Device-Independent Randomness Generation in the Presence of Weak Cross-Talk

J. Silman, S. Pironio, and S. Massar

Laboratoire d'Information Quantique, Université Libre de Bruxelles (ULB), 1050 Bruxelles, Belgium

(Received 26 November 2012; published 8 March 2013)

Device-independent protocols use nonlocality to certify that they are performing properly. This is achieved via Bell experiments on entangled quantum systems, which are kept isolated from one another during the measurements. However, with present-day technology, perfect isolation comes at the price of experimental complexity and extremely low data rates. Here we argue that for device-independent randomness generation—and other device-independent protocols where the devices are in the same lab—we can slightly relax the requirement of perfect isolation and still retain most of the advantages of the device-independent approach, by allowing a little cross-talk between the devices. This opens up the possibility of using existent experimental systems with high data rates, such as Josephson phase qubits on the same chip, thereby bringing device-independent randomness generation much closer to practical application.

DOI: 10.1103/PhysRevLett.110.100504 PACS numbers: 03.67.Ac, 03.65.Ud, 03.67.Dd

Introduction.—The great advantage of device-independent (DI) protocols is their reliance on a small set of tests, which are nevertheless sufficient to certify that they are performing properly. This is achieved by carrying out nonlocality tests on entangled quantum systems. In particular, no assumptions are made regarding the inner workings of the devices (the Hilbert space dimension of the underlying quantum systems, etc.) [1,2]. Each device is treated as a "black box" with knobs and registers for selecting and displaying (classical) inputs and outputs. Applications include quantum key distribution [2–7], coin flipping [8], state tomography [6,9,10], genuine multipartite entanglement detection [11], self-testing of quantum computers [12,13], as well as DI randomness generation (RG) [14–18].

It is often remarked that DI cryptographic protocols remain secure even if the devices have been provided, or sabotaged, by an adversary. This scenario, while conceptually fascinating, is of little (if any) practical relevance because (i) there are so many types of attacks available to a malicious provider—the majority being classical—that eliminating them all is an enormous task, and (ii) in any case we assume the existence of honest providers of, e.g., the source of randomness, the jamming technology to prevent information leakage from the labs, or the classical devices used to process the data. A scenario where one can trust the providers of all of the above, but not the provider of the *quantum* devices, is highly implausible.

The actual advantage of DI protocols is that they allow us to monitor the performance of the devices irrespective of noise, imperfections, lack of knowledge regarding their inner workings, or limited control over them. Indeed, even if the devices were obtained from a trusted provider and thoroughly inspected, many things can still unintentionally go wrong (as demonstrated by the attacks on commercial quantum key-distribution systems [19–21], which exploited unintentional design flaws).

This problem is particularly acute in the case of DI RG, as it is very difficult even for honest parties to manufacture reliable randomness generators (whether classical or quantum) and monitor them for malfunction. The generation of randomness in a DI manner solves many of the shortcomings of customary RG protocols, because, as mentioned above, the degree of violation of a Bell inequality provides an accurate estimate of the amount of randomness generated irrespective of experimental imperfections and lack of control. DI RG has so far been proven secure against adversaries with classical side information about the devices (which is the relevant case when the provider is trusted) for arbitrary Bell inequalities and degrees of violation [16,17], and against adversaries with quantum side information in the case of very high violations of the Clauser-Horne-Shimony-Holt (CHSH) inequality [18].

Unfortunately, DI RG is experimentally highly challenging. It requires a Bell experiment with the detection loophole closed and with the quantum systems isolated from one another. A proof of principle experiment was reported in Ref. [15] using two ions in separate vacuum traps, but this system operates at an extremely low rate ($\sim$1 mHz), precluding any practical application. Nevertheless, there exist today experiments involving, for example, two Josephson phase qubits on the same chip coupled by a radio frequency resonator [22], or two ions in the same trap coupled via their vibrational modes [23,24], which allow for Bell violating experiments (with the detection loophole closed) at much higher data rates ($\gtrsim$1 kHz).

In these experiments the quantum systems are very close to one another. This proximity provides the non-negligible coupling required for high entanglement generation rates. Adapting DI RG to these types of experiments would bring it much closer to real-life application. The problem is that precisely because the systems are close to one another and non-negligibly coupled, they can no longer be considered as completely isolated (see Refs. [25,26] for a discussion of the couplings involved). The aim of the present work is to show how to take this coupling into account by relaxing slightly the assumptions behind the DI approach, while keeping as much as possible all of its advantages.

We begin by showing how to derive bounds on the RG rate in a DI setting given a known amount of cross-talk (CT) between the devices. Next, we present methods for estimating the amount of CT present in an experiment. Our approach is then illustrated on Josephson phase qubits, showing that efficient DI RG is possible using already established technology. We start, however, by recalling briefly the essential ingredients of DI RG relevant to our analysis. We refer to Refs. [15–17] for a more detailed presentation.

Bell inequalities and device-independent randomness generation.—A Bell experiment is characterized by the probabilities $\mathcal{P} = \{P_{ab|xy}\}$ of obtaining the outcomes (or outputs) a and b given the measurement settings (or inputs) x and y. A Bell expression $I(\mathcal{P}) = \sum_{abxy} c_{abxy} P_{ab|xy}$ is a linear function of these probabilities. For instance, the CHSH inequality has the form $I(\mathcal{P}) = \sum_{a,b,x,y\in\{0,1\}} (-1)^{a\oplus b\oplus xy} P_{ab|xy} \leq 2$. To any Bell expression, one can associate a bound on the randomness of the outputs given the inputs x and y through a function $P^*_{xy}(I)$ such that $\max_{a,b} P_{ab|xy} \leq P^*_{xy}(I)$ holds for any $\mathcal{P}$ for which $I(\mathcal{P}) = I$ [15–17]. The function $P^*_{xy}(I)$ should be monotonically decreasing and concave in I (if not we can take its concave hull). Higher values of $P^*_{xy}(I)$ imply less randomness, in particular when $\min_{x,y} P^*_{xy}(I) = 1$ the system is fully deterministic.

Given knowledge of such a function and the degree of Bell violation I observed in an experiment where the devices are used n times in succession, one can infer a lower bound on the min-entropy of the measurement outcomes. By applying a randomness extractor to the resulting string of outcomes, one then obtains a new private string of random numbers of length $\simeq -n\log_2 P^*_{xy}(I)$, which is arbitrarily close (up to a security parameter) to the uniform distribution. Depending on the assumptions made regarding the devices and the adversary, such a protocol may also require an initial random seed (in which case one talks about DI randomness expansion) that may be polynomially [15] or exponentially [16,17] smaller than the output string.

Device-independent randomness generation with weak cross-talk.—In the security analysis of DI RG protocols the assumption that the two Bell violating devices are isolated from one another only appears in the derivation of the bound $P^*_{xy}(I) \geq \max_{a,b} P_{ab|xy}$. If we introduce a similar bound $P^*_{xy}(I, \chi)$ that is valid in the presence of a given amount of CT χ (defined below), then the rest of the reasoning of Refs. [15–17] will apply without modification.

To define such a CT-dependent bound, we write the probabilities observed in a Bell experiment as $P_{ab|xy} = \mathrm{Tr}(\rho \Pi_{ab|xy})$, where $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ and $\{\Pi_{ab|xy}\}$ is a positive operator valued measure (POVM) on $\mathcal{H}_A \otimes \mathcal{H}_B$ (i.e., the $\Pi_{ab|xy}$ are positive semidefinite, which we write as $\Pi_{ab|xy} \succeq 0$, and $\sum_{ab} \Pi_{ab|xy} = \mathbb{1}$). The novelty with respect to the standard mathematical description of Bell experiments is in allowing the measurement $\Pi_{ab|xy}$ to act collectively on the two systems. We will say that such a collective measurement requires no more than χ amount of CT if there exists a product POVM $\{\Pi_{a|x} \otimes \Pi_{b|y}\}$ satisfying

$$-\chi\mathbb{1} \preceq \Pi_{ab|xy} - \Pi_{a|x} \otimes \Pi_{b|y} \preceq \chi\mathbb{1}, \tag{1}$$

for all combinations of a and b. This condition restricts how far each collective POVM may be from a product of two independent POVMs. In particular, when $\chi = 0$ the $\Pi_{ab|xy}$ can be expressed as products, while when $\chi = 1$ they are unconstrained.

Consider now a fixed value of χ and a Bell violation I. The solution of the following program provides the minimal amount of randomness $P^*_{xy}(I, \chi)$ compatible with I and χ:

$$P^*_{xy}(I, \chi) = \max_{a,b} \max_{Q} \quad P_{ab|xy} \tag{2}$$

such that

$$P_{ab|xy} = \mathrm{Tr}(\rho \Pi_{ab|xy}), \qquad I(\mathcal{P}) = I,$$
$$-\chi\mathbb{1} \preceq \Pi_{ab|xy} - \Pi_{a|x} \otimes \Pi_{b|y} \preceq \chi\mathbb{1},$$

where the optimization runs over the set $Q = \{\rho, \{\Pi_{a|x}\}, \{\Pi_{b|y}\}, \{\Pi_{ab|xy}\}, \mathcal{H}_A, \mathcal{H}_B\}$ specifying the state, measurements, and the Hilbert spaces. This formulation is therefore DI in spirit because the bound is formulated without fixing the dimension of the Hilbert spaces, nor how the measurements are implemented, etc.

Upper bounds on the optimization problem Eq. (2) can be obtained using the techniques of Refs. [27,28], which relax the problem to a hierarchy of semidefinite programs. In particular, the resulting series of bounds is guaranteed to converge to the true solution. Nevertheless, depending on the problem, even the lowest order relaxation may be computationally intractable. We may then obtain a weaker bound in terms of $P^*_{xy}(I, 0)$—the solution in the absence of CT. Let ρ', $\{\Pi'_{a|x}\}$, $\{\Pi'_{b|y}\}$, and $\{\Pi'_{ab|xy}\}$ be the state and POVMs corresponding to the solution of Eq. (2), and let $P'_{ab|xy} = \mathrm{Tr}(\rho' \Pi'_{a|x} \otimes \Pi'_{b|y})$ and $\mathcal{P}' = \{P'_{ab|xy}\}$. From the last constraint in Eq. (2) we have that $|P_{ab|xy} - P'_{ab|xy}| \leq \chi$, and so $I(\mathcal{P}') \geq I(\mathcal{P}) - \gamma\chi$ where $\gamma = \sum_{a,b,x,y} |c_{abxy}|$ (in the case of the CHSH inequality, for instance, $\gamma = 16$). Taken together, the last two inequalities imply that

$$P^*_{xy}(I, \chi) \leq P^*_{xy}(I - \gamma\chi, 0) + \chi. \tag{3}$$

Figure 1 displays upper bounds on P^*_{00} obtained from Eqs. (2) and (3) in the case of the CHSH inequality.

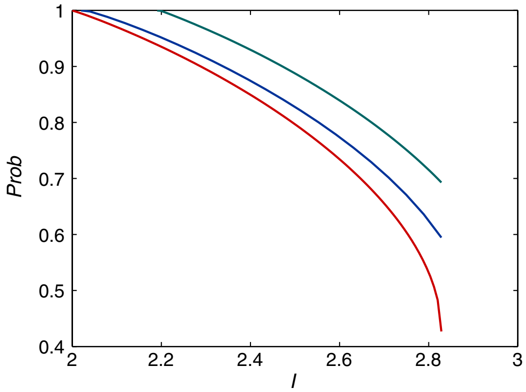

FIG. 1 (color online). DI upper bounds on P^*_{00}. The middle and top curves give semidefinite programming based upper bounds obtained from Eqs. (2) and (3), respectively, as a function of the CHSH violation I, given $\chi = 0.01$. The bottom curve bounds P^*_{00} when $\chi = 0$.

Finally, we note that the last constraint in Eq. (2) implies that the signaling—the extent to which the output of one device depends on the input of the other—is constrained. Specifically, if to each input x and each input y correspond N outputs, $|P_{a|xy} - P_{a|xy'}| \le 2N\chi$ for all a, x, y, y', etc. (in the case of zero signaling, one has $P_{a|xy} = P_{a|xy'}$). This allows us to derive a simpler bound on P^*_{xy}, depending solely on the amount of signaling present, in contrast to the bounds Eqs. (2) and (3), which rely on the full structure of quantum mechanics. To this end we define the maximal amount of signaling allowed as

$$\delta = \max\{\max_{a,x,y,y'} |P_{a|xy} - P_{a|xy'}|, \max_{b,y,x,x'} |P_{b|xy} - P_{b|x'y}|\}. \quad (4)$$

When $\delta = 0$, $\mathcal{P}$ resides within the no-signaling polytope [29], while when $\delta > 0$ $\mathcal{P}$ resides within a larger, higher-dimensional polytope. The bound can be obtained by solving the linear program $P^*_{xy}(I, \delta) = \max_{ab} P_{ab|xy}$, given that $\mathcal{I}(\mathcal{P}) = I$, $|P_{a|xy} - P_{a|xy'}| \le \delta$, and $|P_{b|xy} - P_{b|x'y}| \le \delta$. In the case of the CHSH inequality, one can show that (see Section A of the Supplemental Material [30])

$$P^*_{xy}(I, \delta) \le \frac{3}{2} - \frac{1}{4} I + 2\delta. \quad (5)$$

This bound applies to any postquantum theory that restricts the amount of signaling (as well as to quantum mechanics).

Estimating the amount of cross-talk.—We have just seen how the introduction of a new security parameter χ, quantifying the amount of CT between the devices, allows us to extend the scope of DI RG to settings with a limited amount of CT. To apply this approach, we therefore need a reliable prior estimate of χ and a means of guaranteeing or verifying that the CT will not exceed this estimate during latter operations of the devices. This obviously requires some modeling of the devices' inner workings. Indeed, it is impossible to set an upper bound for the amount of CT from first principles only or from any set of observed data $\mathcal{P}$ alone, since communicating devices can deterministically reproduce any $\mathcal{P}$, and therefore simulate any degree of Bell violation.

At first, this may seem an unwelcome departure from the purely DI approach (i.e., $\chi = 0$). Nevertheless, our approach has the advantage over fully device-dependent approaches in that only a *single* parameter χ must be device-*dependently* estimated to ensure that the protocol performs properly, and this same parameter is used irrespective of the underlying physical realization. Moreover, even in purely DI protocols the absence of communication cannot be deduced from the observed data alone, and to verify that there is indeed no communication will necessarily involve putting our trust in certain general assumptions regarding the behavior of the devices, or relying on some trusted external hardware. Seen in this light, our approach is not very different from the standard (DI) one, except that instead of verifying in some trusted way that $\chi = 0$, we must verify that χ is no greater than some finite value. Finally, we note that our approach allows us as a safeguard to set χ to be greater than its expected value—a feature that may be useful even in purely DI protocols with (allegedly) noncommunicating devices.

Even though a maximal amount of CT χ cannot be guaranteed without some modeling of the devices, there are several ways to set a lower bound for χ from the observed data $\mathcal{P}$ only. If the devices were not fabricated by an adversary and do not act maliciously, then these lower bounds may provide good estimates of χ.

A simple way to set a lower bound for χ in a DI manner is via the degree of violation of the no-signaling conditions Eq. (4), computed from the observed data $\mathcal{P}$. From Eq. (4) it follows that $\chi \ge \delta/2N$. Improved DI bounds are obtainable, however, reflecting the fact that δ does not capture all of the information contained in $\mathcal{P}$. The minimal amount of CT that is compatible with a given $\mathcal{P}$ is given by the solution of the following optimization problem:

$$\min_{Q} \chi \quad (6)$$

such that

$$\mathrm{Tr}(\rho \Pi_{ab|xy}) = P_{ab|xy},$$
$$-\chi \mathbb{1} \preceq \Pi_{ab|xy} - \Pi_{a|x} \otimes \Pi_{b|y} \preceq \chi \mathbb{1},$$

which can be lower bounded using the techniques of Refs. [27,28]. It is clear that this bound is optimal, since the optimization runs over all possible states ρ and sets of projectors $\{\Pi_{a|x}\}$, $\{\Pi_{b|y}\}$, and $\{\Pi_{ab|xy}\}$ satisfying the constraints in Eq. (6). That it constitutes an improvement over the bound provided by Eq. (4) is seen by considering the case of postquantum nonsignaling distributions (including those that do not violate Tsirelson's bound [31]). Such distributions will not give rise to a nonvanishing bound via Eq. (4). However, because they cannot be realized quantumly without communication, they will give rise to a nonvanishing bound via Eq. (6). See Fig. 2.

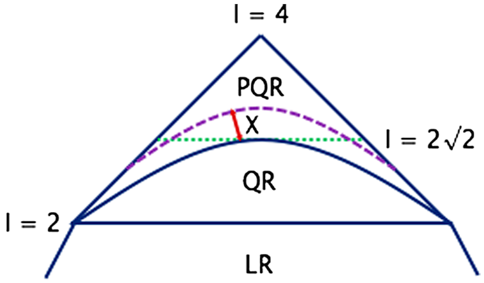

FIG. 2 (color online). Part of the no-signaling polytope. The curved solid line separates the postquantum region (PQR) from the quantum region (QR)—the set of probabilities that can be realized by product measurements on quantum states. The horizontal dotted line represents Tsirelson's bound. The horizontal solid line separates QR from the classical or local region (LR). The top vertex corresponds to the PR box [34]. Although nonsignaling, points in PQR cannot be realized by product measurements, but only by nonproduct ones. Restricting the amount of CT to χ, only points below the curved dashed line are (quantumly) realizable.

It is possible of course that the true value of χ is not revealed by the above lower bounds (for instance, points in QR in Fig. 2 can be reproduced either with or without CT, and thus the real value of χ cannot be unambiguously determined from the observed data $\mathcal{P}$ alone). Nevertheless, one can also adopt a more device-dependent approach to estimating χ. In particular, if the lower bound provided by Eq. (6) equals zero, one can vary the state and the measurements. Such a procedure could in principle reveal the presence of any fixed interaction Hamiltonian H, since it has been shown that for any such interaction there exists a strategy involving only local operations and classical communication that reveals the presence of the interaction as signaling [32]. However, we do not know of any systematic way for finding this strategy if H is unknown, nor do we know how to relate in a systematic way the observed signaling to H.

Finally, by modeling the physical systems, their interaction and the measurement procedure, it is possible to estimate the amount of CT. An example of this last approach are given below.

Candidates for real-life implementation.—A system ideally suited for the implemenation of DI RG will (i) give rise to a sufficiently high Bell violation with the detection loophole kept closed, (ii) exhibit a negligible amount of CT, and (iii) allow for very high data rates. We discuss below an experiment based on Josephson phase qubits that meets all of these requirements. Another possibility is based on trapped ions, as discussed in Section B of the Supplemental Material [30].

In the CHSH experiment of Ref. [22] two Josephson phase qubits, coupled by a radio frequency strip resonator, are used. The qubits are located on the same chip, separated by 3.1 mm, and are entangled by successively coupling them to the strip resonator. Single qubit rotations are effected by applying microwaves at the resonance frequency of the corresponding qubit. Readout is effected by letting the excited state tunnel to an auxiliary state macroscopically distinct from both the ground state and the excited state. All operations can be carried out on time scales significantly shorter than 1 μs. (For a recent review of Josephson phase qubits experiments see Ref. [25].)

The constant coupling between the qubits gives rise to some CT. From the analysis of the experimental setup performed in Refs. [22,33], it appears that the most significant contribution to the CT occurs during the readout: The tunneling of one qubit from the excited state to a macroscopically distinct state sometimes forces the other qubit to tunnel when in the ground state. This allows us to estimate the CT at 0.0030 (see Section C of the Supplemental Material [30]. The same value is also obtained by solving the second order relaxation of Eq. (6) using the set of observed data found in the Supplemental Material of Ref. [22].

For the reported degree of CHSH violation $I = 2.0732$, and the above value of the CT, we find that $P_{00}^* \leq 0.983$. To establish robustness we note that for as low a violation as $I = 2.002$ $P_{00}^* \leq 0.998$. This shows that useful randomness is extractable from this experiment.

Conclusion.—The analysis of any DI protocol requires that we specify the amount of CT between the devices (irrespective of whether it is vanishing or finite)—a requirement that cannot be fully verified or implemented in a DI manner. In this work we have shown that one can relax the maxims appearing in previous works on DI RG, by allowing for a small amount of CT between the quantum systems. In this way we can keep most of the advantages of the DI approach and at the same time reach data rates of practical interest. Finally, we note that our approach can be generalized to other DI protocols where the devices are in the same lab, such as DI tests of genuine multipartite entanglement [11]. More generally, it introduces a general formalism to detect, quantify, and exploit quantum nonlocality in a rapidly increasing number of experimental systems where some amount of cross-talk is present.

J. S. thanks Nati Aharon for valuable discussions. We acknowledge support from the European project QCS, Project No. 255961, from the Inter-University Attraction Poles (Belgian Science Policy) Project Photonics@be, from the Brussels Capital Region through a BB2B grant, and from the FRS-FNRS. The Matlab toolboxes YALMIP [35] and SEDUMI [36] were used to obtain Fig. 2 and solve Eqs. (2) and (6).

[1] D. Mayers and A. Yao, Quantum Inf. Comput. **4**, 273 (2004).

[2] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).

[3] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007); S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[4] M. McKague, New J. Phys. **11**, 103037 (2009).

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

[6] B. W. Reichardt, F. Unger, and U. Vazirani, arXiv:1209.0448.

[7] U. Vazirani and T. Vidick, arXiv:1210.1810.

[8] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, Phys. Rev. Lett. **106**, 220501 (2011).

[9] C.-E. Bardyn, T. C. H. Liew, S. Massar, M. McKague, and V. Scarani, Phys. Rev. A **80**, 062327 (2009).

[10] M. McKague, T. H. Yang, and V. Scarani, J. Phys. A **45**, 455304 (2012).

[11] J.-D. Bancal, N. Gisin, Y. C. Liang, and S. Pironio, Phys. Rev. Lett. **106**, 250404 (2011).

[12] F. Magniez *et al.*, in *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming* (Springer, New York, 2006), p. 72.

[13] M. McKague and M. Mosca, in *Proceedings of the 5th Conference on Theory of Quantum Computation, Communication, and Cryptography* (Springer, New York, 2011), p. 113.

[14] R. Colbeck, Ph.D. dissertation, University of Cambridge, 2007, arXiv:0911.3814; R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).

[15] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).

[16] S. Pironio and S. Massar, Phys. Rev. A **87**, 012336 (2013).

[17] S. Fehr, R. Gelles, and C. Schaffner, Phys. Rev. A **87**, 012335 (2013).

[18] U. Vazirani and T. Vidick, Phil. Trans. R. Soc. A **370**, 3432 (2012).

[19] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H. K. Lo, Phys. Rev. A **78**, 042333 (2008).

[20] F. Xu, B. Qi, and H.-K. Lo, New J. Phys. **12**, 113026 (2010).

[21] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[22] M. Ansmann *et al.*, Nature (London) **461**, 504 (2009).

[23] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland, Nature (London) **409**, 791 (2001).

[24] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and R. Blatt, Phys. Rev. Lett. **106**, 130506 (2011).

[25] J. M. Martinis, Quantum Inf. Process. **8**, 81 (2009).

[26] H. Häffner, C. F. Roosa, and R. Blatt, Phys. Rep. **469**, 155 (2008).

[27] M. Navascués, S. Pironio, and A. Acín, Phys. Rev. Lett. **98**, 010401 (2007); M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008).

[28] S. Pironio, M. Navascués, and A. Acín, SIAM J. Optim. **20**, 2157 (2010).

[29] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, Phys. Rev. A **71**, 022101 (2005).

[30] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.110.100504 for derivations of Eq. (5) and of the estimate of the CT in the experiment of Ref. [22], and a discussion of DI RG using trapped ions.

[31] B. S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).

[32] C. H. Bennett, A. W. Harrow, D. W. Leung, and J. A. Smolin, IEEE Trans. Inf. Theory **49**, 1895 (2003).

[33] A. G. Kofman and A. N. Korotkov, Phys. Rev. B **77**, 104502 (2008).

[34] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).

[35] J. Löfberg, yalmip: A Toolbox for Modeling and Optimization in MATLAB. Available at http://users.isy.liu.se/johanl/yalmip.

[36] J. F. Sturm and I. Pólik, SeDuMi: A Package for Conic Optimization. Available at http://sedumi.ie.lehigh.edu.