Semi-Device-Independent Framework Based on Restricted Distrust in Prepare-and-Measure Experiments

Armin Tavakoli*
Institute for Quantum Optics and Quantum Information–IQOQI Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

(Received 28 January 2021; accepted 30 April 2021; published 25 May 2021)

A semi-device-independent framework for prepare-and-measure experiments is introduced in which an experimenter can tune the degree of distrust in the performance of the quantum devices. In this framework, a receiver operates an uncharacterized measurement device and a sender operates a preparation device that emits states with a bounded fidelity with respect to a set of target states. No assumption on Hilbert space dimension is required. The set of quantum correlations is investigated and bounded from both the interior and the exterior. Furthermore, the optimal performance of quantum state discrimination with bounded distrust is derived and applied to certification of detection efficiency. Quantum-over-classical advantages are demonstrated and the magnitude of distrust compatible with such advantages is explored. Finally, efficient schemes for semi-device-independent random number generation are developed.

DOI: 10.1103/PhysRevLett.126.210503

Introduction.—Quantum information protocols often assume the precise control of quantum devices. Precise control is, however, an idealization that experiments only can aspire to approximate. In contrast, the device-independent (DI) approach to quantum information processing uses violations of Bell inequalities to perform quantum information protocols without requiring any characterization of the involved quantum devices. Nevertheless, this stringent approach faces substantial experimental obstacles due to its demanding requirements.

Partly motivated by finding a compromise between the black-box spirit of device independence and the experimental advantages of conventional protocols, and partly motivated by understanding quantum communications, much research attention has been directed at semi-DI quantum information processing. The semi-DI approach is commonly investigated in simple prepare-and-measure experiments in which a sender prepares states and a receiver measures them. Up to a weak and reasonable assumption, the resulting correlations are analyzed without requiring any detailed characterization of the involved devices.

The most thoroughly researched semi-DI setting is that in which only the Hilbert space dimension is known. This has led to protocols for quantum key distribution [1,2], random number generation [3,4], random access coding [5–7], numerous quantum certification protocols [8–18], and several experiments [18–24]. More recently, also alternative settings have been investigated, based on a bound on the overlap [25–27], energy [28–31], and information content [32,33] of the states.

Here, we introduce a framework for semi-DI quantum information processing in which the only assumption is based on the experimenter estimating a bound on how accurately the prepared states correspond to the ideal states targeted in the lab. We model this through a bound on the fidelity between the lab states and the target states. Thus, this tunable distrust (or lack of control) corresponds to a physically observable quality estimate of the preparation procedure.

In what follows, we introduce the framework and proceed to analyze quantum correlations under bounded distrust. We show that the set of correlations can be efficiently bounded from both the interior and the exterior via semidefinite programming (SDP) methods. Then, focusing on quantum state discrimination, which is the simplest scenario, we analytically determine the optimal performance under bounded distrust. This is applied to construct experimentally friendly semi-DI certification of the detection efficiency of a memoryless measurement device. Next, we investigate hybrid models based on classical measurement devices and show that quantum correlations can elude such models even at substantial degrees of distrust. Moreover, we investigate semi-DI random number generation and show that high rates of randomness can be obtained at experimentally realistic levels of distrust.

Framework.—Consider a scenario in which Alice and Bob independently select inputs x and y, respectively. Alice prepares a quantum state ρ_x which she sends to Bob who performs a measurement $\{M_{b|y}\}$ with outcome b. When the experiment is repeated in many independent rounds, the correlations are described by the probability distribution $p(b|x,y) = tr(\rho_x M_{b|y})$. We may also permit the devices of Alice and Bob to be classically correlated through a shared parameter λ. This leads to the more general probability distribution

$$p(b|x,y)=\sum_{\lambda}p(\lambda)tr(\rho_x^{(\lambda)}M_{b|y}^{(\lambda)}). \tag{1}$$

Suppose that Alice's intention is to prepare a particular set of target states $\{|\psi_x\rangle\}$. However, her preparation device is subject to a degree of imperfection due to the lack of flawless control. Moreover, her device, or the states it emits (before reaching Bob), could be maliciously influenced. We quantify the accuracy of the preparation procedure through the fidelities

$$F_{\psi_x}\equiv\langle\psi_x|\rho_x|\psi_x\rangle, \tag{2}$$

where $\rho_x=\sum_\lambda p(\lambda)\rho_x^{(\lambda)}$ is the average state and the target states $|\psi_x\rangle$ are embedded into the arbitrary, but finite, dimensional Hilbert space of ρ_x. An ideal procedure ($\rho_x=|\psi_x\rangle\langle\psi_x|$) is represented by $F_{\psi_x}=1$. In contrast, a smaller fidelity signifies that the lab states deviate further from the target states. In our model, we let the experimenter provide a bound on the degree of distrust in their preparation procedure. Specifically, we consider that the fidelities are subject to a lower bound of the form

$$F_{\psi_x}\geq 1-\epsilon_x, \tag{3}$$

where $\epsilon_x\in[0,1]$ is the distrust in each state preparation. The fidelity (2) can then be interpreted as the probability of obtaining the first outcome of the measurement $\{|\psi_x\rangle\langle\psi_x|,\mathbb{1}-|\psi_x\rangle\langle\psi_x|\}$ when performed on ρ_x. Therefore, if there are no side channels used to send information about x, the choice of ϵ_x can based on direct observation.

Quantum correlations.—We develop tools to analyze quantum correlations under bounded distrust. This analysis is considerably simplified by first identifying three key properties. (i) The shared parameter λ can be absorbed in the preparations by sending the classical-quantum state $\rho_x=\sum_\lambda p(\lambda)\rho_x^{(\lambda)}\otimes|\lambda\rangle\langle\lambda|$. Bob learns λ by measuring the second register and then proceeds to apply $\{M_{b|y}^{(\lambda)}\}$ to the first register to generate the correlations (1). The fidelity is preserved since $F_{\psi_x}=tr[(|\psi_x\rangle\langle\psi_x|\otimes\mathbb{1})\rho_x]=\sum_\lambda p(\lambda)\langle\psi_x|\rho_x^{(\lambda)}|\psi_x\rangle$. (ii) We can w.l.g restrict to considering only pure states ρ_x. Because of Uhlmann's theorem [34], for every mixed ρ_x there exists a pure state $|\phi_x\rangle$ such that the fidelity (2) is preserved, i.e., $F_{\psi_x}=|\langle\psi_x|\phi_x\rangle|^2$. Then, by considering measurements that act trivially on the ancillary space of the purification, we recover the quantum correlations; $tr(\rho_x M_{b|y})=\langle\phi_x|M_{b|y}\otimes\mathbb{1}|\phi_x\rangle$. (iii) We can w.l.g restrict to considering only states of dimension $2n$, where n is the number of possible inputs of Alice. This follows from the fact that m pure states span at most an m-dimensional subspace of Hilbert space and that our problem involves a total of $2n$ such states. Furthermore, based on systematic numerical evidence discussed in Supplemental Material (SM) [35], we conjecture that the dimension can further be restricted to n.

Equipped with these properties, we investigate linear correlation functions. These are written

$$\mathcal{W}=\sum_{b,x,y}c_{bxy}p(b|x,y), \tag{4}$$

where c_{bxy} are real coefficients. For a general function $\mathcal{W}$, how can we determine the values attainable in quantum theory for a given set of target states $\{|\psi_x\rangle\}$ and a given set of distrust parameters $\{\epsilon_x\}$? We answer this by providing generally applicable methods to establish both lower and upper bounds on the extremal (for simplicity, the maximal) quantum value of the function, which we denote $\mathcal{W}^Q$.

Any set of states $\{\rho_x\}$ and measurements $\{M_{b|y}\}$ that respect the constraint (3) imply a lower bound on $\mathcal{W}^Q$. Systematic and increasingly accurate lower bounds can be obtained via alternating convex search. This follows from the fact that for fixed measurements, the optimization problem $\max_{\{\rho_x\}}\mathcal{W}$ over states ρ_x of dimension $2n$ subject to the constraints (3) is an SDP. Similarly, fixing the states to those found optimal by this SDP, the optimization $\max_{\{M_{b|y}\}}\mathcal{W}$ over the measurements also constitutes an SDP. Since SDPs can be efficiently evaluated [36], this routine of two SDPs can be iterated to bound $\mathcal{W}^Q$ from below.

The task of bounding $\mathcal{W}^Q$ from outside the quantum set is less straightforward. Nevertheless, this can be achieved through a hierarchy of SDP relaxations of the task. For this purpose, we exploit that we can limit the analysis to pure states of dimension $2n$. SDP relaxations of quantum correlations subject only to such dimensional constraints were introduced in Refs. [37,38] based on randomly sampling from the state and measurement spaces. In SM [35], we show that this method can be extended to also incorporate the constraints (3). The key adaptation is that the target states are included in the sampling procedure in such a way that the fidelities (2), which are merely quantum probabilities, explicitly appear as elements of the final SDP matrix. Notably, this algorithm can be implemented very efficiently by appropriately adapting the methods of Ref. [39].

Remark:The methods, for bounding the quantum set from the interior and the exterior, respectively, have been explored in several case studies and were almost always found to produce coinciding bounds, thus identifying $\mathcal{W}^Q$ up to solver precision. This attests to their usefulness in practice.

State discrimination with distrust.—The simplest task relevant to the distrust-bounded framework is that of quantum state discrimination. Alice has two target states ($x\in\{1,2\}$) which, w.l.g, can be chosen as qubit states with Bloch vectors $\vec{n}_1=(0,0,1)$ and $\vec{n}_2=(\sin\theta,0,\cos\theta)$ for some $\theta\in[0,\pi]$. Bob's aim is to guess their label, i.e., to output $b = x$. The average success probability is $\mathcal{W}_{\mathrm{SD}} = \frac{1}{2}p(1|1) + \frac{1}{2}p(2|2)$. The well-known textbook scenario corresponds to the special case in which the distrust parameter $\epsilon \equiv \epsilon_1 = \epsilon_2 = 0$, i.e., Alice's states are known. In contrast, when $\epsilon > 0$, Bob attempts discrimination without knowing the precise set of states sent by Alice.

Correlations in distrust-bounded state discrimination can be analyzed by solely analytical means, i.e., without employing the above discussed numerical methods. In SM [35], the following optimal success probability is derived for any choice of target state (θ) and any distrust parameter (ϵ):

$$\mathcal{W}_{\mathrm{SD}}^{Q} = \frac{1}{2}\left(1 + \sin\frac{\theta}{2}\right) + \left[\sqrt{\epsilon(1-\epsilon)}\cos\frac{\theta}{2} - \epsilon\sin\frac{\theta}{2}\right], \quad (5)$$

for $\epsilon \leq \frac{1}{2}(1 - \sin(\theta/2))$ and otherwise $\mathcal{W}_{\mathrm{SD}}^{Q} = 1$. The expression can be interpreted as an ϵ-dependent correction (second term) to the Helstrom bound [40] (first term) which governs conventional state discrimination. Thus, the consequence of not assuming a specific model for how the allowed distrust is manipulated is that the measured correlations become increasingly suboptimal as ϵ increases.

Certification of detection efficiency.—The simplicity of the state discrimination protocol makes it a natural platform for application in semi-DI certification of detection efficiency. Notably, such certification has previously been considered in a dimension-based semi-DI framework [15]; however, the present framework is based on a more natural assumption, experimentally simpler and gives stronger certification.

A simple model of a measurement device endows it with a detection efficiency $\eta \in [0,1]$ which is the probability that it successfully detects an incoming physical system. Consequently, the measurement effectively has three outcomes, $\{\tilde{M}_1, \tilde{M}_2, \tilde{M}_{\emptyset}\}$, where $\tilde{M}_{\emptyset}$ represents failed detection. The most general measurement therefore takes the form $M_b = \sum_{\tilde{b}=1,2,\emptyset} p(b|\tilde{b})\tilde{M}_{\tilde{b}}$ for some postprocessing $p(b|\tilde{b})$ determining the final outcome $b \in \{1,2\}$. We assume that the efficiency is independent of the incoming state, i.e., $\forall \rho$: $tr(\rho\tilde{M}_{\emptyset}) = 1 - \eta$, which implies $\tilde{M}_{\emptyset} = (1-\eta)\mathbb{1}$. In state discrimination, it is optimal to map the outcome $\emptyset$ into one of the outcomes $b \in \{1,2\}$, while otherwise setting $b = \tilde{b}$. Therefore, given (θ, ϵ, η), the optimal success probability is $\eta W_{\mathrm{SD}}^{Q} + 1 - \eta/2$. Upon observing $\mathcal{W}_{\mathrm{SD}}$ in the lab, one certifies that $\eta \geq 2\mathcal{W}_{\mathrm{SD}} - 1/2\mathcal{W}_{\mathrm{SD}}^{Q} - 1$.

We investigate the usefulness of this bound by modeling realistic imperfections. Suppose that Alice prepares noisy target states; $\rho_x = v|\psi_x\rangle\langle\psi_x| + 1 - v/2\mathbb{1}$ for some visibility $v \in [0,1]$. This corresponds to a distrust of $\epsilon = (1-v)/2$. Also, suppose that Bob's optimal measurement, when successful, is perturbed by an alignment error of angle δ in the Bloch sphere and that the true detection efficiency is η_{true}. Then, the certified bound on the detection efficiency becomes

$$\eta \geq \begin{cases} \frac{v\eta_{\mathrm{true}}\cos\delta}{v+\sqrt{1-v^2}\cot\frac{\theta}{2}} & \text{if } v \geq \sin\frac{\theta}{2} \\ v\eta_{\mathrm{true}}\cos\delta\sin\frac{\theta}{2} & \text{otherwise,} \end{cases} \quad (6)$$

which is linear in η_{true}. For instance, if our target states correspond to $\theta = 5\pi/6$ and the imperfections are given by $v = 99\%$ ($\epsilon = 0.5\%$) and $\delta = 1$ deg, we obtain $\eta \geq 0.963\eta_{\mathrm{true}}$, which is a nearly optimal bound. In contrast, with an order of magnitude larger imperfections ($v = 90\%$, $\delta = 10$ deg), the bound remains reasonably good; $\eta \geq 0.855\eta_{\mathrm{true}}$. Note that (6) becomes stronger for more distinguishable target states.

Correlations from classical measurements.—How do we describe classical correlations in the distrust-bounded framework? The source is inherently quantum since the target states generally do not commute. However, we may consider the situation in which the measurement device is classical, i.e., all measurements are diagonal in the same basis. Within the quantum formalism, such measurements are written $M_{b|y} = \sum_k p(b|y,k)|e_k\rangle\langle e_k|$, where $\{|e_k\rangle\}$ is some orthonormal basis of Hilbert space. The correlations then take the form

$$p(b|x,y) = \sum_k p(b|y,k)\langle e_k|\rho_x|e_k\rangle, \quad (7)$$

which can be interpreted as a postprocessing of the outcome obtained from measuring ρ_x in the basis $\{|e_k\rangle\}$.

How can we bound any given function (4) in such a model? As shown in SM [35], we can w.l.g restrict to considering only the finitely many deterministic postprocessing, $p(b|y,k) \in \{0,1\}$ (again, we may restrict to dimension $2n$). This simplification allows us to bound the maximal value of $\mathcal{W}$ by largely recycling the SDP relaxation method previously discussed for bounding quantum correlations. However, now the SDP relaxation is based only on a single quantum measurement and must be considered separately for every deterministic postprocessing (see SM [35]).

Interestingly, there exists a critical value $\epsilon_{\mathrm{crit}} = n - 1/n$ of the distrust parameter $\epsilon \equiv \epsilon_x$, at which Alice can send her input to Bob. Then, Bob can classically generate any distribution $p(b|x,y)$. To show this, consider the worst-case scenario in which all target states are identical, $|\psi_x\rangle = |0\rangle$, and choose the preparations $|\phi_x\rangle = 1/\sqrt{n}\sum_{j=0}^{n-1} e^{[2\pi i j(x-1)]/n}|j\rangle$ corresponding to the Fourier basis of $\mathbb{C}^n$. The fidelities are $|\langle\psi_x|\phi_x\rangle|^2 = 1/n = 1 - \epsilon_{\mathrm{crit}}$ and x is recovered by measuring the basis $\{|\phi_x\rangle\}$.

Quantum advantages.—Quantum correlations that do not admit the form (7) constitute a certificate of the impossibility of viewing Bob's set of measurements as a postprocessing of a single measurement. It is therefore evident that if such an advantage exists, it requires at least two measurements. This motivates us to go beyond state discrimination and consider a scenario featuring three preparations and two binary-outcome measurements. We choose the function

$$\mathcal{W}_{322} = E_{11} + E_{12} + E_{21} - E_{22} - E_{32}, \qquad (8)$$

where $E_{xy} = p(0|x,y) - p(1|x,y)$ and select the target states $\{|\psi_1\rangle, |\psi_2\rangle, |\psi_3\rangle\}$ as qubits forming an isosceles triangle in the xz plane of the Bloch sphere. Their Bloch vectors are $\vec{n}_1 = (0,0,1)$, $\vec{n}_2 = (1,0,0)$, and $\vec{n}_3 = 1/\sqrt{2}(-1,0,-1)$.

We have employed an alternating convex search together with SDP relaxations of the quantum set of correlations in order to bound $\mathcal{W}_{322}$ from below and above [41], respectively. It is found that these bounds generally coincide, thus constituting a tight bound. Similarly, we have also employed SDP relaxations to bound the function in models with classical measurements. The results are presented in Fig. 1. It is found that quantum theory allows stronger correlations for distrust up $\epsilon \approx 33\%$. This threshold is marginally lower than the value of ϵ at which the algebraically maximal value $\mathcal{W}_{322} = 5$ is attained. Moreover, the maximal quantum value $\mathcal{W}_{322}^{Q} = 1 + 2\sqrt{2}$, which corresponds to exactly preparing the target states and then performing the optimal measurements, certifies a quantum advantage over classical measurement models even if we supplement the latter with a distrust of up to $\epsilon \approx 3.1\%$. This illustrates a quantum advantage robust to distrusted models with classical measurements. Furthermore, in SM [35], we analogously compare correlations based on a random access code and find that the value of ϵ required to model an ideal quantum protocol with classical measurements is increased to $\epsilon \approx 4.5\%$.

Random number generation.—We consider the task of semi-DI random number generation in the presence of an external eavesdropper. The eavesdropper can possess a detailed description of the devices on the level of a hidden variable λ with distribution $p(\lambda)$. For each λ, the eavesdropper prepares a quantum realization for Alice and Bob, thus creating correlations $p_\lambda(b|x,y)$, that on average return Alice's and Bob's observed correlations, $p = \sum_\lambda p(\lambda)p_\lambda$. The task is to certify that Bob's outcome (for specific inputs x^* and y^*) contains some randomness from the eavesdropper's point of view. A standard quantifier of randomness is the conditional minimum entropy $H_{\min} = -\log_2(G)$, which is based on the eavesdropper's highest probability of guessing Bob's outcome: $G = \max \sum_\lambda p(\lambda) \max_b p_\lambda(b|x^*,y^*)$, where the first maximization is over $p(\lambda)$ together with all conditional quantum realizations compatible with the observed correlations p. If one does not use p but only a linear function $\mathcal{W}[p]$ to certify randomness, then an upper bound on G can be obtained in the following handy way. Evaluate the $G'(\mathcal{W}) = \max \max_b p(b|x^*,y^*)$, where the first maximization now is over all quantum realizations consistent with $\mathcal{W}[p] = \mathcal{W}$. The concave hull of $G'(\mathcal{W})$ is an upper bound on G [42–45]. This method has been used in many previous semi-DI randomness generation protocols [3,4,20,25,33].

In our protocol based on $\mathcal{W}_{322}$, using the same target states as earlier, it is favorable to extract randomness from the specific inputs $(x^*,y^*) = (3,2)$. Upper bounds on $G'(\mathcal{W}_{322})$ can be obtained systematically using the previously discussed hierarchy of SDP relaxations of the quantum set of correlations. In Fig. 2, we show the trade-off between the generated randomness and the distrust parameter as obtained from three different function values $\mathcal{W}_{322} = k \times (1 + 2\sqrt{2})$, for $k \in \{0.97, 0.99, 1\}$, where $1 + 2\sqrt{2}$ is the ideal value obtained in a quantum protocol implementing the precise target states and optimal

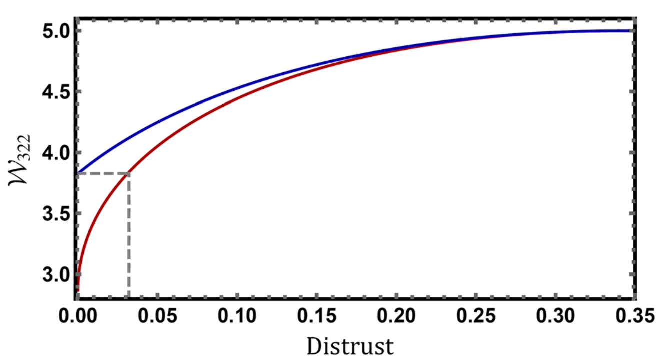

FIG. 1. The function $\mathcal{W}_{322}$ versus the distrust parameter ϵ for target states forming an isosceles triangle with angles $\{90°, 135°\}$ in the xz plane of the Bloch sphere. The blue curve is the tight quantum bound. The red curve is an upper bound for hybrid quantum-classical models.

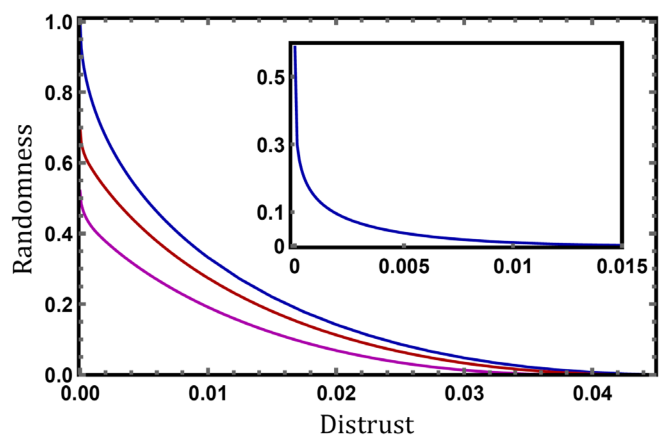

FIG. 2. Randomness versus distrust parameter ϵ for the function $\mathcal{W}_{322}$ based on target states forming an isosceles triangle in the xz plane of the Bloch sphere. The randomness is evaluated for the function values $\mathcal{W}_{322}^{Q}$ (blue), $0.99\mathcal{W}_{322}^{Q}$ (red), and $0.97\mathcal{W}_{322}^{Q}$ (purple), where $\mathcal{W}_{322}^{Q} = 1 + 2\sqrt{2}$ corresponds to the precise target states. Inset plot: randomness versus distrust based on the optimal value of the function $\mathcal{W}_{\mathrm{SD}}$ for $\theta = \pi/5$.

measurements. We find that even for suboptimal correlations a large amount of randomness can be generated if the distrust is small. Moreover, some randomness is still obtained even when the distrust is around a few percent. In addition, we have illustrated randomness generation based on the simpler state discrimination protocol (see Fig. 2 inset) which is found to give a less robust rate.

The function (8) has been experimentally realized [46] in the context of dimension witnessing using polarization qubits. Considering the same target states as here, the reported experimental value was $\mathcal{W}_{322}^{\mathrm{exp}} = 3.7815 \pm 0.0782$. While the distrust could be estimated through explicit additional measurements, let us consider the drastic case in which all the imperfections are attributed to white noise in the preparation device. Then, the average measured value implies $\epsilon \approx 0.6\%$ from which we can extract 0.052 bits of randomness. This may be viewed as a proof of principle. However, it is relevant to note that recent experiments have performed similar prepare-and-measure experiments achieving visibilities well above 99% in the preparation devices (see, e.g., [18,24]). Such state of the art makes possible substantially higher rates of semi-DI randomness.

Discussion.—Here, we have introduced a framework for semi-DI quantum information processing based on a tunable degree of distrust in the quantum devices, investigated the correlations that it may give rise to, and harvested these toward quantum information protocols. The tools outlined here are versatile as they apply to general prepare-and-measure scenarios. The introduced framework has two important conceptual features: (i) it tailors the analysis directly to the set of states targeted by the experimenter, and (ii) the notion of distrust is an observable quantity. The first point distinguishes the framework from all previous approaches to semi-DI quantum information. The second point distinguishes it from the standard dimension-based approach [1], the overlap-based approach [25], and the information-based approach [32], but not from the energy-based approach [28]. It is then interesting to note that the energy-based framework emerges as a special instance of the distrust-based framework, corresponding to when all target states are identical.

A few natural avenues for further research are mentioned. (i) Exploration of other quantum information protocols, e.g., in cryptography, that are interesting to consider in the distrust-bounded framework. How robust are common quantum information protocols to uncontrolled imperfections? (ii) Experimental realization of efficient random number generators based on bounded distrust. To this end, it may be relevant to also consider protocols different from those investigated here. (iii) We discussed hybrid models based on quantum sources and classical measurements. Can one define a natural notion of fully classical models? Is it possible to have a quantum advantage over such models when the latter are permitted any degree of distrust smaller than the critical limit $\epsilon = (n-1)/n$?

The author thanks Jef Pauwels, Erik Woodhead, Stefano Pironio, and Nicolas Brunner for feedback. This work was supported by the Swiss National Science Foundation through Early PostDoc Mobility fellowship P2GEP2 194800.

*armin.tavakoli@oeaw.ac.at

[1] M. Pawłowski and N. Brunner, Phys. Rev. A **84**, 010302(R) (2011).

[2] E. Woodhead and S. Pironio, Phys. Rev. Lett. **115**, 150501 (2015).

[3] H.-W. Li, Z.-Q. Yin, Y.-C. Wu, X.-B. Zou, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **84**, 034301 (2011).

[4] H.-W. Li, M. Pawłowski, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **85**, 052308 (2012).

[5] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, in *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, STOC '99* (Association for Computing Machinery, New York, NY, USA, 1999), pp. 376–383.

[6] A. Ambainis, D. Leung, L. Mancinska, and M. Ozols, arXiv:0810.2937v3.

[7] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane, Phys. Rev. Lett. **114**, 170502 (2015).

[8] A. Tavakoli, J. Kaniewski, T. Vértesi, D. Rosset, and N. Brunner, Phys. Rev. A **98**, 062307 (2018).

[9] M. Farkas and J. Kaniewski, Phys. Rev. A **99**, 032316 (2019).

[10] A. Tavakoli, A. A. Abbott, M.-O. Renou, N. Gisin, and N. Brunner, Phys. Rev. A **98**, 052333 (2018).

[11] K. Mohan, A. Tavakoli, and N. Brunner, New J. Phys. **21**, 083034 (2019).

[12] N. Miklin, J. J. Borkała, and M. Pawłowski, Phys. Rev. Research **2**, 033014 (2020).

[13] P. Mironowicz and M. Pawłowski, Phys. Rev. A **100**, 030301(R) (2019).

[14] C. Spee, Phys. Rev. A **102**, 012420 (2020).

[15] A. Tavakoli, Phys. Rev. Lett. **125**, 150503 (2020).

[16] N. Miklin and M. Oszmaniec, Quantum **5**, 424 (2021).

[17] C. Carmeli, T. Heinosaari, and A. Toigo, Europhys. Lett. **130**, 50001 (2020).

[18] A. Tavakoli, M. Smania, T. Vértesi, N. Brunner, and M. Bourennane, Sci. Adv. **6**, eaaw6664 (2020).

[19] T. Lunghi, J. B. Brask, C. C. Wen Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).

[20] P. Mironowicz, A. Tavakoli, A. Hameedi, B. Marques, M. Pawłowski, and M. Bourennane, New J. Phys. **18**, 065004 (2016).

[21] D. Martínez, A. Tavakoli, M. Casanova, G. Cañas, B. Marques, and G. Lima, Phys. Rev. Lett. **121**, 150504 (2018).

[22] G. Foletto, L. Calderaro, G. Vallone, and P. Villoresi, Phys. Rev. Research **2**, 033205 (2020).

[23] H. Anwer, S. Muhammad, W. Cherifi, N. Miklin, A. Tavakoli, and M. Bourennane, Phys. Rev. Lett. **125**, 080403 (2020).

[24] M. Farkas, N. Guerrero, J. Cariñe, G. Cañas, and G. Lima, Phys. Rev. Applied **15**, 014028 (2021).

[25] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, H. Zbinden, and N. Brunner, Phys. Rev. Applied **7**, 054018 (2017).

[26] Y. Wang, I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, npj Quantum Inf. **5**, 17 (2019).

[27] W. Shi, Y. Cai, J. B. Brask, H. Zbinden, and N. Brunner, Phys. Rev. A **100**, 042108 (2019).

[28] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, Quantum **1**, 33 (2017).

[29] T. Van Himbeeck and S. Pironio, arXiv:1905.09117.

[30] D. Rusca, T. van Himbeeck, A. Martin, J. B. Brask, W. Shi, S. Pironio, N. Brunner, and H. Zbinden, Phys. Rev. A **100**, 062338 (2019).

[31] H. Tebyanian, M. Avesani, G. Vallone, and P. Villoresi, arXiv:2009.08897v1.

[32] A. Tavakoli, E. Zambrini Cruzeiro, J. B. Brask, N. Gisin, and N. Brunner, Quantum **4**, 332 (2020).

[33] A. Tavakoli, E. Z. Cruzeiro, E. Woodhead, and S. Pironio, arXiv:2007.16145v2.

[34] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).

[35] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.126.210503 for details on the dimension restriction for the set of correlations, the SDP methods and quantum state discrimination.

[36] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).

[37] M. Navascués and T. Vértesi, Phys. Rev. Lett. **115**, 020501 (2015).

[38] M. Navascués, A. Feix, M. Araújo, and T. Vértesi, Phys. Rev. A **92**, 042117 (2015).

[39] A. Tavakoli, D. Rosset, and M.-O. Renou, Phys. Rev. Lett. **122**, 070501 (2019).

[40] C. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, NY, 1976).

[41] The following hierarchy level was used $\{\mathbb{1}, \rho, \psi, M, \rho^2, \rho\psi, \rho M, M^2, \rho^2\}$ which corresponds to an SDP of size 66. Notice that we can restrict to considering only projective measurements since these are the extremal binary-outcome measurements.

[42] S. Pironio, A. Acín, S. Massar, A. B. de la Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, and C. Monroe, Nature (London) **464**, 1021 (2010).

[43] L. Masanes, S. Pironio, and A. Acín, Nat. Commun. **2**, 238 (2011).

[44] O. Nieto-Silleras, S. Pironio, and J. Silman, New J. Phys. **16**, 013035 (2014).

[45] J.-D. Bancal, L. Sheridan, and V. Scarani, New J. Phys. **16**, 033011 (2014).

[46] J. Ahrens, P. Badziag, A. Cabello, and M. Bourennane, Nat. Phys. **8**, 592 (2012).