# Measuring Entangled Qutrits and Their Use for Quantum Bit Commitment

N. K. Langford,* R. B. Dalton, M. D. Harvey, J. L. O'Brien, G. J. Pryde, A. Gilchrist, S. D. Bartlett, and A. G. White

*Department of Physics, University of Queensland, Brisbane, QLD 4072, Australia*

(Received 30 November 2003; published 26 July 2004)

We produce and holographically measure entangled qudits encoded in transverse spatial modes of single photons. With the novel use of a quantum state tomography method that only requires two-state superpositions, we achieve the most complete characterization of entangled qutrits to date. Ideally, entangled qutrits provide better security than qubits in quantum bit commitment: we model the sensitivity of this to mixture and show experimentally and theoretically that qutrits with even a small amount of decoherence cannot offer increased security over qubits.

DOI: 10.1103/PhysRevLett.93.053601 PACS numbers: 42.50.Dv, 03.65.Wj, 03.67.Dd, 03.67.Mn

Many two-level quantum systems, or *qubits*, have been used to encode information [1]; using $d$-level systems, or *qudits*, enables access to larger Hilbert spaces, which can provide significant improvements over qubits such as increased channel capacity in quantum communication [2]. When entangled, *qutrits* ($d = 3$) provide the best known levels of security in quantum bit commitment and coin-flipping protocols, which cannot be matched using qubit-based systems [3]. The ability to completely characterize entangled qudits is critical for applications. This is only possible using quantum state tomography [4,5].

Entangled qudits have been realized in few physical systems, and only indirect measurements have been made of the quantum states of these systems. Qutrit entanglement has been generated between the arrival times of correlated photon pairs, where fringe measurements were used to infer features such as fidelities with specific entangled states and to estimate a potential Bell violation [6]. It is also possible to encode qudits in the transverse spatial modes of a photon, Fig. 1. There have been measurements demonstrating, but again not quantifying, spatial mode entanglement in parametric down-conversion [7], including fringe measurements [8,9] and the violation of a two-qutrit Bell inequality [10,11].

Here, we use quantum state tomography to completely characterize entangled, photonic qudits (both $d = 2$ and 3) encoded in transverse spatial modes, measuring the amount of entanglement and the degree of mixture. We show how to use the qutrit system in a quantum bit-commitment protocol and investigate the experimental requirements for achieving the best known security [3]. To illustrate these results, we first introduce and demonstrate two conceptually distinct ways of encoding information in transverse spatial modes, which differ in the behavior of superposition states. This work constitutes the most complete characterization of spatially encoded qubits and qutrits and the first quantitative measurement of entangled qutrit states.

The Gaussian spatial modes are a complete basis for describing the paraxial propagation of light [13]. Two orthonormal mode families are shown in Fig. 1(a): the Hermite-Gauss ($HG_{rs}$) and the Laguerre-Gauss-Vortex ($LGV_{pl}$). These modes are self-similar under propagation; modes of the same *order* experience the same propagation-dependent phase shift, the Gouy phase shift. We define *degenerate* qudits to be constructed from basis states of the same order [Fig. 1(b)]. Conversely, *nondegenerate* qudits contain states of different orders [Fig. 1(c)]; the different Gouy phases cause nondegenerate qudit superpositions to change phase as they propagate.

When encoding in photon polarization, the quantum state is manipulated with wave plates and selected using a polarizing beam splitter [14]. In spatial encoding, the wave plate function is achieved with a hologram, and the beam splitter with a single-mode fiber (SMF), which selects the lowest order spatial component ($HG_{00} \equiv LGV_{00} \equiv G$) and interferometrically rejects all higher-order modes. A spatial mode analyzer (SMA) combines these two components with a detector. The hologram first converts the target mode into the mode $G$, which is then

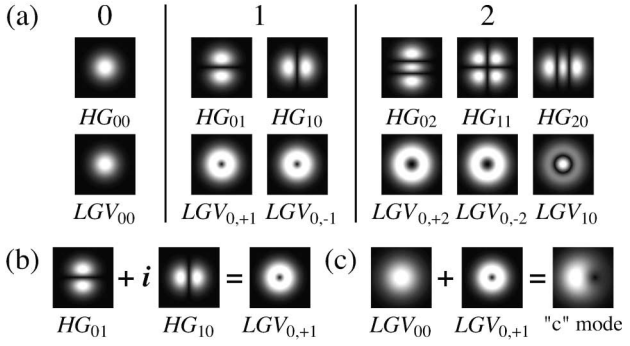


FIG. 1. (a) The first three orders of two paraxial mode families: the Hermite-Gauss modes ($HG_{rs}$), with $r$ horizontal and $s$ vertical lines of phase discontinuity; the Laguerre-Gauss-Vortex modes ($LGV_{pl}$), with $p$ ring phase discontinuities and a charge $l$ phase singularity, or vortex. The mode order is $r + s$ for $HG_{rs}$ modes and $2p + l$ for $LGV_{pl}$ modes. Superposition states for (b) degenerate and (c) nondegenerate qubits, where the logical modes are, respectively, of the same and different orders. The displaced singularity in the nondegenerate qubit moves around the beam center as it propagates.

 0031-9007/04/93(5)/053601(4)$22.50  

selected by the fiber, Fig. 2(a). All other modes are rejected, Fig. 2(b), with typical extinctions of $\sim 10^{-3}$—equivalent to standard commercial polarizing beam splitters. We use different holograms to measure different states, as described below.

Quantum state tomography requires a series of complementary measurements on a large ensemble of identically prepared copies of the system [4]. Rather than measure $d$-part superpositions [5], we choose a set of measurements constructed from only basis states, $|j\rangle$, and two-state superpositions, $|p^+\rangle$ and $|q^+\rangle$, where $|p^\pm\rangle = (|j\rangle \pm |k\rangle)/\sqrt{2}$, $|q^\pm\rangle = (|j\rangle \pm i|k\rangle)/\sqrt{2}$, and $j, k \in \{0, 1, \ldots, d-1\}$ [15]. In practice, we use an overcomplete set including $|p^-\rangle$ and $|q^-\rangle$, which allows more accurate normalization when converting the data to measurement probabilities. We obtain a physical density matrix using an optimization procedure [4]; the overspecification also makes this optimization less sensitive to outlying data points. Using this two-state tomographic technique, we characterize the output from a type-I down-conversion source pumped by a blue diode laser [Fig. 2(c)]. The two SMAs image partial, banana-shaped sections of the cone

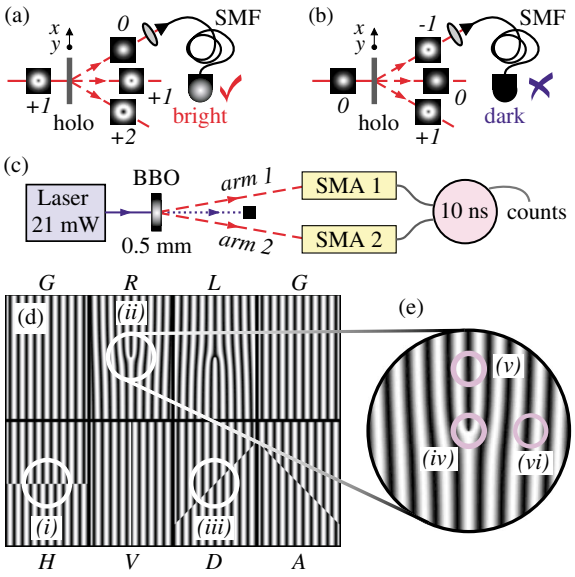


FIG. 2 (color online). Quantum state tomography of spatial modes. A spatial mode analyser (SMA) realized with a $LGV_{0,+1}$ hologram: (a) the target mode ($LGV_{0,+1}$) couples into a single-mode fiber (SMF); (b) other modes (e.g., $LGV_{00}$) are rejected. The images are labeled with the charge of the phase singularity in the beam. (c) Conceptual layout for tomography. Two SMAs analyze the mode of the energy degenerate pairs (820 ± 10 nm), postselected by counting in coincidence for 100 s with fiber-coupled avalanche photodiodes ($\sim$ 100 counts/s). (d) The 8-segment analysis hologram [29] used in all our experiments: the labels ($G$, $R$, etc.) correspond to the main spatial mode analyzed by that segment. The positions ($i$)–($iii$) for (d) degenerate and ($iv$)–($vi$) for (e) nondegenerate qubits correspond, respectively, to measuring one computational basis state and the two equal superposition states, $(|0\rangle + i|1\rangle)/\sqrt{2}$ and $(|0\rangle + |1\rangle)/\sqrt{2}$.

of energy degenerate photon pairs and so see significant contributions from spatial components other than $G$.

The simplest degenerate qubit encoding has first order logical basis states, e.g., $HG_{10} \equiv 0$, $HG_{01} \equiv 1$. The corresponding physical measurements required for tomography are then the states described by Padgett *et al.* [16]: the $HG_{01}$-type modes with horizontal ($H$), vertical ($V$), diagonal ($D$), and antidiagonal ($A$) phase discontinuities, and the $LGV_{0,\pm1}$ modes with charge ±1 phase singularities (right, $R$, and left, $L$). These states are measured using six different plane-wave hologram segments as shown in Fig. 2(d) [17]. To test the performance of the SMA, we holographically created and measured a range of single qubit states using a coherent source (10 mW HeNe laser). In all cases, we obtained extremely high purities ($> 0.999$) and fidelities with their ideal counterpart ($> 0.98$). Figure 3(a) shows the two-photon state of the down-converter measured in the qubit basis: the state is highly entangled, the fidelity with the maximally entangled $\phi^+$ Bell state is $F_{\phi^+} = 0.97$. The degree of entanglement and mixture of the measured state is quantified, respectively, by the *tangle*, $T = 0.90$, and *linear entropy*, $S_L = 0.06$ [14].

The simplest nondegenerate qubit encoding has zero ($G \equiv 0$) and first order (e.g., $R$ or $L \equiv 1$) basis states. The basis states are measured with the appropriate hologram segments, and the superposition states are simply accessed by displacing the $R$ or $L$ singularity a distance $\omega/\sqrt{2}$ from the center of the beam, Fig. 2(e), where $\omega$ is the intensity $1/e^2$ point [18,19]. The analyzer quality is

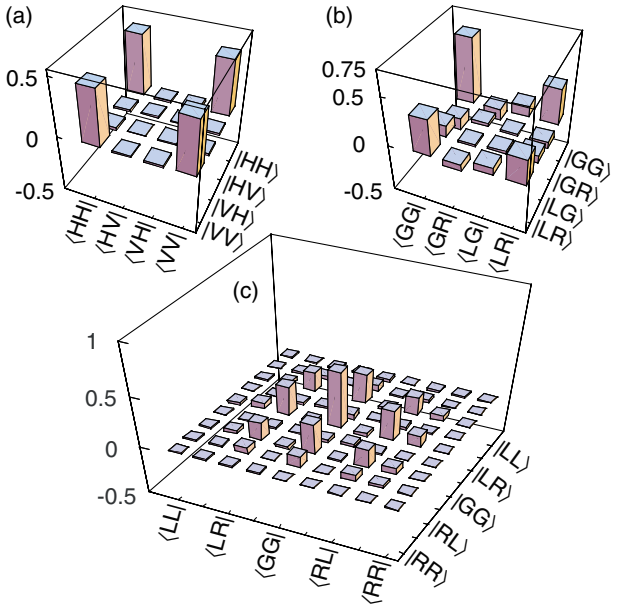


FIG. 3 (color online). Measured density matrices (real parts) for (a) entangled degenerate qubits ($H \equiv 0$, $V \equiv 1$); (b) entangled nondegenerate qubits, ($G \equiv 0$, $L \equiv 1$ in arm 1; $G \equiv 0$, $R \equiv 1$ in arm 2); and (c) entangled nondegenerate qutrits, ($L \equiv 0$, $G \equiv 1$, $R \equiv 2$), where every second row is labeled. For all three cases, imaginary components were $<0.03$.

equivalent to the degenerate case. The measured nondegenerate, two-qubit state [Fig. 3(b), $T = 0.65$ and $S_L = 0.11$] has a lower tangle, reflecting the larger component of $G$ in the down-conversion beam. This state has a high fidelity, $F = 0.95$, with a nonmaximally entangled state [21] of the form $(|GG\rangle + \varepsilon|LR\rangle)/\sqrt{1+\varepsilon^2}$ for $\varepsilon = 0.60$. The results for both types of qubit indicate that a Bell inequality could be violated [12].

We now encode a nondegenerate qutrit using basis states from the lowest two mode orders [10]: $L \equiv 0$, $G \equiv 1$, and $R \equiv 2$. Our two-state tomographic technique enabled us to use the hologram in Figs. 2(d) and 2(e); the resulting measured two-qutrit state is shown in Fig. 3(c). This state is quite pure, with linear entropy $S_L = 0.18$, and highly entangled. There are several ways to quantify the entanglement of this state. Given the relative populations of the basis states, we expect a nonmaximally entangled state of the form, $(|LR\rangle + \varepsilon|GG\rangle + |RL\rangle)/\sqrt{2+|\varepsilon|^2}$; for $\varepsilon = 1.79e^{-0.07i\pi}$, found using numerical optimization, the fidelity between the ideal and measured nonmaximally entangled states is $F = 0.88$. More directly, we calculate an upper bound to the measured *entanglement of formation* of 0.74 [22,23].

One advantage that entangled qutrits offer over qubits is increased security in cryptographic protocols such as quantum bit commitment (BC) and coin flipping. Quantum BC binds a sender (Alice) to one message (a bit) and prevents the receiver (Bob) from determining the message before Alice later chooses to reveal it. BC is the basis for the most secure known strong quantum coin-flipping protocols [3]. While BC protocols with unconditional security are impossible [26,27], they can be partially secure [3]. The best known BC protocols are purification protocols, where Alice supplies the only quantum system, which consists of two parts. She sends the *token* subsystem to Bob to commit her bit and the *proof* subsystem later to reveal it. Maximum security in such protocols can be achieved by using two entangled qutrits for the token and proof, but not qubits.

We now outline one procedure for using our entangled qutrit state analyzed above to implement a purification BC protocol. Depending on her choice of bit, Alice should prepare two qutrits in one of the orthogonal states $|0\rangle_L = \sqrt{\lambda}|12\rangle + e^{i\phi}\sqrt{1-\lambda}|01\rangle$ or $|1\rangle_L = e^{i\phi}\sqrt{1-\lambda}|21\rangle + \sqrt{\lambda}|10\rangle$, where $\lambda$ is a parameter characterizing the security of the protocol. To prepare such states using our system, Alice needs to postselect the entangled states that have no photons in one of the basis modes of one subsystem: e.g., consider the proof subsystem in arm 1: zero photons in the "2" basis mode yield $|0\rangle_L$; zero photons in the "0" mode yield $|1\rangle_L$. In principle, manipulating the individual modes of the proof subsystem can be accomplished using a holographic interferometer in that arm. Postselection would then require either perfect detectors or spatial-mode quantum nondemolition (QND) measurements. Here, however, we simulate this process and reconstruct the new states [28]. The logical states are then created by swapping the remaining proof subsystem modes. Figures 4(a) and 4(b) show the two-qutrit logical states that result from this simulated state preparation step. In this simulation, the only imperfections in the protocol arise from the initial state, thus giving a bound for the usefulness of our entangled qutrits.

After preparing the appropriate state, Alice then sends the token qutrit to Bob. Because of the entanglement (quantified by $\lambda$), the reduced token state possessed by Bob is mixed, which lies at the heart of the security of the purification protocol. The fact that *orthogonal* two-qutrit logical states produce *nonorthogonal* token states provides some security against Bob cheating. His maximum knowledge gain, $K$, is limited by the distinguishability of these states and quantified by the trace distance. However, it is this partial distinguishability which in turn limits Alice's ability to cheat and change her bit after her commitment. Her maximum control, $C$, can be quantified by the fidelity between the token states. Details can be found in Ref. [3]. The protocol is concluded by Alice sending the proof qutrit to Bob, who performs the

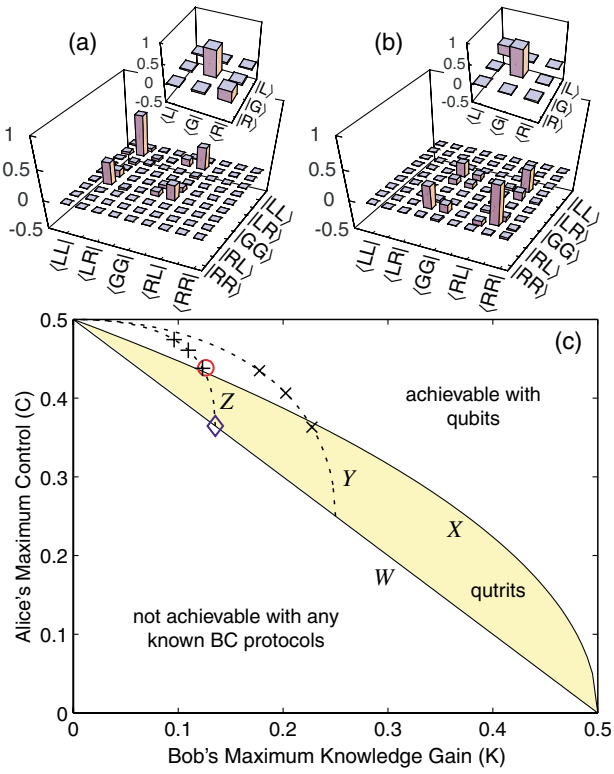


FIG. 4 (color online). A purification bit-commitment (BC) protocol. The logical bits generated by Alice as described in the text: (a) $|0\rangle_L$; (b) $|1\rangle_L$. Insets: Bob's reduced density matrices—the token subsystems. (c) Plot of Alice's control vs Bob's knowledge gain. ○: the measured protocol; ◇: the closest ideal protocol. $W$ and $X$: the best known qutrit and qubit protocols. $Y$ and $Z$: imperfect purification protocols with token states of the form, $\rho_{0,1} = p/3I + (1-p)\rho_{0,1}^{\text{ideal}}$, where $Y$ is $\lambda = 0.5$ and $Z$ is $\lambda = 0.27$. The positions for $p = 0.09$, 0.19, and 0.29 are marked with × ($Y$) and + ($Z$).

orthogonal, two-qutrit projective measurement, and either decodes the bit $\{|0\rangle_L\langle 0|, |1\rangle_L\langle 1|\}$ or catches Alice cheating.

Figure 4(c) shows a plot of $C$ vs $K$, where the bottom left corner represents unconditional security and the top right corner represents no security. The ideal token states for this scheme give $K = \lambda/2$ and $C = (1 - \lambda)/2$, and varying $\lambda$ produces the best known security curve ($W$). The shaded region between $W$ and $X$ highlights the area inaccessible to qubit-based, but accessible to qutrit-based BC protocols. The insets to Figs. 4(a) and 4(b) show the reduced density matrices for the token resulting from our initial state. They are closest to ideal states with $\lambda = 0.27$ ($F \sim 0.99$). However, in spite of this high fidelity, if we determine $C$ and $K$ directly from the measured token states, the protocol lies just inside the area accessible to qubits: a direct result of the slight ($< 3\%$) residual population in the other mode of Bob's token subsystems, originating from the defects of Alice's original state. In other words, a two-qutrit state with residual populations of $<1\%$ is required to surpass the qubit boundary ($X$).

To implement this BC protocol, Alice must be able to perform deterministic postselection (e.g., using QND measurements). This is hard. Even if she achieves this perfectly, we have shown that the protocol still lies in the qubit-accessible regime. In our simulation, the only differences between our protocol and the ideal resulted from imperfections in the initial state. This result demonstrates that the requirements on the initial two-qutrit entangled state are extremely stringent, and that future theoretical work in this area should consider the critical role of even small amounts of mixture.

We have performed the first full characterization of entangled, spatially encoded quantum states and achieved the first complete measurement of an entangled, two-qutrit state in *any* encoding, using a novel quantum tomography technique that requires only two-state superpositions. We have outlined a scheme for using this system to implement the best known BC protocol. With this measured state, this protocol would not reach maximal security, but we can see from the results what improvements are required. This analysis would have been impossible without access to the complete two-qutrit state, gained through quantum tomography.

This work was supported in part by the ARC and by the MURI Center for Photonic Quantum Information Systems, ARO/ARDA Program No. DAAD19-03-1-0199. A. G. acknowledges support from the NZ FRST, J. L. O'B. and G. J. P. from the ARC COE QCT.

*Corresponding author.
Email address: langford@physics.uq.edu.au.

[1] See, e.g., special issue of Quantum Inf. Comput. **1** (2001).
[2] M. Fujiwara *et al.*, Phys. Rev. Lett. **90** 167906 (2003).
[3] R. W. Spekkens *et al.*, Phys. Rev. A **65**, 012310 (2001).
[4] D. F. V. James *et al.*, Phys. Rev. A **64**, 052312 (2001).
[5] R. T. Thew *et al.*, Phys. Rev. A **66**, 012303 (2002).
[6] R. T. Thew *et al.*, Quantum Inf. Comput. **4**, 093 (2004).
[7] G. Molina-Terriza *et al.*, Opt. Commun. **228**, 155 (2003).
[8] A. Mair *et al.*, Nature (London) **412**, 313 (2001).
[9] A. Vaziri *et al.*, Phys. Rev. Lett. **91** 227902 (2003).
[10] A. Vaziri *et al.*, Phys. Rev. Lett. **89**, 240401 (2002).
[11] Violating Bell's inequality is not a measure of entanglement, as states with different amounts of entanglement and mixture can give the same Bell violation [12].
[12] W. J. Munro *et al.*, J. Mod. Opt. **48**, 1239 (2001).
[13] A. E. Siegman, *Lasers* (University Science Books, Mill Valley, CA, 1986).
[14] A. G. White *et al.*, Phys. Rev. A **65**, 012301 (2001).
[15] This forms the complete set $|j\rangle\langle k| = |p^+\rangle\langle p^+| + i|q^+\rangle\langle q^+| - |j\rangle\langle j|(i+1)/2 - |k\rangle\langle k|(i+1)/2$; see M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (CUP, Cambridge, 2000), p. 391.
[16] M. J. Padgett and J. Courtial, Opt. Lett. **24**, 430 (1999).
[17] Plane-wave holograms do not produce/analyze single Gaussian modes, e.g., $|\mathrm{LGV}_{0,-1}\rangle$. Instead they yield Gaussian-mode superpositions, e.g., $\sum_{i=0}^{\infty} c_i|\mathrm{LGV}_{i,-1}\rangle$, where $c_i > c_{i+1}$—a weighted sum of modes of the same charge ($-1$), but with increasingly greater spatial extent and number of circumferential rings. A good approximation to single-mode behavior can be obtained by appropriate normalization of the Stokes' parameters used in tomography, i.e., $S_j = (\mathcal{N}_X - \mathcal{N}_Y)/(\mathcal{N}_X + \mathcal{N}_Y)$, where $(j, X, Y)$ is $(1, H, V)$, $(2, D, A)$, or $(3, R, L)$, and $\mathcal{N}_X$ is the number of counts in the $X$ basis. If exact behavior is required, then Gaussian holograms should be used.
[18] A. Vaziri *et al.*, J. Opt. B Quantum Semiclassical Opt. **4**, S47 (2002).
[19] This should not be done for higher-order, $|l| > 1$, modes. Displacing a charge $|l| > 1$ hologram to measure nondegenerate qudit superpositions—as was done in [8,9]—analyses a superposition of several orders, not just the desired superposition of $|\zeta\rangle = (|\mathrm{LGV}_{00}\rangle + |\mathrm{LGV}_{0,\pm l}\rangle)/\sqrt{2}$. This is apparent in the output intensity pattern: a displaced charge $|l|$ hologram produces a mode with a single displaced vortex [8]; whereas a hologram for $|\zeta\rangle$ will produce/analyze a mode with $|l|$ single-charge vortices [20].
[20] M. S. Soskin *et al.*, Phys. Rev. A **56**, 4064 (1997).
[21] A. G. White *et al.*, Phys. Rev. Lett. **83**, 3103 (1999).
[22] C. H. Bennett *et al.*, Phys. Rev. A **54**, 3824 (1996).
[23] The pure-state qutrit entanglement of formation, EOF, is $-\mathrm{Tr}(\rho_A \log_3 \rho_A)$, where $\rho_A = \mathrm{Tr}_B \rho$ is the partial trace of the two-qutrit state, so that EOF = 1 for a maximally entangled state. Our EOF was calculated following the minimization algorithm given in [24] using the parametrization for unitaries given in [25]. Only $9 \times 9$ unitaries were searched, so the figure quoted is an upper bound.
[24] K. Audenaert *et al.*, Phys. Rev. A **64**, 052304 (2001).
[25] P. Dita, J. Phys. A **36**, 2781 (2003).
[26] H.-K. Lo *et al.*, Phys. Rev. Lett. **78**, 3410 (1997).
[27] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[28] By setting to zero terms associated with the zero-photon mode and renormalizing the remainder appropriately.
[29] Computer-generated, sinusoidal, phase gratings; diffraction angle of $\sim 0.28°$ at 670 nm; efficiencies of 20%–30%.