Entanglement swapping of generalized cat states and secret sharing

Vahid Karimipour* and Alireza Bahraminasab†
Department of Physics, Sharif University of Technology, P. O. Box 11365-9161, Tehran, Iran

Saber Bagherinezhad‡
Department of Computer Science, Sharif University of Technology, P. O. Box 11365-9161, Tehran, Iran
(Received 8 December 2001; published 4 April 2002)

We introduce generalized cat states for *d*-level systems and obtain concise formulas for their entanglement swapping with generalized Bell states. We then use this to provide both a generalization to the *d*-level case and a transparent proof of validity for an already proposed protocol of secret sharing based on entanglement swapping.

DOI: 10.1103/PhysRevA.65.042320 PACS number(s): 03.67.Dd, 03.67.Hk, 03.65.Ta

I. INTRODUCTION

There are numerous uses of spatially separated entangled pairs of particles such as quantum key distribution (QKD) and secret sharing [1–5], teleportation [6,7], superdense coding [8], and cheating bit commitment [9,10]. It has been argued that three or more spatially separated particles in an entangled state [such as a Greenberger-Horne-Zeilinger (GHZ) or cat state [11–14]] may have similar or even broader applications. It is first essential to distinguish between GHZ states and cat states. By an *n*-party cat state, we mean a highly entangled state of *n* particles, while by a GHZ state we mean one that contradicts an interpretation in terms of any local hidden variable theory. Constructing the latter type of state for general multilevel multiparticle systems is quite a difficult task, although some general criteria have been outlined for their identification [15]. On the other hand, we will show that one can easily define *n*-party cat states with nice properties (i.e., entanglement swapping) which allows them to be used in a secret sharing protocol and possibly in many other communication protocols, although they may not be used for testing nonlocality properties of quantum mechanics. More recently, applications such as reducing communication complexity [16,17], quantum telecomputation [18], and networked cryptographic conferencing [19–22] have also been suggested as possible applications of these multiparticle entangled states.

For practical applications such as those mentioned above, there has been much interest in manipulating entangled states of many particles [23–26]. In particular, it has been shown that by appropriate Bell measurements entanglement can be swapped between different particles [23], a scheme which was generalized to the multiparticle case in [25]. In fact, to the question of ''Which particles get entangled when we make a cat state measurement on a group of particles?'' there is a general pencil and paper rule which provides the answer [25]. One just has to connect the particles being measured to frame a polygon and those not being measured to frame a complementary polygon. These two polygons represent the two multiparticle cat states obtained after the manipulation. However, for most applications it is highly necessary to know exactly the type (e.g., the labels) of cat state that the particles are forming and a knowledge only of the particles sharing the entanglement is not enough. In fact, in almost any of the communication protocols mentioned above, the information to be transferred is encoded in the type of label of the cat states involved. For this reason one needs also a simple pencil and paper rule for determining the types and labels of the cat states involved in a swapping process.

It may not be very illuminating to derive a general formula for such a purpose, although it is rather straightforward to do so. However, if we restrict ourselves to the most common type of swapping, that is, the swapping of a cat state and a Bell state, then transparent, graphical, and very useful rules can be derived as we will show below. Furthermore, we will derive the rules for general *d*-level systems. We will then apply these rules to the quantum key distribution and secret sharing protocols of [3,4] and show that the rules of encoding and decoding of this protocol, expressed otherwise only in tables, even when few parties are involved [4], can be neatly expressed by closed formulas in the general case.

The structure of this paper is as follows. In Sec. II we review the basic properties of *d*-level Bell states [27–29] and introduce *d*-level cat states. In Sec. III we derive simple graphical rules for entanglement swapping of *d*-level Bell and cat states. We then apply these rules in Sec. IV to the secret sharing protocol of Cabello [4] to see how simple the encoding and decoding rules of this protocol are. We conclude the paper with a discussion.

II. GENERALIZED CAT STATES FOR *d*-LEVEL SYSTEMS

In studying *d*-level states and their entanglement properties we are following an interesting trend to generalize the well known quantum algorithms and protocols of quantum computation and communication to nonbinary systems, like quantum gates for qudits [30], quantum error correcting codes [31,32], and generalization of the Bennett-Brassard 1984 (BB84) protocol [33] for quantum key distribution [2]. (For a review on quantum key distribution, see [34].)

In fact, considerations of quantum hardware may bring about some advantage for nonbinary systems, since bigger

*Electronic address: vahid@sina.sharif.edu
†Electronic address: baramina@physics.sharif.edu
‡Electronic address: bagherin@ce.sharif.edu

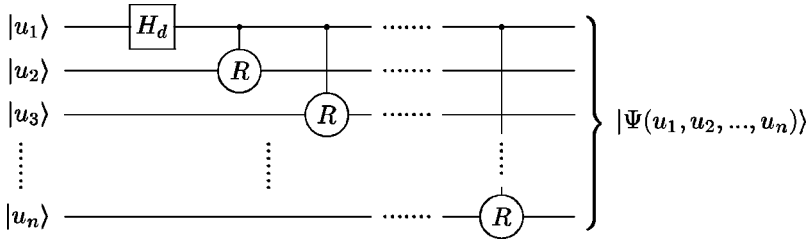

FIG. 1. Circuit for constructing d-level cat states.

Hilbert spaces can be made by coupling fewer d-dimensional systems than two-dimensional ones, and it is well known that complete coupling of quantum bits gets much more difficult with an increasing number of qubits. Some researchers have even considered quantum computation and communication with continuous variables [35,36]. Besides these, it is very instructive to study quantum computation and communication for d-level systems (qudits) to understand them in a general dimension-free setting.

We start by reviewing a generalization of the familiar Bell states for qudits introduced in [27–29]. These are a set of d^2 maximally entangled states which form an orthonormal basis for the space of two qudits. Their explicit forms are

$$|\mathbf{\Psi}(u_1,u_2)\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \zeta^{ju_1} |j, j+u_2\rangle, \tag{1}$$

where $\zeta = e^{2\pi i/d}$ and u_1 and u_2 run from 0 to $d-1$. Each Bell state is thus characterized by a pair of two Z_d labels. For $d=2$ these states reduce to the familiar Bell states, usually denoted by $|\mathbf{\Psi}^{\pm}\rangle$ and $|\Phi^{\pm}\rangle$. One can also expand any computational basis vector in terms of Bell states:

$$|j,k\rangle = \frac{1}{\sqrt{d}} \sum_{u=0}^{d-1} \zeta^{-ju} |\mathbf{\Psi}(u, k-j)\rangle. \tag{2}$$

It is also useful to consider a generalization of the familiar Hadamard gate to the d-level case. It is defined as follows [37,38]:

$$H_d = \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \zeta^{ij} |i\rangle\langle j|. \tag{3}$$

This operator is really not new and it is known as the quantum Fourier transform when $d=2^n$. In that case it acts on n qubits. Here we are assuming it to be a basic gate on one single qudit, in the same way that the ordinary Hadamard gate is a basic gate on one qubit. It is also useful to generalize the NOT and the controlled-NOT gates. We note that in the context of qubits, the NOT gate, is basically a mod-2 adder. For qudits this operator gives way to a mod-d adder, or a right-shift gate R, which is the same as the generalized Pauli operator X_d of Gottesman [37]:

$$R: |j\rangle \rightarrow |j+1\rangle \mod d. \tag{4}$$

Note that in [39] this operator was denoted by R to convey more directly its operation as a right-shifter. Also note that $R^d = \mathbb{1}$, compared to the NOT gate, which squares to unity. For any unitary operator U, the controlled operator U_c is naturally generalized as follows:

$$U_c: \quad |i\rangle \otimes |j\rangle \rightarrow |i\rangle \otimes U^i |j\rangle. \tag{5}$$

Here the first and second qudits are, respectively, the controller and the target qudits. In particular, the controlled right-shift gate which generalizes the controlled-NOT gate [37,39], act as follows:

$$R_c: \quad |i,j\rangle \rightarrow |i, j+i\rangle. \tag{6}$$

This operator has also been defined in [30], where it is called the SUM gate. Equipped with the d-level Hadamard and controlled-NOT (R_c) gates, one can construct d-level cat states simply as in the two-level case by the circuit shown in Fig. 1, where $|u_1,u_2,\ldots,u_n\rangle$ is a computational basis vector, in which $u_i \in \{0,1,2,\ldots,d-1\}$.

The resulting cat state will be

$$|\mathbf{\Psi}(u_1,u_2,\ldots,u_n)\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \zeta^{ju_1} |j, j+u_2, j+u_3, \ldots, j+u_n\rangle. \tag{7}$$

For three parties ($n=3$) and two level states ($d=2$ or $\zeta=-1$), these states reduce to the familiar GHZ states, including, for example,

$$|\mathbf{\Psi}(0,0,0)\rangle := \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle, \tag{8}$$

or

$$|\mathbf{\Psi}(1,0,0)\rangle := \frac{1}{\sqrt{2}} (|000\rangle - |111\rangle. \tag{9}$$

These states are orthonormal,

$$\langle \mathbf{\Psi}(v_1,\ldots,v_n) | \mathbf{\Psi}(u_1,\ldots,u_n)\rangle = \delta_{u_1,v_1} \ldots \delta_{u_n,v_n},$$

and complete: any computational basis vector can be expanded in terms of these generalized cat states:

$$|u_1,u_2,u_3,\ldots,u_n\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \zeta^{-ju_1} |\mathbf{\Psi}(j, u_2-u_1, u_3-u_1, \ldots, u_n-u_1)\rangle. \tag{10}$$

Quite analogously to the two-level case, one can generate a cat state of n particles from a cat state of $n-1$ particles in two ways, either using the Zeilinger *et al.* method [26], that is, acting by an R_c or SUM gate on one particle of the $(n-1)$-cat state and one qudit of a Bell state and subsequently measuring the target qudit, or using the method of [25], that is, performing a Bell state measurement on two particles, one from an $(n-1)$-cat state and the other from a three-cat state, projecting the rest onto an n-cat state.

III. SOME SIMPLE RULES FOR ENTANGLEMENT SWAPPING

Entanglement swapping is nothing but tensor multiplying two cat states, expanding them in the computational basis of the product space, swapping a subset of particles, and then reexpanding the resulting state in terms of the new cat states. The idea and the essential calculation are best illustrated by the simplest example, that is, swapping two Bell states. Suppose particles 1 and 2 are in a Bell state $|\Psi(u_1,u_2)\rangle_{1,2}$ and particles 3 and 4 are in a Bell state $|\Psi(v_1,v_2)\rangle_{3,4}$. This state of the four particles is equal to

$$\begin{aligned}
&\frac{1}{d}\sum_{j,j'}\zeta^{ju_1+j'v_1}|j,j+u_2\rangle_{1,2}|j',j'+v_2\rangle_{3,4}\\
&\quad=\frac{1}{d}\sum_{j,j'}\zeta^{ju_1+j'v_1}|j,j'+v_2\rangle_{1,4}|j',j+u_2\rangle_{3,2}\\
&\quad=\frac{1}{d^2}\sum_{j,j',w,w'}\zeta^{ju_1+j'v_1}\zeta^{-jw-j'w'}|\Psi(w,j'+v_2-j)\rangle_{1,4}\\
&\qquad\times|\Psi(w',j+u_2-j')\rangle_{3,2}. \qquad (11)
\end{aligned}$$

Changing the variables $(j'-j\to\ell)$, using the identity $(1/d)\sum_{j=0}^{d-1}\zeta^{jn}=\delta(n,0)$, and rearranging terms, we finally arrive at

$$\begin{aligned}
&|\Psi(u_1,u_2)\rangle_{1,2}|\Psi(v_1,v_2)\rangle_{3,4}\\
&\quad=\frac{1}{d}\sum_{k,\ell}\zeta^{-k\ell}|\Psi(u_1+k,v_2+\ell)\rangle_{1,4}\\
&\qquad\times|\Psi(v_1-k,u_2-\ell)\rangle_{3,2}. \qquad (12)
\end{aligned}$$

It is customary to represent a cat state by a polygon. However, a cat state is not symmetric and a polygon cannot represent it properly. In fact, as is clear from Eq. (7), a cat state is symmetric under the interchange of both the labels and the particles from 2 to n, i.e.,

$$\begin{aligned}
&|\Psi(u_1,\ldots,u_k,\ldots,u_l,\ldots,u_n)\rangle_{1,\ldots,k,\ldots,l,\ldots,n}\\
&\quad=|\Psi(u_1,\ldots,u_l,\ldots,u_k,\ldots,u_n)\rangle_{1,\ldots,l,\ldots,k,\ldots,n}; \qquad (13)
\end{aligned}$$

however, it has no such symmetry under the interchange of the first particle with another one. We therefore depict a cat state by a line with n nodes on it, distinguishing the first node from the others by assigning a black circle to it compared with empty circles assigned to others (Fig. 2). With this convention, the result of swapping calculated in Eq. (11) can be depicted as in Fig. 3, where we have ignored the coefficients of the expansion and the arrow is meant to imply that the right-hand side is a possible outcome of the Bell measurement performed on the left-hand side particles designated by the dashed line. The simple rule is that the sums of labels on the black nodes and white nodes are conserved separately in such a swapping. We will see that this type of rule will also hold true with slight modifications in swapping of Bell states and cat states.

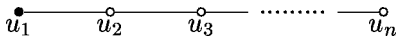

FIG. 2. Visualization of the $|\Psi(u_1,u_2,\ldots,u_n)\rangle$ cat state.

We now derive formulas for swapping Bell states and cat states. We distinguish two cases, one in which a Bell state measurement involves the first particle (the black node) of the cat state and one in which it does not. For the first case we find after some straightforward calculations

$$\begin{aligned}
&|\Psi(u_1,u_2,\ldots,u_n)\rangle_{1,2,\ldots,n}\otimes|\Psi(v,v')\rangle_{s,s'}\\
&\quad=\frac{1}{d}\sum_{k,\ell}\zeta^{-lk}\\
&\qquad\times|\Psi(v+k,u_2-\ell,u_3-\ell,\ldots,u_n-\ell)\rangle_{s,2,3,4,\ldots,n}\\
&\qquad\otimes|\Psi(u_1-k,v'+\ell)\rangle_{1,s'}. \qquad (14)
\end{aligned}$$

This formula is depicted graphically in Fig. 4(a). Again we see a simple rule in terms of the conservation of the labels on the black and white nodes. For the second case where the Bell state measurement does not involve the black node of the cat state we find

$$\begin{aligned}
&|\Psi(u_1,u_2,\ldots,u_n)\rangle_{1,2,3,\ldots,n}\otimes|\Psi(v,v')\rangle_{s,s'}\\
&\quad=\frac{1}{d}\sum_{k,\ell}\zeta^{-\ell k}\\
&\qquad\times|\Psi(u_1+k,u_2,u_3,\ldots,v'+\ell,\ldots,u_n)\rangle_{1,\ldots,s',\ldots,n}\\
&\qquad\otimes|\Psi(v-k,u_m-\ell)\rangle_{s,m}. \qquad (15)
\end{aligned}$$

This is depicted in Fig. 4(b). For more general results on entanglement swapping see [40].

IV. SECRET KEY SHARING BY ENTANGLEMENT SWAPPING

Among the many applications of entanglement swapping mentioned in the Introduction, in this section we consider the secret key sharing protocol proposed by Cabello in [3,4]. In this protocol n members of a group want to agree upon a

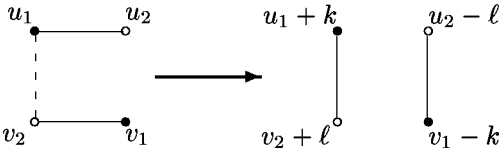

FIG. 3. Entanglement swapping of d-level Bell states.

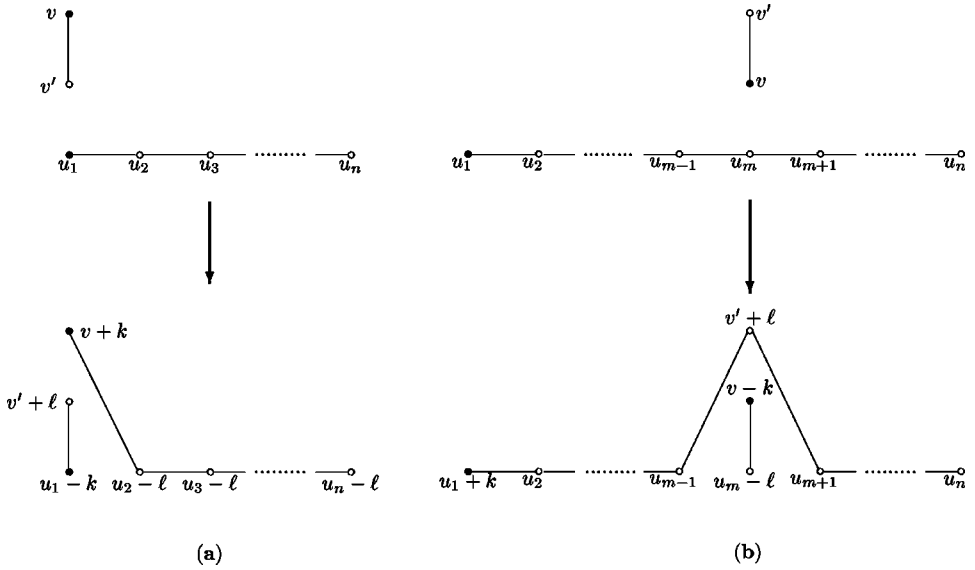

FIG. 4. Entanglement swapping between a cat state and a Bell state.

secret key (for $n=2$, we have the simple QKD scheme). The key is to be such that no proper subset of the group can determine it and its determination requires the cooperation of all members of the group. In the protocol proposed by Cabello [4] the n members of the group share an n-cat state, and each of them also has a Bell state. Each of the members swaps her or his Bell state with the cat state, and then all of them send the resulting cat state to one of the members, say Alice, who measures the cat state and announces the result of her measurement in public. It is then argued that, by using this knowledge and the result of their own Bell measurements, the members of the group can all determine the result of the Bell measurement of Alice, which is to act as a random two-bit key. In [4], it is shown by way of two examples for three and four parties and compiling the results of measurements in tables that this is indeed possible. Here we generalize the results of [4] in two respects. First, we consider general d-level systems instead of two-level ones; second, by using our simple rules for entanglement swapping we derive general and concise formulas for determining the final secret key in terms of measurements of individual members. As mentioned above, we can carry out all of the analysis graphically, where by our graphics we not only imply the particles that get entangled under swapping but also indicate precisely the entangled states they form in this process. The first stage of the process is depicted in Fig. 5(a), where each member (i) has a Bell state (v_i,v_i') and all the members also share a cat state $(u_1,u_2,\ldots,u_n)$. When the first member, whom we call Alice, performs her Bell measurement the entanglement swaps to the form shown in Fig. 5(b), where we have used the first rule of Fig. 4(a). Subsequently, members numbered 2,3,..., and n perform their Bell measurements and the states swap to those of Fig. 5(c). The random two-bit key is the pair of labels of Alice's Bell state, that is, $(u_1-k_1,v_1'+\ell_1)$. At this stage the cat state is sent to Alice; she measures the state and announces the labels $(v_1+k_1+k_2+\cdots+k_n,v_2'+\ell_2,v_3'+\ell_3,\ldots,v_n'+\ell_n)$ of this state in public. It is now clear that each member of the group, say the ith one $(i=2,3,\ldots,n)$, knowing his own Bell state (v_i,v_i') at the beginning of the protocol, his final Bell state $(v_i-k_i,u_i-\ell_1-\ell_i)$, and the publicly announced cat state, can independently determine ℓ_1 and hence the second label of the secret key, $v_1'+\ell_1$. [Note that the shared cat state labels and all the Bell labels including those of Alice (v_1,v_1') are as-

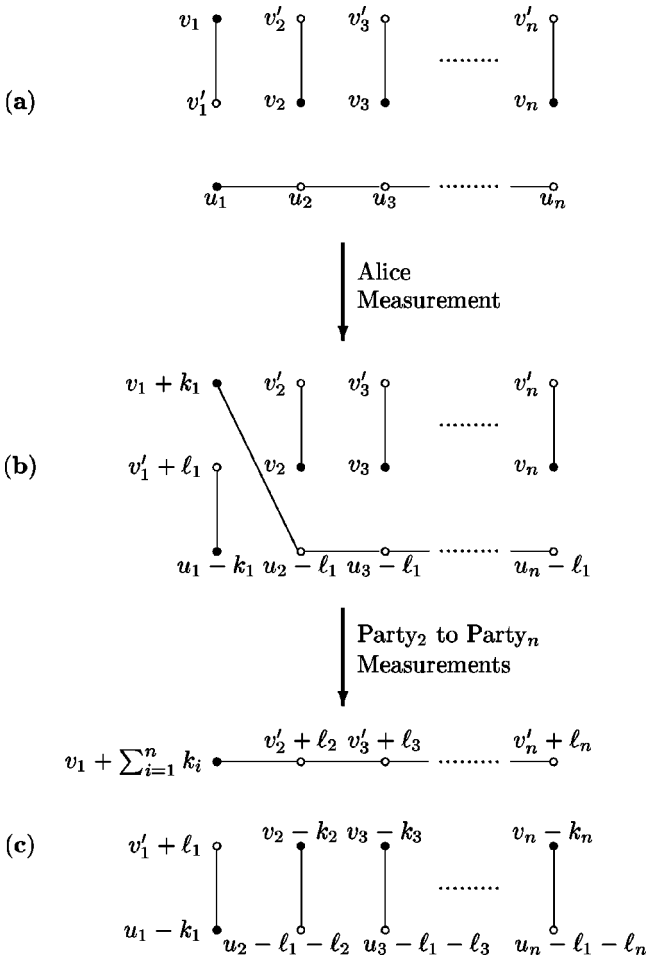

FIG. 5. A protocol for d-level secret sharing.

sumed to be known to all the members at the beginning of the protocol.] However, to determine the first label of the key, that is, $u_1 - k_1$, the members need a knowledge of k_1, which no subset of the group can determine independently. It can only be found by sharing their values of k_i, $i = 2,3,\ldots,n$, with each other. Once this is done all members can determine the value of k_1 from the publicly announced label of Alice $v_1 + k_1 + k_2 + \cdots + k_n$.

The way we have presented this protocol, which starts with general cat and Bell states, rather than with special ones with, say, all the labels being zero [i.e., $\Psi(0,...,0)\rangle$], has the advantage that it shows how the encoding and decoding scheme works for consecutive qudits, when the same Bell and cat states are reused. To compare our results with those of [4], it is enough to set all the original labels $u_i, v_i, v_i' = 0$. It is then easy to see from Fig. 5 that our results completely match the tables presented in that article.

V. DISCUSSION

We have provided closed formulas for entanglement swapping of *d*-level cat states and Bell states. We have then used our formulas for providing transparent proof of the validity of a secret sharing protocol between *n* parties based on entanglement swapping. We expect that our graphical method of representing cat states and our formulas for entanglement swapping (ES) may find applications in every ES-based protocol in quantum communication.

ACKNOWLEDGEMENT

The work of V.K. was partially supported by the Institute of Theoretical Physics and Mathematics (IPM), Tehran, Iran.

[1] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).
[2] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, e-print quant-ph/0107130.
[3] A. Cabello, Phys. Rev. A **61**, 052312 (2000).
[4] A. Cabello, e-print quant-ph/0009025.
[5] Y. S. Zhang, C. F. Li, and G. C. Guo, e-print quant-ph/0011034.
[6] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wooters, Phys. Rev. Lett. **70**, 1895 (1993).
[7] S. L. Braunstein and A. Mann, Phys. Rev. A **51**, R1727 (1995).
[8] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[9] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[10] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[11] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, The Netherlands, 1989).
[12] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[13] N. D. Mermin, Am. J. Phys. **58**, 731 (1990).
[14] N. D. Mermin, Phys. Today **43** (6), 9 (1990).
[15] A. Cabello, Phys. Rev. A **63**, 022104 (2001).
[16] H. Buhrman, R. Cleve, and W. van Dam, quant-ph/9705033.
[17] R. Cleve and H. Buhrman, quant-ph/9704026.
[18] L. K. Grover, quant-ph/9704012.
[19] S. J. D. Phoenix, S. M. Barnett, P. D. Townsend, and K. J. Blow, J. Mod. Opt. **42**, 1155 (1995).
[20] P. D. Townsend, C. Marand, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, Philos. Trans. R. Soc. London, Ser. A **354**, 805 (1996).
[21] P. D. Townsend, Nature (London) **385**, 47 (1997).
[22] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).
[23] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993).
[24] M. Zukowski, A. Zeilinger, and H. Weinfurter, Fund. Prob. Quantum Theor. **755**, 91 (1995).
[25] S. Bose, V. Vedral, and P. L. Knight, e-print quant-ph/9708004.
[26] A. Zeilinger, M. A. Horne, H. Weinfurter, and M. Zukowski, Phys. Rev. Lett. **78**, 3031 (1997).
[27] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[28] N. J. Cerf, J. Mod. Opt. **47**, 187 (2000).
[29] N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998).
[30] S. D. Bartlett, H. de Guise, and B. C. Sanders, e-print quant-ph/0109066.
[31] E. Knill, e-print quant-ph/9608048.
[32] H. F. Chau, e-print quant-ph/9610023.
[33] C. H. Bennett and G. Brassard, in *IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984), p. 175.
[34] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, e-print quant-ph/0101098.
[35] S. L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
[36] A. K. Pati, S. L. Braunstein, and S. Loyd, e-print quant-ph/0002082.
[37] D. Gottesman, e-print quant-ph/9802007.
[38] N. D. Mermin, e-print quant-ph/0105117.
[39] V. Karimipour, S. Bagherinezhad, and A. Bahraminasab, e-print quant-ph/0111091.
[40] J. Bouda and V. Buzek, J. Phys. A, Math. Gen. **34**, 4301 (2001).