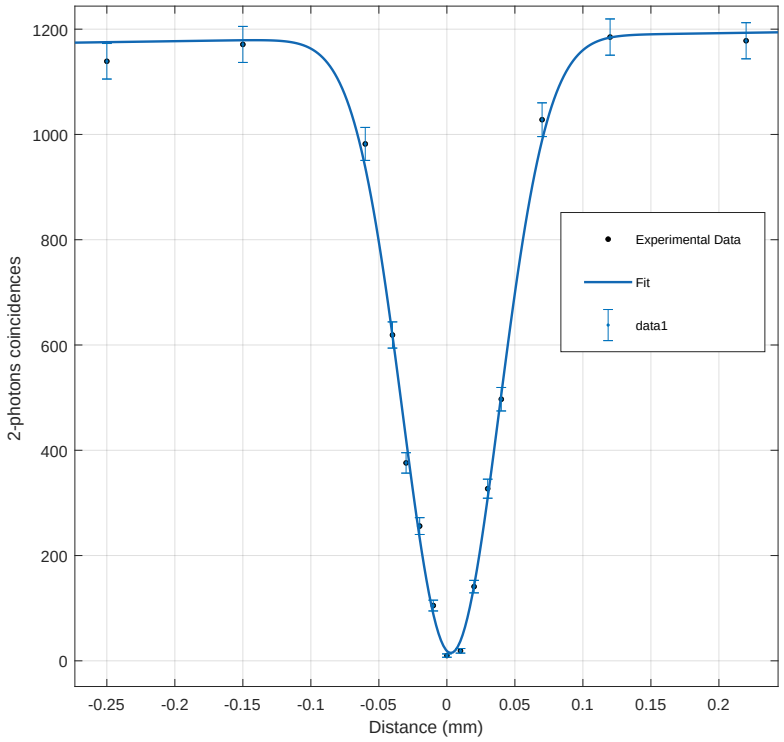

FIG. 4. Two-fold Hong-Ou-Mandel dip. The plot displays the two-fold photon counting coincidences versus the delay (the path difference between the two arms). The error bars indicate the Poissonian photon counting error statistics. The data is fitted with a Gaussian curve.

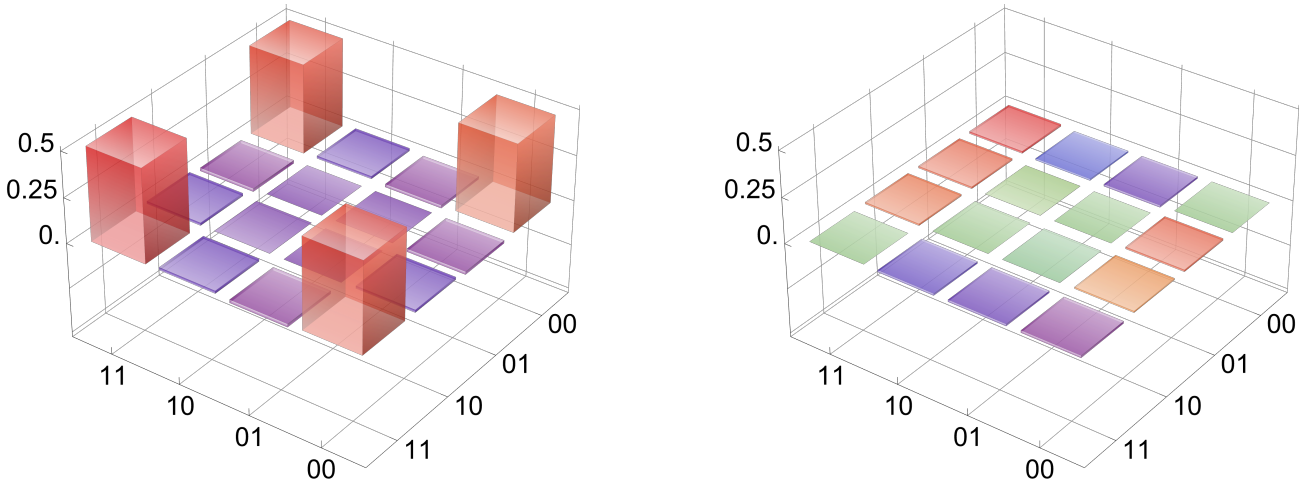

FIG. 5. State tomography of ρ_v for $v = 1$.

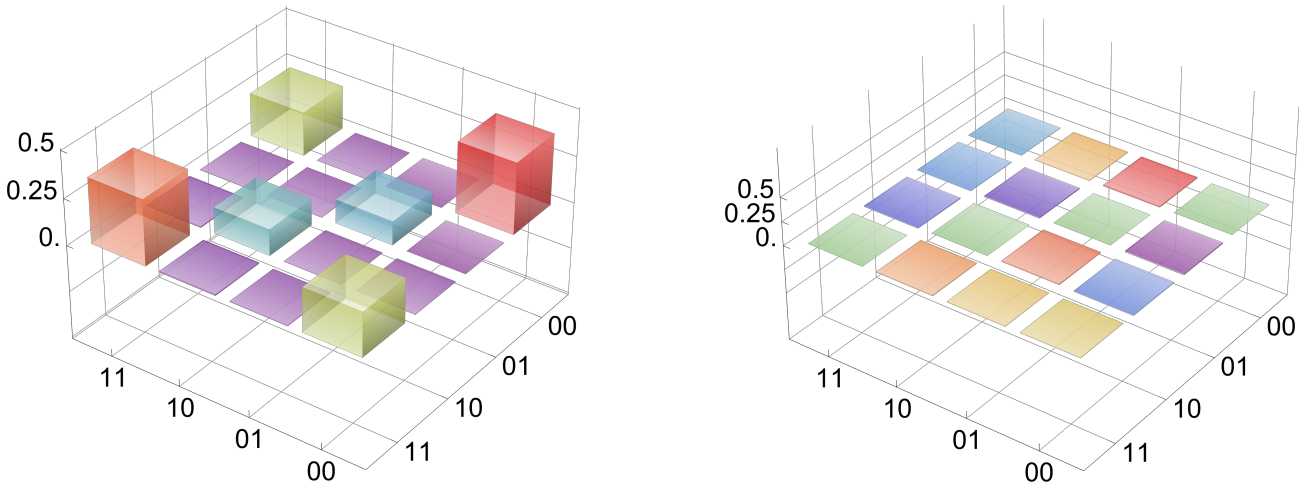

FIG. 6. State tomography of ρ_v for $v = 0.47$.

TABLE VIII. Fidelity of each measured state with the ideal isotropic state ρ_v.

Visibility v	Fidelity with ρ_v	error
0.4	0.9982	0.0004
0.41	0.9982	0.0004
0.42	0.9983	0.0004
0.43	0.9983	0.0004
0.44	0.9983	0.0004
0.45	0.9983	0.0004
0.46	0.9983	0.0004
0.47	0.9983	0.0004
0.48	0.9983	0.0004
0.49	0.9983	0.0004
0.50	0.9983	0.0004
1.00	0.9947	0.0009