24th IMEKO TC4 International Symposium
22nd International Workshop on ADC and DAC Modelling and Testing
IMEKO TC-4 2020
Palermo, Italy, September 14-16, 2020

Weak Measurements for Reutilizing Entanglement

Giulio Foletto[1], Luca Calderaro[1], Armin Tavakoli[2], Matteo Schiavon[1], Francesco Picciariello[1], Adán Cabello[3,4], Paolo Villoresi[1,5], Giuseppe Vallone[1,6]

[1]*Dipartimento di Ingegneria dell'Informazione, Università di Padova, IT-35131 Padova, Italy.*
[2]*Département de Physique Appliquée, Université de Genève, CH-1211 Genève, Switzerland*
[3]*Departamento de Física Aplicada II, Universidad de Sevilla, E-41012 Sevilla, Spain*
[4]*Instituto Carlos I de Física Teórica y Computacional, Universidad de Sevilla, E-41012 Sevilla, Spain*
[5]*Istituto di Fotonica e Nanotecnologie, CNR, IT-35131 Padova, Italy*
[6]*Dipartimento di Fisica e Astronomia, Università di Padova, IT-35131 Padova, Italy*

***Abstract* – Weak measurements are a relevant tool for quantum information because they allow tuning the disturbance on the observed state and the amount of information extracted from it. They can be used to harness repeatedly a quantum resource from the same state, thus boosting the performance of many protocols. We verified experimentally that sequences of weak measurements can generate correlations strong enough to violate the CHSH inequality multiple times, and yet can leave the state entangled enough for the next CHSH test. This means that entanglement can be certified and utilized more times, which is important for fundamental tests of quantum theory and above all for device-independent quantum information.**

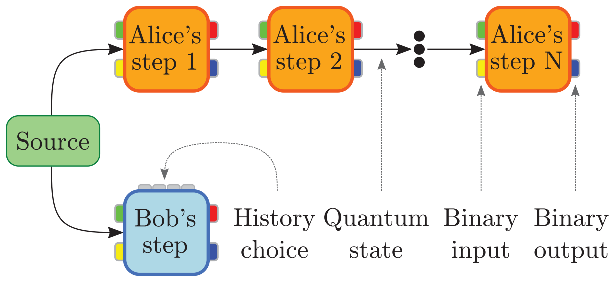

Fig. 1. Visualization of the protocol.

I. INTRODUCTION

The quantum weak measurements, introduced by Aharonov, Albert, Vaidman in 1988 [1], are an important class of generalized measurements that have the property of not perturbing a state as much as projections. They do so by weakly coupling the system they observe to a measuring device. Despite their worse precision, they are at the heart of protocols for the amplification of feeble signals [2, 3, 4], the investigation of quantum paradoxes [5, 6], the measurement of incompatible observables [7, 8], and the tomography of quantum states [9, 10]. Recently, they have become relevant in the field of quantum information because they allow careful manipulation of the states and precise tuning of the amount of information extracted from them. This opens the way for a broad set of protocols [11, 12, 13] that aim to use the quantum features of individual states more than once, overcoming the limits of projections that, instead, inevitably ruin these features.

Entanglement is one of these important features and is at the center of both foundational and applied aspects of quantum theory [14]. It is used for cryptography [15], metrology [16], and in general for device-independent quantum information [17]. Interestingly, it is possible to certify the presence of entanglement without any a priori assumption on the state or on the measurements being performed on it: this happens when outcome statistics violate a Bell inequality [18]. This result is naturally important when the devices preparing the states or performing the measurements cannot be trusted, for example because they could be controlled by an adversary, a situation common in quantum randomness extraction [19] or quantum key distribution [20]. However, a violation of a Bell inequality attained via projections typically destroys entanglement. Instead, weak measurements allow to repeat this step of certification multiple times, thus harnessing the resource of entanglement repeatedly from the same quantum state.

We experimentally verify [21] the possibility of sequentially violating three times the CHSH inequality [22]. At each step, the measurements are strong enough to violate the inequality and yet weak enough so that entanglement is not destroyed and can be certified again. Although we stop at the third step, the protocol we use could in principle continue for an unlimited sequence of measurements [23].

II. PROTOCOL

We first summarize the theoretical protocol aimed at the sequential certification of entanglement which was introduced in Ref. [23] and that is depicted in Fig. 1. Two parties, Alice and Bob, each hold a qubit in a maximally entangled state

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) , \tag{1}$$

where $|0\rangle$ and $|1\rangle$ are the eigenstates of the Pauli operator σ_Z. They want to exploit this entanglement for a quantum information task, and they must certify its presence by observing a violation of the CHSH inequality. However, they want to do this repeatedly on every copy of the system they hold. Alice randomly chooses one of two binary observables A_0 and A_1:

$$A_m(\mu_1) = K^\dagger_{+1|m}(\mu_1)K_{+1|m}(\mu_1) - K^\dagger_{-1|m}(\mu_1)K_{-1|m}(\mu_1) , \tag{2}$$

in which $m \in \{0, 1\}$ and the Kraus operators $K_{\pm1|m}$ are expressed as:

$$K_{\pm1|m}(\mu_1) = \cos(\mu_1)\Pi^{\pm}_m + \sin(\mu_1)\Pi^{\mp}_m , \tag{3}$$

Π^+_0 and Π^-_0 (Π^+_1 and Π^-_1) are the projectors onto the positive and negative eigenvectors of σ_Z (σ_X). This means that Alice is weakly measuring σ_Z or σ_X, indeed $A_0(\mu_1) = \cos(2\mu_1)\sigma_Z$ and $A_1(\mu_1) = \cos(2\mu_1)\sigma_X$. Parameter $\mu_1 \in [0, \pi/4]$ labels the strength of the measurement, with the two extrema 0 and $\pi/4$ corresponding to a projective and a non-interactive measurement respectively. Any intermediate value corresponds to a weak measurement.

At this point, the state has the form

$$|\psi_2\rangle = U_{A,2} \otimes U_{B,2}(\cos(\eta_2)|00\rangle + \sin(\eta_2)|11\rangle) , \tag{4}$$

where $U_{A,2}$ and $U_{B,2}$ are unitary transformations determined by Alice's choice of measurement and observed outcome and η_2 quantifies the entanglement remaining in the state (the exact details of all these parameters are in [21]). Because she knows the outcome of the first measurement, Alice can apply $U^\dagger_{A,2}$.

After this, she can simply repeat the above operations, with another random choice between A_0 and A_1, a possibly different strength value, and the application of another unitary operation. In this way, she performs a sequence of measurements.

At any (randomly chosen) step of the sequence, Bob can decide to measure his subsystem with the purpose of certifying the presence of entanglement in the pair. He selects his bases depending on the history of measurements and outcomes of Alice previous to the chosen step, he applies $\prod_{i=1}^k U^\dagger_{B,i}$ and then measures either of the two observables

$$B_m = (-1)^m \cos(\theta_k)\sigma_X + \sin(\theta_k)\sigma_Z , \tag{5}$$

where $m \in \{0, 1\}$ and $\theta_k = \text{arccot}(\sin(2\eta_k))$. It is important to understand that Bob requires the history of Alice's previous measurements and outcomes, but of course he does not need information on the current step: in a CHSH test, Alice and Bob's measurements are independent. This also means that the parties must perform separate CHSH tests on each of Alice's possible histories, whose number grows exponentially with base four, because at every step Alice chooses between two observables and each has one of two outcomes. As a consequence of this, the number of systems that contributes to each test decreases exponentially with the number of steps, which poses a practical limitation to the length of the sequence, which can only be unlimited if the number of available copies of the system also is.

Alice must not know a priori when Bob is going to act, otherwise she could rig the certification. Hence, either she always gives Bob her history of previous choices and outcomes before the beginning of a new step, or she communicates nothing and Bob takes a guess. In this second option, after the experiment, when the two exchange their data, only the cases when Bob's guess was right are postselected and used for the certification. From the correlations between Alice and Bob's outcomes, the CHSH quantity can be calculated:

$$S = \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle , \tag{6}$$

and finding $S > 2$ certifies the presence of entanglement at the input state of each step.

III. EXPERIMENT

We now move to our proof-of-concept experiment, which aims at verifying that the weak measurements required by the protocol are feasible and can indeed generate correlations strong enough to violate the CHSH inequality repeatedly and without destroying the entanglement.

We generate polarization-entangled photon pairs at 808 nm using a custom-built source based on a PPKTP crystal. Their polarization is manipulated with waveplates to produce the bipartite state $|\psi_1\rangle$ of Eq. (1), where $|0\rangle$ and $|1\rangle$ label the horizontal and vertical polarizations respectively. The two photons are sent to two setups which we refer to as Alice and Bob, shown in Fig. 2.

Alice performs the weak measurements with a Mach-Zehnder interferometer (MZI). A polarizing beam displacer (PBD, Thorlabs BD40) splits the two polarization components $|0\rangle$ and $|1\rangle$ in two separate and parallel paths. After two half-wave plates (HWPs) placed one per path, a third HWP that spans across both sets the strength of the measurement through the angle of its fast axis $\theta_1 = \pi/8 - \mu_1/2$, where we chose $\mu_1 \approx 0.34$ rad. Another PBD closes the interferometer but only one of its exits continues to the rest of the setup. A photon takes this exit with the probability of obtaining outcome $+1$ in the measurement of A_0 and its polarization state corresponds to the initial state transformed by $K_{+1|0}$. In other words, observing a photon at that exit means that Alice has measured A_0 and has obtained outcome $+1$. HWPs before and after the MZI can change $K_{+1|0}$ into any of $\{K_{-1|0}, K_{+1|1}, K_{-1|1}\}$, thus allowing Alice to perform both her measurements and to observe any outcome.

Alice uses HWPs to apply $U_{A,2}^{\dagger}$ and then performs the second measurement of the sequence by repeating the operations described above with another, identical, MZI, with strength parameter $\mu_2 \approx 0.19\,\mathrm{rad}$ in our experiment. For practical reasons, we stop the protocol at most at the third step, which is why the last measurement is projective and is implemented by a linear polarizer (LP) preceded by a HWP that sets measurement and outcome. The photons finally reach a single photon avalanche diode (SPAD).

Bob, who also requires only projective measurements, uses a setup identical to the third step of Alice and a SPAD. A coincident detection in the two SPADs carries the information of which exits have been taken by the photons and therefore corresponds to the specific sequence of measurement choices and outcomes selected by Alice in her three steps and by Bob in his one. By rotating waveplates we iterate over all combinations of measurement and outcomes and we record the number of coincident detections in a fixed exposure time (20 s). From these, we find the correlations between Alice and Bob's outcomes and the CHSH quantity S.

This implementation is simplified with respect to the theoretical protocol described above and introduces some loopholes. First, Alice and Bob should be able to observe both measurement outcomes for each photon, whereas in our setup only one outcome is available at any given time and we observe only the frequency of its occurrence. Moreover, the choice of measurement bases should be random and not predetermined, as this could give Alice and Bob the possibility to violate the CHSH inequality with classical means. Finally, Alice should either give her previous history of measurements and outcomes to Bob before each step, or he should take a guess. Neither of these options happens in our experiment, where all choices are predetermined.

To close these loopholes in a photonic system, one would probably require an optical setup that separates outcomes in different paths, and an exponentially growing number of detectors. However, our single-path setup is sufficient for this proof-of-concept experiment, which does not aim at excluding local-hidden-variable models with a loophole-free Bell test, but at verifying the feasibility of the measurements needed for the sequential Bell violation. Indeed, it can show that weak measurements can generate correlations that violate the CHSH inequality and at the same time can maintain enough entanglement for subsequent violations.

IV. RESULTS

We observed violations of the CHSH inequality backed by several standard deviations of statistical significance. However, at the third step we could do so only for four of the 16 possible input states (each corresponding to a combination of measurement and outcomes at Alice's previous two steps). These states have the greater amount of remaining entanglement, whereas in the other 12 cases it is so small that we had to use a different measurement strategy. Bob applies $\prod_{i=1}^{k} U_{B,i}^{\dagger}$ and then the two parties measure the entanglement witness $W = \mathbb{1}\otimes\mathbb{1} - \sigma_Z\otimes\sigma_Z - \sigma_X\otimes\sigma_X$ [24] which has negative mean value only for entangled states. This method provides a weaker certification of entanglement, but is less affected by experimental inaccuracies, and indeed we observed $\langle W \rangle < 0$ in all 12 cases. Table 1 contains all our results.

We attribute our difficulty in violating the CHSH inequality to systematic alignment errors in our setup. In particular, the phase between the arms of the MZIs must be accurately tuned, and if the plates are not flat enough, their rotation might deviate the photons, changing this phase or moving them out of the detectors' entrance, thus invalidating the polarization measurement.

Statistical uncertainties are mainly affected by the Poissonian error on photon counts, as the automated rotations of the waveplates we use are repeatable enough that their contribution is negligible. The number of photon pairs that contribute to our measurements is approximately 3×10^4, limited by the production rate of the source and the optical losses in the setup, dominated by the fiber couplings. When the detections are used to certify entanglement at the second or third step, their useful number is less than that, because only photons that have followed a particular history of outcomes at the previous steps can be used for each correlation. This, together with the alignment difficulties, is the reason why we stopped the protocol at three steps. Achieving statistically significant violations at a fourth step would have been prohibitive.

V. CONCLUSION

This experiment proves that weak measurements can certify entanglement without destroying it, allowing this resource to be reutilized more times. This can boost the performance of device-independent quantum information protocols, for instance for randomness extraction. A weak point of this scheme is robustness to imperfections, which, although non-zero, seems to be small. Entanglement is still a fragile resource, and must be manipulated carefully, even with weak measurements that are in principle capable of not breaking it. It would be interesting to run similar tests with other physical systems that allow longer and more accurate sequences of measurements and possibly close the loopholes that affect our setup, without the need for an exponentially growing number of components.

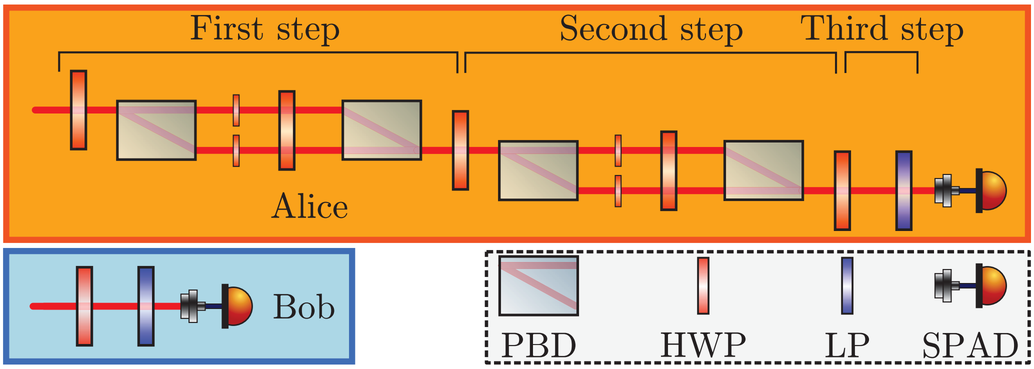

Fig. 2. Scheme of the setups that perform the measurements.

Table 1. Observed values of the CHSH quantity S and entanglement witness $\langle W \rangle$. The second column reports the history of measurements and outcomes that precede the one that yields the result on Alice's side. The notation is: outcome | measurement choice at step 1; outcome | measurement choice at step 2. The standard deviations in the last two columns are derived from poissonian error on the counts and error propagation.

Step	Alice's history	S	$\langle W \rangle$
1	/	2.15 ± 0.01	/
2	$+1\|0$	2.13 ± 0.01	/
2	$-1\|0$	2.07 ± 0.01	/
2	$+1\|1$	2.12 ± 0.01	/
2	$-1\|1$	2.09 ± 0.01	/
3	$+1\|0; +1\|0$	/	-0.12 ± 0.01
3	$+1\|0; -1\|0$	2.48 ± 0.03	-0.75 ± 0.01
3	$+1\|0; +1\|1$	/	-0.17 ± 0.01
3	$+1\|0; -1\|1$	/	-0.20 ± 0.01
3	$-1\|0; +1\|0$	/	-0.07 ± 0.01
3	$-1\|0; -1\|0$	2.53 ± 0.03	-0.79 ± 0.01
3	$-1\|0; +1\|1$	/	-0.12 ± 0.01
3	$-1\|0; -1\|1$	/	-0.14 ± 0.01
3	$+1\|1; +1\|0$	/	-0.06 ± 0.01
3	$+1\|1; -1\|0$	2.47 ± 0.03	-0.78 ± 0.01
3	$+1\|1; +1\|1$	/	-0.13 ± 0.01
3	$+1\|1; -1\|1$	/	-0.18 ± 0.01
3	$-1\|1; +1\|0$	/	-0.07 ± 0.01
3	$-1\|1; -1\|0$	2.46 ± 0.03	-0.68 ± 0.02
3	$-1\|1; +1\|1$	/	-0.17 ± 0.01
3	$-1\|1; -1\|1$	/	-0.16 ± 0.01

REFERENCES

[1] Y. Aharonov, D. Z. Albert, L. Vaidman, "How the result of a measurement of a component of the spin of a spin- 1/2 particle can turn out to be 100", Phys. Rev. Lett., vol. 60, no. 14, 1988, pp. 1351–1354.

[2] O. Hosten, P. Kwiat, "Observation of the Spin Hall Effect of Light via Weak Measurements", Sci., vol. 319, no. 5864, 2008, pp. 787–790.

[3] P. B. Dixon, D. J. Starling, A. N. Jordan, J. C. Howell, "Ultrasensitive Beam Deflection Measurement via Interferometric Weak Value Amplification", Phys. Rev. Lett., vol. 102, no. 17, 2009, p. 173601.

[4] G. Jayaswal, G. Mistura, M. Merano, "Observation of the Imbert–Fedorov effect via weak value amplification", Opt. Lett., vol. 39, no. 8, 2014, p. 2266.

[5] K. Resch, J. Lundeen, A. Steinberg, "Experimental realization of the quantum box problem", Phys. Lett. A, vol. 324, no. 2-3, 2004, pp. 125–131.

[6] T. Ravon, L. Vaidman, "The three-box paradox revisited", J. Phys. A: Math. Theor., vol. 40, no. 11, 2007, pp. 2873–2882.

[7] F. Piacentini, et al., "Measuring Incompatible Observables by Exploiting Sequential Weak Values", Phys. Rev. Lett., vol. 117, no. 17, 2016, p. 170402.

[8] J.-S. Chen, M.-J. Hu, X.-M. Hu, B.-H. Liu, Y.-F. Huang, C.-F. Li, C.-G. Guo, Y.-S. Zhang, "Experimental realization of sequential weak measurements of non-commuting Pauli observables", Opt. Express, vol. 27, no. 5, 2019, p. 6089.

[9] J. S. Lundeen, B. Sutherland, A. Patel, C. Stewart, C. Bamber, "Direct measurement of the quantum wavefunction", Nat., vol. 474, no. 7350, 2011, pp. 188–191.

[10] L. Calderaro, G. Foletto, D. Dequal, P. Villoresi, G. Vallone, "Direct Reconstruction of the Quantum Density Matrix by Strong Measurements", Phys. Rev. Lett., vol. 121, no. 23, 2018, p. 230501.

[11] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, A. Acín, "Unbounded randomness certification using sequences of measurements", Phys. Rev. A, vol. 95, no. 2, 2017, p. 020102.

[12] K. Mohan, A. Tavakoli, N. Brunner, "Sequential random access codes and self-testing of quantum measurement instruments", New J. Phys., vol. 21, no. 8, 2019, p. 083034.

[13] G. Foletto, L. Calderaro, G. Vallone, P. Villoresi, "Experimental Demonstration of Sequential Quantum Random Access Codes", arXiv:2001.04885.

[14] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki, "Quantum entanglement", Rev. Mod. Phys., vol. 81, no. 2, 2009, pp. 865–942.

[15] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett., vol. 67, no. 6, 1991, pp. 661–663.

[16] V. Giovannetti, "Quantum-Enhanced Measurements: Beating the Standard Quantum Limit", Sci., vol. 306, no. 5700, 2004, pp. 1330–1336.

[17] S. Pironio, V. Scarani, T. Vidick, "Focus on device independent quantum information", New J. Phys., vol. 18, no. 10, 2016, p. 100202.

[18] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, "Bell nonlocality", Rev. Mod. Phys., vol. 86, no. 2, 2014, pp. 419–478.

[19] S. Pironio, et al., "Random numbers certified by Bell's theorem", Nat., vol. 464, no. 7291, 2010, pp. 1021–1024.

[20] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, "Device-Independent Security of Quantum Cryptography against Collective Attacks", Phys. Rev. Lett., vol. 98, no. 23, 2007, p. 230501.

[21] G. Foletto, L. Calderaro, A. Tavakoli, M. Schiavon, F. Picciariello, A. Cabello, P. Villoresi, G. Vallone, "Experimental Demonstration of Sustained Entanglement and Nonlocality After Sequential Measurements", Phys. Rev. Appl., vol. 13, no. 4, 2020, p. 044008.

[22] J. F. Clauser, M. A. Horne, A. Shimony, R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories", Phys. Rev. Lett., vol. 23, no. 15, 1969, pp. 880–884.

[23] A. Tavakoli, A. Cabello, "Quantum predictions for an unmeasured system cannot be simulated with a finite-memory classical system", Phys. Rev. A, vol. 97, no. 3, 2018, p. 032131.

[24] O. Gühne, G. Tóth, "Entanglement detection", Phys. Reports, vol. 474, no. 1-6, 2009, pp. 1–75.