Error tolerance of two-basis quantum-key-distribution protocols using qudits and two-way classical communication

Georgios M. Nikolopoulos, Kedar S. Ranade, and Gernot Alber
Institut für Angewandte Physik, Technische Universität Darmstadt, 64289 Darmstadt, Germany
(Received 12 December 2005; published 17 March 2006)

We investigate the error tolerance of quantum cryptographic protocols using d-level systems. In particular, we focus on prepare-and-measure schemes that use two mutually unbiased bases and a key-distillation procedure with two-way classical communication. For arbitrary quantum channels, we obtain a sufficient condition for secret-key distillation which, in the case of isotropic quantum channels, yields an analytic expression for the maximally tolerable error rate of the cryptographic protocols under consideration. The difference between the tolerable error rate and its theoretical upper bound tends slowly to zero for sufficiently large dimensions of the information carriers.

DOI: 10.1103/PhysRevA.73.032325 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Provable entanglement has been shown to be a necessary precondition for secure quantum key-distribution (QKD) in the context of any protocol [1,2]. Recently [3], we investigated the maximal average disturbance (error rate) up to which the two legitimate users (Alice and Bob) of a QKD protocol can prove the presence of quantum correlations in their sifted classical data. In particular, we focused on qudit-based QKD protocols using two Fourier-dual bases (to be referred to hereafter as $2d$-state protocols). Under the assumption of arbitrary joint (coherent) attacks, we showed that the threshold disturbance for provable entanglement scales with the qudit-dimension d as

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

This theoretical upper bound on tolerable error rates for $2d$-state protocols is valid for arbitrary dimensions, provided that Alice and Bob focus on their sifted key and do not apply any collective measurements on their halves. Its implications are obvious for estimated disturbances above D_{th}, namely, Alice and Bob are not able to infer whether the correlations in their data have originated from an entangled state or not, and the protocol must be aborted. However, for detected disturbances below D_{th}, the picture is incomplete. In particular, based on the above result we only know that the two honest parties can be confident that they share provable entanglement with high probability. Thus, the necessary precondition for secret-key distillation is satisfied for disturbances up to D_{th}. Nevertheless, the details of a prepare-and-measure (P&M) scheme which will be capable of attaining this theoretical bound are unknown. In fact, it is not at all clear whether such a P&M scheme exists.

So far, the highest tolerable error rates in the framework of P&M QKD schemes have been reported for protocols using a two-way Gottesman-Lo-type procedure for key distillation [4]. This procedure was introduced and improved in the context of the standard qubit-based ($d=2$) QKD protocols [4,5]. It is based on local quantum operations and two-way classical communication (LOCC2) and is able to provide the two legitimate users with an unconditionally secure key up to high error rates. In particular, for the standard four-state qubit-based protocol [Bennett-Brassard 1984 (BB84)], the tolerable error rate is 20% [5,6], which is well below the corresponding theoretical upper bound given by Eq. (1), that is, 25%. The natural question arises, therefore, whether this gap still persists for higher dimensions ($d>2$) and, in particular, how it scales with the dimension d of information carriers.

Recently, extending the Gottesman-Lo two-way key distillation (GL2KD) procedure to higher dimensions, Chau addressed this open question in the context of fully symmetric qudit-based QKD schemes using all $(d+1)$ possible mutually unbiased bases [7]. More precisely, he showed that if d is a prime power, the tolerable error rate scales with dimension as $1-(3+\sqrt{5})/2d$, for $d\to\infty$.

In this paper, our purpose is to analyze the error tolerance of $2d$-state QKD protocols using a GL2KD process. In contrast to the protocols considered in [7], the protocols considered here are not necessarily fully symmetric. In general, we have only one symmetry constraint, i.e., the symmetry between the two Fourier-dual bases used in the protocol. Hence, the problem in its most general form is analytically solvable to some extent only. Specifically, we are able to derive a sufficient condition for secret-key distillation in which the number of open parameters scales quadratically with d. However, the derivation of an analytic expression for the tolerable error rate is possible under additional symmetry assumptions related to isotropic quantum channels. In this case, we find that the asymptotic $(d\to\infty)$ tolerable error rate scales with dimension as $1/2-1/4\sqrt{d}$, and slowly approaches, therefore, its theoretical upper bound determined by Eq. (1), that is, $1/2$.

The organization of the paper follows the three phases of a typical P&M QKD scheme. In Sec. II, for the sake of completeness we briefly summarize basic facts about the first two phases of a $2d$-state QKD protocol, i.e., quantum state distribution and verification test. Subsequently, in Sec. III we focus on the key-distillation phase which is the main subject of this work. In particular, we consider a GL2KD procedure. Our analysis is based on the entanglement-based version of

the $2d$-state QKD protocol, whose reduction to a P&M scheme is summarized at the end of the section. An analytic expression for the tolerable error rate is derived in Sec. IV under the assumption of isotropic quantum channels. Finally, we conclude with a short summary and outlook in Sec. V.

II. THE FIRST TWO STAGES OF TWO-BASIS QKD PROTOCOLS

For the sake of simplicity, and without loss of generality, we will focus on prime dimensions only. Thus, throughout this work all the arithmetics are performed in the finite (Galois) field $\mathbb{F}_d=\{0,1,\ldots,d-1\}$ [8]. It has to be noted, however, that similar arguments hold if d is a prime power but the formalism is more involved (e.g., see [3]).

In general, theoretical investigations of d-level quantum systems (qudits) are performed conveniently with the help of the generalized Pauli operators

$$\mathfrak{A}_{mn} := \sum_{l\in\mathbb{F}_d} \Phi(ln)|l-m\rangle\langle l| \quad \text{for } m,n \in \mathbb{F}_d, \tag{2}$$

where $\Phi(x)\equiv\exp(\mathrm{i}2\pi x/d)$. These d^2 operators form a faithful projective unitary representation of $(\mathbb{Z}\backslash d\mathbb{Z})\times(\mathbb{Z}\backslash d\mathbb{Z})$ and an error basis on the Hilbert space of a qudit $\mathbb{C}^d$ [9].

In a typical $2d$-state P&M scheme, Alice and Bob use for their purposes two mutually unbiased bases. Following [3,10,11], throughout this work we choose the eigenbasis $\{|\alpha\rangle:\alpha\in\mathbb{F}_d\}$ of $\mathfrak{A}_{01}$ as the standard (computational) basis $\mathcal{B}_1$, while the second basis $\mathcal{B}_2$ is the Fourier dual of the computational basis with the discrete Fourier transformation given by

$$\mathfrak{F} := \frac{1}{\sqrt{d}} \sum_{i,j\in\mathbb{F}_d} \Phi(ij)|i\rangle\langle j|.$$

Hence, the indices m and n in Eq. (2) refer to dit-flip and phase errors in the standard basis $\mathcal{B}_1$, respectively. Moreover, $\mathfrak{F}^\dagger\mathfrak{A}_{mn}\mathfrak{F}=\Phi(-mn)\mathfrak{A}_{nm}^*$, which indicates that dit-flip errors in the computational basis become phase errors in the complementary basis and vice versa.

In general, the first stage of a QKD protocol is the quantum state distribution stage which involves quantum state (signal) preparation and transmission via an insecure quantum channel. The purpose of this phase is to establish correlations between Alice and Bob, which may also involve correlations with a third untrusted party (eavesdropper). As far as a typical $2d$-state P&M scheme is concerned, this first stage proceeds as follows [3,7,10,11]. Alice sends to Bob a sequence of qudits each of which is randomly prepared in one of the $2d$ nonorthogonal basis states (d states for each basis). Bob measures each received particle randomly in $\mathcal{B}_1$ or $\mathcal{B}_2$. Alice and Bob publicly discuss the bases chosen, discarding all the dits where they have selected different bases (sifting).

Generalizing the ideas presented in [12], the aforementioned state-distribution process can be viewed as follows [3,7,10,11]. Alice prepares each of $N\gg 1$ entangled-qudit pairs in the maximally entangled state $|\Psi_{00}\rangle$. Thereby, the generalized maximally entangled states in the Hilbert space of two distinguishable qudits $\mathbb{C}_\mathrm{A}^d\otimes\mathbb{C}_\mathrm{B}^d$ are defined as $|\Psi_{mn}\rangle := \Sigma_{j\in\mathbb{F}_d}|j_\mathrm{A}\rangle\otimes\mathfrak{A}_{mn}^{(\mathrm{B})}|j_\mathrm{B}\rangle/\sqrt{d}$, where from now on the subscripts A and B refer to Alice and Bob, respectively [7,10,11,13,14]. Alice keeps half of each pair and submits the other half to Bob after having applied at random and independently a unitary transformation chosen from the set $\{\mathbb{1},\mathfrak{F}\}$. As soon as Bob receives the particles, he acknowledges the fact and applies at random $\mathbb{1}$ or $\mathfrak{F}^{-1}$ on each qudit independently. Alice reveals the sequence of operations she performed, and all the pairs which involve different operations on the transmitted qudit are discarded. This is the associated entanglement-based (EB) version of the $2d$-state QKD protocol and offers many advantages, in particular with respect to security issues and error tolerance.

The second stage of the QKD protocol is the verification test (also called signal-quality test) which we discussed in detail elsewhere [3]. In this stage, the two legitimate users sacrifice part of their (quantum) signal in order to quantify the eavesdropping rate during the transmission stage. More precisely, after a random permutation of their sifted (qu)dit pairs, Alice and Bob randomly select a sufficiently large number of them and determine their average error probability (disturbance). If as a result of a noisy quantum channel (from now on all the noise in the channel is attributed to eavesdropping) the estimated disturbance is too high, the protocol is aborted. Otherwise, Alice and Bob proceed to the key-distillation phase, which will be discussed in detail in the following section.

At any rate, it is always worth keeping in mind that the success of the verification test (and thus security) relies on two key points. First, an eavesdropper does not know in advance which qudit-pairs will be chosen for quality checks and which qudit-pairs will contribute to the final key. Second, any joint eavesdropping attack can be reduced to a classical (probabilistic) cheating strategy for which classical sampling theory can be safely applied [4,7,15,16].

In particular, the action of the quantum channel can be regarded as a Pauli one [4,7]. At the end of the distribution stage of the $2d$-state protocol, each transmitted qudit may have undergone any of the d^2 possible types of errors $\mathfrak{A}_{mn}$. Let p_{mn} denote the rate (probability) of errors of the form $\mathfrak{A}_{mn}$ in the particles shared between Alice and Bob, with

$$\sum_{m,n\in\mathbb{F}_d} p_{mn} = 1. \tag{3}$$

In general, any symmetries underlying the QKD protocol under consideration may imply additional constraints on p_{mn}. For the protocols under consideration, both Fourier-dual bases are used at random and independently on each qudit-pair during the transmission. Moreover, the choices of the bases are not known to an eavesdropper, and they are publicly announced only after all the particles are in Bob's possession. Thus, as a result of the symmetry between the two bases, the quantum channel connecting Alice and Bob yields different sets of identical error probabilities [3]. In particular, we have that

$$p_{mn} = p_{n,d-m} = p_{d-m,d-n} = p_{d-n,m}, \quad \forall\ m,n \in \mathbb{F}_d. \tag{4}$$

Note that in highly symmetric protocols, the corresponding symmetry between all $(d+1)$ mutually unbiased bases leads to a depolarizing quantum channel with $p_{mn}=p_{01}$ for all $(m,n)\neq(0,0)$ [7].

In view of the symmetries (4), the estimated disturbance during the verification test is given by [3]

$$D = \sum_{m\in\mathbb{F}_d^*} p_{m0} + \sum_{m\in\mathbb{F}_d^*}\sum_{n\in\mathbb{F}_d^*} p_{mn}, \tag{5}$$

where $\mathbb{F}_d^* := \mathbb{F}_d \backslash \{0\}$. This estimated error rate should not be confused with the so-called quantum-channel (overall) error rate $Q=1-p_{00}$, which is not estimable in a typical verification test of a P&M $2d$-state QKD protocol.

At this point, we have all the necessary formalism and we turn to investigate the error tolerance of $2d$-state P&M protocols.

III. ANALYSIS OF THE TWO-WAY KEY DISTILLATION

Throughout this work, we focus on the GL2KD procedure in the context of which the highest tolerable error rates have been reported for various P&M QKD schemes [4,5,7]. Our purpose is to investigate the conditions under which an insecure quantum channel allows the distillation of a secret key in the context of $2d$-state QKD protocols and the GL2KD procedure. Such an analysis can be performed conveniently in the EB version of the protocols we described in the previous section and adopt from now on. We will close this section with the reduction of the EB scheme to a P&M one.

A. Dit-flip error rejection (DER)

As any other key-distillation process, the GL2KD has two stages [4,5,7]. The first stage is a typical two-way entanglement purification with LOCC2 [13,14,17,18]. More precisely, in order to reduce the dit-flip-error rate in their signal, Alice and Bob apply a number of D-steps. In each D-step, they form tetrads of particles by randomly pairing up their qudit-pairs. Then, within each tetrad of particles they apply a bilateral exclusive OR (BXOR) operation. Specifically, Alice and Bob individually apply to their halves the unitary operation [13,14]

$$\mathrm{XOR}_{\mathrm{c}\to\mathrm{t}}: |x\rangle_{\mathrm{c}} \otimes |y\rangle_{\mathrm{t}} \mapsto |x\rangle_{\mathrm{c}} \otimes |x-y\rangle_{\mathrm{t}}, \tag{6}$$

where c and t denote the control and target qudit, respectively. Subsequently, they measure their target qudits in the computational basis and compare their outcomes. The control qudit-pair is kept if and only if their outcomes agree, while the target pair is always discarded.

In general, this procedure is repeated many times (many rounds of D-step) until the dit-flip-error rate in the surviving qudit-pairs is sufficiently low to guarantee an arbitrarily small total error rate at the end of the key-distillation protocol. We are going to make this statement more precise later on. For the time being, we turn to analyze the effect of the D-steps on the signal shared between Alice and Bob.

Following [4,5,7], our analysis will be based on classical probability arguments since any eavesdropping attack can be reduced to a classical probabilistic one. In particular, let $S=\{p_{mn}|m,n\in\mathbb{F}_d\}$ be the set of error rates (error-probability distribution) at the beginning of DER (i.e., at the end of the first stage of the QKD protocol). It has been shown [14] that the effect of k rounds of D-step (with $k\in\mathbb{N}$) on S can be identified by a mapping $\mathcal{D}_k: S\mapsto S_k$, where $S_k=\{p_{mn}^{(k)}|m,n\in\mathbb{F}_d\}$ and

$$p_{mn}^{(k)} = \frac{\sum_{l\in\mathbb{F}_d}\Phi(-nl)\left[\sum_{j\in\mathbb{F}_d}\Phi(lj)p_{mj}\right]^{2^k}}{d\sum_{i\in\mathbb{F}_d}\left(\sum_{j\in\mathbb{F}_d}p_{ij}\right)^{2^k}}. \tag{7}$$

One can readily check that by setting $d=2$, this mapping reduces to the well-known mapping for qubit-based protocols [4,5].

Clearly, $p_{mn}^{(k)*}=p_{mn}^{(k)}$ since the summations in Eq. (7) run over all the finite field $\mathbb{F}_d$. Furthermore, for the same reason, Eq. (7) can be rewritten as

$$p_{mn}^{(k)} = \frac{[C(m)]^{2^k} + \sum_{l\in\mathbb{F}_d^*}\Phi(-ln)[A(m,l)]^{2^k}}{d[1+\sum_{l\in\mathbb{F}_d^*}[C(l)]^{2^k}]}, \tag{8}$$

where

$$A(m,l) = \frac{\sum_{j\in\mathbb{F}_d}\Phi(lj)p_{mj}}{\sum_{j\in\mathbb{F}_d}p_{0j}}, \tag{9a}$$

$$C(m) = \frac{\sum_{j\in\mathbb{F}_d}p_{mj}}{\sum_{j\in\mathbb{F}_d}p_{0j}}, \tag{9b}$$

for $m,l\in\mathbb{F}_d$.

From now on we restrict ourselves to estimated disturbances $D<D_{\mathrm{th}}$, since for $D\geqslant D_{\mathrm{th}}$ Alice and Bob do not share provable entanglement [3–5]. Furthermore, for $D<D_{\mathrm{th}}$ we also have

$$\sum_{n\in\mathbb{F}_d} p_{0n} > \sum_{n\in\mathbb{F}_d} p_{mn} \quad \forall\ m\in\mathbb{F}_d^*, \tag{10}$$

which implies that $0\leqslant C(m)<1, \forall\, m\in\mathbb{F}_d$. Besides, a necessary condition for $0\leqslant p_{mn}^{(k)}\leqslant 1$ after many rounds of D-step is $|A(m,l)|<1$ for all $m,l\in\mathbb{F}_d$. Thus, as $k\to\infty$, we have $|A|^{2^k}\to 0$ and $|C|^{2^k}\to 0$, which imply that $p_{0n}^{(k)}\to 1/d$ and $p_{mn}^{(k)}\to 0$ for $m,n\in\mathbb{F}_d$ and $m\neq 0$. In other words, the main effect of DER on the surviving particles shared between Alice and Bob is to reduce errors of the form $\mathfrak{A}_{mn}$ with $m\neq 0$, while increasing the rate of pure phase errors of the form $\mathfrak{A}_{0n}$with $n\neq 0$.

In particular, let

$$R_{\mathrm{D}}^{(k)} = \sum_{m\in\mathbb{F}_d^*}\sum_{n\in\mathbb{F}_d} p_{mn}^{(k)} \tag{11a}$$

and

$$R_{\mathrm{P}}^{(k)} = \sum_{m\in\mathbb{F}_d} \sum_{n\in\mathbb{F}_d^*} p_{mn}^{(k)} \equiv \sum_{n\in\mathbb{F}_d^*} q_n^{(k)} \tag{11b}$$

be the total dit-flip and phase-error rates after k rounds of D-step, respectively. In general, as $k\to\infty$, $R_{\mathrm{D}}^{(k)}\to 0$ whereas $R_{\mathrm{P}}^{(k)}\to(d-1)/d$. We must therefore have a closer look at the corresponding individual phase-error rates $q_n^{(k)}$ which, using Eq. (8), are given by

$$q_n^{(k)} = \sum_{m\in\mathbb{F}_d} p_{mn}^{(k)} = \frac{1}{d} + \frac{\xi_n^{(k)}}{d[1+\chi^{(k)}]} \tag{12}$$

for all $n\in\mathbb{F}_d$, where

$$\xi_n^{(k)} = \sum_{m\in\mathbb{F}_d} \sum_{l\in\mathbb{F}_d^*} \Phi(-ln)[A(m,l)]^{2^k}, \tag{13a}$$

$$\chi^{(k)} = \sum_{m\in\mathbb{F}_d^*} [C(m)]^{2^k}. \tag{13b}$$

Clearly, the parameters $\xi_n^{(k)}$ and $\chi^{(k)}$ also take arbitrarily small values as $k\to\infty$, since $|A|^{2^k}\to 0$ and $|C|^{2^k}\to 0$.

Observation 1. The phase-error rates after k rounds of D-step satisfy the inequality

$$q_0^{(k)} > q_n^{(k)} \quad \forall\, n\in\mathbb{F}_d^*, \tag{14}$$

where $q_0^{(k)}$ is the no-phase-error probability.

Proof. First of all, recall that throughout this work we assume prime dimensions only. Starting from Eq. (12), we have to show that $\xi_0^{(k)} > \xi_n^{(k)}$ for all $n\neq 0$. Using the symmetry condition (4), Eq. (13a) reads

$$\xi_n^{(k)} = \frac{2\sum_{m=0}^{\lfloor d/2\rfloor}\sum_{l=1}^{\lfloor d/2\rfloor}\cos(ln)T(m,l)}{\left[\sum_{j\in\mathbb{F}_d} p_{0j}\right]^{2^k}} \quad \forall\, n\in\mathbb{F}_d, \tag{15}$$

where all $T(m,l)$ are real and positive. In particular, we have that

$$T(0,l) = \left[p_{00} + 2\sum_{j=1}^{\lfloor d/2\rfloor}\cos(lj)p_{0j}\right]^{2^k},$$

$$T(m,l) = 2\,\mathrm{Re}\left\{\left[\sum_{j\in\mathbb{F}_d}\Phi(lj)p_{mj}\right]^{2^k}\right\} \quad \text{for } m\neq 0,$$

where $\mathrm{Re}(x)$ denotes the real part of x. In view of Eq. (15), Eq. (14) now follows immediately from the inequality $\xi_0^{(k)} > \xi_n^{(k)}$ as a consequence of the fact that $\cos(x)<1, \forall\, x\in\mathbb{F}_d^*$. A similar but more involved calculation can be performed if d is a prime power. ■

B. Phase error correction (PEC)

Assume now that Alice and Bob have applied a DER process involving many ($k\gg 1$) rounds of D-step. As we have just discussed, at this point the dit-flip-error rate in their surviving pairs will be negligible (i.e., $p_{mn}^{(k)}\simeq 0$ for $m\neq 0$), whereas the phase-error rate has possibly increased. It is therefore reasonable that the second stage of the GL2KD (usually called privacy amplification) deals with phase error correction (PEC) [4,5,7].

In general, at the beginning of the PEC we have a d-ary asymmetric channel with respect to phase errors. In particular, we have $(d-1)$ possible phase errors with corresponding probabilities (rates) $q_n^{(k)}$ given by Eq. (12). To correct the phase errors, Alice and Bob apply an $[r,1,r]_d$ repetition code with a relative majority-vote decoding [8]. The key point is that, according to inequality (14), the necessary condition [8] for such an error correction to work is satisfied at the end of the DER process.

For the sake of completeness, let us briefly summarize the main steps of the PEC procedure [4,5,7]. Alice and Bob randomly divide their qudit-pairs into sets (blocks), each containing r qudit-pairs. Within each block, they perform a discrete Fourier transform $\mathfrak{F}_{\mathrm{A}}\otimes\mathfrak{F}_{\mathrm{B}}$ on each pair. Subsequently, they perform a sequence of $(r-1)$ BXOR operations with the same control pair (say the first one) and target each one of the remaining pairs. For each target pair, they measure their corresponding halves and estimate the parity of their outcomes. Finally, they apply $\mathfrak{F}_{\mathrm{A}}^{-1}\otimes\mathfrak{F}_{\mathrm{B}}^{-1}$ on the control pair and Bob performs $\mathfrak{A}_{0s}$ on his control-qudit, where $s\in\mathbb{F}_d$ is the parity corresponding to the relative majority of their $(r-1)$ outcomes. If the relative majority of the outcomes is ambiguous, Bob applies $\mathfrak{A}_{00}$. In this way, each block may result in one phase-error-free qudit-pair at most.

Our task now is to investigate the effect of such a PEC process on the signal shared between Alice and Bob. Let us denote by p_{mn}^{P} the various error rates in the remaining qudit-pairs at the end of the process. We are mainly interested in the corresponding total dit-flip and phase-error rates.

1. Phase-error rate

Let us start with the estimation of an upper bound on the total phase-error rate $R_{\mathrm{P}}\equiv\Sigma_m\Sigma_{n\neq 0}p_{mn}^{\mathrm{P}}$ of the signal at the end of PEC. We are basically interested in the limit of large block lengths r that is in the limit of a large number of distributed qudit-pairs.

Before we proceed further, it is worth noting that the problem under consideration belongs to a well known class of stochastic processes, the so-called occupancy problems or Balls-and-Bins experiments. In this picture, our problem can be viewed as a probabilistic experiment where r balls (qudit-pairs) are randomly distributed among d different (error-) bins. This class of problems is fundamental to the analysis of randomized algorithms and has been extensively studied in the literature (e.g., see [19–21]). A particularly useful result in this context is the so-called Chernoff-Hoeffding bounds [22], which are basically large-deviation estimates. In general, these bounds are applicable to sums of negatively associated, identically distributed random variables. Their precise derivation can be found in various papers and standard textbooks (e.g., see [20–23]).

Observation 2. The phase-error rate in the surviving pairs at the end of PEC satisfies the condition

$$R_{\mathrm{P}} \leqslant \sum_{n\in\mathbb{F}_d^*}\left[1-\left(\sqrt{q_0^{(k)}}-\sqrt{q_n^{(k)}}\right)^2\right]^r. \tag{16}$$

Proof. Clearly, we have that R_{P} is upper bounded by the probability of failure for the repetition code P_{fail}. It suffices, therefore, to estimate an upper bound on P_{fail}.

As we mentioned before, PEC is applied on a particular asymmetric channel with phase-error rates $q_0 > q_j$ for all $j \neq 0$ (to simplify notation throughout this proof, we write q_j instead of $q_j^{(k)}$). Let us denote by η_j the total number of qudit-pairs within a block of length r suffering from phase errors of the form $\mathfrak{A}_{mj}$, with $m \in \mathbb{F}_d$. Clearly, majority voting fails only if $\eta_j > \eta_0$ for some $j \neq 0$, where η_0 denotes the number of error-free pairs in the block. For asymmetric channels satisfying Eq. (14), this may occur for sufficiently large deviations of η_j from their mean values. In particular, we expect for the failure probability of the majority-vote decoding,

$$P_{\mathrm{fail}} \leqslant P\left[\bigvee_{j \in \mathbb{F}_d^*} (\eta_j \geqslant \eta_0)\right] \leqslant \sum_{j \in \mathbb{F}_d^*} P(\eta_j \geqslant \eta_0), \qquad (17)$$

where $\vee$ is the logical OR operator. The next step now is to upper bound each of the probabilities $P(\eta_j \geqslant \eta_0)$ appearing in the last summation.

Let us focus on a particular term, say $P(\eta_i \geqslant \eta_0)$. We will work with the random variables η_i, η_0, and η_{rest}, where $\eta_i + \eta_0 + \eta_{\mathrm{rest}} = r$ and $\eta_{\mathrm{rest}} = \Sigma_{j \notin \{0,i\}} \eta_j$. Accordingly, the corresponding probability distribution of interest is $(q_0, q_i, q_{\mathrm{rest}})$ with $q_i + q_0 + q_{\mathrm{rest}} = 1$. Obviously, $(\eta_0, \eta_i, \eta_{\mathrm{rest}})$ have a trinomial distribution which is given by

$$P(\eta_0, \eta_i, \eta_{\mathrm{rest}}) = \sum_{\eta_{\mathrm{rest}}=0}^{r} \binom{r}{\eta_{\mathrm{rest}}} q_{\mathrm{rest}}^{\eta_{\mathrm{rest}}} \left[\sum_{\eta_i=0}^{r_i} \binom{r_i}{\eta_i} q_0^{\eta_0} q_i^{\eta_i}\right],$$

where $r_i = \eta_0 + \eta_i = r - \eta_{\mathrm{rest}}$. Introducing the new normalized probabilities $\tilde{q}_l = q_l/(q_0 + q_i)$ with $l \in \{0, i\}$, the trinomial distribution can be rewritten as

$$P(\eta_0, \eta_i, \eta_{\mathrm{rest}}) = \sum_{\eta_{\mathrm{rest}}=0}^{r} \binom{r}{\eta_{\mathrm{rest}}} q_{\mathrm{rest}}^{\eta_{\mathrm{rest}}} (q_0 + q_i)^{r - \eta_{\mathrm{rest}}} \times \left[\sum_{\eta_i=0}^{r_i} \binom{r}{\eta_i} \tilde{q}_0^{\eta_0} \tilde{q}_i^{\eta_i}\right].$$

Note now that the expression in the brackets is the well known binomial distribution involving the two events of interest, i.e., the event of phase-error i, and the event of no-phase-error. In particular, for a given η_{rest} the probability that $\eta_i \geqslant \eta_0$ is given by

$$P(\eta_i \geqslant \eta_0 | \eta_{\mathrm{rest}}) = \sum_{\eta_i = \lceil r_i/2 \rceil}^{r_i} \binom{r}{\eta_i} \tilde{q}_0^{\eta_0} \tilde{q}_i^{\eta_i} \leqslant (4 \tilde{q}_0 \tilde{q}_i)^{r_i/2} = \left[\frac{4 q_0 q_i}{(q_0 + q_i)^2}\right]^{r_i/2}.$$

The above inequality is the well-known Chernoff-Hoeffding bound for the binomial distribution [23], which also applies here since $q_0 > q_i \, \forall \, i \in \mathbb{F}_d^*$. Thus, in total we have

$$\begin{aligned} P(\eta_i \geqslant \eta_0) &= \sum_{\eta_{\mathrm{rest}}=0}^{r} \binom{r}{\eta_{\mathrm{rest}}} q_{\mathrm{rest}}^{\eta_{\mathrm{rest}}} (1 - q_{\mathrm{rest}})^{r - \eta_{\mathrm{rest}}} P(\eta_i \geqslant \eta_0 | \eta_{\mathrm{rest}}) \\ &\leqslant \sum_{\eta_{\mathrm{rest}}=0}^{r} \binom{r}{\eta_{\mathrm{rest}}} q_{\mathrm{rest}}^{\eta_{\mathrm{rest}}} (1 - q_{\mathrm{rest}})^{r - \eta_{\mathrm{rest}}} \left[\frac{4 q_0 q_i}{(q_0 + q_i)^2}\right]^{(r - \eta_{\mathrm{rest}})/2}. \end{aligned} \qquad (18)$$

Finally, given that $R_{\mathrm{P}} \leqslant P_{\mathrm{fail}}$, inequality (16) is obtained from the condition (17) by using inequality (18) and the identity

$$\sum_{a=0}^{r} \binom{r}{a} p^a (1 - p)^{r-a} x^{r-a} = [p + (1 - p)x]^r.$$

■

According to observation 2, the phase-error rate in the signal after PEC decreases exponentially in the block-length r. If we are not interested in a tight upper bound on R_{P}, we may upper-bound the right-hand side of this condition as follows:

$$\begin{aligned} R_{\mathrm{P}} &\leqslant \sum_{n \in \mathbb{F}_d^*} \left[1 - \left(\sqrt{q_0^{(k)}} - \sqrt{q_n^{(k)}}\right)^2\right]^r \\ &\leqslant (d - 1)\left[1 - \left(\sqrt{q_0^{(k)}} - \sqrt{q_{\tilde{n}}^{(k)}}\right)^2\right]^r, \end{aligned} \qquad (19)$$

where $q_{\tilde{n}}^{(k)} = \max\{q_n^{(k)} | n \in \mathbb{F}_d^*\}$, while the equality in the latter part holds if and only if $q_n^{(k)} = q_{\tilde{n}}^{(k)}$, $\forall \, n \in \mathbb{F}_d^*$. Although this last step is not at all necessary, it simplifies considerably the subsequent notation and discussion.

Recall now that the quantities $\xi_n^{(k)}$ and $\chi^{(k)}$ become arbitrarily small as $k \to \infty$. Thus, in view of Eq. (12), Eq. (19) may be further simplified to

$$R_{\mathrm{P}} \leqslant (d - 1)\left[1 - \frac{(\xi_0^{(k)} - \xi_{\tilde{n}}^{(k)})^2}{4d} + O(3)\right]^r,$$

where $O(3)$ denotes third-order terms in $\xi_{\tilde{n}}^{(k)}, \chi^{(k)}$, and $\xi_0^{(k)}$. Inclusion of such higher-order terms may only lead to negligible corrections in the argument of the exponent. At any rate, the phase-error rate will always be upper-bounded by a quantity that decreases exponentially fast in r. Alternatively, using the inequality $(1 - x)^r \leqslant \exp(-rx)$ for all $x < 1$, we obtain

$$R_{\mathrm{P}} \leqslant (d - 1)\exp\left[-r\frac{(\xi_0^{(k)} - \xi_{\tilde{n}}^{(k)})^2}{4d}\right]. \qquad (20)$$

We turn now to estimate the corresponding dit-flip-error rate in the signal.

2. Dit-flip-error rate

As we mentioned before, the PEC involves $(r - 1)$ BXOR gates in the complementary basis. During these gates, the dit-flip errors propagate backwards from the target to the control qudit. As a result, at the end of the PEC the dit-flip-error rate in the remaining particles increases by at most r times (the control qudit-pair itself may initially suffer from a dit-flip-error), i.e.,

$$R_{\mathrm{D}} \equiv \sum_{m\in\mathbb{F}_d^*}\sum_{n\in\mathbb{F}_d} p_{mn}^{P} \leqslant r \sum_{m\in\mathbb{F}_d^*}\sum_{n\in\mathbb{F}_d} p_{mn}^{(k)}. \tag{21}$$

According to the preceding discussion, the net effect of the PEC is to reduce any phase errors of the form $\mathfrak{A}_{mn}$ with $n\neq 0$, while possibly increasing dit-flip errors of the form $\mathfrak{A}_{m0}$ with $m\neq 0$. Thus, at first site, the whole situation seems to be a vicious circle since PEC tends to destroy what was achieved in DER and vice versa. A way out of this stumbling block relies on the judicious combination of DER and PEC.

C. A judicious combination of DER and PEC

For a given $2d$-state protocol (i.e., for a fixed d), Alice and Bob agree in advance upon a fixed and arbitrarily small security parameter $\epsilon>0$. They apply many rounds ($k\gg 1$) of D-step, until there exists an integer $r>0$ such that a single application of the PEC will bring the quantum-channel error rate in the finally surviving pairs to values below ϵ. Clearly, the protocol has to be aborted if the estimated integer r exceeds the number of remaining pairs immediately after the DER procedure. More precisely, at the end of DER, Alice and Bob may choose the block length for the repetition code to be

$$r \approx \frac{\epsilon}{2\sum_{m\in\mathbb{F}_d^*}\sum_{n\in\mathbb{F}_d} p_{mn}^{(k)}} = \frac{\epsilon}{2}\left(1+\frac{1}{\chi^{(k)}}\right) \geqslant \frac{\epsilon}{2\chi^{(k)}}. \tag{22}$$

Note that for this particular choice of the block-length, $r\to\infty$ as $k\to\infty$.

The key point now is that for such a choice of r, the overall channel error rate $Q=1-p_{00}^{\mathrm{P}}$ can be upper-bounded as follows:

$$Q \leqslant R_{\mathrm{D}} + R_{\mathrm{P}} \leqslant \frac{\epsilon}{2} + (d-1)\exp\left[-\frac{\epsilon}{8}\frac{(\xi_0^{(k)}-\xi_{\tilde{n}}^{(k)})^2}{d\chi^{(k)}}\right], \tag{23}$$

where inequalities (21) and (20) have been used. Thus, for any given dimension of the information carriers, $Q<\epsilon$ provided that

$$\frac{[\xi_0^{(k)}-\xi_{\tilde{n}}^{(k)}]^2}{d\chi^{(k)}} > \frac{8}{\epsilon}\ln\left[\frac{2(d-1)}{\epsilon}\right]. \tag{24}$$

As long as $Q<\epsilon$, Alice and Bob share a number of nearly perfect pairs whose fidelity with respect to the ideal state $|\Psi_{00}\rangle$ is exponentially close to 1. The final key can then be obtained by measuring each pair separately along the standard basis, and the information that an eavesdropper may have on it is also upper bounded by the security parameter ϵ.

The condition (24) is a sufficient condition for secret-key distillation in the context of $2d$-state QKD protocols using two Fourier-dual bases. In particular, it determines the error rates which can be tolerated by such protocols using a GL2KD procedure. From that point of view, it is a generalization of the corresponding condition for fully symmetric qudit-based protocols obtained by Chau [7].

Unfortunately, the number of independent parameters in inequality (24) scales quadratically with d, and thus an analytical (or even numerical) solution becomes rather difficult for $d>3$. Hence, in order to obtain an analytic expression for the tolerable error rate for arbitrary dimensions, we had to resort to isotropic quantum channels. The related results will be discussed in detail in Sec. IV. For the time being, we close this section by summarizing the main points in the reduction of the EB version of the $2d$-state QKD protocol to a P&M one.

D. Reduction to a P&M QKD scheme

In general, not every EB QKD protocol can be reduced to a P&M one. The main difficulty appears in the reduction of the underlying quantum-key-distillation procedure to a purely classical one. The advantage of the GL2KD is that by construction it allows for such a reduction [4].

The reduction of the EB $2d$-state QKD protocol to a P&M one, which tolerates precisely the same error rates, follows the same steps as for other protocols [4,7,16]. Here, for the sake of completeness, we would like to summarize the four cornerstones of such a reduction. First, during the distribution stage, Alice can measure all the halves of the pairs before sending the other halves to Bob. This is equivalent to choosing a random dit-string and encoding each dit in the corresponding qudit-state, in one of the two Fourier-dual bases. Second, the XOR operation used in the quantum-key-distillation procedure can be easily replaced by its classical analogue. Thus, the DER stage is immediately reduced to a classical error-rejection (advantage distillation) process. Third, the quantum circuit of the PEC can also be reduced to a classical one. Such a reduction relies on the fact that the sequence of gates applied independently by Alice and Bob in each block of r qudits during PEC, i.e., $\mathfrak{F}_1^{-1}(\mathrm{XOR}_{1\to r}\cdots\mathrm{XOR}_{1\to 2})\otimes_{j=1}^{r}\mathfrak{F}_j$, is equivalent to $\otimes_{j=2}^{r}\mathfrak{F}_j^{-1}(\mathrm{XOR}_{r\to 1}^{(+)}\cdots\mathrm{XOR}_{2\to 1}^{(+)})$. This equivalence follows by induction from the fact that for any two qudits, $(\mathfrak{F}_{\mathrm{c}}^{-1}\otimes\mathbb{I}_{\mathrm{t}})\mathrm{XOR}_{\mathrm{c}\to\mathrm{t}}(\mathfrak{F}_{\mathrm{c}}\otimes\mathfrak{F}_{\mathrm{t}})=(\mathbb{I}_{\mathrm{c}}\otimes\mathfrak{F}_{\mathrm{t}}^{-1})\mathrm{XOR}_{\mathrm{t}\to\mathrm{c}}^{(+)}$, where $\mathrm{XOR}_{\mathrm{c}\to\mathrm{t}}^{(+)}:|x\rangle_{\mathrm{c}}\otimes|y\rangle_{\mathrm{t}}\mapsto|x\rangle_{\mathrm{c}}\otimes|x+y\rangle_{\mathrm{t}}$. Finally, the last essential point in the reduction is the observation that the key-distillation procedure does not rely on phase information.

The above steps lead to a P&M $2d$-state QKD protocol with the distribution and the verification-test stages discussed in Sec. II. The corresponding classical key-distillation stage of the protocol proceeds as follows [4,5,7].

DER: Alice and Bob perform many rounds of D-step. In each round, they randomly form tetrads of their dits. For each tetrad j, Alice announces the parity of her dits, i.e., she announces $X_1^{(j)}-X_2^{(j)}$, where $X_i^{(j)}$ denotes the ith pair of tetrad j. Similarly, Bob announces the parity of his corresponding dits $Y_1^{(j)}-Y_2^{(j)}$. One of the dit-pairs (say $X_1^{(j)}$ and $Y_1^{(j)}$) survives if and only if the announced parities agree. This process is repeated (many rounds of D-step), until there is an integer $r>0$ such that a single application of the following phase-error correction will bring the overall error rate in the remaining signal below ϵ. The protocol is aborted if the estimated parameter r exceeds the number of remaining dits.

PEC: In the classical PEC (which is essentially privacy amplification), Alice and Bob randomly divide their remaining dit-pairs into blocks each containing r dit-pairs. Let us

denote by $(X_i^{(j)}, Y_i^{(j)})$ the ith dit-pair in block j. Alice and Bob replace each block by the parity of its dits, i.e., by $\Sigma_{i=1}^{r} X_i^{(j)}$ and $\Sigma_{i=1}^{r} Y_i^{(j)}$, respectively. In this way, the final secret key essentially consists of the estimated parities for each one of the blocks.

In closing, it has to be noted here that for a more efficient secret-key distillation, the two legitimate users may follow the adaptive key-distillation procedure introduced by Chau [5,7]. The main difference is that Alice and Bob do not apply many rounds of D-step and PEC in order to bring the overall error rate below the security parameter ϵ. Instead, they simply adjust their DER and PEC in order to bring the overall error rate below, let us say, 5%. From that point on, they switch to more efficient error-correction and privacy amplification using concatenated Calderbank-Shore-Steane codes.

IV. ISOTROPIC QUANTUM CHANNELS

An isotropic channel is characterized by $p_{0j}=p_{j0}=p_{10}$ and $p_{ij}=p_{11}$ for $i,j \in \mathbb{F}_d^*$. It turns out that isotropy is an inherent property of the two-basis protocols using qubits (standard BB84) or qutrits [3]. The validity of this particular correctability condition will be discussed in detail elsewhere.

The robustness and security of various QKD protocols under the assumption of isotropic eavesdropping has been extensively studied in the QKD literature [10,11,24–27]. In particular, we know that at any rate the isotropy assumption does not affect the threshold disturbance for secret-key distillation which, for $2d$-state protocols, is given by Eq. (1) [3]. In this section, our purpose is to further analyze the sufficient condition for key distillation (24) in the framework of isotropic quantum channels and derive an analytic expression for the tolerable error rate of $2d$-state QKD protocols.

Instead of isotropic channels, we may consider a slightly more general class of channels for which $p_{0j} \neq p_{j0}$, that is,

$$p_{mn} = \begin{pmatrix} p_{00} & p_{01} & \cdots & p_{01} \\ p_{10} & p_{11} & \cdots & p_{11} \\ \vdots & \vdots & \ddots & \vdots \\ p_{10} & p_{11} & \cdots & p_{11} \end{pmatrix}. \tag{25}$$

Given the normalization condition (3), such a channel involves three independent parameters and thus the derivation of an analytic expression for the tolerable error rate is possible. Moreover, by setting $p_{01}=p_{10}$ we can easily obtain the corresponding expressions for isotropic channels.

A. Tolerable error rates

For channels satisfying Eq. (25), Eq. (8) yields for the probabilities after k rounds of D-step

$$p_{00}^{(k)} = \frac{[p_{00}+(d-1)p_{01}]^{2^k} + (d-1)(p_{00}-p_{01})^{2^k}}{d\Pi},$$

$$p_{0n}^{(k)} = \frac{[p_{00}+(d-1)p_{01}]^{2^k} - (p_{00}-p_{01})^{2^k}}{d\Pi},$$

$$p_{m0}^{(k)} = \frac{[p_{10}+(d-1)p_{11}]^{2^k} + (d-1)(p_{10}-p_{11})^{2^k}}{d\Pi},$$

$$p_{mn}^{(k)} = \frac{[p_{10}+(d-1)p_{11}]^{2^k} - (p_{10}-p_{11})^{2^k}}{d\Pi},$$

where $\Pi=[p_{00}+(d-1)p_{01}]^{2^k}+(d-1)[p_{10}+(d-1)p_{11}]^{2^k}$. In view of these relations, the form (25) is invariant under D-steps since we have that $p_{0n}^{(k)}=p_{01}^{(k)}$, $p_{m0}^{(k)}=p_{10}^{(k)}$ and $p_{mn}^{(k)}=p_{11}^{(k)}$, $\forall\, m,n\neq 0$. Therefore, all the phase-error rates $q_n^{(k)}$ with $n\neq 0$ are equal at the end of DER and the corresponding quantum channel is therefore symmetric with respect to phase errors.

As in the previous section, we may also introduce the parameters $A(m,n)$ and $C(m)$. In fact, for the particular class of channels under consideration, $A(m,n)=A(m)$ for all $m \in \mathbb{F}_d$ and

$$A(0) = \frac{p_{00}-p_{01}}{p_{00}+(d-1)p_{01}}, \tag{26a}$$

$$A(m) = A(1) = \frac{p_{10}-p_{11}}{p_{00}+(d-1)p_{01}} \quad \text{for } m \neq 0, \tag{26b}$$

$$C(m) = C(1) = \frac{p_{10}+(d-1)p_{11}}{p_{00}+(d-1)p_{01}} \quad \text{for } m \neq 0, \tag{26c}$$

while $C(0)=1$. To proceed further, we note that $A(m)=B(m)C(m)$, where

$$B(m) = \frac{p_{m0}-p_{m1}}{p_{m0}+(d-1)p_{m1}} = B(1), \tag{27}$$

and $[B(m)]^{2^k} \to 0$, as $k \to \infty$. Thus, using Eqs. (26) and (27) Eqs. (13) can be simplified to

$$\xi_0^{(k)} = (d-1)\sum_{m\in\mathbb{F}_d} [A(m)]^{2^k}, \tag{28a}$$

$$\xi_n^{(k)} = -\sum_{m\in\mathbb{F}_d} [A(m)]^{2^k} \quad \text{for} \quad n\neq 0, \tag{28b}$$

$$\chi^{(k)} = (d-1)[C(1)]^{2^k}, \tag{28c}$$

where

$$\sum_{m\in\mathbb{F}_d} [A(m)]^{2^k} = [A(0)]^{2^k} + \sum_{m\in\mathbb{F}_d^*} [B(m)]^{2^k}[C(m)]^{2^k}$$
$$= [A(0)]^{2^k} + (d-1)[B(1)C(1)]^{2^k}. \tag{29}$$

Accordingly, condition (24) now reads

$$\frac{d\{[A(0)]^{2^k} + (d-1)[B(1)C(1)]^{2^k}\}^2}{(d-1)[C(1)]^{2^k}} > \frac{8}{\epsilon}\ln\left[\frac{2(d-1)}{\epsilon}\right],$$

or equivalently [setting $A=A(0)$, $B=B(1)$, and $C=C(1)$]

$$\frac{dA^{2^{k+1}}}{(d-1)C^{2^k}} + d(d-1)C^2B^{2^{k+1}} + 2dA^{2^k}B^{2^k} > f(d,\epsilon), \quad (30)$$

where $f(d,\epsilon)=8\epsilon^{-1}\ln[2(d-1)/\epsilon]$.

Recall now that the positive quantities $A^{2^k}\to 0$, $C^{2^k}\to 0$, and $B^{2^k}\to 0$ for $k\to\infty$. Thus, inequality (30) can always be satisfied for any k such that

$$\frac{dA^{2^{k+1}}}{(d-1)C^{2^k}} > f(d,\epsilon). \quad (31)$$

For a given dimension, this latter inequality defines the critical number of D-steps k_c, such that for $k>k_c$, inequality (30) is satisfied. In particular, solving Eq. (31) with respect to k, we obtain

$$k_c = \log_2\left\{\frac{\ln[(d-1)f(d,\epsilon)/d]}{\ln(A^2/C)}\right\}. \quad (32)$$

This is a well defined quantity provided that $A^2>C$, i.e., for

$$(p_{00}-p_{01})^2 > [p_{10}+(d-1)p_{11}][p_{00}+(d-1)p_{01}], \quad (33)$$

where Eqs. (26) have been used. The same inequality holds for isotropic channels but $p_{01}=p_{10}$. This is therefore a sufficient condition for secret-key distillation in the context of any $2d$-state QKD protocol under the assumption of isotropic quantum channels. In particular, it determines the error rates which can be tolerated by such protocols using a GL2KD process.

Recall now that according to Eq. (5) the estimated disturbance for the isotropic channel is $D=[1-p_{00}+(d-1)^2p_{11}]/2$. Moreover, due to the normalization condition (3), inequality (33) actually involves two independent parameters (say p_{00},p_{11}). Thus, estimating the values of p_{00} which satisfy it, we obtain the tolerable error rate (disturbance) which depends on both d and p_{11}, i.e., $D_{2CC}(d,p_{11})$. In fact, we find that $D_{2CC}(d,p_{11})$ increases monotonically with respect to p_{11}. Hence, the worst-case scenario (from Alices' and Bob's point of view) corresponds to $p_{11}=0$, for which we obtain for the tolerable disturbance

$$D_{2CC}(d) = \frac{1-p_{00}}{2} = \frac{2(d-1)}{4d-1+\sqrt{1+4d}}, \quad (34)$$

where $D_{2CC}(d)=D_{2CC}(d,p_{11}=0)$. Given a particular dimension of the information carriers (i.e., a specific $2d$-state protocol), the GL2KD procedure enables Alice and Bob to generate a provably secure key whenever the estimated disturbance is below $D_{2CC}(d)$, or else the quantum channel error rate is below $2D_{2CC}(d)$.

B. Discussion

The tolerable disturbance D_{2CC} and its theoretical upper bound D_{th} are plotted as functions of the dimension d, in Fig. 1. First of all, we see that $D_{2CC}(d)<D_{th}$ for all d. Actually, the difference between the two bounds $\delta(d)\equiv D_{th}-D_{2CC}$ scales with dimension as

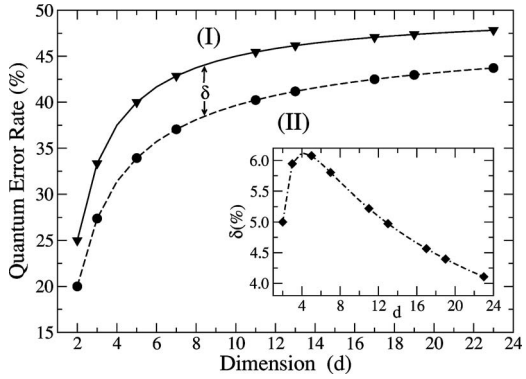

FIG. 1. $2d$-state QKD protocols: The tolerable error rate D_{2CC} (dashed line) and its theoretical upper bound D_{th} (solid line) as functions of the dimension d. Secret-key distillation is impossible in the regime (I), while it may be possible for error rates below D_{th}. In the regime (II), a secret key can be distilled by means of the key-distillation procedure considered here. Inset: The gap between the two regimes $\delta(d)=D_{2CC}-D_{th}$ is plotted as a function of the dimension. The symbols (triangles, circles, and squares) correspond to prime dimensions.

$$\delta(d) = \frac{(d-1)(-2+\sqrt{1+4d})}{2d(4d-3)}, \quad (35)$$

and is also plotted in the inset of Fig. 1. It is also worth noting that δ increases as we go from qubits ($d=2$) to qutrits ($d=3$). It reaches its maximum value around $d=4$ (i.e., for quatrits) and decreases monotonically for higher dimensions. Note that the same behavior also appears in the case of $(d+1)$-basis protocols [7]. Moreover, as $d\to\infty$, we have that

$$D_{2CC}(d) \approx \frac{1}{2} - \frac{1}{4\sqrt{d}},$$

while $\delta(d)\approx 1/4\sqrt{d}$. In other words, we see that the tolerable error rate for the $2d$-state QKD protocols approaches its theoretical upper bound as $1/\sqrt{d}$ for $d\to\infty$. This is in contrast to the $(d+1)$-basis protocols where the corresponding asymptotic behavior scales with dimension as $1/d$.

A special case of the isotropic channel we have just considered is the so-called depolarizing channel for which $p_{mn}=p_{01}$ for $(m,n)\neq(0,0)$. In this case, condition (33) reduces to Eq. (36) of Ref. [7], i.e.,

$$(p_{00}-p_{10})^2 > dp_{10}[p_{00}+(d-1)p_{10}].$$

Note also that for $d=2$ we recover the well-known tolerable error rate of the standard BB84 protocol, i.e., $D_{2CC}(2)=20\%$ [5,6].

In closing, it is worth noting that condition (33) can also be obtained by generalizing the ideas of Ref. [6] to higher dimensions. More precisely, let us define the characteristic exponent $r_{ch}^{(d)}\in\mathbb{R}$ with the defining property that there exists an $\alpha>0$ such that

$$\lim_{k\to\infty}\frac{R_{\mathrm{D}}^{(k)}}{\left(\frac{d-1}{d}-R_{\mathrm{P}}^{(k)}\right)^{r_{\mathrm{ch}}^{(d)}}}=\alpha, \tag{36}$$

where $R_{\mathrm{D}}^{(k)}$ and $R_{\mathrm{P}}^{(k)}$ are given by Eqs. (11), respectively.

For channels satisfying Eq. (25), the quantities $R_{\mathrm{D}}^{(k)}$ and $[(d-1)/d]-R_{\mathrm{P}}^{(k)}$ tend to zero from above, as $k\to\infty$. Moreover, we obtain the following expression for the characteristic exponent:

$$r_{\mathrm{ch}}^{(d)}=\ln\left[\frac{p_{00}+(d-1)p_{01}}{p_{10}+(d-1)p_{11}}\right]/\ln\left[\frac{p_{00}+(d-1)p_{01}}{p_{00}-p_{11}}\right].$$

Following [6], Eq. (33) can now be obtained from the condition for asymptotic correctability, that is, $r_{\mathrm{ch}}^{(d)}>2$. The validity of this particular correctability condition will be discussed in detail elsewhere.

V. CONCLUSIONS

We have discussed the error tolerance of qudit-based QKD protocols using two mutually unbiased (Fourier-dual) bases. In particular, we focused on Gottesman-Lo-type key-distillation procedures. For arbitrary quantum channels subject only to the symmetry between the two bases used in the protocol, we derived a sufficient condition for secret-key distillation, thus extending known results on depolarizing quantum channels.

In the case of isotropic quantum channels, we were able to analyze this condition further and to obtain an analytical expression for the tolerable error rate as a function of the dimension d of the information carriers. Specifically, as $d\to\infty$, the tolerable error rate scales with dimension as $1/2-1/4\sqrt{d}$, thus approaching its upper theoretical bound, that is, $1/2$. This asymptotic behavior is substantially different from the corresponding behavior in the fully symmetric $(d+1)$-basis protocols, where the tolerable error rate scales as $1-(3+\sqrt{5})/2d$.

Unfortunately, for moderate values of d, the tolerable error rate is always well below its corresponding theoretical upper bound $D_{\mathrm{th}}(d)$. Hence, the development of new classical key-distillation protocols which will be able to bridge this gap still remains an interesting open problem.

ACKNOWLEDGMENTS

This work is supported by the EU within the IP SECOQC. K. S. R. is supported by the Technische Universität Darmstadt.

[1] 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).
[2] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[3] G. M. Nikolopoulos and G. Alber, Phys. Rev. A **72**, 032320 (2005).
[4] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).
[5] H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002).
[6] K. S. Ranade and G. Alber, J. Phys. A **39**, 1701 (2006).
[7] H. F. Chau, IEEE Trans. Inf. Theory **51**, 1451 (2005); , e-print quant-ph/0212055.
[8] F. J. MacWilliams and N. J. A. Slone, *The Theory of Error-Correcting Codes* (North-Holland, Amsterdam, 1997); M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[9] A. Klappenecker and M. Rötteler, IEEE Trans. Inf. Theory **48**, 2392 (2002); **48**, 2396 (2002); A. Ashikhmin and E. Knill, IEEE Trans. Inf. Theory **47**, 3065 (2001); E. Knill, e-print quant-ph/9608048.
[10] 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).
[11] A. Acín, N. Gisin, and V. Scarani, Quantum Inf. Comput. **3**, 563 (2003).
[12] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[13] G. Alber, A. Delgado, N. Gisin, and I. Jex, J. Phys. A **34**, 8821 (2001).
[14] M. A. Martín-Delgado and N. Navascués, Eur. Phys. J. D **27**, 169 (2003).
[15] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[16] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[17] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[18] 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).
[19] D. Dubhashi and D. Ranjan, Random Struct. Algorithms **13**, 99 (1998).
[20] J. P. Schmidt, A. Siegel, and A. Srinivasan, SIAM J. Discrete Math. **8**, 223 (1995).
[21] R. Motwani and P. Raghavan, *Randomized Algorithms* (Cambridge University Press, New York, 1995).
[22] H. Chernoff, Ann. Math. Stat. **23**, 493 (1952); W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).
[23] S. Roman, *Coding and Information Theory* (Springer, Berlin, 1992).
[24] D. Bruss and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[25] N. J. Cerf, T. Durt, and N. Gisin, J. Mod. Opt. **49**, 1355 (2002); T. Durt and B. Nagler, Phys. Rev. A **68**, 042323 (2003).
[26] 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).
[27] 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); H. Bechmann-Pasquinucci and N. Gisin, *ibid.* **59**, 4238 (1999).