Experimental demonstration of sequential quantum random access codes

Giulio Foletto,1,* Luca Calderaro,1,2 Giuseppe Vallone,1,2 and Paolo Villoresi1
1Dipartimento di Ingegneria dell’Informazione, Università di Padova, via Gradenigo 6B, 35131 Padova, Italy
2Dipartimento di Fisica e Astronomia, Università di Padova, via Marzolo 8, 35131 Padova, Italy

(Received 17 January 2020; accepted 24 June 2020; published 6 August 2020)

A random access code (RAC) is a communication protocol that requires a transmitter (Alice) to encode a message into a shorter one in a way that any bit of the original can still be recovered with nontrivial probability. Encoding with quantum bits rather than classical ones can improve this probability but has an important limitation: Due to the disturbance caused by standard quantum measurements, qubits cannot be used more than once. However, as recently shown by Mohan, Tavakoli, and Brunner [New J. Phys. 21, 083034 (2019)], weak measurements can alleviate this problem, allowing two sequential decoders to perform better than with the best classical RAC. We use single photons to experimentally show that these weak measurements are feasible and nonclassical success probabilities are achievable by two decoders. We prove this for different values of the measurement strength and use our experimental results to put tight bounds on them, certifying the accuracy of our setting. This proves the feasibility of using sequential quantum RACs for quantum information tasks, such as the self-testing of untrusted devices.

DOI: 10.1103/PhysRevResearch.2.033205

I. INTRODUCTION

A random access code (RAC) is a communication protocol that requires a transmitter (Alice) to encode a n-bit long random sequence into a shorter m-bit message, and a receiver (Bob) to be able to decode any of the n bits with nontrivial probability \( p > 1/2 \). These parameters are often grouped in expression \( n \rightarrow m \) that describes the task. A quantum random access code (QRAC) is the very similar situation in which Alice sends \( m \) qubits rather than bits. This concept was introduced by Wiesner [1] but caught the interest of the scientific community only after subsequent research by Ambainis et al. [2] who showed quantum strategies that achieve \( 2 \rightarrow 1 \) and \( 3 \rightarrow 1 \), which beat the best classical RACs for these choices of \( n, m \). Further studies found that a \( 4 \rightarrow 1 \) QRAC that reaches \( p > 1/2 \) does not exist [3], but a \( 4^n \rightarrow 1 \) always does [4]. Other investigations considered different values of \( n, m \) [5], the use of qubits (d-level quantum systems) rather than qubits [6–8], or the request of decoding more than 1 bit [9]. Applications include communication complexity [10], network coding [11], locally decodable codes [12], dimension witnessing of quantum states [13], self-testing of quantum devices [14,15], semi-device-independent quantum randomness extraction (SDI-QRE) [16–18], and semi-device-independent key distribution (SDI-QKD) [19,20].

Recently, improvements in the theory and implementation of weak and sequential quantum measurements [21–27], prompted the introduction of sequential QRACs by Mohan, Tavakoli, and Brunner (MTB) in what follows [28]. Their protocol is a variation of the \( 2 \rightarrow 1 \) QRAC: Alice encodes a two-bit message into 1 qubit and sends it to Bob, who, after measuring it, forwards the resulting quantum state to a third party (Charlie) who shares the same goal as Bob: decoding any of the two bits of Alice with nontrivial probability \( p > 1/2 \). The core tenets of quantum physics remind us that Bob’s measurement disturbs the initial state, making it more difficult for Charlie to extract information from it. However, if Bob uses weak measurements rather than projective ones, he can tune this disturbance and give back some information to Charlie at the cost of some of his own. This means that Alice’s qubit can be used more than once, overcoming a crucial limit of previously studied QRACs, but there is a trade-off between Bob’s and Charlie’s attainable information that depends on Bob’s measurement strength. The observation of decoding probabilities that saturate this trade-off self-tests the use of a unique set of states and measurements under the assumption that states are two dimensional and measurements have binary outcomes. Additionally, even imperfect results can bind Bob’s measurement strength. This can be important for the characterization of untrusted quantum devices.

In this paper, we verify MTB’s protocol in a quantum optics experiment for different values of the strength parameter. We show that it is possible to observe near-optimal decoding probabilities and we put tight bounds on Bob’s strength using MTB’s self-testing expressions. Finally, we discuss some applications of these results.

II. MODEL

We briefly introduce the quantitative relations presented by MTB and add some comments. Let \( x = (x_0, x_1) \in \{0, 1\}^2 \) be the two-bit sequence that Alice wants to encode. Let \( y \) and \( z \in \{0, 1\} \) label the positions of the bit in \( x \) that Bob...
and Charlie randomly choose, respectively, to decode. Finally, let \( b \) and \( c \) be the results of Bob and Charlie’s respective measurements, associating bit 0 with outcome +1 and bit 1 with −1. We define the two correlation witnesses,

\[
W_{AB} = \frac{1}{8} \sum_{x,y} p(b = x, y),
\]

(1)

\[
W_{AC} = \frac{1}{8} \sum_{x,z} p(c = x, z),
\]

(2)

which quantify the probabilities that Bob and Charlie correctly decode the bit they are interested in, averaged over all possible input sequences and bit choices.

If the parties use classical physics, these probabilities are independent of each other and limited by \( W_{AB}, W_{AC} \leq \frac{1}{2} \). This upper bound is reached, for example, if Alice sends the first of her bits, meaning that when Bob and Charlie want to decode the second, they can only guess. Yet, MTB found that the two decoders can both violate this limit in a quantum scenario. The aforementioned trade-off between the information that each of them can extract translates into an upper bound to \( W_{AC} \) that depends on the attained value of \( W_{AB} \). In particular,

\[
W_{AC} \leq \frac{1}{8} (4 + \sqrt{2} + \sqrt{16W_{AB} - 16W_{AB}^2 - 2}),
\]

(3)

with \( W_{AB} \) itself being limited by previous results at \( W_{AB} \leq \frac{1}{2} + \frac{\sqrt{2}}{2} \) [2]. MTB also proposed a strategy to saturate this trade-off and proved that it is unique up to unitary transformations and under the assumption that Alice’s state is two dimensional and all measurements have binary outcomes. This strategy reads

(C1) Alice encodes her two-bit sequence \( x = (x_0, x_1) \) into one of four pure states and sends it to Bob. These states form the angles of a square in the XZ equatorial line of the Bloch sphere and are equidistant from the eigenstates of \( \sigma_X \) and \( \sigma_Z \) \( \varphi \sigma_\pm = \frac{1}{2}[1 + (-1)^{\eta}\eta^\sigma_\pm + (-1)^{\eta}\eta^\sigma_\pm] \).

(C2) Bob weakly measures \( \sigma_\pm \) if \( y = 0 \) or \( \sigma_X \) if \( y = 1 \) on the qubit with strength parameter labeled \( \eta \) \( \in [0, 1] \) as in Ref. [28]. The first case \( (y = 0) \) entails using the two-outcome positive operator-valued measure (POVM) (\( M_{b|0}, b \in \{0, 1\} \)) where \( M_{b|0} = \frac{1}{2}[1 + (-1)^{\eta}\eta^{\sigma_X}] \). The state is transformed according to Kraus operator \( K_{b|0} = \frac{1}{2}[(cos \mu + sin \mu)1 + (-1)^{\eta}(cos \mu - sin \mu)\sigma_X] \), where \( \mu = \frac{1}{2} \arccos(\eta) \). In this way, \( K_{0|0} K_{0|0} - K_{1|0} K_{1|0} = M_{0|0} - M_{1|0} = \eta \sigma_X \). The second case \( (y = 1) \) is similar with \( \sigma_X \) replaced by \( \sigma_Z \). Bob then sends the resulting state to Charlie.

(C3) Charlie performs projective measurements of \( \sigma_X \) if \( z = 0 \) or \( \sigma_Z \) if \( z = 1 \).

In this situation, the following relations hold:

\[
W_{AB} = \frac{1}{2} + \frac{\sqrt{2}}{4} \eta,
\]

(4)

\[
W_{AC} = \frac{1}{2} + \frac{\sqrt{2}}{4} \left(1 + \sqrt{1 - \eta^2}\right),
\]

(5)

which, when combined, make Expression (3) an equality. Notably, at least, one of these witnesses is always above the classical limit of \( \frac{1}{2} \) and if \( \eta \in [\frac{1}{\sqrt{2}}, \sqrt{2\sqrt{2}-2}] \) both are. For \( \eta = \frac{1}{\sqrt{2}} \), they take the same value of \( \frac{1}{2} + \frac{\sqrt{2}}{4} \).

However, we add that this strategy cannot be straightforwardly extended to a third decoder. Even if Charlie also uses weak measurements with strength \( \eta' \) and relays the resulting qubit to David, there are no values of \( (\eta, \eta') \) that provide correlation witnesses greater than \( \frac{1}{2} + \frac{\sqrt{2}}{4} \) for all three decoders. We show this in Appendix A finding similar results to those attained in the context of the Clauser-Horne-Shimony-Holt inequality [29].

One can wonder whether MTB’s protocol can improve the decoding probability of the entire input sequence. In a communication scenario in which Bob and Charlie cooperate and agree to always decode different bits, the joint probability of both being correct follows the law:

\[
W_{ABC} = \frac{1}{8} \sum_{x,y,z} p(b = x, c = x, y, z \neq y)
\]

\[
= \frac{1}{4} \left(1 + \sqrt{1 - \eta^2}\right).
\]

(6)

It holds that \( W_{ABC} \leq \frac{1}{2} \) with the bound reached only for \( \eta = \frac{1}{\sqrt{2}} \). This agrees with the limits present in the literature: a \( m \)-qubit system cannot make the decoding probability of a \( n \)-bit message better than \( 2^m / 2^n \) [5, Theorem 2.4.2].

The uniqueness of the strategy consisting of C1–C3 allows MTB to conclude that finding \( W_{AB} \) and \( W_{AC} \) correlated to saturate Expression (3) self-tests that the state preparation was that of C1 and the measurements were those of C2 and C3. This is an important result for protocols of SDI-QRE or SDI-QKD in which devices cannot be trusted, and their behavior can be checked only from the outcomes they provide. Moreover, even if the values of the witnesses are suboptimal, they still give a lower and an upper bound on parameter \( \eta \),

\[
\eta \geq \eta_{low} = \sqrt{\frac{2}{2}} (2W_{AB} - 1),
\]

(7)

\[
\eta \leq \eta_{up} = 2\sqrt{2} (2W_{AC} - 1),
\]

(8)

which become tight when conditions C1–C3 are fulfilled. These bounds can also be extended to self-tests on the incompatibility between Bob’s measurements [30], which is a crucial resource for many quantum information tasks. For instance, \( W_{AB} \) and \( W_{AC} \) can be used as self-tests for the characterization of the QKD state decoders even if the optimal conditions are not reached.

Finally, we add that trade-off (3) and its inverse,

\[
W_{AB} \leq \frac{1}{2} \left[1 + \sqrt{4(4 + 2W_{AC} - 16W_{AC}^2 - 4 - 2\sqrt{2})}\right]
\]

(9)

can provide a security bound in an adversarial scenario in which Alice and Charlie try to detect a man in the middle (Bob) or infer the properties of his actions. In particular, if \( W_{AC} > \frac{1}{2} + \frac{\sqrt{2}}{4} \approx 0.783 \), then \( W_{AC} > W_{AB} \) (see Fig. 3), meaning that Alice and Charlie can extract a cryptographic key secure from Bob’s eavesdropping using a SDI-QKD protocol, such as that of Ref. [19]. Compared to the one present in the latter, Eq. (9) is a tighter upper bound on \( W_{AB} \) and, in turn, on the mutual information between the legitimate parties’ key and the eavesdropper’s. Therefore, the performance of the protocol would be increased, although, here, we have the
additional assumption that Bob’s measurements have binary outcomes.

III. METHOD

Our experiment aims at verifying all these relations and showing that it is feasible to meet conditions C1–C3 and find the optimal trade-off. We also use Eqs. (7) and (8) to bound the value of η. We choose single photons as our experimental platform and their polarization as the degree of freedom that encodes the information. We produce photon pairs at 808 nm through spontaneous parametric down-conversion using a periodically poled potassium titanyl phosphate crystal in a type-II collinear-phase-matching configuration so that the generated state after the polarizing beam splitter (PBS) is $|\psi\rangle = |H\rangle_{A} |V\rangle_{\text{herald}}$ [31]. One photon of each pair is selected in the $|V\rangle$ polarization to filter out imperfections in state preparation and background light and is sent to a single-photon avalanche diode (SPAD) detector. Its presence heralds the other photon of the pair which reaches the core of the setup.

This is divided into three stages that play the role of Alice, Bob, and Charlie as shown in Fig. 1. First, Alice changes the state from $|H\rangle = |\text{herald}\rangle |\psi\rangle (|\psi\rangle |\text{herald}\rangle)_{\text{herald}}$ to one of the four optimal states of condition C1 using a pair of HWPs. Bob carries out the weak measurement with a MZI based on polarizing beam displacers [(PBDs), Thorlabs BD40]. A first PBD entangles polarization with the path qubit, then the two arms encounter one HWP each, HWP$_{\text{H}}$ and HWP$_{V}$ in Fig. 1 with axes at angles 0 and $\pi/4$ relative to the horizontal direction defined by $|H\rangle$. HWP$_{\text{COM}}$ spans across both arms and sets the strength of the measurement through its angle $\theta = \frac{\pi}{2} \arccos(\eta)$. A second PBD has the dual purpose of closing the interferometer and performing the measurement. It does this by selecting the outcome 0 and sending the corresponding photons to the one exit that continues to the rest of the setup where they meet a HWP at angle $\pi/4$. This MZI + HWP scheme implements $K_{00}$: Two more HWPs, one before and one after it, can be rotated to select the other outcome or change the measurement basis. This means that Bob’s apparatus observes one outcome at a time; extensions that allow observing both in separate exits, thus, performing a full measurement, are possible (see Appendix B) but beyond the scope of this experiment. Charlie’s measurements are projective, therefore, his setup consists of a fixed linear polarizer (LP) preceded by a HWP that selects one combination of basis and outcome at a time. To reduce the number of components, we replaced the two groups of three consecutive HWPs with a single HWP each, which is controlled by two parties (HWP$_{\text{AB}}$ and HWP$_{\text{BC}}$ in Fig. 1). Finally, light is coupled into a single-mode fiber and sent to a SPAD detector. Its electrical signals are correlated with those of the herald and coincidences (within a ±1-ns window) are counted for a fixed exposure time of 2 s. The total number of coincidences in this time and for each measurement choice is approximately $8 \times 10^3$.

Our implementation represents a proof of principle demonstration of a QRAC without active random choice of preparation and measurements. Moreover, Bob and Charlie do not observe their outcomes independently, but only when the detectors at the end of the setup click. We iterate sequentially over all the possible configurations of preparation ($x$), measurement choice ($y$, $z$), and outcome ($b$, $c$) by rotating HWP$_{\text{AB}}$ and HWP$_{\text{BC}}$, whose angles are listed in Table I (Appendix C). For each, we record the number of coincident counts. These are proportional to the joint probability of the outcomes selected by Bob and Charlie, and we use them to compute the conditional probabilities required by Eqs. (1) and (2) to find the correlation witnesses.

IV. RESULTS

We measure $W_{\text{AB}}$ and $W_{\text{AC}}$ for 11 different values of the strength parameter, equally spaced in [0, 1]. We use the HWP inside Bob’s MZI to set its value of $\eta_{\text{set}}$. All the results that we report here are extracted from the same experimental data.

Figure 2 plots $W_{\text{AC}}$ as a function of $W_{\text{AB}}$ and compares it with the optimal trade-off that saturates Expression (3). The quantum features of the experiment are most evident from the fact that not only all points are outside of the classical region, but also they lie on the boundary of the set of quantum correlations between the witnesses, which certifies that we were able to match the optimal conditions C1–C3.

Figure 3 compares the individual witnesses with the expected values of Eqs. (4) and (5). We clearly see that we could sample the very interesting region in which both $W_{\text{AB}}$ and $W_{\text{AC}}$ are nonclassical.

Figure 4 confirms the validity of Eq. (6) and shows that if Bob and Charlie cooperate to decode the entire input sequence, they cannot succeed with probability better than $\frac{1}{4}$. However, this scheme does allow them to saturate the upper bound for a specific measurement strength.

Finally, we evaluated the self-testing capabilities of the protocol, computing upper and lower bounds on $\eta$ from the experimental $W_{\text{AB}}$ and $W_{\text{AC}}$ using Eqs. (7) and (8). Figure 5 plots them as a function of $\eta_{\text{set}}$. The tightness of the bounds is another proof that our setup achieved the optimal conditions C1–C3.

V. DISCUSSION

Our experiment confirms the relations presented by MTB and proves that it is possible for two decoders in a QRAC to share higher success probabilities than admitted by classical
The quantum weak measurement is the key to this as it allows reducing the disturbance on the state observed by the first decoder so that it can be used again by the second. This is a new situation in which weak measurements prove to be useful and to be able to overcome the limitations of axiomatic projective measurements.

A crucial point of this protocol is that it offers a different way to self-test quantum devices with limited assumptions: Observing the optimal values of $W_{AB}$ and $W_{AC}$ pinpoints (up to unitary transformations) Alice’s state preparation and Bob and Charlie’s measurements. Even without optimality, some properties of Bob’s measurements can be bounded. This is important for the characterization of setups that implement qubit measurements and require accurate strength setting or exploit incompatibility. We have also shown that the concept of sequential QRACs can provide a security bound for a SDI-QKD scenario. Additionally, in a communication scenario in which Bob and Charlie cooperate to decode the entirety of Alice’s string, there is one value of strength that can reach the performance limit imposed by information theory.

It would also be interesting to study robust self-testing relations for MTB’s scheme that can bound other properties of the quantum devices in suboptimal conditions. If needed, other assumptions could be added, e.g., perfect knowledge of
Alice’s preparations could help characterize Bob and Charlie’s operations in a measurement-device-independent scenario.

Finally, extensions of Bob’s MZI scheme that allow full polarization measurements should be explored, considering also an implementation in integrated optics where polarizing directional couplers and polarization rotators are now feasible and could provide better accuracy than free-space discrete components [32–35].

ACKNOWLEDGMENTS

The authors would like to thank M. Avesani for the useful conversations about information theory and F. Picciariello for his contribution to setting up the experiment. Part of this work was supported by MIUR (Italian Ministry of Education, University and Research) under the initiative “Departments of Excellence” (Law No. 232/2016).

APPENDIX A: EXTENSION OF THE PROTOCOL TO MORE RECEIVERS

The protocol can be extended to any number of receivers if they all use weak measurements like Bob. However, we show here that this strategy does not allow more than two receivers two achieve correlation witnesses higher than $\frac{1}{2}$ together. Suppose the first receiver (Bob) uses strength parameter $\eta_1$, then,

$$W_{AB}(\eta_1) = \frac{1}{8} \sum_{x,y} \text{tr}(\rho_x M_{x|y}) = \frac{1}{2} + \frac{\sqrt{2}}{4} \eta_1, \quad (A1)$$

where $\rho_x = \frac{1}{2} (\mathbb{1} + (-1)^{y} X_{x} + (-1)^{y} X_{\bar{x}})$ is the state prepared by Alice and $M_{b|y}$ are the operators,

$$M_{0|0} = \frac{1}{2}(\mathbb{1} + \eta_1 X_{\bar{x}}),$$
$$M_{1|0} = \frac{1}{2}(\mathbb{1} - \eta_1 X_{\bar{x}}),$$
$$M_{0|1} = \frac{1}{2}(\mathbb{1} + \eta_1 Z_{\bar{x}}),$$
$$M_{1|1} = \frac{1}{2}(\mathbb{1} - \eta_1 Z_{\bar{x}}). \quad (A2)$$

Note that $\{M_{0|0}, M_{1|0}\}$ and $\{M_{0|1}, M_{1|1}\}$ are two two-outcome POVMs, indeed, $\sum_y M_{b|y} = \mathbb{1}, \forall y$. Moreover $\sum_y (-1)^y M_{b|y} = \eta_1 X_{\bar{x}}$ and $\sum_y (-1)^y M_{b|\bar{y}} = \eta_1 Z_{\bar{x}}$, which is why these POVMs correspond to weak measurements of $X_{\bar{x}}$ and $Z_{\bar{x}}$, respectively. To each $M_{b|y}$ corresponds a Kraus operator $K_{b|y}$ such that $K_{b|y}^\dagger K_{b|y} = M_{b|y}$,

$$K_{0|0} = \frac{1}{2}[(\cos \mu_1 + \sin \mu_1)\mathbb{1} + (\cos \mu_1 + \sin \mu_1)X_{\bar{x}}],$$
$$K_{1|0} = \frac{1}{2}[(\cos \mu_1 + \sin \mu_1)\mathbb{1} - (\cos \mu_1 + \sin \mu_1)X_{\bar{x}}],$$
$$K_{0|1} = \frac{1}{2}[(\cos \mu_1 + \sin \mu_1)\mathbb{1} + (\cos \mu_1 + \sin \mu_1)Z_{\bar{x}}],$$
$$K_{1|1} = \frac{1}{2}[(\cos \mu_1 + \sin \mu_1)\mathbb{1} - (\cos \mu_1 + \sin \mu_1)Z_{\bar{x}}]. \quad (A3)$$

where $\mu_1 = \frac{1}{2} \arccos(\eta_1)$.

The second receiver (Charlie) ignores Bob’s measurement choice $y$ and outcome $b$, therefore, his correlation witness must be calculated from the postmeasurement state averaged over $y$ and $b$,

$$\varrho_{b}^{C} = \frac{1}{2} \sum_{y,b} K_{b|y} \rho_x K_{b|y}^\dagger = \frac{1}{2} \left( \mathbb{1} + \frac{1 - \eta_1^2}{2} (-1)^{y} X_{\bar{x}} + (-1)^{y} Z_{\bar{x}} \right). \quad (A4)$$

This expression is remarkably similar to the initial state $\rho_x$ but contains factor $\frac{1 + \sqrt{1 - \eta_1^2}}{2}$ that shortens the Bloch vector of the state. Supposing that Charlie also performs weak measurements with strength parameter $\eta_2$, his correlation witness is as follows:

$$W_{AC}(\eta_1, \eta_2) = \frac{1}{8} \sum_{x,z} \text{tr}(\varrho_{x}^{C} M_{x|z})$$
$$= \frac{1}{2} \left( \mathbb{1} + \frac{\sqrt{2}}{4} \eta_2 + \sqrt{1 - \eta_1^2} \frac{1 + \sqrt{1 - \eta_1^2}}{2} \right). \quad (A5)$$

which coincides with Eq. (5) for $\eta_2 = 1$.

This can continue for any number of receivers, and the witness for the $n$th one is as follows:

$$W_{A_{Bn}}(\eta_1 \cdots \eta_n) = \frac{1}{2} + \frac{\sqrt{2}}{4} \eta_n \prod_{i=1}^{n-1} \frac{1 + \sqrt{1 - \eta_i^2}}{2}. \quad (A6)$$

This is an increasing function of $\eta_n$ but a decreasing one of $\eta_i$, $\forall i < n$. It can be seen as a generalization of Eq. (15) of Ref. [28] and is similar to Eq. (24) of Ref. [29] (for the case of $n = 3$), which was obtained in the context of Bell inequality violations.

We can see from Eq. (A1) that $W_{AB} > \frac{3}{4}$ for $\eta_1 = \frac{1}{\sqrt{2}} + \epsilon_1, \forall \epsilon_1 > 0$. Plugging this value into Eq. (A5) shows that $W_{AC} > \frac{3}{4}$ for $\eta_2 = 2(\sqrt{2} - 1) + \epsilon_2, \forall \epsilon_2 > (6\sqrt{2} - 8)\epsilon_1 + \ldots$
| Settings | Angles (rad) | Coincident counts in 2 s, $\eta_{cm} = \cdots$ |
|----------|-------------|---------------------------------------------|
| $x_0$   | $x_1$  | $y$   | $b$  | $z$  | $c$ | HWP$_{AB}$ | HWP$_{BC}$ |
| 0       | 0      | 0     | 0    | 0    | 0  | 0.1       | 0.2         | 0.3       | 0.4       | 0.5       | 0.6       | 0.7       | 0.8       | 0.9       | 1         |
| 0       | 0      | 0     | 0    | 0    | 0  | 0.1       | 0.2         | 0.3       | 0.4       | 0.5       | 0.6       | 0.7       | 0.8       | 0.9       | 1         |
| 0       | 0      | 0     | 0    | 0    | 0  | 0.1       | 0.2         | 0.3       | 0.4       | 0.5       | 0.6       | 0.7       | 0.8       | 0.9       | 1         |

---

**Table 1.** HWP angles and coincident counts for each configuration of $x_0$, $x_1$, $y$, $b$, $z$, and $c$.
ever, if implemented with discrete optical table components, allow better accuracy in a much more compact setup. How-

to integrated optics should be explored, because direct
translations of PBSs and wave plates exist [32,35] and could
idea to integrated optics should be explored, because direct
translations of PBSs and wave plates exist [32,35] and could

this scheme has the disadvantage that PBS-based MZIs are
difficult to align. A more practical idea is the use of large
PBDs that offer three exits, two of which would correspond
to the other measurement outcome. They would still need
to be recombined with further PBDs, which, if identical to
the ones in the MZI, would not ruin the optical coherence.
The beams could then reach Charlie, who could implement
a full measurement using a PBS and two detectors for each
input beam. HWPs would need to be rotated only to select the
measurement basis. Figure 6 depicts this idea.

Note that, with this scheme, Charlie would know Bob’s
outcome by observing which detector clicks. If this informa-
tion cannot be simply ignored and must be physically erased,
one can imagine to further recombine Bob’s exit beams using
a (nonpolarizing) beam splitter and delay lines before reaching
a single PBS in Charlie’s setup.

APPENDIX B: FULL MEASUREMENTS WITH THE
MACH-ZEHNDER INTERFEROMETER

The apparatus made up of a MZI and a HWP that Bob
uses to perform the weak polarization measurements can
only implement one Kraus operator at a time. As described
in Sec. III, it is possible to switch from one to another by
rotating HWPs before and after the MZI. However, there are
many ways to change the scheme to make a full measure-
ment possible without moving optical components. One is the
replacement of PBDs with polarizing beam splitters which
would make both exits available. A more detailed description
of this proposal is in Ref. [27]. The feasibility of bringing this
idea to integrated optics should be explored, because direct
translations of PBSs and wave plates exist [32,35] and could
allow better accuracy in a much more compact setup. How-
ever, if implemented with discrete optical table components,

the beams could then reach Charlie, who could implement
a full measurement using a PBS and two detectors for each
input beam. HWPs would need to be rotated only to select the
measurement basis. Figure 6 depicts this idea.

Note that, with this scheme, Charlie would know Bob’s
outcome by observing which detector clicks. If this informa-
tion cannot be simply ignored and must be physically erased,
one can imagine to further recombine Bob’s exit beams using
a (nonpolarizing) beam splitter and delay lines before reaching
a single PBS in Charlie’s setup.

APPENDIX B: FULL MEASUREMENTS WITH THE
MACH-ZEHNDER INTERFEROMETER

The apparatus made up of a MZI and a HWP that Bob
uses to perform the weak polarization measurements can
only implement one Kraus operator at a time. As described
in Sec. III, it is possible to switch from one to another by
rotating HWPs before and after the MZI. However, there are
many ways to change the scheme to make a full measure-
ment possible without moving optical components. One is the
replacement of PBDs with polarizing beam splitters which
would make both exits available. A more detailed description
of this proposal is in Ref. [27]. The feasibility of bringing this
idea to integrated optics should be explored, because direct
translations of PBSs and wave plates exist [32,35] and could
allow better accuracy in a much more compact setup. How-
ever, if implemented with discrete optical table components,
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, Phys. Rev. Lett. 60, 1351 (1988).

G. Mitchison, R. Jozsa, and S. Popescu, Sequential weak measurement, Phys. Rev. A 76, 062105 (2007).

M. Schiavon, L. Calderaro, M. Pittaluga, G. Vallone, and P. Villalessi, Three-observer Bell inequality violation on a two-qubit entangled state, Quantum Sci. Technol. 2, 015010 (2017).

H.-W. Li, Y.-S. Zhang, X.-B. An, Z.-F. Han, and G.-C. Guo, Three-observer classical dimension witness violation with weak measurement, Commun. Phys. 1, 10 (2018).

X.-B. An, H.-W. Li, Z.-Q. Yin, M.-J. Hu, W. Huang, B.-J. Xu, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Experimental three-party quantum random number generator based on dimension witness violation and weak measurement, Opt. Lett. 43, 3437 (2018).

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, Opt. Express 27, 6089 (2019).

G. Foletto, L. Calderaro, A. Tavakoli, M. Schiavon, F. Picciariello, A. Cabello, P. Villalessi, and G. Vallone, Experimental demonstration of sustained entanglement and nonlocality after sequential measurements, Phys. Rev. Appl. 13, 044008 (2020).

K. Mohan, A. Tavakoli, and N. Brunner, Sequential random access codes and self-testing of quantum measurement instruments, New J. Phys. 21, 083034 (2019).

S. Mal, A. Majumdar, and D. Home, Sharing of nonlocality of a single member of an entangled pair of qubits is not possible by more than two unbiased observers on the other wing, Mathematics 4, 48 (2016).

H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, Experimental characterisation of unsharp qubit measurements in a semi-device-independent setting, arXiv:2001.04768.

L. Calderaro, G. Foletto, D. Dequal, P. Villalessi, and G. Vallone, Direct reconstruction of the quantum density matrix by strong measurements, Phys. Rev. Lett. 121, 230501 (2018).

G. Corrielli, A. Crespi, R. Geremia, R. Ramponi, L. Sansoni, A. Santinelli, P. Mataloni, F. Sciarrino, and R. Osellame, Rotated waveplates in integrated waveguide optics, Nat. Commun. 5, 4249 (2014).

L. Gao, Y. Huo, K. Zang, S. Paik, Y. Chen, J. S. Harris, and Z. Zhou, On-chip plasmonic waveguide optical waveplate, Sci. Rep. 5, 15794 (2015).

J. D. Sarmento-Merenguel, R. Halir, X. Le Roux, C. Alonso-Ramos, L. Vivien, P. Cheben, E. Durán-Valdeiglesias, I. Molina-Fernández, D. Marris-Morini, D.-X. Xu, J. H. Schmid, S. Janz, and A. Ortega-Moñux, Demonstration of integrated polarization control with a 40 dB range in extinction ratio, Optica 2, 1019 (2015).

I. Pitiños, F. Samara, G. Corrielli, A. Crespi, and R. Osellame, Geometrically-controlled polarization processing in femtosecond-laser-written photonic circuits, Sci. Rep. 7, 11342 (2017).

H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, Experimental demonstration of sustained entanglement and nonlocality after sequential measurements, Phys. Rev. Appl. 13, 044008 (2020).

K. Mohan, A. Tavakoli, and N. Brunner, Sequential random access codes and self-testing of quantum measurement instruments, New J. Phys. 21, 083034 (2019).

S. Mal, A. Majumdar, and D. Home, Sharing of nonlocality of a single member of an entangled pair of qubits is not possible by more than two unbiased observers on the other wing, Mathematics 4, 48 (2016).

H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, Experimental characterisation of unsharp qubit measurements in a semi-device-independent setting, arXiv:2001.04768.

L. Calderaro, G. Foletto, D. Dequal, P. Villalessi, and G. Vallone, Direct reconstruction of the quantum density matrix by strong measurements, Phys. Rev. Lett. 121, 230501 (2018).

G. Corrielli, A. Crespi, R. Geremia, R. Ramponi, L. Sansoni, A. Santinelli, P. Mataloni, F. Sciarrino, and R. Osellame, Rotated waveplates in integrated waveguide optics, Nat. Commun. 5, 4249 (2014).

L. Gao, Y. Huo, K. Zang, S. Paik, Y. Chen, J. S. Harris, and Z. Zhou, On-chip plasmonic waveguide optical waveplate, Sci. Rep. 5, 15794 (2015).

J. D. Sarmento-Merenguel, R. Halir, X. Le Roux, C. Alonso-Ramos, L. Vivien, P. Cheben, E. Durán-Valdeiglesias, I. Molina-Fernández, D. Marris-Morini, D.-X. Xu, J. H. Schmid, S. Janz, and A. Ortega-Moñux, Demonstration of integrated polarization control with a 40 dB range in extinction ratio, Optica 2, 1019 (2015).

I. Pitiños, F. Samara, G. Corrielli, A. Crespi, and R. Osellame, Geometrically-controlled polarization processing in femtosecond-laser-written photonic circuits, Sci. Rep. 7, 11342 (2017).