Security bound of two-basis quantum-key-distribution protocols using qudits

Georgios M. Nikolopoulos and Gernot Alber
Institut für Angewandte Physik, Technische Universität Darmstadt, 64289 Darmstadt, Germany
(Received 21 January 2005; published 16 September 2005)

We investigate the security bounds of quantum-cryptographic protocols using d-level systems. In particular, we focus on schemes that use two mutually unbiased bases, thus extending the Bennett-Brassard 1984 quantum-key-distribution scheme to higher dimensions. Under the assumption of general coherent attacks, we derive an analytic expression for the ultimate upper security bound of such quantum-cryptography schemes. This bound is well below the predictions of optimal cloning machines. The possibility of extraction of a secret key beyond entanglement distillation is discussed. In the case of qutrits we argue that any eavesdropping strategy is equivalent to a symmetric one. For higher dimensions such an equivalence is generally no longer valid.

DOI: 10.1103/PhysRevA.72.032320 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

During the last two decades, several quantum-key-distribution (QKD) protocols have been proposed, which use two-level quantum systems (qubits) as information carriers [1–3]. The security of these protocols against all kinds of attacks has been analyzed extensively and various unconditional security proofs have been presented [4–10]. From the experimental point of view, a number of prototypes based on qubits have been developed [11], while QKD has been successfully performed outside the laboratory at distances up to about 67 km using telecom fibers [12,13], and up to 23.4 km [14] through open air.

In contrast to qubits, the use of high-dimensional quantum systems in quantum cryptography has attracted considerable attention only recently. Currently, qudits (d-dimensional quantum systems) can be realized experimentally in several ways (including multiport beam splitters, biphotons, higher-order parametric down-conversion, and energy-time entanglement) [15–17]. As far as QKD protocols are concerned, qudits can carry more information than qubits, increasing thus the flux of information between the two legitimate users (Alice and Bob). For a prime power d it has been demonstrated that there exist $(d+1)$ mutually unbiased bases. Hence, the natural extensions of the standard Bennett-Brassard 1984 (BB84) and six-state qubit-based QKD protocols to higher dimensions involve $2d$ and $d(d+1)$ states, respectively [18,19]. These latter qudit-based QKD schemes are able to tolerate higher error rates than their qubit-based counterparts [20–25].

The maximal error rate that can be tolerated by a particular QKD protocol (also referred to as *threshold disturbance*) quantifies the robustness of the protocol against a specific eavesdropping strategy, and depends on the algorithm that Alice and Bob are using for postprocessing their raw key. In practice, nowadays secret keys can be distilled efficiently by means of one- or even two-way classical postprocessing [26,27], while advantage distillation protocols using two-way classical communication seem to be still rather inefficient [28]. In principle, however, quantum-distillation protocols involving two-way communication between Alice and Bob [also referred to as two-way entanglement purification protocols (EPPs)] can tolerate substantially higher error rates than their classical counterparts and can be applied whenever the quantum state shared between the two honest parties is freely entangled, i.e., distillable [29–32].

For $2\otimes 2$ quantum systems, nondistillability is equivalent to separability [33,34] and thus there seems to exist a complete equivalence between entanglement distillation and secrecy. In particular, for qubit-based QKD protocols and under the assumption of individual attacks, it was proven recently that the extraction of a secret key from a quantum state is possible if and only if entanglement distillation is possible [35]. For higher dimensions, however, the complete equivalence between entanglement distillation and secrecy, has been put into question by Horodecki *et al.* [36], who showed that a secret key can, in principle, be extracted even from bound entangled states [37]. Nevertheless, for arbitrary dimensions, provable quantum entanglement is always a necessary precondition for secure QKD [38]. Therefore, the natural question arises whether qudit-based QKD protocols can indeed go beyond entanglement distillation. In other words, what is the maximal error rate that can, in principle, be tolerated by a qudit-based QKD under the assumption of general coherent attacks?

In this paper, we address this question by focusing on qudit-based QKD protocols that use two mutually unbiased bases. Up to date, all investigations related to the security of such protocols have concentrated mainly on individual attacks (e.g., quantum cloning machines) and/or one-way postprocessing of the raw key [21–25]. Here, under the assumption of general coherent (joint) attacks, we show that for estimated disturbances below $(d-1)/2d$ Alice and Bob can be confident that they share distillable entanglement with high probability. On the other hand, an estimated disturbance above $(d-1)/2d$ does not enable Alice and Bob to infer that their quantum state is entangled (no provable quantum entanglement). Hence, in view of the necessary precondition for secure key distribution [38], our result demonstrates that $(d-1)/2d$ is also the ultimate threshold disturbance for the prepare-and-measure schemes of the protocols. Furthermore, our result implies that, for the postprocessing we consider

throughout this work, the extraction of a secret key beyond entanglement distillation is impossible in the framework of qudit-based QKD protocols using two bases.

This paper is organized as follows. For the sake of completeness, in Sec. II we summarize basic facts which are necessary for the subsequent discussion. In Sec. III we briefly describe the prepare-and-measure and the entanglement-based versions of the two-basis QKD protocols using qudits. Subsequently, Sec. IV focuses on the key quantity of this work, namely, the estimated error rate (disturbance) and its symmetries. Finally, the threshold disturbance for two-basis qudit-based QKD protocols, is derived in Sec. V and various examples are presented.

II. QUDITS AND THE GENERALIZED PAULI GROUP

Throughout this work we consider QKD protocols with qudit systems as information carriers. Each qudit corresponds to a d-dimensional Hilbert space $\mathbb{C}^d$ where $d=p^r$ is a prime power, i.e., p is a prime and r is an integer [39]. From now on all the arithmetic is performed in the finite (Galois) field $\mathbb{F}_d$ [40].

Theoretical investigations of d-level quantum systems are performed conveniently with the help of the generalized Pauli group. For this purpose let us define the unitary operators

$$\mathcal{X}^m = \sum_{\alpha\in\mathbb{F}_d} |\alpha+m\rangle\langle\alpha|, \quad \text{for } m\in\mathbb{F}_d \tag{1}$$

$$\mathcal{Z}^n = \sum_{\alpha\in\mathbb{F}_d} \omega^{\mathrm{tr}(n\cdot\alpha)}|\alpha\rangle\langle\alpha|, \quad \text{for } n\in\mathbb{F}_d \tag{2}$$

where $\omega=\exp(i2\pi/p)$ is a primitive pth root of unity and

$$\mathrm{tr}(\alpha) = \sum_{j=0}^{r-1} \alpha^{p^j} \tag{3}$$

is the absolute trace of $\alpha\in\mathbb{F}_d$. The states $\{|\alpha\rangle;\alpha\in\mathbb{F}_d\}$ constitute an orthonormal computational basis on the Hilbert space of a qudit $\mathbb{C}^d$. The unitary operators $\mathcal{X}$ and $\mathcal{Z}$ generate the generalized Pauli group with unitary elements

$$\mathcal{E}_{mn} = \{\mathcal{X}^m\mathcal{Z}^n : m,n\in\mathbb{F}_d\}. \tag{4}$$

These d^2 unitary operators form an error group on $\mathbb{C}^d$ [41], and are the generalizations of the Pauli operators for qubits. In fact the indices m and n refer to shift and phase errors in the computational basis, respectively. Thus the generalized Pauli operators can be represented in the form

$$\mathcal{E}_{mn} = \sum_{k\in\mathbb{F}_d} \omega^{\mathrm{tr}(k\cdot n)}|k+m\rangle\langle k|, \tag{5}$$

with

$$\mathcal{Z}^n\mathcal{X}^m = \omega^{\mathrm{tr}(m\cdot n)}\mathcal{X}^m\mathcal{Z}^n. \tag{6}$$

Consider now a bipartite system of two qudits A and B. It is not hard to show that the operators $\mathcal{X}_A\otimes\mathcal{X}_B^*$ and $\mathcal{Z}_A\otimes\mathcal{Z}_B^*$ constitute a *complete set of commuting operators* in the Hilbert space of two distinguishable qudits $\mathbb{C}_A^d\otimes\mathbb{C}_B^d$, while their simultaneous eigenstates are the d^2 maximally entangled states

$$|\Psi_{mn}\rangle = \frac{1}{\sqrt{d}}\sum_{k\in\mathbb{F}_d} \mathbb{1}_A|k_A\rangle\otimes\mathcal{E}_{mn;B}|k_B\rangle, \tag{7}$$

with $m,n\in\mathbb{F}_d$. These states are the generalization of the Bell states to higher dimensions and they form an orthonormal basis in $\mathbb{C}_A^d\otimes\mathbb{C}_B^d$. The singlet state $|\Psi_{00}\rangle$ is of particular interest because it remains invariant under any unitary transformation of the form $\mathcal{U}_A\otimes\mathcal{U}_B^*$. In fact $|\Psi_{00}\rangle$ is one of the key elements of the entanglement-based version of the qudit cryptographic protocols described in the following section.

III. TWO-BASIS QKD PROTOCOLS

A. Mutually unbiased bases

Of central importance in the context of QKD is the notion of mutually unbiased (maximally conjugated) bases. It has been demonstrated that for a prime power d, there exist $d+1$ such bases, e.g. for prime d, the eigenbases of the operators $\mathcal{Z},\mathcal{X},\mathcal{XZ},\mathcal{XZ}^2,\ldots,\mathcal{XZ}^{d-1}$ [18,19]. In a qudit-based two-basis QKD protocol (to be referred to hereafter as the $2d$-state protocol), Alice and Bob use for their purposes only two mutually unbiased bases $\mathcal{B}_1$ and $\mathcal{B}_2$ with d basis states each. Following [24,25], from now on the eigenbasis $\{|k\rangle:k\in\mathbb{F}_d\}$ of the operator $\mathcal{Z}$ is chosen as the standard (computational) basis $\mathcal{B}_1$, while the second basis $\mathcal{B}_2\equiv\{|\bar{l}\rangle:l\in\mathbb{F}_d\}$ is chosen as the Fourier dual of the computational basis, i.e., $|\bar{l}\rangle\equiv\Sigma_k\mathcal{H}_{lk}|k\rangle$, with

$$\mathcal{H} = \frac{1}{\sqrt{d}}\sum_{i,j\in\mathbb{F}_d} \omega^{\mathrm{tr}(i\cdot j)}|i\rangle\langle j| \tag{8}$$

denoting the discrete Fourier transformation. One can verify easily that $\mathcal{H}$ is symmetric and thus unitary, i.e., $\mathcal{H}^\dagger=\mathcal{H}^{-1}=\mathcal{H}^*$. This property will be used extensively in the following sections. Besides, errors in the two maximally conjugated bases are related via the discrete Fourier transform, i.e.,

$$\mathcal{H}^\dagger\mathcal{E}_{mn}\mathcal{H} = \omega^{-\mathrm{tr}(m\cdot n)}\mathcal{E}_{nm}^*. \tag{9}$$

In other words, shift errors in the computational basis become phase errors in the complementary basis, and vice versa.

B. Prepare-and-measure QKD scheme

In a typical $2d$-state prepare-and-measure scheme Alice sends to Bob a sequence of qudits each of which is randomly prepared in one of the $2d$ nonorthogonal basis states $\{|k\rangle\}$ or $\{|\bar{l}\rangle\}$. Bob measures each received particle randomly in $\mathcal{B}_1$ or $\mathcal{B}_2$. After the distribution stage, Alice and Bob agree on a random permutation of their data and publicly discuss the bases chosen, discarding all the dits where they have selected different bases (sifting procedure). Subsequently, they randomly select a sufficient number of dits [42] from the remaining random sifted key and determine their error probability. If, as a result of a noisy quantum channel or of an

eavesdropper, the estimated disturbance is too high the protocol is aborted. Otherwise, Alice and Bob perform error correction and privacy amplification with one- or two-way classical communication, in order to obtain a smaller number of secret and perfectly correlated random dits [10,20,24–28].

C. Entanglement-based QKD scheme

From the point of view of an arbitrarily powerful eavesdropper the above prepare-and-measure scheme is equivalent to an entanglement-based QKD protocol [20,25,43]. In this latter form of the protocol Alice prepares each of $2N$ entangled-qudit pairs in the maximally entangled state

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{d}} \sum_{k \in \mathbb{F}_d} |k_A\rangle \otimes |k_B\rangle, \tag{10}$$

where the subscripts A,B refer to Alice and Bob, respectively. Alice uses for her purposes the set of bases $\{\mathcal{B}_1,\mathcal{B}_2\}$ whereas Bob uses the set $\{\mathcal{B}_1,\mathcal{B}_2^*\}$, where $\mathcal{B}_2^* \equiv \{\mathcal{H}^*|k\rangle : k \in \mathbb{F}_d\}$ [20,25].

More precisely, Alice keeps half of each pair and submits the other half to Bob after having applied a random unitary transformation chosen from the set $\{\mathbb{1},\mathcal{H}\}$. As soon as Bob acknowledges the reception of all the particles, Alice reveals the sequence of operations she performed on the transmitted qudits and Bob undoes all of them, i.e., he applies $\mathbb{1}$ or $\mathcal{H}^{-1}$ on each qudit separately. Thus, at this point, in an ideal system Alice and Bob would share $2N$ qudit pairs in the state $|\Psi_{00}\rangle^{\otimes 2N}$. However, in real systems, due to noise and/or eavesdropping all the $2N$ entangled-qudit pairs will be corrupted. In order to ensure secret key distribution Alice and Bob *permute randomly* all the pairs before doing any other operations [10]. In this way, any influence of the eavesdropper (from now on we assume that all the noise in the channel is due to eavesdropping) is equally distributed among all the pairs.

The next step of the protocol now involves a verification test which will determine whether the protocol should be aborted or not. More precisely, Alice and Bob randomly select a number of pairs (say N_c) [42] as check pairs and measure each one of them *separately* along the standard (computational) basis. They compare their results publicly thus estimating the average error rate during the transmission. After the verification test all the check pairs are dismissed and, if the estimated error rate is too high the protocol is aborted. Otherwise, Alice and Bob apply an appropriate EPP with classical one-or two-way communication [20,29–32] on the remaining $2N-N_c$ pairs, in order to distill a smaller number of almost pure entangled-qudit pairs. Finally, measuring these almost perfectly entangled qudit pairs in a common basis, Alice and Bob obtain a secret random key, about which an adversary has negligible information. In our subsequent treatment we focus on the entanglement-based version of the $2d$-state QKD protocol.

IV. ESTIMATED DISTURBANCE AND SYMMETRIES

The verification test performed by Alice and Bob immediately after the transmission stage is perhaps the most crucial stage of the two-basis QKD protocol and its success relies on the "commuting-observables" idea [4]. More precisely, the fact that all the operations performed in a typical EPP commute with a Bell measurement allows one to reduce any quantum eavesdropping attack to a classical probabilistic cheating strategy [4,7,10,20].

During the verification test Alice and Bob focus on the parity of their outcomes. Moreover, note that for the check pairs where Alice and Bob have performed $\mathcal{H}$ and $\mathcal{H}^{-1}$ respectively, the measurements are effectively performed in the complementary $\mathcal{B}_2$ basis rather than the standard basis $\mathcal{B}_1$ [6]. Thus, given the unitarity of $\mathcal{H}$ and the invariance of $|\Psi_{00}\rangle$ under any unitary transformation of the form $\mathcal{U}_A \otimes \mathcal{U}_B^*$, the average estimated disturbance (error rate) is given by

$$D = \frac{1}{2N_c} \sum_{b=0,1} \sum_{j_i=1}^{N_c} \mathrm{Tr}_{A,B}\{[(\mathcal{H}_A^{b\dagger} \otimes \mathcal{H}_B^b)\mathcal{P}(\mathcal{H}_A^b \otimes \mathcal{H}_B^{b\dagger})]_{j_i}\rho_{AB}\}, \tag{11}$$

where ρ_{AB} denotes the reduced density operator of Alice and Bob for all $2N$ pairs. The index j_i indicates that the corresponding physical observable refers to the j_ith randomly selected qudit pair. In particular, the projection operator entering Eq. (11) is given by

$$\mathcal{P}_{j_i} \equiv \sum_{l \in \mathbb{F}_d} \sum_{k \in \mathbb{F}_d^*} |l_A,(l+k)_B\rangle\langle l_A,(l+k)_B|, \tag{12}$$

where $\mathbb{F}_d^*$ denotes the set of all nonzero elements in the field $\mathbb{F}_d$ [44]. In other words, the inner summation in Eq. (12) is performed over all the nonzero elements of the finite field $\mathbb{F}_d$, such that $(l+k)_B \neq l_A$. Moreover, the powers of the discrete Fourier transformation $\mathcal{H}^b$, with $b \in \{0,1\}$, in Eq. (11) reflect the fact that the errors in the sifted key originate from measurements in both complementary bases which have been selected randomly by Alice and Bob with equal probabilities. One can easily verify that all the measurements performed during the verification test are equivalent to Bell measurements. Indeed, using the definition of the Bell states (7) the projector $\mathcal{P}_{j_i}$ can be written in the form

$$\mathcal{P}_{j_i} = \sum_{m,n \in \mathbb{F}_d} (1 - \delta_{m,0})|\Psi_{mn}\rangle\langle\Psi_{mn}|, \tag{13}$$

where $\delta_{m,0}$ is the Kronecker delta [44]. This last relation indicates that the verification test performed by Alice and Bob is nothing else than a quality-check test of the fidelity of the $2N$ pairs with respect to the ideal state $|\Psi_{00}\rangle^{\otimes 2N}$. Hence, classical sampling theory can be applied for the estimation of the average error rate and the establishment of confidence levels [4,7,10,20].

We can simplify further our discussion by taking into account the symmetry of the QKD protocol under any permutation of the pairs. As we discussed earlier, a random permutation of all the pairs at the beginning of the entanglement-based protocols ensures a homogeneous distribution of the errors introduced by a potential eavesdropper (Eve) over all the qudit pairs [10]. This is equivalent to saying that the eavesdropping attack is symmetric on all the pairs, and such a symmetrization argument is one of the key elements of

various unconditional security proofs [6,7,10,20]. Indeed, Eve does not know in advance which of the qudit pairs will be used for quality checks and which qudit pairs will contribute to the final key. Hence, she is not able to treat them differently and the check pairs constitute a classical random sample of all the pairs.

Invariance of the eavesdropping attack under any permutation of the pairs implies that all the reduced density operators describing the state of each pair shared between Alice and Bob are equal, i.e.,

$$\rho_{AB}^{(1)} = \rho_{AB}^{(2)} = \cdots = \rho_{AB}^{(2N)}, \tag{14}$$

where the reduced density operator of Alice's and Bob's kth pair is denoted by $\rho_{AB}^{(k)} = \mathrm{Tr}_{AB}^{(k)}(\rho_{AB})$, with $\mathrm{Tr}_{AB}^{(k)}$ indicating the tracing (averaging) procedure over all the qudit pairs except the kth one. It should be stressed that Eq. (14) does not at all imply that the overall reduced density operator ρ_{AB} of the $2N$ pairs itself, is a product state of all the reduced pair states $\rho_{AB}^{(k)}$. On the contrary, ρ_{AB} is expected to have a complicated structure as it includes all the effects arising from a general coherent (joint) attack of a possible eavesdropper.

In view of Eq. (14), the average disturbance defined in Eq. (11) is determined by the average error probability of an arbitrary qudit pair, say the pair j_1, i.e.,

$$D = \frac{1}{2}\sum_{b=0,1} \mathrm{Tr}_{A,B}^{(j_1)}\{[(\mathcal{H}_A^{b\dagger} \otimes \mathcal{H}_B^{b})\mathcal{P}(\mathcal{H}_A^{b} \otimes \mathcal{H}_B^{b\dagger})]_{j_1}\rho_{AB}^{(j_1)}\}, \tag{15}$$

where $\mathrm{Tr}_{A,B}^{(j_1)}$ denotes the tracing procedure over the j_1th qudit pair of Alice and Bob. In other words, the reduced single-pair state $\rho_{AB}^{(j_1)}$ contains all the information about the noisy quantum channel and a possible general coherent attack by an eavesdropper, which is relevant for the evaluation of the error rate. In particular, this implies that an arbitrary joint eavesdropping attack which gives rise to a particular state ρ_{AB} obeying Eq. (14) is indistinguishable, from the point of view of the estimated disturbance, from a corresponding collective attack which addresses each qudit individually and results in the $2N$-pair state of the form $\otimes_{j=1}^{2N}\rho_{AB}^{(j)}$, for example.

According to Eqs. (12) and (15) the average estimated disturbance is invariant under the transformations

$$(l,b) \to (l+m,b), \tag{16a}$$

$$(l,b) \to (l,b \oplus 1), \tag{16b}$$

with $m \in \mathbb{F}_d$, while $\oplus$ denotes addition modulo 2. This invariance implies that there are various reduced density operators of the j_1th qudit pair, which all give rise to the same observed value of the average disturbance. This can be seen from Eq. (9) which implies elementary relations of the form

$$\mathcal{E}_{mn}\mathcal{H}^b|j\rangle\langle j|(\mathcal{H}^b)^\dagger\mathcal{E}_{mn}^\dagger = \mathcal{H}^b|j+bn+(1-b)m\rangle\langle j+bn + (1-b)m|\mathcal{H}^{b\dagger}. \tag{17}$$

Together with the invariance of D under the transformations (16), these elementary relations imply that the reduced operators $\rho_{AB}^{(j_1)}$ and the symmetrized state

$$\tilde{\rho}_{AB}^{(j_1)} = \frac{1}{4d^2}\sum_{g\in\mathcal{G}_1, h\in\mathcal{G}_2} U(h)U(g)\rho_{AB}^{(j_1)}U(g)^\dagger U(h)^\dagger \tag{18}$$

give rise to the same value of D. Thereby, the unitary operators

$$U(g_{mn}) = \mathcal{E}_{mn;A} \otimes \mathcal{E}_{mn;B}^*, \tag{19}$$

$$U(h_1) = \mathbb{1}_A \otimes \mathbb{1}_B, \quad U(h_3) = (\mathcal{H}_A \otimes \mathcal{H}_B^*)^2,$$

$$U(h_2) = \mathcal{H}_A \otimes \mathcal{H}_B^*, \quad U(h_4) = (\mathcal{H}_A \otimes \mathcal{H}_B^*)^3, \tag{20}$$

have been introduced, which form unitary representations of two discrete Abelian groups $\mathcal{G}_1 = \{g_{00}, g_{01}, \ldots\}$ and $\mathcal{G}_2 = \{h_1, h_2, h_3, h_4\}$. The key point is now that, invariance of $\tilde{\rho}_{AB}^{(j_1)}$ under both of these groups is induced by the symmetry transformations (16) which leave D invariant.

V. ENTANGLEMENT DISTILLATION AND SECRET KEY

Having exploited the symmetries underlying the estimated disturbance, in this section we estimate the threshold disturbance that can, in principle, be tolerated by any $2d$-state QKD protocol, under the assumption of arbitrary coherent (joint) attacks. To this end, we make use of the *necessary precondition* for secret key distillation that is, the correlations established between Alice and Bob during the state distribution cannot be explained by a separable state [38].

Throughout this work, we consider that Alice and Bob focus on the sifted key during the post processing (i.e., they discard immediately all the polarization data for which they have used different bases) and that they treat each pair independently. Thus, according to the aforementioned precondition, given a particular value of the estimated disturbance D, the task of Alice and Bob is to infer whether their correlations may have originated from a separable state or not. So, our aim is to estimate the threshold disturbance D_{th} such that for any $D < D_{\mathrm{th}}$ Alice and Bob share provable entanglement with certainty. To this end, we proceed as follows. First, we estimate the regime of disturbances for which Alice and Bob share distillable entanglement. Second, we demonstrate that for the remaining regime of disturbances the correlations shared between Alice and Bob can always be described by a separable state.

A. Threshold disturbance

Adopting the entanglement-based version of the protocol defined in Sec. III C, let us estimate the regime of disturbances for which Alice and Bob share free entanglement. From the symmetries underlying the observed average error rate and in particular from Eq. (18) we have that the density operator $\rho_{AB}^{(j_1)}$ is freely entangled if $\tilde{\rho}_{AB}^{(j_1)}$ is freely entangled, as both states are related by local unitary operations and convex summation. Hence, to determine the values of the disturbance for which the real state $\rho_{AB}^{(j_1)}$ is distillable, it suffices to determine the disturbances for which the most general two-qubit state $\tilde{\rho}_{AB}^{(j_1)}$ (which is invariant under the discrete Abelian groups $\mathcal{G}_1$ and $\mathcal{G}_2$) is distillable.

TABLE I. The notation of the sets and the number of eigenvalues per set for even and odd dimensions.

	Number of sets		
Members per set	Even d	Odd d	Notation
1	2	1	ξ_j
2	1	0	ζ
4	$(d^2-4)/4$	$(d^2-1)/4$	η_j

We already know that the operators $U(g_{10}) \equiv \mathcal{X}_A \otimes \mathcal{X}_B^*$ and $U(g_{01}) \equiv \mathcal{Z}_A \otimes \mathcal{Z}_B^*$ of the group $\mathcal{G}_1$ constitute a *complete set of commuting operators* in $\mathbb{C}_A^d \otimes \mathbb{C}_B^d$, while their simultaneous eigenstates are the d^2 maximally entangled states defined in Eq. (7). Thus, the most general two-qudit state which is invariant under the Abelian group $\mathcal{G}_1$ is given, by a convex sum of all $|\Psi_{mn}\rangle$, i.e.,

$$\tilde{\rho}_{AB}^{(j_1)} = \sum_{m,n \in \mathbb{F}_d} \lambda_{mn} |\Psi_{mn}\rangle\langle\Psi_{mn}|, \tag{21}$$

where the non-negative parameters λ_{mn} have to satisfy the normalization condition

$$\sum_{m,n \in \mathbb{F}_d} \lambda_{mn} = 1. \tag{22}$$

Moreover, the operations $\mathcal{H}_A \otimes \mathcal{H}_B^*$, $(\mathcal{H}_A \otimes \mathcal{H}_B^*)^2$, and $(\mathcal{H}_A \otimes \mathcal{H}_B^*)^3$ transform Bell states into other Bell states. Thus, additional invariance of the quantum state (21) under the discrete group $\mathcal{G}_2$ implies that

$$\lambda_{m,n} = \lambda_{n,d-m} = \lambda_{d-m,d-n} = \lambda_{d-n,m}. \tag{23}$$

As a consequence of Eq. (23) there are different sets of identical parameters λ_{mn}. Each set j contains four members η_j unless the chain (23) is truncated. The latter case occurs for $d-m=m$ and $d-n=n$, i.e., for $m,n \in \{0, d/2\}$. More precisely, the sets j with $m=n \in \{0, d/2\}$ contain one eigenvalue ξ_j each, whereas the set with $m \neq n \in \{0, d/2\}$ has two equal eigenvalues denoted by ζ. From now on we distinguish between even and odd dimensions d. All the sets for both cases as well as their notation are summarized in Table I.

Given the various sets of eigenvalues, the normalization condition (22) now reads

$$\xi_0 + 4\sum_{j=1}^{\eta_{odd}} \eta_j = 1, \quad \text{odd } d,$$

$$\xi_0 + \xi_1 + 2\zeta + 4\sum_{j=1}^{\eta_{even}} \eta_j = 1, \quad \text{even } d, \tag{24}$$

where in both cases the index j runs over all the possible four-member groups, i.e., $\eta_{odd} \equiv (d^2-1)/4$ and $\eta_{even} \equiv (d^2-4)/4$ (see Table I). Similarly, using Eqs. (13), (15), and (21), the estimated average disturbance can be expressed in the form

$$D = 2\sum_{j=1}^{\lfloor d/2 \rfloor} \eta_j + 4\sum_{j=\lfloor d/2 \rfloor+1}^{\eta_{odd}} \eta_j, \quad \text{odd } d,$$

$$D = \xi_1 + \zeta + 2\sum_{j=1}^{d/2-1} \eta_j + 4\sum_{j=d/2}^{\eta_{even}} \eta_j, \quad \text{even } d, \tag{25}$$

with $\lfloor x \rfloor$ denoting the largest integer not greater than x, while all the parameters (disturbance and eigenvalues) are real valued and non-negative, i.e.,

$$0 \leqslant D, \xi_j, \zeta, \eta_j \leqslant 1.$$

Let us evaluate now the disturbances for which the state $\tilde{\rho}_{AB}^{(j_1)}$ is distillable. According to the reduction criterion [32], if $\tilde{\rho}_{AB}^{(j_1)}$ is separable, then

$$\tilde{\rho}_A^{(j_1)} \otimes \mathbb{1}_B - \tilde{\rho}_{AB}^{(j_1)} \geqslant 0 \tag{26}$$

(and also $\mathbb{1}_A \otimes \tilde{\rho}_B^{(j_1)} - \tilde{\rho}_{AB}^{(j_1)} \geqslant 0$), with $\tilde{\rho}_A^{(j_1)} \equiv \mathrm{Tr}_B(\tilde{\rho}_{AB}^{(j_1)})$. Using the explicit form of $\tilde{\rho}_{AB}^{(j_1)}$ given by Eq. (21) we have $\tilde{\rho}_A^{(j_1)} = \tilde{\rho}_B^{(j_1)} = \mathbb{1}_d/d$, where $\mathbb{1}_d$ denotes the unit operator in $\mathbb{C}_{A(B)}^d$. Thus inequality (26) reads

$$\sum_{m,n \in \mathbb{F}_d} \left(\frac{1}{d} - \lambda_{mn} \right) |\Psi_{mn}\rangle\langle\Psi_{mn}| \geqslant 0. \tag{27}$$

Violation of the above inequality (27) for any of the eigenvalues λ_{mn}, i.e.,

$$\lambda_{mn} > \frac{1}{d}, \tag{28}$$

is *sufficient* for distillability of the entanglement of $\tilde{\rho}_{AB}^{(j_1)}$ and implies violation of the Peres criterion (i.e., a nonpositive partial transpose) for this state [32,33]. In particular, as long as the fidelity f of $\tilde{\rho}_{AB}^{(j_1)}$ with respect to $|\Psi_{00}\rangle$ satisfies

$$f \equiv \langle\Psi_{00}|\tilde{\rho}_{AB}^{(j_1)}|\Psi_{00}\rangle > \frac{1}{d}, \tag{29}$$

the state can be distilled with the help of unitary twirling operations $\mathcal{U}_A \otimes \mathcal{U}_B^*$ which leave f invariant [32]. In our case, using Eqs. (21) and (23) the distillability condition (29) reads $\xi_0 > 1/d$ or equivalently

$$D < D_0 + 2\sum_{j=\lfloor d/2 \rfloor+1}^{\eta_{odd}} \eta_j, \quad \text{odd } d,$$

$$D < D_0 + \frac{1}{2}\xi_1 + 2\sum_{j=d/2}^{\eta_{even}} \eta_j, \quad \text{even } d, \tag{30}$$

where

$$D_0 \equiv \frac{d-1}{2d}. \tag{31}$$

According to these last inequalities, and given the fact that $\xi_j, \zeta, \eta_j \geqslant 0$, the threshold disturbance D_{th} for entanglement distillation at any dimension satisfies the inequality

$$D_{\mathrm{th}} \geqslant D_0, \tag{32}$$

with D_0 given by Eq. (31). For any $D < D_{\mathrm{th}}$, the symmetrized state $\tilde{\rho}_{AB}^{(j_1)}$ is always distillable (i.e., freely entangled). Given that $\rho_{AB}^{(j_1)}$ and $\tilde{\rho}_{AB}^{(j_1)}$ are related via local operarations and convex summation, the original state $\rho_{AB}^{(j_1)}$ must also be distillable in the same regime of disturbances.

Nevertheless, the fact that inequality (29) is not satisfied for $D \geqslant D_{\mathrm{th}}$ does not necessarily imply that the state $\tilde{\rho}_{AB}^{(j_1)}$ is not at all distillable for $D \geqslant D_{\mathrm{th}}$. For instance, there might exist another eigenvalue λ_{mn} (and not ξ_0) which satisfies inequality (28) [i.e., it violates inequality (26)] and this fact, according to the the reduction criterion, is also sufficient for distillability of $\tilde{\rho}_{AB}^{(j_1)}$ [32]. Hence, we must now evaluate the precise value of the threshold disturbance D_{th}.

One way to prove that strict equality holds in Eq. (32) for any $2d$-state QKD protocol is to demonstrate that for $D \geqslant D_0$, there always exist separable states which can describe Alice's and Bob's correlations and simultaneously are indistinguishable from the real bipartite state $\rho_{AB}^{(j_1)}$. To this end, let us focus on bipartite Bell-diagonal states, i.e., states which can be written in the form (21), and consider the following particularly simple family of such separable states:

$$\sigma_{AB}(D) = y \mathbb{1}_{d^2} + d|x-y| \sum_{k \in \mathbb{F}_d} \frac{(|k_A\rangle\langle k_A|) \otimes (|k_B\rangle\langle k_B|)}{d} + d|x-y| \sum_{i \in \mathbb{F}_d} (\tilde{\sigma}_A^{(i)} \otimes \tilde{\sigma}_B^{(i)}). \tag{33}$$

Thereby

$$x = \frac{1 + d(d-2)(1-D)}{d^2(d-1)},$$

$$y = \frac{1 + d(-1+2D)}{d^2(d-1)},$$

and

$$\tilde{\sigma}_C^{(i)} = \frac{1}{d} \sum_{k \in \mathbb{F}_d} |k_C\rangle\langle (k+i)_C|,$$

while $\mathbb{1}_{d^2}$ denotes the unit operator in $\mathbb{C}_A^d \otimes \mathbb{C}_B^d$.

This family is parametrized by the estimated average disturbance D detected by Alice and Bob and is valid for

$$\frac{d-1}{2d} = D_0 \leqslant D \leqslant \frac{2d-1}{2d}. \tag{34}$$

Moreover, any separable state which belongs to this family is indistinguishable, from the point of view of the estimated error rate, from the real state shared between Alice and Bob. In other words, whenever the detected disturbance D is within the interval (34), the correlations shared between Alice and Bob can be very well described in the framework of the family of seprable states $\sigma_{AB}(D)$. In such a case, the necessary precondition for secret key distillation is not met for disturbances within this regime, so that the protocol must be aborted.

So, we have proved that strict equality holds in (32) and thus, from Alice's and Bob's point of view, the threshold disturbance for entanglement distillation in the context of entanglement-based $2d$-state QKD protocols is

$$D_{\mathrm{th}} = \frac{d-1}{2d}. \tag{35}$$

In particular, if the detected average disturbance is below this threshold, the two legitimate users can be assured that they share freely entangled qudit pairs with high probability. In other words, under the assumption of general coherent attacks, for $D < D_{\mathrm{th}}$ Alice and Bob are always able to extract a secret key by application of a two-way EPP which purifies towards the maximally entangled state $|\Psi_{00}\rangle$. On the other hand, an estimated disturbance above $D_{\mathrm{th}} = (d-1)/2d$, does not allow Alice and Bob to infer whether the state they share is entangled or not. In particular, we have seen that there is at least one simple family of separable states which can describe Alice's and Bob's correlations up to high error rates of magnitude $(2d-1)/2d$. Finally, note that for $d=2$ we reveal the threshold disturbance for the standard BB84 QKD protocol, that is, $D_{\mathrm{th}} = 1/4$ [45]. Moreover, $D_{\mathrm{th}} \to 1/2$ for $d \to \infty$ reflecting the possible advantage of using higher-dimensional quantum systems as information carriers in quantum cryptography.

In view of the necessary precondition for secret key distillation [38], our results imply that D_{th} is also the ultimate upper security bound of any $2d$-state prepare-and-measure QKD protocol. Nevertheless, the details of a particular prepare-and-measure scheme (that is the error correction and privacy amplification protocols required) which will be capable of meeting this upper security bound remain an open question. In fact one has to specify a classical distillation (postprocessing) protocol which has the same bounds of tolerable noise as quantum-distillation protocols. It is worth mentioning, however, that the security bound (35) relies on certain conditions. In particular, it relies on the complete omission of any polarization data from the raw key that involve different bases for Alice and Bob, as well as on the individual manipulation of each pair during the postprocessing. If some of these conditions are changed, also the threshold disturbance may change.

Recently, under the same conditions, Acin *et al.* [25] derived another bound for entanglement distillation, namely,

$$D_{\mathrm{th}}^{(\mathrm{CM})} = 1 - \frac{1}{\sqrt{d}}. \tag{36}$$

As depicted in Fig. 1, $D_{\mathrm{th}}^{(\mathrm{CM})}$ is well above the threshold we have derived in this work for any dimension of the information carriers. The reason is basically that $D_{\mathrm{th}}^{(\mathrm{CM})}$ has been obtained under the additional assumption that Eve is restricted to so-called optimal incoherent attacks. These attacks rely on cloning machines and maximize Eve's information gain. One can easily verify, for example, that the class of separable states (33) is not optimal (in the sense of [25]). In our work we allow for arbitrary eavesdropping attacks and thus we have demonstrated that the distillation of a secret key for disturbances above D_{th} is impossible. So, although

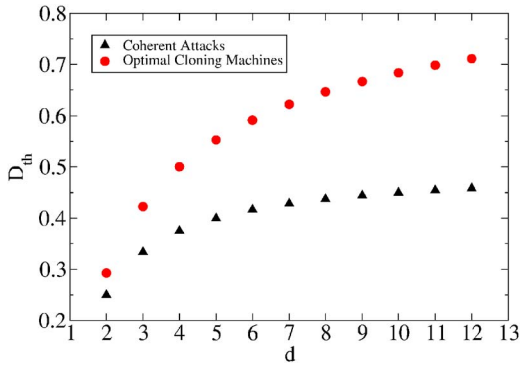

FIG. 1. (Color online) $2d$-state QKD protocols: The threshold disturbance for entanglement distillation as a function of dimension. The triangles refer to Eq. (35) and arbitrary coherent attacks whereas the circles correspond to Eq. (36) and optimal cloning machines.

the incoherent attacks considered in [25] are optimal with respect to the information gain of an eavesdropper, they are not able to disentangle Alice and Bob at the lowest possible disturbance. The cost of information loss that Eve has to accept by employing an attack that disentangles Alice and Bob at each particular disturbance above D_{th} remains an open question. Clearly, to this end one has to consider in detail the eavesdropping attack and this is beyond the purpose of this work.

A further issue ought to be brought up here in connection with the existence of bound entanglement. For $2\otimes 2$ systems (i.e., for the BB84 QKD protocol) nondistillability is equivalent to separability [34] and this fact seems to lead to a complete equivalence between entanglement distillation and secrecy [35]. However, for higher dimensions the situation is more involved due to the existence of bound entangled states with positive or nonpositive partial transpose [33,37]. Moreover, in a recent work [36] Horedecki *et al.* showed that a secret key can be distilled even from bound entangled states. As a consequence, a qudit-based (with $d>2$) QKD scheme could, in principle, go beyond entanglement distillation. However, this does not seem to be the case for the post processing and the protocols we consider throughout this work.

Indeed, for $D<D_{\text{th}}$ we have seen that the state shared between Alice and Bob is always distillable, i.e., it is freely entangled. Bound entangled states are expected to exist for $D\geqslant D_{\text{th}}$ and this is precisely the regime of parameters where the ideas presented in [36] can be used for the extraction of a secret key beyond entanglement distillation. We have demonstrated, however, that an eavesdropper is always able to break any entanglement between Alice and Bob for $D\geqslant D_{\text{th}}$ without being detected, by preparing, for example, a separable state from the family $\sigma_{AB}(D)$. As a consequence, according to [38], the protocol must be aborted at $D=D_{\text{th}}$. Under these circumstances, the extraction of a secret key beyond entanglement distillation seems to be practically impossible. The reason is basically that, based on the estimated error rate, Alice and Bob are incapable of verifying whether they share a separable state or not for disturbances above $D\geqslant D_{\text{th}}$. Alice and Bob can improve their situation only if they do not restrict themselves to the sifted data only. In particular, constructing appropriate entanglement witnesses from their raw data [38], Alice and Bob can verify whether they share a separable state or not, even for $D\geqslant D_{\text{th}}$.

Closing this section, let us briefly compare the performance of two different realizations of a six-state QKD protocol, namely, a three-basis scheme using qubits and a qutrit-based scheme using two out of four mutually unbiased bases. In principle, both protocols can tolerate precisely the same error rate, that is, $1/3$. Nevertheless, the qutrit-based protocol offers a higher yield since $1/2$ of the transmissions pass the sifting procedure (compared to $1/3$ for the qubit-based protocol). Thus, although both six-state protocols appear to be equally secure, the qutrit based scheme seems to be more efficient.

B. Examples

So far, our discussion involved arbitrary dimensions and general coherent attacks. For the sake of illustration, in this subsection we briefly discuss low dimensions (i.e., $d=2,3$) as well as symmetric (isotropic) channels [24,25] and arbitrary dimensions. In particular, we present evidence of the fact that for $d=3$ any eavesdropping strategy is equivalent to a symmetric one. However, for $d>3$ this equivalence does not seem to exist anymore. Moreover, we present numerical results for $d=3,4$, and 5, verifying the security bounds derived in the previous subsection.

1. Qubits

As a consequence of Eq. (23), for $d=2$ there are three different eigenvalues entering Eq. (21). So, in a matrix form we may write

$$\lambda_{mn}=\begin{pmatrix} u & x \\ x & y \end{pmatrix}, \tag{37}$$

with the eigenvalues u, x, and y satisfying the normalization condition $u+2x+y=1$. In this notation, the estimated disturbance can be expressed in the form $D=x+y$. One can easily verify that the state $\tilde{\rho}_{AB}^{(j_1)}$ is entangled for $1/4<D$ and $D>3/4$ [45]. Moreover, for $1/4\leqslant D\leqslant 3/4$ the state $\tilde{\rho}_{AB}^{(j_1)}$ is always separable and indistinguishable (as far as the estimated disturbance is concerned) from the real state $\rho_{AB}^{(j_1)}$ shared between Alice and Bob.

2. Qutrits

In analogy to qubits, applying Eq. (23) for $d=3$ and without any additional assumptions one finds that there are three different eigenvalues entering Eq. (21). In particular, the matrix of eigenvalues reads

$$\lambda_{mn}=\begin{pmatrix} u & x & x \\ x & y & y \\ x & y & y \end{pmatrix}, \tag{38}$$

while the average estimated disturbance is of the form $D=2x+4y$. Hence, taking into account the normalization condition $u+4(x+y)=1$, we have two real-valued and non-

negative independent parameters in the problem. Moreover, the partial transpose of $\tilde{\rho}_{AB}^{(j_1)}$ is block-diagonal with all three blocks being identical and equal to

$$M_3 = \frac{1}{3}\begin{pmatrix} u+2x & x-y & x-y \\ x-y & x+2y & u-x \\ x-y & u-x & x+2y \end{pmatrix}. \tag{39}$$

Hence, the following two eigenvalues:

$$\nu_1 = \frac{1}{3}(-u+2x+2y),$$

$$\nu_2 = \frac{1}{3}[u+x+y-\sqrt{3}(x-y)]$$

determine the sign of the partial transpose of $\tilde{\rho}_{AB}^{(j_1)}$. Related numerical results will be presented below.

3. Isotropic quantum channels

For $d>3$ the number of independent parameters in the problem increases enormously with d, e.g., for $d=4$ we have

$$\lambda_{mn} = \begin{pmatrix} \xi_0 & \eta_1 & \zeta & \eta_1 \\ \eta_1 & \eta_2 & \eta_3 & \eta_2 \\ \zeta & \eta_3 & \xi_1 & \eta_3 \\ \eta_1 & \eta_2 & \eta_3 & \eta_2 \end{pmatrix}. \tag{40}$$

However, the situation becomes tractable in the case of isotropic channels (e.g., open-space QKD) where disturbances involving different errors [46] are equal, thus leading to an eigenvalue matrix of the form [22,24,25]

$$\lambda_{mn} = \begin{pmatrix} u & x & \cdots & x \\ x & y & \cdots & y \\ \vdots & \vdots & \ddots & \vdots \\ x & y & \cdots & y \end{pmatrix} \tag{41}$$

for any dimension d.

In the case of qubits, such an isotropy argument does not seem to be a restriction. Thus, any eavesdropping strategy is equivalent to a symmetric (i.e., isotropic) one [47]. This might be due to the fact that such a symmetry arises automatically as an inherent property of the qubit-based QKD protocols [the matrix (37) is of the form (41)]. As a consequence, one is always able to substitute any eavesdropping attack with a symmetric one which yields the same results for all the properties which are defined as averages over all the possible messages sent by Alice to Bob (e.g., estimated disturbance) [47]. Besides, here we see that the symmetry (isotropy) arises automatically for qutrits [the matrix (38) is of the form (41)] and thus similar arguments must hold for $d=3$ as well. Nevertheless, we have found that for $d>3$ this symmetry does not exist [see for instance Eq. (40) for $d=4$] and one has to apply it explicitly. Hence, unless the quantum channel itself is isotropic, a restriction to symmetric eavesdropping strategies for $d>3$ seems unreasonable and might, in general, underestimate Eve's power. However, in our case such a restriction does not seem to affect the threshold disturbance, while simultaneously enabling us to present numerical results regarding $2d$-state QKD protocols with $d>3$.

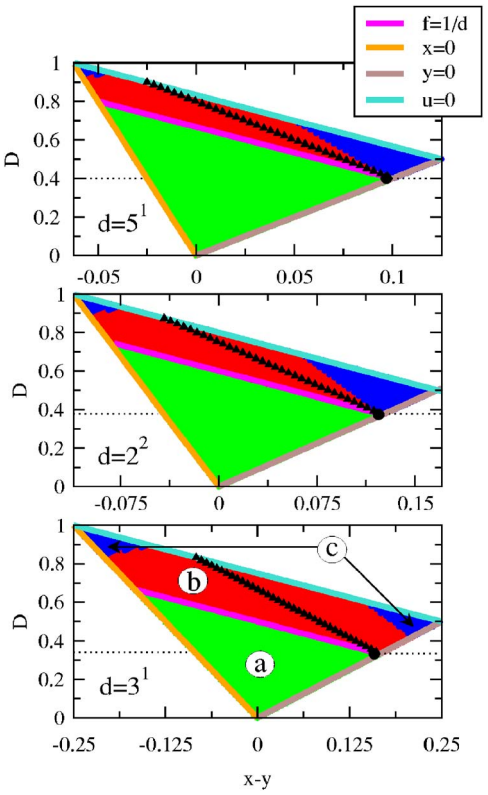

FIG. 2. (Color online) $2d$-state QKD protocols: The regions of the independent parameters D and $x-y$ for which the qudit-pair state $\tilde{\rho}_{AB}^{(j_1)}$ is (a) NPPT and distillable; (b) PPT; (c) NPPT but the reduction criterion is satisfied. From the top to the bottom, the "distillability maps" correspond to $d=5$, 4, and 3, respectively. The non-negativity of x, y, and u (straight lines) defines the region of parameters where the protocols operate while the distillability condition (29) separates distillable from nondistillable states. The threshold disturbances for entanglement distillation are indicated by black dots. The triangles correspond to the separable state (33). Note the different scales of the horizontal axis.

So, using the matrix (41), the normalization condition (22) reads

$$u+2(d-1)x+(d-1)^2y=1,$$

and only two of the three parameters (u,x,y) are independent. Moreover, combining Eqs. (13), (15), and (21) we have that the average estimated disturbance is given by

$$D=(d-1)x+(d-1)^2y.$$

Finally, in analogy to the case of qutrits, the partial transpose of $\tilde{\rho}_{AB}^{(j_1)}$ is block diagonal with each block being a $d\times d$ matrix. For odd dimensions all the blocks are identical whereas for even dimensions two different blocks appear.

4. Numerical results and discussion

We have been able to test the results of Sec. V A numerically for qutrits, while for higher dimensions we had to resort

to the assumption of isotropic quantum channels, to reduce the number of independent parameters in our simulations. More precisely, fixing two independent parameters, say D and $x-y$, we evaluated all the remaining parameters u,x,y which are consistent with all the constraints. Subsequently, for the parameters at hand we checked whether the distillability condition (28) is satisfied and whether the two-qudit state $\tilde{\rho}_{AB}^{(j_1)}$ has a nonpositive partial transpose (NPPT). The corresponding "distillability maps" for $d=3,4,5$ are presented in Fig. 2.

Our simulations confirm the validity of

$$D_{\text{th}} = \frac{d-1}{2d}$$

as the ultimate robustness bound for $2d$-state QKD protocols. More precisely, for $D<D_{\text{th}}$ Alice and Bob share always freely entangled qudit pairs (regime a in Fig. 2). On the contrary, for $D \geqslant D_{\text{th}}$ we can identify two different regimes of parameters. The dominant regime b involves parameters which yield a $\tilde{\rho}_{AB}^{(j_1)}$ with (PPT). These states can not be distilled and are either separable or bound entangled [33,37]. Besides, we have the regime of parameters c, for which $\tilde{\rho}_{AB}^{(j_1)}$ has a NPPT but the reduction criterion is not violated. These states probably belong to the hypothetical set of bound entangled states with NPPT [32,33]. At this point, it could be argued that $D \geqslant D_{\text{th}}$ is the regime of parameters where the ideas of Horodecki *et al.* might be applicable for the distillation of a secret key from bound entangled states [36]. To this end, however, Alice and Bob have to confirm whether the state they share is indeed bound entangled. Such an identification is only possible with the help of appropriate additional entanglement witnesses constructed from the polarization data of the raw key [38].

VI. CONCLUSIONS

We have discussed the robustness of qudit-based QKD protocols that use two mutually unbiased bases, under the assumption of general coherent (joint) attacks. For $d=3$ (i.e., for qutrits), we have presented evidence of the fact that any eavesdropping strategy is equivalent to a symmetric one, while for higher dimensions this equivalence is no longer valid.

The lowest possible disentanglement bound that an eavesdropper can saturate in the context of these cryptographic protocols scales with dimension as $(d-1)/2d$. Whenever Alice and Bob detect disturbances above $(d-1)/2d$, they are not able to infer whether their correlations originate from an entangled state or not, and the protocol must be aborted. On the contrary, if the detected disturbance is below $(d-1)/2d$, the two honest parties can be confident that they share free entanglement with high probability and the extraction of a secret key is, in principle, possible.

In particular, for the entanglement-based version of the protocols such a secure key can be obtained after applying an appropriate EPP which purifies the qudit pairs shared between Alice and Bob towards $|\Psi_{00}\rangle$ [29–32]. Moreover, in view of the fundamental role of entanglement in secret key distribution [38], the development of qudit-based prepare-and-measure schemes that can tolerate bit error rates up to $(d-1)/2d$ is also possible. For this purpose, however, the construction of additional appropriate two-way EPPs which are consistent with the associated prepare-and-measure schemes seems to be of vital importance. Our results generalize the results of [25] to arbitrary coherent attacks and simultaneously answer (to some extent) many of the open issues raised in the concluding remarks of that paper.

Finally, it should be stressed that the disturbance thresholds we have obtained depend on the postprocessing of the QKD protocol. In particular, they rely on the complete omission of those qudits of the raw key for which Alice and Bob measured in different bases. Furthermore, they also rely on the fact that Alice and Bob manipulate each qudit pair separately. Under these conditions, we have demonstrated that the extraction of a secret key from bound entangled states is impossible in the framework of qudit-based QKD protocols that use two mutually unbiased bases.

ACKNOWLEDGMENTS

Stimulating discussions with Markus Grassl and Antonio Acin are gratefully acknowledged. This work is supported by the EU within the IP SECOQC.

[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), p. 175.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); C. H. Bennett, *ibid.* **68**, 3121 (1992); D. Bruss, *ibid.* **81**, 3018 (1998); W.-Y. Hwang, *ibid.* **91**, 057901 (2003); V. Scarani, A. Acin, G. Ribordy, and N. Gisin, *ibid.* **92**, 057901 (2004).
[3] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[4] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[5] D. Mayers, J. ACM **48**, 351 (2001); M. Christadl, A. Ekert, and R. Renner, e-print quant-ph/0402131.
[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000); K. Tamaki, M. Koashi, and N. Imoto, *ibid.* **90**, 167904 (2003); M. Koashi, *ibid.* **93**, 120501 (2004).
[7] H.-K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004); H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017.
[9] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001); K. Tamaki and N. Lütkenhaus, *ibid.* **69**, 032316 (2004).
[10] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003); H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[12] D. Stucki *et al.*, New J. Phys. **4**, 41 (2002).

[13] S. Fasel, N. Gisin, G. Ribordy, and H. Zbinden, Eur. Phys. J. D **30**, 143 (2004); A. Poppe *et al.*, quant-ph/0404115.
[14] C. Kurtsiefer *et al.*, Nature (London) **419**, 450 (2002); R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).
[15] A. Trifonov *et al.*, J. Opt. B: Quantum Semiclassical Opt. **2**, 105 (2000); G. A. Maslennikov, A. A. Zhukov, M. V. Chekhova, and S. P. Kulik, *ibid.* **5**, S530 (2003).
[16] R. Thew, A. Acin, H. Zbinden, and N. Gisin, Quantum Inf. Comput. **4**, 93 (2004); H. de Riedmatten, I. Marcikic, H. Zbinden, and N. Gisin, *ibid.* **2**, 425 (2002).
[17] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **69**, 050304(R) (2004); A. Vaziri, G. Weihs, and A. Zeilinger, Phys. Rev. Lett. **89**, 240401 (2002).
[18] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).
[19] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan, Algorithmica **34**, 512 (2002).
[20] H. F. Chau, IEEE Trans. Inf. Theory **51**, 1451, 2005; e-print quant-ph/0212055.
[21] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000); D. Bruss and C. Macchiavello, *ibid.* **88**, 127901 (2002).
[22] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000); T. Durt, N. J. Cerf, N. Gisin, and M. Zukowski, *ibid.* **67**, 012311 (2003); T. Durt and B. Nagler, *ibid.* **68**, 042323 (2003).
[23] T. Durt, D. Kaszlikowski, J.-L. Chen, and L. C. Kwek, Phys. Rev. A **69**, 032313 (2004); V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, *ibid.* **65**, 052331 (2002).
[24] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002); M. Burennane *et al.*, J. Phys. A **35**, 10065 (2002).
[25] A. Acin, N. Gisin, and V. Scarani, Quantum Inf. Comput. **3**, 563 (2003).
[26] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **IT-24**, 339 (1978); C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, *ibid.* **41**, 1915 (1995).
[27] G. Brassard and L. Salvail, *Advances in Cryptology–EUROCRYPT'93*, Lecture Notes in Computer Science Vol. 765, edited by T. Helleseth (Springer, Berlin, 1994), p. 410.
[28] U. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).
[29] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[30] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996); C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996).
[31] G. Alber, A. Delgado, N. Gisin, and I. Jex, J. Phys. A **34**, 8821 (2001).
[32] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
[33] M. Lewenstein *et al.*, J. Mod. Opt. **47**, 2481 (2000).
[34] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996); M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 8 (1996).
[35] A. Acin, L. Masanes, and N. Gisin, Phys. Rev. Lett. **91**, 167901 (2003).
[36] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[37] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **80**, 5239 (1998).
[38] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2003); M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005); A. Acin and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[39] However, it is worth noting that many of the subesequent arguments are also valid for dimensions which are not prime powers.
[40] F. J. MacWilliams and N. J. A. Slone, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1997).
[41] A. Klappenecker and M. Rötteler, IEEE Trans. Inf. Theory **48**, 2392 (2002); A. Ashikhmin and E. Knill, *ibid.* **47**, 3065 (2001); E. Knill, e-print quant-ph/9608048.
[42] It is worth noting that a logarithmic scaling of the size of the random sample with the length of Alice's and Bob's key, is sufficient for security issues. See Ref. [20] for a rigorous proof.
[43] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[44] Clearly, the kets and bras here refer to the j_ith check pair. In order not to overload notation, however, we have dropped the indices j_i on the left-hand side of this equation.
[45] G. M. Nikolopoulos and G. Alber, e-print quant-ph/0403148.
[46] In general, as is clearly reflected in the projector (12), the qudit state $|l_B\rangle$ sent from Alice to Bob may undergo $d-1$ different "dit-flip" errors, i.e., $|l_B\rangle \rightarrow |(l+k)_B\rangle$ with $k \in \mathbb{F}_d^*$. In particular, if d is prime, then $k \in \{1,2,\ldots,d-1\}$.
[47] J. I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997); C. A. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).