Security of quantum key distribution with entangled qutrits

Thomas Durt,[1] Nicolas J. Cerf,[2] Nicolas Gisin,[3] and Marek Żukowski[4]
[1]*Toegepaste Natuurkunde en Fotonica, Theoretische Natuurkunde, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussels, Belgium*
[2]*Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[3]*Group of Applied Physics-Optique, Université de Genève, 20 rue de l'Ecole de Médecine, Genève 4, Switzerland*
[4]*Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*
(Received 30 August 2002; published 21 January 2003)

The study of quantum cryptography and quantum entanglement have traditionally been based on two-level quantum systems (qubits). In this paper, we consider a generalization of Ekert's entanglement-based quantum cryptographic protocol where qubits are replaced by three-level systems (qutrits). In order to investigate the security against the optimal individual attack, we derive the information gained by a potential eavesdropper applying a cloning-based attack. We exhibit the explicit form of this cloner, which is distinct from the previously known cloners, and conclude that the protocol is more robust than those based on entangled qubits as well as unentangled qutrits.

DOI: 10.1103/PhysRevA.67.012311 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum cryptography aims at distributing a random key in such a way that the presence of an eavesdropper who monitors the quantum communication is revealed via the induced disturbances in the transmission of the key (for a review, see, e.g., Ref. [1]). Practically, in order to realize a cryptographic protocol, it is enough that the key signal is encoded into quantum states that belong to incompatible bases, as in the original protocol of Bennett and Brassard (1984) known as BB84 [2]. In 1991, Ekert suggested to base the security of quantum cryptography on properties of the maximally entangled two-qubit state or Einstein-Podolsky-Rosen state [3]. The key signals are derived from measurements when they lead to perfect correlations (same base used by the two parties), and otherwise data for a Bell [4] or Clauser-Horne-Shimony-Holt (CHSH) [5] inequality are collected and used to reveal the presence of an eavesdropper. Recently, it was shown that the violation of Bell-type inequalities is more pronounced in the case of entangled qutrits (i.e., three-dimensional systems) than entangled qubits [6–8]. Also, several qutrit-based cryptographic protocols were shown to be more secure than their qubit-based counterparts [9–12]. It appears therefore very tempting to investigate the performances of a generalization of Ekert's protocol relying on a pair of entangled qutrits [13] instead of qubits.

From the experimental viewpoint, there are several ways of physically realizing qutrits using photons. The first possibility is to utilize multiport beam splitters, and more specifically those that split the incoming single light beam into three [13]. The second one exploits the polarization degree of freedom. However, since this is intrinsically a two-dimensional variable, one needs to use two photons per qutrit [14,15]. A third possibility, which uses only one photon per qutrit, exploits the spatial angular momentum of photons [16]. Finally, another realization of qutrits, possibly the most straightforward one, exploits time bins [17]. This approach has already been demonstrated for entangled photons up to eleven dimensions [18]. Thus, exploring an entanglement-based quantum cryptographic protocol that uses qutrits instead of qubits may lead to new applications of quantum informational technology as it lies in the reach of the current state-of-the-art quantum optical techniques.

In what follows, we shall analyze the security of this entanglement-based protocol against individual attacks (where the eavesdropper Eve monitors the qutrits separately or incoherently). To this end, we will consider a fairly general class of eavesdropping attacks that are based on (state-dependent) quantum cloning machines [19–21]. This will yield an upper bound on the acceptable error rate, which is a *necessary* condition for security against individual attacks, that is, higher error rates cannot permit us to establish a secret key using one-way communication. We will show that this maximum acceptable error rate is higher, with this qutrit protocol, than with Ekert's qubit protocol, and even slightly higher than with a three-dimensional extension of BB84.

II. THE FOUR QUTRIT BASES THAT MAXIMIZE THE VIOLATION OF LOCAL REALISM

In the protocol Ekert-91 [3], the four qubit bases chosen by Alice and Bob (the authorized users of the quantum cryptographic channel) are the four bases that maximize the violation of the CHSH inequalities [5]. They consist of two pairs of mutually unbiased bases.[1] When representing these four bases on the Bloch sphere, their eight states form a perfect octagon [see Fig. 1 (right)]. Similarly, there exists a natural generalization of this set of bases in the case of qutrits [22]. In analogy with the CHSH qubit bases, which belong to a great circle, these four qutrit bases belong to a set of bases parametrized by a phase ϕ on a generalized equator, which we shall call the ϕ bases from now on. The expression

[1]By definition, two orthonormal bases of an N-dimensional Hilbert space are said to be mutually unbiased if the norm of the scalar product between any two vectors belonging each to one of the bases is equal to $1/\sqrt{N}$.

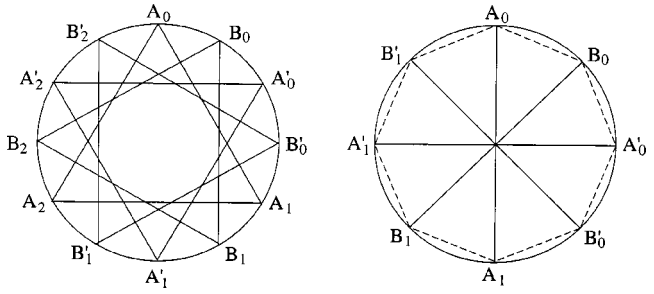

FIG. 1. (Left) the four optimal qutrit bases; (right) the qubit ones.

of the component states of any ϕ basis in the computational basis $\{|0\rangle,|1\rangle,|2\rangle\}$ is

$$|l_\phi\rangle=\frac{1}{\sqrt{3}}\sum_{k=0}^{2}e^{ik[(2\pi l/3)+\phi]}|k\rangle=\frac{1}{\sqrt{3}}e^{i[(2\pi l/3)+\phi]}\Bigg[|1\rangle+\cos\left(\frac{2\pi l}{3}+\phi\right)(|0\rangle+|2\rangle)+\sin\left(\frac{2\pi l}{3}+\phi\right)(-i)\times(|0\rangle-|2\rangle)\Bigg], \quad (1)$$

with $l=0,1,2$. Obviously, these basis vectors form an equilateral triangle on a great circle centered in $|1\rangle$. When ϕ varies, these triangles turn around $|1\rangle$. Note that the state $|1\rangle$ plays a privileged role compared with the states $|0\rangle$ and $|2\rangle$. The invariance under a cyclic permutation of the basis vectors of the computational basis is indeed broken in the ϕ bases because it can happen that $k=k'$ mod 3 while $e^{ik\phi}=e^{ik'\phi}$ $(k,\ k'=0,1,2)$ when $\phi\neq 2\pi l/3$ $(l=0,1,2)$. It has been shown that when local observers measure the correlations exhibited by the maximally entangled state

$$|\phi_3^+\rangle=\frac{1}{\sqrt{3}}(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle+|2\rangle\otimes|2\rangle) \quad (2)$$

in the four ϕ bases obtained when $\phi_i=(2\pi/12)i$ (with $i=0,1,2,3$), then the degree of nonclassicality that characterizes the correlations is higher than the degree of nonclassicality allowed by Cirelson's theorem [23] for qubits, and also higher than for a large class of other qutrit bases. This can be shown by estimating the resistance of the nonclassicality of correlations against noise admixture [6], or by considering generalizations of Bell inequalities to a situation in which trichotomic observables are considered [7,8] instead of dichotomic ones. Note that the states making up the four qutrit bases which maximize the violation of local realism (we shall call them the *optimal bases* from now on) form a perfect dodecagon, which generalizes the octagon encountered in the qubit case [see Fig. 1 (left)].

Finally, it is worth noting that the state that optimizes the violation of local realism when considering the four optimal bases is not the maximally entangled state, but the state $|\phi_{mv}\rangle=(1/\sqrt{n})(|0\rangle\otimes|0\rangle+\gamma|1\rangle\otimes|1\rangle+|2\rangle\otimes|2\rangle)$, where $\gamma=(\sqrt{11}-\sqrt{3})/2$ and $n=2+\gamma^2$ [24]. This state is not invariant under a cyclic permutation of the basis vectors of the computational basis. We noted already that this invariance is broken by the ϕ bases. We shall not discuss here the implementation of this state in quantum cryptography.

III. THREE-DIMENSIONAL ENTANGLEMENT-BASED (3DEB) PROTOCOL

Let us now assume that the source emits the maximally entangled qutrit state $|\phi_3^+\rangle$ and that Alice and Bob share this entangled pair and perform measurements along one of the four optimal bases described above. It is easy to check that $|\phi_3^+\rangle$ may be rewritten as

$$|\phi_3^+\rangle=\frac{1}{\sqrt{3}}(|0_\phi\rangle\otimes|0_\phi^*\rangle+|1_\phi\rangle\otimes|1_\phi^*\rangle+|2_\phi\rangle\otimes|2_\phi^*\rangle, \quad (3)$$

where

$$|l_\phi^*\rangle=\frac{1}{\sqrt{3}}\sum_{k=0}^{2}e^{-ik[(2\pi l/3)+\phi]}|k\rangle \quad (l=0,1,2). \quad (4)$$

Therefore, when Alice performs a measurement in the ϕ basis $\{|l_\phi\rangle\}$ and Bob in the conjugate basis $\{|l_\phi^*\rangle\}$, their results are 100% correlated. In addition, the four optimal bases defined above can be shown to be 100% correlated two by two. This can be understood graphically by noting that phase conjugation corresponds to a reflection with respect to the vertical axis that crosses the center of the circle on the left of Fig. 1, a symmetry that interchanges the bases of the dodecagon.

It is therefore natural to consider the following generalization of the Ekert-91 protocol for qutrits, which we shall denote the 3DEB protocol [25]. In this protocol, Alice and Bob share the entangled state $|\phi_3^+\rangle$ and choose each their measurement basis at random among one of the four bases maximizing the violation of local realism (according to the statistical distribution that they consider to be optimal). Because of the existence of 100% correlations between measurements in local bases of the same ϕ_i, a fraction of the measurement outcomes can be used in order to establish a deterministic cryptographic key. The rest of the data, for the cases when the left and right phases are different, can be used in order to detect the presence of an eavesdropper for example with the Bell inequalities of Ref. [8] or with the computer algorithm of Ref. [6]. Let us now study the security of this protocol against optimal individual attacks.

IV. INDIVIDUAL ATTACKS AND OPTIMAL QUTRIT CLONING MACHINES

We use a general class of cloning transformations as defined in Refs. [19–21]. If Alice sends the input state $|\psi\rangle$ belonging to an N-dimensional space (we will consider $N=3$ later on), the resulting joint state of the two clones (noted A and B) and of the cloning machine (noted C) is

$$|\psi\rangle \rightarrow \sum_{m,n=0}^{N-1} a_{m,n} U_{m,n} |\psi\rangle_A |B_{m,-n}\rangle_{B,C}$$

$$= \sum_{m,n=0}^{N-1} b_{m,n} U_{m,n} |\psi\rangle_B |B_{m,-n}\rangle_{A,C}, \quad (5)$$

where

$$U_{m,n} = \sum_{k=0}^{N-1} e^{2\pi i(kn/N)} |k+m\rangle\langle k| \quad (6)$$

and

$$|B_{m,n}\rangle = N^{-1/2} \sum_{k=0}^{N-1} e^{2\pi i(kn/N)} |k\rangle |k+m\rangle, \quad (7)$$

with $0 \leqslant m,n \leqslant N-1$. $U_{m,n}$ is an "error" operator: it shifts the state by m units (modulo N) in the computational basis, and multiplies it by a phase so as to shift its Fourier transform by n units (modulo N). Equation (7) defines the N^2 generalized Bell states for a pair of N-dimensional systems.

Tracing over systems B and C (or A and C) yields the final states of clone A (or clone B): if the input state is $|\psi\rangle$, the clones A and B are in a mixture of the states $|\psi_{m,n}\rangle = U_{m,n}|\psi\rangle$ with respective weights $p_{m,n}$ and $q_{m,n}$:

$$\rho_A = \sum_{m,n=0}^{N-1} p_{m,n} |\psi_{m,n}\rangle\langle\psi_{m,n}|,$$

$$\rho_B = \sum_{m,n=0}^{N-1} q_{m,n} |\psi_{m,n}\rangle\langle\psi_{m,n}|. \quad (8)$$

In addition, the weight functions of the two clones ($p_{m,n}$ and $q_{m,n}$) are related by

$$p_{m,n} = |a_{m,n}|^2, \quad q_{m,n} = |b_{m,n}|^2, \quad (9)$$

where $a_{m,n}$ and $b_{m,n}$ are two (complex) amplitude functions that are dual under a Fourier transform [20,21]:

$$b_{m,n} = \frac{1}{N} \sum_{x,y=0}^{N-1} e^{2\pi i(nx-my)/N} a_{x,y}. \quad (10)$$

Let us now analyze the possibility of using such a cloning procedure in the eavesdropping attack of the 3DEB protocol. Therefore, we put $N=3$. Assume that Eve clones the state of the qutrit that is sent to Bob [represented as the key $|\psi\rangle$ in Eq. (5)], and resends the imperfect clone (labeled by A) to Bob while she conserves the other one (labeled by B). Then, in analogy with Ref. [11], Eve will measure her clone in the same basis as Bob (the ϕ basis) and her ancilla (labeled by C) in the conjugate basis (the ϕ^* basis). For deriving Eve's information, we need first to rewrite the cloning transformation in these bases. By straightforward computations we get, when ϕ is equal to zero, that

$$|B_{m,n}\rangle = 3^{-1/2} \sum_{l=0}^{2} e^{im[(2\pi/3)(l-n)+\phi]} |l_\phi\rangle |(l-n)^*_\phi\rangle$$

$$= e^{im[(-2\pi/3)n+\phi]} |\tilde{B}_{-n_\phi, m^*_\phi}\rangle, \quad (11)$$

where, by definition,

$$|\tilde{B}_{m_\phi, n^*_\phi}\rangle = 3^{-1/2} \sum_{k=0}^{2} e^{2\pi i(kn/3)} |k_\phi\rangle |(k+m)^*_\phi\rangle \quad (12)$$

and

$$U_{m,n} = \sum_{k=0}^{2} e^{-im[(2\pi/3)(k+n)+\phi]} |(k+n)_\phi\rangle\langle k_\phi|$$

$$= e^{-im[(2\pi/3)n+\phi]} \tilde{U}_{n_\phi, -m_\phi}, \quad (13)$$

where the tilde refers to the new (ϕ and ϕ^*) bases. After substitution in Eq. (5), we get

$$|\psi\rangle \rightarrow \sum_{m,n=0}^{2} a_{m,n} U_{m,n} |\psi\rangle_A |B_{m,-n}\rangle_{B,C}$$

$$= \sum_{m,n=0}^{2} \tilde{a}_{m,n} \tilde{U}_{m_\phi, n_\phi} |\psi\rangle_A |\tilde{B}_{m_\phi, n_\phi}\rangle_{B,C}, \quad (14)$$

where the new amplitudes are defined as $\tilde{a}_{n,-m} = a_{m,n}$.

We are interested in a cloning machine that has the same effect when expressed in the four optimal bases, i.e., when $\phi_i = (2\pi/12)i$ ($i=0,1,2,3$). This imposes strong constraints on the amplitudes $a_{m,n}$ characterizing the cloner, which must be of the form

$$(a_{m,n}) = \begin{pmatrix} v & x & x \\ y & y & y \\ z & z & z \end{pmatrix}. \quad (15)$$

It is possible to check that, in analogy with the qubit case [26], such a cloner is phase covariant, which means that it acts identically on each state of the ϕ bases. In particular, the identity (14) can be shown to hold for all values of ϕ. The reason for this property is that, roughly speaking, if the cloner remains invariant when expressed in several bases, then it means that certain combinations of Bell states possess several Schmidt biorthogonal decompositions. It is well known that when at least two such decompositions exist for a bipartite pure state, then there exist infinitely many. This explains why requiring the same cloning fidelity in two optimal bases ($\phi_i = 2\pi i/12$, $\phi_j = 2\pi j/12$ with $i,j=0,1,2,3$ and $i \neq j$) implies phase-covariance (i.e., ϕ arbitrary). A proof of this property is out of the scope of the present paper.

Let us now evaluate the fidelity of this phase-covariant cloner for qutrits, along with the information that Bob and Eve obtain about Alice's state. The fidelity of the first clone (the one that is sent to Bob) when copying a state $|\psi\rangle$ can be written, in general, as

$$F_A=\langle\psi|\rho_A|\psi\rangle=\sum_{m,n=0}^{N-1}|a_{m,n}|^2|\langle\psi|\psi_{m,n}\rangle|^2. \quad (16)$$

Of course, the same relation holds for the second clone (the one that is kept by Eve) by replacing $a_{m,n}$ by $b_{m,n}$. For the cloning machine defined by Eq. (15), it is possible to compute the fidelities when cloning the component states of the ϕ bases by a straightforward but lengthy computation. It can be shown that the fidelity of the first clone does not depend on ϕ, that is,

$$F_A=\langle l_\phi|\rho_A|l_\phi\rangle=v^2+y^2+z^2 \quad (17)$$

for all ϕ. The disturbances D_{A1} and D_{A2} of the first clone, defined respectively, as $\langle l_{\phi+(2\pi/3)}|\rho_A|l_{\phi+(2\pi/3)}\rangle$ and $\langle l_{\phi-(2\pi/3)}|\rho_A|l_{\phi-(2\pi/3)}\rangle$ yield both $x^2+y^2+z^2$. Making use of Eq. (10), we obtain that, for the second clone, the states of the bases used in the cryptographic protocol are all copied with the same fidelity, which is maximum when $y=z$, and is given by

$$F_B=(v^2+2x^2+12y^2+8xy+4vy)/3. \quad (18)$$

Also, we get the same disturbance for all ϕ (minimal when $y=z$) given by $D_{B1}=D_{B2}=(v^2+2x^2+3y^2-4xy-2vy)/3$.

We must now find what is the optimal strategy for Eve. In virtue of the phase covariance and in order to simplify the notations, we shall from now on omit the labels that refer to the particular basis ϕ in which the measurement is carried out. After substitution in Eq. (5), we get

$$|\psi_k\rangle\rightarrow 3^{-1/2}\sum_{m,l=0}^{2}\tilde{c}_{m,k-l}|\psi_{k+m}\rangle_A|\psi_l\rangle_B|\psi_{l+m}\rangle_C, \quad (19)$$

where $\tilde{c}_{m,j}=\Sigma_{n=0}^{2}\tilde{a}_{m,n}e^{i(2\pi/3)jn}$. Now, $\tilde{a}_{m,n}=y+\delta_{n0}[(v-y)\delta_{m0}+(x-y)(\delta_{m1}+\delta_{m2})]$ so that $\tilde{c}_{m,j}=[3y\delta_{j0}+(v-y)\delta_{m0}+(x-y)(\delta_{m1}+\delta_{m2})]$. Therefore,

$$|\psi_k\rangle\rightarrow 3^{-\frac{1}{2}}\Bigg\{|\psi_k\rangle_A\Bigg[3y|\psi_k\rangle_B|\psi_k\rangle_C+(v-y)\sum_{l=0}^{2}|\psi_l\rangle_B|\psi_l\rangle_C\Bigg]+|\psi_{k+1}\rangle_A\Bigg[3y|\psi_k\rangle_B|\psi_{k+1}\rangle_C$$
$$+(x-y)\sum_{l=0}^{2}|\psi_l\rangle_B|\psi_{l+1}\rangle_C\Bigg]+|\psi_{k-1}\rangle_A\Bigg[3y|\psi_k\rangle_B|\psi_{k-1}\rangle_C+(x-y)\sum_{l=0}^{2}|\psi_l\rangle_B|\psi_{l-1}\rangle_C\Bigg]\Bigg\}. \quad (20)$$

After Alice's (or Bob's) measurement basis is disclosed, Eve's optimal strategy can be shown [11] to be the following: first she measures both her copy B and the cloning machine C in the same basis as Bob, the difference (modulo 3) of the outcomes simply giving Bob's error m. Conditionally on Eve's measured value of m (i.e., conditionally on Bob's error), the information Eve has on the state $|\psi\rangle$ can be expressed as

$$I(A{:}E|m=0)=\log_2(3)-H\left[\frac{(v+2y)^2}{3F_A},\frac{(v-y)^2}{3F_A},\frac{(v-y)^2}{3F_A}\right]$$

$$I(A{:}E|m\neq 0)=\log_2(3)$$
$$-H\left[\frac{2(x+2y)^2}{3(1-F_A)},\frac{2(x-y)^2}{3(1-F_A)},\frac{2(x-y)^2}{3(1-F_A)}\right], \quad (21)$$

where $F_A=v^2+2y^2$ since we have $y=z$, and $H[\,]$ denotes Shannon entropy. On average, we get for Eve's information

$$I_{AE}=F_AI(A{:}E|m=0)+(1-F_A)I(A{:}E|m\neq 0). \quad (22)$$

Of course, Bob's information is given by

$$I_{AB}=\log_2(3)-H\left[F_A,\frac{1-F_A}{2},\frac{1-F_A}{2}\right]. \quad (23)$$

We now use a theorem due to Csiszár and Körner [27] which provides a lower bound on the secret key rate, that is, the rate R at which Alice and Bob can generate secret key bits via privacy amplification: if Alice, Bob, and Eve share many independent realizations of a probability distribution $p(a,b,e)$, then there exists a protocol that generates a number of key bits per realization satisfying

$$R\geqslant\max(I_{AB}-I_{AE},I_{AB}-I_{BE}). \quad (24)$$

In our case, $I_{AE}=I_{BE}$ since Eve knows exactly Bob's error m. It is therefore sufficient that $I_{AB}>I_{AE}$ in order to establish a secret key with a nonzero rate. If we restrict ourselves to one-way communication on the classical channel, this actually is also a necessary condition. Consequently, the quantum cryptographic protocol above ceases to generate secret key bits precisely at the point where Eve's information matches Bob's information.

We thus need to estimate the maximal fidelity F_A (or minimal error rate) for which a cloning machine exists such that $I_{AE}=I_{AB}$. This constrained optimization problem can be solved numerically, giving

$$F_A=0.7753 \quad (25)$$

corresponding to the solution $(v,x,y)=(0.8320, 0.1711, 0.2038)$. Since $x\neq y$, this optimal cloner is therefore distinct from the universal qutrit cloner (which clones all

states with the same fidelity). Actually, it is slightly better than the (asymmetric) universal qutrit cloner, which gives a fidelity $F_A=0.7733$ at the crossing point of Bob's and Eve's information curves [11]. This means that the quantum cryptographic protocol where the four mutually unbiased qutrit bases are used (see Ref. [9]) is slightly better than the 3DEB protocol as it admits a 0.2% higher error rate ($1-F_A=22.67\%$ instead of 22.47%).

The cloner that we have derived here is an asymmetric version of the so-called two-phase-covariant qutrit cloner that is described in Refs. [28,29] [this symmetric two-phase-covariant qutrit cloner has a fidelity $(5+\sqrt{17})/12\approx 0{,}760$]. It copies all states of the form $3^{-1/2}(|0\rangle+e^{i\alpha}|1\rangle+e^{i\beta}|2\rangle)$ with a fidelity 0.7753 (>0.7733) for all α and β, while the states of the computational basis $\{|0\rangle,|1\rangle,|2\rangle\}$ are cloned with a lower fidelity 0.7507 (<0.7733). Actually, its relation with the symmetric two-phase-covariant cloner is of the same kind as the relation between the asymmetric universal qutrit cloner (of fidelity 0.7733) and the symmetric universal qutrit cloner (of fidelity 3/4).

V. CONCLUSIONS

The Ekert-91 protocol and its qutrit extension, the 3DEB protocol which is analyzed in the present paper, involve encryption bases for which the violation of local realism is maximal. If Alice and Bob measure their member of a maximally entangled qutrit pair in two ''conjugate'' bases, this gives rise to perfect correlations. After measurement is performed on each member of a sequence of maximally entangled qutrit pairs, Alice and Bob can reveal on a public channel what were their respective choices of basis and identify which trit was correctly distributed, from which they will make the key. They can use the rest of the data in order to check that it does not admit a local realistic simulation. For instance they can check that their correlations violate some generalized Bell or CHSH inequalities. Since the resistance of such a violation against noise is maximal when the maximally entangled qutrit pair is measured in the optimal qutrit bases discussed here (and is higher than all what can be achieved with qubits), the 3DEB protocol is optimal from the point of view of the survival of nonclassical correlations in a noisy environment.

Indeed, our results imply that the 3DEB protocol is more robust against optimal incoherent attacks than the Ekert-91 qubit protocol. This is because the optimal qubit phase-covariant cloning machine (which clones the optimal qubit bases involved in CHSH with the same fidelity) gives a somewhat higher fidelity $F_A=1/2+1/\sqrt{8}\simeq 0.8536$ [26,28,30] than Eq. (25). In other words, the acceptable error rate, i.e., the error rate $1-F_A$ above which the security against incoherent attacks is not ensured, is 22.47% for the 3DEB protocol, while it is only 14.64% for the Ekert-91 protocol.

Recently, it has been shown that the violation of a Bell inequality extended to qutrits is possible, as long as the ''visibility'' of the two-qutrit interference exceeds $V_{thr}=(6\sqrt{3}-9)/2\simeq 0.6962$ [7,8]. The visibility mentioned above is directly related the threshold fraction of unbiased noise, $(1-V_{thr})$, which has to be admixed to the maximally entangled state in order to erase the nonclassical character of the correlations, and therefore is a measure of robustness of such a nonclassicality [6]. This means that the nonexistence of a local realistic model of the correlations is guaranteed if the fidelity F_A that characterizes the communication channel between Alice and Bob (detectors included, so $1-F_A$ is the effective error rate in the transmission) is larger than $2/3\times 0.6962+1/3\approx 0.7974$ (instead of $1/2+1/\sqrt{8}\simeq 0.8536$ in the case of qubits [23,5,1]). On the other hand, we have shown here that the 3DEB protocol is secure against a cloning-based individual attack, if $F_A>0.7753$. Consequently, when a violation of a qutrit Bell inequality [7,8] occurs, the security of the 3DEB protocol against individual attacks is automatically guaranteed. Therefore, the violation of Bell inequalities is a *sufficient* condition for security, as it implies that Bob's fidelity is higher than the security threshold. Remarkably, for qubits, the corresponding sufficient condition ($F_A>0.8536$) is also necessary [1] (this is apparently the case for qubits only).

In addition, the violation of Bell inequalities guarantees that the 3DEB protocol is secure against so-called Trojan horse attacks during which the eavesdropper would control the whole transmission line and replace the signal by a fake, predetermined local-variable dependent, signal that mimics the quantum correlations. Such an attack can be thwarted when the signal is encrypted in the optimal bases provided that the noise level is low enough (including now also the inefficiency of the detectors) so that no such local realistic simulation of the signal does exist, and provided that Alice and Bob perform their respective choices of bases independently and quickly enough [31] so that their measurements are independent spatially separated events. Note that all the protocols in which mutually unbiased bases are involved but with no entanglement (such as BB84 [2], the six-state qubit protocol [32,30], or the twelve-state qutrit protocol [9]) admit a local realistic model, so that they are not secure against Trojan horse attacks.

Finally, it is interesting to compare the performances of the 3DEB protocol to those of the three-dimensional extension of BB84. The cloner that must be used in the latter case, where two mutually unbiased qutrit bases are used, has a fidelity of 0.7887 [11], thus a bit higher than the fidelity of the cloner analyzed here, see Eq. (25). Therefore, the 3DEB protocol also gives a slightly higher acceptable error rate than the three-dimensional extension of BB84 (22.47% instead of 21.13%). This, together with the robustness with respect to Trojan horse attacks, clearly establishes the advantage of entanglement-based protocols with respect to BB84-like protocols.

In summary, we have derived a qutrit cloning machine that clones equally well the four optimal qutrit bases (those which maximize the violation of local realism), so it gives the optimal individual attack against the 3DEB protocol introduced here. The acceptable error rate of the 3DEB protocol turns out to be 22.47%, which is higher than that of Ekert-91 qubit protocol (as well as that of the three-dimensional extension of BB84). Our analysis thus confirms a seemingly general property that qutrit schemes for quan-

tum key distribution are more robust against noise than the corresponding qubit schemes.

Note added. A recent, independent paper by Kaszlikowski *et al*. [33] shows that, if Eve acts on one member of a maximally entangled qutrit pair, then her information attains Alice's and Bob's mutual information at a visibility of 0.6629. In our notation, this means that the fidelity at the information crossing point is $2/3\times 0.6629+1/3\simeq 0.7753$, which exactly coincides with our Eq. (25). Nevertheless the two approaches are different in the following sense: in our approach, we assume that Eve clones the state of the qutrit that is sent to Bob according to Eq. (5) and then we impose that the cloning fidelity is identical for all the states of the ϕ bases in order to fix the parameters $a_{m,n}$. Instead, in Ref. [33], a general transformation is postulated from the beginning, and extra-constraints are imposed. We have also checked that our optimal cloning machine satisfies these constraints, so the two approaches are compatible. Our approach being constructive, we obtain the explicit form of the cloner, which is not the case in the approach of Ref. [33]. Moreover, although the optimal cloning machines coincide in both approaches, it can be shown that our approach allows us to build new and more general solutions that satisfy the constraints considered in Ref. [33].

ACKNOWLEDGMENTS

We are grateful to J. Roland for carrying out the numerical calculations. We thank the European Science Foundation for financial support. T.D. is supported by the Fonds voor Wetenschappelijke Onderzoek (FWO Vlaanderen). N.J.C. and N.G. acknowledge funding by the European Union under the project EQUIP (IST-FET program). M.Z. acknowledges the KBN Grant No. 5 P03B 088 20.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] 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), p. 175.
[3] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] J.S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1965).
[5] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[6] D. Kaszlikowski, P. Gnacinski, M. Żukowski, W. Miklaszewski, and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).
[7] D. Kaszlikowski, L.C. Kwek, J.L. Chen, M. Zukowski, and C.H. Oh, Phys. Rev. A **65**, 032118 (2002).
[8] D. Collins, N. Gisin, N. Linden, S. Massar, and S. Popescu, Phys. Rev. Lett. **88**, 040404 (2002).
[9] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[10] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306 (2001).
[11] N.J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002); M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, J. Phys. A **35**, 10065 (2002).
[12] D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[13] A. Zeilinger, M. Żukowski, M. A. Horne, H. J. Bernstein, and D. M. Greenberger, in *Fundamental Aspects of Quantum Theory*, edited by J. Anandan and J. L. Safko (World Scientific, Singapore, 1993); M. Żukowski, A. Zeilinger, and M.A. Horne, Phys. Rev. A **55**, 2564 (1997).
[14] J.C. Howell, A. Lamas-Linares, and D. Bouwmeester, Phys. Rev. Lett. **88**, 030401 (2002).
[15] A.V. Burlakov, L.A. Krivitskiy, S.P. Kulik, G.A. Maslennikov, and M.V. Chekhova, e-print quant-ph/0207096.
[16] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature (London) **412**, 3123 (2001).
[17] W. Tittel and G. Weihs, Quantum Inf. Comput. **1**(2), 3 (2001).
[18] H. De Riedmatten, I. Marcikic, H. Zbinden, and N. Gisin, Quantum Inf. Comput. **2**, 425 (2002).
[19] N.J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[20] N.J. Cerf, Acta Phys. Slov. **48**, 115 (1998), special issue on quantum information.
[21] N.J. Cerf, J. Mod. Opt. **47**, 187 (2000), special issue on quantum information.
[22] T. Durt, D. Kaszlikowski, and M. Żukowski, Phys. Rev. A **64**, 024101 (2000).
[23] B.S. Cirel'son, Lett. Math. Phys. **4**, 93 (1980).
[24] A. Acin, T. Durt, N. Gisin, and J.I. Latorre, Phys. Rev. A **65**, 052325 (2002).
[25] T. Durt, D. Kaszlikowski, and M. Żukowski (private communication).
[26] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997); D. Bruss, M. Cinchetti, G.M. D'Ariano, and C. Macchiavello, *ibid.* **62**, 012302 (2000).
[27] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[28] N.J. Cerf, T. Durt, and N. Gisin, J. Mod. Opt. **49**, 1355 (2002), special issue on quantum information.
[29] G.M. D'Ariano and P. Lo Presti, Phys. Rev. A **64**, 042308 (2001).
[30] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[31] T. Durt, Phys. Rev. Lett. **86**, 1392 (2001).
[32] D. Bruss, Phys. Rev. Lett. **81**, 3018 (1998).
[33] D. Kaszlikowski, D. K. L. Oi, M. Christandl, K. Chang, A. Ekert, L. C. Kwek, and C. H. Oh, preceding paper, Phys. Rev. A **67**, 012310 (2003).