CHINESE OPTICS LETTERS

Vol. 19, No. 11 | November 2021

Sequential 3 → 1 quantum random access code utilizing unsharp measurements

Zhiguang Pang (庞志广)[1,2,3], Jiang Gao (高 江)[1,2,3], Tianlei Hou (侯天磊)[1,2,3], Min Wei (魏 敏)[1,2,3], Jian Li (李 剑)[1,2,3*], and Qin Wang (王 琴)[1,2,3**]

[1] Institute of Quantum Information and Technology, Nanjing University of Posts and Telecommunications (NUPT), Nanjing 210003, China

[2] Key Laboratory of Broadband Wireless Communication and Sensor Network Technology of Ministry of Education, NUPT, Nanjing 210003, China

[3] Telecommunication and Networks National Engineering Research Center, NUPT, Nanjing 210003, China

*Corresponding author: jianli@njupt.edu.cn

**Corresponding author: qinw@njupt.edu.cn

Received February 3, 2021 | Accepted April 30, 2021 | Posted Online August 30, 2021

Quantum random access codes (QRACs) are important communication tasks that are usually implemented in prepare-and-measure scenarios. The receiver tries to retrieve one arbitrarily chosen bit of the original bit-string from the code qubit sent by the sender. In this Letter, we analyze in detail the sequential version of the 3 → 1 QRAC with two receivers. The average successful probability for the strategy of unsharp measurement is derived. The prepare-and-measure strategy within projective measurement is also discussed. It is found that sequential 3 → 1 QRAC with weak measurement cannot be always superior to the one with projective measurement, as the 2 → 1 version can be.

Keywords: quantum random access codes; unsharp measurement; prepare-and-measure scenario.

DOI: 10.3788/COL202119.112701

1. Introduction

Random access code (RAC) is a type of collaborative communication task which is suitable for a wide variety of applications. Usually, RAC is implemented in a prepare-and-measure (PM) scenario[1], where the sender encodes the long message (string of more than one bit) into a short code (one bit usually) and sends it to the receiver, who tries to decode an arbitrarily chosen bit from the initial message. If the sender is allowed to encode the messages into a qubit state, the receiver can successfully retrieve the random bit with an average probability higher than that of the classical version, via corresponding measurements, which is the so called quantum RAC (QRAC). QRAC was introduced in Refs. [2–4], which is useful to certify quantum systems, e.g., dimension witnesses[5], self-testing[6–8], and comparison of different quantum resources[9,10]. It can also be implemented in quantum information processing protocols such as quantum key distribution[11,12], network coding[13], and random number generation[14].

The PM scenario of RAC/QRAC above involves one sender and one receiver. For two receivers, Bob and Charlie, two classical RACs can be implemented parallelly and independently, as the classical code can be copied or broadcast.

However, in a quantum version, as the number of all possible messages is larger than two, there must be at least a pair of non-orthogonal states in the set of encoded states, which cannot be cloned perfectly. The quantum system can be accessible by the receivers sequentially. Assuming that Bob, the first receiver, performs quantum operations on the quantum message from the sender, Alice, he gets a classical result, which reveals some information of the original message, and a quantum output, which will be delivered to Charlie, the second receiver, who also tries to retrieve the original message. There is no doubt that the average successful probabilities for both receivers are affected by Bob's operation. As the quantum system will collapse in one of the eigenstates of the sharp (projective) measurement operator, a weaker measurement performed by Bob is helpful for Charlie's further retrieving. As a special kind of positive operator-valued measurement (POVM)[15–20], unsharp measurement is a weak version of projection measurement, introducing less damage to a system[21–26], as the trade-off between information gain and disturbance. It plays an important role in certain quantum information processing tasks, such as quantum tomography[27,28], state discrimination[29,30], and randomness certification[31,32]. In the sequential QRACs, the total probability of successful retrieval with optimal trade-off using weak measurement has been characterized in Refs. [33,34] and demonstrated[35] in a photonic experiment.

All of the scenarios above[33–35] adopt 2 → 1 QRAC (encode 2 bit into a qubit), and it is shown that unsharp measurement can be better than the sharp projective one. Here, in this Letter, we extend it to the 3 → 1 QRAC. The total successful probability of sequential QRAC for two receivers with Bob's unsharp measurement is derived. For comparison, we also investigate the sequential QRAC, where Bob uses sharp measurement. However, numerical results show that unsharp measurement does not always show merits in the case of 3 → 1.

2. Quantum Random Access Code

In the $n \to 1$ RAC, Alice, the sender, encodes an n bit-string, $\boldsymbol{x} \in \{0,1\}^n$, into 1 bit a, via a classical function $a = f(\boldsymbol{x})$. Given the random input $y \in \{0,1,\ldots,n-1\}$ corresponding to the bit to be retrieved, the receiver, Bob, gets the estimate $b \in \{0,1\}$ using a decode function, $b = g(a,y)$. As the simplest case, Alice sends one of the origial bits, and Bob guesses all of the others randomly. So, the average success probability is $\frac{1+1/n}{2}$.

In the $n \to 1$ QRAC, as shown in Fig. 1, the sender encodes her classical n bit message $\boldsymbol{x}$ into one qubit ρ_x, and Bob extracts the required bit as $b \in \{0,1\}$ according to the random variable $y \in \{0,1,\ldots,n-1\}$ he receives by performing some measurement $\{M_{b|y}\}_{b\in\{0,1\}}$, where $M_{b|y} > 0$ and $\sum_b M_{b|y} = \mathbb{I}$. Generally, the statistical results of this PM scheme can be expressed by conditional probability by the Born rule, $P(b|\boldsymbol{x},y) = \mathrm{tr}(\rho_x M_{b|y})$. The average probability of a successful guess P_{succ} is expressed as

$$P_{\text{succ}} = \frac{1}{n2^n}\sum_{\boldsymbol{x},y} P(b = x_y|\boldsymbol{x},y). \tag{1}$$

For $n = 2$, the optimal probability is $\frac{1}{2} + \frac{1}{2\sqrt{2}}$[4]. It exceeds the limit of the classic scheme 3/4.

For the sequential QRAC, as depicted in Fig. 2, the second receiver, Charlie, receives a random classical variable $z \in \{0,1,\ldots,n-1\}$ and performs corresponding measurements $\{N_{c|z}\}_{c\in\{0,1\}}$ on the post-processing state $\rho^y_{x,b}$ delivered by Bob. The classical output for Charlie is $c \in \{0,1\}$. The total probability of a successful guess for the senario is written as

$$P_{\text{succ}} = \frac{1}{n2^n}\sum_{x,y} P(b = x_y|\boldsymbol{x},y) + \frac{1-\alpha}{n2^n}\sum_{\boldsymbol{x},z} P(c = x_z|\boldsymbol{x},z), \tag{2}$$

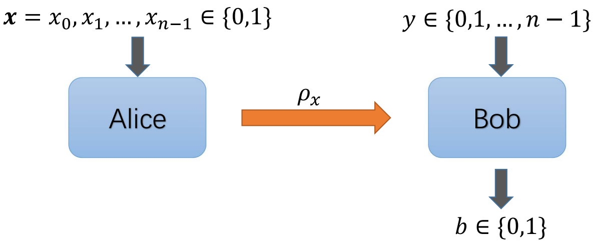
$\boldsymbol{x} = x_0, x_1, \ldots, x_{n-1} \in \{0,1\}$
$y \in \{0,1,\ldots,n-1\}$
Alice
ρ_x
Bob
$b \in \{0,1\}$

Fig. 1. Scenario with two participants. $\boldsymbol{x}$: input message of Alice; y, b: input and output of Bob, respectively; ρ_x: state that Alice sends to Bob.

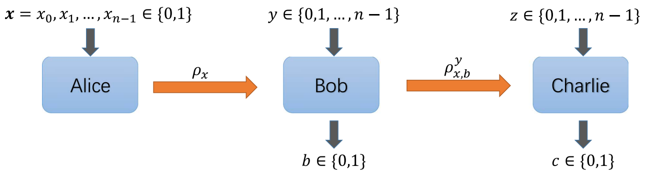
$\boldsymbol{x} = x_0, x_1, \ldots, x_{n-1} \in \{0,1\}$
$y \in \{0,1,\ldots,n-1\}$
$z \in \{0,1,\ldots,n-1\}$
Alice
ρ_x
Bob
$\rho^y_{x,b}$
Charlie
$b \in \{0,1\}$
$c \in \{0,1\}$

Fig. 2. Scenario with three participants. $\boldsymbol{x}$: input message of Alice; y, b: input and output of Bob, respectively; ρ_x: state that Alice sends to Bob; $\rho^y{}_{x,b}$: post-processing state that Bob sends to Charlie.

with $\alpha \in [0,1]$ indicating the contribution of Bob to a successful guess.

In general, we can use a quantum instrument[36] to describe Bob's two-outcome measurement, which is characterized by Kraus operators $\{K_{b|y}\}_{b\in\{0,1\}}$ satisfying $\sum_b K^\dagger_{b|y} K_{b|y} = \mathbb{I}$. It is an ordered set of the completely positive trace non-increasing map $\Gamma_{b|y}(\rho_x) = K_{b|y}\rho_x K^\dagger_{b|y}$ acting on the input state ρ_x, with the probability $p(b|\boldsymbol{x},y) = \mathrm{tr}(\rho_x K^\dagger_{b|y} K_{b|y})$. The normalized post-measurement state will be described by $\rho^y_{x,b} = \frac{K_{b|y}\rho_x K^\dagger_{b|y}}{p(b|\boldsymbol{x},y)}$ on the outcome b. The sharp measurement, projection-valued measure (PVM), can be considered as a special case, where $K_{b|y}K_{b'|y} = K_{b|y}\delta_{bb'}$.

For $n = 2$, the difference of strategies for Bob, the unsharp POVM and the PVM, is discussed in detail[34]. As shown in Fig. 3, the PVM strategy is divided into three schemes: (i) unitary, where Bob does not extract information for any y; (ii) measure and prepare, where Bob performs the corresponding PVM according to y; and (iii) mixed, which is the synthesis of the first two strategies. It is found that the POVM scheme

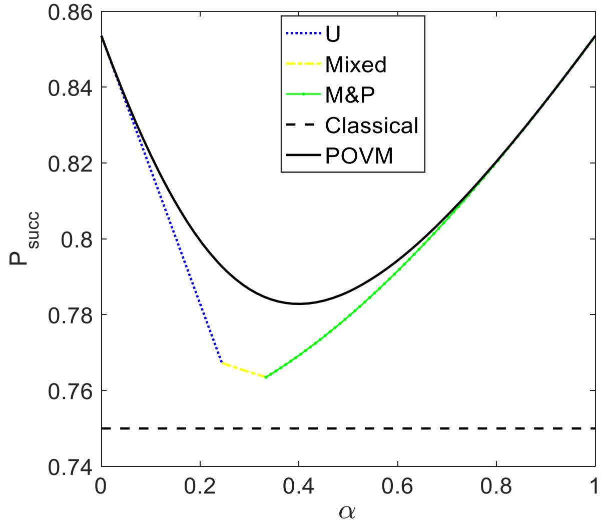

Fig. 3. Bounds on average success probability under 2 → 1 task. Short dashed line corresponds to the classical strategy. Dotted line, dotted and dashed line, and dotted and solid line correspond to the "unitary," "mixed," and "measure and prepare" projective strategies, respectively. Solid line corresponds to the general strategy with unsharp measurements. All of the bounds are tight.

is always better than PVM schemes for all α, In other words, unsharp measurements can provide advantages.

3. 3 → 1 QRAC for Two Receivers with Weak Measurement

Let us consider the 3 → 1 QRAC task in this section. For the one receiver case, the successful probability can be written as

$$P_{\text{succ}}^{B}=\frac{1}{24}\sum_{\boldsymbol{x},y}P(b=x_y|\boldsymbol{x},y),\tag{3}$$

where x_y is the yth bit of the input string $\boldsymbol{x}$. $P_{\text{succ}}^{B}\leq 2/3$, for a classical verion, while $P_{\text{succ}}^{B}=\frac{1}{2}+\frac{1}{2\sqrt{3}}\approx 0.7887$ for a standard QRAC.

In the sequential QRAC process, Bob receives the code qubit from Alice, and Charlie receives the post-measurement state from Bob. Here, the state set $\{\rho_x\}$ sent by Alice corresponds to the eight vertices of the inscribed cube of the Bloch sphere, i.e.,

$$\rho_x=\frac{1}{2}\mathbb{I}+\frac{1}{2\sqrt{3}}\sum_i(-1)^{x_i}\sigma_i,\tag{4}$$

where $\{\sigma_i\}_{i=0,1,2}$ denotes the three Pauli matrices $\{\sigma_x,\sigma_y,\sigma_z\}$, respectively. Bob's unsharp measurements can be written in Kraus operators,

$$K_{b|y}=\frac{\sqrt{\lambda}+\sqrt{1-\lambda}}{2}\mathbb{I}+\frac{\sqrt{\lambda}-\sqrt{1-\lambda}}{2}(-1)^b\sigma_y,\tag{5}$$

where $\lambda\in[0.5,1]$ is the maximal eigenvalue of Bob's operations, as the sharpness of the corresponding measurement. When Bob performs a projective measurement, where $\lambda=1$, we will get the optimal value $P_{\text{succ}}^{B}\approx 0.7887$, which is higher than the classical bound 2/3.

As a sequential communication task, Charlie receives a post-measurement state. Without any information of Bob's measurement choice y or outcome b, the post-measurement state is written as

$$\rho_x^{'}=\frac{1}{3}\sum_{b,y}K_{b|y}\rho_x K_{b|y}^{\dagger}.\tag{6}$$

Subsequently, he performs the two-outcome measurement. Here, the best strategy of Charlie is the sharp measurement, $\{N_{c|z}=\frac{1}{2}[\mathbb{I}+(-1)^c\sigma_z]\}$. The average successful probability P_{succ}^{C} for Charlie is

$$P_{\text{succ}}^{C}=\frac{1}{24}\sum_{\boldsymbol{x},z}P(c=x_z|\boldsymbol{x},z).\tag{7}$$

Although Charlie's choice of measurements is independent of Bob's measurement choice and outcome, P_{succ}^{C} will be potentially affected by Bob's operations. Given the sharpness λ of Bob's measurment, we can obtain

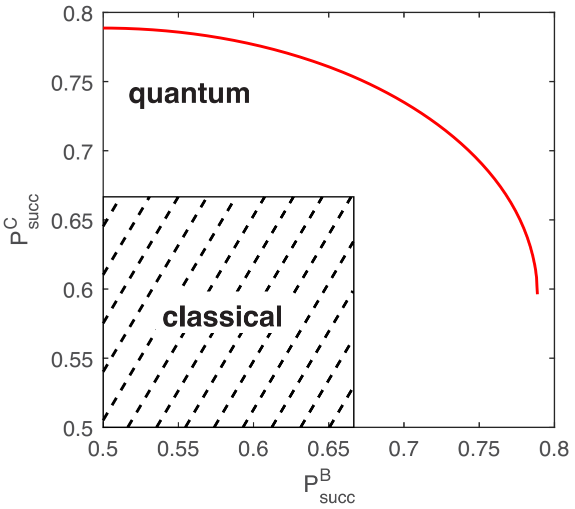

Fig. 4. Correlations between the two success probabilities (P_{succ}^{B}, P_{succ}^{C}). The curve represents the boundary of the quantum set under 3 → 1; shadow rectangle represents classical boundary under 3 → 1.

$$P_{\text{succ}}^{B}=\frac{1}{2}+\frac{2\lambda-1}{2\sqrt{3}},\tag{8}$$

$$P_{\text{succ}}^{C}=\frac{1}{2}+\frac{1+4\sqrt{\lambda(1-\lambda)}}{6\sqrt{3}}.\tag{9}$$

A complementary relationship between P_{succ}^{B} and P_{succ}^{C} is found, as shown in Fig. 4. The superiority of quantum RAC over the classical one is obvious, as either P_{succ}^{B} or P_{succ}^{C} is greater than the classical bound. Further, by bringing Eqs. (8) and (9) into Eq. (2), the optimal λ is found as a function of α:

$$\lambda=\frac{1}{2}+\frac{3\alpha}{2\sqrt{4-8\alpha+13\alpha^2}}.\tag{10}$$

Eventually, we could obtain the optimal average success probability:

$$P_{\text{succ}}^{\text{POVM}}=\frac{1}{2}+\frac{1-\alpha}{6\sqrt{3}}+\frac{1}{6\sqrt{3}}\sqrt{4-8\alpha+13\alpha^2}.\tag{11}$$

4. 3 → 1 QRAC for Two Receivers without Weak Measurement

Now let us consider the strategies without weak measurement. For the unitary strategy, where Bob does nothing but guessing, and Charlie receives the identical state that Alice sends, we have

$$P_{\text{succ}}=\frac{\alpha}{2}+(1-\alpha)\left(\frac{1}{2}+\frac{1}{2\sqrt{3}}\right).\tag{12}$$

For the PVM scheme, we also use the methods proposed in Ref. [32]. The total successful probability is written as

$$P_{\text{succ}}^{\text{PVM}} = \frac{1}{72} \sum_{x,y,z,b,c} \text{tr}[\sigma_{x,b}^{y} N_{c}^{z}][\alpha\delta_{b,x_y} + (1-\alpha)\delta_{c,x_z}], \tag{13}$$

where $\sigma_{x,b}^{y}$ is the unnormalized post-measurement state. For pure state $\rho_x = |\phi_x\rangle\langle\phi_x|$ and Bob's projective measurement on the base $\{|\psi_0^y\rangle,|\psi_1^y\rangle\}$,

$$\sigma_{x,b}^{y} = |\langle\psi_b^y|\phi_x\rangle|^2 |\psi_b^y\rangle\langle\psi_b^y|. \tag{14}$$

To optimize the parameters in the measure-and-prepare strategy, we use the unit vectors on the Bloch sphere to denote an arbitrary pure state of Eq. (4) and get

$$|\langle\psi|\phi\rangle|^2 = \text{tr}(\rho_1\rho_2) = \frac{1}{2}(1 + \vec{r}_1 \cdot \vec{r}_2). \tag{15}$$

Note that the above formula is a function about angles (θ, φ) while using spherical coordinate vector $\vec{r} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$. The result of numerical simulation is shown in Fig. 5.

It is found that the optimal strategy for 3 → 1 QRAC is quite different from that of 2 → 1 QRAC. In this guessing game, the unsharp scheme cannot always have advantages. The average success probability of the "measure and prepare" strategy is always 0.75 when α is approximately in the range of [0,0.71). It is always higher than that of the POVM strategy for $\alpha \geq 0.15$. The average successful probability 0.75 can be achieved by another kind of classical RAC[4]. In the classical scheme, the 8 bit-strings $\{\boldsymbol{x}\}$ are divided into two categories according to the number of ones in it, i.e., $\{\boldsymbol{x}\}_0 = \{000,001,010,100\}$ and $\{\boldsymbol{x}\}_1 = \{111,110,101,011\}$, which are encoded into classical bits to be sent, 0 and 1, respectively. Therefore, when the receiver gets bit 0, he can guess that the original bit-string is 000 in set $\{\boldsymbol{x}\}_0$, and, when it gets bit 1, the guess is 111 in set $\{\boldsymbol{x}\}_1$. In both cases, the average success probability is $(1 + \frac{2}{3}\cdot 3)/4 = 0.75$.

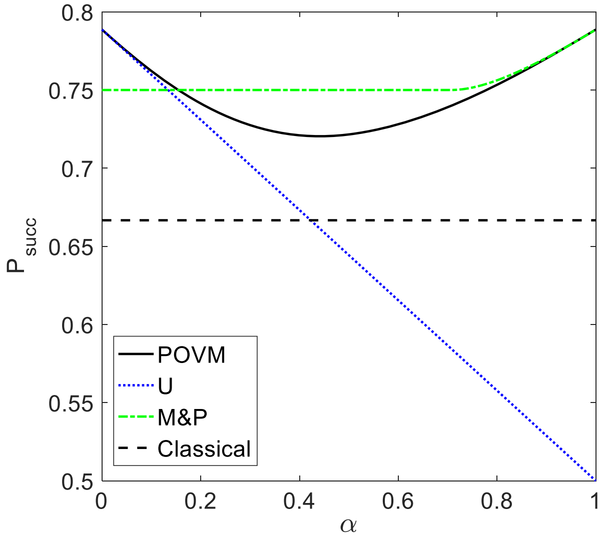

Fig. 5. Bounds on average success probability under 3 → 1 task. Short dashed line corresponds to the classical strategy. Dotted line and dotted and dashed line correspond to the "unitary" and "measure and prepare" projective strategies, respectively. Solid line corresponds to the general strategy with unsharp measurements.

5. Summary

In this Letter, we have discussed the sequential version of the 3 → 1 QRAC task with two receivers through unsharp measurements. As a trade-off between information gain and state disturbance, the successful probability for the first receiver and the second one will increase and decrease, respectively, with the sharpness of the first one's measurement increasing. The optimal average probability of successful retrieval with unsharp measurements is derived. Furthermore, two strategies for the first receiver are discussed, i.e., the unitary one and the measure-and-prepare one with PVM. It is found that for most of the weight for averaging, the measure-and-prepare strategy with PVM achieves a higher total success probability of 0.75 than the POVM one, which is different from the 2 → 1 case. Moreover, this success probability can be reproduced by a classical scenario. Therefore, our present work can provide useful references for further implementation of QRAC and RAC. We believe that our theory can be expanded to the scheme with more receivers or higher-dimensional QRACs and can be applicable to the implementation of a quantum random number generator (QRNG) based on QRACs[37].

Acknowledgement

This work was supported by the National Key Research and Development Program of China (Nos. 2018YFA0306400 and 2017YFA0304100), the National Natural Science Foundation of China (Nos. 12074194, 11774180, and U19A2075), and the Leading-Edge Technology Program of Jiangsu Natural Science Foundation (No. BK20192001).

References

1. L. Guerini, M. T. Quintino, and L. Aolita, "Distributed sampling, quantum communication witnesses, and measurement incompatibility," Phys. Rev. A **100**, 042308 (2019).
2. A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, "Quantum random access codes using single d-level systems," Phys. Rev. Lett. **114**, 170502 (2015).
3. A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, "Dense quantum coding and a lower bound for 1-way quantum automata," in *Proceedings of 31st ACM STOC* (1999).
4. A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, "Quantum random access codes with shared randomness," arXiv:0810.2937 (2008).
5. S. Wehner, M. Christandl, and A. C. Doherty, "A lower bound on the dimension of a quantum system given measured data," Phys. Rev. A **78**, 062112 (2008).
6. A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, "Self-testing quantum states and measurements in the prepare-and-measure scenario," Phys. Rev. A **98**, 062307 (2018).
7. M. Farkas and J. Kaniewski, "Self-testing mutually unbiased bases in the prepare-and-measure scenario," Phys. Rev. A **99**, 032316 (2019).

8. A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, "Self-testing nonprojective quantum measurements in prepare-and-measure experiments," Sci. Adv. **6**, eaaw6664 (2020).
9. A. Tavakoli, B. Marques, M. Pawłowski, and M. Bourennane, "Spatial versus sequential correlations for random access coding," Phys. Rev. A **93**, 032336 (2016).
10. A. Hameedi, D. Saha, P. Mironowicz, M. Pawłowski, and M. Bourennane, "Complementarity between entanglement-assisted and quantum distributed random access code," Phys. Rev. A **95**, 052345 (2017).
11. M. Pawłowski and N. Brunner, "Semi-device-independent security of one-way quantum key distribution," Phys. Rev. A **84**, 010302(R) (2011).
12. Y. Guo, K. S. Wang, D. Huang, and X. Q. Jiang, "High efficiency continuous-variable quantum key distribution based on QC-LDPC codes," Chin. Opt. Lett. **17**, 112701 (2019).
13. M. Hayashi, K. Iwama, H. Nishimura, R. Raymond, and S. Yamashita, "Quantum network coding," Lect. Notes Comput. Sci. **4393**, 610 (2007).
14. H. W. Li, Z. Q. Yin, Y. C. Wu, X. B. Zou, S. Wang, W. Chen, G. C. Guo, and Z. F. Han, "Semi-device independent random number expansion without entanglement," Phys. Rev. A **84**, 034301 (2011).
15. G. M. D'Ariano, P. L. Presti, and P. Perinotti, "Classical randomness in quantum measurements," J. Phys. A: Math. Gen. **38**, 5979 (2005).
16. R. Derka, V. Bužek, and A. K. Ekert, "Universal algorithm for optimal estimation of quantum states from finite ensembles," Phys. Rev. Lett. **80**, 1571 (1998).
17. J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, "Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination," Phys. Rev. Appl. **7**, 054018 (2017).
18. E. S. Gómez, S. Gómez, P. González, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi, and G. Lima, "Device-independent certification of a nonprojective qubit measurement," Phys. Rev. Lett. **117**, 260401 (2016).
19. A. Tavakoli, D. Rosset, and M. O. Renou, "Enabling computation of correlation bounds for finite-dimensional quantum systems via symmetrisation," Phys. Rev. Lett. **122**, 070501 (2019).
20. J. M. Renes, "Spherical-code key-distribution protocols for qubits," Phys. Rev. A **70**, 052314 (2004).
21. Y. Aharonov, D. Z. Albert, and L. Vaidman, "How the result of a measurement of a component of the spin of a spin-1/2 particle can turn out to be 100," Phys. Rev. Lett. **60**, 1351 (1988).
22. P. Busch, "Unsharp reality and joint measurements for spin observables," Phys. Rev. D **33**, 2253 (1986).
23. P. Busch, "Surprising features of unsharp quantum measurements," Phys. Lett. A **130**, 323 (1988).
24. N. W. M. Ritchie, J. G. Story, and R. G. Hulet, "Realization of a measurement of a 'weak value'," Phys. Rev. Lett. **66**, 1107 (1991).
25. G. J. Pryde, J. L. O'Brien, A. G. White, T. C. Ralph, and H. M. Wiseman, "Measurement of quantum weak values of photon polarization," Phys. Rev. Lett. **94**, 220405 (2005).
26. Y. Aharonov, E. Cohen, and A. C. Elitzur, "Foundations and applications of weak quantum measurements," Phys. Rev. A **89**, 052105 (2014).
27. J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, "Symmetric informationally complete quantum measurements," J. Math. Phys. **45**, 2171 (2004).
28. A. Bisio, G. Chiribella, G. M. D'Ariano, S. Facchini, and P. Perinotti, "Optimal quantum tomography of states, measurements, and transformations," Phys. Rev. Lett. **102**, 010404 (2009).
29. A. Chefles, "Quantum state discrimination," Contemp. Phys. **41**, 401 (2000).
30. S. M. Barnett and S. Croke, "Quantum state discrimination," Adv. Opt. Photon. **1**, 238 (2009).
31. A. Acín, S. Pironio, T. Vértesi, and P. Wittek, "Optimal randomness certification from one entangled bit," Phys. Rev. A **93**, 040102(R) (2016).
32. C. X. Liu, K. Liu, X. R. Wang, L. Y. Wu, J. Li, and Q. Wang, "Experimental randomness certification with a symmetric informationally complete positive operator-valued measurement," Chin. Opt. Lett. **18**, 102701 (2020).
33. K. Mohan, A. Tavakoli, and N. Brunner, "Sequential random access codes and self-testing of quantum instruments," New J. Phys. **21**, 083034 (2019).
34. N. Miklin, J. J. Borkała, and M. Pawłowski, "Semi-device-independent self-testing of unsharp measurements," Phys. Rev. Res. **2**, 033014 (2020).
35. H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, "Experimental characterisation of unsharp qubit measurements in a semi-device-independent setting," arXiv:2001.04768 (2020).
36. T. Heinosaari and M. Ziman, *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement* (Cambridge University, 2011).
37. H. W. Li, M. Pawłowski, Z. Q. Yin, G. C. Guo, and Z. F. Han, "Semi-device-independent randomness certification using $n\rightarrow 1$ quantum random access codes," Phys. Rev. A **85**, 052308 (2012).