Experimental Noise-Resilient Quantum Random Access Code

H. S. Karthik[‡,1,*] S. Gómez[‡,2,3,†] F. M. Quinteros,[2,3] Akshata Shenoy H.,[1] S. P. Walborn,[2,3] E. S. Gómez,[2,3] M. Pawłowski,[1] and G. Lima[2,3]

[1]*International Centre for Theory of Quantum Technologies, University of Gdańsk, 80-308 Gdańsk, Poland.*
[2]*Departamento de Física, Universidad de Concepción, Casilla 160-C, Concepción, Chile.*
[3]*Millennium Institute for Research in Optics, Universidad de Concepción, Casilla 160-C, Concepción, Chile.*

A $n^d \xrightarrow{\text{p}} 1$ Quantum Random Access Code (QRAC) is a communication task where Alice encodes n classical bits into quantum states of dimension d and transmits them to Bob, who performs appropriate measurements to recover the required bit with probability p. In the presence of a noisy environment, the performance of a QRAC is degraded, losing the advantage over classical strategies. We propose a practical technique that enables noise tolerance in such scenarios, recovering the quantum advantage in retrieving the required bit. We perform a photonic implementation of a $2^2 \xrightarrow{\text{p}} 1$ QRAC using polarization-encoded qubits under an amplitude-damping channel, where simple operations allow noise robustness showing the revival of the quantum advantage when the noisy channel degrades the performance of the QRAC. This revival can be observed by violating a suitable Dimension Witness (DW) inequality, which is closely related to the average success probability of the QRAC. This technique can be extended to other applications in the so-called prepare and measure scenario, enhancing the semi-device independent protocol implementations.

I. INTRODUCTION

Quantum communication is quite unique as compared to its classical counterpart due to the fundamental differences in their physical principles [1, 2]. Quintessential quantum features like quantum superposition, entanglement, and no-cloning theorem form the basis of security and privacy in any quantum communication protocol [3, 4]. Amongst them, QRAC is a well-known communication protocol where a sender, namely Alice, encodes a string of classical bit onto a quantum state and sends it to a receiver, called Bob, who needs to extract the required subset string of bits by performing appropriate measurements [5, 6]. The performance of this protocol is measured in terms of Bob's average success probability (ASP) of extracting the value of the desired bit. For instance, in a $2^{d=2} \xrightarrow{\text{p}} 1$ QRAC protocol, Alice encodes two bits (a_0, a_1) onto quantum states of a single qubit ($d = 2$). The prepared state is transmitted to Bob, who extracts the bit value by performing an optimal measurement, called the *strategy*. The ASP for this QRAC is $p = 0.85$, which is greater than the case for the optimal classical strategy ($p_c = 0.75$), exhibiting a quantum advantage [7]. The classical strategy consists in Alice encoding and sending the same bit always– say it is a_0. If Bob is interested in a_0, he is correct always and if interested in a_1, he simply has to guess which gives the success probability in the worst case as $\frac{1}{2} + \frac{1}{2}\cdot\frac{1}{2} = \frac{3}{4}$. It has been demonstrated that the performance of a QRAC protocol can be further enhanced by using entanglement-assistance [8] or using d-level quantum systems [9].

To understand the overall performance of any quantum communication protocol, the assumptions used to derive its security parameters are crucial. Given that a $2^{d=2} \xrightarrow{\text{p}} 1$ QRAC is represented as a *prepare-and-measure protocol*, one finds it apt to consider such performance in the *semi-device-independent (SDI)* paradigm with the following main assumptions: (i) devices used for state preparation and measurement are uncharacterized, and (ii) the dimension of the Hilbert space of the prepared quantum system is bounded. The dimension of a system is an important resource in quantum theory. In SDI scenarios, the emphasis is only on analyzing the data collected in an experiment to characterize the dimension of a system independent of any theory. In this regard, a suitably constructed dimension witness (DW) allows one to certify the given Hilbert space dimension by placing an upper bound on it [10]. In a given scenario involving a system of dimension d, the saturation of the upper bound corresponds to the presence of a classical or quantum system of dimension d. On the other hand, given a classical and a quantum system of the same dimension, these witnesses can be violated by the quantum system, distinguishing it as a potentially more useful resource in comparison to its classical counterpart (say for realizing some quantum communication protocol). Thus, the classical system needs to be augmented with more dimension to reproduce the observed measurement statistics. It has been shown that the problem of constructing a dimension witnesses is related to the designing of QRACs [11]. Thus, by utilizing the connection between DWs, QRACs, and quantum key distribution protocols (QKD), the security of any prepare-and-measure protocol in the SDI scenario can be established under individual attacks by checking either the DW or the ASP of a QRAC protocol [12, 13].

Some other important applications of QRACs include SDI random number expansion [14, 15], randomness certification [16], SDI-QKD and foundational studies [17, 18]. Additionally, in the prepare-and-measure scenario, sequential QRACs are employed for self-testing of quantum measurements performed by an untrusted device[19, 20]. It is surprising to note that all these investigations involving QRACs have been carried out in an ideal noiseless setting. Recently, Ref. [21] considered the effect of different kinds of noise on a QRAC protocol and reported that the noise in the channel causes degrada-

* hsk1729@gmail.com
† santgomezlopez@gmail.com

tion in a manner that even a classical RAC could outperform it. They also attempt to mitigate the losses by considering semi-definite programming techniques in scenarios when the channel noise is known. Against this backdrop, it becomes relevant and pertinent for us to ask whether it is possible to *activate* a QRAC protocol and restore its overall performance in the presence of noise. In Ref. [21], they protect the QRAC against bit flip, phase flip, and dephasing channels. Nevertheless, they left the question of how to protect the QRAC from amplitude damping and depolarizing channels. We propose using stochastic filters to overcome scenarios where we face an amplitude-damping channel. This is to get closer to protecting all QRAC protocols in any noise channel scenarios.

Therefore, in this work, we present a $2^2 \xrightarrow{\text{p}} 1$ QRAC protocol for a qubit ($d = 2$) and its performance under a noisy channel. In a practical experimental realization of QRACs, a noisy channel can affect the quantum state. Hence, it becomes pertinent to quantify the maximum tolerable noise beyond which the ASP of the QRAC protocol is entirely degraded. In order to avoid such deterioration, we propose a scheme for activating QRACs by employing suitable stochastic operations, resulting in the revival of the ASP. Naturally, this method extends to any SDI scenario when testing a suitable DW to calculate its noise robustness. Finally, we present a proof of principle experiment. We demonstrate this activation in an amplitude channel using suitable optical devices and photonic qubits encoded in the polarization degree of freedom.

II. METHOD

QRACs.- A $2^2 \xrightarrow{\text{p}} 1$ QRAC protocol involves a sender (Alice) encoding a uniformly random two-bit string $x = a_0a_1 \in \{0,1\}^2$ onto a two-dimensional quantum state ρ_x. Given x, Alice prepares and transmits the state to the receiver (Bob). He wants to recover a subset of the encoded bit string x by performing a projective measurement M_y defined by the random classical bit $y \in \{0,1\}$. The ASP of Bob in extracting the required bit can be written as

$$P_b = \frac{1}{8}\sum_x \text{Tr}\left[\rho_x(M_0 + M_1)\right], \tag{1}$$

where Bob measurements are defined by the operators $M_j = \frac{\mathbb{1}+n_j\vec{\sigma}\cdot\vec{n_j}}{2}$, with $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, the outcomes $n_j = \pm 1$, and $\vec{n_j}$ are vectors in the Bloch sphere. A QRAC is successfully implemented if the ASP of extracting each of the bits transmitted by Alice exceeds the optimal classical ASP $P_b^{class} = 0.75$.

Semi-device independence and dimension witness.- In the semi-device independence scenario, no assumptions are made about the preparation and measurement of quantum states. In contrast, an upper limit for the dimension of the states is assumed. [12]. Such a scenario is depicted in Fig.1(a). Alice prepares states ρ_x with the assumption that everything except the dimension of the Hilbert space is uncharacterized. Now,

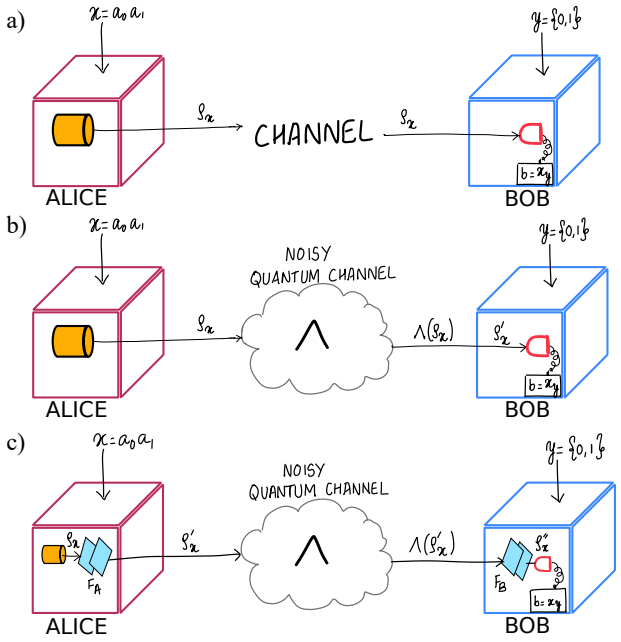

FIG. 1. A schematic representation of (a) QRACs in the ideal SDI scenario when Alice transmits states ρ_x to Bob. Quantum advantage is observed when Bob recovers the required subset of bits with an ASP $P_b > P_b^{class} = 0.75$ by measuring M_y. Further, violation of the DW by the encoded states certifies that they are quantum states of dimension 2, ensuring semi-device independence. (b) QRACs in the SDI scenario when Alice's states are transmitted over a noisy quantum channel Λ. After transmission along the channel, the state $\rho'_x = \Lambda(\rho_x)$ reaches Bob. (c) QRACs in the noisy SDI scenario with activation. A filter F_A is applied at Alice's end before transmitting the encoded state, ρ_x, rendering the new state ρ'_x. After transmission along the channel, the state $\Lambda(\rho'_x)$ is again filtered by Bob using F_B before performing measurements M_y on the final state ρ''_x.

Bob can apply projective measurements M_y^b with outcomes $b \in \{0,1\}$. Then, the conditional probability distribution $P(b|x,y) = \text{Tr}(\rho_x M_y^b)$ can be used to construct a DW in the form

$$\begin{aligned} W = E_{00,0} + E_{00,1} + E_{01,0} - E_{01,1} \\ - E_{10,0} + E_{10,1} - E_{11,0} - E_{11,1} \leq 2, \end{aligned} \tag{2}$$

which is a linear inequality of the conditional probability distribution $E_{a_0a_1,y} = P(b=0|a_0a_1,y) = \text{Tr}(\rho_{a_0a_1}M_y^{b=0})$. Here, $\rho_{x=a_0a_1}$ is an encoded state on which the measurement $M_y^{b=0}$ acts. Without loss of generality, only the projector corresponding to the outcome value $b = 0$ is considered. The upper bound of the W corresponds to the optimal capacity of a classical system of dimension 2 in conveying 1 bit of communication. On the other hand, the inequality is violated by qubits with a maximum value $2\sqrt{2}$, thereby establishing their resourceful nature in transferring enhanced communication > 1 bit. Moreover, is possible to generalize for an arbitrary dimension d [[STG: [CITA]]]. Thus, DWs aid in characterizing any arbitrary system of dimension d under consideration as classical or quantum in a *semi-device independent* way without any characterization of the experimental setup used to perform these tests.

Rewriting Eq.(1) using the above parameters [12], we obtain a relationship between ASP and DW in the SDI scenario as follows

$$P_b = \frac{1}{8}\sum_{x,y} P(b = x_y|a_0a_1, y) = \frac{W+4}{8}. \tag{3}$$

From the above equation we can infer that given a physical system of dimension $d = 2$ and W is violated, then a *quantum* system of $d = 2$ was prepared and correspondingly, a QRAC protocol with ASP $P_b > 0.75$ can be realized. Classical systems of dimension $d = 2$ can never violate the DW though higher dimensional ones can. Thus, DWs are useful tools in certifying a system as classical or quantum with dimension d and in the case of $d = 2$ also warrants the realization of a $2^2 \xrightarrow{\text{P}} 1$ QRAC protocol in the SDI scenario.

Noise adapted QRACs.- We now consider the SDI-QRAC protocol's performance under a noisy channel's action. Specifically, we will consider the amplitude damping channel (ADC) denoted by Λ, where it acts on the encoded states being transmitted (see Fig.1(b)). After the transmission, Bob receives each encoded state affected by the noise. The amplitude damping channel, parametrized by γ, can be represented in terms of Kraus operators $K_0(\gamma)$ and $K_1(\gamma)$, such that

$$\begin{aligned} K_0(\gamma) &= |0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1| \\ K_1(\gamma) &= \sqrt{\gamma}|0\rangle\langle 1|, \end{aligned} \tag{4}$$

where $K_i(\gamma) \geq 0$, $\sum_i K_i^\dagger(\gamma)K_i(\gamma) = \mathbb{1}$, and $\gamma \in [0, 1]$. Thus, Alice's states after the transformation due to the amplitude damping can be written as

$$\Lambda(\rho_x) = \sum_i K_i(\gamma)\,\rho_x\,K_i^\dagger(\gamma). \tag{5}$$

Therefore, the corresponding expressions for the DW and ASP considering the ADC and the optimal states are

$$\begin{aligned} W(\gamma) &= \sqrt{2}\left(1 + \sqrt{1-\gamma} - \gamma\right) \\ P_b(\gamma) &= \frac{W(\gamma)+4}{8}. \end{aligned} \tag{6}$$

In the absence of noise ($\gamma = 0$), the maximum achievable ASP is $P_b \approx 0.85$, corresponding to the maximal violation of W given by $W = 2\sqrt{2}$. Then, we define γ_c as the critical amplitude damping parameter beyond which the SDI-QRAC protocol is unsuccessful. From Eq. (7), $\gamma_c \approx 0.375$, where the QRAC no longer surpasses the optimal classical ASP of 3/4. For $\gamma \leq \gamma_c$, a violation of $W(\gamma)$ proves the realization of an SDI-QRAC scheme with $P_b > 3/4$.

It has been recently identified that it is possible to overcome the effects of the amplitude-damping noise upon applying certain stochastic operations at appropriate points along the channel. In this sense, *activation* is restoring the quantum advantage of an SDI-QRAC protocol under the action of noise, recovering the violations of the DW by applying suitable stochastic operations [22]. In our case and considering the prepare and measure scenario, these stochastic operations have to be applied by Alice at the input of the ADC and by Bob before his measurement apparatus (see Fig.1(c)) [23]. These operations filter the noisy encoded state $\Lambda(\rho_x)$. For the ADC, these filtering operations are given as

$$\begin{aligned} F_A &= |0\rangle\langle 0| + \sqrt{(1-f)}|1\rangle\langle 1| \\ F_B &= \sqrt{(1-f)}|0\rangle\langle 0| + |1\rangle\langle 1|, \end{aligned} \tag{7}$$

where $f \in [0, 1]$ is the filter parameter. Therefore, a noise-adapted SDI-QRAC protocol can now be formulated as follows:

1. The state $\rho_x \in \{\rho_{00}, \rho_{01}, \rho_{10}, \rho_{11}\}$ is prepared by Alice, and then is applied a filtering operation F_A before transmission across the amplitude damping channel Λ.

$$\rho_x \xrightarrow{F_A} \rho'_x = \frac{F_A\rho_x F_A^\dagger}{\text{Tr}(F_A\rho_x F_A^\dagger)}. \tag{8}$$

2. The amplitude damped state $\Lambda(\rho'_x)$ is received by Bob. Bob applies another filtering operation F_B on this state to obtain

$$\Lambda(\rho'_x) \xrightarrow{F_B} \rho''_x = \frac{F_B\Lambda(\rho'_x)F_B^\dagger}{\text{Tr}(F_B\Lambda(\rho'_x)F_B^\dagger)}. \tag{9}$$

3. Bob performs the measurement M_y on the received state ρ''_x to extract the required bit.

Therefore, the probability distribution of the measurement outcome b at Bob's end is given as,

$$p(b|y, x) = \text{Tr}\left[\Pi_y^b\left(\frac{F_B \circ \Lambda \circ F_A(\rho_x)}{N(x)}\right)\right], \tag{10}$$

where the normalization constant

$$N(x) = \text{Tr}\left[F_B\left(\sum_i K_i(\gamma)(F_A\,\rho_x\,F_A^\dagger)K_i(\gamma)^\dagger\right)F_B^\dagger\right],$$

and Π_y^b is the projector associated to the the measurement y when the outcome b is obtained.

III. EXPERIMENTAL DESCRIPTION

Our noise-adapted implementation of the QRAC is depicted in Fig.2. The experiment consists of (i) a sender (Alice) who encodes four states into the polarization state of single photons, (ii) a receiver (Bob) who performs projective measurements on the photons, (iii) a noisy channel through which the polarization qubits propagate from Alice to Bob, and (iv) a set of filter operations F_A and F_B that Alice and Bob will use to attempt to improve the performance of the protocol in the presence of noise. Let us present these four components in sequence.

Single photons are produced using a heralded single-photon source based on the spontaneous parametric downconversion (SPDC) process. A continuous-wave laser at 405 nm pumps

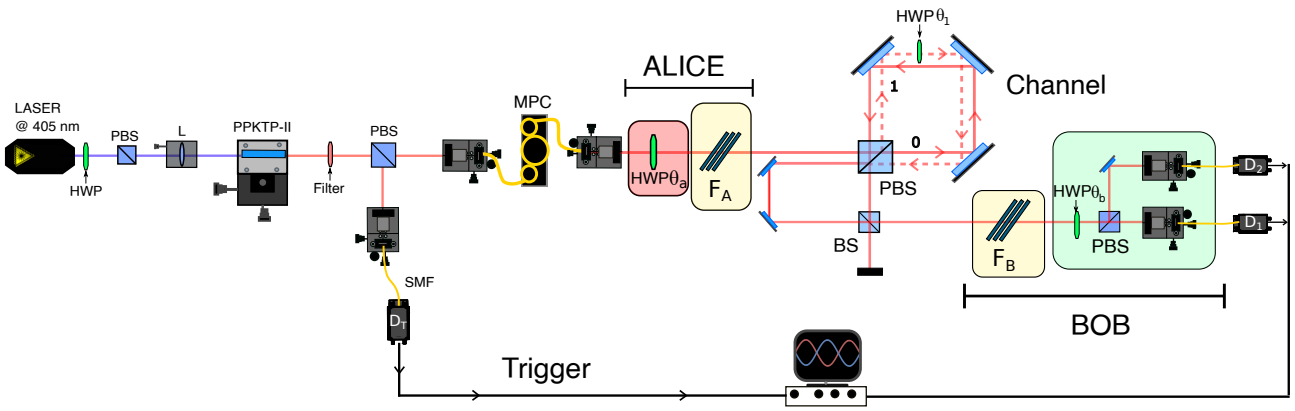

FIG. 2. A heralded photon source based on the SPDC process is used to study the behavior of the SDI QRAC protocol in a noisy scenario. Alice's setup includes an HWP (θ_a)that is used to prepare four states encoded in the polarization degree of freedom: ρ_{00}, ρ_{11}, ρ_{01}, and ρ_{10}. Additionally, a filter denoted F_A, is applied before sending the state. Subsequently, a two-path Sagnac interferometer implements the amplitude damping channel, where the amount of amplitude damping is controlled by θ_1. After transmitting the state through the channel, Bob applies F_B, and finally, two measurements are performed by an HWP, a PBS, and two photon detectors. The two stochastic filters, one before and one after the noisy channel, are implemented using glass windows set at the Brewster angles.

a 20 mm long periodically poled potassium titanyl phosphate (PPKTP - type-II) crystal, producing a pair of photons with orthogonal polarization at 810 nm. The pump laser power is controlled actively (@2 mW) to reduce intensity fluctuations. A high-quality narrow bandpass filter with 0.5 nm bandwidth (peak transmission $> 95\%$) ensures frequency degeneracy. Moreover, single-mode optical fibers are used to spatially filter the down-converted photons, removing undesirable spatial correlations. A numerical model is considered in the setup design to maximize the coincidences rate [24]. The optimal coupling condition is reached when $\omega_{DCP} = \sqrt{2}\omega_p$, where ω_p and ω_{DCP} are the waist modes of the pump beam and the down-converted photons at the center of the PPKTP crystal, respectively. Our configuration achieves these waists with a lens L of 20 cm focal length at the front of the crystal and $10\times$ objective lenses for coupling the down-converted photons. A polarizing beam splitter (PBS) is placed after the PPKTP crystal to separate the generated photons by polarization. One photon is sent directly to a single photon detector D_T, which acts as a trigger, while the other photon is sent to the Alice stage to initialize the protocol. The coincidence counts between the trigger detector D_T and Bob's detectors D_1 (D_2), announce the presence of the heralded single-photon event used in the experiment. In addition, a manual fiber polarization controller (MPC) is used to adjust the initial polarization of Alice's photon.

Alice uses a half-wave plate (HWP) to prepare polarization qubits of the form $|\psi\rangle = \cos 2\theta_a |H\rangle + \sin 2\theta_a |V\rangle$, where θ_a is the angle of the HWP concerning its fast axis. The four states prepared by Alice for use in the QRAC are

$$\begin{aligned} \rho_{00} &= |H\rangle\langle H|, \quad \rho_{01} = |-\rangle\langle -|, \\ \rho_{10} &= |+\rangle\langle +|, \quad \rho_{11} = |V\rangle\langle V|, \end{aligned} \tag{11}$$

where $|\pm\rangle = (|H\rangle \pm |V\rangle)/\sqrt{2}$ are the diagonal and anti-diagonal polarization states, respectively.

Bob's optimal measurements for extracting the required bit in the SDI-QRAC protocol are given as,

$$\begin{aligned} M_{y=0} &= \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x), \\ M_{y=1} &= \frac{1}{\sqrt{2}}(\sigma_z + \sigma_x), \end{aligned} \tag{12}$$

where $\sigma_z = |H\rangle\langle H| - |V\rangle\langle V|$ and $\sigma_x = |+\rangle\langle +| - |-\rangle\langle -|$ are the Pauli matrices. The measurements are implemented using the HWP(θ_b) setting at $\theta_b = \{\frac{7\pi}{16}, \frac{\pi}{16}\}$ for $y = 0, 1$, respectively, and a polarizing beam splitter followed by two avalanche single photon detectors D_1 and D_2, as shown in Fig. 2. The signals from these detectors are processed by a coincidence counting module with calibrated delays between the output of D_1 (D_2) and Alice's trigger detector D_T. The module has a 1 ns coincidence window to reduce accidental counts.

The ADC, represented as a decomposition of the Kraus operators $K_0(\gamma)$ and $K_1(\gamma)$ given in (5), is implemented by a two-path Sagnac interferometer [25–29]. As described in detail in Refs. [25, 26], by incoherently combining the two outputs of the interferometer, we can implement a controllable decoherence channel described by the Kraus operators

$$K_0(\theta_1) = |H\rangle\langle H| + \cos(2\theta_1)|V\rangle\langle V|, \tag{13}$$

$$K_1(\theta_1) = \sin(2\theta_1)|H\rangle\langle V|. \tag{14}$$

More details about the optical decoherence channel are given in the Appendix. Comparing these expressions with Eq.(5) we see that $\sin 2\theta_1 = \sqrt{\gamma}$ and $\cos 2\theta_1 = \sqrt{1-\gamma}$, allowing for control of γ using the waveplate angle θ_1.

Finally, the filter operations F_A and F_B are implemented using thin glass plates placed at the Brewster angle so that the reflected light contains only one polarization component [30]. Thus, one polarization mode is partially filtered from the transmitted beam, while the other is left unchanged. The difference between F_A and F_B lies in the position of the principal axis of the glass plate, which are orthogonal to each

other, allowing the vertical or horizontal components to be filtered, respectively. Figure 3 shows the corresponding f parameter for different glass plate amounts. We denote the f_a (f_b) parameter when filtering the vertical (horizontal) polarization, represented by the blue (orange) dots. To illustrate the advantages of using stochastic filters in this protocol, we consider two sets of glass configurations: one with 3 glass plates and the other with 8 glass plates, corresponding to filter parameters of $f_a \approx \{0.44 \pm 0.05, 0.88 \pm 0.01\}$ and $f_b \approx \{0.44 \pm 0.06, 0.91 \pm 0.01\}$.

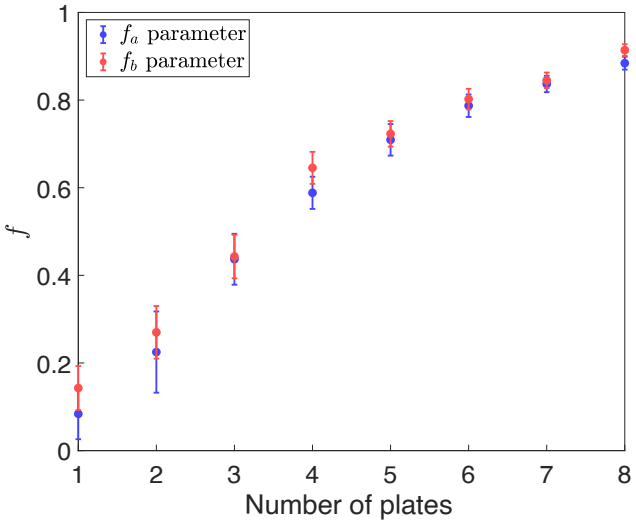

FIG. 3. Filter parameters f_a and f_b as a function of the number of glasses. The blue and orange points represent experimental results. These results were obtained using down-converted photons (@810 nm), with error bars calculated using Gaussian error propagation and Poisson statistics of the coincidence counts.

IV. RESULTS

We can observe in Fig. 4 that, depending on the value of f, an increase in the corresponding value of the critical amplitude damping parameter is achieved, beyond which the scheme no longer improves on the classical bound, indicating that the protocol becomes more robust to a noisy channel. For $f = 0.45$ and, $f = 0.90$ the ASP can beat the classical bound for $\gamma_c = 0.52$ and $\gamma_c = 0.82$, respectively. To experimentally validate the SDI nature of the scheme, we measure the DW, and then the ASP is obtained from Eq. (7). The probabilities $E_{a_0a_1,y}$ involved in the inequality are calculated following the expression

$$E_{a_0a_1,y} = \frac{c(0|a_0a_1,y)}{c(0|a_0a_1,y) + c(1|a_0a_1,y)}, \qquad (15)$$

where $c(0|a_0a_1,y)$ $\big(c(1|a_0a_1,y)\big)$ are the coincidence counts recorded between the trigger detector D_T and detector D_1 (D_2) when the state ρ_{a_0,a_1} is prepared by Alice and the M_y is performed by Bob. Each coincidence count is recorded after 10 s of integration time. The results are displayed in

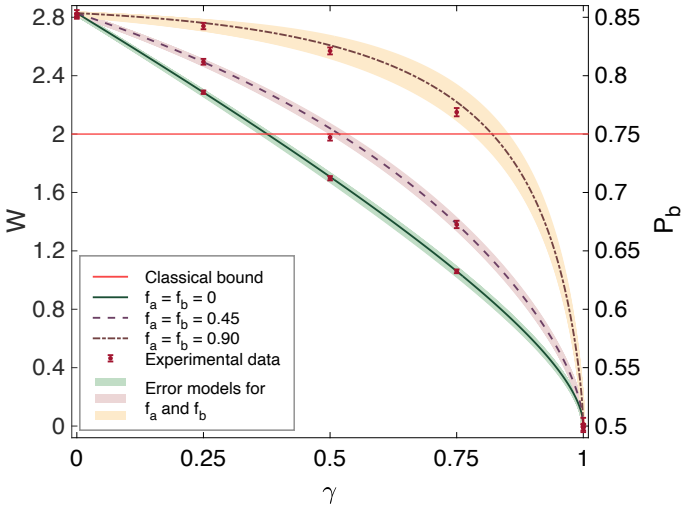

FIG. 4. Average success probability (ASP) as a function of amplitude damping parameter (ADP). The horizontal line represents the ASP of a classical RAC, which is 0.75. The solid, dashed, and dotted lines represent the theoretical predictions when $f = \{0, 0.45, 0.90\}$. The red dots are the experimental results. The error bars are obtained using Gaussian error propagation and considering the Poisson statistics of the recorded coincidence counts. The green, red, and yellow areas illustrate how the DW and ASP change when common experimental errors are included, such as half-wave plate settings or errors characterizing f_a and f_b.

Fig.4, where the DW and the ASP are shown as a function of five different amplitude damping parameters $\gamma = \{0, 0.25, 0.5, 0.75, 1\}$. As we observed in Section III, it is possible to implement different values of γ changing the angle θ_1: when $\theta_1 = 0$, all photons leave the interferometer through output $|0\rangle$, which means that there is no amplitude attenuation in the channel, as expected. In addition, when $\theta_1 \neq 0$, the photons start to populate the $|1\rangle$ mode, indicating an increase in noise.

Consider first the experimental results without any filtering, as shown in the green region of Fig. 4. The red dots indicate that the DW decreases rapidly as a function of γ, falling below the classical limit (represented by the horizontal line) when $\gamma_c \approx 0.38$. However, there is an improvement when F_A and F_B are applied with $f_a = 0.44 \pm 0.05$ and $f_b = 0.44 \pm 0.06$ ($f_a = 0.88 \pm 0.01$ and $f_b = 0.91 \pm 0.01$), which are displayed in the red (yellow) region. The experimental data demonstrate activation of the SDI QRAC scheme for values of $\gamma \geq \gamma_c$ when filtering operations are applied. As the parameter f increases, more red data points appear above the classical bound.

An error model based on Monte Carlo simulations is developed to show how the experimental imperfections can affect our experimental results through the colored areas in Fig. 4. To simulate the error from Alice's state preparation, a mismatch of $\pm 1^o$ on the angle of the HWP(θ_a) is considered. Also, in the simulation a deviation of $\pm 1\%$ in the characterization of f_a and f_b is included. In addition, a mismatch of $\pm 1^o$ on the HWP(θ_b) placed in the measurement has been considered. The error bars are obtained with Gaussian error

propagation, considering the Poisson statistics of the recorded coincidence counts.

V. CONCLUSION

In this work, we have proposed and experimentally demonstrated the revival of the quantum advantage in establishing a quantum random access code when two distant parties send qubits through a noisy quantum channel, described by the amplitude damping channel. We observe that the quantum advantage of the protocol over the corresponding classical case is lost for a critical noise value. We then show that stochastic filtering operations can be applied locally by Alice and Bob to counter the noise degradation and restore the quantum advantage for noise levels above the critical value. Given the interest in quantum random access codes as primitive in quantum information protocols, we expect our results to be used in other applications, such as random number generation.

ACKNOWLEDGEMENTS

HSK and MP thank NCN Poland, ChistEra-2023/05/Y/ST2/00005 under the project Modern Device Independent Cryptography (MoDIC). This work was initiated when ASH and MP were supported by the Foundation for Polish Science (IRAP project, ICTQT, contract No. 2018/MAB/5, co-financed by EU within Smart Growth Operational Programme. Rest of the authors acknowledge support from the Fondo Nacional de Desarrollo Científico y Tecnológico (FONDECYT) (Grant Nos. 3210359, 1180558, 1231940, 1200266, and 1200859).

APPENDIX: SAGNAC INTERFEROMETER AS AN AMPLITUDE DAMPING CHANNEL

As demonstrated and described in previous work [25, 26, 31, 32], an interferometer can be used to implement a decoherence channel. Here we briefly describe the Sagnac interferometer used to implement the amplitude damping channel in the experiment, illustrated in the "channel" portion of figure 2. The photon is first incident onto a polarizing beamsplitter (PBS), which separates the horizontal and vertical components of the polarization qubit into two linear momntum modes $|0\rangle$ and $|1\rangle$, depicted as continuous and dashed lines in Fig.2, respectively. The PBS can be thought of as a controlled-NOT (CNOT) gate between the polarization and momentum degrees of freedom, described as

$$\text{PBS} = \hat{h} \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + i\hat{v} \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|),$$

where $\hat{h} = |h\rangle\langle h|$ and $\hat{v} = |v\rangle\langle v|$. Applying the PBS to an input state $|\Psi\rangle = |\psi\rangle\, 0$, where $|\psi\rangle$ is the initial polarization state,we obtain

$$|\Psi^{'}\rangle = \hat{h}\,|\psi\rangle\,|0\rangle + i\hat{v}\,|\psi\rangle\,|1\rangle\,.$$

Inside the interferometer, a half-wave plate HWP(θ_1) is added in path 1 with its fast axis aligned at angle θ_1. Experimentally, it is important to consider that the optical path length difference between the paths 0 and 1 that is caused by HWP(θ_1). Hence, it is necessary to include another half-wave plate in the path 0 to compensate the optical path length. After the wave plate, the state is described as

$$|\Psi^{''}\rangle = \hat{h}\,|\psi\rangle\,|0\rangle + i\hat{\mathrm{H}}(\theta_1)\hat{v}\,|\psi\rangle\,|1\rangle\,,$$

where $\hat{\mathrm{H}}$ is the Jones matrix representation of a half-wave plate [33]. The two paths are routed using the three mirrors, so that the photon again passes through the same PBS, implementing a second CNOT gate as described in (V). After the PBS, we have the following state:

$$|\Psi^{'''}\rangle = \left[\hat{h} - \hat{v}\hat{\mathrm{H}}(\theta_1)\hat{v}\right]|\psi\rangle\,|0\rangle + i\left[\hat{h}\hat{\mathrm{H}}(\theta_1)\hat{v}\right]|\psi\rangle\,|1\rangle\,. \quad (16)$$

The two output modes of the PBS are then combined incoherently at a beam splitter (BS), such that the the optical path lengths are different by a few millimeters, which is much more than the longitudal conherence length of the photons (a few hundred microns). This is the experimental equivalent of "tracing out" the environment, which here is the linear momentum degree of freedom. The output state is then described by a density matrix,

$$\rho_{out} = K_0\,|\psi\rangle\langle\psi|\,K_0^{\dagger} + K_1\,|\psi\rangle\langle\psi|\,K_1^{\dagger} \quad (17)$$

where the Kraus operators are given by

$$K_0 = \hat{h} - \hat{v}\hat{\mathrm{H}}(\theta_1)\hat{v},$$
$$K_1 = \hat{h}\hat{\mathrm{H}}(\theta_1)\hat{v}.$$

Replacing the components of the Jones matrix makes it possible to write these Kraus operators in the form given in Eq. (14) of the main text.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[2] N. Gisin and R. Thew, Quantum communication, Nature Photonics **1**, 165 (2007).
[3] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, Theoretical Computer Science **560**, 7 (2014), theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.
[4] A. K. Ekert, Quantum cryptography based on bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).
[5] A. T.-S. Andris Ambainis, Ashwin Nayak and U. Vazirani, Dense quantum coding and a lower bound for 1-way quantum automata, in Proceedings of the Thirty-First Annual ACM Symposium on Theory of Com

STOC '99 (Association for Computing Machinery, New York, NY, USA, 1999) pp. 376–383.
[6] A. T.-S. Andris Ambainis, Ashwin Nayak and U. Vazirani, Dense quantum coding and quantum finite automata, J. ACM **49**, 496 (2002).
[7] L. M. Andris Ambainis, Debbie Leung and M. Ozols, Quantum random access codes with shared randomness (2009), 0810.2937v3.
[8] M. Pawłowski and M. Żukowski, Entanglement-assisted random access codes, Phys. Rev. A **81**, 042326 (2010).
[9] B. M. Armin Tavakoli, Alley Hameed and M. Bourennane, Quantum random access codes using single d-level systems, Phys. Rev. Lett. **114**, 170502 (2015).
[10] R. Gallego, N. Brunner, C. Hadley, and A. Acín, Device-independent tests of classical and quantum dimensions, Phys. Rev. Lett. **105**, 230501 (2010).
[11] S. Wehner, M. Christandl, and A. C. Doherty, Lower bound on the dimension of a quantum system given measured data, Phys. Rev. A **78**, 062112 (2008).
[12] M. Pawłowski and N. Brunner, Semi-device-independent security of one-way quantum key distribution, Phys. Rev. A **84**, 010302 (2011).
[13] A. Chaturvedi, M. Ray, R. Veynar, and M. Pawłowski, On the security of semi-device-independent qkd protocols, Quantum Information Processing **17**, https://doi.org/10.1007/s11128-018-1892-z (2018).
[14] 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, Phys. Rev. A **84**, 034301 (2011).
[15] V. Mannalath and A. Pathak, Bounds on semi-device-independent quantum random-number expansion capabilities, Phys. Rev. A **105**, 022435 (2022).
[16] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Semi-device-independent randomness certification using $n \to 1$ quantum random access codes, Phys. Rev. A **85**, 052308 (2012).
[17] A. Grudka, K. Horodecki, M. Horodecki, W. Kłobus, and M. Pawłowski, When are popescu-rohrlich boxes and random access codes equivalent?, Phys. Rev. Lett. **113**, 100401 (2014).
[18] M. Pawłowski, T. Paterek, D. Kaszlikowski, V. Scarani, A. Winter, and M. Żukowski, Information causality as a physical principle, Nature **461**, 1101 (2009).
[19] 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).
[20] N. Miklin, J. J. Borkała, and M. Pawłowski, Semi-device-independent self-testing of unsharp measurements, Phys. Rev. Research **2**, 033014 (2020).
[21] B. Marques and R. A. da Silva, Quantum random access code in noisy channels (2022), 2204.09485v1.
[22] P. Horodecki and R. Horodecki, Distillation and bound entanglement., Quantum Inf. Comput. **1**, 45 (2001).
[23] H.-Y. Ku, H.-C. Weng, Y.-A. Shih, P.-C. Kuo, N. Lambert, F. Nori, C.-S. Chuu, and Y.-N. Chen, Hidden nonmacrorealism: Reviving the leggett-garg inequality with stochastic operations, Phys. Rev. Research **3**, 043083 (2021).
[24] D. Ljunggren and M. Tengner, Optimal focusing for maximal collection of entangled narrow-band photon pairs into single-mode fibers, Phys. Rev. A **72**, 062301 (2005).
[25] M. P. A. F. de Melo, M. Hor-Meyll, A. Salles, S. P. Walborn, P. H. S. Ribeiro, and L. Davidovich, Environment-induced sudden death of entanglement, Science **316**, 579 (2007).
[26] A. Salles, F. de Melo, M. P. Almeida, M. Hor-Meyll, S. P. Walborn, P. H. Souto Ribeiro, and L. Davidovich, Experimental investigation of the dynamics of entanglement: Sudden death, complementarity, and continuous monitoring of the environment, Phys. Rev. A **78**, 022322 (2008).
[27] S. Gómez, A. Mattar, E. S. Gómez, D. Cavalcanti, O. J. Farías, A. Acín, and G. Lima, Experimental nonlocality-based randomness generation with nonprojective measurements, Phys. Rev. A **97**, 040102 (2018).
[28] E. S. Gómez, S. Gómez, P. González, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi, and G. Lima, Device-independent certification of a nonprojective qubit measurement, Phys. Rev. Lett. **117**, 260401 (2016).
[29] M. A. Solís-Prosser, P. González, J. Fuenzalida, S. Gómez, G. B. Xavier, A. Delgado, and G. Lima, Experimental multiparty sequential state discrimination, Phys. Rev. A **94**, 042309 (2016).
[30] P. G. Kwiat, S. Barraza-Lopez, A. Stefanov, and N. Gisin, Experimental entanglement distillation and 'hidden' non-locality, Nature **409**, 1014–1017 (2001).
[31] O. Jiménez Farías, A. Valdés-Hernández, G. H. Aguilar, P. H. Souto Ribeiro, S. P. Walborn, L. Davidovich, X.-F. Qian, and J. H. Eberly, Experimental investigation of dynamical invariants in bipartite entanglement, Phys. Rev. A **85**, 012314 (2012).
[32] G. H. Aguilar, O. J. Farías, A. Valdés-Hernández, P. H. Souto Ribeiro, L. Davidovich, and S. P. Walborn, Flow of quantum correlations from a two-qubit system to its environment, Phys. Rev. A **89**, 022339 (2014).
[33] B. E. Saleh and M. C. Teich, Fundamentals of photonics (john Wiley & sons, 2019).