Semi-device independent certification of multiple unsharpness parameters through sequential measurements

Sumit Mukherjee* and A. K. Pan†
National Institute of Technology Patna, Ashok Rajpath, Patna, Bihar 800005, India

Based on a sequential communication game, semi-device independent certification of an unsharp instrument has recently been demonstrated [New J. Phys. 21 083034 (2019), Phys. Rev. Research 2, 033014 (2020)]. In this paper, we provide semi-device independent self-testing protocols in the prepare-measure scenario to certify multiple unsharpness parameters along with the states and the measurement settings. This is achieved through the sequential quantum advantage shared by multiple independent observers in a suitable communication game known as parity-oblivious random-access-code. We demonstrate that in 3-bit parity-oblivious random-access-code, at most three independent observers can sequentially share quantum advantage. The optimal pair (triple) of quantum advantages enables us to uniquely certify the qubit states, the measurement settings, and the unsharpness parameters. The practical implementation of a given protocol involves inevitable losses. In a sub-optimal scenario, we derive a certified interval within which a specific unsharpness parameter has to be confined. We extend our treatment to the 4-bit case and show that at most two observers can share quantum advantage for the qubit system. Further, we provide a sketch to argue that four sequential observers can share the quantum advantage for the two-qubit system, thereby enabling the certification of three unsharpness parameters.

I. INTRODUCTION

Bell’s theorem [1] is regarded by many as one of the most profound discoveries of modern science. This celebrated no-go proof asserts that any ontological model satisfying locality cannot account for all quantum statistics. This feature is commonly demonstrated through the quantum violation of suitable Bell inequalities. Besides the immense conceptual insights Bell’s theorem adds to the quantum foundations research, it provides a multitude of practical applications in quantum information processing (see, for extensive reviews, [2–4]). Moreover, the non-local correlation is device-independent, i.e., no characterization of the devices is needed to be assumed. Only the observed output statistics are enough to certify non-locality. The device-independent non-local correlation is used as a resource for secure quantum key distribution [5–8], randomness certification [9–12], witnessing Hilbert space dimension [13–20] and for achieving advantages in communication complexity tasks [21].

Optimal quantum value of a given Bell expression enables device-independent certification of state and measurements commonly known as self-testing [22–25]. For example, optimal violation of CHSH inequality self-tests the maximally entangled state and mutually anti-commuting local observables. Note that the device-independent certification encounters practical challenges arises from the requirement of the loophole-free Bell test. Such tests have recently been realized [26–30] enabling experimental demonstrations of device-independent certification of randomness [31, 32]. However, practically such a loophole-free certification of non-local correlation remains an uphill task.

In recent times, there is an upsurge of interest in semi-device independent (SDI) protocols in prepare-measure scenario [22–24, 33–46, 48]. It is less cumbersome than full device-independent test and hence experimentally more appealing. In most of the SDI certification protocols, it is commonly assumed that there is an upper bound on dimension, but otherwise the devices remain uncharacterized. Of late, a flurry of SDI protocols has been developed for certifying the states and sharp measurements [22], non-projective measurements [41, 42], mutually unbiased bases [23], randomness [33–35]. Very recently, the SDI certification of unsharpness parameter has been reported [43–46].

In this work, we provide interesting SDI protocols in the prepare-measure scenario to certify multiple unsharpness parameters. This is demonstrated by examining the quantum advantage shared by multiple observers. Sharing various forms of quantum correlations by multiple sequential observers has recently received considerable attention among researchers. Quite many works [49–54] have recently been reported to examine at most how many sequential observers can share different quantum correlations, viz., entanglement, coherence, non-locality, and preparation contextuality. Any such sharing of quantum correlation protocol requires the prior observers to perform unsharp measurements [55] represented by a set of positive operator valued measures (POVMs). This allows the subsequent observer to extract the quantum advantage. In ideal sharp measurements [56], the system collapses to one of the eigenstates of the measured observable. From an information-theoretic perspective, the information gained in sharp measurement is maximum; thereby, the system is most disturbed. It may be natural to expect that the projective measurement provides an optimal advantage in contrast to POVMs, but there are certain tasks where unsharp measurement showcases its supremacy over projective measurement. Examples include sequential quantum state discrimination [57, 58], unbounded randomness certification [59] and many more.

However, the statistics corresponding to POVMs can be simulated by projective measurements unless they are extremal ones [60]. The unsharp POVMs that are the noisy variants of sharp projective measurements can be simulated through the classical post-processing of ideal projective mea-
**POVMs** are implemented differently, leading to different post-measurement states. The same optimal quantum value of a Bell expression may be obtained even when the POVMs are implemented differently, subject to imperfections for various reasons, and emerging quantum technologies demand certified instruments for conclusive experimental tests. Standard self-testing protocols certify the states and measurements based on the optimal quantum value, but such protocols do not certify the post-measurement states. The same optimal quantum value, the post-measurement states. But the sequential measurements have the potential to certify the post-measurement states and consequently the unsharpness parameter.

Recently, in an interesting work, such a certification was put forwarded by Mohan, Tavakoli and Brunner (henceforth, MTB) [43] through the sequential quantum advantages of two independent observers in an SDI prepare-measure communication game. In particular, they have considered 2-bit Random-access code (RAC) and showed that two sequential observers can get the quantum advantage at most. Both the observers cannot have optimal quantum advantages, but there exists an optimal trade-off between quantum advantages of two sequential observers, enabling the certification of the prepared qubit states and measurement settings. Another interesting protocol for the same purpose is proposed in [44], but significantly differs from the approach used in [43]. MTB protocol [43] also provided a certified interval of values of sharpness parameter in the loss tolerant scenario. MTB proposal has been experimentally tested in [45–47].

Against this backdrop, natural questions may arise, such as whether two or more independent unsharp parameters can be certified and the certified interval of values of unsharp parameter of a measurement instrument can be fine-tuned. Here we answer both the questions affirmatively. Intuitively, two or more unsharp parameters can be certified if multiple independent observers can share the quantum advantage. In such a case, the certified interval of unsharp parameters of a measurement instrument will also be fine-tuned. By using a straightforward mathematical approach, we provide SDI prepare-measure protocols to demonstrate that more than two sequential observers can share the quantum advantage, thereby enabling us to certify multiple unsharpness parameters instead of a single unsharpness parameter as it is in [43, 44]. However, in the practical scenario, the perfect optimal quantum correlations cannot be achieved. In such a case, we derive an interval of unsharpness parameter using the sub-optimal witness pair. The closer the observed statistics are to the optimal values, the narrower is the interval to which the sharpness parameter can be confined. We also provide a methodology for how sequential measurement schemes can be used to fine-tune a certified interval of the unsharpness parameter of a quantum measurement device. Furthermore, we argue that the higher the number of observers shares the quantum advantage narrower the certified interval.

We first propose the aforementioned SDI certification scheme based on 3-bit RAC in a prepare-measure scenario and demonstrate that at most, three independent observers can share the quantum advantage sequentially. Throughout this paper, we assume that the quantum system to be a qubit; otherwise, the devices remain uncharacterized. We show that the optimal pair of quantum advantage corresponding to the first two observers certifies the first observer’s unsharpness parameter, and the optimal triple of quantum advantage provides the certification of unsharpness parameters of the first two observers. As indicated earlier, we further provide a fine-tuning of the interval of values of unsharpness parameter compared to the 2-bit RAC presented in [43]. We also show that if the quantum advantage is extended to a third sequential observer, then the interval of values of unsharpness parameter for the first observer can be more fine-tuned, thereby certifying a narrow interval in the sub-optimal scenario. This scheme is further extended to the 4-bit case, where we demonstrate that at least two observers can share quantum advantage for a qubit system. If the two-qubit system is taken, four independent observers can share the quantum advantage at most. We provide a sketch of how to certify three unsharpness parameters corresponding to the first three observers and the input two-qubit states and measurement settings.

This paper is organized as follows. In Sec. II, we discuss a general n-bit quantum parity-oblivious RAC. In section III, we explicitly consider the 3-bit case and find the optimal and sub-optimal relationships between sequential success probabilities for two observers. In Sec. IV, we generalize the scenario to three or more observers. In Sec. V we discuss the certification of multiple unsharpness parameters when the third observer gets the quantum advantage. In Sec. VI, we extend the protocol for the 4-bit case. We discuss our results in Sec. VII.

### II. PARITY-OBLIVIOUS RANDOM-ACCESS-CODE

We start by briefly encapsulating the notion of parity-oblivious RAC which is used here as a tool to demonstrate our results. It is a two-party one-way communication game. The n-bit RAC [61] in terms of a prepare-measure scenario that involves a sender (Alice), who has a length-n string x, randomly sampled from x ∈ {0, 1}n. On the other hand, a receiver (Bob) receives uniformly at random, index y ∈ {1, 2, ..., n} as his input. Bob’s task is to recover the bit x_y with a probability. In an operational theory, Alice encodes her n-bit string x into the states prepared by a procedure P_x. After receiving the system, for every y ∈ {1, 2, ..., n}, Bob performs a two-outcome measurement M_y and reports outcome b as his output. As mentioned, the winning condition of the game is b = x_y, i.e., Bob has to predict the y-th bit of Alice’s input string x correctly. Then the average success probability of the game is given by,

\[
S_n(b = x_y) = \frac{1}{2^n} \sum_{x,y} p(b = x_y | P_x, M_y).
\] (1)

Now, to help Bob, Alice can communicate some bits to him over a classical communication channel. The game becomes trivial if Alice communicates n number of bits to Bob, and Non-triviality may arise if Alice communicates less than that. For our purpose here, we impose a constraint - the parity-oblivious condition [62] that has to be satisfied by Alice’s
inputs. This demands that Alice can communicate any number of bits to Bob, but that must not reveal any information about the parity of Alice’s input. The parity-oblivious condition eventually provides an upper bound on the number of bits that can be communicated.

Following Spekkens et al. [62], we define a parity set \( \mathbb{P}_n = \{ x | x \in \{0,1\}^n, \sum x_r \geq 2 \} \) with \( r \in \{1,2,...,n\} \). Explicitly, the parity-oblivious condition dictates that for any \( s \in \mathbb{P}_n \), no information about \( s \cdot x = \Theta_r s_r x_r \) (s-parity) is to be transmitted to Bob, where \( \Theta \) is sum modulo 2. We then have s-parity 0 and s-parity-1 sets. Explicitly, the parity-oblivious condition demands that in an operational theory the following relation is satisfied,

\[
\forall s : \frac{1}{2^{n-1}} \sum_{x | x, s = 0} P(P_s | b, M_x) = \frac{1}{2^{n-1}} \sum_{x | x, s = 1} P(P_s | b, M_x).
\]  

(2)

For example, when \( n = 2 \) the set is \( \mathbb{P} = \{11\} \), so no information about \( x_1 \oplus x_2 \) can be transmitted by Alice. It was shown in [62] that the parity-oblivious condition in the \( n \)-bit case, the communication from Alice to Bob has to be restricted to be one bit.

The maximum average success probability in such a classical \( n \)-bit parity-oblivious RAC is \( (n + 1)/2n \). While the explicit proof can be found in [62], a simple trick can saturate the bound as follows. Assume that Alice always encodes the first bit (prior agreement between Alice and Bob) and sends it to Bob. If \( y = 1 \), occurring with probability \( 1/n \), Bob can predict the outcome with certainty, and for \( y \neq 1 \), occurring with the probability of \( (n - 1)/n \), he at best guesses the bit with probability \( 1/2 \). Hence the total probability of success is derived [62] as

\[
(S_n(b = x_y))_r \leq \frac{1}{n} + \frac{(n - 1)}{2n} = \frac{1}{2} \left(1 + \frac{1}{n}\right).
\]  

(3)

In quantum RAC, Alice encodes her length-\( n \) string \( x \in \{0,1\}^n \) into quantum states \( \rho^n_x \), prepared by a procedure \( P_x \). Bob performs a two-outcome measurement \( M_y \) for every \( y \in \{1,2,...,n\} \) and reports outcome \( b \) as his output. Average success probability in quantum theory can then be written as,

\[
S_n = \frac{1}{2^n n} \sum_{y=1}^{n} \sum_{x \in \{0,1\}^n} \text{Tr}[\rho^n_x M_{b|y}].
\]  

(4)

The parity-oblivious constraint imposes the following condition to be satisfied by Alice’s input states,

\[
\forall s : \frac{1}{2^{n-1}} \sum_{x | x, s = 0} \rho^n_x = \frac{1}{2^{n-1}} \sum_{x | x, s = 1} \rho^n_x.
\]  

(5)

It has been shown in [62, 63] that the optimal quantum success probability for 2-bit parity-oblivious RAC is \( (S_2)^{opt} = (1/2)(1 + 1/\sqrt{2}) \) and 3-bit case is \( (S_3)^{opt} = (1/2)(1 + 1/\sqrt{3}) \). In both the cases, the qubit system is enough to obtain the optimal quantum value. But, for \( n > 3 \) one requires higher dimensional system. In entanglement assisted variant of parity-oblivious RAC with \( n > 3 \), optimal values of success probabilities achievable with qubit systems were found in [20]. However, in this work we consider the prepare-measure scenario and hence we separately prove the results for \( n = 3 \) and \( n = 4 \).

A remark on the ontological model of quantum theory could be useful to understand the type of non-classicality appearing in parity-oblivious quantum RAC. The satisfaction of parity-oblivious condition in an operational theory implies that no measurement can distinguish the parity of the inputs. This is regarded as an equivalent class of preparations [64, 65, 67] which will have equivalent representation at the level of the ontic states. It has been demonstrated in [62] that the parity-obliviousness at the operational level must be satisfied at the level of ontic states if the ontological model of quantum theory is preparation non-contextual. Thus, in a preparation non-contextual model, the classical bound remains the same as given in Eq.(3). Quantum violation of this bound thus demonstrates a form of non-classicality - the preparation contextuality. Throughout this paper, by quantum advantage, we refer to the violation of preparation non-contextuality (unless stated otherwise) but to avoid clumsiness, we skip detailed discussion about it. We refer [62, 64, 65, 67] for detailed discussion about it.

We first consider the 3-bit parity-oblivious RAC and demonstrate that three independent Bobs can sequentially share the quantum advantage at most by assuming the quantum system to be a qubit. We then demonstrate how this sequential measurement scenario enables the SDB certification of multiple unsharpness parameters along with the qubit states and the measurement settings. We note here that the MTB protocol was extended [68] for 3-bit standard RAC to certify a single unsharpness parameter. In our work, we consider the parity-oblivious RAC and certify multiple unsharpness parameters. While the mathematical approach in [68] follows the MTB protocol[43], our approach is quite different from [43, 68]. Also, we extend our approach to 4-bit standard and parity-oblivious RACs and provide some important results in Sec. VI.

III. SEQUENTIAL QUANTUM ADVANTAGE IN 3-BIT RAC

In sequential quantum RAC [22], multiple independent observers perform a prepare-transform-measure task. Alice encodes her bit into a quantum system and sends it to the next observer (say, Bob). There are one Alice and multiple numbers of independent Bobs. After receiving the system, first Bob (say, Bob_1) performs random measurements to decode the information and relays the system to the second Bob (Bob_2), who does the same as the first Bob. The chain continues until \( k^{th} \) Bob (where \( k \) is arbitrary and has to be determined) gets the quantum advantage.

Before examining how many independent Bobs can get quantum advantage sequentially in a 3-bit RAC, let us first discuss the classical RAC task in sequence. When the physical devices are classical, the states that are being sent by Alice...
are diagonal in the same basis on which multiple independent Bobs perform their measurements sequentially. In that case, the measurement of first Bob does not disturb the system, and hence decoding measurement for second Bob will not be influenced by the first Bob. In other words, there exists no trade-off between sequential Bobs, and each of them can obtain optimal classical success probability. The range in which classical success probabilities of standard RAC lie is $\frac{1}{2} \leq (S_1, S_2, \ldots, S_L) \leq \frac{3}{4}$. However, in parity-oblivious RAC, as explained in Sec. II, classical success probabilities lie in $\frac{1}{2} \leq (S_1, S_2, \ldots, S_L) \leq \frac{3}{4}$. We find that at most, two independent Bobs can share quantum advantage, the measurements of previous Bobs have to be so sharpened that they are just enough to reveal the quantum advantage, the measurements of previous Bobs have to be so unsharpen POVMs. To obtain the maximum number of independent Bobs who can share quantum advantage, the measurements of previous Bobs have to be so unsharpen that they are just enough to reveal the quantum advantage. We find that at most, two independent Bobs can share quantum advantage in 3-bit standard RAC, but at most three Bobs can share quantum advantage in 3-bit parity-oblivious RAC.

In 3-bit sequential quantum RAC, Alice randomly encodes her three bit string $x = (x_0, x_1, x_2) \in \{0, 1\}^3$ into eight qubits $\rho^0_x$ and sends them to Bob$_1$. After receiving the system, Bob$_1$ randomly performs unsharp measurement (with unsharpness parameter $\lambda_1$) of dichotomic observables $B_{y_1}$, $(y_1 = 1, 2, 3)$ and relays the system to Bob$_2$ who carries out unsharp measurement of the observables $B_{y_2}$ with $y_2 = 1, 2, 3$ with unsharpness parameter $\lambda_2$ and so on. The scheme is depicted in figure Fig1. Each Bob examines if quantum advantage over classical RAC is obtained and for the $k^{th}$ Bob if the advantage is not obtained then the process stops. Let us also define the measurement observables of Bob$_1$ as $B_{y_1}$ with $y_1 \in \{1, 2, 3\}$. Here we assume that a particular observer (say Bob$_2$) is provided with different possible measurement instruments with same value of unsharpness parameters $\lambda_k$. Although, each Bob can take different values to the unsharpness parameters for different measurement settings, for our purpose it is sufficient to assume the same value of unsharpness parameters for all the measurement settings that a particular Bob uses.

If $k^{th}$ Bob’s instruments are characterized by Kraus operators $\{K_{k|y_k}\}$ then after $k^{th}$ Bob’s measurement, the average state relayed to Bob$_{k+1}$ is given by

$$\rho^k_x = \sum_{y_k} K_{k|y_k} \rho^{k-1}_x K_{k|y_k}^\dagger,$$  \hspace{1cm} (6)

where $\forall k, b_k \in \{0, 1\}$ and $\sum_{b_k} K_{k|y_k}^\dagger K_{k|y_k} = I$ and $K_{k|y_k} = U \sqrt{M_{k|y_k}}$ where $U$ is an unitary operator. For simplicity, here we set $U = I$, and our arguments remains valid up to any unitary transformation. Here $M_{b_k|y_k} = (\mathbb{1} + \lambda_k (\pm 1)^{y_k} b_k \cdot \sigma) / 2$ is the POVM corresponding to the result $b_k$ of measurement $B_{y_k}$.

The Kraus operators for $k^{th}$ Bob can be written as, $K_{\pm y_k} = \sqrt{\frac{(1+\lambda_k)}{2}} P_{y_k} + \sqrt{\frac{(1-\lambda_k)}{2}} P_{y_k}$ and $P_{y_k} = (\mathbb{1} \pm B_{y_k}) / 2$ are the projectors and $\lambda_k$ is the unsharpen parameter. Here $\alpha_k = \frac{1}{2} \sqrt{\frac{(1+\lambda_k)}{2}} \sqrt{\frac{(1+\lambda_k)}{2}}$ and $\beta_k = \frac{1}{2} \sqrt{\frac{(1+\lambda_k)}{2}} \sqrt{\frac{(1-\lambda_k)}{2}}$.

By using Eq. (4) the quantum success probability for the $k^{th}$ Bob can be written as,

$$S_3^k = \sum_{y_1} \sum_{y_2} \sum_{y_3} Tr[\rho^{k-1}_x M_{b_k|y_k}] \cdot$$ \hspace{1cm} (7)

Let us consider that Alice’s eight input qubit states $\rho^0_x = \frac{1 + d_x \cdot \sigma}{2}$ where $d_x$ is the Bloch vector with $||d_x|| \leq 1$. By using Eq. (7), the quantum success probability for Bob$_1$ can be written as

$$S_3^1 = \sum_{y_1} \sum_{y_2} \sum_{y_3} Tr[\rho^{0,0}_x M_{b_1|y_1}] \cdot$$ \hspace{1cm} (8)

We consider that $M_{b|y}$ are unbiased POVMs represented by $M_{b|y} = (\mathbb{1} + 4\alpha_1 \beta_1 (\pm 1)^{y_1} B_{y_1}) / 2$. Using it in Eq. (8) and further simplifying, we get

$$S_3^1 = \frac{1}{2} + \alpha_1 \beta_1 \sum_{y_1=1,2,3} (\beta_{y_1} m_y \cdot b_{y_1}),$$ \hspace{1cm} (9)

where $m_y = ||m_y|| \cdot m_y$ ($m_y$ is the unit vector) are unnormalized vectors can explicitly be written as,

$$m_1 = (\hat{d}_{000} - \hat{d}_{111}) + (\hat{d}_{001} - \hat{d}_{110}) + (\hat{d}_{010} - \hat{d}_{101}) + (\hat{d}_{100} - \hat{d}_{011})$$

$$m_2 = (\hat{d}_{000} - \hat{d}_{111}) + (\hat{d}_{001} - \hat{d}_{110}) + (\hat{d}_{010} - \hat{d}_{101}) + (\hat{d}_{100} - \hat{d}_{011})$$

$$m_3 = (\hat{d}_{000} - \hat{d}_{111}) - (\hat{d}_{001} - \hat{d}_{110}) + (\hat{d}_{010} - \hat{d}_{101}) + (\hat{d}_{100} - \hat{d}_{011}).$$ \hspace{1cm} (10)

Next, if Bob$_1$ performs unsharp measurements then the average state that is relayed to Bob$_2$ is obtained from Eq. (6) and is given by,

$$\rho^1_x = \frac{1}{2} (I + d_x \cdot \sigma),$$ \hspace{1cm} (11)

where

$$d_x = 2 (\alpha_1^2 - \beta_1^2) d_x + \frac{4\beta_1^2}{3} \sum_{y_1=1,2,3} (b_{y_1} \cdot d_x) b_{y_1} \cdot$$ \hspace{1cm} (12)

is the Bloch vector of the reduced state. The quantum success probability for Bob$_2$ is calculated by using Eqs.(7) and (12).
FIG. 1: Prepare-transform-measure Block diagram for sequential encoding decoding scheme involving four parties. The first party gets a random three-bit string which she encodes into a qubit system. It is being sent to the next party, who thereby performs three binary outcome measurements at random to decode the message and send the system to the next party and so on.

As,

\[ S_3^2 = \frac{1}{24} \sum_{x \in \{0,1\}^3} \sum_{y \in \{1,2,3\}} Tr[\rho_x^y M_{y \rightarrow y_2}] = \frac{1}{2} + \frac{1}{48} \left[ 2(\alpha_1^2 - \beta_1^2) \sum_{r \neq y_2=1,2,3} (\delta_{r,y_2} \cdot \hat{b}_{y_2}) \right] + \frac{4\beta_2^2}{3} \sum_{r \neq y_2=1,2,3} (\delta_{y_2} \cdot \hat{b}_{y_2_2}) (\hat{b}_{y_2} \cdot \hat{b}_{y_2}), \tag{13} \]

In order to find the optimal trade-off between the success probabilities of Bob_{1} and Bob_{2}, the maximum quantum value of S_3^2 for the given value of S_1^2 has to be derived. This leads to an optimization of S_3^2 over all \rho_x^y, \hat{b}_{y_1} and \hat{b}_{y_2}. To optimize S_3^2 we note that the states \rho_x^y prepared by Alice should be pure i.e., ||\delta|| = 1. Otherwise the magnitudes ||\tilde{m}_r||s decrease leading to an decrement of overall success probability. Again, we must have antipodal pairs (joining vertices of a unit cube inside the Bloch sphere) constituting each \tilde{m}_r in Eq. (10). So overall maximization of S_3^2 requires the following: \tilde{d}_{000} = -\tilde{d}_{111}, \tilde{d}_{001} = -\tilde{d}_{100}, \tilde{d}_{010} = -\tilde{d}_{101} and \tilde{d}_{100} = -\tilde{d}_{011}. From this choice we can rewrite the \tilde{m}_r_s as, \tilde{m}_1 = 2(\tilde{d}_{000} + \tilde{d}_{001} + \tilde{d}_{010} - \tilde{d}_{100}) , \tilde{m}_2 = 2(\tilde{d}_{000} + \tilde{d}_{010} - \tilde{d}_{100}) and \tilde{m}_3 = 2(\tilde{d}_{000} - \tilde{d}_{010} + \tilde{d}_{100}).

It is seen from Eq. (13) that as \alpha_1 > \beta_1 so for the maximization of S_3^2 we must have \tilde{m}_r to be along the direction of \hat{b}_{y_2} when r = y_2. We can then write

\[ S_3^2 \leq \frac{1}{2} + \frac{1}{48} \left[ 2(\alpha_1^2 - \beta_1^2) \sum_{r \neq y_2=1,2,3} ||\tilde{m}_r|| \right] + \frac{4\beta_2^2}{3} \sum_{r \neq y_2=1,2,3} (\tilde{m}_r \cdot \hat{b}_{y_2}) (\hat{b}_{y_2} \cdot \hat{b}_r), \tag{14} \]

Using concavity of the square root \sum_{y_2=1}^3 ||\tilde{m}_r||^2 \leq \sqrt{3} \sum_{y_2=1}^3 ||\tilde{m}_r||^2 and putting the expressions of \tilde{m}_r_s, we have

\[ \sum_{y_2=1}^3 ||\tilde{m}_r|| \leq 2 \sqrt{48 - 3 (\tilde{d}_{000} - \tilde{d}_{001} - \tilde{d}_{010} - \tilde{d}_{100})^2}. \tag{15} \]

We can then get max(\sum_{y_2=1}^3 ||\tilde{m}_r||) = 8 \sqrt{3} when the condition

\[ \tilde{d}_{000} - \tilde{d}_{001} - \tilde{d}_{010} - \tilde{d}_{100} = 0 \tag{16} \]

in Eq. (15) is satisfied. This in turn provides each of the ||\tilde{m}_r|| is 8/\sqrt{3} when equality in Eq. (15) holds. The condition in Eq. (16) leads the following relations between the input Bloch vectors, \tilde{d}_{000}, \tilde{d}_{001}, \tilde{d}_{001}, \tilde{d}_{010} = 1, \tilde{d}_{000} \cdot \tilde{d}_{001} - \tilde{d}_{000} \cdot \tilde{d}_{010} = \tilde{d}_{000} \cdot \tilde{d}_{010} = \tilde{d}_{000} \cdot \tilde{d}_{010} = \tilde{d}_{010} \cdot \tilde{d}_{010} = 1, \tilde{d}_{000} \cdot \tilde{d}_{010} = \tilde{d}_{010} \cdot \tilde{d}_{010} = \tilde{d}_{010} \cdot \tilde{d}_{010} = 1. Solving the above set of relations one finds \tilde{d}_{000} = -\tilde{d}_{001} = -\tilde{d}_{010} = -\tilde{d}_{100} = 0. Further by noting that ||\tilde{m}_r|| = ||\hat{m}_r||, we get \tilde{d}_x \cdot \tilde{d}_x = \left( +\frac{1}{3} \right) \delta_{x'x} for x = 000, x' \in (001, 010, 100) and \tilde{d}_x \cdot \tilde{d}_x = \left( -\frac{1}{3} \right) \delta_{x'x} for other combinations of x and x' where x' \neq x and \tilde{d}_x \cdot \tilde{d}_x = 1 for x' = x. It can be easily checked that the four unit vectors \tilde{d}_{000}, \tilde{d}_{101}, \tilde{d}_{101} and \tilde{d}_{100} form a regular tetrahedron when represented on the Bloch sphere.

Impinging the above conditions into Eq. (10) we immediately get, \tilde{m}_r \cdot \tilde{d}_x = \delta_{x'r}, i.e., \tilde{m}_1, \tilde{m}_2 and \tilde{m}_3 are mutually orthogonal unit vectors. Without loss of generality we can then fix \tilde{m}_1 = \hat{x}, \tilde{m}_2 = \hat{y} and \tilde{m}_3 = \hat{z}. This implies that the maximum value max(S_3^2) = \Delta_2 can be obtained when the unit vectors of Bob_{2} are \hat{b}_{y_2=1} = \hat{x}, \hat{b}_{y_2=2} = \hat{x} and \hat{b}_{y_2=3} = \hat{z}. It is then straightforward to understand from the last part of Eq. 23.
Fig. 2 represents the optimal trade-off characteristics between $\Delta_1$ and $\Delta_2$. The blue line corresponds to the maximum success probability in classical strategy showing no information-disturbance trade-off between the measurements. Each observer can get maximum success probability without any dependence on other observers. On the other hand, the optimal pair $(\Delta_2, \Delta_1)$ in quantum theory provide a trade-off. The more the Bob disturbs the system more the information is gained by him, and $\Delta_1$ increases. This eventually decreases the success probability $\Delta_2$ of Bob2 and vice-versa. The orange curve gives the trade-off for quantum success probabilities, and each point on it certifies a unique value of unsharpness parameter $\lambda$. For example when Bob1 and Bob2 gets equal quantum advantage, i.e., $\Delta_1 = \Delta_2 = (17 + \sqrt{3})/26 \approx 0.72$, the sharpness parameter of the Bob1 is $\lambda_1 = (4 \sqrt{3} + 3)/13 \approx 0.763$. This is shown in Fig. 2 by the blue point on the orange curve. Similarly, each point in the orange region in Fig. 2 certify an unique value of $\lambda_1$.

Thus the optimal pair $(\Delta_1, \Delta_2)$ uniquely certify the preparation of Alice and measurements of Bob1 and Bob2, and the unsharpness parameter $\lambda$. The certification statements are the following.

(i) Alice has encoded her message into the eight quantum states that are pure and pairwise antipodal represented by points at the vertices of a unit cube inside the Bloch sphere. One of the examples is, $\rho_{000} = (\hat{x} + \hat{y} + \hat{z})/\sqrt{3}, \rho_{001} = (\hat{x} - \hat{y} + \hat{z})/\sqrt{3}, \rho_{010} = (-\hat{x} + \hat{y} + \hat{z})/\sqrt{3}, \rho_{100} = (\hat{x} - \hat{y} - \hat{z})/\sqrt{3}$ and their respective antipodal pairs.

(ii) Bob1 performs unsharp measurement corresponding to the observables along three mutually unbiased bases, say, $B_1 = \lambda_1 \sigma_x, B_2 = \lambda_1 \sigma_y$ and $B_3 = \lambda_1 \sigma_z$ where $\lambda_1 = \sqrt{3}/(2\Delta_1 - 1)$. Bob2’s measurement settings are same as Bob1 but sharp measurement of rank one projective value measures.

It is important to note here that the input states those provides the optimal pair $(\Delta_1, \Delta_2)$ must satisfy the parity-oblivious condition in quantum theory. Otherwise the comparison between the classical and quantum bounds becomes unfair. For $n = 3$ the parity set $\mathbb{P}_3$ contains four elements $\mathbb{P}_3 := \{011, 101, 110, 111\}$. For every element $s \in \mathbb{P}_3$ the parity-oblivious condition given by Eq. (5) has to be satisfied. We see that for $s = 011$, Alice’s input states satisfy the parity-oblivious condition, $(\rho_{000} + \rho_{100} + \rho_{001} + \rho_{110})/4 = (\rho_{010} + \rho_{101} + \rho_{011} + \rho_{111})/4 = 1/2$. This is due to the fact that for the optimal pair $(\Delta_1, \Delta_2)$ one requires antipodal pairs, i.e., $(\rho_{000} + \rho_{100})/2 = (\rho_{011} + \rho_{111})/2 = 1/2$ and $(\rho_{010} + \rho_{101})/2 = (\rho_{011} + \rho_{111})/2 = 1/2$. Similarly, for $s = 101$ and $s = 110$ the parity-oblivious condition is automatically satisfied and constitute a trivial constraint to Alice’s inputs. But for $s = 111$, to satisfy parity-oblivious condition Alice’s input must satisfy the relation $(\rho_{111} + \rho_{100} + \rho_{001} + \rho_{010})/4 = (\rho_{010} + \rho_{101} + \rho_{011} + \rho_{110})/4 = 1/2$. This demands a non-trivial relation to be satisfied by Alice’s inputs is $d_{000} - d_{001} - d_{010} - d_{100} = 0$. Interestingly, this is the condition which was required to obtain $\Delta_2$ and $\Delta_1$ in Eq. (16). Thus, Alice’s input satisfy the parity-oblivious constraint as imposed in the classical RAC.

\begin{align}
\Delta_1 &= \frac{1}{2} \left( 1 + \frac{\lambda_1}{\sqrt{3}} \right); \quad \Delta_2 = \frac{1}{2} \left( 1 + \frac{1 + 2 \sqrt{1 - \lambda_1^2}}{3 \sqrt{3}} \right) \\
\Delta_2(\Delta_1) &= \frac{1}{2} \left( 1 + \frac{1 + 2 \sqrt{12\Delta_1 - 12\Delta_1^2 - 2}}{6 \sqrt{3}} \right). 
\end{align}
A. Sub-optimal scenario

Note that there are many practical reasons due to which the precise certification may not be possible in the real experimental scenario. In other words, the optimal pair of success probabilities may not be achieved in a practical scenario, and hence certification of $\lambda_1$ may not be possible uniquely. We argue that even in sub-optimal scenarios when $\delta_3^2 \leq \Delta_1$ and $\delta_2^2 \leq \Delta_2$ the certification of an interval of values of $\lambda_1$ is possible from our protocol.

From Eq. (19) we find that $\Delta_1$ can provide a lower bound $(\lambda_1)^{\min}$ to the unsharpness parameter $\lambda_1$ as,

$$\lambda_1 \geq \sqrt{3}(2\Delta_1 - 1) \equiv (\lambda_1)^{\min},$$

and the upper bound $(\lambda_1)^{\max}$ of $\lambda_1$ as,

$$\lambda_1 \leq \sqrt{1 - \left(\frac{3\sqrt{3}(2\Delta_1 - 1)}{2} - 1\right)^2} \equiv (\lambda_1)^{\max}.$$ (22)

Here we assumed that Bob 2 performs sharp projection measurement with $\lambda_2 = 1$. Note that, both the upper and the lower bounds saturate and become equal to each other when $\Delta_2$ reaches its maximum value. Now, the quantum advantage for Bob 1 requires $\Delta_1 > 2/3$ which fixes the $(\lambda_1)^{\min} = 1/\sqrt{3} \approx 0.57$ yielding that any value of $\lambda_1 \in [1/\sqrt{3}, 1]$ provides quantum advantage for Bob 1. Again as there is a trade-off between $\Delta_1$ and $\Delta_2$, in order to obtain the quantum advantage for Bob 2 the value of $\lambda_1$ has the upper bound $(\lambda_1)^{\max} = \sqrt{3}/2 \approx 0.93$.

Hence, when both Bob 1 and Bob 2 get quantum advantage the following interval $0.57 \leq \lambda_1 \leq 0.93$ can be certified. The more the accuracy of the experimental observation the more precise certification of $\lambda_1$ is achieved. Importantly, this range can be further fine-tuned (in particular the upper bound) if Bob 1 gets the quantum advantage. This is explicitly discussed in the Sec. IV and Sec. V.

IV. SEQUENTIAL 3-BIT RAC FOR THREE OR MORE BOBS

Let us now investigate the case when more than two independent Bobs perform the sequential measurement. The question is how many can share quantum advantage sequentially. First, to find the success probability for Bob 3 we assume that Bob 2 performs unsharpness measurement with unsharpness parameter $\Delta_2$. By using Eq. (6) again, we calculate the average state received by Bob 3 is $\rho_3^{\hat{x}} = (\hat{\mu}_r \cdot \sigma)/2$, where

$$\hat{\mu}_r = 4 \left(\frac{1}{2} - \beta_1^a\right)\left(\frac{1}{2} - \beta_2^a\right)\hat{a}_r + \frac{8}{3} \beta_1^a \left(\frac{1}{2} - \beta_2^a\right) \sum_{y_1,y_2} (\hat{b}_{y_2} \cdot \hat{a}_r) \hat{b}_{y_1}
+ \frac{8}{3} \beta_2^a \left(\frac{1}{2} - \beta_1^a\right) \sum_{y_2,y_3} (\hat{b}_{y_3} \cdot \hat{a}_r) \hat{b}_{y_2}
+ \frac{16\beta_1^a\beta_2^a}{9} \sum_{y_1,y_2,y_3} (\hat{b}_{y_1} \cdot \hat{a}_r) (\hat{b}_{y_2} \cdot \hat{b}_{y_3}).$$

The quantum success probability for Bob 3 can then be written as,

\[
S_3 = \frac{1}{2} + \frac{1}{48} Tr \left\{ 4 \left(\frac{1}{2} - \beta_1^a\right)\left(\frac{1}{2} - \beta_2^a\right) \sum_{y_1,y_2} (\hat{b}_{y_2} \cdot \hat{b}_{y_1}) \right\}
+ \frac{8}{3} \beta_1^a \left(\frac{1}{2} - \beta_2^a\right) \sum_{y_1,y_2} (\hat{b}_{y_2} \cdot \hat{b}_{y_1})
+ \frac{8}{3} \beta_2^a \left(\frac{1}{2} - \beta_1^a\right) \sum_{y_2,y_3} (\hat{b}_{y_3} \cdot \hat{b}_{y_2})
+ \frac{16\beta_1^a\beta_2^a}{9} \sum_{y_1,y_2,y_3} (\hat{b}_{y_1} \cdot \hat{b}_{y_2}) (\hat{b}_{y_3}).
\]

Using the maximization scheme presented in Sec. III, it is straightforward to obtain that $m_a$ must be in the same direction of $\hat{b}_{y_3}$ when $r=y_3$ and $\hat{b}_{y_1}$ for $y_1 = y_2$ and so on. We can then write,

\[
S_3 \leq \frac{1}{2} + \frac{1}{6 \times 7^2} \left\{ (3\alpha_1^a - \beta_1^a)(3\alpha_2^a - \beta_2^a) \sum_{y_1,y_2} \|\hat{m}_r\| \right\} \equiv \Delta_3,
\]

where the maximum value $max(S_3^2) = \Delta_3$. It can then be seen that $S_3^2$, $S_3^2$ and $S_3^2$ can be jointly optimized if the quantity $\sum_{y_1,y_2} \|\hat{m}_r\|$ is maximized. Using the fact $max(\sum_{y_1,y_2} \|\hat{m}_r\|) = 8 \sqrt{3}$ and putting the values of $\alpha_1, \alpha_2, \beta_1$ and $\beta_2$ we have

\[
\Delta_3 = \frac{1}{2} \left( 1 + \frac{(1 + 2\sqrt{(1 - \lambda_1^3)}) (1 + 2\sqrt{(1 - \lambda_1^3)})}{9 \sqrt{3}} \right). \]

Using the values of $\Delta_1$ and $\Delta_2$ from Eq. (19), by combining them in Eq. (26) and further simplifying we find the optimal triple between success probabilities of Bob 1, Bob 2 and Bob 3, is given by,

\[
\Delta_{3,\Delta_1,\Delta_2} = \frac{1}{2} \left( 1 + \frac{\Xi_1 + 2\sqrt{(\Xi_1^2 - \Xi_2^2)}}{9 \sqrt{3}} \right),
\]

where $\Xi_1 = 1 + 2\sqrt{(12\Delta_1 - 12\Delta_1^2 - 2)}$ and $\Xi_2 = 3 \sqrt{3}(2\Delta_2 - 1)$.

This becomes nontrivial when at least one of the $\Delta_1, \Delta_2$ or $\Delta_3$ surpasses classical bound, as discussed earlier.

The above approach can be generalized for $k$th number of Bobs where $k$ is arbitrary. When Bob 3 uses optimal choice of observables, the average state relayed to $(k + 1)^{th}$ Bob can be written as $\rho_k^{\hat{x}} = \frac{1}{2} (1 + \hat{a}_r \cdot \sigma)$, where,

\[
\hat{a}_r = \prod_{i=1}^{k} \frac{(1 + 2\sqrt{(1 - \lambda_1^3)})\hat{a}_r}{3^i}.
\]
Here $\mathbf{d}_i^k$ are the Bloch vectors of the states prepared by Alice. Simply, this state is along the same direction of the initial state prepared by Alice, but the length of the the Bloch vector is shrunk by an amount, $\prod_{i=1}^{k} (1 + 2 \sqrt{1 - \lambda_i^2})/3^k$. The optimal success probability of $k^{th}$ Bob can be written as

$$\Delta_k = \frac{1}{2} \left[ 1 + \frac{1}{3^k} \prod_{i=1}^{k-1} \sqrt{3}(1 + 2 \sqrt{1 - \lambda_i^2}) \right].$$

(29)

where $k^{th}$ Bob performs sharp projective measurement. In order to examine this the longest sequence to which all Bobs can get quantum advantage, let us consider the situation when Bob$_1$, Bob$_2$ and Bob$_3$ implement their unsharp measurements with lower critical values of unsharpness parameters at their respective sites. From Eq. (29), we get the lower critical values of $\lambda$ at their respective sites. From Eq. (29), we get the lower critical values of $\lambda_1 = \frac{1}{\sqrt{3}} = 0.5773$, $\lambda_2 = 0.6578$ and $\lambda_3 = 0.7873$. Putting these values in Eq. (29) we get $\Delta_3 = 0.6575 < 2/3$ for $k = 4$, i.e., no quantum advantage is obtained for the fourth Bob.

V. CERTIFICATION OF MULTIPLE INDEPENDENT UNSHARPNESS PARAMETERS

Optimal triple of the success probabilities of Bob$_1$, Bob$_2$ and Bob$_3$ are given by Eq. (27) is plotted in Fig.3. The orange cube represents the classical success probabilities showing no trade-off. The three dimensional semi-paraboloid over the cube represents quantum trade-off between success probabilities. Each point on the surface of semi-paraboloid in Fig. 3 uniquely certify $\lambda_1$ and $\lambda_2$ while we take measurement of Bob$_3$ is projective having $\lambda_3 = 1$. For instance, let us consider the point when all the success probabilities have the equal value, $(\Delta_1, \Delta_2, \Delta_3) = (0.686, 0.686, 0.686)$. This particular point uniquely certify $\lambda_1 = 0.6443$ and $\lambda_2 = 0.7641$. We can take any arbitrary point, for example, $(\Delta_1, \Delta_2, \Delta_3) = (0.67, 0.675, 0.704)$ on the graph. This point certifies the unsharpness parameters $\lambda_1 = 0.588$ and $\lambda_2 = 0.695$.

In principle, one can uniquely certify unsharpness parameters $\lambda_1$ and $\lambda_2$ through the optimal triple but in practical scenario quantum instruments are subjected to imperfections and losses. We show that our scheme can also certify a range of values of $\lambda_1$ and $\lambda_2$. When all the three Bobs get quantum advantage, the optimal values of success probabilities fix the range of $\lambda_1$ and $\lambda_2$ obtained from Eqs. (19) and (26) are respectively given by

$$\sqrt{3}(2\Delta_1 - 1) \leq \lambda_1 \leq \sqrt{1 - \left( \frac{3 \sqrt{3}(2\Delta_2 - 1) - 1}{2\Delta_2} \right)^2}).$$

(30)

and

$$\frac{3 \sqrt{3}(2\Delta_2 - 1)}{1 + 2 \sqrt{1 - \lambda_1^2}} \leq \lambda_2 \leq \sqrt{1 - \left( \frac{9 \sqrt{3}\Delta_1 - 1}{4 + 2 \sqrt{1 - \lambda_1^2}} \right)^2}. \tag{31}$$

It is seen from Eq. (30) that although the lower bound of $\lambda_1$ depends only on the observational statistics $\Delta_1$, the upper bound does not. Rather, the upper bound of $\lambda_1$ is a function of $\lambda_2$ and the optimal success probability $\Delta_2$ of Bob$_2$. On the other hand, Eq. (31) shows that both the upper and lower bound of $\lambda_2$ are not only dependent on the observational statistics but also on $\lambda_1$. This interdependence of sharpness parameters suggests a trade-off between them. By taking a value of $\lambda_2$, which is just above the lower critical value, we sustain the quantum advantage to subsequent Bobs. Each value of $\lambda_1$ above the lower critical value fixes the minimum value of unsharpness that is required to get the quantum advantage for Bob$_2$ while the need for a sustainable advantage to a subsequent Bob fixes its upper bound. The whole program runs as follows.

As already mentioned, the minimum value of unsharpness parameter required to get a quantum advantage is $\lambda_{min} = \frac{1}{\sqrt{3}}$. So a value $\lambda_1 = \frac{1}{\sqrt{3}} + \epsilon_1$ where $\epsilon_1 > 0$ would suffice. Furthermore putting this value of $\lambda_1$ into Eq. (19) we can estimate the minimum value of unsharpness in Bob$_2$’s measurement as $\lambda_2 = 0.6578 + \epsilon_2$ for all $\epsilon_2 > 0.3533\epsilon_1 + O(\epsilon_1^2)$. Similarly, to get advantage for Bob$_3$ the minimum value of unsharpness parameter can be estimated from Eq. (26) as $\lambda_3 = 0.7873 + \epsilon_3$ where $\epsilon_3 = 0.1187\epsilon_1 + O(\epsilon_1^2)$.

For an explicit example of how to estimate the interval of values of unsharpness parameters, let us consider the task where Bob$_1$ chooses the optimal measurement settings with unsharpness $\lambda_1 = \frac{1}{\sqrt{3}} + 0.05 = 0.6273$. Now their task is to set the unsharpness parameter such that Bob$_2$ and Bob$_3$ can get the quantum advantage. From Eq. (31) Bob$_2$ can set the unsharpness parameter any value in the range $0.6772 \leq \lambda_2 \leq 0.8566$. The minimum value of unsharpness parameter required to get an advantage at Bob$_3$’s site depends on both $\lambda_1$ and $\lambda_2$. With the same $\lambda_1$, for a lower critical value of $\lambda_2 (= 0.6772)$, the unsharpness parameter of Bob$_3$’s measurement is lower bounded as $0.8220 \leq \lambda_3$, on the other hand.

FIG. 3: Optimal trade-off between success probabilities for Bob$_1$, Bob$_2$ and Bob$_3$. Blue point on the three dimensional graph indicates the point where the success probabilities coincide, i.e., $\Delta_1 = \Delta_2 = \Delta_3 = 0.686 \geq \frac{2}{3}$. 
when Bob₂ performed his measurement with upper critical unsharpness ($\lambda₂ = 0.8566$) the bounds on $\lambda₃$ becomes unity, which comes directly from Eq. (26).

Due to the fact that when Bob₁ gets the quantum advantage, the upper bound of $\lambda₁$ depends on both $\lambda₂$ and the success probabilities of respective Bobs, $(\lambda₁)^{max}$ is more restricted than the one obtained when quantum advantages only for Bob₁ and Bob₂ were considered. Using Eq. (30) by putting $\Delta₂ = 2/3$ and $\lambda₂ = 1$ we had earlier fixed the allowed interval of $\lambda₁$ as, $0.57 \leq \lambda₁ \leq 0.93$ when only two Bobs are able to get advantage. This is discussed in Sec. III. Now if Bob₃ gets quantum advantage ( $\Delta₃ > 2/3$) along with Bob₁ and Bob₂, then using Eq. (19) and Eq. (26) we get the the interval of $\lambda₁$ has to be $0.57 \leq \lambda₁ \leq 0.77$. Thus, the quantum advantage extended to the Bob₃ provides a narrower interval $\lambda₁$ by decreasing the upper bound. In such case more efficient experimental verification is required to test it.

Let us denote these two ranges by $R₁$ and $R₂$ respectively. To get a practical impression of how such a certification works, let us consider a seller who sells a measurement instrument and claims that it works with a particular noise given by its unsharpness parameter $\lambda₁$ that belongs to a value within $R₂$. We can check by a sequential arrangement discussed above and by observing the statistics of Bob₂ whether the instrument is trusted or not. If we see that Bob₂ is getting a quantum advantage, then we conclude that the seller is trusted and $\lambda₁$ must lie in $R₂$. On the other hand, a failure of Bob₂ in getting an advantage will compel us to decide that the instrument is not trusted and $\lambda₁$ lie in $R₁$ which may or may not be useful for a particular purpose.

It is then natural to think that if more numbers of Bobs get the quantum advantage, then the interval of $\lambda₁$ will be narrower. However, for 3-bit RAC, a fourth observer cannot get the quantum advantage. In search of such a possibility, we consider the 4-bit sequential RAC.

VI. 4-BIT SEQUENTIAL RAC

In 4-bit sequential quantum RAC Alice now has a length-4 string randomly sampled from $x \in \{0,1\}^4$ which she encodes into sixteen qubits states $\rho_x = \frac{I + \hat{d}_x \cdot \sigma}{2}$, and sends them to Bob₁. After receiving the system, Bob₁ randomly performs the measurements of dichotomic observables $B_y$ with $y_1 \in \{4\}$ and relay the system to Bob₂ and so on. This process goes on as long as $k^{th}$ Bob gets the quantum advantage, as also discussed for the 3-bit case. The main purpose of extending our analysis to the 4-bit case is to examine whether more than three Bobs can get quantum advantage sequentially. This may then provide the certification of more than two unsharpness parameters and more efficient fine-tuning of the interval of values of unsharpness parameter of a given measurement instrument.

For 4-bit sequential quantum RAC, we found that for the qubit system, the optimal quantum value of success probability is different in standard and parity-oblivious RAC. Note here that the classical success probability is also different in standard and parity-oblivious RAC. For the latter case, the quantum advantage can be obtained for two Bobs, but for the former case, the quantum advantage cannot exceed one Bob. However, we demonstrate that instead of a single qubit system, if the input states are encoded in a two-qubit system, then four Bobs can get the quantum advantage in parity-oblivious RAC. In fact, in that case, the input two-qubit states required for achieving optimal quantum value naturally satisfy the parity-oblivious conditions for the 4-bit case. This feature is similar to the 3-bit case.

A. Standard 4-bit RAC with qubit input states

We first consider the case when the parity-oblivious constraint is not imposed, and input states are qubit. In that case the success probability for 4-bit classical RAC is bounded by $S₄ ≤ \frac{11}{16}$ [20]. In quantum RAC, we first consider the input states are in the qubit system. We have taken slightly different calculation steps than that of the 3-bit case (Sec. II), as presented in the Appendix. The quantum success probability for Bob₁ can be written as

$$S₄ = \frac{1}{64} \sum_{x \in \{0,1\}^4} \sum_{y_1=1}^4 Tr[\rho_x^2 B_x[y_1]]$$

$$= \frac{1}{2} + \frac{\alpha_1 \beta_1}{16} \sum_{y_1=1}^4 (-1)^{y_1} \hat{d}_x \cdot \hat{b}_{y_1}. \tag{32}$$

Here $x_{y_1}$ is the $y_{1}^{th}$ bit of the 4-bit input string $x \in \{0,1\}^4$ with first bit 0, i.e., $x_1' = 0$ for all $i \in \{8\}$. Let us now analyze the case when Bob₂ can get quantum advantage. We find the maximum success probability for Bob₂ from (A6) is achieved when $\hat{b}_1 \cdot \hat{b}_3 = \hat{b}_1 \cdot \hat{b}_3 = \hat{b}_2 \cdot \hat{b}_3 = 0$ and $\hat{b}_3 \cdot \hat{b}_4 = 1$. As presented in detail in the Appendix the maximum success probability for the Bob₂ $\max(S₄₂') = \Omega₂$ can be written as

$$\max(S₄₂') = \Omega₂ = \frac{1}{2} + \lambda₂ \left(\sqrt{\frac{\sqrt{2} + \sqrt{6}}{64}}\right)(1 + 3 \sqrt{1 - \lambda₁^2}). \tag{33}$$

The directions of the Bloch vectors $\hat{a}_x$ and $\hat{b}_y$, and relations between the different Bloch vectors $\hat{d}_x$ are explicitly provided in the Appendix. It is seen that conditions for maximization of $S₄₂'$ also leads the maximum value $\Omega₁ = \max(S₄₁')$ of Bob₁ in Eq. (32), which can be written as,

$$\max(S₄₁') = \Omega₁ = \frac{1}{2} + \lambda₁ \left(\sqrt{\frac{\sqrt{2} + \sqrt{6}}{16}}\right). \tag{34}$$

From Eqs. (32) and (33) we found that to get simultaneous quantum advantage for Bob₁ and Bob₂ the minimum values of the unsharpness parameters are $\lambda₁^{min} = 0.776$ and $\lambda₂^{min} = 1.074$ respectively. Since the allowed value of $\lambda₂$ is $0 \leq \lambda₂ \leq 1$, it is evident that Bob₂ cannot get quantum advantage.
FIG. 4: Optimal trade-off between quantum success probabilities of Bob$_1$ and Bob$_2$ for 4-bit sequential RAC is shown by solid orange curve while the shaded portion gives the sub-optimal range. Blue solid line is classical success probability for the same two observer constrained by parity-oblivious condition.

B. 4-bit RAC with qubit input states with parity-oblivious constraint

We now show that when the parity-oblivious constraint is imposed on Alice’s encoding, two sequential Bobs can get quantum advantage which enables certification of the unsharpness parameter of the Bob$_1$’s instrument even when the input states are qubit. In such case, the classical preparation non-contextual bound on success probabilities is $(S^2_1) \leq \frac{5}{8} \approx 0.625$. As outlined in Appendix A, respective maximum success probabilities for Bob$_1$ and Bob$_2$ are

$$\max(S^1_1) = \Omega_1 = \frac{1}{2} + \lambda_1 \left( \frac{1}{4\sqrt{2}} \right) \quad (35)$$

and

$$\max(S^2_2) = \Omega_2 = \frac{1}{2} + \lambda_2 \left( \frac{1 + 3\sqrt{1 - \lambda_1^2}}{16\sqrt{2}} \right). \quad (36)$$

The optimal trade-off between the success probabilities of Bob$_1$ and Bob$_2$ (by considering $\lambda_2 = 1$), is given by

$$\Omega_2(\Omega_1) = \frac{1}{2} + \left( \frac{1 + 3\sqrt{1 - 8(2\Omega_1 - 1)^2}}{16\sqrt{2}} \right) \quad (37)$$

In Fig.4 we plotted $\Omega_2$ against $\Omega_1$ which gives the optimal trade-off relation between successive success probabilities. The solid orange curve provides an optimal trade-off, while the shaded portion gives the sub-optimal range. The solid blue line is for the classical case for the same two observers, and there is no trade-off. As explained for the 3-bit case, one can uniquely certify the unsharpness parameter from this trade-off relation. For example, when $\Omega_2 = \Omega_1 = 0.6805$ the unsharpness parameter is $\lambda_1 = \frac{4 + \sqrt{6}}{25} \approx 0.7478$. This point is shown in Fig.4 by the black dot on the solid orange curve.

Thus the optimal pair $(\Omega_1, \Omega_2)$ self-test the preparation of Alice, the measurement settings of Bob$_1$ and Bob$_2$, and the unsharpness parameter $\lambda_1 = 2\sqrt{2}(2\Omega_1 - 1)$. The self-testing statements similar to the 3-bit case can also be made here.

In sub-optimal scenario, by taking $\lambda_2 = 1$, the Bo$_b_1$ and Bob$_2$ both get quantum advantage for a interval of values of $\lambda_1$ is given by,

$$2\sqrt{2}(2\Omega_1 - 1) \leq \lambda_1 \leq \sqrt{1 - \left( \frac{8\sqrt{2}(2\Omega_1 - 1) - 1}{3} \right)^2} \quad (38)$$

This above range is calculated by using Eqs.(35) and (36). Putting the classical bounds of $\Omega_1 = \Omega_2 = 5/8$, the numerical values of the interval of $\lambda_1$ is calculated as $0.707 \leq \lambda_1 \leq 0.792$. The more accurate the experimental observation, the more precise the $\lambda_1$ can be certified. This implies that an efficient experimental verification is required to confine the $\lambda_1$ in a narrow region. Note that the above interval can be made narrower if Bob$_1$ gets the quantum advantage. But we found that not more than two Bobs can get the advantage in this case, as given in the Appendix.

C. 4-bit RAC with two-qubit input states

We provide a sketch of the argument here. If in 4-bit parity oblivious RAC the input states are a two-qubit system, then four sequential Bobs can share the quantum advantage (see Appendix), and thus three unsharpness parameters can be certified. Note that the input states providing the optimal quantum value of the success probabilities satisfy the parity-oblivious constraints. The optimal trade-off relation between Bob$_1$ and Bob$_2$ can be derived by using the Eqs. (A25)-(A26).

In the sub-optimal scenario, the interval within which the unsharpness parameter is confined becomes much narrower. We argue again that this requires sophisticated experimental realization. When only Bob$_1$ and Bob$_2$ get quantum advantage, the interval of $\lambda_1$ in sub-optimal scenario is $0.517 \leq \lambda_1 \leq 0.934$ and when Bob$_1$, Bob$_2$ and Bob$_3$ get the quantum advantage, the interval becomes $0.517 \leq \lambda_1 \leq 0.807$. However, four Bobs get quantum advantage, the interval of $\lambda_1$ becomes further narrower $0.517 \leq \lambda_1 \leq 0.663$. This then shows that the range of $\lambda_1$ becomes more narrow when four sequential Bobs share quantum advantage compared to the case when only the first two Bobs get the quantum advantage. Note that the analytic expressions can be straightforwardly calculated using Eq.(A26). To avoid clumsiness, we skipped them and provided only numerical values.

VII. SUMMARY AND DISCUSSION

In summary, based on a communication game known as the parity-oblivious RAC, we provided two SDI protocols in the prepare-measure scenario to certify multiple unsharpness
parameters. Such a certification is demonstrated by examining the quantum advantage shared by multiple sequential observers (we denote Bob\(_k\) for \(k\)th observer). First, we demonstrated that for 3-bit parity-oblivious sequential RAC, a maximum of three sequential Bobs gets the quantum advantage over the classical preparation non-contextual strategies. We showed that the optimal pair of quantum success probabilities between Bob\(_1\) and Bob\(_2\), self-test the qubit states and the measurements of Bob\(_1\) and Bob\(_2\). Our treatment clearly shows that in the 3-bit case, the prepared states providing the optimal quantum success probability satisfy the parity-oblivious restriction. The optimal triple of success probabilities self-test the unsharpness parameters \(\lambda_1\) and \(\lambda_2\) of Bob\(_1\) and Bob\(_2\) respectively. In realistic experimental scenarios, loss and imperfection are inevitable, and the success probabilities become sub-optimal. In such a case, when only Bob\(_1\) and Bob\(_2\) get the quantum advantage, we derived a certified interval of \(\lambda_1\) within which it has to be confined. The more the precision of the experiment, the more accurate the bound to \(\lambda_1\) can be certified. We showed that when the quantum advantage is extended to Bob\(_3\), the interval of \(\lambda_1\) will be narrower, thereby requiring more efficient experiment realization.

We extended our treatment to the 4-bit case. We found that the qubit system cannot achieve the global optimal quantum value of success probability. But if the prepared states are two-qubit systems, we obtain the optimal quantum success probability. The qubit input states for which the maximum success probability is attained do not naturally satisfy the parity-oblivious constraints on input states. We studied three different cases in 4-bit sequential RAC. First, when input states are qubit, and parity-oblivious constraints are not imposed. In such a case, we have standard RAC, and we found the quantum advantage cannot be extended to Bob\(_2\). Thus, this result can be used to certify the states and measurements but cannot certify the unsharpness parameter. We then considered the case when input states are qubit and imposed the parity-oblivious constraints. We showed that, in this case, Bob\(_1\) and Bob\(_2\) can share the quantum advantage. We derived a trade-off relation between the success probabilities between Bob\(_1\) and Bob\(_2\). Consequently, we demonstrated the certification of the unsharpness parameter of Bob\(_1\). In the third case, when the input states are in a two-qubit system, the input states maximize the quantum success probability naturally satisfy the parity-oblivious conditions. In this case, the quantum advantage is extended to four sequential Bobs, and hence three unsharpness parameters can be certified. However, we provided a sketch of this argument, and details of it will be published elsewhere.

The MTB [43] protocol of 2-bit sequential quantum RAC for certifying the unsharpness parameter has recently been experimentally tested in [45–47]. Our protocols can also be tested using the existing technology already adopted in [45–47]. Finally, our protocol can also be extended to arbitrary-bit sequential RAC or other parity-oblivious communication games [66] which may demonstrate the quantum advantage to more independent observers. This will eventually pave the path for certifying more number of unsharpness parameters. In such a case, in a sub-optimal scenario, the interval of unsharpness parameter of the first Bob will be very narrow. Efficient experimental realization is required to certify such an interval. Study along this line could be an exciting avenue for future research. We also note here that in the other interesting work [44] along this line, the authors have used the 2-bit sequential RAC as a tool for certifying the unsharpness parameter. However, the approach adopted in [44] is different from the MTB protocol. It would then be interesting to extend their certification protocol for \(n\)-bit RAC or other parity-oblivious communication games. This also calls for further study.

**VIII. ACKNOWLEDGMENTS**

The authors acknowledge the support from the project DST/ICPS/QuST/Theme-1/2019/4.

---

**Appendix A: Details of the calculation for 4-bit sequential quantum RAC**

For the 4-bit case, we provide three conditional maximizations. i) The case when input states are qubit, and parity-oblivious constraints are not imposed. ii) The case when input states are qubit, and parity-oblivious constraints on the input state are imposed. iii) When the input states are a two-qubit system. In this case, the input states maximize the success probability naturally satisfy the parity-oblivious conditions.

1. **Maximum success probability for qubit system without imposing parity-oblivious constraints**

In the 4-bit scenario as Alice has encoded her 4-bit string into sixteen quantum states, and Bob\(_1\) performs four random measurements. From Eq. (4) of the main text, the quantum success probability of Bob\(_1\)’s site is given by:

\[
S_x^1 = \frac{1}{64} \sum_{x \in \{0,1\}^4} \sum_{y_1=1}^4 \text{Tr}[\rho_x B_{x_1} y_1] = \frac{1}{2} + \frac{\alpha_1 \beta_1}{32} \sum_{x \in \{0,1\}^4} \sum_{y_1=1}^4 (-1)^{y_1} \hat{d}_x \cdot \hat{b}_{y_1},
\]

(A1)

which is Eq. (32) in the main text. We denote \(m_{y_1} = (-1)^{y_1} \hat{d}_x\), which are unnormalized vectors and can explicitly be written...
as

\[
\hat{m}_1 = (\hat{a}_{0000} - \hat{a}_{1111}) + (\hat{a}_{0001} - \hat{a}_{1110}) + (\hat{a}_{0100} - \hat{a}_{1011}) + (\hat{a}_{0101} - \hat{a}_{1010}) + (\hat{a}_{0011} - \hat{a}_{1100}) + (\hat{a}_{0010} - \hat{a}_{1101}) + (\hat{a}_{0111} - \hat{a}_{1000}) + (\hat{a}_{0110} - \hat{a}_{1001}).
\]

\[
\hat{m}_2 = (\hat{a}_{0000} - \hat{a}_{1111}) + (\hat{a}_{0001} - \hat{a}_{1110}) + (\hat{a}_{0010} - \hat{a}_{1011}) + (\hat{a}_{0011} - \hat{a}_{1000}) + (\hat{a}_{0100} - \hat{a}_{1101}) + (\hat{a}_{0101} - \hat{a}_{1100}) + (\hat{a}_{1000} - \hat{a}_{0111}) + (\hat{a}_{1001} - \hat{a}_{0110}).
\]

\[
\hat{m}_3 = (\hat{a}_{0000} - \hat{a}_{1111}) + (\hat{a}_{0001} - \hat{a}_{1110}) + (\hat{a}_{0010} - \hat{a}_{1011}) + (\hat{a}_{0011} - \hat{a}_{1000}) + (\hat{a}_{0100} - \hat{a}_{1101}) + (\hat{a}_{0101} - \hat{a}_{1100}) + (\hat{a}_{1000} - \hat{a}_{0111}) + (\hat{a}_{1001} - \hat{a}_{0110}).
\]

\[
\hat{m}_4 = (\hat{a}_{0000} - \hat{a}_{1111}) + (\hat{a}_{0001} - \hat{a}_{1110}) + (\hat{a}_{0010} - \hat{a}_{1011}) + (\hat{a}_{0011} - \hat{a}_{1000}) + (\hat{a}_{0100} - \hat{a}_{1101}) + (\hat{a}_{0101} - \hat{a}_{1100}) + (\hat{a}_{1000} - \hat{a}_{0111}) + (\hat{a}_{1001} - \hat{a}_{0110}).
\]

By observing the expressions for \(\hat{m}_y\)'s, we can easily recognize that each Bloch vector must be a unit vector. In other words, the states should be pure unless it would lead to a decrement of the overall magnitude of \(m_y\) s. Along with this requirement, we can observe that among the sixteen unit vectors, eight appears with minus sign, the optimal magnitude of \(\hat{m}_y\)'s would imply that all sixteen Bloch vectors would form eight antipodal pairs. Hence maximization of \(S_4^0\) demands the two vectors in each parenthesis of Eq. (A.1) are antipodal pairs, and hence we can write,

\[
\hat{m}_1 = 2(\hat{a}_{0000} + \hat{a}_{0001} + \hat{a}_{0010} + \hat{a}_{0011} + \hat{a}_{0100} + \hat{a}_{0101} + \hat{a}_{0110} + \hat{a}_{0111}), \quad \hat{m}_2 = 2(\hat{a}_{0000} + \hat{a}_{0001} + \hat{a}_{0010} + \hat{a}_{0011} + \hat{a}_{0100} + \hat{a}_{0101} + \hat{a}_{0110} + \hat{a}_{0111}),
\]

\[
\hat{m}_3 = 2(\hat{a}_{0000} + \hat{a}_{0001} + \hat{a}_{0010} + \hat{a}_{0011} + \hat{a}_{0100} + \hat{a}_{0101} + \hat{a}_{0110} + \hat{a}_{0111}), \quad \hat{m}_4 = 2(\hat{a}_{0000} + \hat{a}_{0001} + \hat{a}_{0010} + \hat{a}_{0011} + \hat{a}_{0100} + \hat{a}_{0101} + \hat{a}_{0110} + \hat{a}_{0111}).
\]

In a compact form it can be written as \(m_y = (-1)^{y_i} \hat{a}_{y'}\) where \(x_i\) is the \(y_i^{th}\) bit of the 4-bit input string \(x' \in \{0,1\}^4\) with first bit 0, i.e., \(x_i = 0\) for all \(i \in [8]\). With this notation, the Eq. (A.1) can be re-written as

\[
S_4^0 = \frac{1}{2} + \frac{\alpha \beta_1}{16} \sum_{y} \sum_{y_1 = 1} (-1)^{y_i} \hat{a}_{y'} \cdot \hat{b}_{y_1}. \quad \text{(A2)}
\]

Now using Eq. (6) the reduced density operator after Bob_1’s measurement can be represented as,

\[
\hat{\rho}_{1} = \frac{1}{4} \sum_{y_1,b} K_{b|y} K_{b|y_1} = \frac{\hat{1} + \hat{d}_s^\dagger \cdot \hat{\sigma}}{2}, \quad \text{(A3)}
\]

where \(\hat{d}_s^\dagger\) is given by,

\[
\hat{d}_s^\dagger = 2(\hat{a}_{1}^2 - \beta_1^2) \hat{d}_{y'} + \beta_1^2 \sum_{y_1 = 1} \hat{b}_{y_1} \cdot \hat{b}_{y_1}. \quad \text{(A4)}
\]

Using Eq. (A4) we find the success probability of Bob_2 as,

\[
S_2 = \frac{1}{64} \sum_{x' \in \{0,1\}^4} \sum_{y_2 = 1} T \{ \hat{\rho}_{1} \hat{B}_{y_2} \} \]

\[
= \frac{1}{2} + \frac{1}{128} \left[ 2(\alpha_1^2 - \beta_1^2) \sum_{x' \in \{0,1\}^4} \sum_{y_2 = 1} (-1)^{y_2} \hat{d}_{y'} \cdot \hat{b}_{y_2} + \beta_1^2 \sum_{x' \in \{0,1\}^4} \sum_{y_1,y_2 = 1} (-1)^{y_2} \hat{d}_{y'} \cdot \hat{b}_{y_1} \sum_{y_1,y_2 = 1} (-1)^{y_2} \hat{b}_{y_1} \cdot \hat{b}_{y_2}. \right] \quad \text{(A5)}
\]

which we can re-write as

\[
S_2 = \frac{1}{2} + \frac{1}{64} \left[ 2(\alpha_1^2 - \beta_1^2) \sum_{x' \in \{0,1\}^4} \sum_{y_2 = 1} (-1)^{y_2} \hat{d}_{y'} \cdot \hat{b}_{y_2} + \beta_1^2 \sum_{x_1,y_2 = 1} \sum_{y_1,y_2 = 1} (-1)^{y_2} \hat{b}_{y_1} \cdot \hat{b}_{y_2}. \right] \quad \text{(A6)}
\]

Let us now first maximize the first term in right hand side first. We consider a positive number \(\gamma\) whose expectation value can be written as \(\langle \gamma \rangle = \beta - \Delta\), where \(\beta\) is a real number and \(\Delta = \sum_{y_2} \sum_{y_2 = 1} (-1)^{y_2} \hat{b}_{y_2} \cdot \hat{b}_{y_2}. \) Furthermore, we consider a set of positive vectors \(\hat{L}_y\) which is polynomial functions of \(\hat{d}_{y'}\) and \(\hat{b}_{y_2}\) so that \(\gamma\) acquires the form,

\[
\gamma = \frac{\sum_{y_2} W_2}{2} \langle \hat{L}_y \rangle^2. \quad \text{(A7)}
\]

Suitable vectors \(\hat{L}_y\) can be chosen for function given in equation (A7) as,

\[
\hat{L}_y = \frac{1}{W_2} \sum_{y_2 = 1} (-1)^{y_2} \hat{b}_{y_2} - \hat{d}_{y'}, \quad \text{(A8)}
\]
where $w_i$ is any positive semi definite function of $b_{y_i}$. Now substituting Eq. (A8) into Eq. (A7) and noting that $(\hat{b}_{y_i})^2 = (\hat{d}_i)^2 = 1$, we get,

$$\langle \gamma \rangle = \sum_{i=1}^{8} \left[ \frac{1}{2w_i} \left( \sum_{y=1}^{4} (-1)^{y_i} \hat{b}_{y_i} \right)^2 + \frac{w_i}{2} \right] - \Delta. \quad (A9)$$

We can now conveniently put $w_i = \| \sum_{y=1}^{4} (-1)^{y_i} \hat{b}_{y_i} \|$ in Eq. (A9) to finally get, $\Delta = \sum_{i=1}^{8} w_i - \langle \gamma \rangle$. Since $\langle \gamma \rangle \geq 0$ the maximum quantum value of $\Delta$ can be written as

$$(\Delta)_{\text{max}} = \max_{b_2} \left( \sum_{i=1}^{8} w_i \right). \quad (A10)$$

Since maximum value of $\Delta$ demands $\langle y_n \rangle = 0$ which further implies that $\hat{L}_i = 0$ and consequently we have the input Bloch vectors $\hat{d}_i = \sum_{y=1}^{n} (-1)^y \hat{b}_i$. Using the concavity inequality $\sum_{i=1}^{n} w_i \leq \sqrt{n \sum_{i=1}(w_i)^2}$, and applying it two times we have

$$\left( \Delta \right)_{\text{max}} \leq 4\sqrt{4(w_{1}^2 + w_{2}^2 + w_{3}^2 + w_{4}^2) + 64(w_{2}^2 + w_{0}^2 + w_{2}^2 + w_{8}^2)}$$

$$= 4\sqrt{4 + 2b_3 \cdot b_4 + 4\sqrt{4 - 2b_3 \cdot b_4}}. \quad (A11)$$

In the first line of Eq. (A11), the equality holds when $w_1 = w_2 = w_3 = w_4$ and same for the third term. This provides $b_1 \cdot b_2 = \hat{b}_1 \cdot \hat{b}_2 = \hat{b}_3 = \hat{b}_4 = 0$. Then, in qubit system it is not possible to obtain $\hat{b}_3 \cdot \hat{b}_4 = 0$. The maximum value of Eq. (A11) can be obtained when $\hat{b}_3 \cdot \hat{b}_4 = 1$. We then have,

$$(\Delta)_{\text{max}} = 4\left( \sqrt{2} + \sqrt{6} \right). \quad (A12)$$

We can then chose $\hat{b}_1 = \hat{x}$, $\hat{b}_2 = \hat{y}$, $\hat{b}_3 = \hat{z}$ and $\hat{b}_4 = \hat{\xi}$. This in turn provides from the optimization condition $\hat{L}_i = 0$ that $m_{y_i} = (-1)^y \hat{d}_i = \hat{b}_{y_i}$. Thus the input Bloch vectors $\hat{d}_i$ can be written as

$$\hat{d}_{0000} = \frac{\hat{x} + \hat{y}}{\sqrt{2}}, \quad \hat{d}_{0001} = \frac{\hat{x} + \hat{y} + 2\hat{z}}{\sqrt{6}}, \quad \hat{d}_{0010} = \frac{\hat{x} + \hat{y} - 2\hat{z}}{\sqrt{6}}, \quad \hat{d}_{0100} = \frac{\hat{x} - \hat{y}}{\sqrt{2}}. \quad (A13)$$

$$\hat{d}_{1000} = \frac{-\hat{x} + \hat{y}}{\sqrt{2}}, \quad \hat{d}_{0011} = \frac{\hat{x} + \hat{y}}{\sqrt{2}}, \quad \hat{d}_{0101} = \frac{\hat{x} - \hat{y} + 2\hat{z}}{\sqrt{6}}, \quad \hat{d}_{0110} = \frac{\hat{x} - \hat{y} - 2\hat{z}}{\sqrt{6}}.$$ 

It can be easily checked that the second term in Eq. (A6) is maximized when $\hat{b}_{y_2} = \hat{b}_{y_1}$ when $y_1 = y_2$. By putting the values of $\Delta$, $\alpha$ and $\beta$ we have

$$\max(S^2_{\frac{1}{2}}) = \Omega_2 = \frac{1}{2} + \lambda_2 \left( \frac{\sqrt{2} + \sqrt{6}}{64} \right) \left( 1 + \sqrt{1 - \lambda_2^2} \right) \quad (A14)$$

and consequently

$$\max(S^2_{\frac{1}{4}}) = \Omega_1 = \frac{1}{2} + \lambda_1 \left( \frac{\sqrt{2} + \sqrt{6}}{16} \right). \quad (A15)$$

Considering the situation when Bob$_1$ and Bob$_2$ implement their unsharp measurements so that the quantum advantage to Bob$_3$ persists, we can calculate the minimum value of the unsharpness parameters from Eqs. (A15) and (A14) as, $\lambda_1^{\text{min}} = 0.776$, $\lambda_2^{\text{min}} = 1.074$. It is clear now that as $\lambda_2^{\text{min}} \geq 1$ is not a legitimate value, Bob$_2$ does not get any quantum advantage. But we can change the scenario by putting the restriction of parity-obliviousness to see whether in 4-bit RAC quantum advantage can be extended to Bob$_2$.

### 2. Maximum success probability for parity-oblivious RAC for qubit system

Let us now discuss the case when the same game is constrained by parity-obliviousness constrains. In this case the classical bound of the game becomes the preparation non contextual bound and is equal to, $S_d = \frac{1}{2}(1 + \frac{3}{2}) = 0.625$. We recall the parity
set \( \mathbb{P}_n = \{ x \in \{0, 1 \}^n, \sum r x_r \geq 2 \} \) with \( r \in \{1, 2, \ldots, n\} \). For any \( s \in \mathbb{P}_n \), no information about \( s \cdot x = \oplus_r x_r \) (s-parity) is to be transmitted to Bob, where \( \oplus \) is sum modulo 2. We then have s-parity-0 and s-parity-1 sets. For 4-bit case the cardinality of parity set is eleven. Among them only four elements, 1011, 0111, 1110 and 0111, provide nontrivial constraints on the inputs are respectively given by

\[
R_{1011} = (\hat{d}_{0000} - \hat{d}_{0001} - \hat{d}_{0100} + \hat{d}_{0101} - \hat{d}_{0110}) = 0
\]

\[
R_{0111} = (\hat{d}_{0000} - \hat{d}_{0001} - \hat{d}_{0100} + \hat{d}_{0101} + \hat{d}_{0110}) = 0
\]

\[
R_{1110} = (\hat{d}_{0000} + \hat{d}_{0001} - \hat{d}_{0100} - \hat{d}_{0101} - \hat{d}_{0110} + \hat{d}_{0110}) = 0
\]

\[
R_{1101} = (\hat{d}_{0000} - \hat{d}_{0001} + \hat{d}_{0100} - \hat{d}_{0101} - \hat{d}_{0110} + \hat{d}_{0110}) = 0.
\]  

(A16)

When the parity-oblivious restriction is imposed on Alice’s inputs then we get \( \Delta_{\text{max}} = 8 \sqrt{2} \). This in turn provides the maximum success probability of Bob,

\[
\max(S_2^4) = \Omega_2 = \frac{1}{2} + \lambda_2 \left( \frac{1 + 3 \sqrt{1 - \lambda_2^2}}{16 \sqrt{2}} \right),
\]  

which also fixes the maximum success probability of Bob in 4-bit parity-oblivious RAC is given by,

\[
\max(S_1^4) = \Omega_1 = \frac{1}{2} + \lambda_1 \left( \frac{1}{4 \sqrt{2}} \right).
\]  

(A18)

The respective minimum values of sharpness parameter required to get quantum advantage for Bob1 and Bob2 are \( \lambda_{\text{1 min}} = 0.707, \lambda_{\text{2 min}} = 0.906 \). Thus both Bob1 and Bob2 both get the quantum advantage. We then extend our calculation to Bob3 to check whether he gets any quantum advantage or not. As a continuation to the previous section we can write the reduced state after Bob2’s measurement will be,

\[
\rho^2_x = \frac{1}{16} \left\{ 8 \mathbf{I} + 32 \alpha^2 \alpha^2 (\hat{a}_s \cdot \sigma) + 8 \alpha^2 \beta^2 \sum_{y_1=1}^4 B_{y_1}(\hat{a}_s \cdot \sigma) B_{y_1} + 8 \beta^2 \beta^2 \sum_{y_2=1}^4 \sum_{y_3,y_4=1}^4 B_{y_3} B_{y_4}(\hat{a}_s \cdot \sigma) B_{y_3} B_{y_4} \right\}.
\]  

(A19)

After some simplification we can represent above equation as \( \rho^2_x = \frac{1 + \hat{d}_s \cdot \sigma}{2} \) where the Bloch vector \( \hat{d}_s \) can be written as,

\[
\hat{d}_s = 4 \left( \alpha^2 - \beta^2 \right) \hat{a}_s + \beta^2 \sum_{y_1=1}^4 (\hat{b}_{y_1} \cdot \hat{a}_s) \hat{b}_{y_1} + \beta^2 \sum_{y_1=1}^4 (\hat{b}_{y_1} \cdot \hat{a}_s) \hat{b}_{y_1} + \beta^2 \sum_{y_1=1}^4 (\hat{b}_{y_1} \cdot \hat{a}_s) \hat{b}_{y_1}.
\]  

(A20)

The success probability for Bob3 is

\[
S_4^4 = \frac{1}{2} + \frac{1}{128} \left[ 4 \left( \alpha^2 - \beta^2 \right) \sum_{x' y_2=1}^4 \sum_{x'=1}^4 \left( -1 \right)^{x'} \hat{a}_{x'} \cdot \hat{b}_{y_2} + \beta^2 \sum_{x' y_2=1}^4 \sum_{x'=1}^4 \left( -1 \right)^{x'} \hat{a}_{x'} \cdot \hat{b}_{y_2} \right] + \beta^2 \sum_{x' y_2,y_3=1}^4 \sum_{x'=1}^4 \left( -1 \right)^{x'} \hat{a}_{x'} \cdot \hat{b}_{y_2} \right] \hat{b}_{y_1} \hat{b}_{y_2} \hat{b}_{y_3}.
\]  

We finally obtain the maximum success probability for Bob3 as,

\[
\max(S_4^4) = \Omega_3 = \frac{1}{2} + \left( \frac{\sqrt{2}}{128} \right) \prod_{k=1}^2 \left( 1 + 3 \sqrt{1 - \lambda_3^2} \right).
\]  

(A22)

The minimum sharpness parameter that Bob3’s instrument has to be \( \lambda_{\text{3 min}} = 1.56 \geq 1 \). Since this value is not legitimate we have no advantage for Bob3.
3. Optimal success probability in parity-oblivious RAC for two-qubit system

We provide sketch of the argument when Alice’s input states are two-qubit system. From the entanglement assisted parity-oblivious RAC in [63], in our prepare-measure scenario we find that to obtain the optimal quantum success probability the input states has to be

\[ \rho_x = \frac{1}{4} \left( \mathbb{I} \otimes \mathbb{I} + \frac{(-1)^x B_x}{2} \right) \quad (A23) \]

where \( B_x \)'s are mutually anticommuting observables in two-qubit system. One of such choices are \( B_1 = \sigma_x \otimes \sigma_x, B_2 = \sigma_x \otimes \sigma_y, B_3 = \sigma_y \otimes \sigma_x, \) and \( B_4 = \sigma_y \otimes \mathbb{I}. \) Importantly, the sixteen two-qubit input states corresponding to \( x \in \{0, 1\}^4 \) satisfy the four nontrivial parity-oblivious conditions. The optimal quantum success probability for Bob1 can be obtained as,

\[ \max(S_4^1) = \xi_4^1 = \frac{1}{2} + \lambda_4 \] (A24)

and for Bob2,

\[ \max(S_4^2) = \xi_4^2 = \frac{1}{2} + \lambda_2 \left( \frac{1}{16} \right) \left( 1 + 3 \sqrt{1 - \lambda_2^2} \right). \] (A25)

The general form of optimal quantum success probability for \( k^{th} \) Bob can be written as,

\[ \max(S_4^k) = \xi_k^4 = \frac{1}{2} + \lambda_2 \left( \frac{1}{4^k} \right) \prod_{i=1}^{k-1} \left( 1 + 3 \sqrt{1 - \lambda_i^2} \right). \] (A26)

The preparation non-contextual bound on 4-bit parity-oblivious RAC is \( S_4 = \frac{1}{2} \right( \frac{1}{16} \right) \approx 0.625. \) In this case we get the minimum value of unsharpness parameters of five sequential Bobs are \( \lambda_2^{\min} = 0.5, \lambda_4^{\min} = 0.556, \lambda_3^{\min} = 0.679, \lambda_4^{\min} = 0.795 \) and \( \lambda_5^{\min} = 1.12 \geq 1. \) Hence, if Alice’s encoding quantum states are in two-qubit system, at most four Bobs can get quantum advantage. Similar trade-off relation can be demonstrated by following the prescription in 3-bit parity-oblivious RAC.

[1] J.S. Bell, On the Einstein Podolsky Rosen paradox, Physics, 1, 195 (1964).
[2] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. 81, 865 (2009).
[3] O. Gühne and G. Tóth, Entanglement detection, Phys. Rep. 474, 1 (2009).
[4] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, Bell nonlocality, Rev. Mod. Phys. 86, 419 (2014).
[5] J. Barrett, L. Hardy and A. Kent, No Signaling and Quantum Key Distribution, Phys. Rev. Lett. 95, 010503 (2005).
[6] A. Acín, N. Gisin and L. Masanes, From Bell’s Theorem to Secure Quantum Key Distribution, Phys. Rev. Lett. 97, 120405 (2006).
[7] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio and V. Scarani, Device-Independent Security of Quantum Cryptography against Collective Attacks, Phys. Rev. Lett. 98, 230501 (2007).
[8] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar and V. Scarani, Device-independent quantum key distribution secure against collective attacks, New J. Phys. 11, 045021 (2009).
[9] R. Colbeck, Quantum and relativistic protocols for secure multi-party computation, Ph.D. thesis, University of Cambridge (2006); arXiv:0911.3814v2.
[10] S. Pironio et al., Random numbers certified by Bell’s theorem, Nature volume 464, 1021 (2010).
[11] O. Nieto-Silleras, S. Pironio and J. Silman, Using complete measurement statistics for optimal device-independent randomness evaluation, New J. Phys. 16, 013035 (2014).
[12] R. Colbeck and R. Renner, Free randomness can be amplified, Nature Physics 8, 450 (2012).
[13] 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).
[14] R. Gallego, N. Brunner, C. Hadley and A. Acín, Device-Independent Tests of Classical and Quantum Dimensions, Phys. Rev. Lett. 105, 230501 (2010).
[15] J. Ahrens, P. Badziag, A. Cabello and M. Bourennane, Experimental device-independent tests of classical and quantum dimensions, Nat. Phys. 8, 592 (2012).
[16] N. Brunner, M. Navascues and T. Vertesi, Dimension Witness and Quantum State Discrimination, Phys. Rev. Lett. 110, 150501 (2013).
[17] J. Bowles, M. Quintino and N. Brunner, Certifying the Dimension of Classical and Quantum Systems in a Prepare-and-Measure Scenario with Independent Devices, Phys. Rev. Lett. 112, 140407 (2014).
17

tum Random Access Codes with Shared Randomness, arXiv:0810.2937v3

[62] R. W. Spekkens, D. H. Buzacott, A. J. Keehn, B. Toner and G. J. Pryde, Preparation contextuality powers parity-oblivious multiplexing, Phys. Rev. Lett. 102, 010401 (2009).

[63] S. Ghorai and A. K. Pan, Optimal quantum preparation contextuality in an $n$-bit parity-oblivious multiplexing task, Phys. Rev. A, 98, 032110 (2018).

[64] R. W. Spekkens, Contextuality for preparations, transformations, and unsharp measurements, Phys. Rev. A, 71, 052108 (2005).

[65] A. K. Pan, Revealing universal quantum contextuality through communication games, Scientific Reports volume 9, 17631 (2019).

[66] A. K. Pan, Oblivious communication game, self-testing of projective and nonprojective measurements, and certification of randomness, Phys. Rev. A, 104, 022212 (2021).

[67] R. Kunjwal and R. W. Spekkens, From the Kochen-Specker Theorem to Noncontextuality Inequalities without Assuming Determinism, Phys. Rev. Lett. 115, 110403 (2015).

[68] S. Wei, F. Guo, F. Gao and Q. Wen, Certification of three black boxes with unsharp measurements using $3 \rightarrow 1$ sequential quantum random access codes, New J. Phys. 23 053014 (2021).