

**Symmetric extendibility for qudits and tolerable error rates in quantum cryptography**

Kedar S. Ranade

*Institut für Angewandte Physik, Technische Universität Darmstadt, 64289 Darmstadt, Germany*

(Received 31 May 2009; published 3 August 2009)

Symmetric extendibility of quantum states has recently drawn attention in the context of quantum cryptography to judge whether quantum states shared between two distant parties can be purified by means of one-way error correction protocols. In this paper we study the symmetric extendibility in a specific class of two-qudit states, i.e., states composed of two  $d$ -level systems, in order to find upper bounds on tolerable error rates for a wide class of qudit-based quantum cryptographic protocols using two-way error correction. In important cases these bounds coincide with previously known lower bounds, thereby proving sharpness of these bounds in arbitrary finite-dimensional systems.

DOI: [10.1103/PhysRevA.80.022301](https://doi.org/10.1103/PhysRevA.80.022301)

PACS number(s): 03.67.Dd, 03.67.Hk

Quantum cryptography or quantum key distribution was introduced by the seminal work of Bennett and Brassard [1] in 1984. It was widely conjectured to provide means for unconditionally secure communication of two distant parties, Alice and Bob, even in the presence of an adversary, Eve, who can be detected by the quantum-mechanically-induced noise every attack produces. However, security proofs still left loopholes, until Mayers [2] came up with a proof which provided unconditional security even for some finite amount of noise. Since every real physical channel inevitably produces noise, however low it may be, this proof amounts to the advent of practically useful quantum cryptography. Starting from this work, the security of quantum cryptography has been investigated in various scenarios and its security was proved therein. Whereas most of the efforts have been performed with respect to two-dimensional systems (*qubits* with Hilbert space  $\mathcal{H}=\mathbb{C}^2$ ) as basic quantum systems, a large number of concepts and methods carry through for arbitrary finite-dimensional systems (*qudits* with Hilbert space  $\mathcal{H}=\mathbb{C}^d$ ). Such general finite-dimensional systems will be the main focus of this paper. However, we do not consider infinite-dimensional systems (continuous-variable quantum key distribution), since the protocols and scenarios employed there differ considerably from the finite-dimensional case.

A particularly important task in quantum-cryptography-related research is to identify maximally tolerable error rates, i.e., the error rates measurable by Alice and Bob, up to which a physical channel may be used for quantum key distribution without compromising the unconditional security. For the BB84 protocol, this question can be answered by considering an entanglement-based version [3] of that protocol with an appropriate choice of entanglement purification. Under particular circumstances, this protocol can be reduced to yield security of the original BB84 protocol itself by transforming the entanglement purification to some postprocessing, namely error correction and privacy amplification. One generically distinguishes two types of postprocessing. The first kind only uses one-way classical communication, i.e., in the course of postprocessing Alice may send classical information to Bob, but not vice versa; Shor and Preskill [4] used such protocols to show security of the BB84 protocol up to an error rate of 11.0%. The second kind of postprocessing uses both one- and two-way classical communication [5] and this can be used to derive tolerable error rates of 20% for the

BB84 protocol [6–8]. (One should note, that by one-way protocols only, it is impossible to exceed a rate of about 15%, since an arbitrary qubit state can be duplicated, if this rate of error is allowed.) By now no protocol is known which works above 20% error rate, although it has been shown [9] that effective entanglement, which is necessary for key generation, exists up to an error rate of 25%. At present, there exists no purification protocol which works between these two bounds and it is unknown whether this gap can be closed at all.

A different approach to investigate this problem was recently undertaken by Myhr *et al.* [10,11], who posed the question, which condition a quantum state has to fulfill in order to be correctable, using one-way classical communication only. They found that the concept of symmetric extendibility served their purpose, i.e., that a state which possesses a symmetric extension cannot be purified by any possible protocol with one-way communication only. By working out a criterion for symmetric extendibility for two-qubit states they achieved to show that the above-mentioned bound of 20% cannot be surpassed by standard means of two-way entanglement purification [5–8], which indicates the need of new two-way protocols. Finally, we should note that all results we mentioned for the BB84 protocol carry over for the six-state protocol [12], if the rates of 20% and 25% are replaced by 27.6% and 33.3% [6–11].

The aforementioned results show that the tolerable error rates of the most important qubit-based protocols are known, at least in a reasonable scenario using the error correction and privacy amplification available at present. One may ask whether similar results hold true for general finite-dimensional systems, in case we use generalized BB84 and six-state schemes. While lower bounds for such cases are known [13–16], with the exception of disentanglement bounds [17] we are not aware of a systematic study of upper bounds, which is the main purpose of this paper. By performing an analysis similar to that of Myhr *et al.*, we will derive upper bounds on the tolerable error rates with two-way communication. As Myhr *et al.* did for qubit-based protocols, we show that these upper bounds coincide with the lower bounds already known [13–16], thus proving sharpness of these bounds. In the following we will state the details of the model and our proof.

Let us start by introducing the concept of symmetric ex-

tendibility and its relevance in quantum cryptography [10,11,18].

*Definition (symmetric extendibility).* A state  $\rho_{AB}$  on the tensor product  $\mathcal{H}_A \otimes \mathcal{H}_B$  of two Hilbert spaces is said to be symmetrically extendible, if there exists a tripartite state  $\rho_{ABE}$  on  $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$  with  $\mathcal{H}_E = \mathcal{H}_B$ , such that  $\text{Tr}_E \rho_{ABE} = \rho_{AB}$  (extendibility) and  $\rho_{ABE} = \rho_{AEB}$  (symmetry) hold.

Obviously all separable states possess symmetric extensions, while no pure entangled state can be extended. The general solution to the problem, whether a state is symmetrically extendible or not is unsolved, however, a criterion for Bell-diagonal two-qubit states is known [10] and, more generally, criteria for general two-qubit states have been investigated [11]. The relevance of symmetric extendibility in quantum cryptography arises from the following observation [10]: if Alice and Bob share a symmetrically extendible state, we cannot exclude the possibility that Eve holds the extension. If Alice then tries to use one-way communication to establish a secret key with Bob, she will fail, since Eve could do precisely the same as Bob, and Bob and Eve are indistinguishable to Alice.

We shall now introduce a class of two-qudit states, which was shown to be relevant in quantum cryptography. For states within this class we have derived a criterion for symmetric extendibility (theorem 1), which enables us to obtain a simple sufficient condition for this property. Based upon this condition, we will derive upper bounds for qudit-based quantum cryptographic protocols and compare them with the previously known results. To this end, we will in the course of this paper focus on a particular two-way error correction step, the  $B_n^{(d)}$  step (see below), which is essentially the only genuine two-way postprocessing method used in quantum cryptography. Applying this step to a chosen initial state, we will check whether we can reach a state which does not possess a symmetric extension. If this is not the case, we conclude that no protocol in the class considered can produce a secret key for a particular given error rate. The bounds which we derive lie below the disentanglement threshold [17]. Thus, in order to achieve this threshold—if it is possible at all—new two-way methods have to be invented.

To determine whether a general state is symmetrically extendible or not is a complicated task, even for two-qubit states [11]. However, in the context of entanglement-based quantum cryptography by using arguments of the Gottesman-Lo type [5] we may concentrate on a subclass of all states, namely, the (generalized) Bell-diagonal states [5–8,13–15] on  $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^d$ , where  $d$  is the dimension of a single quantum system shared by Alice and Bob. This is achieved by a fictive-measurement argument [5]: one can perform a measurement in the so-called Bell basis before starting the actual protocol and such measurement does not have any measurable effect on the key. The Bell basis consists of vectors (we denote  $z := \exp[2\pi i/d]$ , and  $\ominus$  is to be taken modulo  $d$ )

$$|\Psi_{lm}\rangle := d^{-1/2} \sum_{k=0}^{d-1} z^{lk} |k\rangle |k \ominus m\rangle \quad (1)$$

for  $l, m \in \{0, \dots, d-1\}$ , and the Bell-diagonal states can be written in the form

$$\rho = \sum_{l,m=0}^{d-1} A_{lm} |\Psi_{lm}\rangle \langle \Psi_{lm}|. \quad (2)$$

These states are completely determined by their coefficient matrix  $(A_{lm})_{l,m=0}^{d-1}$ . Choosing the perfect state to be  $|\Psi_{00}\rangle \langle \Psi_{00}|$ —Alice and Bob can locally measure in the standard basis and get one perfectly correlated key dit—we can interpret nonzero  $l$  and  $m$  to be phase and dit errors, respectively.

In quantum cryptography we may assume that Alice and Bob share a large number of identical Bell-diagonal states, i.e.,  $\rho^{\otimes N}$  for Bell-diagonal  $\rho$  and  $N \gg 1$ , which have to be processed by using one-way and two-way communication to yield the state  $|\Psi_{00}\rangle \langle \Psi_{00}|$  [5]. Assuming that the state is symmetrically extendible, we have to use two-way entanglement purification in order to transform it into a state which is not [10,11]. Apart from minor modifications, all known genuine two-way protocols are variations of the  $B_n^{(d)}$  step, so we may focus on that particular step [15]: Alice and Bob choose  $n \in \mathbb{N}$  qudit pairs, all prepared in the state  $\rho$  with coefficients  $(A_{lm})_{l,m=0}^{d-1}$ . They then locally apply generalized XOR operations  $|i\rangle |j\rangle \mapsto |i\rangle |i \ominus j\rangle$  from the first to all other pairs and afterward measure the dit values of all pairs except the first one. They compare the parities of all  $n-1$  measurements by means of classical (two-way) communication and keep the first pair, only if all parities coincide. If they keep the first pair, it will be described by coefficients  $(A'_{lm})_{l,m=0}^{d-1}$ , which are given by [15]

$$A'_{lm} = (dN)^{-1} \sum_{i=0}^{d-1} \left[ z^{-il} \left( \sum_{j=0}^{d-1} z^{ij} A_{jm} \right)^n \right], \quad (3)$$

where  $N := \sum_{m=0}^{d-1} (\sum_{l=0}^{d-1} A_{lm})^n$ . This state has in general less dit errors but more phase errors than the original state by the properties of the generalized XOR. Since we can assume an error rate below 50% [17], i.e.,  $\sum_l A_{l0} > 1/2$ , in the limit of large  $n \in \mathbb{N}$ , the output state of the  $B_n^{(d)}$  step lies in the neighborhood of the separable state defined by  $A_{lm} = d^{-1} \delta_{m0}$ .

We can even further reduce the set of states which have to be taken into consideration by enforcing their invariance with respect to the Abelian unitary group  $\mathfrak{U}_2 := \{U \otimes U^* \mid U \text{ diagonal in the standard basis}\}$ . This is due to the fact that the  $B_n^{(d)}$  step eliminates all kinds of error affected by this symmetrization, so that they do not enter in the one-way correction part [15]. Such  $\mathfrak{U}_2$ -invariant Bell-diagonal states are characterized by the additional property that  $A_{lm} = d^{-1} A_{*m}$  holds with  $A_{*m} := \sum_l A_{lm}$  for all  $m \neq 0$ .

One can now try to explicitly construct a symmetric extension of the given state as a  $d^3 \times d^3$  matrix. The  $\mathfrak{U}_2$  invariance implies that a symmetric extension, if it exists at all, can be chosen to be invariant with respect to  $\mathfrak{U}_3 := \{U \otimes U^* \otimes U^* \mid U \text{ diagonal in the standard basis}\}$ , and this leads to a block matrix structure of the extension. By some further processing, one can work out a criterion for symmetric extendibility for  $\mathfrak{U}_2$ -invariant Bell-diagonal states. Defining  $\tilde{A}_{ip} := \sum_l A_{l0} z^{l(i-p)}$ , this criterion reads as follows ([19],[20], p. 91):

*Theorem 1 (symmetric extendibility).* A  $\mathfrak{U}_2$ -invariant Bell-

diagonal state is symmetrically extendible, if and only if  $(d^{-1}\tilde{A}_{ip})_{i,p=0}^{d-1} \in \mathbb{C}^{d \times d}$  can be decomposed into the sum of  $d$  matrices  $B_0, B_1, \dots, B_{d-1}$ , such that every matrix  $B_k = (a_{ip}^{(k)})_{i,p=0}^{d-1}$  is positive and  $a_{ii}^{(k)} \leq d^{-1}A_{*,i \oplus k}$  for all  $i, k \in \{0, \dots, d-1\}$ .

Although this condition is in general difficult to check, it turns out that it is sufficient for calculating upper bounds on tolerable error rates in quantum cryptography. To this end, we have to find an explicit solution to theorem 1 nearby the state with coefficients  $A_{lm} = d^{-1}\delta_{m0}$  as mentioned before.

For such a state  $A_{*0} \approx 1$  and  $A_{*m} \approx 0$  for  $m \neq 0$  hold. Comparing this with theorem 1, we conclude that in every matrix  $B_k$  one of the diagonal elements can be large, while all others have to be small. Thus we are tempted to choose the matrix, e.g.,  $B_0$  to have the form

$$\begin{pmatrix} \alpha & \eta_1^* & \eta_2^* & \dots & \eta_{d-1}^* \\ \eta_1 & \beta_1 & 0 & \dots & 0 \\ \eta_2 & 0 & \beta_2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ \eta_{d-1} & 0 & \dots & 0 & \beta_{d-1} \end{pmatrix} \in \mathbb{C}^{d \times d}, \quad (4)$$

where  $\alpha = a_{00}^{(0)}$  may be large and the  $\beta_i = a_{ii}^{(0)}$  have to be small. For the other  $B_k$  we assume a similar structure, but  $\alpha$  and the  $\eta_i$  lie on the  $(k-1)$ th row and column. Since the matrix has to be positive, and thus every  $2 \times 2$  principal minor must be non-negative, we may say that the elements set to zero have to be quadratically small in  $\beta_i^{1/2}$ , while the  $\eta_i$  are only linearly small. (The restriction to matrices of the given form results in sufficient conditions for symmetric extendibility, but this is sufficient for our purpose.)

The point of enforcing this matrix structure is that it is positive, if and only if (a) all diagonal elements are non-negative and (b) its determinant is non-negative. This follows by direct application of the well-known Hurwitz-Sylvester criterion for positive semidefiniteness, which states that a Hermitian matrix is positive semidefinite, if and only if all principal minors are non-negative; see, e.g., ([21], p. 282). If all  $\beta_k$  are strictly positive, we can write the determinant of the matrix in Eq. (4) as

$$\left( \prod_{l=0}^{d-1} \beta_l \right) \left( \alpha - \sum_{k=1}^{d-1} \frac{|\eta_k|^2}{\beta_k} \right), \quad (5)$$

and we may focus on the right factor of that product.

We now want to construct a matrix  $B_0$  of the form mentioned in Eq. (4). The other matrices  $B_k$  shall have the same entries, but the row and column structure is permuted according to the conditions of theorem 1. Note that the exceptional element  $\alpha$  for these  $B_k$  wanders along the diagonal with increasing  $k=0, 1, \dots, d-1$ , but that does not alter positivity. It seems appropriate to set the small values to their maximally possible value  $\beta_m := d^{-1}A_{*m}$  according to theorem 1, so normalization enforces  $\alpha := (2A_{*0} - 1)/d$ . Since all diagonal elements are non-negative, we find

$$\sum_{m=1}^{d-1} \frac{|\eta_m|^2}{d^{-1}A_{*m}} \leq \frac{2A_{*0} - 1}{d} = \frac{1 - 2(1 - A_{*0})}{d} \quad (6)$$

to be necessary and sufficient for positivity. (Given the case that some  $A_{*m} = 0$ , this is to be interpreted that the coefficient  $\eta_m$  must vanish.) For a state to be symmetrically extendible,  $\eta_m + \eta_{d \oplus m}^* = d^{-1}\tilde{A}_{m0}$  must hold in addition for all  $m \in \{1, \dots, d-1\}$ . Since in inequality (6), there appear only absolute values, we may set the phases of  $\eta_m$  and  $\eta_{d \oplus m}^*$  to be equal, for choosing small  $|\eta_i|$  does not harm positivity. We thus remain with the condition  $|\eta_m| + |\eta_{d \oplus m}| = d^{-1}|\tilde{A}_{m0}|$ . Setting  $|\eta_m| := \chi_m d^{-1}|\tilde{A}_{m0}|$ , we can rewrite the inequality as

$$\sum_{m=1}^{d-1} \left[ \chi_m^2 \frac{|\tilde{A}_{m0}|^2}{A_{*m}} + 2A_{*m} \right] \leq 1, \quad (7)$$

which is to be fulfilled under the additional constraint  $\chi_m + \chi_{d \oplus m} = 1$ .

Applying a  $B_n^{(d)}$  step to the state, Eq. (3) implies  $A'_{*m} = A_{*m}^n/N$  and  $\tilde{A}'_{m0} = \tilde{A}_{m0}^n/N$  with  $N = \sum_m A_{*m}^n$ , and the condition then reads

$$\sum_{m=1}^{d-1} \left[ \chi_m^2 \frac{1}{N} \left( \frac{|\tilde{A}_{m0}|^2}{A_{*m}} \right)^n + 2 \frac{A_{*m}^n}{N} \right] \leq 1. \quad (8)$$

We shall ignore the second term in the limit  $n \rightarrow \infty$ , since it converges to zero. For the first term we can use the inequality  $N \leq A_{*0}^n$ , which gets tight for  $n \rightarrow \infty$ . The term in question then is  $|\tilde{A}_{m0}|^2 / (A_{*0}A_{*m})$ ; if it is less than 1, it will disappear for  $n \rightarrow \infty$ , otherwise we have to suppress it by setting  $\chi_m := 0$ . This will not be possible, if both  $|\tilde{A}_{m0}|^2 / (A_{*0}A_{*m})$  and  $|\tilde{A}_{m0}|^2 / (A_{*0}A_{*,d \oplus m})$  are greater than 1, which shows the following theorem.

*Theorem 2 (noncorrectability).* After the application of a  $B_n^{(d)}$  step for sufficiently large  $n$  to a  $\mathfrak{U}_2$ -invariant Bell-diagonal state with  $A_{*0} > 1/2$ , the output state is symmetrically extendible, if there hold the inequalities  $|\tilde{A}_{m0}|^2 < A_{*0} \max\{A_{*m}, A_{*,d \oplus m}\}$  for all  $m \in \{1, \dots, d-1\}$ .

In the apparently isotropic case, that is the case where we enforce  $A_{*m} = (1 - A_{*0}) / (d-1)$  for all  $m \neq 0$ , the condition reads

$$(\max_{m=1}^{d-1} |\tilde{A}_{m0}|)^2 < A_{*0} \frac{1 - A_{*0}}{d-1}. \quad (9)$$

If we replace “<” by “>,” this is our sufficient condition for correctability [15], so that these two results are complementary (apart from the case of equality).

A particularly simple and instructive case is the generalized-isotropic case [14,15]. In the  $\mathfrak{U}_2$ -invariant case, we have two non-negative real parameters  $\alpha$  and  $\beta$  which fulfill  $\alpha + (d-1)\beta \leq 1$  and the coefficients of the state are given by

$$A_{lm} = \begin{cases} \alpha, & \text{if } l = m = 0, \\ \beta, & \text{if } l \neq m = 0, \\ \frac{1 - \alpha - (d-1)\beta}{d(d-1)} & \text{else.} \end{cases} \quad (10)$$

Denoting  $x := \alpha + (d-1)\beta$ , we thus compute

$$\tilde{A}_{ip} = \begin{cases} x, & \text{if } i = p \\ \alpha - \beta, & \text{else} \end{cases}, \quad A_{*m} = \begin{cases} x, & \text{if } m = 0, \\ \frac{1-x}{d-1}, & \text{else,} \end{cases} \quad (11)$$

inequality (9) now reads  $(\alpha - \beta)^2(d-1) < x(1-x)$  and can be rewritten as

$$\alpha^2 + (d-1)\beta^2 - \frac{\alpha + (d-1)\beta}{d} < 0. \quad (12)$$

This again is complementary to our result [15], that a state

can indeed be corrected, if the left-hand side is strictly positive, leaving apart the case where we have equality.

To conclude this paper, we have used a criterion for the symmetric extendibility (theorem 1) within the class of  $\mathcal{U}_2$ -invariant two-qudit states in order to show that standard two-way error-correction procedures ( $B_n^{(d)}$  steps) cannot be used to improve on the already known constructive bounds stated, e.g., in [13–15] by any type of one-way communication. This was done by choosing a well-suited class of matrices for that problem, which enabled us to derive upper bounds; these bounds coincide with the previously known bounds, thereby showing their sharpness. In particular, our results coincide with those of Myhr *et al.* [10] in the case of qubits ( $d=2$ ).

The author thanks Gernot Alber, Matthias Christandl, Norbert Lütkenhaus, Geir Ove Myhr, and Joseph M. Renes for helpful discussions. He was supported by the Technische Universität Darmstadt; financial support by CASED is acknowledged.

- 
- [1] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore* (IEEE, New York, 1984), pp. 175–179.
- [2] D. Mayers, *J. ACM* **48**, 351 (2001).
- [3] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [4] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000).
- [5] D. Gottesman and H.-K. Lo, *IEEE Trans. Inf. Theory* **49**, 457 (2003).
- [6] H.-F. Chau, *Phys. Rev. A* **66**, 060302(R) (2002).
- [7] A. Acín, J. Bae, E. Bagan, M. Baig, Ll. Masanes, and R. Muñoz-Tapia, *Phys. Rev. A* **73**, 012327 (2006).
- [8] K. S. Ranade and G. Alber, *J. Phys. A* **39**, 1701 (2006).
- [9] G. M. Nikolopoulos, A. Khalique, and G. Alber, *Eur. Phys. J. D* **37**, 441 (2006).
- [10] G. O. Myhr, J. M. Renes, A. C. Doherty, and N. Lütkenhaus, *Phys. Rev. A* **79**, 042329 (2009).
- [11] G. O. Myhr and N. Lütkenhaus, *Phys. Rev. A* **79**, 062307 (2009).
- [12] D. Bruß, *Phys. Rev. Lett.* **81**, 3018 (1998).
- [13] H.-F. Chau, *IEEE Trans. Inf. Theory* **51**, 1451 (2005).
- [14] G. M. Nikolopoulos, K. S. Ranade, and G. Alber, *Phys. Rev. A* **73**, 032325 (2006).
- [15] K. S. Ranade and G. Alber, *J. Phys. A* **40**, 139 (2007).
- [16] J. Bae and A. Acín, *Phys. Rev. A* **75**, 012334 (2007).
- [17] G. M. Nikolopoulos and G. Alber, *Phys. Rev. A* **72**, 032320 (2005).
- [18] B. M. Terhal, A. C. Doherty, and D. Schwab, *Phys. Rev. Lett.* **90**, 157903 (2003).
- [19] K. S. Ranade, e-print arXiv:0906.5255.
- [20] K. S. Ranade, Ph.D. dissertation, Technische Universität Darmstadt, 2009 ([http://tuprints.ulb.tu-darmstadt.de/1318/1/Dissertation\\_160\\_2009-02-20\\_modif2.pdf](http://tuprints.ulb.tu-darmstadt.de/1318/1/Dissertation_160_2009-02-20_modif2.pdf)).
- [21] F. R. Gantmacher, *Matrizenrechnung, Teil I* (VEB Deutscher Verlag der Wissenschaften, Berlin, 1958).