Randomness requirement on the Clauser-Horne-Shimony-Holt Bell test in the multiple-run scenario

Xiao Yuan, Zhu Cao, and Xiongfeng Ma

Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China

(Received 4 December 2014; published 16 March 2015)

The Clauser-Horne-Shimony-Holt inequality test is widely used as a means of invalidating the local deterministic theories and a tool of device-independent quantum cryptographic tasks. There exists a randomness (free will) loophole in the test, which is widely believed impossible to be closed perfectly, that is, certain random inputs are required for the test. Following a randomness quantification method used in literature, we investigate the randomness required in the test under various assumptions. By comparing the results, we conclude that, in order to make the test result reliable, it is more important to rule out the correlation between multiple runs than the correlation between two parties.

DOI: 10.1103/PhysRevA.91.032111 PACS number(s): 03.65.Ud, 03.67.Bg, 03.67.Mn

I. INTRODUCTION

Historically, Bell tests [1] are proposed for distinguishing quantum theory from local hidden variable models (LHVMs) [2]. In a general picture, a Bell test involves multiple parties who randomly choose inputs and generate outputs with pre-shared physical resources. Based on the probability distributions of inputs and outputs, an inequality, called Bell's inequality, is defined. A Bell test is meaningful when all LHVMs satisfy the underlying Bell's inequality, while such inequality can be violated via certain quantum settings. Then, a violation of the Bell's inequality in experiment would show that LHVMs are not sufficient to describe the world, and other theories, such as the quantum mechanics, are demanded.

In this work, we focus on the bipartite scenario and investigate one of the most well-known Bell tests, the Clauser-Horne-Shimony-Holt (CHSH) inequality [3]. As shown in Fig. 1(a), two spacelike separated parties, Alice and Bob, randomly choose input bits x and y and generate output bits a and b, respectively. In general, the output bits depend on the inputs and pre-shared quantum (ρ) and classical (λ) resources. The probability distribution $p(a,b|x,y)$, obtaining outputs a and b conditioned on inputs x and y, are determined by specific strategies of Alice and Bob. By assuming that the input settings x and y are chosen fully randomly and equally likely, the CHSH inequality is defined by a linear combination of the probability distribution $p(a,b|x,y)$ according to

$$S = \sum_{a,b,x,y} (-1)^{a\oplus b+xy} p(a,b|x,y) \leqslant S_C = 2, \tag{1}$$

where the plus operation $\oplus$ is modulo 2, and S_C is the (classical) bound of Bell value S for all LHVMs. Similarly, there is an achievable bound $S_Q = 2\sqrt{2}$ for the quantum theory [4]. In this case, a violation of the classical bound S_C indicates the need for alternative theories other than LHVMs, such as quantum theory. For general no signaling (NS) theories [5], denote the corresponded upper bound as $S_{\mathrm{NS}} = 4$. It is straightforward to see that $S_{\mathrm{NS}} \geqslant S_Q \geqslant S_C$.

In practice, the technique of violating a Bell's inequality can be applied to other quantum information tasks, such as device-independent quantum key distribution [6,7] and randomness expansion [8,9]. Security proofs of these tasks are generally independent of the realization devices or correctness of quantum theory, but rely on violating a Bell's inequality. For instance, consider the devices of Alice and Bob as black boxes. In this case, assume, in the worse scenario, that an adversary Eve, instead of Alice and Bob, performs measurements as shown in Fig. 1(b). Because the two parties are spacelike separated, the probability distribution generated in this way is always within the scope of LHVMs, that is, $p(a,b|x,y) = p(a|x,\lambda)p(b|y,\lambda)$, where λ is a hidden variable that is controlled by Eve. Therefore, Eve cannot fake a violation of any Bell tests, which intuitively explains the security of the device-independent tasks.

Since the first experiment in the early 1980s [10], lots of laboratory demonstrations of the CHSH inequality have been presented. These experiment results show explicit violations of the LHVMs bound S_C, and meanwhile, suffer from a few technical and inherent loopholes, which might invalidate the conclusions. Two well-known technical obstacles are due to the locality loophole and the detection efficiency loophole, which can be closed with more delicately designed experiments and developed instruments [11–13]. In contrast to the technical loopholes, there also exists an inherent loophole that cannot be closed completely in any Bell test—the input settings may not be chosen randomly. In the worst case, the inputs can be all predetermined, which makes it possible to violate the Bell inequalities even with LHVMs. In this case, witnessing a violation of a Bell's inequality does not imply the demand for non-LHVM theories and such a Bell test cannot be used for the device-independent tasks either. On the other hand, without the quantum theory or violation of Bell's inequalities, one cannot get provable randomness. Therefore, the assumption of true input randomness is indispensable in Bell tests because one cannot prove or disprove its existence.

The case of not fully random inputs can be modeled by the scenario where the input settings are partially controlled by an adversary Eve, who wants to convince Alice and Bob a violation of Bell's inequality with classical settings. In this case, Eve is able to *simultaneously* control the input settings and measurement devices, as shown in Fig. 1(c). We model the imperfect randomness by assuming that the inputs x and y are chosen according to some probability distribution $q(x,y|\lambda)$, conditioned on Eve's local hidden variable λ which also controls the measurement devices. Now, the probability distribution $p(a,b|x,y)$ of LHVMs is defined by

$$p(a,b|x,y) = \frac{\sum_\lambda p_A(a|x,\lambda)p_B(b|y,\lambda)q(x,y|\lambda)q(\lambda)}{q(x,y)}, \tag{2}$$

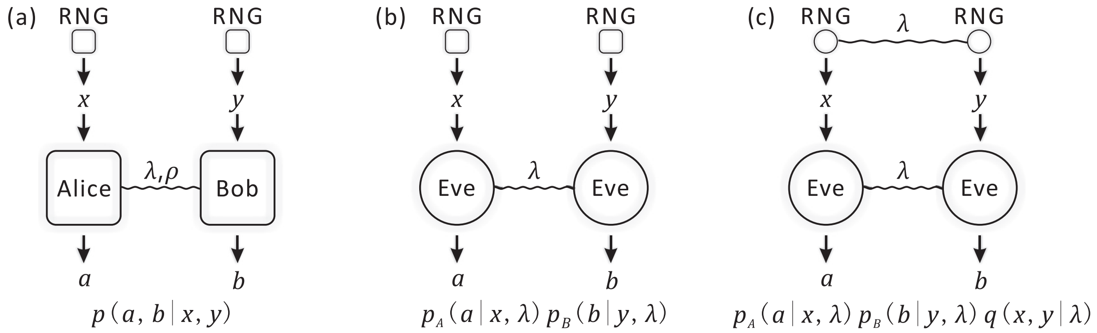

FIG. 1. Bell tests in the bipartite scenario. (a) The inputs of Alice and Bob, x and y, are decided by perfect random number generators (RNGs), which produce uniformly distributed random numbers. (b) The measurement devices are controlled by an adversary Eve through local hidden variables λ. (c) The input random numbers are also controlled by the same local hidden variable λ, which is accessible to Eve.

where $q(\lambda)$ is the prior probability distribution of λ, and $q(x,y) = \sum_\lambda q(x,y|\lambda)q(\lambda)$ is the observed average probability of the input settings x and y. Notice that $q(\lambda)$ is normalized by restricting $\sum_\lambda q(\lambda) = 1$. Now, the CHSH S value under the classical strategy given in Fig. 1(c) can be rewritten according to

$$S = 4\sum_{\lambda}\sum_{a,b,x,y}(-1)^{a\oplus b+xy}p_A(a|x,\lambda)$$
$$\times\, p_B(b|y,\lambda)q(x,y|\lambda)q(\lambda), \qquad (3)$$

where we additionally require the observed probability of choosing x and y to be uniform, that is, $q(x,y) = 1/4, \forall x,y$.

Notice that, in the extreme (deterministic) case where $q(x,y|\lambda) = 0$ or 1 for all x, y, the local hidden variable λ deterministically controls the input settings. Then Eve is able to violate Bell tests to an arbitrary value with LHVMs. On the other hand, if Eve has no control of the input settings where $q(x,y|\lambda) = 1/4$ for all x, y, she cannot fake a violation at all. Therefore, a meaningful question to ask is how one can assure that a violation of the CHSH inequality is not caused by Eve's attack on imperfect input randomness. That is, we want to know what the requirement of the input randomness is to guarantee that an observed violation truly stems from quantum effects. In the following, we first introduce the quantification of input randomness and review previous works on this question in Sec. II. Then we study a simplified case to gain the intuition behind Eve's optimal strategy in Sec. III. Finally, we investigate the randomness requirement of the CHSH test and conclude our result in Sec. IV.

II. RANDOMNESS REQUIREMENT

Let us start with quantifying the input randomness. Here, we make use of the randomness parameter P adopted in Ref. [14] to fulfill such an attempt; other tools such as the Santha-Vazirani source [15] may work similarly. The parameter P is defined to be the maximum probability of choosing the inputs conditioned on the hidden variable λ,

$$P = \max_{x,y,\lambda} q(x,y|\lambda). \qquad (4)$$

With this definition, the larger P is, the less input randomness, the more information about the inputs Eve has, and the easier for her to fake a quantum violation with LHVMs. In the CHSH test, P takes values in the regime of $[1/4,1]$. When $P = 1$, it represents the case that Eve has whole information of Alice and Bob's inputs, that is, Eve can always correctly infer the values of x and y by accessing the local hidden variable λ. When $P = 1/4$, it corresponds to the case of complete randomness, where the adversary has no additional information on the inputs compared to a naive guess. Note that the definition of P essentially follows the min entropy, which is widely used to quantify randomness of a random variable X in information theory, $H_{\min} = -\log_2[\max_x \text{prob}(X = x)]$.

Intuitively, given complete randomness where $P = 1/4$, the value S with LHVMs are bounded by S_C as shown in Eq. (1); while given the most dependent (on λ) randomness where $P = 1$, the value S with LHVMs could reach the mathematical maximum, S_{NS} in the CHSH test. Then it is interesting to check the maximal S value for $P \in (1/4,1)$ with LHVMs. In this work, we are interested in when the adversary can fake a quantum violation given certain randomness P. We thus exam the lower bound P_Q of P such that the Bell test result can reach the quantum bound S_Q with an optimal LHVM. This lower bound P_Q puts a minimal randomness requirement in a Bell test experiment. Only if the freedom of choosing inputs satisfies $P < P_Q$, can one claim that the Bell test is free of the randomness loophole.

Recently, lots of efforts have been spent on investigating such a requirement of randomness needed to guarantee the correctness of Bell tests [14,16–21]. These works analyze under different conditions. One condition is about whether the input settings of the same party are dependent or not in different runs. We call it *single run*, referring to the case that the input settings of Alice (Bob) are correlated for different runs, and *multiple run* referring to otherwise. The other condition is about whether the random inputs of Alice and Bob are correlated or not. Conditioned on these different assumptions of the input randomness, the lower bound P_Q that allows LHVMs to saturate the quantum bound S_Q in the CHSH Bell test is summarized in Table I.

In the single-run scenario, the optimal strategies for Eve reach $S = 24P - 4$ and $S = 8P$ in the case that Alice's and Bob's input settings are correlated and uncorrelated, respectively [14,16]. To achieve the maximum quantum violation $S_Q = 2\sqrt{2}$, the critical randomness requirement is shown in Table I. It is worth mentioning that if one has randomness $P \geqslant P_{\text{NS}} = 1/3$ and $P \geqslant P_{\text{NS}} = 1/2$ for the case of correlated

TABLE I. The lower bound for randomness parameter P defined in Eq. (4) that allows the CHSH value S, defined in Eq. (3), to reach the quantum bound S_Q by LHVMs in the CHSH test under different conditions.

	Correlated inputs	Uncorrelated inputs
Single run	0.285 [14,16]	0.354 [14]
Multiple run	0.258 [19]	⩽0.264 (Our work)

and uncorrelated inputs, respectively, Eve is able to recover arbitrary NS correlations.

In a more realistic scenario, the multiple-run case, the input settings of Alice (Bob) are dependent in different runs. Now, suppose the inputs may correlate for each N sequent runs, where $N = 1$ stands for the single-run case, and $N > 1$ for the multiple-run case. For each unit of N runs, denote x_j (y_j) and a_j (b_j) to be the input and output of Alice (Bob) for the jth run, where $j = 1,2,\dots,N$, respectively. In the multiple-run scenario, correlations of the inputs of each N runs can be represented by

$$q(x_1,x_2,\dots,x_N,y_1,y_2,\dots,y_N|\lambda). \tag{5}$$

Therefore, similar to the definition of Eq. (3), the S value with LHVMs in the multiple-run case can be defined by

$$S = \frac{4}{N}\sum_{j=1}^{N}\sum_{\lambda}\sum_{a_j,b_j,x_j,y_j}(-1)^{a_j\oplus b_j+x_jy_j}p_A(a_j|x_j,\lambda) \times p_B(b_j|y_j,\lambda)q(\mathbf{x},\mathbf{y}|\lambda)q(\lambda), \tag{6}$$

where the index j denotes the jth run, and $\mathbf{x} = (x_1,x_2,\dots,x_N)$, $\mathbf{y} = (y_1,y_2,\dots,y_N)$. Notice that we only consider the correlations of inputs in the unit of N runs, which is not the total number of runs in experiment. To get an accurate estimation of the S value defined in Eq. (6), one also needs to perform the N runs multiple times similar to the single-run case.

In the multiple-run scenario, as an extension of Eq. (4), the input randomness parameter is defined according to

$$P = (\max_{\mathbf{x},\mathbf{y},\lambda} q(\mathbf{x},\mathbf{y}|\lambda))^{1/N}. \tag{7}$$

It is quite straightforward that the adversary is easier to fake a violation of a Bell test with LHVMs with an increasing number of correlation N of the inputs. This is because the adversary can take advantage of additional dependence of the inputs in different runs. It has been shown that with randomness $P \geqslant P_Q \approx 0.258$, Eve is able to fake the maximum quantum violation S_Q [19] when the number of input correlation N goes to infinity. This result [19] lower bounds P_Q for all finite N, and thus puts a very strict requirement on the input randomness to guarantee a faithful CHSH test.

A remaining meaningful question is thus to consider the multiple run but uncorrelated case. As all Bell experiments must run many times to sample the probability distribution, it is reasonable and also practical to consider a joint attack by Eve. On the other hand, the uncorrelated assumption is also reasonable when the inputs of Alice and Bob are independent conditioned on λ, $q_A(x|\lambda,y) = q_A(x|\lambda)$ and $q_B(y|\lambda,x) = q_B(y|\lambda)$. Equivalently, the probability of the inputs are required to be factorizable,

$$q(x,y|\lambda) = q_A(x|\lambda)q_B(y|\lambda). \tag{8}$$

This factorizable (uncorrelated) condition constrains the power of Eve in controlling or inferring the inputs of Alice and Bob. A general distribution $q(x,y|\lambda)$ requires Eve to jointly control the instruments that Alice and Bob use to generate random inputs. In the case when the experiment instruments of Alice and Bob are manufactured independently or the inputs are determined by sources causally disconnected from each other, such as cosmic photons [22], the inputs x and y can be assumed to be independent to each other conditioned on the hidden variable λ. That is, Eve can only control each of the input settings independently according to Eq. (8).

In the multiple-run and uncorrelated scenario, the S value with LHVMs is defined by

$$S = \frac{4}{N}\sum_{j=1}^{N}\sum_{\lambda}\sum_{a_j,b_j,x_j,y_j}(-1)^{a_j\oplus b_j+x_jy_j}p_A(a_j|x_j,\lambda) \times p_B(b_j|y_j,\lambda)q_A(\mathbf{x}|\lambda)q_B(\mathbf{y}|\lambda)q(\lambda). \tag{9}$$

Our purpose is to investigate the optimal attack of the CHSH test with restricted randomness input P. Therefore we want to maximize Eq. (9) with the constraint of Eq. (7). In particular, we are interested to see when this maximal value can reach $S_Q = 2\sqrt{2}$.

III. SINGLE-RUN CASE

We first review the optimal strategy in the single-run scenario [14] to get an intuition behind the optimal attack of the adversary. Hereafter, we mainly focus on the scenario that Alice and Bob's inputs are uncorrelated as defined in Eq. (8). Thus, what we want is to maximize the S value,

$$S = \sum_{\lambda} q(\lambda)S_\lambda, \tag{10}$$

where

$$S_\lambda = 4\sum_{a,b,x,y}(-1)^{a\oplus b+xy}p_A(a|x,\lambda)p_B(b|y,\lambda)q_A(x|\lambda)q_B(y|\lambda), \tag{11}$$

with restricted randomness P, given in Eq. (4).

Since any probabilistic LHVM, that is, $p_A(a|x,\lambda)$ $p_B(b|y,\lambda)$, could be realized by a convex combination of deterministic ones [23], it is therefore sufficient to only consider deterministic LHVMs. Due to the symmetric definition of the CHSH inequality, we only need to consider a specific strategy of $p_A(0|x,\lambda) = p_B(0|y,\lambda) = 1$, and $p_A(1|x,\lambda) = p_B(1|y,\lambda) = 0$ for some given λ, and all the other ones work similarly. By substituting the special strategy into Eq. (11), we get

$$S_\lambda = 4[q_A(0)q_B(0) + q_A(0)q_B(1) + q_A(1)q_B(0) - q_A(1)q_B(1)]. \tag{12}$$

Suppose $P_A = \max_{x,\lambda}\{q_A(x|\lambda)\}$, $P_B = \max_{y,\lambda}\{q_B(x|\lambda)\}$, and hence $P = P_A P_B$, S_λ can be maximized to

$$S_\lambda \leqslant 4\,[1 - 2(1 - P_A)(1 - P_B)] = 8(P_A + P_B - P) - 4. \tag{13}$$

Given P, S_λ is upper bounded by

$$S_\lambda \leqslant 8P, \tag{14}$$

where the equality holds when $P_B = 1/2$ and $P_A = 2P$. Thus, the optimal strategy with LHVMs is $S = 8P$. Note that when the input settings are fully random, $P = 1/4$, the optimal strategy of LHVMs is $S = 2$, which recovers the original LHVMs bound S_C. It is easy to see that, to saturate the quantum bound $S_Q = 2\sqrt{2}$, the randomness should be at least $P_Q = S_Q/8 = \sqrt{2}/4 \approx 0.354$, as shown in Table I.

In the single-run case, we only need to consider one specific deterministic strategy of $p(a,b|x,y)$ due to the symmetric definition of the CHSH inequality. We also take advantage of this property in the derivation of the multiple-run case. In addition, we can see that the optimal strategy of LHVMs is to choose x or y fully randomly and the other one as biased as possible. This biased optimal strategy is counterintuitive since the adversary does not need to control the inputs of both parties, but only those of one party. We show that this counterintuitive feature does not hold in the optimal strategy in the multiple-run case.

IV. MULTIPLE-RUN CASE

Now we consider the multiple-run scenario with uncorrelated input randomness, that is, optimizing Eve's LHVM strategy Eq. (9) with constraints defined in Eq. (7). Similar to the single-run case, from the symmetric argument, we can also solely consider one specific deterministic strategy, that is, $p_A(0|x,\lambda) = p_B(0|y,\lambda) = 1$, and $p_A(1|x,\lambda) = p_B(1|y,\lambda) = 0$. Given the probabilities of Alice's and Bob's inputs, $q_A(\mathbf{x}|\lambda)$, $q_B(\mathbf{y}|\lambda)$, the S value, defined in Eq. (9), for this specific strategy labeled with λ is given by

$$S_\lambda = 4\left(1 - \frac{2}{N}\sum_{\mathbf{x},\mathbf{y}\in\{0,1\}^N}(\mathbf{x}\cdot\mathbf{y})q_A(\mathbf{x}|\lambda)q_B(\mathbf{y}|\lambda)\right), \tag{15}$$

where $\cdot$ is the vector inner product. Our attempt is therefore to maximize Eq. (15) with constraints

$$q_A(\mathbf{x}|\lambda)q_B(\mathbf{y}|\lambda) \leqslant P^N, \tag{16}$$

for all $q_A(\mathbf{x}|\lambda)$ and $q_B(\mathbf{y}|\lambda)$.

Since in the single-run scenario, the optimal strategy requires only one party with biased conditional probability, we first analyze the case with only Alice's inputs biased and Bob's inputs uniformly distributed. Then we investigate the case where the inputs of both parties are biased. We can see that the one-party-biased strategy is not optimal in the multiple-run case, even when $N = 2$.

A. One party biased

In the case when Eve only (partially) controls one of the inputs, say Alice's, the probability of Alice's input string $q_A(\mathbf{x}|\lambda)$ is biased and Bob's input string is uniformly distributed, that is,

$$q_B(\mathbf{y}|\lambda) = \frac{1}{2^N}. \tag{17}$$

The randomness is characterized by Eq. (7), after substituting Eq. (17),

$$P = \frac{P_A}{2}, \tag{18}$$

where P_A is defined by $P_A = \max_{\lambda,\mathbf{x}} q_A(\mathbf{x}|\lambda)^{1/N}$. Then, the S value, defined in Eq. (15), becomes

$$S_\lambda = 4\left(1 - \frac{1}{N2^{N-1}}\sum_{\mathbf{x},\mathbf{y}\in\{0,1\}^N}\mathbf{x}\cdot\mathbf{y}\,q_A(\mathbf{x}|\lambda)\right). \tag{19}$$

Denote the number of bit 1 in an N string $\mathbf{a}$ as $L_1(\mathbf{a})$. Given the number of bit 1 in $\mathbf{x}$, $k_A = L_1(\mathbf{x})$, we can sum over $\mathbf{y}$,

$$\sum_{\mathbf{y}\in\{0,1\}^N}\mathbf{x}\cdot\mathbf{y} = \sum_{j=1}^{k_A}2^{N-k_A}j\binom{k_A}{j} = 2^{N-1}k_A, \tag{20}$$

and group the summation of $\mathbf{x}$ according to k_A,

$$S_\lambda = 4\left(1 - \frac{1}{N}\sum_{k_A=0}^{N}\sum_{L_1(\mathbf{x})=k_A}q_A(\mathbf{x}|\lambda)k_A\right). \tag{21}$$

One only need to consider the LHVMs whose probabilities of $q_A(\mathbf{x}|\lambda)$ with the same k_A are the same. Otherwise, we can always take an average of $q_A(\mathbf{x}|\lambda)$ with the same k_A without increasing the randomness parameter P. Thus we can rewrite S_λ as

$$S_\lambda = 4\left(1 - \frac{1}{N}\sum_{k_A=0}^{N}q_{k_A}(\mathbf{x}|\lambda)\binom{N}{k_A}k_A\right), \tag{22}$$

with normalization requirement,

$$\sum_{k_A=0}^{N}q_{k_A}(\mathbf{x}|\lambda)\binom{N}{k_A} = 1, \tag{23}$$

and constraints defined in Eq. (16).

The optimization of Eq. (22) can be solved efficiently via linear programming. Intuitively, to maximize S_λ with given P defined in Eq. (18), we can simply assign $q_{k_A}(\mathbf{x}|\lambda)$ that has large k_A as 0 and small k_A as $(2P)^N$. Suppose there exists an integer l such that P can be written as

$$P = \frac{1}{2}\left[\sum_{k_A=0}^{l}\binom{N}{k_A}\right]^{-1/N}, \tag{24}$$

then, Eq. (22) can be rewritten as

$$S = 4\left[1 - \frac{1}{N}\sum_{k_A=0}^{N}\frac{1}{2}\left(\sum_{k_A=0}^{l}\binom{N}{k_A}\right)^{-1/N}\binom{N}{k_A}k_A\right]. \tag{25}$$

For a general case where an integer l cannot be found satisfying Eq. (24), we can first find an integer l such that

$$\frac{1}{2}\left[\sum_{k_A=0}^{l+1}\binom{N}{k_A}\right]^{-1/N} < P \leqslant \frac{1}{2}\left[\sum_{k_A=0}^{l}\binom{N}{k_A}\right]^{-1/N}. \tag{26}$$

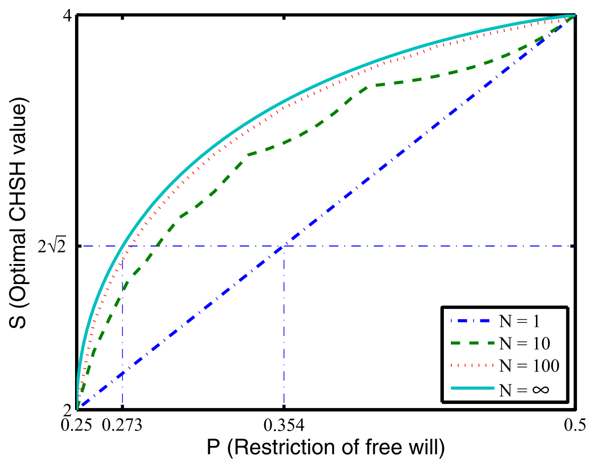

FIG. 2. (Color online) Optimal values of the CHSH test for different randomness P with various rounds N based on only Alice's inputs biased when conditioned on the hidden variable λ. The solid line is the optimal strategy for $N \to \infty$, which upper bounds all finite N rounds. Note that the curve is not smooth for finite runs N because the optimal strategy q_{k_A} defined in Eq. (27) jumps on l. With N grows larger, the curve tends to be smoother.

Then we can assign $q_{k_A}(\mathbf{x}|\lambda)$ to be

$$q_{k_A}(\mathbf{x}|\lambda) = \begin{cases} (2P)^N & k_A \leqslant l \\ \frac{\left[1-\sum_{k_A=0}^{l}(2P)^N\binom{N}{k_A}\right]^{-1/N}}{\binom{N}{l+1}} & k_A = l+1 \\ 0 & k_A > l+1 \end{cases}. \quad (27)$$

For finite N, one can numerically solve the problem according to Eq. (27). As shown in Fig. 2, the optimal strategies for $N = 1, 10, 100$ are calculated. With increasing N, the optimal value S increases and hence a valid Bell test requires a smaller P (more randomness).

In the case of $N \to \infty$, we can derive an analytic bound for all finite N strategies. By following the technique used in Ref. [19], we first estimate P defined in Eq. (26) with the limit of $N \to \infty$ by

$$\lim_{N\to\infty} P = \tfrac{1}{2}\bar{l}^{\bar{l}}(1-\bar{l})^{1-\bar{l}}, \quad (28)$$

where $\bar{l} = l/N$, and similarly S by

$$\lim_{N\to\infty} S = 4 - 4\bar{l}. \quad (29)$$

Then we can substitute Eq. (29) into Eq. (28), and get a relation between the optimized S value and the corresponding randomness parameter P,

$$P = \frac{1}{2}\left(\frac{4-S}{4}\right)^{(4-S)/4}\left(\frac{S}{4}\right)^{(S/4)}. \quad (30)$$

By substituting the quantum bound $S_Q = 2\sqrt{2}$ into Eq. (30), we can get the critical randomness requirement to be $P_Q \approx 0.273$. Note that, although Eve only controls Alice's input settings, she can still fake a quantum violation with sufficiently low randomness, which is lower than the single-run case even when Alice's and Bob's inputs are correlated. Thus we show that the randomness is more demanded for the conditions of multiple and single runs compared to the correlation between Alice and Bob.

B. Both parties biased

Now we consider a general attack, where Eve controls both inputs of Alice and Bob. In this case, we need to optimize Eq. (15) with constraints defined in Eq. (16). Similarly, we group the summation of $\mathbf{x}$ and $\mathbf{y}$ according to the corresponded number of bit 1, $k_A = L_1(\mathbf{x})$ and $k_B = L_1(\mathbf{y})$,

$$S_\lambda = 4\left(1 - \frac{2}{N}\sum_{k_A,k_B=0}^{N}\sum_{L_1(x)=k_A}\sum_{L_1(y)=k_B} q_A(\mathbf{x}|\lambda)q_B(\mathbf{y}|\lambda)\mathbf{x}\cdot\mathbf{y}\right). \quad (31)$$

Now, if we assume that $q_A(\mathbf{x}|\lambda)$ $(q_B(\mathbf{y}|\lambda))$ has the same value for equal k_A (k_B), we can sum over $\mathbf{x}$ and $\mathbf{y}$ for given k_A and k_B,

$$\begin{aligned} \sum_{k_A,k_B}\mathbf{x}\cdot\mathbf{y} &= \binom{N}{k_A}\sum_{j=\max\{1,k_A+k_B-N\}}^{\min\{k_A,k_B\}} j\binom{k_A}{j}\binom{N-k_A}{k_B-j} \\ &= \binom{N}{k_A}k_A\binom{N-1}{k_B-1} \\ &= \frac{k_Ak_B}{N}\binom{N}{k_A}\binom{N}{k_B}. \end{aligned} \quad (32)$$

We can then get the S value,

$$S_\lambda = 4\left(1 - \frac{2}{N^2}\sum_{k_A,k_B=0}^{N} q_{k_A}(\mathbf{x}|\lambda)\binom{N}{k_A}q_{k_B}(\mathbf{y}|\lambda)\binom{N}{k_B}k_Ak_B\right), \quad (33)$$

with the constraints of $q_A(\mathbf{x}|\lambda)$ and $q_B(\mathbf{y}|\lambda)$,

$$\begin{aligned} \sum_{k_A=1}^{N} q_{k_A}(\mathbf{x}|\lambda)\binom{N}{k_A} &= 1, \\ \sum_{k_B=1}^{N} q_{k_B}(\mathbf{y}|\lambda)\binom{N}{k_B} &= 1. \end{aligned} \quad (34)$$

It is worth mentioning that the assumption that $q_A(\mathbf{x}|\lambda)$ $(q_B(\mathbf{y}|\lambda))$ takes the same value for equal k_A (k_B) is not obviously equivalent to the original optimization problem defined in Eq. (31). We thus take this step as an additional assumption, and conjecture it to be true for certain cases.

The problem defined in Eq. (33) with constraints of Eq. (34) cannot be solved by linear programming directly, as for the nonlinear terms $q_{k_A}(\mathbf{x}|\lambda)q_{k_B}(\mathbf{y}|\lambda)$. However, we can still optimize it with similar methods used in the previous section. Define the maximum randomness on each side,

$$\begin{aligned} P_A &= [\max_{\lambda,\mathbf{x}} q_{k_A}(\mathbf{x}|\lambda)]^{1/N}, \\ P_B &= [\max_{\lambda,\mathbf{y}} q_{k_B}(\mathbf{y}|\lambda)]^{1/N}. \end{aligned} \quad (35)$$

To maximize S_λ, we can first optimize Alice's side q_{k_A}, and then Bob's side q_{k_B}. By doing so, it is not hard to see that S_λ is maximized by assigning q_{k_A} that has the small number of k_A as P_A and the large number of k_A as 0, and similarly for q_{k_B}.

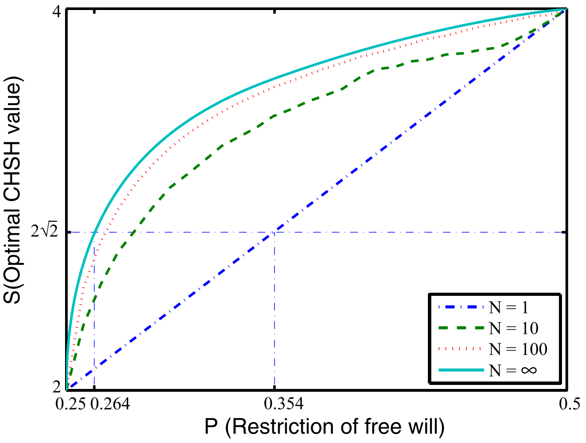

FIG. 3. (Color online) Possible optimal values of the CHSH test for different randomness P with various rounds N based on uncorrelated inputs of Alice and Bob. The solid line corresponds the strategy for $N \to \infty$, which upper bounds all finite N cases. The curves are not smooth for finite N for similar reasons like in the one-party-biased case, and it tends to be smooth with $N \to \infty$.

Thus we need to first find l_A and l_B for Alice and Bob, such that

$$\begin{aligned}\left[\sum_{k_A=0}^{l_A+1}\binom{N}{k_A}\right]^{-1/N} &< P_A \leqslant \left[\sum_{k_A=0}^{l_A}\binom{N}{k_A}\right]^{-1/N},\\ \left[\sum_{k_B=0}^{l_B+1}\binom{N}{k_B}\right]^{-1/N} &< P_B \leqslant \left[\sum_{k_B=0}^{l_B}\binom{N}{k_B}\right]^{-1/N}.\end{aligned} \tag{36}$$

Then we can assign $q_{k_A}(\mathbf{x}|\lambda)$ and $q_{k_B}(\mathbf{y}|\lambda)$ to be

$$\begin{aligned}q_{k_A}(\mathbf{x}|\lambda) &= \begin{cases}(P_A)^N & k_A \leqslant l_A\\ \frac{\left[1-\sum_{k_A=0}^{l_A} P_A^N\binom{N}{k_A}\right]^{-1/N}}{\binom{N}{l_A+1}} & k_A = l_A+1,\\ 0 & k_A > l_A+1\end{cases}\\ q_{k_B}(\mathbf{y}|\lambda) &= \begin{cases}(P_B)^N & k_B \leqslant l_B\\ \frac{\left[1-\sum_{k_B=0}^{l_B} P_B^N\binom{N}{k_B}\right]^{-1/N}}{\binom{N}{l_B+1}} & k_B = l_B+1,\\ 0 & k_B > l_B+1\end{cases}\end{aligned} \tag{37}$$

to optimize S_λ defined in Eq. (33).

For finite N, we can also numerically solve the optimization problem defined in Eq. (33) as shown in Fig. 3. The value S increases with the number of runs N, thus the strategy with infinite rounds puts a bound on the strategy with finite rounds.

In the case of $N \to \infty$, we can also find an analytical relation between optimized S and the corresponded P. Similarly, we first estimate P_A and P_B defined in Eq. (36) with the limit of $N \to \infty$ by

$$\begin{aligned}\lim_{N\to\infty} P_A &= \bar{l}_A^{\bar{l}_A}(1-\bar{l}_A)^{1-\bar{l}_A},\\ \lim_{N\to\infty} P_B &= \bar{l}_B^{\bar{l}_B}(1-\bar{l}_B)^{1-\bar{l}_B},\end{aligned} \tag{38}$$

where $\bar{l}_A = l_A/N$ and $\bar{l}_B = l_B/N$, and S according to

$$S = 4 - 8\bar{l}_A\bar{l}_B. \tag{39}$$

As we still have to optimize over all possible P_A and P_B that satisfies $P_A P_B = P$, we cannot get a direct analytic formula like in Eq. (30), while we can still numerically solve and plot it in Fig. 3. To reach a maximum quantum violation $S_Q = 2\sqrt{2}$ with a LHVM, the randomness is required to be $P \geqslant P_Q \approx 0.264$, which is larger than the case where Eve only controls Alice's input.

V. DISCUSSION

We take an additional assumption in the derivation of the both-parties-biased case, thus the obtained bound $P_Q \approx 0.264$ is still an upper bound of a general optimal attack for the case of N goes to infinity. As we already know, the randomness requirement for the worst case, that is, multiple run with Alice and Bob's inputs correlated, is strictly bounded by $P_Q \approx 0.258$ [19]. Thus, we know that the tight P_Q for the case of multiple run but Alice and Bob uncorrelated should lie in the interval of [0.258,0.264].

To gain intuition why we take the additional assumption, first notice that what we want is to minimize the average contribution of $\mathbf{x}\cdot\mathbf{y}$ in Eq. (31). In our case, where P is near 1/4, $q_A(\mathbf{x}|\lambda)$ and $q_B(\mathbf{y}|\lambda)$ can be regarded as an approximately flat distribution. On average, the $\mathbf{x}$ ($\mathbf{y}$) that contains the smaller number of 1s will contribute more to S, which means we should assign the corresponded probability $q_A(\mathbf{x}|\lambda)$ ($q_B(\mathbf{y}|\lambda)$) larger in order to maximize S. As $q_A(\mathbf{x}|\lambda)$ ($q_B(\mathbf{y}|\lambda)$) is upper bounded by P_A (P_B), an intuitive optimal strategy is then to let $q_A(\mathbf{x}|\lambda)$ ($q_B(\mathbf{y}|\lambda)$) be P_A (P_B) for the $\mathbf{x}$ ($\mathbf{y}$) that contains the smaller number of 1s, and be 0 for the ones that contain more numbers of 1s. As $q_A(\mathbf{x}|\lambda)$ ($q_B(\mathbf{y}|\lambda)$) should also satisfy the normalization condition shown in Eq. (34), we can simply follow the strategy defined in Eq. (37) to realize the intuition, which on the other hand satisfies the assumption we take. Following the above intuition, we conjecture the assumption to be true for certain cases of N. That is, for finite N, we conjecture it to be true when equalities are taken in Eq. (36) for both P_A and P_B.

On the other hand, we want to emphasize that for a finite N, the assumption will not generally hold in the optimal strategy if the equalities in Eq. (36) are not fulfilled. For example, if the probability of $l_A + 1$ and $l_B + 1$ in Eq. (37) is not 0 but very small, we should not take all $q_A(\mathbf{x}|\lambda)$ and $q_B(\mathbf{y}|\lambda)$ equally as q_{k_A} and q_{k_B}, especially for the case of $L_1(\mathbf{x}) = l_A + 1$ and $L_1(\mathbf{y}) = l_B + 1$, respectively. In fact, there does exist a cleverer assignment of $q_A(x|\lambda)$ and $q_B(y|\lambda)$. For all of $\mathbf{x}$ and $\mathbf{y}$, satisfying $L_1(\mathbf{x}) = l_A + 1$ and $L_1(\mathbf{y}) = l_B + 1$, only the $\mathbf{x}$ and $\mathbf{y}$ that give small $\mathbf{x}\cdot\mathbf{y}$ have a nonzero probability. However, with increasing runs N, this kind of clever attack stops working as the equalities can be more approximately satisfied with larger N. Therefore, we also conjecture the assumption to be true for all possible P when N goes to infinity.

As we can see, our obtained $P_Q \approx 0.264$ is already very close to the worst case value that is 0.258; we can therefore conclude that the multiple-run correlation is already a strong resource for the adversary, no matter whether the inputs of Alice and Bob are correlated or not. In addition, as we know that the bound P_Q for the most loose case, that is, single run and Alice and Bob uncorrelated, is given to be 0.354 [14]; we also suggest that the key loophole of the input randomness is the correlation between multiple runs instead of the correlation of Alice and Bob.

VI. CONCLUSION

In this work, we consider the randomness requirement of the CHSH test in the multiple-run scenario. By considering an adversary Eve who independently controls the input randomness of Alice and Bob, we investigate the minimum randomness requirement to guarantee that a violation of the CHSH inequality is not due to Eve's attack (LHVM).

Considering that Eve controls only Alice's input but leaves Bob's input uniformly distributed, we found the least randomness Eve needed to control to fake a quantum violation is $P_Q \approx 0.273$. And the least randomness required when controlling both Alice and Bob is $P_Q \leqslant 0.264$. By comparing the results to the ones listed in Table I, we conclude that the key randomness loophole is due to the correlation between multiple runs. Since the multiple-run correlation puts a high requirement on randomness which is not easy to fulfill in practice, we suggest that correlations of the input settings between different runs should be eliminated in real experiments. To guarantee the security of the device-independent tasks, we also suggest that one should check whether there are correlations between random inputs from different runs.

For further research, we are interested to know whether there exist Bell inequalities that suffer less from the randomness loophole. By assuming different kinds of assumptions, the randomness requirement behaves differently. For example, it is interesting to investigate the scenario where the input settings are uncorrelated with the measurement devices by assuming the manufacturers are different. That is, there are two uncorrelated hidden variables in Fig. 1(c), controlling the input settings and measurement devices independently. Moreover, recently, by considering a nonzero lower bound for the input random probability $p(x,y|\lambda)$, Pütz *et al.* show a Bell inequality which suffers very little from the randomness loophole [21]. That is, no adversary can fake a quantum violation as long as the lower bound of $p(x,y|\lambda)$ is nonzero regardless of its upper bound P defined in Eq. (4). Therefore, it is interesting to investigate the multiple-run randomness requirement of the CHSH inequality with additional assumptions.

ACKNOWLEDGMENTS

The authors acknowledge insightful discussions with G. Pütz, S. Yang, Q. Zhao, and Z. Zhang. This work was supported by the National Basic Research Program of China Grants No. 2011CBA00300 and No. 2011CBA00301, and the 1000 Youth Fellowship program in China.

[1] J. S. Bell, *On the Einstein-Podolsky-Rosen Paradox. Physics 1, 195–200 (1964)*, Speakable and Unspeakable in Quantum Mechanics (Cambridge University Press, Cambridge, 1987).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[4] B. S. Cirel'son, Letters in Mathematical Physics **4**, 93 (1980).

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

[6] D. Mayers and A. Yao, in *Proceedings of 39th Annual Symposium on the Foundations of Computer Science* (IEEE, Washington, DC, 1998), pp. 503–509.

[7] A. Acín, N. Gisin, and L. Masanes, Phys. Rev. Lett. **97**, 120405 (2006).

[8] R. Colbeck and R. Renner, Nature Physics **8**, 450 (2012).

[9] C. Dhara, G. de la Torre, and A. Acín, Phys. Rev. Lett. **112**, 100402 (2014).

[10] A. Aspect, P. Grangier, and G. Roger, Phys. Rev. Lett. **49**, 91 (1982).

[11] G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).

[12] B. G. Christensen, K. T. McCusker, J. B. Altepeter, B. Calkins, T. Gerrits, A. E. Lita, A. Miller, L. K. Shalm, Y. Zhang, S. W. Nam, N. Brunner, C. C. W. Lim, N. Gisin, and P. G. Kwiat, Phys. Rev. Lett. **111**, 130406 (2013).

[13] M. Giustina, A. Mech, S. Ramelow, B. Wittmann, J. Kofler, J. Beyer, A. Lita, B. Calkins, T. Gerrits, S. W. Nam *et al.*, Nature (London) **497**, 227 (2013).

[14] D. E. Koh, M. J. W. Hall, Setiawan, J. E. Pope, C. Marletto, A. Kay, V. Scarani, and A. Ekert, Phys. Rev. Lett. **109**, 160404 (2012).

[15] M. Santha and U. V. Vazirani, J. Comput. Syst. Sci. **33**, 75 (1986).

[16] M. J. W. Hall, Phys. Rev. Lett. **105**, 250404 (2010).

[17] J. Barrett and N. Gisin, Phys. Rev. Lett. **106**, 100406 (2011).

[18] M. J. W. Hall, Phys. Rev. A **84**, 022102 (2011).

[19] J. E. Pope and A. Kay, Phys. Rev. A **88**, 032110 (2013).

[20] L. P. Thinh, L. Sheridan, and V. Scarani, Phys. Rev. A **87**, 062121 (2013).

[21] G. Pütz, D. Rosset, T. J. Barnea, Y.-C. Liang, and N. Gisin, Phys. Rev. Lett. **113**, 190402 (2014).

[22] J. Gallicchio, A. S. Friedman, and D. I. Kaiser, Phys. Rev. Lett. **112**, 110405 (2014).

[23] A. Fine, Phys. Rev. Lett. **48**, 291 (1982).