# Quantum cryptography based on qutrit Bell inequalities

Dagomir Kaszlikowski,[1] D. K. L. Oi,[2] Matthias Christandl,[3] Kelken Chang,[1] Artur Ekert,[3] L. C. Kwek,[4,1] and C. H. Oh[1]

[1]*Department of Physics, Faculty of Science, National University of Singapore, Lower Kent Ridge,*
*Singapore 119260, Republic of Singapore*
[2]*Centre for Quantum Computation, Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom*
[3]*Centre for Quantum Computation, DAMTP, University of Cambridge, Wilberforce Road, Cambridge CB3 OWA, United Kingdom*
[4]*National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 639798, Republic of Singapore*

(Received 25 July 2002; published 21 January 2003)

We present a cryptographic protocol based upon entangled qutrit pairs. We analyze the scheme under a symmetric incoherent attack and plot the region for which the protocol is secure and compare this with the region of violations of certain Bell inequalities.

DOI: 10.1103/PhysRevA.67.012310 PACS number(s): 03.67.Dd

The need to communicate secretly has always been an important issue for military strategists during wartime. The one-time pad (Vernam cipher) has been shown to be an absolutely secure means of encrypting a message provided the key is truly random, is long as the message, and is never reused [1]. However, a major problem with the one-time pad is the establishment of a secure key between the two physically separated parties without the services of a courier. A recent proposal in this direction is to apply the laws of quantum mechanics to establish this crucial key [2]. One such protocol is based on entangled pairs of particles and detecting the presence of an eavesdropper using Bell inequalities [3]. This protocol (E91) is interesting as it is an example of fundamental physics, i.e., violations of local realism, being applied to a practical problem.

In this paper, we propose an extension of this protocol using three-dimensional systems, or qutrits. The extension of Bell inequalities to three dimensions is a nontrivial and interesting problem. As higher-dimensional entangled quantum systems are more resistant to noise than two-dimensional systems (qubits), it was suspected that this may lead to stronger violations of local realism which was shown numerically using linear optimization [4] and later confirmed analytically [5]. Hence, using higher-dimensional systems may lead to more robust cryptographic protocols.

The quantum channel we consider consists of a source producing two qutrits [6], $A$ and $B$, in the maximally entangled state $|\psi\rangle=(1/\sqrt{3})\Sigma_{k=0}^{2}|k\rangle_A\otimes|k\rangle_B$, where $|k\rangle_A$ and $|k\rangle_B$ are the $k$th (computational) basis state of the qutrit $A$ and $B$, respectively (these basis states can represent, for instance, spatial degrees of freedom of photons) [7]. Qutrit $A$ flies towards Alice whereas qutrit $B$ flies towards Bob. Each observer has at his disposal a symmetric unbiased six-port beam splitter. An unbiased symmetric six-port beam splitter performs a unitary transformation between "mutually unbiased" bases for qutrits [8–10]. Such devices were tested in several quantum optical experiments [11], and also analyzed theoretically [12,13]. This device has three input and three output ports (Fig. 1). In front of each input port there is a phase shifter, $\varphi_\ell$. With all phase shifters set to zero, an incoming photon through one of the input ports has equal probability of leaving through any of the output ports. The elements of the unitary transformation, which describes its action, are given by $U^{k\ell}=(1/\sqrt{3})\alpha^{k\ell}e^{i\varphi_\ell}$, where $\alpha=e^{2\pi i/3}$ and the indices $k$, $\ell$ ($k,\ell=0,1,2$) denote the input and exit ports, respectively. The phase shifters can be changed by an observer. For convenience, we will denote the values of the three phase shifts as $\vec{\varphi}=(\varphi_1,\varphi_2,\varphi_3)$. In our protocol, both observers perform three distinct unitary transformations on their qutrits. The transformations at Alice's side are defined by $\vec{\varphi}_1^A=(0,0,0)$, $\vec{\varphi}_2^A=(0,\pi/3,-\pi/3)$, $\vec{\varphi}_3^A=(\pi,0,-\pi)$, whereas Bob's transformations are $\vec{\varphi}_1^B=(0,\pi/6,-\pi/6)$, $\vec{\varphi}_2^B=(0,-\pi/6,\pi/6)$, $\vec{\varphi}_3^B=(-\pi,0,\pi)$. The observers choose their transformations randomly and independently for each pair of qutrits. After performing the pair of transformation $\vec{\varphi}_m^A,\vec{\varphi}_n^B$, the final state is $|\tilde{\psi}\rangle_{mn}=U_A(\vec{\varphi}_m^A)\otimes U_B(\vec{\varphi}_n^B)|\psi\rangle$. The observers perform a measurement of the state of their qutrit in the computational basis, $|0\rangle_\mu,|1\rangle_\mu,|2\rangle_\mu$ ($\mu=A,B$).

We adopt an uncommon but useful complex value assignment to the results of the measurements, first used in Ref. [11]: namely, for the result of the measurement of the ket $|k\rangle_x$ we ascribe the value $\alpha^k$. This assignment naturally leads to the following definition of the correlation function $Q(\vec{\varphi}_k^A,\vec{\varphi}_\ell^B)$ ($Q_{k\ell}$ for short) between the values of Alice's and Bob's results of measurements [11], $Q_{k\ell}=\Sigma_{a,b=0}^{2}\alpha^{a+b}P(a,b;\vec{\varphi}_k^A,\vec{\varphi}_\ell^B)$, where $P(a,b;\vec{\varphi}_k^A,\vec{\varphi}_\ell^B)$ denotes the probability of Alice and Bob obtaining the results $a$ and $b$, respectively, for phase shifts $(\vec{\varphi}_k^A,\vec{\varphi}_\ell^B)$. It can be shown that the correlation function reads $Q_{k\ell}=\frac{1}{3}\Sigma_{j=0}^{2}[e^{i(\varphi_j^A(k)-\varphi_{j+1}^A(k)+\varphi_j^B(\ell)-\varphi_{j+1}^B(\ell))}]$ where, for instance, $\varphi_2^A(k)$ denotes the second component of the $k$th vector of phases for Alice, and the addition in the indices (henceforth) is modulo 2.

Note that $Q_{33}=1$, which means that the results of the measurement obtained by Alice and Bob in this case are strictly correlated. When Alice obtains the results $1$, $\alpha$, or $\alpha^2$, Bob must register the results $1$, $\alpha^2$, or $\alpha$, respectively.

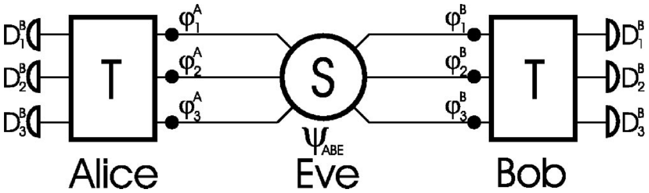

FIG. 1. Qutrit cryptographic protocol.

Thus, only the following pairs of the results are possible $\{(1,1),(\alpha,\alpha^2),(\alpha^2,\alpha)\}$ [denoted subsequently by $\{(0,0),(1,2),(2,1)\}$], and each pair of results occurs with equal probability $\frac{1}{3}$. Let us also define the following quantity:

$$S=\mathrm{Im}(-\alpha^2Q_{11}+\alpha Q_{12}+\alpha^2Q_{21}-\alpha^2Q_{22}). \tag{1}$$

It can be shown, using the recently discovered Bell inequality for two qutrits [14], that according to local realistic theory $S$ cannot exceed $\sqrt{3}$. However, when using the quantum-mechanical correlation function $(Q_{kl})$, $S$ acquires the value $\frac{2}{3}(2+\sqrt{3})$. Therefore, to satisfy the above Bell inequality in this case one must reduce the correlation function by the factor $6\sqrt{3}-9/2$ (such reduction is possible by adding the symmetric noise to the system). It has been proved [15] that the above Bell inequality gives a necessary and sufficient condition for local realism in this case.

After the transmission has taken place, Alice and Bob publicly announce the vectors of phase shifts that they have chosen for each particular measurement and divide the measurements into two separate groups: a first group for which they have used the vectors $\vec{\varphi}_1^A$, $\vec{\varphi}_2^A$ and $\vec{\varphi}_1^B$, $\vec{\varphi}_2^B$, and a second group for which they have used $\vec{\varphi}_3^A,\vec{\varphi}_3^B$. Subsequently, Alice and Bob announce in public the results of the measurements they have obtained within the first group. In this way they can compute the value of $S$. If this value is not equal to $\frac{2}{3}(2+\sqrt{3})$, it means that the qutrits have somehow been disturbed. The source of this disturbance can be either an eavesdropper or noise. For sufficiently low disturbance the results from the second group allow them, due to the mentioned correlations, to generate a ternary cryptographic key.

Let us consider a symmetric incoherent attack in which the eavesdropper (Eve) controls the source that produces the pairs of qutrits. Naturally, if Eve wants to acquire any information about the key, she must introduce some disturbance in the state of the qutrits. Her only chance of being undetected is to hide herself behind what, to Alice and Bob, may look like an environmental noise in the channel. We assume that the noise is symmetrical in the sense that the disturbed correlation function reads

$$Q_{noise}(\vec{\phi},\vec{\psi})=VQ(\vec{\phi},\vec{\psi}), \tag{2}$$

where $0\leqslant V\leqslant 1$. This can only be fulfilled if the reduced density operator for Alice and Bob (after tracing out Eve's degrees of freedom) is of the form

$$\varrho_{AB}=A|\psi\rangle\langle\psi|+B|\chi_1\rangle\langle\chi_1|+C|\chi_2\rangle\langle\chi_2|+\frac{D}{9}I\otimes I, \tag{3}$$

where the (not necessarily all positive) numbers satisfy $A+B+C+D=1$, and the maximally entangled orthogonal states $|\chi_1\rangle=(1/\sqrt{3})(|00\rangle+\alpha|11\rangle+\alpha^2|22\rangle)$ and $|\chi_2\rangle=(1/\sqrt{3})(|00\rangle+\alpha^2|11\rangle+\alpha|22\rangle)$. This choice stems from the fact that only the above states generate correlation functions that are proportional to $Q(\vec{\phi},\vec{\psi})$, specifically, the state $|\chi_1\rangle$ gives the correlation function $\alpha Q(\vec{\phi},\vec{\psi})$ whereas the state $|\chi_2\rangle$ gives the correlation function $\alpha^2Q(\vec{\phi},\vec{\psi})$. Thus, the correlation function on the state $\varrho_{AB}$ is

$$Q_{noise}(\vec{\phi},\vec{\psi})=(A+\alpha B+\alpha^2C)Q(\vec{\phi},\vec{\psi}). \tag{4}$$

From Eq. (2), we obtain the condition $A+\alpha B+\alpha^2C=V$, which is only possible if $B=C$ ($V$ is real).

Eve can prepare the reduced density operator (3) by constructing an entangled state of the form

$$\begin{aligned}|\psi_{ABE}\rangle=&\sqrt{\frac{F}{3}}(|00\rangle|E_{00}\rangle+|11\rangle|E_{11}\rangle+|22\rangle|E_{22}\rangle)\\&+\sqrt{\frac{G}{6}}(|01\rangle|E_{01}\rangle+|10\rangle|E_{10}\rangle+|20\rangle|E_{20}\rangle\\&+|02\rangle|E_{02}\rangle+|12\rangle|E_{12}\rangle+|21\rangle|E_{21}\rangle),\end{aligned} \tag{5}$$

where $\{|kl\rangle\}$ are the computational basis states of the two qutrits, and $\{|E_{kl}\rangle\}$ are states of the ancilla. Without loss of generality, we can assume that they are normalized (which implies that $F+G=1$). Note that the most general state of the joint system of Alice's and Bob's qutrits and Eve's ancilla reads $\Sigma_{kl=0}^2|kl\rangle|E_{kl}\rangle$. However, Eq. (3) imposes the following conditions on the states of the ancilla, $F\langle E_{kk}|E_{ll}\rangle=A-B$ and $\langle E_{kl}|E_{mn}\rangle=\delta_{kl}, k\neq l$. Letting $\langle E_{kk}|E_{ll}\rangle=\lambda$, we arrive at the following set of conditions, $A+2B+D=1$, $A-B=F\lambda$, and $D=\frac{3}{2}(1-F)$.

Eve's strategy is the following. She prepares the state (5), sends the qutrits to Alice and Bob, and keeps her ancilla. She then waits for public communication between Alice and Bob. When the settings of Alice's and Bob's apparatus (phase shifts) are revealed: (i) if the chosen settings are not the ones used for the key generation Eve ignores the ancilla; (ii) if the settings are the ones for which the key is generated, i.e., $\vec{\varphi}_3^A,\vec{\varphi}_3^B$, Eve attempts to identify the ancilla state.

By straightforward computation, the final state in the second case is

$$|\tilde{\psi}_{ABE}\rangle=U_A(\vec{\varphi}_3^A)\otimes U_B(\vec{\varphi}_3^B)\otimes I|\psi_{ABE}\rangle=\sum_{a,b=0}^{2}|ab\rangle|\tilde{E}_{ab}\rangle, \tag{6}$$

where the unnormalized states $|\tilde{E}_{ab}\rangle$ are

$$\begin{aligned}|\tilde{E}_{ab}\rangle=\frac{1}{3}\Bigg(&\sqrt{\frac{F}{3}}\sum_{k=0}^{2}\alpha^{(a+b)k}e^{i(\varphi_k^A(3)+\varphi_k^B(3))}|E_{kk}\rangle\\&\times\sqrt{\frac{G}{6}}\sum_{m\neq n}\alpha^{am+bn}e^{i(\varphi_m^A(3)+\varphi_n^B(3))}|E_{mn}\rangle\Bigg).\end{aligned} \tag{7}$$

Note that $|\tilde{\psi}_{ABE}\rangle$ can also be written more conveniently as

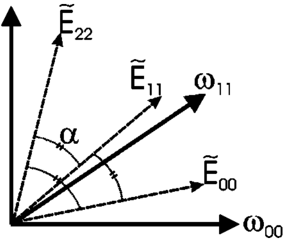

FIG. 2. The optimal three-state discrimination procedure for states in the first subspace. The angle between each of the states is $\alpha = \arccos \tilde{\lambda}_1$.

$$|\tilde{\psi}_{ABE}\rangle = \sum_{i=0}^{2} (|i,i\rangle|\tilde{E}_{i,i}\rangle + |i+1,i+2\rangle|\tilde{E}_{i+1,i+2}\rangle + |i+2,i+1\rangle|\tilde{E}_{i+2,i+1}\rangle), \tag{8}$$

where we have grouped the terms into three orthogonal subspaces associated with Alice and Bob generating the correct key $\{(0,0),(1,2),(2,1)\}$, and the two incorrect keys, $\{(1,1),(2,0),(0,2)\}$ or $\{(2,2),(1,0),(0,1)\}$. Note also that the ancilla states of one subspace are orthogonal to the ancilla states of the other subspaces. The probabilities that Eve projects into the subspaces spanned by the states $\{|\tilde{E}_{00}\rangle,|\tilde{E}_{12}\rangle,|\tilde{E}_{21}\rangle\}$, $\{|E_{11}\rangle,|E_{20}\rangle,|E_{02}\rangle\}$ and $\{|E_{22}\rangle,|E_{10}\rangle,|E_{01}\rangle\}$ are $P_0 = 3\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle = (1+2F\lambda)/3$, $P_1 = 3\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle = (1-F\lambda)/3$ and $P_2 = 3\langle\tilde{E}_{22}|\tilde{E}_{22}\rangle = (1-F\lambda)/3$, respectively. We have considered the fact that the states within each bracket in Eq. (8) have the same norms with the same mutual scalar products. Moreover, these scalar products are all real.

Eve now has to determine the state of her ancilla, given that Alice and Bob have projected the whole state into one of the three subspaces associated with the three cases. These subspaces are orthogonal so that Eve can, in principle, determine without error, which of these cases Alice and Bob have.

The three ancilla vectors in each subspace corresponding to the result obtained by Alice and Bob are symmetric and equiprobable. This makes Eve's task of discrimination easier as this case has an analytic optimal solution [16] using the so-called "square-root measurement." We define the operator $\Phi = \Sigma_{ab}|\tilde{E}_{ab}\rangle\langle\tilde{E}_{ab}|$, where $\{|\tilde{E}_{ab}\rangle\}$ are the ancilla states spanning the subspace associated with Alice and Bob's measurement outcomes. Since we are discriminating three vectors in a three-dimensional space, the optimum measurement directions, $|\omega_{ab}\rangle = \Phi^{-1/2}|\tilde{E}_{ab}\rangle$, are orthogonal, hence, Eve simply performs a projective measurement on her ancilla (Fig. 2). Thus, Eve's error rate is given by

$$\mathcal{E}_{\text{Eve}} = \sum_{i=0}^{3} P_i(1-W_i), \tag{9}$$

where $W_i = (\frac{1}{3}\sqrt{1+2\tilde{\lambda}_i} + \frac{2}{3}\sqrt{1-\tilde{\lambda}_i})^2$ is the probability of correctly identifying the three states of the ancilla in the $i$th subspace, and $\tilde{\lambda}_1 = \frac{1}{2}(3F+4F\lambda-1)/(1+2F\lambda)$ and $\tilde{\lambda}_2 = \frac{1}{2}(3F-2F\lambda-1)/(1-F\lambda) = \tilde{\lambda}_3$. Due to the symmetry of the noise introduced by Eve, the error rate between Alice and Bob is given by $\mathcal{E}_{\text{AB}} = 2(1-F\lambda)/3$. We also note that whenever Eve eavesdrops, the correlation function obtained by Alice and Bob is reduced by $F\lambda$. Therefore, if this factor is less than $(6\sqrt{3}-9)/2$, the Bell inequality is not violated [5] and so Alice and Bob will abort the protocol. This implies that Eve must keep this factor above this value.

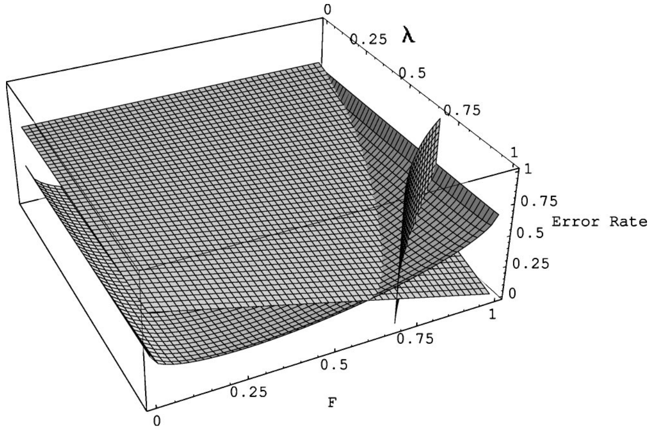

FIG. 3. Three-dimensional plots of the error rates.

Figure 3 shows the three-dimensional plots of the error rates of Eve as a function of the parameters $F$ and $\lambda$ (labeled by surface I) as well as the error rate between Alice and Bob (labeled by surface II). The region in which the factor $F\lambda$ is greater than the threshold value $[V_0 = (6\sqrt{3}-9)/2]$ is demarcated by the "wall" labeled $\mathcal{C}$. In the region bounded by $F\lambda \geqslant V_0$, the error rate of Eve is always greater than the error rate between Alice and Bob.

An alternative approach to test the security of the protocol is to compare the mutual information between Alice and Eve, and Alice and Bob. The mutual information between Alice and Eve is given by the following expression:

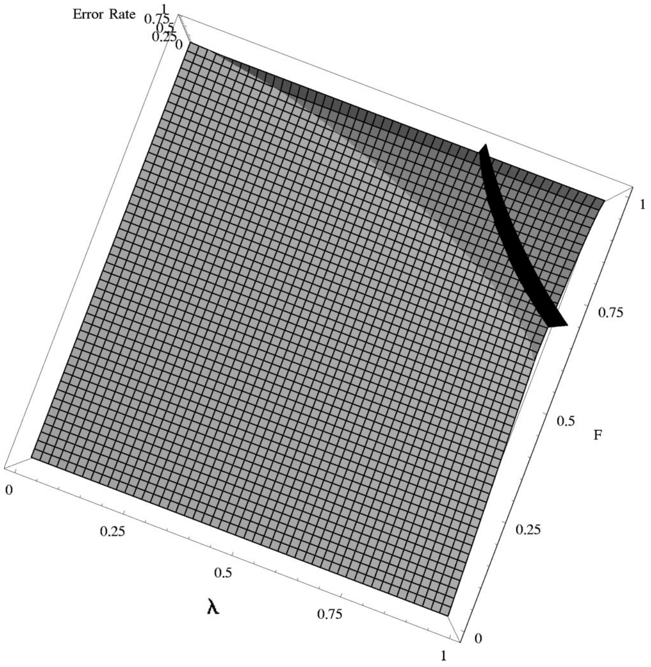

FIG. 4. Plan elevation of a three-dimensional plot of mutual information between Alice and Bob and Alice and Eve.

$$
\begin{aligned}
\mathcal{I}_{\mathrm{AE}}=&\log 3-3\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle\log\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle-6\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle\log\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle-\{-3\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle W_1\log(\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle W_1)\\
&-3\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle(1-W_1)\log[\langle\tilde{E}_{00}|\tilde{E}_{00}\rangle(1-W_1)/2]-6\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle W_2\log(\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle W_2)\\
&-6\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle(1-W_2)\log[\langle\tilde{E}_{11}|\tilde{E}_{11}\rangle(1-W_2)/2]\}.
\end{aligned}
\tag{10}
$$

The mutual information between Alice and Bob is

$$
\mathcal{I}_{\mathrm{AB}}=2\log 3+\frac{1}{3}(1+F\lambda)\{\log(1+F\lambda)-\log 9\}+\frac{2}{3}(1-F\lambda)\{\log(1-F\lambda)-\log 9\},
\tag{11}
$$

where log refers to logarithm base 3. Figure 4 shows the plan elevation of the three-dimensional plots of the mutual information as a function of the parameters $F$ and $\lambda$. The line of intersection between $\mathcal{I}_{\mathrm{AE}}$ and $\mathcal{I}_{\mathrm{AB}}$ clearly lies behind the wall separating the region in which the Bell inequality is violated from the region $(R1)$ in which local realistic description is possible $(R2)$. In the region $R1$, $\mathcal{I}_{\mathrm{AB}}>\mathcal{I}_{\mathrm{AE}}$. From numerical calculation, the maximum value of $V$ for which Eve's mutual information equals Alice and Bob's is 0.6629, thus Alice's and Bob have a buffer region in which to operate securely from this kind of attack by Eve. To summarize, we have presented a cryptographic protocol using qutrits which is resistant to a form of symmetric, incoherent attacks. The qutrit Bell inequality provides a sufficient condition for secure communication. However, this attack may not be optimal, so the Bell inequality may prove to be necessary. Moreover, our protocol is more robust against noise compared to E91 protocol. The protocol tolerates 33.7% noise, whereas it is 29.2% for E91 or BB84 protocol [17].

D.K., C.H. Oh, A.E., and L.C.K. acknowledge financial support provided under the ASTAR Grant No. 012-104-0040. D.K.L.O. acknowledges the support of CESG (UK) and QAIP Grant No. IST-1999-11234. D.K. and L.C.K. would like to thank Jing-Ling Chen for invaluable discussions.

[1] C.E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[2] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2001); H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000); M. Genovese and C. Novero, e-print quant-ph/0107118; N.J. Cerf *et al.*, Phys. Rev. Lett. **88**, 127902 (2002); N.J. Cerf, M. Bourennane, A. Karlson, and N. Gisin, *ibid.* **88**, 127902 (2002).

[3] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).

[5] D. Kaszlikowski, L.C. Kwek, J.L. Chen, M. Żukowski, and C.H. Oh, e-print quant-ph/0106010.

[6] T. Durt and M. Żukowski (private communication).

[7] M. Zukowski, A. Zeilinger, and M.A. Horne, Phys. Rev. A **55**, 2564 (1997).

[8] J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960).

[9] I.D. Ivanovic, J. Phys. A **14**, 3241 (1981).

[10] W.K. Wootters, Found. Phys. **16**, 391 (1986).

[11] C. Mattle, M. Michler, H. Weinfurter, A. Zeilinger, and M. Żukowski, Appl. Phys. B: Lasers Opt. **60**, S111 (1995).

[12] M. Reck, A. Zeilinger, H.J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).

[13] I. Jex, S. Stenholm, and A. Zeilinger, Opt. Commun. **117**, 95 (1995).

[14] D. Kaszlikowski, L.C. Kwek, Jing Ling Chen, M. Żukowski, and C.H. Oh, Phys. Rev. A **65**, 032118 (2002).

[15] J.L. Chen, D. Kaszlikowski, L.C. Kwek, C.H. Oh, and M. Żukowski, Phys. Rev. A **64**, 052109 (2001).

[16] A. Chefles, Contemp. Phys. **41**, 401 (2000).

[17] C.H. Bennett and G. Brassard, in *Proceedings of IEEE Conference on Computers, Systems, and Signal Processing*, Bangalore, India (IEEE, New York, 1984), p. 175.