Effects of Reduced Measurement Independence on Bell-Based Randomness Expansion

Dax Enshan Koh,[1] Michael J. W. Hall,[2] Setiawan,[3] James E. Pope,[4] Chiara Marletto,[4] Alastair Kay,[1,5] Valerio Scarani,[1,3] and Artur Ekert[1,4]

[1]*Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543, Singapore*
[2]*Centre for Quantum Computation and Communication Technology (Australian Research Council), Centre for Quantum Dynamics, Griffith University, Brisbane, Queensland 4111, Australia*
[3]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore*
[4]*Mathematical Institute, University of Oxford, 24-29 St. Giles', OX1 3LB, United Kingdom*
[5]*Keble College, Parks Road, Oxford, OX1 3PG, United Kingdom*

(Received 22 February 2012; published 18 October 2012)

With the advent of quantum information, the violation of a Bell inequality is used to witness the absence of an eavesdropper in cryptographic scenarios such as key distribution and randomness expansion. One of the key assumptions of Bell's theorem is the existence of experimental "free will," meaning that measurement settings can be chosen at random and independently by each party. The relaxation of this assumption potentially shifts the balance of power towards an eavesdropper. We consider a no-signaling model with reduced "free will" and bound the adversary's capabilities in the task of randomness expansion.

DOI: 10.1103/PhysRevLett.109.160404 PACS numbers: 03.65.Ta, 03.65.Ud

Introduction.—A source of random data that can be trusted to be truly random, and not just repeating a predetermined, apparently random, sequence is a vital resource in a vast array of applications, not least cryptography. Within the scientific community, numerical tools such as Monte Carlo simulations find that classically generated pseudo-randomness is insufficient [1] while in a much broader community, the lack of trust in randomness generation leads, for instance, to widespread accusations of deck rigging in online gambling. Quantum mechanics has long been known to provide intrinsic randomness (see references in [2]), but it has recently been noticed that Bell tests allow us to go further: they provide quantitative bounds for the amount of randomness that is generated [3–6]. Moreover, these bounds are device-independent, in the sense that they are obtained only from the observed statistics, without reference to a description of the physical system or the implemented operations. Two different types of bound can be achieved, either by assuming the validity of quantum mechanics or merely with the weaker assumption of no-signaling in a fully black-box scenario.

In a randomness expansion protocol [3,6], a preestablished stock of randomness (for instance, a string of random bits) is used to make measurement selections in a series of Bell tests, operated by two parties (Alice and Bob) in distantly separated parts of the same laboratory. The correlation statistics of the outcomes are used to violate a Bell inequality [7], giving a quantitative bound on the degree to which an adversary or eavesdropper (Eve) is excluded. This bound can be used to measure the randomness of the outcomes, which can be added to the stock of private randomness [3]. To certify the private randomness produced, it is crucial to not only determine what we call the guessing probability G (defined below), but also to ensure that Eve cannot somehow fake this bound, perhaps by bypassing some of the assumptions used in the derivation of the bound. One of these assumptions is that Alice and Bob can randomly and independently select their measurements. While Alice and Bob could rely on making these choices with their own free will, in practice they use random number generators, which Eve could potentially manipulate to deliberately introduce patterns undetected by standard statistical tests, giving rise to the interpretation that Eve compromises the experimental free will of Alice and Bob.

We study the extent to which Eve, by influencing those measurement choices, can manipulate the degree of violation (S) of a Bell test using a no-signaling model [8,9]. Eve does her best to preprogram the outcomes of Alice's and Bob's measurements so that, for prescribed S and degree of influence upon Alice's and Bob's measurement choices, her probability of guessing the measurement outcomes correctly is maximized. The more influence she has, the less "free will" can be attributed to Alice and Bob, and if they wrongly assume that they have complete free will, they can be fooled into thinking that their observed outputs are not predetermined.

Previous discussions of the free will assumption have quantified the concept in differing ways [8–11]. The upshot is that free will seems to be a critical resource for the violation of Bell inequalities in order to derive their usual interpretation. Indeed, if free will is given up on 41% of the runs of an experiment in the Clauser-Horne-Shimony-Holt (CHSH) scenario [12], singlet state correlations can be reproduced from classical correlations [13].

An operational way of quantifying randomness involves the notion of guessing probability or predictability: a process has large randomness if it is hard to guess its outcomes. Here, we establish bounds on the average probability of guessing an outcome of a Bell test, for a given amount of free will, using a variant of Hall's relaxed Bell inequalities [14]. While these results require only the no-signaling restriction, for comparison we also establish bounds on a quantum-limited Eve who eavesdrops each run independently.

Model.—We work in the simplest scenario of two parties, each with two inputs and two outputs, for which the CHSH inequality [12] is the unique Bell test. The devices that Alice and Bob use are treated as black boxes, potentially prepared by Eve. The inputs are labelled A_j and B_k respectively, where $j, k \in \{0, 1\}$, and the outputs are labelled $a, b \in \{0, 1\}$. The CHSH test is repeated a large number of times, yielding a probability distribution of the outputs $\{\tilde{p}(a, b|A_j, B_k)\}$, which we assume to be no-signaling. In terms of these probabilities, the CHSH correlation function S can be defined as

$$S = \left| \sum_{a,b,j,k \in \{0,1\}} (-1)^{a+b+jk} \tilde{p}(a, b|A_j, B_k) \right|. \quad (1)$$

By imposing that the probability of each input is equally likely, $p(A_j, B_k) = \frac{1}{4}$ for all $j, k \in \{0, 1\}$, Alice and Bob, with no knowledge of the underlying strategy, are not able to detect any deviations of these probabilities from the uniform distribution $(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4})$ that they expect. Eve's control over the inputs and outputs is described by an underlying variable λ, corresponding to conditional probability densities $\tilde{p}(a, b|A_j, B_k, \lambda)$ and $\rho(\lambda|A_j, B_k)$. These are related by Bayes' theorem: $\tilde{p}(a, b|A_j, B_k) = \int d\lambda \tilde{p}(a, b|A_j, B_k, \lambda)\rho(\lambda|A_j, B_k)$. The summation over b and a, respectively, produce the marginals $\tilde{p}^{(A)}(a|A_j, \lambda)$ and $\tilde{p}^{(B)}(b|B_k, \lambda)$. No-signaling imposes that the marginal probabilities $\tilde{p}^{(A)}$ and $\tilde{p}^{(B)}$ are independent of B_k and A_j, respectively.

Guessing probability.—The guessing probability, or predictability, $G(\lambda)$ for a given underlying variable λ is the maximum over all these marginal probabilities

$$G(\lambda) = \max_{a,A_j,b,B_k} [\tilde{p}^{(A)}(a|A_j, \lambda), \tilde{p}^{(B)}(b|B_k, \lambda)],$$

i.e., it upper bounds the probability of Eve, who knows λ, guessing one of Alice's or Bob's outcomes. For Alice, Bob or any observer without access to the underlying variables, the guessing probability is the weighted average of $G(\lambda)$ over λ, i.e.,

$$G = \int d\lambda \rho(\lambda) G(\lambda), \quad (2)$$

where $\rho(\lambda)$ is the probability distribution of the variable λ. When $G = \frac{1}{2}$ $(G = 1)$ the underlying model is completely indeterministic (deterministic).

For a given Bell violation, tight bounds for G have been calculated in the literature [15] for the case of complete free will. In order to formulate the relaxation of free will, we define a free will parameter, P, as the maximum probability that a particular pair of measurement settings is chosen, maximized over all control variables λ, i.e.,

$$P = \max_{j,k,\lambda} p(A_j, B_k|\lambda). \quad (3)$$

This quantifies the maximum deviation of $p(A_j, B_k|\lambda)$ from the uniform distribution, i.e., the extent of Eve's influence over the supposedly free choice. For a two-party, two-setting protocol, P takes values in the interval $[\frac{1}{4}, 1]$; $P = \frac{1}{4}$ corresponds to the case of complete free will, while $P = 1$ corresponds to a deterministic selection specified by Eve. This definition relates directly to the probability that a pair of inputs is chosen for a given underlying variable. While being more natural for our model, this differs from that given in Ref. [8], which involves conditional probability distributions of the underlying variable given the measurement inputs. Nevertheless, a correspondence between the two can be found via Bayes's theorem. From these definitions, we obtain the following theorem (proved in Ref. [16]):

Theorem 1: The maximum possible CHSH expectation value $S^{\max}(G, P)$, for a guessing probability G and free will parameter P, for any no-signaling model with $p(A_j, B_k) = \frac{1}{4}$ (i.e., all inputs are equally likely), is

$$S^{\max}(G, P) = \begin{cases} 4–8(2G - 1)(1 - 3P) & P \leq \frac{1}{3}, \\ 4 & P \geq \frac{1}{3}. \end{cases} \quad (4)$$

We illustrate this result with three limiting cases. If Eve knows exactly, for each instance of the measurement, what will be measured, then Alice and Bob have no "free will" $(P = 1)$; their measurement settings are predetermined. Eve can then preprogram the outcomes of the measurements in such a way that the outcomes are completely predictable $(G = 1)$, while allowing Alice and Bob to attain any value of S up to its maximum value of 4. On the other hand, if Eve has no prior knowledge of what will be measured $(P = \frac{1}{4})$, Alice's and Bob's actions are not predetermined and hence, we say that they have complete experimental free will. Any attempts to preprogram the outcomes of the measurements with complete predictability $(G = 1)$ will result in values $S \leq 2$, familiar from the standard CHSH inequality. Finally, if Eve gives up any intention of extracting information $(G = \frac{1}{2})$, then Alice and Bob could share an arbitrary no-signaling distribution, which will allow any $S \leq 4$.

From Theorem 1: Eve's knowledge of Alice's and Bob's bits, as quantified by G, can be estimated given an observed CHSH correlation S as the free will parameter P. The

bound in the theorem is tight, i.e., for any G and P, there exists a no-signaling model for which the CHSH correlation is equal to $S^{\max}(G, P)$ (see Ref. [16] for explicit constructions). In particular, suppose that Alice and Bob measure a CHSH correlation S. If $S \leq S^{\max}(1, P)$, then Alice and Bob know that the bits could have been completely preprogrammed before the Bell measurements were carried out. On the other hand, if $S > S^{\max}(1, P)$ (anywhere above the $G = 1$ (NS) line in Fig. 1), then Alice and Bob can conclude that some indeterminism has been introduced into the model, and that the guessing probability is less than unity. They can then use Eq. (4) to determine an upper bound for the guessing probability G. For the case $P \geq \frac{1}{3}$, we have $S^{\max}(1, P) = 4$, which implies that $G = 1$; i.e., Eve can use a deterministic protocol to achieve maximal Bell violation. The case where $P < \frac{1}{3}$ is more interesting because only in this case is the upper bound on the maximum guessing probability for a given CHSH correlation S nontrivial:

$$G \leq \min\left\{\frac{1}{2}\left(1 + \frac{4 - S}{4 - S^{\max}(1, P)}\right), 1\right\}, \qquad P < \frac{1}{3}. \quad (5)$$

The observed values for S and G thus give a tight upper bound on the guessing probability (Fig. 2), from which the tradeoff between the degree of free will and Bell violation can be seen.

Since our motivation is the task of randomness expansion, we need to evaluate the amount of true randomness that we can produce via postprocessing. The degree to which this can be achieved is characterized by the min-entropy, which is used by a classical randomness extraction procedure in order to guarantee total privacy of a (shorter) random output string. For a single run, the min-entropy is defined to be $H_\infty(AB|XY) = -\log_2 \max_{a,b,x,y} \tilde{p}(a, b|x, y)$ [17], which is clearly bounded from below by $-\log_2 G$. For experimental estimation of a Bell violation, a Bell test must be performed on the devices many times in succession, requiring a bound for the min-entropy over a series of n runs. Assuming that Eve can only perform a collective attack without memory, i.e., that the devices behave independently and identically in each run, then $\tilde{p}(r|s) = \tilde{p}(a^n b^n|x^n y^n) = \prod_i \tilde{p}(a_i b_i|x_i y_i)$ by independence and so $H_\infty(R|S) \geq -n \log_2 G$ [3].

Existing privacy amplification methods rely on the use of a perfectly random seed to, for instance, select uniformly from a family of hashing functions. Such perfect randomness may not be available in the present scenario of reduced free will. Assuming (as we have throughout this Letter) only memoryless collective attacks by Eve, we can outline an effective privacy amplification strategy, and, in the instance where Eve is more sophisticated, refer the reader to [10]. Suppose that Alice and Bob have succeeded in generating a string of bits x_k, and have obtained a bound on Eve's maximum probability for guessing any one of Alice's bits, G. If Alice takes N such bits and XORS them, the resulting output bit can be guessed by Eve only if she has incorrectly guessed an even number of the outcomes of the individual measurements, which occurs with probability $[1 + (2G - 1)^N]/2$. Evidently, as N becomes large, this tends to $1/2$. By setting an allowable threshold ϵ and choosing $N = \log(\epsilon)/\log(2G - 1)$, Alice and Bob can pick their desired bound on security of the generated bit as a compromise on the number of raw key bits required to calculate it.

Restricted adversary.—Theorem 1 did not impose any restrictions on the probability distribution $p(A_j, B_k|\lambda)$.

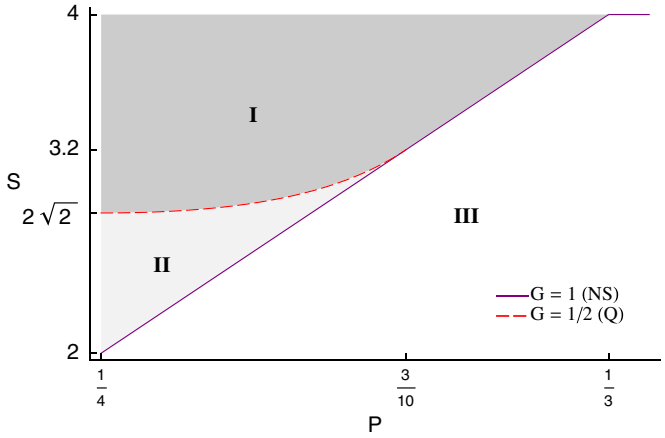

FIG. 1 (color online). The maximal CHSH expectation value $S^{\max}(G, P)$ plotted against the free will parameter P, for the no-signaling (NS) $G = 1$ model (solid line), and the quantum (Q) $G = \frac{1}{2}$ model (dashed line). Region III (unshaded) can be explained by a deterministic $G = 1$ model. In regions I (darker gray) and II (lighter gray), the results cannot be deterministic; Eve cannot know the outputs with certainty. Regions II and III together give the set of (S, P) values that may be attained by a quantum model.

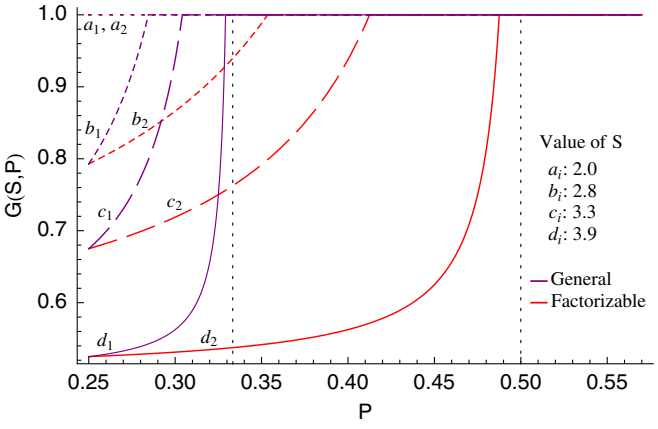

FIG. 2 (color online). Optimal guessing probability $G(S, P)$ for no-signaling models at different CHSH expectation values, including $S = 2$ (local deterministic) and $S = 2\sqrt{2}$ (Tsirelson bound). In the cases of general and factorizable distributions, the optimal guessing probabilities approach the vertical dotted lines as S goes to 4.

Although a nonfactorizable distribution can always be made factorizable by utilizing more hidden variables, this changes the value of P. Therefore, for a fixed value of P, Eve requires access to quantum technology in order to generate the most general of such distributions, e.g., random number generators which share the entangled state $|\phi_\lambda\rangle = \sum_{j,k} \sqrt{p(A_j, B_k|\lambda)}\,|j\rangle \otimes |k\rangle$. In its absence, one should impose that the probability distributions are factorizable, i.e., $p(A_j, B_k|\lambda) = p^{(A)}(A_j|\lambda)p^{(B)}(B_k|\lambda)$. The results of Theorem 1 hold in the case of an arbitrary probability distribution. Imposing this factorizability condition changes the upper bound for the Bell violation. In this case, as shown in Ref. [16],

$$S^{\max}_{\text{fac}}(G, P) = \begin{cases} 4 - 4(2G-1)(1-2P) & P \le \frac{1}{2} \\ 4 & P \ge \frac{1}{2} \end{cases}, \quad (6)$$

reducing Eve's influence compared to Eq. (4). The upper bound on the guessing probability G for an observed CHSH expectation value S is analogous to Eq. (5), upon replacing $S^{\max}$ with $S^{\max}_{\text{fac}}$ and the validity range by $P < \frac{1}{2}$. Also, note that for $P = \frac{1}{4}$, corresponding to the case of complete free will, the bounds on G for both the general and factorizable cases, reduce to the result in [3]: $G \le \frac{3}{2} - \frac{S}{4}$.

Quantum limit.—The previously derived bounds apply under the weak assumption of no-signaling, which means that Eve might be able to supply Alice and Bob with any no-signaling distribution, such as a PR box [18–20], giving the maximal violation of the CHSH inequality. However, assuming the validity of quantum mechanics, Eve can achieve only much lower limits; in the case of $P = \frac{1}{4}$, she can do no better than $S = 2\sqrt{2 - (2G-1)^2}$ [3]. In the case of $P > \frac{1}{4}$, Alice and Bob perform a CHSH test and calculate their expectation value averaged over all runs of the experiment, as before. Eve uses a hidden variable model to determine the probabilities $p(A_j, B_k|\lambda)$ that, on a given run, Alice and Bob use to select their measurement settings. As far as Eve is concerned, she just has to optimize her quantum strategy for each of the different values of λ independently, and the corresponding probabilities $p(A_j, B_k|\lambda)$. For a given λ, Alice and Bob (unbeknownst to them) are effectively playing a CHSH subgame, with the correlation function

$$S(\lambda) = 4\left|\sum_{a,b,j,k} (-1)^{a+b+jk}\tilde{p}(a, b|A_j, B_k)p(A_j, B_k|\lambda)\right|. \quad (7)$$

In Ref. [16], we derive the generalized Tsirelson bound for this class of games, and find the optimal distribution of probabilities to maximize $S(\lambda)$ for a given P. We also prove that for $P < \frac{3}{10}$, this maximum necessarily corresponds to the case $G = \frac{1}{2}$. This implies that, for the optimal quantum strategy (meaning largest achievable CHSH expectation value), we have for $P < \frac{3}{10}$,

$$S^{\max}_{Q}\left(\frac{1}{2}, P\right) = \frac{4(1-2P)^{3/2}}{\sqrt{(1-3P)}}. \quad (8)$$

For $P \ge \frac{3}{10}$, a deterministic strategy is used, and hence, $S^{\max}_{Q}(1, P) = S^{\max}(1, P)$.

This considerably restricts the region of operation for Eve, as can be seen in Fig. 1. Interestingly, for $P \ge \frac{3}{10}$, there is no quantum strategy that outperforms the deterministic strategy. This means that if Alice and Bob estimate that $P \ge \frac{3}{10}$, a randomness expansion protocol based on the CHSH inequality cannot function. We have not succeeded in finding a closed form for the general $S^{\max}(G, P)$ tradeoff in the quantum strategy, except for recovering known limits such as $P = \frac{1}{4}$ [3] and $G = 1$ [Eq. (4)], although it can be solved numerically.

Conclusions.—We have shown that by influencing the apparently free choice of measurement settings in a Bell test, the adversary can fool the participants into thinking they share quantum correlations when, in fact, they do not and are being manipulated. We have specified the optimal models for Eve to maximize the guessing probabilities based on only no-signaling models, thereby specifying, for a given Bell correlation, a bound on the extent of private randomness that can be extracted. This universal bound requires only that Eve is limited to the use of no-signaling devices (including PR boxes, etc.). We have also obtained stronger results when Eve is further assumed to be limited to quantum devices.

In order to bound the exclusion of an eavesdropper, a prior about the degree of manipulation is required. How Alice and Bob might assess this value remains an open challenge. We have also restricted Eve to performing collective attacks. Whilst this is made possible by ensuring that each run of the protocol is performed on causally disconnected devices, this approach eschews practicality. Attempts to bypass the restriction to collective attacks [10,15,21] merit further investigation.

A natural extension of this work is to ask whether the local strategies employed here could be used to take advantage of a key distribution scheme, where Eve fakes a Bell violation to undermine the security that Alice and Bob believe is in their key. There are a number of subtleties that necessitate a more detailed study.

This work is supported by the National Research Foundation and the Ministry of Education, Singapore. D. E. K. is supported by Exploratory Initatives R-710-000-016-271. M. J. W. H. is supported by the ARC Centre of Excellence CE110001027. J. E. P. acknowledges support from an EPSRC postgraduate studentship. C. M. is supported by EPSRC and the Istituto Superiore Mario Boella.

[1] P. D. Coddington, Northeast Parallel Architecture Center, Paper 14 (1994)
[2] C. S. Calude and K. Svozil, Adv. Sci. Lett. **1**, 165 (2008).
[3] S. Pironio *et al.*, Nature (London) **464**, 1021 (2010).
[4] E. Hänggi, R. Renner, and S. Wolf, in *Advances in Cryptology EUROCRYPT 2010*, edited by H. Gilbert (Springer, Berlin, Heidelberg, 2010), p. 216.
[5] R. Colbeck and A. Kent, J. Phys. A **44**, 095305 (2011).
[6] R. Colbeck, Ph.D. thesis, University of Cambridge, 2007.
[7] J. S. Bell, Physics **1**, 195 (1964).
[8] M. J. W. Hall, Phys. Rev. Lett. **105**, 250404 (2010).
[9] J. Barrett and N. Gisin, Phys. Rev. Lett. **106**, 100406 (2011).
[10] R. Colbeck and R. Renner, Nature Phys. **8**, 450 (2012).
[11] J. Kofler, T. Paterek, and C. Brukner, Phys. Rev. A **73**, 022104 (2006).
[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[13] Indeed, in Ref. [8], the optimal way of tampering with ''free will'' in the CHSH scenario leads to choosing three pairs of settings with equal probability P and the last pair with probability $1 - 3P$; when $P = \frac{2+\sqrt{2}}{12}$, singlet statistics are recovered. This can be reinterpreted as a convex combination: in a fraction f of cases, Alice and Bob have full free will, so each pair of settings is chosen with probability $\frac{1}{4}$; in the remaining $1 - f$ cases, a device is used, such that the last pair of settings is never chosen. By identification, free will must be given up in a fraction of runs $1 - f = \sqrt{2} - 1 \approx 41\%$.
[14] M. J. W. Hall, Phys. Rev. A **84**, 022102 (2011).
[15] L. Masanes, S. Pironio, and A. Acín, Nature Commun. **2**, 238 (2011).
[16] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.109.160404 for the proof of Bell violation bounds and optimal models, as well as optimal quantum strategies.
[17] R. Koenig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).
[18] B. S. Tsirelson, Lett. Math. Phys. **4**, 93 (1980).
[19] P. Rastall, Found. Phys. **15**, 963 (1985);
[20] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379 (1994).
[21] E. Hänggi, R. Renner, arXiv:1009.1833v2.