QRAC Implementation with Optimal Resource Allocation

Domenico Ribezzo[1,2], Roberto Salazar[3], Flora Segur[1], Jakub Czartowski[3], Gianmarco Lemmi[1], Antoine Petitjean[1], Noel Farrugia[4], André Xuereb[4,5], Davide Bacco[4,7], Alessandro Zavatta*[1,7]

[1] National Research Council - National Institute of Optics (CNR-INO), 50125 Florence, Italy [2] University of Naples Federico II, Naples, Italy
[3] Faculty of Physics, Astronomy and Appl. C.S., Jagiellonian University, 30348 Krakòw, Poland,
[4]Merqury Cybersecurity Limited, Malta
[5] Department of Physics, University of Malta, Msida MSD 2080, Malta,
[6] Department of Physics and Astronomy, University of Florence, 50019 Sesto Fiorentino, Italy
[7]QTI S.r.l., 50125, Firenze, Italy
(*)alessandro.zavatta@ino.cnr.it

Abstract *We implement a novel quantum random access code protocol exploiting weak pulses and made by a fiber setup fully integrable in the standard telecomunication infrastructure. We demonstrate a quantum advantage compared to the classical RAC schemes for two and four-dimensional encoding for different noise level. ©2023 The Author(s)*

Introduction

Quantum networks use quantum properties for secure data transmission. While not yet widely adopted by end-users, numerous implementations are reported in the literature both exploiting terrestrial links and satellite technology[1],[2]. However, practical challenges, such as the maximum distance between the users and a limited key generation rate, must be overcome before quantum networks become ubiquitous. In this context, a more efficient communication protocol able at compressing a string of n-bits into a shorter one would be particularly useful. Quantum Random Access Code (QRAC) is the quantum extension of a Classical Random Access Code (CRAC), which compresses a n-bit message into a shorter m-bit string, where $m < n$. This message is shared between two users with a probability $p > 50\%$ of retrieving a subset of the original message ($n \xrightarrow{\text{p}} m$). QRAC is obtaining increasing attention in the quantum community for its quantum advantage: for fixed *n* and *m*, *p*, is always higher exploiting a quantum system. Moreover, QRAC can be used in different applications like Quantum key Distribution (QKD)[3],[4], quantum randomness certification[5], dimension witness of quantum systems[6] and network coding[7].

Currently, all of QRAC implementations used single photons generated through nonlinear optics processes[8]–[11]. Our work proposes and experimentally demonstrates a novel QRAC scheme based on weak coherent pulses, thus simplifying the overall generation and detection of the quantum states. In addition, we extended our protocol to higher dimensionality and characterize the two systems in terms of noise resilience.

Encoding and decoding strategy

In quantum mechanics, two measurements M1 and M2 are defined *incompatible* if it is impossible to perform them simultaneously with arbitrary precision. A resource theory of incompatibility offers a tool for quantifying this incompatibility, which has no counterparts in the classical world.[12]. Monotones are used to quantify the advantage of incompatible measurements over any compatible set[13], or advantage in QRAC over CRAC[14]. A Monotone $\mathcal{M}$ is a functions that is zero if a pair of measurements are compatible and is greater than zero otherwise. Furthermore, a monotone is nonincreasing for any possible operation, such as for noise addition[15]. According to the resource theory of incompatibility, the sets of measurements defined by pairs of mutually unbiased bases (MUBs) are the most incompatible pairs of measurements[16]. A pair of orthonormal bases $\{|e_i\rangle\}_{i=0}^{d-1}$ and $\{|f_i\rangle\}_{j=0}^{d-1}$ in $\mathcal{H}^d$ is unbiased if the product of any pair of states taken from them satisfies $\left|\langle e_i|f_j\rangle\right|^2 = 1/d$. The most used pair of MUBs are composed by the eigenvectors of the Pauli matrices σ_Z (computation basis) and σ_X (diagonal basis). Based on the previous statement, the measurement $\mathbf{M} = \{M_1, M_2\}$ performed using a pair of MUBs represents the optimal decoding strategy. On the other side, the optimal encoding strategy is realized when $\mathcal{E}(\mathbf{x})$ is an eigenstate corresponding to the maximal eigenvalue of the operator $M_1(x_1) + \cdots + M_n(x_n)$[14],[17]. The encoding scheme for the QRAC (2,2) and QRAC

(2,4) – where QRAC(n,d) is referred to *n* bits of dimension *d* – is reported in table1 and table2. For practical reasons, we chose to experimentally generate a limited subset of the sixteen different messages available with QRAC (2,4). Once the message has been prepared by the transmitter Alice (see fig.1) and sent through the quantum channel, Bob (the receiver) performs projective measurements on the qudit.

Message	00	01	10	11
$\|0\rangle \propto$	a_1	a_1	b_1	b_1
$\|1\rangle \propto$	$+b_1$	$-b_1$	$+a_1$	$-a_1$

Tab. 1: Scheme of the states encoded for QRAC(2,2); $a_1 = \frac{\sqrt{2+\sqrt{2}}}{2}$ and $b_1 = \frac{\sqrt{2-\sqrt{2}}}{2}$, the sign - means π phase).

Setup

To implement the QRAC, we used the time-bin encoding scheme exploiting its simplicity and scalability to higher dimensions[18]. Specifically in table 1 and 2 we report our optimal encoding parameters. Fig. 2 reports a graphical representation of the states. These quantum states are generated by carving a continuum wave C-band laser at 1551.72 nm (channel 32 of DWDM ITU grid[19]). A first intensity modulator, driven by a 1.2 GHz signal, creates a train of pulses equally separated by 800 ps. A second intensity modulator partially suppresses some of the pulses according to the values reported in tables 1 and 2. Subsequently, a phase modulator introduces a o or π-phase between the different pulses. A variable optical attenuator is inserted in the setup for reducing the intensity of the quantum states to the single-photon level. In our case we used a mean photon number per pulse of 0.2.

In the case of d=2, each state is made by two pulses whose size is proportional to a_1^2 or b_1^2, as defined in table 1, with a relative phase of 0 or π. In the case of d=4, the quantum states are composed of four pulses.

After the transmission of the quantum states through an optical fiber link with 10 dB losses, a 50:50 beam splitter makes the passive basis choice. In the Z basis, the arrival time of the photons is detected using an InGaAs single-photon avalanche diode (SPAD). In the X basis, the relative phase of the two pulses composing a QRAC (2,2) state is measured by sending them through a delay line interferometer (DLI)[20]. Regarding the implementation of the QRAC (2,4), we only employ the Z basis for simplicity reasons. To test the performance of the QRAC in a co-propagation link, a classical channel is emulated by sending an optical signal generated by a tunable laser emitting with a different frequency. The signal is attenuated by a VOA and injected into the quantum channel thanks to a DWDM filter[21].

Message	Binary	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
00	00 00	a_2	$+b_2$	$+b_2$	$+b_2$
10	01 00	b_2	$+a_2$	$+b_2$	$+b_2$
20	10 00	b_2	$+b_2$	$+a_2$	$+b_2$
30	11 00	b_2	$+b_2$	$+b_2$	$+a_2$

Tab. 2: Scheme of the states encoded for QRAC(2,4). $a_2 = \sqrt{3}/2$ and $b_2 = 1/(2\sqrt{3})$.

Results

	00	01	10	11
p_Z	0.8537	0.8532	0.8520	0.8555
p_X	0.8502	0.8140	0.8184	0.7937

Tab. 3: p_Z and p_X are the probabilities p in Z and X basis.

Tab. 3 reports the results achieved measuring the generated QRAC(2,2) without noise source. The theoretical upper bound for QRAC(2,2) $p^{Q(2,2)} = 1/2(1 + 1/\sqrt{2}) \approx 0.854$[6] is approached. Since the threshold given by CRAC is $p^{CRAC(2,2)} = 1/2(1 + 1/2) = 0.75$[6], we have demonstrated a quantum advantage $\delta A = max\{p^{QRAC} - p^{CRAC}, 0\}$. In addition in Fig. 3 we report the results for the noisy channel configuration.

Successively, we study the case of two quarts (4-dimensional bit). As pointed out in tab. 2, two quarts can be represented by four bits. When Bob performs a measurement on the qudit, he retrieves two bits out of four. Moreover, he can also perform a partial measurement of the quantum states, to retrieve only one bit over four. In the Z basis, in order to retrieve one bit of information, we define M_1 the measurement over the subset made by the first and the second pulse, and M_2 the measurement over a second subset made by the third and fourth pulse. In other words, M_1 checks if the photon arrives in the first two time-bins of the quantum state, M_2 if it arrives in the last two. By measuring the exact time of arrival of the photon, i.e., distinguishing the precise time-bin, it is possible to retrieve two bits. This measurement is called M_{12}.

	M_1	M_2	M_{12}
p	79.1%	82.9%	75.0%
δA	0.041	0.079	0.125

Tab. 4: p and δA for the three measurement sets.

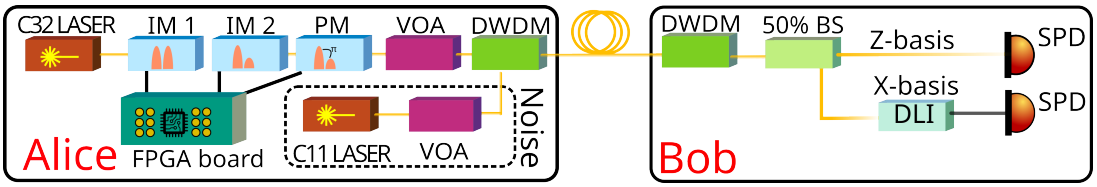

Fig. 1: Scheme of the setup. Alice: C32: laser at 1551.72 nm, FPGA: field programmable gate array board, IMs: intensity modulators, PM: phase modulator, VOA: variable optical attenuator, DWDM: dense wavelength division multiplexing filter, C11: laser at 1568.11. Bob: BS: 50% beam splitter, DLI: delay line interferometer, SPD: single photon detector.

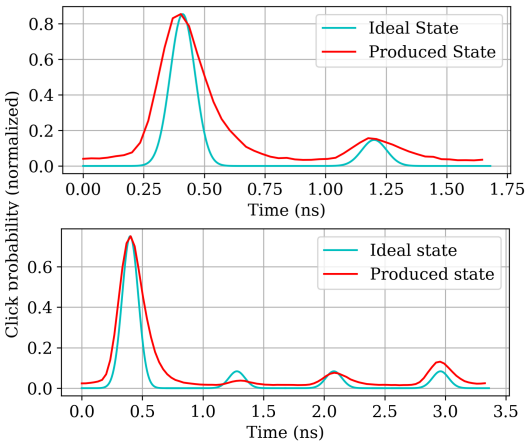

Fig. 2: QRAC(2,2) (top) and QRAC(2,4) (bottom), example of a quantum state. The figure shows the shape of the achieved wave functions of a photon encoding a QRAC state in 2 and 4 dimension (red), with a comparison with the ideal states (cyan). The pulses sizes are reported in the text while the relative phase can be zero or π.

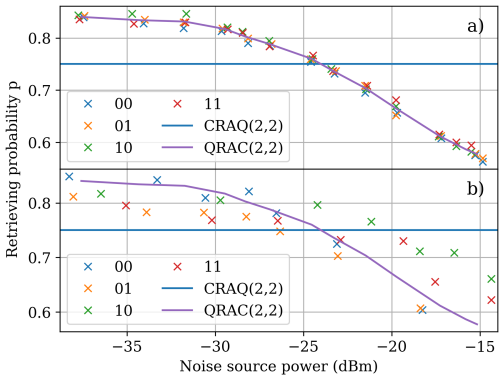

Fig. 3: Probability p for the bit in the **Z basis (a)** and in the **X basis (b)** versus optical power of the coexistent classical communication. The blue line represents the P^{CRAC} threshold, while the purple line shows the average probability.

The results for a noise-free channel are reported in tab. 4, and the fig. 4 represents the quantum advantage δA achieved in the case of co-existence with classical light. The classical thresholds P^{CRAC} for Bob retrieving one or two bits over four are 75% and 62.5% respectively and the quantum bounds P^{QRAC} are 83.3% and 75%[22]. We measured a quantum advantage that matches the theoretical prediction for an ideal state and decreases to zero under the effect of noise. In other words, it behaves as a monotone function, so it can be used as a quantifier of the advantage of incompatible measurements.

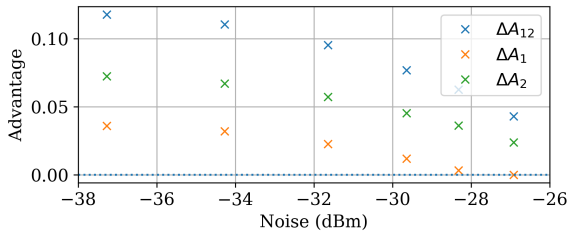

Fig. 4: Quantum advantage of QRAC vs power of channel-coexisting classical light.

It means that if δA approaches the theoretical bound, the MUBs used in our encoding and decoding strategies are the optimal bases according to the allocation criterion of proportional fairness, a criterion utilized to distribute resources between two systems in a proportional way[15].

Discussions and conclusion

We experimentally implement a QRAC system based on weak coherent states and time-bin encoding, which offers the enormous advantage of being simple, robust, and compatible with telecom infrastructure[20],[23]. In addition, we implement the QRAC with two-dimensional and four-dimensional quantum states, proving the reconfigurability of our solution. We prove that our results are in accordance with the theoretical predictions both for the two-dimensional and for the four-dimensional case with and without additional noise in the quantum channel. Moreover, we demonstrate that the quantum advantage acts as a monotone function, thus it can be utilized as a quantifier of the performance of the system concerning resource allocation. We believe that our work establishes a strong foundation for the broad adoption of QRAC, both as a reliable communication protocol and as a practical tool for testing theoretical concepts.

Acknowledgements

This work was supported by the program Rita Levi Montalcini (PGR19GKW5T), the Project EQUO (no 101091561), the Project QUID (no 101091408), the projectLaserlab (no 871124), the Project QuONTENT (CNR program) by PON Ricerca e Innovazione 2014-2020 FESR and the project ARS01/00734 QUANCOM.

References

[1] S.-K. Liao, W.-Q. Cai, J. Handsteiner, *et al.*, "Satellite-relayed intercontinental quantum network", *Physical review letters*, vol. 120, no. 3, p. 030 501, 2018.

[2] Y.-A. Chen, Q. Zhang, T.-Y. Chen, *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres", *Nature*, vol. 589, no. 7841, pp. 214–219, 2021.

[3] M. Pawłowski and N. Brunner, "Semi-device-independent security of one-way quantum key distribution", *Physical Review A*, vol. 84, no. 1, p. 010 302, 2011.

[4] A. Chaturvedi, M. Ray, R. Veynar, and M. Pawłowski, "On the security of semi-device-independent qkd protocols", *Quantum information processing*, vol. 17, pp. 1–20, 2018.

[5] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, "Self-testing quantum states and measurements in the prepare-and-measure scenario", *Physical Review A*, vol. 98, no. 6, p. 062 307, 2018.

[6] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, "Quantum random access codes using single d-level systems", *Phys. Rev. Lett.*, vol. 114, p. 170 502, 17 Apr. 2015. DOI: 10.1103/PhysRevLett.114.170502. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.114.170502.

[7] H. Yano, Y. Suzuki, K. M. Itoh, R. Raymond, and N. Yamamoto, "Efficient discrete feature encoding for variational quantum classifier", *IEEE Transactions on Quantum Engineering*, vol. 2, pp. 1–14, 2021.

[8] G. Foletto, L. Calderaro, G. Vallone, and P. Villoresi, "Experimental demonstration of sequential quantum random access codes", *Physical Review Research*, vol. 2, no. 3, p. 033 205, 2020.

[9] 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*, vol. 125, no. 8, p. 080 403, 2020.

[10] X.-R. Wang, L.-Y. Wu, C.-X. Liu, T.-J. Liu, J. Li, and Q. Wang, "Experimental generation of entanglement-assisted quantum random access code", *Physical Review A*, vol. 99, no. 5, p. 052 313, 2019.

[11] Y. Xiao, X.-H. Han, X. Fan, H.-C. Qu, and Y.-J. Gu, "Widening the sharpness modulation region of an entanglement-assisted sequential quantum random access code: Theory, experiment, and application", *Physical Review Research*, vol. 3, no. 2, p. 023 081, 2021.

[12] F. Buscemi, E. Chitambar, and W. Zhou, "Complete resource theory of quantum incompatibility as quantum programmability", *Phys. Rev. Lett.*, vol. 124, p. 120 401, 12 Mar. 2020. DOI: 10.1103/PhysRevLett.124.120401. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.124.120401.

[13] P. Skrzypczyk, I. Šupi ć, and D. Cavalcanti, "All sets of incompatible measurements give an advantage in quantum state discrimination", *Phys. Rev. Lett.*, vol. 122, p. 130 403, 13 Apr. 2019. DOI: 10.1103/PhysRevLett.122.130403. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.122.130403.

[14] C. Carmeli, T. Heinosaari, and A. Toigo, "Quantum random access codes and incompatibility of measurements", *EPL (Europhysics Letters)*, vol. 130, no. 5, p. 50 001, Jun. 2020. DOI: 10.1209/0295-5075/130/50001. [Online]. Available: https://doi.org/10.1209/0295-5075/130/50001.

[15] R. Salazar, T. Biswas, J. Czartowski, K. Życzkowski, and P. Horodecki, "Optimal allocation of quantum resources", *Quantum*, vol. 5, p. 407, 2021.

[16] S. Designolle, M. Farkas, and J. Kaniewski, "Incompatibility robustness of quantum measurements: A unified framework", *New Journal of Physics*, vol. 21, no. 11, p. 113 053, Nov. 2019. DOI: 10.1088/1367-2630/ab5020. [Online]. Available: https://dx.doi.org/10.1088/1367-2630/ab5020.

[17] M. Farkas and J. Kaniewski, "Self-testing mutually unbiased bases in the prepare-and-measure scenario", *Physical Review A*, vol. 99, no. 3, p. 032 316, 2019.

[18] D. Cozzolino, B. Da Lio, D. Bacco, and L. K. Oxenløwe, "High-dimensional quantum communication: Benefits, progress, and future challenges", *Advanced Quantum Technologies*, vol. 2, no. 12, p. 1 900 038, 2019.

[19] ITU. "Dwdm itu grid". (2021), [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.694.1-202010-I!!PDF-E&type=items (visited on 03/30/2023).

[20] D. Ribezzo, M. Zahidy, I. Vagniluca, *et al.*, "Deploying an inter-european quantum network", *Advanced Quantum Technologies*, vol. 6, no. 2, p. 2 200 061, 2023.

[21] D. Bacco, I. Vagniluca, D. Cozzolino, *et al.*, "Toward fully-fledged quantum and classical communication over deployed fiber with up-conversion module", *Advanced Quantum Technologies*, vol. 4, no. 7, p. 2 000 156, 2021.

[22] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum random access codes with shared randomness", *arXiv preprint arXiv:0810.2937*, 2008.

[23] A. Boaron, B. Korzh, R. Houlmann, *et al.*, "Simple 2.5 ghz time-bin quantum key distribution", *Applied Physics Letters*, vol. 112, no. 17, p. 171 108, 2018.