Entangled qutrits: production and characterisation

Nathan K. Langford, Rohan B. Dalton, Michael D. Harvey, Jeremy L. O'Brien,
Geoffrey J. Pryde, Alexei Gilchrist, Stephen D. Bartlett, and Andrew G. White

Centre for Quantum Computer Technology, Department of Physics,
University of Queensland, Brisbane, Queensland 4072, Australia
langford@physics.uq.edu.au *www.quantinfo.org*

(Dated: December 9, 2003)

We produce and measure entangled qubits and qutrits, two- and three-level quantum systems, realised using transverse spatial modes of the optical field. Photons encoded in these modes are manipulated and analysed by a combination of holograms and single-mode fibres. Using quantum state tomography, we achieve the most complete characterisation of entangled qutrits to date. Ideally, entangled qutrits provide better security than qubits in quantum bit-commitment and coin-flipping protocols: we show that to reach this regime places stringent requirements on the initial state.

PACS numbers: 42.50.Dv,03.67.Mn,03.65.Wj,03.67.Dd

Many two-level quantum systems, or *qubits*, have been used to encode information [1]; using higher-dimensional systems, however, enables access to larger Hilbert spaces, which can provide significant improvements over qubits such as increased channel capacity in quantum communication [2]. Such d-level systems, or *qudits*, have not been studied to the same extent. However, 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 characterise these entangled qutrit states is critical if they are to find application, and is only possible using quantum state tomography [4, 5].

Entangled qudits have been realised in few physical systems and information about the entanglement and quantum states of these systems has only been obtained indirectly. Qutrit entanglement has been generated and detected between the arrival times of correlated photon pairs, where a series of fringe measurements was used to infer facts about the quantum state such as fidelities with specific entangled states and an estimate of a potential Bell violation [6]. The transverse spatial modes of a photon (Fig. 1) also allow multi-level encoding. There have been measurements demonstrating, but not quantifying, spatial mode entanglement in paraxial parametric down-conversion [7], including fringe measurements [8, 9] and the violation of a two-qutrit Bell inequality [10].

Here, we use quantum state tomography to completely characterise two entangled, photonic qutrits encoded in transverse spatial modes. We show how this system can be used in a quantum bit-commitment protocol, investigating the experimental requirements for achieving the best known security [3]. To illustrate these qutrit results, we first introduce and demonstrate two conceptually distinct ways of encoding information in transverse spatial modes by post-selecting the chosen modes via coincidence detection. This work constitutes the most complete characterisation of spatially-encoded qubits and qutrits, and the first quantitative measurement of entangled qutrit states.

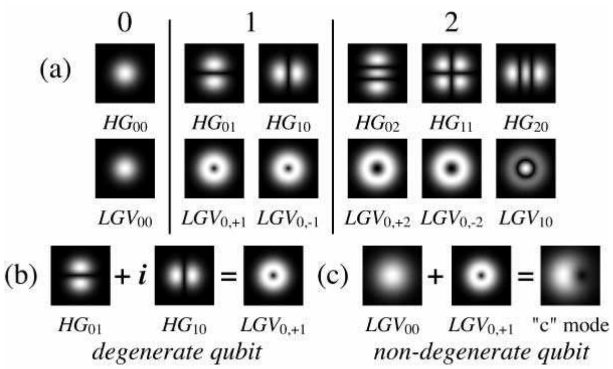

FIG. 1: (a) The first three orders of two Gaussian spatial mode families — the Hermite-Gauss modes (HG_{rs}), with r horizontal and s vertical lines of phase discontinuity, and the Laguerre-Gauss Vortex modes (LGV_{pl}), with p ring phase discontinuities and a charge l phase singularity, or vortex. The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

The Gaussian spatial modes are a complete basis for describing the paraxial propagation of light [11]. Fig. 1(a) shows two convenient ways of constructing orthonormal *mode families*: the Hermite-Gauss (HG_{rs}) and Laguerre-Gauss Vortex (LGV_{pl}) modes. These basic modes are *self-similar* under propagation, i.e., they have an unchanging intensity profile. These families can be further divided into *generations* of the same Gouy phase shift, which the beam experiences as it propagates through a focus. We define *degenerate* qudits to be constructed from basis states of the *same* generation, Fig. 1(b). Conversely, *non-degenerate* qudits contain states of different generations, Fig. 1(c), and thus different Gouy phase shifts, which causes the relative phases in superpositions of basis states to evolve under propagation, unlike the degenerate case.

When encoding in photon polarisation, the quantum state is manipulated with wave-plates and selected using a polarising beam-splitter [12]. In spatial encoding, the wave-plate function is achieved with a hologram, the beam-splitter with a single-mode fibre which selects the lowest order spatial component (the pure Gaussian: $HG_{00} \equiv LGV_{00}$) and interferometrically rejects all higher order modes. We produce a spatial mode analyser (SMA) by combining these two components with a detector. The hologram converts the target mode into a pure Gaussian which is selected by the fibre (Fig. 2(a)). All other modes are rejected (Fig. 2(b)) with typical extinctions of $\sim 10^{-3}$, equivalent to standard commercial polarising 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]. For n qudits, the minimum number of measurements is $N_{\min}{=}d^{2n}$. However, for two reasons, we use an over-complete set of physical measurements constructed from all possible basis states ($|j\rangle$) and two-state equal superpositions: $\frac{1}{\sqrt{2}}(|j\rangle \pm |k\rangle)$ and $\frac{1}{\sqrt{2}}(|j\rangle \pm \mathrm{i}|k\rangle)$ (N=6 and 15 for one qubit and qutrit; c.f. $N_{\min}$=4 and 9). Using all combinations allows more accurate normalisation when converting the data to measurement probabilities, from which we obtain an explicitly physical density matrix using an optimisation procedure [4]. The resulting over-specification also makes the optimisation routine far less sensitive to any outlying data points. Using this general tomographic technique, we characterised the output from a Type-I down-conversion crystal emitting a *c*one of energy degenerate photon pairs (Fig. 2(c)). The modes imaged by the two SMAs therefore have significant contributions from spatial components other than the pure Gaussian.

The simplest degenerate qubit encoding has first order logical basis states, e.g., HG_{10}="0", HG_{01}="1". The corresponding physical measurements required for tomography are then the states described by Padgett *et al.* [13]: the HG_{01}-type modes with horizontal (H), vertical (V), diagonal (D) and anti-diagonal (A) phase discontinuities, and the $LGV_{0,\pm 1}$ modes with charge ± 1 phase singularities (right, R, and left, L). These states are measured using 6 different hologram segments as shown in Fig. 2(d). To test the performance of the SMA, we created and measured a range of single-beam, two-level states using a coherent source (10mW, 632.8nm HeNe laser). In all cases, we obtained extremely high purities (>0.999) and fidelities with their ideal counterpart (>0.98). Fig. 3(a) is the measured two-photon state of the down-conversion output, giving an optimum fidelity with a maximally-entangled state of F_d=0.97. The amount of entanglement and mixture of the state is quantified by the *tangle*, T=0.90, and *linear entropy*, S_L=0.06 [12], respectively.

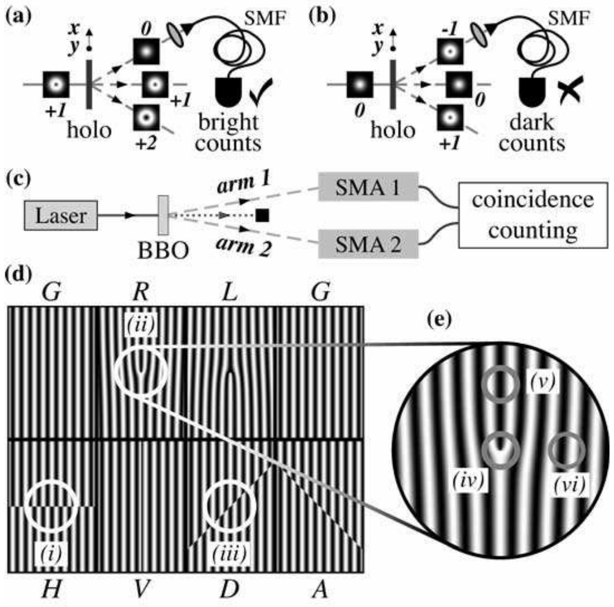

FIG. 2: Quantum state tomography of spatial modes. A spatial mode analyser (SMA) (the example shown is for a $LGV_{0,+1}$ hologram) – (a) the target mode ($LGV_{0,+1}$) couples into a single-mode fibre; (b) other modes (e.g. LGV_{00}) are rejected (details in text). The images are labelled with the charge of the phase singularity in the beam. (c) Conceptual layout for tomography. Pairs of single photons, post-selected by counting in coincidence (10 ns coincidence window, 10 nm detection bandwidth), were produced using a 0.5mm thick BBO (β-barium borate) crystal (optical axis at 28.7°), pumped with a blue diode laser (411nm, 21mW at the crystal). Two SMAs analyse the mode of the energy degenerate pairs, detected using fibre-coupled avalanche photodiodes (EG&G SPCM-AQR). The pump was focussed to $\sim$40μm at the crystal to optimise mode-matching to the fibres. (d) The 8-segment, analysis hologram used in all of our experiments: the labels correspond to the main spatial mode analysed by that segment (see text for definitions). They were computer-generated sinusoidal gratings (diffraction angle of $\sim 0.28°$ at 670nm), contact-printed onto holographic plates and bleached to produce a phase-modulated pattern, giving efficiencies of $20-30\%$, where the theoretical maximum efficiency for sinusoidal holograms is $\sim$34%. Blazed holograms, however, can reach 100%. The hologram positions (*i-iii*) for (d) degenerate and (*iv-vi*) for (e) non-degenerate qubits correspond respectively to measuring the basis state $|1\rangle$, and the two equal superposition states, $\frac{1}{\sqrt{2}}(|0\rangle + \mathrm{i}|1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$.

The simplest non-degenerate qubit encoding has zero and first order basis states, e.g., the pure Gaussian LGV_{00}="0" (G), and one of the first order vortex modes, $LGV_{0,+1}$="1" (R) or $LGV_{0,-1}$="1" (L). 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 centre of the beam (Fig. 2(e)), where ω is the intensity $1/e^2$ point [14]. The analyser quality is equiv-

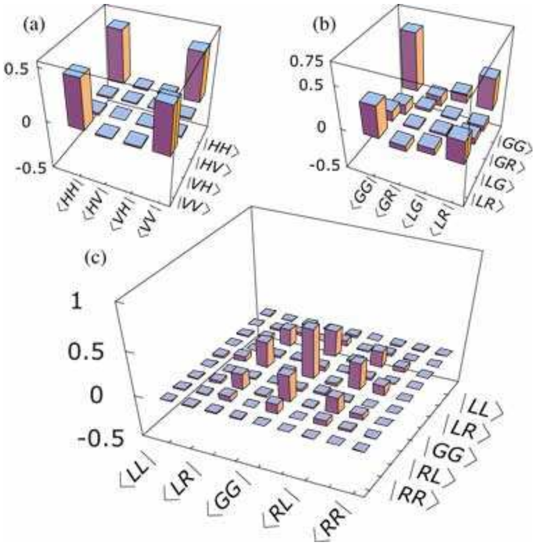

FIG. 3: Measured density matrices (real parts) for: (a) entangled degenerate qubits (H="0", V="1"); (b) entangled non-degenerate qubits, (G="0", L="1") in arm 1 and (G="0", R="1") in arm 2; and (c) entangled non-degenerate qutrits, (L="0", G="1", R="2"), where every second row is labelled. For all three cases, undesirable imaginary components were <0.03.

alent to the degenerate case. Note that this technique for measuring superpositions cannot be used for higher-order LGV modes, as adding a pure Gaussian component causes a charge l singularity to split into $|l|$ single-charge vortices [15]. The measured non-degenerate, 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_n=0.95) with a non-maximally entangled state of the form $\frac{1}{\sqrt{1+\varepsilon^2}}(|GG\rangle + \varepsilon|LR\rangle)$ for ε=0.60. The results for both types of qubit indicate that a Bell inequality could be violated [16].

We now encode a non-degenerate qutrit using basis states from the lowest two mode orders [10]: L="0", G="1" and R="2". Ref. [5] generalises quantum state tomography to higher-dimensional systems and describes an example of a complete set of qutrit measurements involving various three-state superpositions. However, the physical measurements we describe above (involving only basis states and two-state superpositions) are complete and, more importantly, easily accessible. All our qutrit measurements were performed using the hologram in Fig. 2(d): 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 of quantifying the entanglement of this state. Given the relative populations of the basis states, we expect a non-maximally entangled state of the form, $(2 + |\varepsilon|^2)^{-\frac{1}{2}}(|LR\rangle + \varepsilon|GG\rangle + |RL\rangle)$. For ε=1.79 $\exp(-i0.07\pi)$ (found using numerical optimisation), the fidelity between the ideal and measured non-maximally entangled states is F=0.88. We calculated an upper bound to the measured *entanglement of formation* [17] of 0.74. The minimisation required for mixed states was conducted over pure-state decompositions of the density matrix with no more than nine (i.e., d^2) elements and the entanglement is scaled such that a value of 1 corresponds to a maximally-entangled state (ε=1).

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 chooses later 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 [18], 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, but not qubits, for the token and proof.

We now outline one procedure for using our entangled qutrit state analysed above to implement a purification BC protocol. Depending on her choice of bit, Alice should prepare two qutrits in one of the following orthogonal states:

$$\begin{aligned}|0\rangle_L &= \sqrt{\lambda}|12\rangle + e^{i\phi}\sqrt{1-\lambda}|01\rangle \\ |1\rangle_L &= e^{i\phi}\sqrt{1-\lambda}|21\rangle + \sqrt{\lambda}|10\rangle,\end{aligned}$$

where λ is a parameter characterising the security of the protocol. To prepare such states using our system, Alice needs to post-select the entangled states with no photons in one mode of one subsystem (e.g. for the proof subsystem in arm 1: zero photons in "2" to prepare $|0\rangle_L$, "0" for $|1\rangle_L$). In principle, manipulating the individual modes of the proof subsystem can be accomplished using a holographic interferometer in that arm. Post-selection would then require either perfect detectors or QND measurements. Here, however, we simulate this process [19] and then reconstruct the new states. This simulation produces a protocol where the only imperfections in the protocol arise from the initial state, which will give us a bound for the utility of our entangled qutrits. The logical states are then created by swapping the remaining proof subsystem modes. Figs 4(a) and (b) show the two-qutrit logical states that would result from this simulated state preparation step.

After preparing the appropriate state, Alice then sends the token qutrit to Bob. Because of the entanglement (quantified by λ), the reduced token state possessed by Bob is mixed, which lies at the heart of the security of the purification protocol. The *orthogonal* two-qutrit logical states produce *non-orthogonal* token states, which pro-

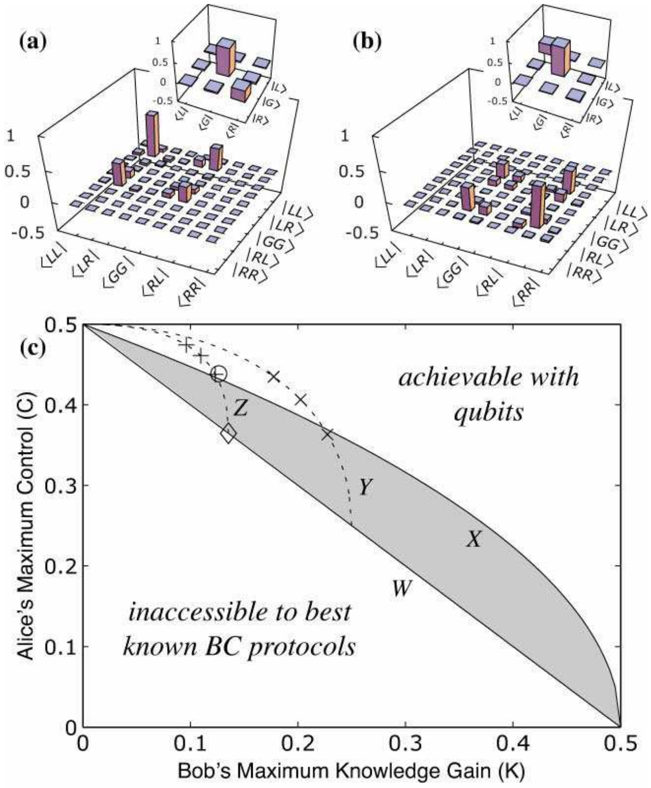

FIG. 4: A purification bit-commitment (BC) protocol. The logical bits generated by Alice as described in the text: (a) $|0\rangle_L$; (b) $|1\rangle_L$. Insets: Bob's reduced density matrices (the token subsystem). (c) Plot of Alice's Control vs Bob's Knowledge Gain. ◯: the measured protocol; ◇: the closest ideal protocol. W: the optimal qutrit protocols; X: the optimal qubit protocols. Y & Z: Imperfect purification protocols with token states of the form, $\rho_{0,1} = \frac{p}{3}I + (1-p)\rho_{0,1}^{\text{ideal}}$, where Y is λ=0.5 and Z is λ=0.27. The positions for $p = 0.09, 0.19, 0.29$ are marked with $\times$ (Y) and $+$ (Z).

vides some security against Bob cheating. His maximum knowledge gain (K) is limited by their distinguishability, and quantified by the trace distance. However, it is this partial distinguishability which in turn limits Alice's ability to cheat by changing 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 Bob the proof qutrit, who performs the orthogonal, two-qutrit projective measurement, and either decodes the bit $\{|0\rangle_L\langle 0|, |1\rangle_L\langle 1|\}$, or catches Alice cheating.

Fig. 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 $K{=}\frac{\lambda}{2}$ and $C{=}\frac{1-\lambda}{2}$, and varying λ produces the optimal Alice-supplied security curve (W). The shaded region highlights the area inaccessible to qubit-based, but accessible to qutrit-based BC protocols (between W and X). The insets to Fig. 4(a) and (b) show the reduced density matrices for the token resulting from our initial state, which are closest to ideal states with λ=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 impurity 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 post-selection (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.

We have performed the first full characterisation of entangled, spatially-encoded quantum states using quantum state tomography, which also constitutes the first complete measurement of an entangled, two-qutrit state. We have also outlined a scheme for using this system to implement the best known BC protocol. With this measured state, this protocol would not reach optimal 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.

Acknowledgements: This work was supported in part by the Australian Research Council (ARC), the US Army Research Office (ARO) and Advanced Research and Development Activity (ARDA). AG acknowledges support form the New Zealand Foundation for Research, Science and Technology (FORT).

[1] Quant. Inform. Comput. **1** (2001).
[2] M. Fujiwara et al., e-print quant-ph/0304037 (2003).
[3] R. W. Spekkens and T. Rudolph, 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., e-print quant-ph/0307122 (2003).
[7] G. Molina-Terriza et al., Opt. Comm. **228**, 155 (2003).
[8] A. Mair et al., Nature **412**, 313 (2001).
[9] A. Vaziri et al., e-print quant-ph/0303003 (2003).
[10] A. Vaziri et al., Phys. Rev. Lett. **89**, 240401 (2002).
[11] A. E. Siegman, *Lasers* (University Science Books, Mill Valley, CA, 1986).
[12] A. G. White et al., Phys. Rev. A **65**, 012301 (2001).
[13] M. J. Padgett and J. Courtial, Opt. Lett. **24**, 430 (1999).
[14] A. Vaziri et al., J. Opt. B-Quantum S. O. **4**, S47 (2002).
[15] M. S. Soskin et al., Phys. Rev. A **56**, 4064 (1997).
[16] W. J. Munro et al., J. Mod. Opt. **48**, 1239 (2001).
[17] C. H. Bennett et al., Phys. Rev. A **54**, 3824 (1996); N.B. Here, we have defined the pure-state *qutrit* entanglement of formation to be $-\text{Tr}(\rho_A \log_{\mathbf{3}} \rho_A)$, where $\rho_A{=}\text{Tr}_B\rho$ is the partial trace of the two-qutrit state, so that it is 1 for a maximally-entangled state.

[18] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997); D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[19] We do this by only considering the contribution of the remaining two modes of the proof subsystem in the two-qutrit tomographic reconstruction, e.g. for $|0\rangle_L$, we only consider the "0" and "1" modes and define $P_{2k}{=}\langle 2k|\rho|2k\rangle{=}0$ and $P_{\phi_{j2},k}{=}\frac{1}{2}P_{jk}$ $(j{=}\{0,1\})$, where $\phi_{j2}{=}\frac{1}{\sqrt{2}}(|j\rangle + e^{\mathrm{i}\phi}|2\rangle)$. This is equivalent to physically discarding this mode of the proof subsystem.