Intermediate states in quantum cryptography and Bell inequalities

H. Bechmann-Pasquinucci[1] and N. Gisin[2]
[1]*UCCI.IT, via Olmo 26, I-23888 Rovagnate (LC), Italy*
[2]*Group of Applied Physics, University of Geneva, CH-1211, Geneva 4, Switzerland*
(Received 7 August 2002; published 26 June 2003)

Intermediate states are known from intercept/resend eavesdropping in the Bennett-Brassard 1984 (BB84) quantum cryptographic protocol. But they also play fundamental roles in the optimal eavesdropping strategy on the BB84 protocol and in the CHSH (Clauser-Horne-Shimony-Holt) inequality. We generalize the intermediate states to an arbitrary dimension and consider intercept/resend eavesdropping, optimal eavesdropping on the generalized BB84 protocol and present a generalized Clauser-Horne-Shimony-Holt inequality for two entangled qudits based on these states.

DOI: 10.1103/PhysRevA.67.062310 PACS number(s): 03.67.Dd, 03.65.Ud

I. INTRODUCTION

The quantum cryptographic protocol by Bennett and Brassard (1984), known as the BB84 protocol [1], was originally developed for qubits. In this protocol, the legitimate users, Alice and Bob, both use the same mutually unbiased bases A and A'. Alice uses them for state preparation[1] and Bob chooses between the two bases for his measurement. But an eavesdropper performing the simple intercept/resend eavesdropping may choose to measure in what is known as the intermediate basis or the Breidbart basis [2]. In the case of qubits, it is possible to form four intermediate states, which fall into two mutually unbiased bases. However, the eavesdropper need only use one of these bases.

It turns out that it is not only in the simple intercept/resend eavesdropping that these intermediate states appear. Also in the optimal eavesdropping strategy [3,4], which consists of the eavesdropper using the optimal cloning machine, these states enter. In this case, they appear at the point where Bob and the eavesdropper, Eve, have the same amount of information, i.e., where their information lines cross. At this point, their mixed states may be decomposed into a mixture of some of the intermediate states.

That the intermediate states also appear in the optimal eavesdropping strategy, also explains a curious observation. Namely, the amount of information obtained by the eavesdropper at the crossing point between the information lines using optimal eavesdropping, and the amount of information she obtains on performing intercept/resend eavesdropping in the intermediate basis are the same. However, the error rates are quite different.

Furthermore, intermediate states reappear in the Clauser-Horne-Shimony-Holt (CHSH) inequality [5] for two entangled qubits, where the maximal violation is obtained when on the first qubit the measurement settings correspond to the two mutually unbiased bases A and A', and on the second qubit to the two intermediate bases. Moreover, when introducing the same kind of noise as the eavesdropper does in the optimal eavesdropping strategy, the Bell violation naturally decreases. However, it is interesting to note that for the critical disturbance where the classical limit is reached, Bob and Eve have the same amount of information, i.e., this happens at the crossing point of the information lines. This crossing point between the two information lines is a very important point, since up to this limit Alice and Bob can use the fact that they have more mutual information than the eavesdropper and they can create a secure key just by using classical error correction and one-way privacy amplification. Hence, the CHSH inequality for qubits can be used as a security measure [6,7].

In the three situations just described: intercept/resend eavesdropping, optimal eavesdropping, and the CHSH inequality, the intermediate states keep reappearing and seem to play a fundamental role.

A natural question to ask is ''what happens in higher dimensions''?. This is the question we try to answer, at least partially, here. It is possible to generalize the BB84 protocol to an arbitrary dimension [8–10,3,4], simply by adding basis vectors to the two mutually unbiased bases, so that for N dimensions each basis contains N vectors. The intermediate states may also be generalized to arbitrary dimensions. However, in higher dimensions they, in general, do not form bases. But it is possible to associate with each intermediate state a projector, which represents a binary measurement.

With the use of these generalized intermediate states, we investigate intercept/resend eavesdropping, optimal eavesdropping, and a generalized CHSH inequality in an arbitrary dimension to see if they play the same roles as in two dimensions.

In this paper, we discuss the connection between some specific eavesdropping attacks in quantum cryptography and Bell inequalities in the arbitrary dimension. In Sec. II, we introduce the intermediate states for qudits (N-dimensional quantum systems). In Sec. III we discuss intercept/resend eavesdropping using the intermediate states and compare optimal eavesdropping with the intercept/resend eavesdropping strategy. Then, in Sec. IV, we present a generalized Bell inequality for two entangled qudits. In Sec. V, we consider the Bell violation as a function of the disturbance that the optimal eavesdropping strategy would lead to. The final sections of the paper are devoted to studying the inequality we have

[1]Notice that Alice may use a maximally entangled state of two qubits for preparing the state she sends to Bob, since a measurement on one qubit will ''prepare'' the state of the other qubit.

TABLE I. The intermediate states formed by the states from the two bases A and A'.

	a'_0	a'_1	$\cdots$	a'_{N-1}
a_0	m_{00}	m_{01}	$\cdot$	$m_{0,N-1}$
a_1	m_{10}	m_{11}	$\cdot$	$m_{1,N-1}$
$\vdots$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
a_{N-1}	$m_{N-1,0}$	$m_{N-1,1}$	$\cdot$	$m_{N-1,N-1}$

presented. In Sec. VI, we discuss some features of the inequality by giving examples in three dimensions. Since recently the strength of a Bell inequality has been measured in terms of its resistance to noise, we discuss this issue in Sec. VII. Section VIII is devoted to a brief study of the required detection efficiency. Finally, in Sec. IX, we have conclusion and discussion.

II. THE INTERMEDIATE STATES

The quantum cryptographic protocol BB84 can easily be generalized to the arbitrary dimension, this has already been discussed in the literature [8,10]. The protocol works in exactly the same way as it did for qubits, with the sole exception that for qudits each of the two mutually unbiased bases A and A' used by Alice and Bob contain N basis states instead of two. So Alice sends at random (and with equal probability) one of the $2N$ possible states, and Bob chooses to measure in one of the two bases A and A'.

In this section, we define the intermediate states between these two bases. The basis A is chosen as the computational basis,

$$|a_0\rangle, \ldots, |a_{N-1}\rangle, \tag{1}$$

and the second basis A' is the Fourier transform of the computational basis:

$$|a'_k\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \exp\left(\frac{2\pi i\, kn}{N}\right) |a_n\rangle. \tag{2}$$

These two bases are mutually unbiased, i.e.,

$$\langle a_n|a'_k\rangle = \frac{\exp\left(\frac{2\pi i\, kn}{N}\right)}{\sqrt{N}}. \tag{3}$$

This means that the distance between pairs of state from the two bases is $\cos(\theta)=1/\sqrt{N}$.

On having two states, it is possible to define a state that lies exactly in between the two, which means that it has the same overlap with both states and it is the state closest to the two original states that have this property. The intermediate states are obtained by forming all possible pairs of the states from the two bases. They are shown in Table I. Explicitly, the intermediate state between $|a_n\rangle$ and $|a'_k\rangle$ is defined in the following way:

$$|m_{nk}\rangle = \frac{1}{\sqrt{C}}\left[\exp\left(\frac{2\pi i\, kn}{N}\right)|a_n\rangle + |a'_k\rangle\right], \tag{4}$$

where $C=2(1+1/\sqrt{N})$ is the normalization constant and the phase comes from the overlap between $|a_n\rangle$ and $|a'_k\rangle$, see Eq. (3). The indices of the m states are such that the first index always refers to the A basis and the second to the A' basis. Since each basis contains N states it is possible to form N^2 intermediate states, simply by forming all pairs of states from the two bases.

In general, the intermediate state $|m_{\alpha\beta}\rangle$ between two arbitrary initial states $|\alpha\rangle$ and $|\beta\rangle$ is defined as

$$|m_{\alpha\beta}\rangle = \frac{\sqrt{\langle\alpha|\beta\rangle}|\alpha\rangle + \sqrt{\langle\beta|\alpha\rangle}|\beta\rangle}{\sqrt{2}\sqrt{|\langle\alpha|\beta\rangle| + |\langle\alpha|\beta\rangle|^2}}. \tag{5}$$

The intermediate states may be defined in complete generality for arbitrary initial states and any number of them. In this case, the intermediate state is found by forming the mixture of all the initial states with equal weight, the eigenstate state with the largest eigenvalue of this mixture corresponds to the intermediate state. Naturally, these definitions are equivalent and lead to the same intermediate state.

Consider that the intermediate states lead to the following conditional probabilities:

$$p(m_{nk}|a_n) = p(m_{nk}|a'_k) = \frac{1+\frac{1}{\sqrt{N}}}{2} \equiv F. \tag{6}$$

Note that this definition indeed recovers the formula for cosine of half the angle: $\cos(\theta/2)=\sqrt{[1+\cos(\theta)]/2}$. Therefore, the states have been named intermediate states, since they indeed lie in between the two original states.

The probability for making an error is

$$p(m_{nk}|a_q) = p(m_{nk}|a'_p) = \frac{1-\frac{1}{\sqrt{N}}}{2(N-1)} \equiv \frac{D}{N-1}. \tag{7}$$

It is important to notice that the intermediate states, in general, are not orthogonal, indeed we have

$$\langle m_{kl}|m_{nm}\rangle = \frac{1}{\sqrt{N}C}\left[\sqrt{N}\,\delta_{kn}\exp\left(\frac{2\pi i}{N}(mn-lk)\right) + \sqrt{N}\,\delta_{lm} + \exp\left(\frac{2\pi i}{N}(m-l)k\right) + \exp\left(\frac{2\pi i}{N}(m-l)n\right)\right]. \tag{8}$$

This means that the generalized intermediate states, in general, do not form bases, as in the two-dimensional case. But they can still be used as binary measurements, this is discussed in the following section.

A. Intermediate states as binary measurements

It has just been shown that, in general, the intermediate states $|m_{kl}\rangle$ are not orthogonal, and hence they do not form bases as in the two-dimensional case. It is, however, possible to use the corresponding projectors $|m_{kl}\rangle\langle m_{kl}|$ as binary measurements.

Since the intermediate states are nonorthogonal, it means that the corresponding binary measurements are mutually incompatible. In other words, none of them can be measured together, but they have to be measured one by one. A binary measurement has, as the name indicates, two possible outcomes, 0 and 1, where the zero outcome is *interpreted* as ''I guess the state was not $|m_{kl}\rangle$,'' and the ''1'' outcome is *interpreted* as ''I guess the state was $|m_{kl}\rangle$.'' However, the answers are statistical, in the sense that there is a certain probability for making the wrong identification.

It should be mentioned that the N^2 intermediate states constitute a generalized measurement, namely, a so-called positive operator valued measure (POVM). We have

$$\sum_{n,k=0}^{N-1} \frac{1}{N} |m_{nk}\rangle\langle m_{nk}| = \mathbb{1}. \tag{9}$$

However, we do not make use of this in what follows.

III. EAVESDROPPING

In this section, we consider two different kinds of eavesdropping strategies: intercept/resend eavesdropping and optimal eavedropping by using the optimal cloning machine. We show that the amount of information obtained by the eavesdropper at the crossing point between the information lines using optimal eavesdropping, and the amount of information she obtains on performing the much simpler intercept/resend eavesdropping in the intermediate basis are the same. The crossing point between the information lines is of fundamental importance, because it gives the maximum tolerated disturbance that allows Alice and Bob to create a secure key by using classical error correction and one-way privacy amplification.

Until now, the crossing point has been identified by considering the optimal eavesdropping strategy, which, in general, is quite a difficult problem to solve. The fact that it is possible to identify the crossing point by considering the much simpler intercept/resend eavesdropping in the intermediate basis greatly simplifies this problem. We show that this holds for any dimension, and that this is due to the fact that the intermediate states appear in both eavesdropping strategies.

A. Intercept/resend eavesdropping

Assume that the eavesdropper, Eve, performs the simple intercept/resend eavesdropping. This means that she intercepts the particle sent by Alice, performs a measurement, and according to the result prepares a particle which she then sends to Bob. She may choose to measure in the same bases as Alice and Bob, but she may also choose to use the intermediate states. In higher dimensions, where the intermediate states do not form bases, this strategy becomes a bit artificial. It is, nevertheless, interesting to consider it briefly. We will later show that there exists a connection between this simple eavesdropping attack and the optimal eavesdropping attack.

In the arbitrary dimension, where the intermediate states correspond to binary measurements, the intercept/resend strategy using these measurements may appear like this: Whenever Eve obtains a ''1,'' which means she can make a good guess of the state, she prepares a new state and sends it to Bob, whereas in the cases where she gets a ''0,'' which means she is unable to make a good guess, she does not send anything to Bob. In this way, we are only considering the cases where Eve does obtain a useful answer. This strategy, of course, gives rise to a large amount of losses and errors on Bob's side, but it is, however, interesting to evaluate the amount of information that Eve obtains in this case, i.e., considering only the measurements where she gets a positive answer.

The probability of making the correct identification is given by Eq. (6) and is equal to $\frac{1}{2}+1/(2\sqrt{N})$, whereas the probability of wrong identification, i.e., of an error, is given by Eq. (7) and is equal to $[1/(N-1)][\frac{1}{2}-1/(2\sqrt{N})]$. This means that the (Shannon) information obtained by Eve is given by [10]

$$I_{int,Eve}^{N} = \log_2(N) + \left(\frac{1}{2}+\frac{1}{2\sqrt{N}}\right)\log_2\left(\frac{1}{2}+\frac{1}{2\sqrt{N}}\right) + \left(\frac{1}{2}-\frac{1}{2\sqrt{N}}\right)\log_2\left[\frac{1}{(N-1)}\left(\frac{1}{2}-\frac{1}{2\sqrt{N}}\right)\right] \tag{10}$$

on the ''1'' outcomes of her measurements.

In the following section, we will compare this amount of information to the amount of information obtained by performing optimal eavesdropping at the point where the information lines between Bob and Eve cross.

B. The optimal cloning machine

The optimal eavesdropping strategy in any dimension is believed to be given by an asymmetric version of the quantum cloning machine [11], which clones optimally the two mutually unbiased bases [4]. Using this cloner, Eve can obtain two copies of different fidelities of the state prepared by Alice. Usually, Eve keeps the bad copy and sends the good one on to Bob. For a full description of this eavesdropping strategy and the cloning machine involved, see Ref. [4]. Here, we are only concerned with the final state that Bob receives, which means how the optimal eavesdropping strategy influences the state obtained by Bob. In the case of no eavesdropping, Bob receives the same pure state as was sent by Alice. But in the case of eavesdropping, Bob receives a mixed state.

Assume that without eavesdropping Bob would have found the state $|a_n\rangle$ if measuring in the computational basis. The question is what: ''happens to $|a_n\rangle$ as a result of eavesdropping''? Or in other words, how does the cloning ma-

chine influence the state $|a_n\rangle$? We are only interested in the final mixed states that Bob receives, and that may be written as

$$\rho_B = F_B |a_n\rangle\langle a_n| + \frac{D_B}{N-1} \sum_{j=0, j\neq n}^{N-1} |a_j\rangle\langle a_j|, \tag{11}$$

where F_B is the fidelity and $D_B = 1 - F_B$ is the total disturbance. A similar expression can be obtained for the A' basis states. As a result of eavesdropping, the amount of information that Bob gets is

$$I^N_{opt,bob} = \log_2(N) + F_B \log_2(F_B) + (1-F_B)\log_2\left(\frac{1-F_B}{N-1}\right). \tag{12}$$

The optimal eavesdropping strategy is symmetric under the exchange of Bob and Eve. This means that the mixed state ρ_E, which Eve obtains, can be written in the same form as Bob's mixed state, just with different coefficients, i.e.,

$$\rho_E = F_E |a_n\rangle\langle a_n| + \frac{D_E}{N-1} \sum_{j=0, j\neq n}^{N-1} |a_j\rangle\langle a_j| \tag{13}$$

and, equivalently, the amount of information obtained by Eve is given by

$$I^N_{opt,eve} = \log_2(N) + F_E \log_2(F_E) + (1-F_E)\log_2\left(\frac{1-F_E}{N-1}\right). \tag{14}$$

It is interesting and important to consider the point where the information lines between Bob and Eve cross. When Alice and Bob share more information than Alice and Eve, Alice and Bob can use one-way privacy amplification to obtain a secret key. Using the explicit form and coefficients of the cloning machine, it is possible to show (this was done in Ref. [4]) that the information curves cross at the point where

$$F_B = F_E = F = \frac{1}{2} + \frac{1}{2\sqrt{N}}, \tag{15}$$

$$D_B = D_E = D = \frac{1}{2} - \frac{1}{2\sqrt{N}}. \tag{16}$$

This is exactly the same fidelity (or probability of guessing correctly the state) that Eve obtained using the intercept/resend eavesdropping using the intermediate states, which means that we have just shown

$$I^N_{Int,eve} = I^N_{opt,eve}(\text{crossing point}). \tag{17}$$

This is explained by the fact that, at the crossing point of the information lines, Eve's mixed state can be decomposed into a mixture of some of the intermediate states, namely,

$$\rho_E^{cross} = \frac{1}{N} \sum_{j=0}^{N-1} |m_{nj}\rangle\langle m_{nj}|, \tag{18}$$

where again it has been assumed that $|a_n\rangle$ was the correct state. The same result holds for Bob, since at the crossing point Bob and Eve possess the same mixed state.

The mixture of the intermediate states may be interpreted as if Eve with probability $1/N$ has the state $|m_{nj}\rangle$ (there are N possible values of j). Eve, naturally, waits and performs her measurement after Alice has revealed in which basis the qudit was originally prepared. Then, she measures her qudit in the same basis, which means that she uses either the basis A or the basis A'.

This means that the situation is the following. For the optimal eavesdropping strategy, Eve possess one of the intermediate states and she measures in one of the corresponding basis A or A'; whereas in the intercept/resend eavesdropping with the intermediate states, the situation is exactly the opposite, namely, Eve has one of the basis states from A or A' and she measures the intermediate states. The two situations obviously lead to the same probabilities and hence the same amount of information.

This means that by considering the simple intercept/resend eavesdropping with intermediate state, it is possible to identify the crossing point; hence, the computation of the maximal tolerated disturbance becomes a trivial task.

IV. THE BELL INEQUALITY IN ARBITRARY DIMENSION

Recently, there has been considerable interest in generalizing various types of Bell inequalities [12–18] in higher dimensions. The Bell inequality we present here [20] makes use of the intermediate states, in a way similar to the CHSH inequality. This means that first we present the measurements and the quantum limit and only afterwards the local variable bound. So, at first we just write down a particular sum of joint probabilities and later we show that it is a Bell inequality.

In Sec. VI, we describe some of the remarkable properties that the Bell inequality, we present here, posseses, but it should be mentioned that this inequality, compared to other inequalities in higher dimensions, exhibits maximal violation for the maximally entangled state. However, we do not provide an analytic proof for this statement, but refer to numeric results that have been obtained by using polytope software [13,21]—the same kind of software which has been used to show that the other inequalities do not reach their maximal violation for the maximally entangled state.

A. The Bell inequality: The quantum-mechanical limit

Assume that Alice and Bob share many maximally entangled states of two qudits. In the computational basis, this state may be written as

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |a_i, a_i\rangle. \tag{19}$$

For each of her qudits, Alice has the choice of two measurements, namely to measure the basis A or the basis A'; whereas Bob for each of his qudits has the choice between

TABLE II. The values assigned to the basis states and the intermediate states.

Value	A	A'	M_0	M_1	$\cdots$	M_{N-1}
0	$\|a_0\rangle$	$\|a_0'\rangle$	$\|m_{00}\rangle$	$\|m_{01}\rangle$	$\cdots$	$\|m_{0,N-1}\rangle$
1	$\|a_1\rangle$	$\|a_1'\rangle$	$\|m_{11}\rangle$	$\|m_{12}\rangle$	$\cdots$	$\|m_{10}\rangle$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$N-1$	$\|a_{N-1}\rangle$	$\|a_{N-1}'\rangle$	$\|m_{N-1,N-1}\rangle$	$\|m_{N-1,0}\rangle$	$\cdots$	$\|m_{N-1,N-2}\rangle$

N^2 binary measurements, corresponding to all the intermediate states of the two bases used by Alice.

In order to write down the Bell inequality, it is convenient to assign values to the various states. In Table II, the values are shown. Notice that intermediate states have been organized into N sets so that the value of the state is always given by the first index. Moreover, this organization into the sets $M_0, \ldots, M_{N-1}$ simplifies the notation in what follows. However, it is important to remember that the states in each of the sets are not orthogonal, in other words, they do not form N orthogonal bases.

The inequality is a sum of joint probabilities. It is obtained by summing all the probabilities for when the results of the measurements are correlated and from this sum all the probabilities when the results are not correlated are subtracted, i.e.,

$$B_N = \sum p(\text{results correlated}) - \sum p(\text{results not correlated})$$

Assume that Alice measures in the A basis and Bob measures the projectors in the set M_0. For this combination of measurements, there are the following contributions to the sum B_N:

$$P(M_0 = A) = \sum_{i=0}^{N-1} p(m_{ii} \cap a_i) = \frac{1}{2} + \frac{1}{2\sqrt{N}}, \qquad (20)$$

$$P(M_0 \neq A) = \sum_{i,j=0, j\neq i}^{N-1} p(m_{ii} \cap a_j) = \frac{1}{2} - \frac{1}{2\sqrt{N}}, \qquad (21)$$

where $P(M_0 = A)$ should be read as follows: Bob measures one of the projectors in M_0 and Alice measures A, and Bob obtains the value that is correlated with Alice's result. On the other hand, $P(M_0 \neq A)$ means that Bob's result is not correlated with the result obtained by Alice. The probability $p(m_{kl} \cap a_n) = p(m_{kl}|a_n)p(a_n)$ is the joint probability for obtaining both $|a_n\rangle$ and $|m_{kl}\rangle$. The same is the case if Bob measures the projectors in any of the other sets $M_1, \ldots, M_{N-1}$ and Alice always measures in A, and again if Bob uses M_0 and Alice A'. This means that we have $P(M_i = A) = P(M_0 = A') = \frac{1}{2} + 1/(2\sqrt{N})$ and $P(M_i \neq A) = P(M_0 \neq A') = \frac{1}{2} - 1/(2\sqrt{N})$.

Now consider the case where Bob uses M_1 and Alice uses A'; in this case, Bob consistently finds a value that is $N-1$ higher than the value that correlates him with Alice. To observe this, assume, for example, that Bob has the state $|a_0'\rangle$ which is assigned the value 0; but the state in M_1, which gives the correct identification of this state, is $|m_{N-1,0}\rangle$, and this state has been assigned the value $N-1$. Similar is the case for all the other states, which leads to $P(M_1 = A' + (N-1)) = \frac{1}{2} + 1/(2\sqrt{N})$ and $P(M_1 \neq A' + (N-1)) = \frac{1}{2} - 1/(2\sqrt{N})$. Actually, whenever Alice measures A' and Bob uses any of the M_i, Bob consistently finds a value that is $N-i$ higher than the one that correlates him with Alice. This means that $P(M_i = A' + (N-i)) = \frac{1}{2} + 1/(2\sqrt{N})$ and $P(M_i \neq A' + (N-i)) = \frac{1}{2} - 1/(2\sqrt{N})$.

It is now possible to write and evaluate the sum B_N:

$$\begin{aligned} B_N &= \sum_{i=0}^{N-1} P(M_i = A) - \sum_{i=0}^{N-1} P(M_i \neq A) \\ &\quad + \sum_{i=0}^{N-1} P(M_i = A' + (N-i)) \\ &\quad - \sum_{i=0}^{N-1} P(M_i \neq A' + (N-i)) \\ &= 2N\left[\left(\frac{1}{2} + \frac{1}{2\sqrt{N}}\right) - \left(\frac{1}{2} - \frac{1}{2\sqrt{N}}\right)\right] = 2\sqrt{N}. \end{aligned} \qquad (22)$$

The quantity B_N is a sum of $2N \times N^2$ terms if written out explicitly. In the following section, we show that a local variable model that tries to attribute definite values to the observables will reach a maximum value of 2. This shows that we have obtained a Bell inequality where the quantum violation grows with the square root of N.

B. The Bell inequality: The local variable limit

On Alice's side, $a_0, \ldots, a_{N-1}$ are measured simultaneously in a single measurement as the basis A, which means that only one of them can come out true in a local variable model. The same is the case for $a_0', \ldots, a_{N-1}'$, which is measured as the basis A'. This means that, for example, if a_i is true, meaning that the measurement of A will result in the outcome a_i, then all probabilities involving a_j with $j \neq i$ must be zero. It is different on Bob's side where each m_{kl} is measured independently and hence they may all be true at the same time in a local variable model.

Assume now that according to some local variable model, a_i and a_j' are true. At the same time, in principle, all the m_{kl} could be true, too. But notice now that the only m state that will give a positive contribution to the quantity B_N is the one that identifies both a_i and a_j' correctly, i.e., m_{ij}. This will give rise to a contribution of $+2$, whereas m_{il} and m_{kj}, where only one index is correct, will only identify one of the states correctly and the other one wrong. This means that

these states, since this gives rise to one correct and one wrong identification, will result in a zero contribution; and finally the states m_{kl}, where both indices are wrong, will only give rise to errors and will hence give a negative contribution of -2 to the sum B_N. This means that

$$B_N \leqslant 2. \tag{23}$$

However, we have already shown that quantum mechanically it is possible to violate this limit. Quantum mechanically the limit is $2\sqrt{N}$. This means that we have obtained a Bell inequality where the violation increases with the square root of the dimension.

For $N=3$, the inequality has been checked in various ways numerically. First of all, it has been checked that $2\sqrt{3}$ is indeed the quantum-mechanical limit to this sum of probabilities and that this maximum is reached for the maximally entangled state. Moreover, it has been checked using ''polytope software'' [13,21] that the inequality, Eq. (23) is optimal for the measurement settings which we have presented here.

V. BELL PARAMETER AS A FUNCTION OF ρ_B

In this section, we address the question if the Bell inequality we have presented here can be used as a security measure in quantum cryptography. It is known [7] that for qubits, violation of the CHSH inequality is analytically equivalent to security in the BB84 cryptographic protocol. It, therefore, seems natural to investigate how the Bell violation decreases as a function of the disturbance introduced by the eavesdropper in the arbitrary dimension. It is not necessary to think of it in terms of quantum cryptography and eavesdropping, but simply that the quantum channel from Alice to Bob is noisy and that the noise which is introduced is identical to the noise an eavesdropper would introduce, using the optimal cloning machine.

Assume, without loss of generality, that without disturbance, Bob would have received the state $|a_0\rangle$, then we know that the mixed state that he obtains as a function of the disturbance can be written, Eq. (11), as

$$\rho_B = F_B|a_0\rangle\langle a_0| + \frac{D_B}{N-1}\sum_{i=1}^{N-1}|a_i\rangle\langle a_i|.$$

In order to compute $S(\rho_B)$, it is enough to consider the case where Bob, for example, uses the states in M_0 for his measurements, the rest of the terms in the inequality follows by symmetry.

All the states in the M_0 set are of the form $|m_{jj}\rangle$. First, computing the various probabilities $\langle m_{jj}|\rho_B|m_{jj}\rangle$, we find

$$\langle m_{jj}|\rho_B|m_{jj}\rangle = F_B\overbrace{\langle m_{jj}|a_0\rangle\langle a_0|m_{jj}\rangle}^{p(m_{jj}|a_0)} + \frac{D_B}{N-1}\sum_{i=1}^{N-1}\underbrace{\langle m_{jj}|a_i\rangle\langle a_i|m_{jj}\rangle}_{p(m_{jj}|a_i)}. \tag{24}$$

There are two different cases that have to be checked independently, namely, $j=0$ and $j\neq 0$: For $j=0$, we have

$$\langle m_{00}|\rho_B|m_{00}\rangle = F_B F + (N-1)\frac{D_B}{N-1}\frac{D}{N-1}, \tag{25}$$

and for $j\neq 0$, we have

$$\langle m_{jj}|\rho_B|m_{jj}\rangle_{j\neq 0} = F_B\frac{D}{N-1} + F\frac{D_B}{N-1} + (N-2)\frac{D_B}{N-1}\frac{D}{N-1}, \tag{26}$$

where we have used that $p(m_{00}|a_0)=F$ and $p(m_{jj}|a_0)_{j\neq 0} = D/(N-1)$ [see Eq. (6) and Eq. (7)].

In the inequality, $\langle m_{00}|\rho_B|m_{00}\rangle$ appears with a plus sign, since this is the probability of correctly identifying the state. At the same time, $\langle m_{jj}|\rho_B|m_{jj}\rangle_{j\neq 0}$ appear $N-1$ times with a minus sign in the inequality, since these correspond to all the possible errors. This means that we can define

$$\begin{aligned} s(\rho) &= \langle m_{00}|\rho_B|m_{00}\rangle - (N-1)\langle m_{jj}|\rho_B|m_{jj}\rangle_{j\neq 0} \\ &= F_B(F-D) - FD_B - \frac{N-3}{N-1}DD_B. \end{aligned} \tag{27}$$

There are $2N^2$ terms equal to $s(\rho_B)$ in the Bell inequality, since there are N^2 intermediate states and each of them appear twice (once for each of the bases A and A'). On the other hand, in each of the bases A and A' each state appears with a probability $1/N$. This means that the total Bell parameter is equal to

$$S(\rho_B) = 2Ns(\rho_B) = 2N\left(F_B(F-D) - FD_B - \frac{N-3}{N-1}DD_B\right). \tag{28}$$

It is now possible to answer a very interesting question, namely, for which disturbance is $S(\rho_B)=2$? Using the values of F, Eq. (6), and D, Eq. (7), and expressing $F_B = 1 - D_B$, one finds that $S(\rho_B)=2$ for

$$D_B^{S=2} = \frac{N^{3/2} - \sqrt{N} - N + 1}{N^{3/2} + N^2 - 2N}. \tag{29}$$

This can be compared to the disturbance D at the crossing point between the information lines. This is shown in Fig. 1. We find that it is only for $N=2$ that $D_B^{S=2} = D$, and, hence, only in two dimensions that the inequality we have presented here can be used as a security measure in quantum cryptography. However, it should be stressed that the violation of the inequality stops before the crossing point is reached. So a violation of the inequality, in any dimension, still means that Alice and Bob are within the secure zone. A similar result has recently been obtained in a slightly different situation [19].

Why the Bell inequality only works as a perfect security measure in two dimensions, is a very interesting and highly nontrivial question, and a complete answer to this problem

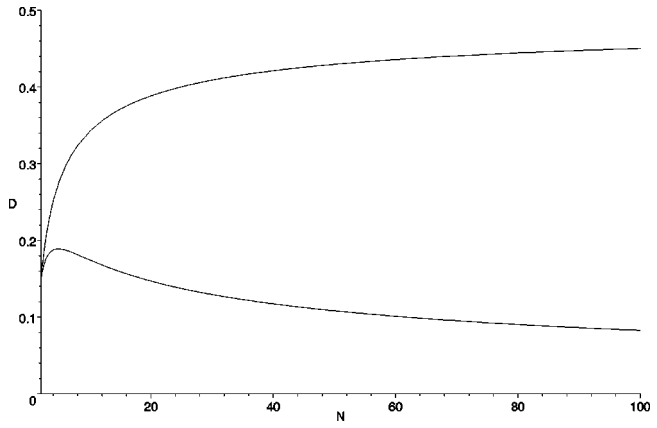

FIG. 1. This figure shows, as a function of the dimension, the disturbance at the crossing point D (upper curve), and the disturbance for which the Bell violation stops $D^{S=2}$ (lower curve).

lies beyond the scope of the present paper. However, an intuitive understanding can be found in the discussion of the clonning machine in Sec. III, especially from the last paragraph.

VI. INTERESTING FEATURES OF THE B_3 INEQUALITY

In this section, we restrict ourselves to three dimensions in order to show, in a simple way, some interesting properties of the inequality.

A. Complex versus real numbers

The first is related to the use of complex numbers. In the CHSH inequality for qubits, the maximal violation may be obtained by using real numbers only. Also, the Collins, Gisin, Linden, Massar, and Popescu (CGLMP) inequality [18] shows no difference between real and complex numbers. Here, we show that if restricted to real numbers it is not possible to obtain the maximal violation for the inequality we have presented.

Numerically, we have found the settings which lead to the largest violation when restricted to real numbers. On Alice's side, the first basis is again the computational basis A, whereas the second basis A^r (r stands for real) is found by making a $\pi/3$ rotation around the (1,1,1) axis in $\mathbb{R}^3$, and is explicitly given by

$$|a_0^r\rangle = \tfrac{1}{3}(2|a_0\rangle + 2|a_1\rangle - 1|a_0\rangle),$$

$$|a_1^r\rangle = \tfrac{1}{3}(-1|a_0\rangle + 2|a_1\rangle + 2|a_0\rangle), \tag{30}$$

$$|a_2^r\rangle = \tfrac{1}{3}(2|a_0\rangle - 1|a_1\rangle + 2|a_0\rangle).$$

The intermediate states are defined in the same way, and the three sets M_0, M_1, and M_2 again consist of nonorthogonal states. We find the following probabilities:

$$P(M_0 = A) = 5/6, \qquad P(M_0 \neq A) = 1/6;$$

$$P(M_1 = A) = 4/6, \qquad P(M_1 \neq A) = 2/6;$$

$$P(M_2 = A) = 5/6, \qquad P(M_2 \neq A) = 1/6;$$

$$P(M_0 = A^r) = 5/6, \qquad P(M_0 \neq A^r) = 1/6;$$

$$P(M_1 = A^r + 2) = 4/6, \qquad P(M_1 \neq A^r + 2) = 2/6;$$

$$P(M_2 = A^r + 1) = 5/6, \qquad P(M_2 \neq A^r + 1) = 1/6.$$

Alice and Bob are still assumed to share the maximally entangled state $|\psi\rangle$. Inserting these probabilities in the B_3 inequality leads to $B_3 = 10/3 \approx 3.333$, which is smaller than the maximal violation that is $2\sqrt{3} \approx 3.464$.

The explanation for this difference can be found in the fact that the inequality B_N has been optimized for mutually unbiased bases. In two dimensions, it is possible to have two such bases, for example, the z and the x-bases are mutually unbiased and both real. But while moving to higher dimensions this is not the case; for example, in three dimension it is not possibles to have two mutually unbiased bases and have them both real. This means that in order to reach the maximum value, for the inequality we have presented here, it is necessary to introduce complex numbers. However, the CGLMP inequality for qutrits has not been optimized for mutually unbiased bases, which explains why it does not require complex numbers.

B. Binary measurements versus basis measurements

The B_N inequality is on Bob's side optimized for the N^2 binary measurements corresponding to the intermediate states of the two bases chosen by Alice. However, it is possible to impose the additional requirement that not only must the measurements chosen by Bob maximize the probabilities, but they must also form a basis. In other words, it is possible to require that the M sets correspond to orthogonal bases M^b (b refers to the basis). We have considered this question in three dimensions.

The M^b bases that provide the optimal solution are defined in the following way. For the two mutually unbiased bases chosen by Alice, there exist unitary operators U_i such that

$$U|a_i\rangle = |a_i'\rangle, \qquad U = A' A^{-1}. \tag{31}$$

In this way, the intermediate *basis* is defined as

$$|m_{ii}^b\rangle = \sqrt{U}|a_i\rangle, \qquad M_i = \sqrt{U}A. \tag{32}$$

Since U is unitary, $\sqrt{U}$ is well defined. It is possible to construct all three bases M_0^b, M_1^b, and M_2^b in this way, choosing the unitary operator such that it transforms the states in A into any of the states in A'. This definition leads to the following probabilities:

$$P(M_0^b = A) = 7/9, \quad P(M_0^b \neq A) = 2/9;$$

$$P(M_1^b = A) = 7/9, \qquad P(M_1^b \neq A) = 2/9;$$

$$P(M_2^b = A) = 7/9, \qquad P(M_2^b \neq A) = 2/9;$$

$$P(M_0^b = A') = 7/9, \qquad P(M_0^b \neq A') = 2/9;$$

$$P(M_1^b = A'+2) = 7/9, \qquad P(M_1^b \neq A'+2) = 2/9;$$

$$P(M_2^b = A'+1) = 7/9, \qquad P(M_2^b \neq A'+1) = 2/9.$$

These probabilities may again be used in the B_3 inequality; but it is important to realize that even if the notation for the inequality is the same, the interpretation is different. Since the states in the M_i^b sets are orthogonal and M_i^b are bases, Bob no longer chooses between the nine different binary measurements but between the three basis measurements. However, it is possible to check that the local variable limit is not changed, i.e., it is still 2. Inserting the above probabilities leads to $B_3^b = 6(7/9 - 2/9) = 10/3 \approx 3.333$.

However, using basis measurements on Bob's side leads to some other interesting results. It turns out that it is possible to reduce the number of terms in the inequality. The B_3 inequality is the sum of all correct guesses, subtracting all the errors. Using the intermediate bases M_i^b, it is possible to subtract only half of the errors and, in this way, obtain a different inequality with a different local variable limit, namely, $S_{12} \leqslant 3$:

$$\begin{aligned} S_{12} = {} & P(M_0^b = A) + P(M_1^b = A) + P(M_2^b = A) + P(M_0^b = A') \\ & + P(M_1^b = A'+2) + P(M_2^b = A'+1) - P(M_0^b = A+1) \\ & - P(M_1^b = A+1) - P(M_2^b = A+1) - P(M_0^b = A'+2) \\ & - P(M_1^b = A'+1) - P(M_2^b = A') \leqslant 3. \end{aligned} \tag{33}$$

Inserting the above probabilities leads to the quantum-mechanical maximum for this inequality, namely, $S_{12} = 6(7/9 - 1/9) = 4$.

VII. RESISTANCE TO NOISE

In the recent papers on Bell inequalities, the strength of the inequality has been measured in terms of its resistance to noise [16–18]. The question is how much noise can be added to the maximally entangled state $|\psi\rangle$ and still obtain the Bell violation. The more the noise added to the system, the better it is, since this means that the inequality is robust against noise.

What is meant by noise naturally has to be specified. In the preceding section we, for example, considered the noise that is introduced by an eavesdropper when she uses the optimally eavesdropping strategy. However, the noise that was until recently used in the measure of the strength of an inequality was uncolored noise. This means that the maximally entangled state is mixed with the maximally mixed state, so that the quantum state becomes

$$\rho_{mix} = \lambda_{mix} |\psi\rangle\langle\psi| + (1 - \lambda_{mix}) \frac{\mathbb{1}}{N^2}. \tag{34}$$

This can be interpreted as if Bob with probability λ_{mix} receives the maximally entangled state, and with probability $1 - \lambda_{mix}$ he receives the maximally mixed state. For the maximally entangled state, the Bell inequality B_N Eq. (23), has maximal violation, i.e., $S = 2\sqrt{N}$; whereas for the maximally mixed state each of the probabilities in the inequality is equal to $1/N$, hence $S(\mathbb{1}/N^2) = 2(2 - N)$. This leads to

$$S(\rho_{mix}) = 2 \Leftrightarrow \lambda_{mix}^{B_N} = \frac{N-1}{N + \sqrt{N} - 2}. \tag{35}$$

For $N = 3$, this is $\lambda_{mix}^{B_3} = 2/(1 + \sqrt{3}) \simeq 0.73$. In comparison, the CGLMP inequality is more robust to this kind of noise, since they find a violation until $\lambda_{mix}^{CGLMP} \simeq 0.69$.

Recently, it has been argued that the use of uncolored noise in this measure leads to problems [22,23]. At the same time, a different kind of noise was introduced, namely, to mix the maximally entangled state with the closest separable state, i.e.,

$$\rho_{cs} = \lambda_{sep} |\psi\rangle\langle\psi| + (1 - \lambda_{sep}) \rho_{sep}, \tag{36}$$

where $\rho_{sep} = (1/N) \Sigma_{i=0}^{N-1} |a_i, a_i\rangle\langle a_i, a_i|$ [24]. Examining what happens to the Bell violation when introducing the state ρ_{sep} in B_N, Eq. (23), shows that when Alice measures in the A basis, Alice and Bob remain perfectly correlated—which means maximal violation of that part of the inequality which concerns the measurement combinations involving A. On the other hand, when Alice measures in the A' basis, Bob is left with the maximally mixed state, which means that all the joint probabilities involving the use of A' on Alice's side are equal to $1/N$. In total, this leads to

$$S(\rho_{cs}) = 2 \Leftrightarrow \lambda_{sep}^{B_N} = \frac{N - \sqrt{N}}{N + \sqrt{N} - 2}, \tag{37}$$

which for $N = 3$ is $\lambda_{sep}^{B_3} = (3 - \sqrt{3})/(1 + \sqrt{3}) \simeq 0.46$, whereas the CGLMP inequality again has $\lambda_{sep}^{CGLMP} \simeq 0.69$. This means that the inequality we have introduced here is much more robust to this kind of noise. However, it should be stressed that the same measurement settings have been used in both evaluations of λ, and that the CGLMP inequality has been optimized to be resistant to the uncolored noise.

As already mentioned, it has recently been shown [22,23] that the use of uncolored noise in the measure of resistance to noise leads to problems. Also, the results that we have obtained here further seem to support the view that resistance to noise is not a good measure of the strength of a Bell inequality, since the robustness of a Bell inequality depends on the choice of the noise added to the system.

VIII. MINIMUM DETECTION EFFICIENCY

To conclude the study of inequality (23), let us consider the minimum detection efficiency required to violate it. This question is interesting both from a fundamental point of view (the so-called detector efficiency loophole [25]) and for the practical question: How does one test a quantum device, such as a quantum cryptography system? [26,7]. For simplicity, we assume that all detectors have the same efficiency η. The problem is what to do with the cases that only one

detector fires. A natural possibility attributes the value zero to Bob whenever his detector did not fire and a random value to Alice whenever her detector did not fire. In this way, if only Alice detects a qudit, the Bell function vanishes; whereas, if only Bob detects, the Bell function is the same as for the maximally mixed state, i.e., $2(2-N)$, as in the preceding section. Thus, the inequality reads

$$\frac{\eta^2 \cdot (2\sqrt{N}) + \eta(1-\eta)[0+2(2-N)]}{\eta^2 + 2\eta(1-\eta)} \leqslant 2. \tag{38}$$

From this inequality, one finds the threshold efficiency

$$\eta_{threshold} = \frac{N}{N+\sqrt{N}-1}. \tag{39}$$

This result was discovered independently by Pironio and Roland [27]. For qubits, i.e., $N=2$, one recovers the well-known threshold, usually derived from the Clauser-Horn inequality [28]: $\eta_{threshold}^{(N=2)} \approx 82.8\%$. This threshold is minimal and slightly better for $N=4$: $\eta_{threshold}^{(N=4)} = 80\%$. For higher dimensions, the threshold increases and tends to 1.

It would be interesting to investigate the behavior of non-maximally entangled states, since Eberhard found that for qubits the threshold then decreases [29]. Let us mention that recently Massar proved that there are inequalities for which the threshold tends to zero exponentially, at least for very large dimensions [30] and, with colleagues he investigated a situation similar to the one studied in this section [31].

IX. CONCLUSION

For qubits, the intermediate states play fundamental roles in at least three different places: intercept/resend eavesdropping in the BB84 protocol for quantum cryptography, optimal eavesdropping also in the BB84 protocol and in the CHSH-inequality for two entangled qubits. The work we have presented here is the result of a study of the use of these intermediate states in the same situations but in an arbitrary dimension.

In this paper, we have first discussed the generalization of the intermediates states of two mutually unbiased bases, showing that these states are, in general, not orthogonal and hence do not form a basis as in the case for qubits. We have also discussed how they, nevertheless, can be used as binary measurements. With these measurements, we have considered the same situations as known from the qubit case.

We have considered eavesdropping in the generalized BB84 protocol (always considering only two bases). When the eavesdropper uses the optimal eavesdropping strategy, her information increases as a function of the disturbance that she introduces, and at the same time Bob's information is a decreasing function of the disturbance. For a given disturbance, their information lines cross. We have shown that the amount of information that the eavesdropper obtains at this crossing point is exactly the same amount of information which she would have obtained using the simple intercept/resend strategy using the intermediate states; however, leading to a much higher disturbance. This is explained by the fact that in any dimension, Eve's mixed state can at the crossing point be decomposed into a sum of some of the intermediate states. Hence, in the optimal eavesdropping strategy, at the crossing point, Eve has one of the intermediate states but performs her measurement in the same basis in which the state was originally prepared. Whereas, in the intercept/resend strategy, using the intermediate states as binary measurements, Eve has the state which was originally prepared by Alice, but measures one of the intermediate states. This means that the two situations are exactly opposite and, therefore, lead to the same probabilities and hence the same information. In other words, we have shown a connection between the intercept/resend eavesdropping strategy where the eavesdropper uses the intermediate states, and the optimal eavesdropping attack where the eavesdropper uses a special version of the quantum cloning machine.

The maximal settings for the CHSH inequality for qubits are two mutually unbiased bases on Alice's side and using the intermediate states on Bob's side. In the case of qubits, the four intermediate states form two bases. This means that in this case, both Alice and Bob have the choice of measuring one of the two mutually unbiased bases.

In higher dimensions, where the intermediate states do not form bases, Bob instead uses the corresponding projectors as binary measurements. This means that he chooses between N^2 mutually incompatible measurements, whereas Alice still chooses between two basis measurements. The generalized inequality, we present, has the local variable limit equal to 2 in any dimension, whereas the maximal quantum-mechanical value is $2\sqrt{N}$. In other words, we find a violation that increases with the square root of the dimension. Due to the construction, we also obtain the familiar CHSH inequality for $N=2$.

It is known that the CHSH inequality may be used as a security measure in quantum cryptography for qubits, since, in this case, a violation of the inequality is obtained until the disturbance introduced by the eavesdropper reaches the disturbance at the crossing point of the information lines between Eve and Bob. Until this point, Alice and Bob can use the fact that they share more mutual information than with Eve to obtain a secret key by means of one-way privacy amplification. We have investigated the violation of the inequality, presented here, as a function of the disturbance introduced by the eavesdropper. We found that it is only for $N=2$ that the inequality can be used as a security measure, in the sense that in higher dimensions the violation stops for a lower disturbance than the disturbance at the crossing point. This, however, does not mean that such an inequality does not exist; it only shows that the inequality which mimics the situation from two dimensions is not the one that has this property in higher dimensions.

On the other hand, the inequality we have presented here may stand as a result by itself, and as a Bell inequality in an arbitrary dimension it has many interesting properties. First of all, compared to other inequalities, which have been presented recently, this inequality gives maximal violation for maximally entangled states. Moreover, we have shown in examples in three dimensions that this inequality requires complex numbers in order to have maximal violation. Re-

striction to the use of real numbers leads to a smaller violation. In comparison, the CHSH inequality for qubits and the CGLMP inequality for qutrits show no difference between using real or complex numbers. The explanation is due to the fact that the inequality we present here is optimized for mutually unbiased bases, and in three dimensions it is not possible to have two such bases without the use of complex numbers. However, in two dimensions the x and z bases are mutually unbiased and both real, and for the CGLMP inequality the explanation is that it is not optimized for mutually unbiased bases.

We have also shown that imposing the additional constraint that the M sets actually form bases leads to new inequalities. We have explicitly given an example in three dimensions, showing the optimal solution, for two basis measurements on Alice's side and three basis measurements on Bob's side.

In recent papers on the subject [16–18], the strength of a Bell inequality has been measured in terms of its resistance to noise. Until recently, the noise was taken to be uncolored noise, which means that the maximally entangled state is mixed with the maximally mixed state. The inequality we present here is less resistant to this kind of noise than other inequalities which have been presented recently. It should however be mentioned that these inequalities have been optimized for this kind of noise. However, recently it was argued that using the uncolored noise leads to problems [22,23]. At the same time, a different kind of noise was introduced, namely, mixing the maximally entangled state with the closest separable state. When using this measure we find that the inequality we present here, is much more robust than, for example, the CGLMP inequality. The results that we have obtained here further seem to indicate that resistance to noise is not a good measure of the strength of a Bell inequality, since the robustness of a Bell inequality depends on the choice of the noise added to the system.

ACKNOWLEDGMENTS

We benefited from stimulating discussions with S. Pironio, J. Roland, and S. Massar. This work was done while H.B.-P. was at the Group of Applied Physics, University of Geneva, CH, supported by the Danish National Science Research Council (Grant No. 9601645). This work was also supported by the Swiss NCCR ''Quantum Photonics'' and by the European IST project EQUIP, sponsored by the Swiss OFES.

[1] C.H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] See, for example, C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
[3] D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[4] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[5] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[6] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[7] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[8] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[9] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[10] M. Bourennane, A. Karlsson, and G. Bjork, Phys. Rev. A **64**, 012306 (2001).
[11] N.J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000); J. Mod. Opt. **47**, 187 (2000); Acta Phys. Slov. **48**, 115 (1998).
[12] J.S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[13] D. Kaszlikowski, P. Gnacinski, M. Zukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).
[14] T. Durt, D. Kaszlikowski, and M. Zukowski, e-print quant-ph/0101084.
[15] J.-L. Chen, D. Kaszlikowski, L.C. Kwek, M. Zukowski, and C.H. Oh, e-print quant-ph/0103099.
[16] D. Kaszlikowski, P. Gnacinski, M. Zukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).
[17] D. Kaszlikowski, L.C. Kwek, J.-L. Chen, M. Zukowski, and C.H. Oh, e-print quant-ph/0106010.
[18] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, e-print quant-ph/0106024.
[19] D. Kaszlikowski, K. Chang, D.K.L. Oi, L.C. Kwek, and C.H. Oh, e-print quant-ph/0206170.
[20] H. Bechmann-Pasquinucci and N. Gisin, Quantum Inf. Comput. **3**, 157 (2003).
[21] R.M. Basoalto and I. Percival, e-print quant-ph/0012024.
[22] D. Collins and S. Popescu, J. Phys. A (to be published), e-print quant-ph/0106156.
[23] A. Acin, T. Durt, N. Gisin, and J.I. Latorre, Phys. Rev. A (to be published), e-print quant-ph/0111143.
[24] M. Plenio and V. Vedral, Phys. Rev. A **57**, 1619 (1998).
[25] P. Pearle, Phys. Rev. D **2**, 1418 (1970); J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969); E. Santos, Phys. Rev. A **46**, 3646 (1992).
[26] D. Mayers and A. Yao, in Proceedings of the 39th IEEE Conference on Foundations of Computer Science, 1998.
[27] S. Pironio and J. Roland (private communication).
[28] J.F. Clauser and M.A. Horne, Phys. Rev. D **10**, 526 (1974).
[29] Ph.H. Eberhard, Phys. Rev. A **47**, R747 (1993).
[30] S. Massar, Phys. Rev. A **65**, 032121 (2002).
[31] S. Massar, S. Pironio, J. Roland, and B. Gisin, e-print quant-ph/0205130.