Experimental test of sequential weak measurements for certified quantum randomness extraction

Giulio Foletto,[1,*] Matteo Padovan,[1,*] Marco Avesani,[1] Hamid Tebyanian,[1] Paolo Villoresi,[1,2] and Giuseppe Vallone[1,3,2,†]

[1] *Dipartimento di Ingegneria dell'Informazione, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*
[2] *Padua Quantum Technologies Research Center, Università degli Studi di Padova, via Gradenigo 6B, IT-35131 Padova, Italy*
[3] *Dipartimento di Fisica e Astronomia, Università degli Studi di Padova, via Marzolo 8, IT-35131 Padova, Italy*

Quantum nonlocality offers a secure way to produce random numbers: Their unpredictability is intrinsic and can be certified just by observing the statistic of the measurement outcomes, without assumptions on how they are produced. To do this, entangled pairs are generated and measured to violate a Bell inequality with the outcome statistics. However, after a projective quantum measurement, entanglement is entirely destroyed and cannot be used again. This fact poses an upper bound to the amount of randomness that can be produced from each quantum state when projective measurements are employed. Instead, by using weak measurements, some entanglement can be maintained and reutilized, and a sequence of weak measurements can extract an unbounded amount of randomness from a single state as predicted in Phys. Rev. A **95**, 020102(R) (2017). We study the feasibility of these weak measurements, analyze the robustness to imperfections in the quantum state they are applied to, and then test them using an optical setup based on polarization-entangled photon pairs. We show that the weak measurements are realizable, but can improve the performance of randomness generation only in close-to-ideal conditions.

I. INTRODUCTION

Classical random number generators cannot produce genuine randomness as they rely on algorithms or deterministic phenomena. However, quantum physics offers several solutions for producing secure and private random numbers [1, 2]. The simplest one arises from the superposition principle, which makes quantum measurements probabilistic on most states. This idea can be exploited, for example, by identifying two mutually unbiased bases, preparing a physical system in a state belonging to one, and measuring it with respect to the other. Neglecting experimental imperfections, in the long run, the measurement outcomes will be random and uniformly distributed. However, this relies on at least two strong assumptions: knowledge of the quantum state and accurate control of the measurement being made. These are often hard to verify in practice, and hence leave an opening for potential attacks.

A different approach to quantum randomness starts from the concept of nonlocality [3], for which the outcomes of measurements on some multipartite systems generate correlations that cannot be explained by theories that are local and realistic. In arguably one of the most important results of quantum theory, J. S. Bell showed that there are relations between the statistics of the measurement outcomes that must hold for such theories but are violated by quantum physics [4]. These relations, now called Bell inequalities, have been violated experimentally countless times, thus proving that local realistic theories are incompatible with the experimental data [5–10]. Assuming that no-signaling still holds, the measurements that violate the inequalities are intrinsically unpredictable, and hence they can produce random numbers [11]. Protocols that exploit the violation of a Bell inequality are often termed *device independent*, because this violation does not require any assumption on the nature of the state nor the measurements, and hence is independent of the inner workings of the devices in use. This level of security is higher than that of other frameworks (e.g., trusted device [2] or semi-device-independent [12–15]), which require full or partial trust on the devices and cannot allow them to be controlled by an adversary, something that, instead, is tolerated in the device-independent case.

This abstract intuition has been made more quantitative with the study and development of device-independent random number generators [16–22]. In general, these instruments consist of a source of entangled states, which are necessary for violating a Bell inequality, and some measurement stations that receive each subsystem, measure it, and attempt to observe nonlocality using the result statistics. The amount of randomness that can be extracted from the measurement outcomes depends on the strength of the violation. For instance, most implementations use two-qubit states, such as polarization-entangled photon pairs and exploit the CHSH inequality [23]. A limitation of this scheme is that the projective measurements irreversibly destroy entanglement, hence each pair can contribute to only one violation and produce at most one bit of randomness if the outcomes on one subsystem are used, or 1.23 bits if both parties are considered [16].

Although there are other ways to overcome this bound (see, e.g., Ref. [24]), we shall focus on the use of the weak measurement [25]. Throughout the last three decades, this tool has found many diverse applications, from the

[*] These authors contributed equally to this work.
[†] vallone@dei.unipd.it

amplification of feeble quantities [26–28], to the measurement of incompatible observables [29–31], through quantum state reconstruction [32–35]. Recently, it has been exploited for sequential protocols, in which a system undergoes multiple measurements without ever completely collapsing or losing its useful quantum features, which can be harvested repeatedly. In this manner, Bell inequalities can be violated more times [36–40], quantum random access codes can be used by two parties [41, 42], and quantum instruments can be tested [43]. More important for this work is using weak measurements to produce random bits from the same physical system repeatedly [44, 45]. The authors of Ref. [44] proposed a device-independent protocol based on the sequential violation of a CHSH-like inequality on a bipartite entangled state. In the case of perfect state preparation and an infinite sequence of ideal measurements, their scheme can produce an unbounded amount of random bits from the outcomes of local measurements on one subsystem.

Albeit valid only in an ideal scenario, this fact encourages an evaluation of the practical feasibility of this protocol, which is the aim of this work. We first theoretically analyze its robustness to imperfections and then show a proof-of-concept experimental implementation based on bulk polarization optics that highlights the difficulties inherent in these measurements, but can be a starting point for further developments using setups of higher accuracy.

II. THEORETICAL MODEL

In Secs. II A, II B, and II C, we summarize and extensively comment on the protocol proposed in Ref. [44] to set the framework we are working in and explain the notation. Then, in Sec. II D, we present the main theoretical result of this work. We first introduce a simple model to characterize the robustness of the protocol to experimental imperfections, and then apply it in numerical simulations to study how much randomness can be generated under different noise conditions.

A. The sequential measurement protocol

The protocol, schematically depicted in Fig. 1, starts with a pure two-qubit entangled state, shared between two parties called Alice and Bob$_1$:

$$|\psi_1\rangle = \cos\theta_1 |00\rangle + \sin\theta_1 |11\rangle , \tag{1}$$

where $\theta_1 \in [0, \pi/4]$ is an indicator of the amount of entanglement in the state, indeed if $\theta_1 = 0$, $|\psi_1\rangle$ is separable, whereas if $\theta_1 = \pi/4$, the state is a maximally entangled Bell pair. In the best-case scenario, the protocol starts with $\theta_1 = \pi/4$ and hence can achieve the best performance. We now focus on the action of Bob$_1$, who is the first in a sequence of observers that work on the same half of the entangled pair. We will describe Alice's role in Sec. II B. Bob$_1$ selects one of two observables to be measured:

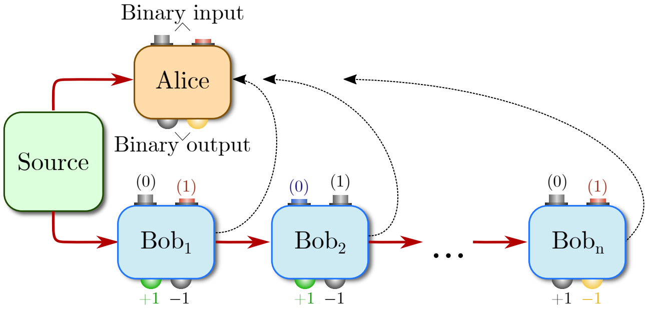


FIG. 1. Scheme of the sequential protocol. The dotted black line indicates that, before attempting to violate the Bell inequality with a Bob, Alice requires the history of outcomes of the previous observers. This communication can also be replaced by post-selection. Alice's measurements are described by Eq. (4), whereas the Bobs' are in Eq. (2).

$$\begin{aligned} B^{(0)} &= \sigma_z, \\ B_1^{(1)} &= \cos(2\xi_1)\sigma_x, \end{aligned} \tag{2}$$

in which $\xi_1 \in [0, \pi/4]$ quantifies the strength of the measurement of σ_x, which is projective for $\xi_1 = 0$, completely noninteractive for $\xi_1 = \pi/4$, and generically weak for any value in between. In this way, the observable $B_1^{(1)}$ corresponds to a generalized measurement of σ_x with Kraus operators $K_{1,\pm} = \frac{1}{2}[(\cos\xi_1 + \sin\xi_1)\mathbb{1} \pm (\cos\xi_1 - \sin\xi_1)\sigma_x]$. Both observables return binary outcomes $y_1 = \pm 1$, collected by Bob$_1$. The state of Eq. (1) is balanced with respect to the measurement of $B_1^{(1)}$, meaning that both outcomes can happen with $\frac{1}{2}$ probability. These outcomes are used to generate random bits, whereas those of $B^{(0)}$ are needed to violate a Bell inequality and certify that state and measurements are indeed those we are describing.

After the measurement, the state takes the form,

$$\left|\psi_{2,\vec{h}}\right\rangle = U_{A,2,\vec{h}} \otimes U_{B,2,\vec{h}} (\cos(\theta_2)|00\rangle + \sin(\theta_2)|11\rangle), \tag{3}$$

where the unitary operations $U_{A,2,\vec{h}}, U_{B,2,\vec{h}}$ depend on Bob$_1$'s strength and outcome. We use symbol $\vec{h}$ to label the *history* of outcomes at the past steps (which in this case contains only one datum, y_1). The value of the parameter θ_2 does not depend on Bob$_1$'s outcome but still depends on his strength, although we do not highlight this in the notation.

Using his knowledge of the outcome, Bob$_1$ applies $U^\dagger_{B,2,\vec{h}}$ to his local state and sends it to Bob$_2$, who can proceed with a similar step. The purpose of this action is to make Bob$_2$'s state again balanced with respect to the outcomes of $B^{(1)}$, so that he can again produce random bits by measuring the $B^{(1)}$ observable. The protocol can continue with an unlimited sequence of measurements of $B^{(1)}$ or can be stopped with a strong measurement of

$B^{(0)}$. There is no reason to continue the protocol after this because the post-measurement state is no longer entangled. To make a long sequence of measurements, we can imagine that $B^{(0)}$ is chosen with low probability, just enough to provide the statistics that violate a Bell inequality.

B. Extraction of random bits

We now move to the other half of the entangled pair, held by Alice. The outcomes of her measurements do not directly provide random bits, but are correlated with those of the Bobs to violate a Bell inequality. For each quantum system, Alice selects a step k and one of the two projective observables:

$$\begin{aligned} A_k^{(0)} &= \cos(\mu_k)\sigma_z + \sin(\mu_k)\sigma_x, \\ A_k^{(1)} &= \cos(\mu_k)\sigma_z - \sin(\mu_k)\sigma_x, \end{aligned} \tag{4}$$

where $\mu_k = \arctan(\sin(2\theta_k))$. These choices change for each quantum state and the Bobs must not know them until after all actions and measurements are completed. Before measuring her selected observable, Alice applies the unitary transformation $U^\dagger_{A,k,\vec{h}}$, so that again the global state takes the form of Eq. (1) (with the generic angle θ_k). To do this, she must wait for $\mathrm{Bob}_1, \cdots, \mathrm{Bob}_{k-1}$ to measure their half of the state and to send her their history $\vec{h}$ of outcomes. However, she is careful to measure her state outside of the light cone of Bob_k's basis choice, otherwise the estimation of the Bell quantity would be affected by the locality loophole [46].

By correlating their outcomes on multiple statistical repetition of this test, Alice and Bob_k can compute the quantity

$$\begin{aligned} I_k = \beta_k \left\langle B^{(0)} \right\rangle + \left\langle A_k^{(0)} B^{(0)} \right\rangle + \left\langle A_k^{(0)} B_k^{(1)} \right\rangle \\ + \left\langle A_k^{(1)} B^{(0)} \right\rangle - \left\langle A_k^{(1)} B_k^{(1)} \right\rangle, \end{aligned} \tag{5}$$

where $\beta_k = 2\cos(2\theta_k)/\sqrt{1+\sin^2(2\theta_k)}$, and the brackets denote the expectation value. A local-hidden-variables model would restrict I_k with the CHSH-like Bell inequality $I_k \leq \beta_k + 2$, however, quantum theory allows a larger upper bound [47]:

$$I_{\max,k} = \sqrt{2(4+\beta_k^2)}. \tag{6}$$

Crucially, observing this maximal value certifies that the state is the one described by Eq. (1) and the measurements are those of Eqs. (2), (4), with $\xi_k = 0$, because this is the *only* configuration (up to unitary transformations) that can reach this upper bound. Moreover, since $\left\langle B_k^{(1)} \right\rangle = 0$ on this state, this also certifies that the outcomes of $B_k^{(1)}$ are uniformly distributed and private, and therefore can be used as random bits, the ultimate goal of this scheme. This is because of the monogamy of entanglement, which is reflected by the fact that the state (1) is bipartite and pure, and hence cannot be correlated with any information held by a third party.

The certification does not apply only to the outcomes of $B_k^{(1)}$ that are used in the estimation of I_k, but also to all the other outcomes of the same measurement and with the same history $\vec{h}$ generated by other entangled pairs (regardless of Alice's actions for those pairs). Indeed, the Bobs' devices cannot know a priori which step k will be chosen for each entangled pair, and therefore cannot apply different strategies to the quantum systems. Any attempt to cheat is detected in the estimation of I_k, although only a subset of the outcomes contributes to said estimation. Similarly, each entangled pair produces many outcomes, one at each step, and only one of these contributes to the estimation of the Bell quantity, the one corresponding to the step k chosen by Alice for this pair. This does not mean that the others are useless: after sufficiently many runs of the experiment, all the steps and all the possible histories undergo the certification and the randomness of all these outcomes is validated.

As previously mentioned, Alice requires to know the history $\vec{h}$ of $\mathrm{Bob}_1, \cdots, \mathrm{Bob}_{k-1}$'s outcomes to apply $U^\dagger_{A,k,\vec{h}}$. This is an important limitation to the practicality of this scheme. Indeed, the Bobs need a fast communication channel to send their outcomes to Alice just after they have produced them, so that she can apply the unitary transformation and measure her state before entering the light cone of Bob_k's basis choice, otherwise she would open the locality loophole. If this communication is deceitful or contains error, the amount of certifiable randomness is reduced because Alice applies the wrong unitary transformation (but this is a denial of service, not a security risk).

A probably easier alternative is that Alice randomly chooses among the 2^{k-1} possible histories and learns whether her guess was correct only afterward, without the need for communication between the measurements. Whenever her guess is wrong, she and Bob_k do not use their outcomes in the estimation of the Bell quantity, but none of the bits generated by the Bobs are thrown away: they will be certified later when Alice guesses correctly. Just as above, even if the Bobs' devices are dishonest, they cannot predict Alice's chosen history, therefore they cannot apply different strategies to different entangled pairs and make those for which Alice's guess is wrong less secure. This strategy introduces a larger delay between the production of the outcomes and their certification, because many more runs are needed to achieve the necessary statistics. Yet, it does not decrease the randomness generation rate, because once the certification is done, it applies to all outcomes, not only to the few that were generated when Alice guessed right. The *net* generation rate is still reduced because Alice spends randomness in the choice of history, but this cost can be lessened using an unbalanced distribution.

Like in event-ready Bell tests [8], discarding outcomes from the certification does not open any loophole [46]. Indeed, the application of the random transformation $U^{\dagger}_{A,k,\vec{h}}$ followed by one of the two measurements $A_k^{(0)}$ or $A_k^{(1)}$, can be interpreted as a measurement randomly chosen between 2^k different observables (defined as $U_{A,k,\vec{h}} A_k^{(0)} U^{\dagger}_{A,k,\vec{h}}$ and $U_{A,k,\vec{h}} A_k^{(1)} U^{\dagger}_{A,k,\vec{h}}$ with the 2^{k-1} possible choices of $\vec{h}$). The actual history of outcomes provided to $\mathrm{Bob}_1, \cdots, \mathrm{Bob}_{k-1}$ by their devices plays the role of a description of the prepared entangled state shared between Alice and Bob_k, given by $\left|\psi_{k,\vec{h}}\right\rangle = U_{A,k,\vec{h}} \otimes \mathbb{1}_B (\cos(\theta_k)\,|00\rangle + \sin(\theta_k)\,|11\rangle)$. Therefore, this scenario can be seen as a Bell test where Alice can choose between 2^k observables and Bob_k can choose between two observables, corresponding to 2^{k-1} Bell inequalities. Depending on the prepared state $\left|\psi_{k,\vec{h}}\right\rangle$, only one of the 2^{k-1} Bell inequalities is optimally violated and used to certify the randomness of the outcomes. Hence, measured data from Alice and Bob_k are post-selected according to the prepared state $\left|\psi_{k,\vec{h}}\right\rangle$. It is important to underline that it is always possible for Alice and Bob_k's to choose their bases outside of the light cones of the outcomes obtained by $\mathrm{Bob}_1, \cdots, \mathrm{Bob}_{k-1}$, physically enforcing independence between the inputs of the Bell test and the post-selection. In this way, dishonest devices cannot influence the outcomes of the test by exploiting the post-selection.

Finally, regardless of whether she takes a guess or not, Alice needs to be able to perform an exponentially growing number of different unitary transformations, which is a further practical difficulty.

C. Nonmaximal violations

The authors of Ref. [44] also conjecture and numerically verify a relation that bounds the guessing probability G_k of the outcomes of $B_k^{(1)}$ with a nonmaximal violation of the Bell inequality:

$$G_k \leq G_{\max,k} = \frac{1}{2} + \frac{\sqrt{I^2_{\max,k} - I_k^2}}{2(2-\beta_k)}. \quad (7)$$

This is important not only because experimental imperfections make maximal violations effectively impossible to observe, but also because the protocol itself requires $\xi_k > 0$ for all but at most the very last step, which means that $I_k = I_{\max,k}$ would be unattainable even if a perfect apparatus were used.

This means that after observing I_k, Alice and Bob_k can conclude that the min-entropy of each outcome of $B_k^{(1)}$ is $H_{\min,k} = -\log_2 G_{\max,k}$, with $G_{\max,k}$ calculated as in Eq. (7). Therefore, at any step k a close-to-maximal violation of the Bell inequality allows to extract close-to-1 random bits from each outcome. The outcomes of $B^{(0)}$ do not contribute to this extraction, but the performance loss can be minimized by choosing $B^{(1)}$ with high probability.

D. Robustness to imperfections

To account for real-world imperfections, we consider an initial state described by the density matrix

$$\rho_1 = (1-p-c)\,|\psi_1\rangle\langle\psi_1| + p\frac{\mathbb{1}}{4} + c\frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2}, \quad (8)$$

where we are setting $\theta_1 = \frac{\pi}{4}$ in the definition of $|\psi_1\rangle$ to use the best possible state as a starting point. The second addend introduces diagonal terms in the ideal density matrix so that the state becomes depolarized. It models the mixing of the ideal state with uncorrelated noise, such as, in the case of a photonics-based experiment, background light, dark counts or accidental coincidences. The third addend induces decoherence in the state because the extreme antidiagonal terms of the matrix are reduced with respect to the diagonal ones. It is especially realistic for states produced via SPDC, for which the indistinguishability between the $|00\rangle$ and $|11\rangle$ components is the result of precise alignment. Unavoidable small inaccuracies generate the classical superpositions described by this addend. This simple model is convenient because parameters p and c are easy to estimate experimentally. Indeed, they are directly related to the visibilities $V_{\mathcal{Z}}$ and $V_{\mathcal{X}}$ of the state:

$$\begin{aligned} V_{\mathcal{Z}} &= \mathrm{Tr}(\sigma_Z \otimes \sigma_Z \rho_1) = 1-p, \\ V_{\mathcal{X}} &= \mathrm{Tr}(\sigma_X \otimes \sigma_X \rho_1) = 1-p-c, \end{aligned} \quad (9)$$

where we are assuming $V_{\mathcal{Z}} \geq V_{\mathcal{X}}$. This is common in sources of polarization-entangled photon pairs, whose polarizing elements define a privileged basis, usually labeled $\mathcal{Z}$, for which visibility is higher. Visibilities are a straightforward characterization technique for such sources, and allow us to easily calculate p and c and to compare the experimental results with the theoretical predictions.

By applying the protocol described in Sec. II to the initial state of Eq. (8), we can evaluate how robust the results can be to imperfections in the preparation of the entangled pair. For simplicity, we set $c = 0$ in this initial characterization, and we will use the full model compared to the experimental results in Sec. IV.

In Fig. 2, we show the min-entropy $H_{\min}$ for a sequence of only two steps, with the last being projective, for several values of p. The curves, which show the sum of the contributions of the two steps, have two kinks and therefore can be divided in three regions. In the leftmost one, the first measurement is too strong to preserve entanglement, therefore $H_{\min,2} = 0$ and only the first step contributes. The opposite happens in the rightmost region, in which $H_{\min,1} = 0$. The region between the two kinks is the most interesting, because here both measurement steps contribute to the production of random bits. For $p < p_{thr}^{(12)} \approx 3.7 \cdot 10^{-3}$ the global maximum of the curve is achieved inside this region, indicating that a weak measurement is optimal. For instance, for $p = 1.4 \cdot 10^{-3}$, the protocol can achieve about 1 bit of min-entropy from the sum of the two steps, using $\xi_1 \approx 0.3$, whereas a single projective measurement would reach only 0.9 bits. As predicted in Ref. [44], the optimal value of ξ_1 is very close to 0 for nearly ideal states, but grows with the introduction of depolarization. For $p > p_{thr}^{(12)}$, this value is 0, indicating that the best strategy is to use a single projective measurement.

We also evaluate the protocol with two weak steps and a third projective one. From Fig. 3(a), we can see that $p = 1.4 \cdot 10^{-3}$ is too large to reach one bit except near the axes of the graph, i.e. when only two extractions are meaningful. We numerically verified that with $p \approx 3.2 \cdot 10^{-4}$ it is possible to reach one bit with three nonzero extractions: this means that adding a third step to the protocol only worsens its robustness to depolarization. Furthermore, in Fig. 3(b) we also show the value of p needed to reach two bits ($\approx 4.3 \cdot 10^{-9}$).

Finally, we investigate whether incrementing the sequence of measurements can increase the amount of extractable randomness. Our analysis considers at most three steps (the last of which projective) and consists of a numerical maximization of the achievable min-entropy over the strength parameters ξ_1 and ξ_2 for each value of p. We show the results in Fig. 4, where we highlight three possible cases with three different colors. In the rightmost region (cyan), for which $p > p_{thr}^{(12)}$, the maximal extraction is achievable by setting $\xi_1 = 0$, i.e. with just one projective measurement. By continuing to the left we find the interval for which $p_{thr}^{(23)} < p < p_{thr}^{(12)}$, where $p_{thr}^{(23)} \approx 1.39 \cdot 10^{-7}$ (yellow). Here, the strategy that maximizes randomness is to begin with a weak measurement ($\xi_1 \neq 0$), and then stop after a second projective one ($\xi_2 = 0$). The leftmost region (red) indicates where two weak extractions plus a projective one outperform the previous two cases: indeed, the maximal min-entropy is achievable if $\xi_1 \neq 0$ and also $\xi_2 \neq 0$. From these results, we can conclude that longer sequences are only beneficial for smaller and smaller amounts of depolarization.

III. EXPERIMENTAL METHOD

We verified experimentally whether these weak measurements could violate the Bell inequality strongly enough to generate randomness.

The source of polarization-entangled photons is a 30 mm long periodically poled potassium titanyl phosphate (PPKTP) crystal, placed inside a Sagnac interferometer. A continuous-wave laser at 404 nm provides the pump light, that enters the polarizing beam splitter of the Sagnac interferometer with a diagonal polarization. The exiting photons at 808 nm are then collected into two single-mode fibers and brought to Alice and the Bobs' measurement sides. Here, a half-wave plate (HWP) and

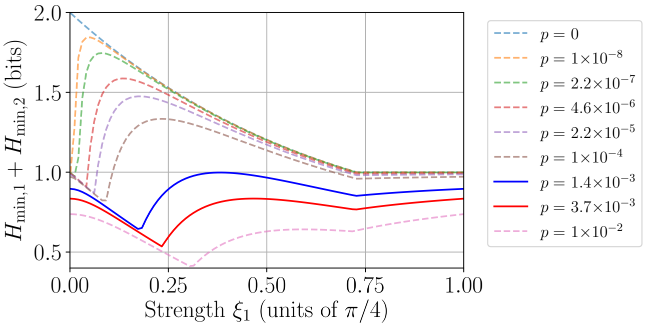
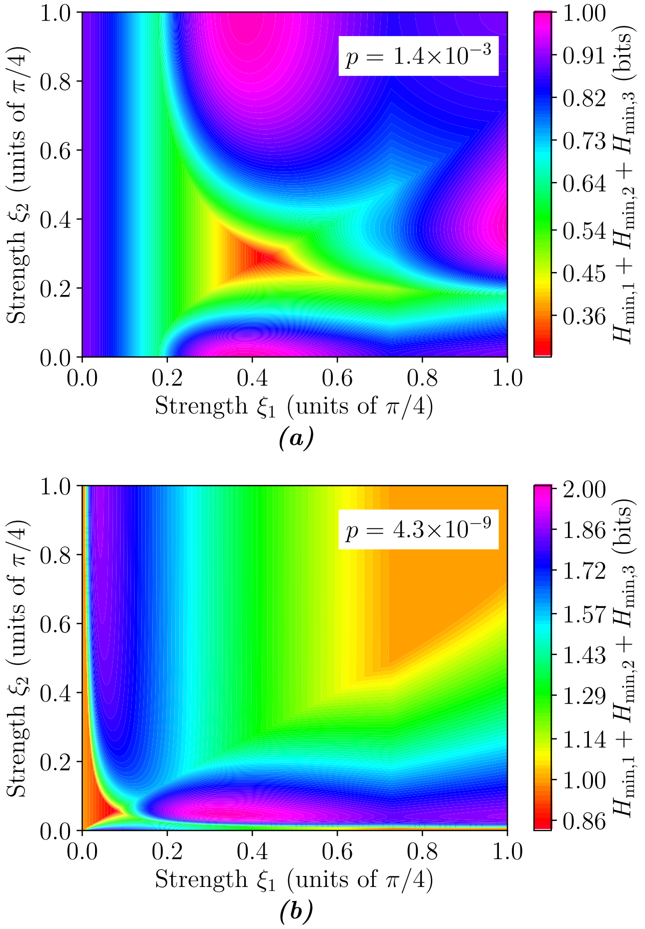


FIG. 2. Achievable secure bits from one weak extraction and a subsequent projective one, for several values of the parameter p. The two highlighted solid lines are related to the values of p that allow to reach 1 total secure bit (blue) and for which one projective measurement starts to outperform the two-steps protocol ($p_{thr}^{(12)}$, red).



(a)

(b)

FIG. 3. Secure bits achievable from three extractions with the last one projective ($\xi_3 = 0$). With $p \approx 1.4 \cdot 10^{-3}$ it is possible to reach one bit only near the axes, i.e. when one of the three steps is not useful. For $p < 4.3 \cdot 10^{-9}$ more than two bits can be extracted.

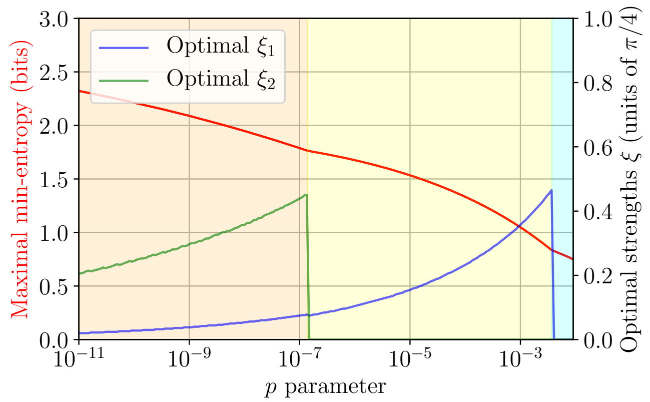


FIG. 4. Maximal secure bits achievable as a function of the value of p. The colored regions represent the three cases in which it is better to perform one (cyan), two (yellow) or three (red) steps in order to achieve the maximal extraction of bits. The two threshold values are $p_{thr}^{(12)} \approx 3.7 \cdot 10^{-3}$ and $p_{thr}^{(23)} \approx 1.39 \cdot 10^{-7}$.

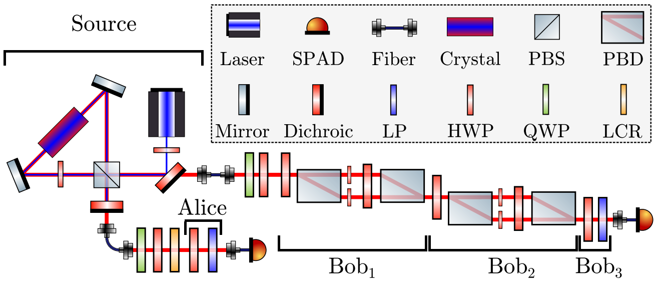


FIG. 5. Scheme of the experimental setup.

a quarter-wave plate are used by both parties to remove the unitary evolutions due to the fibers and to transform the state into the desired one

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle), \tag{10}$$

where the horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarization components correspond to the $|0\rangle$ and $|1\rangle$ states of the theoretical protocol. Furthermore, Alice uses a liquid-crystal retarder (LCR) to fine tune the phase between the two different polarization components. Since Alice needs to measure only linear polarizations, her measurement setup consists of an HWP and a linear polarizer (LP). The complete scheme of the setup is depicted in Fig. 5.

On the Bobs' side we used a series of two Mach-Zehnder interferometers (MZI) that implement the weak measurements described in the protocol. Each of them is composed by two polarizing beam displacers (PBD) that separate and rejoin the horizontal and vertical polarization components, two small HWPs (one per arm) and a shared HWP that selects the strength of the measurement. Two more HWPs, one before and one after the MZI choose the basis for the measurement and apply the unitary operations $U_B^\dagger$. The small HWP in the H path has its fast axis horizontal, while the one in the V path is rotated by $\pi/4$. The strength ξ of the measurement is regulated by setting the shared HWP at $\pi/4 - \xi/2$.

After the two MZIs, a third projective polarization measurement is implemented by an HWP and a LP. At each side, after the evolution of the state, the photons are collected into a fiber and sent to a single-photon avalanche diode connected to an 80-ps resolution time tagger that returns coincidence counts within a ±1-ns window.

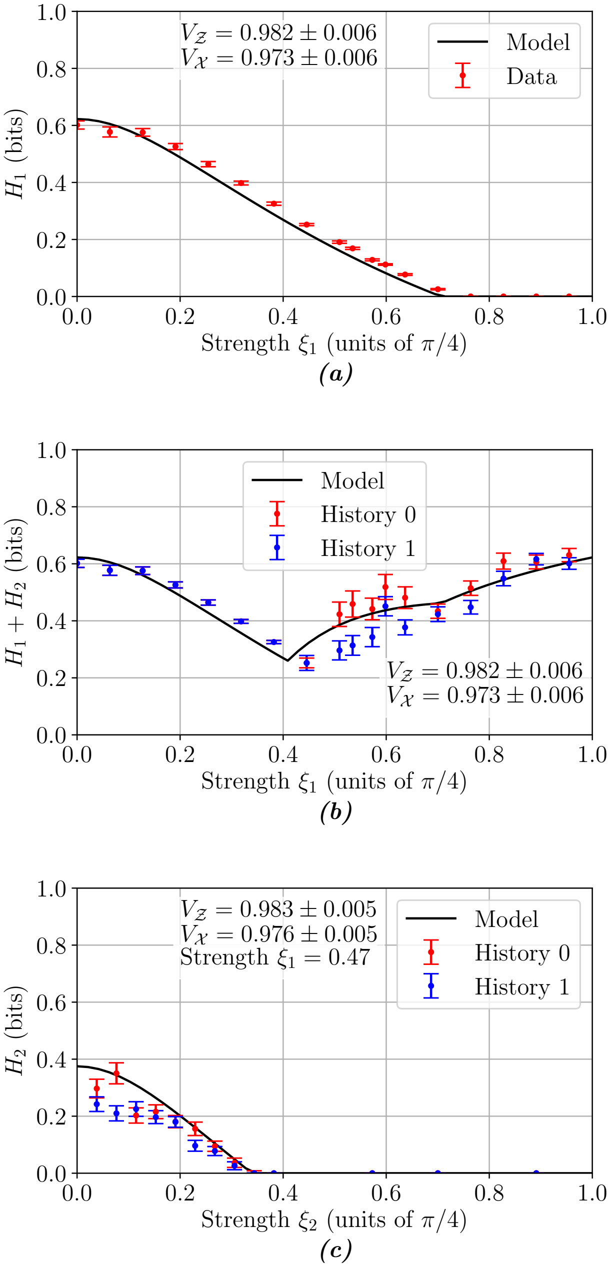
By rotating the HWPs between the interferometers, we set not only the measurement bases, but also the outcomes that correspond to the photons that pass through the only exit of the PBDs that is connected to the rest of the setup. We can then scan all the different combinations of bases and outcomes sequentially, and, for each of them, record the number of coincident events. The exposure time is fixed and chosen to gather enough statistics to obtain small statistical errors (details in Sec. IV). Then, linear combinations of the coincidence rates allow us to estimate the expected values in Eq. (5) and ultimately I_k.

In order to truly observe all outcomes without choosing them beforehand, as is necessary to produce random bits, this setup would require a treelike structure on Bob's side, which would grow exponentially with the number of steps. We also note that the violations of the Bell inequality that we report are affected by several loopholes, such as the locality and detection ones [46]. More profoundly, we do not choose the bases randomly, and do not record random outcomes from each measurement, but only expectation values, hence this is not a true Bell experiment. A faithful implementation of the protocol should address all these issues. However, our setup allows the feasibility study of the weak measurements, which is the focus of this work.

IV. RESULTS

We first characterize the protocol as a function of the strength parameters, adopting the model of Eq. (8) for the initial state. After finding the best strength, we perform longer-exposure experiments with that setting, like a real implementation of a randomness generator would do. We choose an exposure time of about 60s ($\sim 2 \cdot 10^5$ detected coincidences) for the long-exposure tests and about 30s ($\sim 10^5$ detected coincidences) for the variable-strength tests. This makes statistical errors small enough. We do not consider any finite-statistics effect in the estimation of the min-entropy. As we can see from Sec. II D, the protocol is very demanding in terms of purity of the state and, with our experimental visibilities, we must stop at two extraction steps, since we cannot violate the Bell inequality afterward.

Figure 6(a) shows the number of secure bits achievable from one weak step at different values of ξ_1 compared with the prediction of our model calculated with the ini-



(a)

(b)

(c)

FIG. 6. Results of the feasibility tests with variable strength. The continuous line is the model prediction while the dots represent the experimental data with their standard deviations, calculated with a Monte Carlo simulation which considers the Poissonian error on photon counting.

tial visibilities reported in the chart. In Fig. 6(b) we can see the previous bits summed with the bits extracted from a subsequent projective step, while Fig. 6(c) shows the result of a second weak step after a first one with $\xi_1 = 0.47$.

In order to estimate the quality of our state, we measure the initial visibilities in bases $\mathcal{X} = \{|D\rangle, |A\rangle\}$ and $\mathcal{Z} = \{|H\rangle, |V\rangle\}$ before the experiments. To do this, we use an half-wave plate and a linear polarizer in front of the SPAD in the same way that we perform projective measurements for the protocol. We calculate their standard deviations via propagation assuming Poissonian counting errors at the detectors. We report these values in Fig. 6. From them, we can use Eq. (9) to obtain parameters p and c, which we insert in the model to predict the amount of extractable randomness.

We can clearly see that our imperfect preparation prevents us from generating more than one bit of randomness per entangled pair, and enlarges the region of strength parameters where we cannot violate the Bell inequality at all. Although we can generate some randomness at both the first and the second step, we achieve the best results when one measurement is noninteractive and the other is projective: Our state is too depolarized to make the weak measurement useful. Yet, our results closely follow the theoretical predictions, especially at the first step. The second interferometer, by introducing further imperfections in the measurement, makes our data slightly separate from the solid line, as seen in Fig. 6(c).

Table I shows the results of the long-exposure feasibility tests compared with the model prediction. We choose a strength $\xi_1 = 0.4$ when the next step is projective, while we choose $\xi_1 = 0.47$ and $\xi_1 = 0.52$ in order to perform a second nonprojective step with $\xi_2 = 0.1$. The two rightmost columns show the min-entropy predicted by the model and measured experimentally: Our results are slightly below the predictions, probably because of systematic misalignments in the optical setup.

Albeit not shown in the table, we also add a third projective step after the second weak one, but the correlations between Alice and Bob$_3$'s results are not strong enough to violate the CHSH-like inequality, and hence provide $H_{\min,3} = 0$. We attribute this to the visibilities of the state we produced, which do not allow more than two extractions of randomness, as predicted by our analysis.

V. CONCLUSIONS

In this work, we have studied the feasibility of using sequential weak measurements to extract more randomness from entangled pairs. We have evaluated the protocol of Ref. [44] and focused on its robustness to imperfections in the preparation of the initial quantum state. Our analysis shows that even small amounts of depolarization nullify the performance gain (in terms of produced random bits per entangled pair) offered by the addition of a new measurement in the sequence, and the longer the sequence, the closer to ideal the state has to be in order to fully exploit all measurements. For instance, a second step is useful only for $p < p_{thr}^{(12)} \approx 3.7 \cdot 10^{-3}$ and a third for $p < p_{thr}^{(23)} \approx 1.39 \cdot 10^{-7}$.

Our experiment fully confirms the validity of this protocol and of the model summarized by Eq. (8), which includes most of the inaccuracies of our setup, as can

TABLE I. Results of the long-exposure feasibility tests. Standard deviations are calculated with a Monte Carlo simulation which considers the Poissonian error on photon counting.

		Strength	$H_{\min,k}$ (Model)	$H_{\min,k}$ (Experiment)
Step k	Previous outcome	(rad)	(bits)	(bits)
1	Not applicable	0.4	0.165	0.13 ± 0.002
2	0	Projective	0.263	0.38 ± 0.04
2	1	Projective	0.263	0.13 ± 0.02
1	Not applicable	0.47	0.085	0.057 ± 0.002
2	0	0.1	0.303	0.32 ± 0.02
2	1	0.1	0.303	0.25 ± 0.02
1	Not applicable	0.52	0.035	0.005 ± 0.001
2	0	0.1	0.369	0.38 ± 0.02
2	1	0.1	0.369	0.33 ± 0.01

be seen by the resemblance between the data points and theoretical predictions in Fig. 6. Moreover, it produces correlations that would allow to extract up to approximately 0.6 bits of randomness from two sequential steps [Fig. 6(b)]. Yet, it further highlights the challenges in applying this protocol and even just in the preparation of an accurate enough entangled state. Although there are reports of better visibilities [48], the unavoidable imperfections of bulk optical components make it difficult to reduce the value of p much below $p_{thr}^{(12)}$.

However, a simple model such as ours indicates the minimum quality of the initial entangled state required to make the sequential protocol useful. Through it, other experimental platforms could be investigated. Integrated optics can offer polarizing beam splitters with comparable extinction ratio [49–51], and although entanglement sources do not yet reach the same visibilities, their quality [52] and capabilities [53] are developing quickly. In the field of quantum computing, two-qubit gates with fidelities well above 99% have been demonstrated [54, 55], and perhaps, with some more improvements, the same technologies could be used to produce entangled states of the necessary quality for protocols like this. Alternatively, similar schemes that are more robust to noise could be considered. For instance, the protocol of Ref. [56] uses a weak measurement followed by a three-outcome POVM. Albeit limited to only two steps, it can overcome the bound of two bits generated from one-half of an entangled pair, even in experimentally viable noise conditions. Techniques like this will probably allow sequential weak measurements to improve the performance of randomness extraction with presently available optical components.

ACKNOWLEDGMENTS

Part of this work was supported by Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) (Italian Ministry of Education, University and Research) under the initiative "Departments of Excellence" (Law No. 232/2016), and by Fondazione Cassa di Risparmio di Padova e Rovigo within the call "Ricerca Scientifica di Eccellenza 2018", project *QUASAR*.

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quantum Information **2**, 16021 (2016), arXiv:1510.08957.

[2] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Reviews of Modern Physics **89**, 015004 (2017), arXiv:1604.03304.

[3] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Reviews of Modern Physics **86**, 419 (2014), arXiv:1303.2849.

[4] J. S. Bell, On the Einstein Podolsky Rosen paradox, Physics Physique Fizika **1**, 195 (1964).

[5] A. Aspect, P. Grangier, and G. Roger, Experimental Tests of Realistic Local Theories via Bell's Theorem, Physical Review Letters **47**, 460 (1981).

[6] A. Aspect, P. Grangier, and G. Roger, Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities, Physical Review Letters **49**, 91 (1982).

[7] A. Aspect, J. Dalibard, and G. Roger, Experimental Test of Bell's Inequalities Using Time- Varying Analyzers, Physical Review Letters **49**, 1804 (1982).

[8] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature **526**, 682 (2015).

[9] M. Giustina, M. A. M. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits,

A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, and A. Zeilinger, Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons, Physical Review Letters **115**, 250401 (2015), arXiv:1511.03190.

[10] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, J. C. Bienfang, R. P. Mirin, E. Knill, and S. W. Nam, Strong Loophole-Free Test of Local Realism, Physical Review Letters **115**, 250402 (2015), arXiv:1511.03189.

[11] R. Colbeck, *Quantum And Relativistic Protocols For Secure Multi-Party Computation*, Ph.D. thesis, University of Cambridge (2006).

[12] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Semi-device-independent random-number expansion without entanglement, Physical Review A **84**, 034301 (2011).

[13] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, J. Zhang, and J.-W. Pan, Experimental measurement-device-independent quantum random-number generation, Phys. Rev. A **94**, 060301(R) (2016).

[14] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Source-device-independent heterodyne-based quantum random number generator at 17 Gbps, Nature Communications **9**, 5365 (2018).

[15] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, Semi-Device-Independent Heterodyne-Based Quantum Random-Number Generator, Physical Review Applied **15**, 034034 (2021), arXiv:2004.08344.

[16] S. Pironio, A. Acín, S. Massar, A. B. 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 **464**, 1021 (2010), arXiv:0911.3427.

[17] P. Bierhorst, E. Knill, S. Glancy, Y. Zhang, A. Mink, S. Jordan, A. Rommal, Y.-K. Liu, B. Christensen, S. W. Nam, M. J. Stevens, and L. K. Shalm, Experimentally generated randomness certified by the impossibility of superluminal signals, Nature **556**, 223 (2018), arXiv:1803.06219.

[18] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent quantum random-number generation, Nature **562**, 548 (2018), arXiv:1807.09611.

[19] L. Shen, J. Lee, L. P. Thinh, J.-D. Bancal, A. Cerè, A. Lamas-Linares, A. Lita, T. Gerrits, S. W. Nam, V. Scarani, and C. Kurtsiefer, Randomness Extraction from Bell Violation with Continuous Parametric Down-Conversion, Physical Review Letters **121**, 150402 (2018), arXiv:1805.02828.

[20] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, S. W. Nam, C. Abellán, W. Amaya, M. W. Mitchell, H. Fu, C. A. Miller, A. Mink, and E. Knill, Experimental Low-Latency Device-Independent Quantum Randomness, Physical Review Letters **124**, 010505 (2020), arXiv:1812.07786.

[21] L. K. Shalm, Y. Zhang, J. C. Bienfang, C. Schlager, M. J. Stevens, M. D. Mazurek, C. Abellán, W. Amaya, M. W. Mitchell, M. A. Alhejji, H. Fu, J. Ornstein, R. P. Mirin, S. W. Nam, and E. Knill, Device-independent randomness expansion with entangled photons, Nature Physics , 1 (2021), arXiv:1912.11158.

[22] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent randomness expansion against quantum side information, Nature Physics , 1 (2021), arXiv:1912.11159.

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

[24] O. Andersson, P. Badziąg, I. Dumitru, and A. Cabello, Device-independent certification of two bits of randomness from one entangled bit and Gisin's elegant Bell inequality, Physical Review A **97**, 012314 (2018), arXiv:1707.00564.

[25] Y. Aharonov, D. Z. Albert, and 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, Physical Review Letters **60**, 1351 (1988).

[26] O. Hosten and P. Kwiat, Observation of the Spin Hall Effect of Light via Weak Measurements, Science **319**, 787 (2008).

[27] P. B. Dixon, D. J. Starling, A. N. Jordan, and J. C. Howell, Ultrasensitive Beam Deflection Measurement via Interferometric Weak Value Amplification, Physical Review Letters **102**, 173601 (2009), arXiv:0906.4828.

[28] G. Jayaswal, G. Mistura, and M. Merano, Observation of the Imbert–Fedorov effect via weak value amplification, Optics Letters **39**, 2266 (2014), arXiv:1401.0450.

[29] S. Kocsis, B. Braverman, S. Ravets, M. J. Stevens, R. P. Mirin, L. K. Shalm, and A. M. Steinberg, Observing the Average Trajectories of Single Photons in a Two-Slit Interferometer, Science **332**, 1170 (2011).

[30] F. Piacentini, A. Avella, M. P. Levi, M. Gramegna, G. Brida, I. P. Degiovanni, E. Cohen, R. Lussana, F. Villa, A. Tosi, F. Zappa, and M. Genovese, Measuring Incompatible Observables by Exploiting Sequential Weak Values, Physical Review Letters **117**, 170402 (2016).

[31] J.-S. Chen, M.-J. Hu, X.-M. Hu, B.-H. Liu, Y.-F. Huang, C.-F. Li, C.-G. Guo, and Y.-S. Zhang, Experimental realization of sequential weak measurements of non-commuting Pauli observables, Optics Express **27**, 6089 (2019), arXiv:1805.02235.

[32] J. S. Lundeen, B. Sutherland, A. Patel, C. Stewart, and C. Bamber, Direct measurement of the quantum wavefunction, Nature **474**, 188 (2011), arXiv:1112.3575.

[33] G. Vallone and D. Dequal, Strong Measurements Give a Better Direct Measurement of the Quantum Wave Function, Physical Review Letters **116**, 040502 (2016), arXiv:1711.00764.

[34] G. S. Thekkadath, L. Giner, Y. Chalich, M. J. Horton, J. Banker, and J. S. Lundeen, Direct Measurement of the Density Matrix of a Quantum System, Physical Review Letters **117**, 120401 (2016), arXiv:1604.07917.

[35] L. Calderaro, G. Foletto, D. Dequal, P. Villoresi, and G. Vallone, Direct Reconstruction of the Quantum Density Matrix by Strong Measurements, Physical Review Letters **121**, 230501 (2018), arXiv:1803.10703.

[36] M. Schiavon, L. Calderaro, M. Pittaluga, G. Vallone, and P. Villoresi, Three-observer Bell inequality violation on

a two-qubit entangled state, Quantum Science and Technology **2**, 015010 (2017), arXiv:1611.02430.

[37] A. Avella, F. Piacentini, M. Borsarelli, M. Barbieri, M. Gramegna, R. Lussana, F. Villa, A. Tosi, I. P. Degiovanni, and M. Genovese, Anomalous weak values and the violation of a multiple-measurement Leggett-Garg inequality, Physical Review A **96**, 052123 (2017), arXiv:1706.02120.

[38] A. Tavakoli and A. Cabello, Quantum predictions for an unmeasured system cannot be simulated with a finite-memory classical system, Physical Review A **97**, 032131 (2018).

[39] M.-J. Hu, Z.-Y. Zhou, X.-M. Hu, C.-F. Li, G.-C. Guo, and Y.-S. Zhang, Observation of non-locality sharing among three observers with one entangled pair via optimal weak measurement, npj Quantum Information **4**, 63 (2018), arXiv:1609.01863.

[40] G. Foletto, L. Calderaro, A. Tavakoli, M. Schiavon, F. Picciariello, A. Cabello, P. Villoresi, and G. Vallone, Experimental Demonstration of Sustained Entanglement and Nonlocality After Sequential Measurements, Physical Review Applied **13**, 044008 (2020), arXiv:1906.07412.

[41] K. Mohan, A. Tavakoli, and N. Brunner, Sequential random access codes and self-testing of quantum measurement instruments, New Journal of Physics **21**, 083034 (2019), arXiv:1905.06726.

[42] G. Foletto, L. Calderaro, G. Vallone, and P. Villoresi, Experimental demonstration of sequential quantum random access codes, Phys. Rev. Research **2**, 033205 (2020).

[43] 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, Physical Review Letters **125**, 080403 (2020).

[44] F. J. Curchod, M. Johansson, R. Augusiak, M. J. Hoban, P. Wittek, and A. Acín, Unbounded randomness certification using sequences of measurements, Physical Review A **95**, 020102(R) (2017), arXiv:1510.03394.

[45] B. Coyle, M. J. Hoban, and E. Kashefi, One-Sided Device-Independent Certification of Unbounded Random Numbers, Electronic Proceedings in Theoretical Computer Science **273**, 14 (2018), arXiv:1806.10565.

[46] J.-A. Larsson, Loopholes in Bell inequality tests of local realism, Journal of Physics A: Mathematical and Theoretical **47**, 424003 (2014), arXiv:1407.0363.

[47] A. Acín, S. Massar, and S. Pironio, Randomness versus Nonlocality and Entanglement, Physical Review Letters **108**, 100402 (2012).

[48] H. S. Poh, S. K. Joshi, A. Cerè, A. Cabello, and C. Kurtsiefer, Approaching Tsirelson's Bound in a Photon Pair Experiment, Physical Review Letters **115**, 180408 (2015), arXiv:1506.01865.

[49] Y. Zhang, Y. He, J. Wu, X. Jiang, R. Liu, C. Qiu, X. Jiang, J. Yang, C. Tremblay, and Y. Su, High-extinction-ratio silicon polarization beam splitter with tolerance to waveguide width and coupling length variations, Optics Express **24**, 6586 (2016).

[50] C. Li and D. Dai, Compact polarization beam splitter for silicon photonic integrated circuits with a 340-nm-thick silicon core layer, Optics Letters **42**, 4243 (2017).

[51] J. R. Ong, T. Y. L. Ang, E. Sahin, B. Pawlina, G. F. R. Chen, D. T. H. Tan, S. T. Lim, and C. E. Png, Broadband silicon polarization beam splitter with a high extinction ratio using a triple-bent-waveguide directional coupler, Optics Letters **42**, 4450 (2017).

[52] E. Meyer-Scott, N. Prasannan, C. Eigner, V. Quiring, J. M. Donohue, S. Barkhofen, and C. Silberhorn, High-performance source of spectrally pure, polarization entangled photon pairs based on hybrid integrated-bulk optics, Optics Express **26**, 32475 (2018), arXiv:1807.10092.

[53] J. Wang, S. Paesani, Y. Ding, R. Santagati, P. Skrzypczyk, A. Salavrakos, J. Tura, R. Augusiak, L. Mančinska, D. Bacco, D. Bonneau, J. W. Silverstone, Q. Gong, A. Acín, K. Rottwitt, L. K. Oxenløwe, J. L. O'Brien, A. Laing, and M. G. Thompson, Multidimensional quantum entanglement with large-scale integrated optics, Science **360**, 285 (2018), arXiv:1803.04449.

[54] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland, and J. M. Martinis, Superconducting quantum circuits at the surface code threshold for fault tolerance, Nature **508**, 500 (2014).

[55] C. J. Ballance, T. P. Harty, N. M. Linke, M. A. Sepiol, and D. M. Lucas, High-Fidelity Quantum Logic Gates Using Trapped-Ion Hyperfine Qubits, Physical Review Letters **117**, 060504 (2016), arXiv:1512.04600.

[56] J. Bowles, F. Baccari, and A. Salavrakos, Bounding sets of sequential quantum correlations and device-independent randomness certification, Quantum **4**, 344 (2020), arXiv:1911.11056.