Robust multipartite multilevel quantum protocols

Hideomi Nihira* and C. R. Stroud, Jr.
The Institute of Optics, University of Rochester, Rochester, New York 14627, USA
(Received 23 November 2004; published 26 August 2005)

We present a quantum protocol utilizing a tripartite three-level state. The state used in this scheme contains entanglement even after one system is traced out and as a result can be used for both a secret-sharing protocol among the three parties and a quantum-key-distribution protocol between any two parties. We show how to utilize this residual entanglement for quantum-key-distribution purposes, and explore a possible realization of the scheme using entanglement of orbital-angular-momentum states of photons.

DOI: 10.1103/PhysRevA.72.022337 PACS number(s): 03.67.Dd, 03.67.Mn

I. INTRODUCTION

Here we present a simple three-level tripartite quantum protocol that can be generalized to an N-level N-partite scheme. The initial state that the three parties share can be used for either a quantum secret-sharing protocol among all three, or a Bennett-Brassard 1984–(BB84)-like protocol between any two parties. Although BB84 is a protocol in which Alice and Bob perform operations on the same particle, making separate measurements on two entangled particles shared between Alice and Bob can also produce perfectly correlated measurement outcomes. In this manner a BB84-like scheme can be employed for entangled states. The interesting aspect of the proposed state is that, unlike the Greenberger-Horne-Zeilinger (GHZ) $|\mathrm{GHZ}\rangle_N$ state, the reduced density matrix of any two particles still contains some entanglement, and perfectly correlated measurements can be made in the reduced space thus making the protocol robust against particle loss. We also show how this scheme can be realized using entangled orbital-angular-momentum states of light.

The original cryptographic protocol introduced by Bennett and Brassard [1] generated a secure key using two sets of bases that were mutually unbiased. Later, Ekert suggested the use of entangled states to generate a common key in a secure fashion [2]. However, these quantum-key-distribution (QKD) protocols involved only two parties and two-level systems. In recent years researchers have drawn attention to QKD protocols that involve multilevel systems with two parties [3–8], or multiple parties with two-level systems [9,10]. Motivating the pursuit of multilevel quantum key distribution is that more information can be carried by each particle thereby increasing the information flux, and some multilevel protocols have been shown to have greater security against eavesdropping attacks [3,8]. As for multiparty protocols there is the quantum secret-sharing (QSS) protocol which employs $|\mathrm{GHZ}\rangle_N$ states [9,10], but there seems to be little else.

On the experimental side, one of the obstacles for multilevel schemes is the feasibility of such schemes. Atoms have multiple energy levels that can be utilized, but preparing atoms in some prescribed state and sending them off to separate parties is probably not realistic. The decoherence time of the state will determine how far the particles can travel before they become useless for any scheme that requires a particular state. However, recent experimental demonstrations in the entanglement of orbital-angular-momentum states of photons and the generation of arbitrary entangled states with these orbital-angular-momentum quantum numbers [11–13] makes photons a promising resource for multidimensional quantum protocols. Furthermore, much work has been done in detecting these orbital-angular-momentum states of light and their superpositions at the single-photon level [14–16].

Here we investigate another possible multiparty protocol involving a state which, unlike the $|\mathrm{GHZ}\rangle_N$ state, contains some entanglement even after one of the particles is traced out. Although the remaining state is a mixed state, perfectly correlated measurements can be made by making measurements in a reduced space. This makes the state rather interesting because it allows any two parties to create a key without any help from the third.

II. QUANTUM SECRET-SHARING PROTOCOL

Suppose there is a task at hand in which the involvement of more than one party is needed for the sake of checks and balances. This could be for launching missiles, opening bank safes, or other sensitive matters which no one individual can be trusted to execute. To this end, one sends only parts of the launch code, bank vault combination, etc., to each party involved in the task. The message can be deciphered only when all the parties involved cooperate. In our discussion Alice will have the key to encode information, and Bob and Charlie will have the partial keys so that they have to cooperate in order to decipher Alice's message. In recent years quantum-mechanical versions of these secret sharing protocols have been discussed using GHZ states [9,10]. Here we propose another secret-sharing scheme using a three-level system.

We assume that the three parties (Alice, Bob, and Charlie) share the state

$$|\Psi\rangle = \frac{1}{\sqrt{6}}[(|ab\rangle + |ba\rangle)|c\rangle + (|ac\rangle + |ca\rangle)|b\rangle + (|cb\rangle + |bc\rangle)|a\rangle], \tag{1}$$

where $|a\rangle$, $|b\rangle$, and $|c\rangle$ are the three quantum levels and $(|ab\rangle+|ba\rangle)|c\rangle$ is shorthand for $(|a\rangle_{\mathrm{Alice}}\otimes|b\rangle_{\mathrm{Bob}}+|b\rangle_{\mathrm{Alice}}$

*Electronic address: nihira@optics.rochester.edu

$\otimes|a\rangle_{\mathrm{Bob}})\otimes|c\rangle_{\mathrm{Charlie}}$ [17]. Note that this state is the sum of all the permutations of the three levels, and that the state collapses into a Bell state when one of the parties makes a measurement in the representational basis; hence the measurement outcomes are perfectly correlated. Now we define another set of measurement basis vectors

$$|u1\rangle=\frac{1}{\sqrt{3}}(|a\rangle+|b\rangle+|c\rangle), \tag{2}$$

$$|u2\rangle=\frac{1}{\sqrt{3}}(|a\rangle+e^{i\phi}|b\rangle+e^{-i\phi}|c\rangle), \tag{3}$$

$$|u3\rangle=\frac{1}{\sqrt{3}}(|a\rangle+e^{-i\phi}|b\rangle+e^{i\phi}|c\rangle), \tag{4}$$

where $\phi=i2\pi/3$. This set of measurement basis vectors is a mutually unbiased basis set for a three-level system. The original state is perfectly correlated in this measurement basis as well since

$$\langle u1,u1|\Psi\rangle=|u1\rangle,\quad \langle u2,u1|\Psi\rangle=-|u2\rangle,$$
$$\langle u3,u1|\Psi\rangle=-|u3\rangle, \tag{5}$$

$$\langle u1,u2|\Psi\rangle=-e^{-i\phi}|u3\rangle,\quad \langle u2,u2|\Psi\rangle=-e^{-i\phi}|u1\rangle,$$
$$\langle u3,u2|\Psi\rangle=e^{-i\phi}|u2\rangle, \tag{6}$$

$$\langle u1,u3|\Psi\rangle=-e^{i\phi}|u2\rangle,\quad \langle u2,u3|\Psi\rangle=e^{i\phi}|u3\rangle,$$
$$\langle u3,u3|\Psi\rangle=-e^{-i\phi}|u1\rangle, \tag{7}$$

where $\langle u1,u1|\Psi\rangle=|u1\rangle$ is shorthand for ${}_{\mathrm{Bob}}\langle u1|\otimes_{\mathrm{Alice}}\langle u1|\Psi\rangle=|u1\rangle_{\mathrm{Charlie}}$. First, Alice measures her particle using one of the bases, then Bob makes his measurement in one of the bases, and then Charlie does the same. If all the parties involved measure in the same basis, then they will keep the outcome of their measurement. At the very end, Bob and Charlie get together and compare notes to determine Alice's measurement outcomes. Clearly, from the structure of the initial state, neither Bob nor Charlie could tell what Alice's measurement was without getting together and sharing measurement results.

III. QUANTUM-KEY-DISTRIBUTION PROTOCOL

Alice, Bob, and Charlie still share the same initial state described before, but what happens if Charlie loses his particle? Can Alice and Bob still utilize the entanglement they have between their particles to communicate? There is indeed a simple way to take advantage of the residual entanglement Alice and Bob share. The reduced density matrix of the original state when Charlie's system is traced out is

$$\hat{\rho}_{AB}=\frac{1}{3}(|\Psi_{ab}\rangle\langle\Psi_{ab}|+|\Psi_{bc}\rangle\langle\Psi_{bc}|+|\Psi_{ca}\rangle\langle\Psi_{ca}|), \tag{8}$$

where $|\Psi_{ij}\rangle=(1/\sqrt{2})(|ij\rangle+|ji\rangle)$ and $i,j\in(a,b,c)$. Alice and Bob share this mixed state, but the question remains whether they can get perfectly correlated measurement outcomes from this state. Indeed, this can be done if Alice and Bob restrict their measurements to a two-dimensional subspace of the three-level system.

Let us suppose Alice and Bob decide to make measurements in the $(|a\rangle,|b\rangle)$ subspace, so they measure in either the $\{|a\rangle,|b\rangle\}$ basis or $\{(1/\sqrt{2})(|a\rangle+|b\rangle),(1/\sqrt{2})(|a\rangle-|b\rangle)\}$ basis. If the state they shared was $|\Psi_{ab}\rangle$, then they would get perfectly correlated measurement outcomes provided they measured in the same basis. In the case in which the state they shared was $|\Psi_{bc}\rangle$ either Alice or Bob will get a click in his or her detector if they measure in the $\{|a\rangle,|b\rangle\}$ basis since $|\Psi_{bc}\rangle$ has a component in $|b\rangle$. However, in this case it is impossible for both Alice and Bob to get a click in their detectors, since if one measures the state of the particle to be in $|a\rangle$, then the other party's particle will be in state $|c\rangle$, which is not within the two-dimensional subspace in which they are making the measurement. A similar argument holds for the $\{(1/\sqrt{2})(|a\rangle+|b\rangle),(1/\sqrt{2})(|a\rangle-|b\rangle)\}$ basis, it is impossible for both Alice and Bob to get a click in their detectors. Hence, for QKD purposes Alice and Bob will disregard the measurements (1) in which they did not measure in the same basis, and (2) when they did not both register a click in their detectors. The remaining measurements they made will be perfectly correlated.

In fact, Alice and Bob do not even need to previously agree upon the subspace in which they make the measurement. They can randomly choose the subspace and add to the two previous criteria that they also disregard the measurements made in different subspaces.

The two parties involved must decide on whether they would want to perform a QKD protocol or a QSS protocol before they make any measurements. They cannot measure in the three-dimensional basis described in the QSS protocol and later decide to change to a QKD protocol, nor can they measure in the reduced space for the QKD protocol and decide to perform a QSS protocol.

IV. SECURITY ANALYSIS FOR THE QKD PROTOCOL

Here we will discuss the security of the QKD protocol in the presence of an eavesdropper. In particular, we will focus on an eavesdropping attack in which the eavesdropper employs a universal quantum cloning machine (UQCM). First, Eve intercepts Alice's particle and makes two copies of it using the UQCM. Eve keeps one copy to herself and sends the other copy to Alice. After Alice and Bob make their measurements and publish the basis for which they made their measurements, Eve will measure her particles in the same basis as Bob. The scheme would work perfectly if not for the fact that the UQCM cannot make two perfect quantum copies of the intercepted particle. In fact, the maximum value of the fidelity of the two copies are given in Ref. [18] to be $F=(M+2)/[2(M+1)]$, where M is the dimensionality of the Hilbert space spanned by the quantum state being copied.

In presence of error, the mutual information between Alice-Bob and Alice-Eve is given by

FIG. 1. Transmission rate (number of usable bits per pair of particles measured in the same basis) versus the error rate (number of erroneous bits per pair of particles measured in the same basis) for the QKD scheme employing a tripartite three-level system described in this paper.

$$I_{\mathrm{AB}} = \log_2(M) + (1 - e_{\mathrm{Bob}})\log_2(1 - e_{\mathrm{Bob}}) + e_{\mathrm{Bob}} \log_2\left(\frac{e_{\mathrm{Bob}}}{M-1}\right), \tag{9}$$

$$I_{\mathrm{AE}} = \eta \log_2(M) + (1 - e_{\mathrm{Bob}})\log_2(1 - e_{\mathrm{Bob}}) + e_{\mathrm{Bob}} \log_2\left(\frac{e_{\mathrm{Bob}}}{M-1}\right), \tag{10}$$

where η is the fraction of the particle Eve listens into and $e_{\mathrm{Bob}} = \eta(1-F)$ is the effective error rate in Bob's measurement [19]. The lower bound of the transmission rate such that the parties can generate a key reliably is given by [19–21]

$$R_{AB}(\eta) = \frac{1}{N}(I_{\mathrm{AB}} - I_{\mathrm{AE}}) = \frac{1-\eta}{N} \log_2(M), \tag{11}$$

where N is the number of different sets of bases used by Alice and Bob. In the particular example of the tripartite three-level system the number of basis $N=3$, as we can easily see from the reduced density matrix. For the generalized form of the state with P particles and P levels the number of bases is $N=P(P-1)/2$. Notice that in our scheme the number of bases to choose from is not constrained by $N=M+1$, which is the number of unbiased bases for an M-level quantum state. In particular, we are confining our measurement to a two-dimensional subspace, and for a two-level system there are three unbiased bases. For our example with a tripartite three-level system $N=3$. However, for higher-dimensional multipartite systems the number of reduced dimensional bases to choose from exceeds three. In Figs. 1 and 2 the transmission rate of the key is plotted against Bob's error rate. If the error rate exceeds the value of $e_{\mathrm{Bob}} = M/2(M+1)$, then the quantum channel is deemed to be unreliable since the error rate is too high to ensure the absence of an eavesdropper.

For the QKD protocol discussed in this paper, using the straightforward extension of Eq. (1) to M levels and M partitions, Eq. (11) can be expressed as

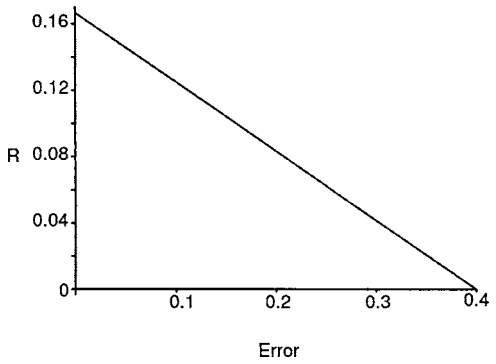

FIG. 2. Transmission rate versus the error rate for the QKD scheme employing a four-partite four-level system.

$$R_{AB}(e_{\mathrm{Bob}}) = 2\frac{[1 - 2e_{\mathrm{Bob}}(M+1)/M]}{M(M-1)} \log_2(M). \tag{12}$$

V. REALIZATION USING ORBITAL ANGULAR MOMENTUM OF LIGHT

Before we go on to discuss a possible realization of the protocols we would like to note that this is by no means an easy experiment, nor do we suggest an experiment be performed in the exact manner described here. The purpose of this section is to explore a possible implementation of the protocols using the orbital angular momentum of light, and to determine the difficulties associated with such an experiment.

Although the protocol is independent of any particular realization, here we present an implementation of the protocol using orbital-angular-momentum states of light. We present both a method to generate the initial entangled state and the means to detect both the orbital-angular-momentum states and their superposition.

It has been experimentally verified that the orbital angular momentum of a photon is conserved through spontaneous parametric down-conversion, and the daughter photons are entangled in their orbital angular momentum [11]. Since there is no upper bound to the orbital angular momentum a photon can carry, it is ideal for multidimensional quantum protocols.

First, we will have to generate the state the three parties are going to share. Here we will use three entangled sources, a three-beam coupler, three detectors, and a computer hologram, to differentiate between the different orbital-angular-momentum states of the photon. The method used is in the same spirit as the method used to generate GHZ states from two entangled sources [22].

The entangled source of light we are going to use is generated through spontaneous parametric down-conversion. Using a suitable computer-generated hologram to modify the pump beam, we can produce the following orbital angular momentum entangled state [12]:

$$|\Psi_{\mathrm{source}}\rangle = \frac{1}{\sqrt{3}}(|0,0\rangle + |1,1\rangle + |2,2\rangle). \tag{13}$$

We then take three of these sources and send one of each source's output into a three-beam coupler. At the output of

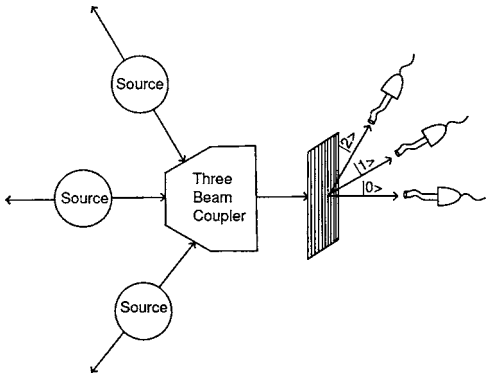

FIG. 3. Generation of tripartite three-level entangled state. The three photons that do not get detected are in the state $|\Psi_{\text{source}}\rangle$ provided all three detectors detect a photon.

the coupler we put another computer-generated hologram with one dislocation and we place a single-mode fiber that goes into a detector at each of the three diffraction orders as shown in Fig. 3. The hologram imparts a $\Delta l=0$ for the zeroth diffraction order, $\Delta l=1$ for the first diffraction order, $\Delta l=2$ for the second diffraction order, and so on to the input beam. The single-mode fibers only couple in the lowest-order orbital-angular-momentum states; hence the detector placed in the second diffraction order will click only if the diffracted photon was originally in the $l=2$ state [11]. If all three detectors register a photon then it means that the photons that were not detected have orbital angular momentum of $l=0$, 1, and 2, but we do not know which photon carries which state. Hence we are left with the state

$$|\Psi_{\text{tripartite}}\rangle = \frac{1}{\sqrt{6}}(|0,2,1\rangle + |0,1,2\rangle + |1,0,2\rangle + |1,2,0\rangle + |2,0,1\rangle + |2,1,0\rangle) = \frac{1}{\sqrt{6}}[(|2,1\rangle + |1,2\rangle)|0\rangle + (|2,0\rangle + |0,2\rangle)|1\rangle + (|0,1\rangle + |1,0\rangle)|2\rangle]. \quad (14)$$

This is the original state with which we started, Eq. (1), by replacing $|a\rangle$, $|b\rangle$, and $|c\rangle$ with $|0\rangle$, $|1\rangle$, and $|2\rangle$.

Now that we have the state that the three parties share, the problem we are left with is to detect the orbital-angular-momentum states and their superposition. This could also be done using holograms [14,15], but it is rather inefficient and it is not particularly suitable when considering single-photon states. The method of choice here is a simple interferometric scheme employing a Mach-Zehnder interferometer with Dove prisms in its paths [16].

In the first stage the Dove prisms in the two arms are rotated with respect to one another by an angle of $\alpha/2=\pi/2$ (see Fig. 4). This creates a relative phase shift between the beams in the two arms of $\theta=l\pi$, where l is the orbital-angular-momentum quantum number. The phase shift is produced because the Dove prism flips the transverse structure of the field. Since the Laguerre Gaussian modes have an $e^{il\phi}$ phase structure, the Dove prism serves as a device that imparts an l-dependent phase shift. Now, by adjusting the path difference appropriately one can make it so that the odd and

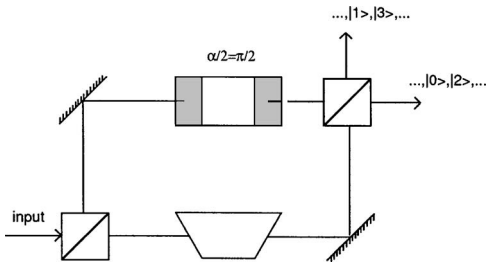

FIG. 4. Sorting orbital-angular-momentum states of light. The Dove prisms in the two arms are rotated with respect to one another by an angle of $\alpha/2=\pi/2$. With appropriate path differences the even and odd orbital-angular-momentum states emerge from different ports of the beam splitter.

even orbital-angular-momentum states come out of the two different output ports of the interferometer. The orbital-angular-momentum states of the incoming beam can be sorted out by cascading these devices with different angles between the Dove prisms [16]. The photon's state can then be collapsed into a particular l state by placing detectors at each of the output ports.

In detecting superposition states Eqs. (2)–(4), the problem comes down to determining the relative phase difference between the orbital-angular-momentum states. Since orthogonal states do not interfere with one another, we have to put holograms at each output port of the sorting device to convert them all into the same l state. After this is done the photons are sent through a three-port interferometer where the paths are appropriately adjusted so that the three output ports are the superposition states of interest [23].

For the case in which only two of the three parties want to generate a secure key the two parties use only two of the three output ports. This too is easily done with the existing setup. After the sorting device the two parties can measure in the orbital angular momentum basis, or its superposition in the two-dimensional space. Later, they will divulge both their measurement basis and the subspace they measured in to determine which measurements to keep.

VI. CONCLUSION

Here we have shown a tripartite three-level system that can be used for both secret-sharing protocols involving all three parties and quantum-key-distribution protocols between any two parties. The two parties generate a secret key by taking advantage of the residual entanglement of the reduced density matrix. This is done by making their measurements in a reduced space. A physical realization of this scheme has also been outlined through the use of entangled orbital-angular-momentum states of photons.

ACKNOWLEDGMENTS

We would like to thank John Howell, Govind Agrawal, Thomas Brown, and Miguel Alonso for helpful discussions. This work was supported in part by the ARO-adminstered MURI Grant No. DAAD 19-99-1-0252, and the NSF through the NIRT program.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[3] T. Durt, N. J. Cerf, N. Gisin, and M. Żukowski, Phys. Rev. A **67**, 012311 (2003).
[4] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[5] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, J. Phys. A **35**, 10065 (2002).
[6] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306 (2001).
[7] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[8] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[9] M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
[10] V. Scarani and N. Gisin, Phys. Rev. A **65**, 012311 (2001).
[11] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature (London) **412**, 313 (2001).
[12] J. P. Torres, Y. Deyanova, L. Torner, and G. Molina-Terriza, Phys. Rev. A **67**, 052313 (2003).
[13] S. Franke-Arnold, S. M. Barnett, M. J. Padgett, and L. Allen, Phys. Rev. A **65**, 033823 (2002).
[14] A. Vaziri, G. Weihs, and A. Zeilinger, J. Opt. B: Quantum Semiclassical Opt. **4**, 47 (2002).
[15] V. V. Kotlyar, V. A. Soifer, and S. N. Khonina, J. Mod. Opt. **44**, 1409 (1997).
[16] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, Phys. Rev. Lett. **88**, 257901 (2002).
[17] The state is similar to the state presented in Ref. [24].
[18] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).
[19] M. Bourennane, A. Karlsson, and G. Björk, Phys. Rev. A **64**, 012306 (2001).
[20] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres, Phys. Rev. A **50**, 1047 (1992).
[21] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[22] A. Zeilinger, M. A. Horne, H. Weinfurter, and M. Żukowski, Phys. Rev. Lett. **78**, 3031 (1997).
[23] M. Żukowski, A. Zeilinger, and M. A. Horne, Phys. Rev. A **55**, 2564 (1997).
[24] M. Fitzi, N. Gisin, and U. Maurer, Phys. Rev. Lett. **87**, 217901 (2001).