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, qudits (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 entangled qudits is critical for applications. This is only possible using quantum state tomography 4,5.

Entangled qudits have been realised 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 downconversion 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 characterise 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 behaviour of superposition states. This work constitutes the most complete characterisation of spatially-encoded qudits 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 12,13. Two orthonormal mode families are shown in Fig. 1(a): the Hermite-Gauss (HGrs) and Laguerre-Gauss-Vortex (LGVpl). 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, non-degenerate qudits contain states of different orders [Fig. 1(c)]; the different Gouy phases cause non-degenerate qudit superpositions to change phase as they propagate.

When encoding in photon polarisation, the quantum state is manipulated with wave plates and selected using a polarising beam splitter 14. In spatial encoding, the wave-plate function is achieved with a hologram, and the beam-splitter with a single-mode fibre (SMF), which selects the lowest order spatial component (HG00 \equiv LGV00 \equiv G) and interferometrically rejects all higher order modes. A spatial mode analyser (SMA)
combines these two components with a detector. The hologram first converts the target mode into the mode $G$, which is then 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 $\mathbb{E}$. Rather than measure $d$-state superpositions $\mathbb{E}$, we choose a set of measurements constructed from only basis states, $|j\rangle$, and two-state superpositions, $|p\rangle$ and $|q\rangle$, where $|p\rangle=\langle j|+|k\rangle/\sqrt{2}$, $|q\rangle=\langle j|\pm|k\rangle/\sqrt{2}$, and $j, k \in \{0, 1, \ldots, d-1\}$. In practice, we use an over-complete set including $|p\rangle$ and $|q\rangle$, which allows more accurate normalisation when converting the data to measurement probabilities. We obtain a physical density matrix using an optimisation procedure $\mathbb{E}$: the over-specification also makes the optimisation less sensitive to outlying data points. Using this two-state tomographic technique, we characterise 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 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. $\mathbb{E}$: 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 $\pm 1$ phase singularities (right, $R$, and left, $L$). These states are measured using 6 different plane-wave hologram segments as shown in Fig. 2(d) $\mathbb{E}$. 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 ($>0.98$). Fig. 2(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 $\mathbb{E}$, $T=0.90$, and linear entropy, $S_L=0.06$ $\mathbb{E}$.

The simplest non-degenerate qubit encoding has zero

FIG. 2: Quantum state tomography of spatial modes. A spatial mode analyser (SMA) realised with a LGV$_{0,\pm 1}$ hologram: (a) the target mode (LGV$_{0,\pm 1}$) couples into a single-mode fibre; (b) other modes (e.g. LGV$_{00}$) are rejected. The images are labelled with the charge of the phase singularity in the beam. (c) Conceptual layout for tomography: Two SMAs analyse the mode of the energy degenerate pairs (820±10 nm), postselected by counting in coincidence for 100 s with fibre-coupled avalanche photodiodes (≈ 100 counts/s). (d) The 8-segment analysis hologram $\mathbb{E}$ used in all our experiments: the labels ($G$, $R$, $etc.$) correspond to the main spatial mode analysed by that segment. The positions (i-iii) for (d) degenerate and (iv-vi) for (e) non-degenerate qubits correspond, respectively, to measuring one computational basis state and the two equal superposition states, $(|0\rangle + i|1\rangle)/\sqrt{2}$ and $(|0\rangle + |1\rangle)/\sqrt{2}$.

FIG. 3: Measured density matrices (real parts) for: (a) entangled degenerate qubits ($H \equiv 0$, $V \equiv 1$); (b) entangled non-degenerate qubits, ($G \equiv 0$, $L \equiv 1$ in arm 1; $G \equiv 0$, $R \equiv 1$ in arm 2); and (c) entangled non-degenerate qutrits, ($L \equiv 0$, $G \equiv 1$, $R \equiv 2$), where every second row is labelled. For all three cases, imaginary components were <0.03.
(G ≡ 0) and first order (e.g. R or L ≡ 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 ω/√2 from the centre of the beam [Fig. 3(c)], where ω is the intensity 1/e² point [10, 13]. The analyser quality is equivalent to the degenerate case. 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=0.95, with a nonmaximally entangled state [21] of the form (∝GG + ε|LR⟩)/√(1 + ε²) for ε=0.60. The results for both types of qubit indicate that a Bell inequality could be violated [12].

We now encode a non-degenerate qutrit using basis states from the lowest two mode orders [10]: L ≡ 0, G ≡ 1 and R ≡ 2. Our two-state holographic technique enabled us to use the hologram in Fig. 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 non-maximally entangled state of the form, (∝|GG⟩ + ε|R⟩)/√(1 + ε²); for ε≈1.79e⁻⁰.⁰⁷iπ, found using numerical optimisation, 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 [22 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 analysed 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⟩_L = √λ|12⟩ + e⁻iθ√1 - λ|01⟩ or ∝|1⟩_L = e⁻iθ√1 - λ|21⟩ + √λ|10⟩, where λ is a parameter characterising 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⟩_L; zero photons in the “0” mode yield |1⟩_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 [23]. The logical states are then created by swapping the remaining proof subsystem modes. Fig. 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 λ), 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 non-orthogonal token states provides some security against Bob cheating. His max-

![FIG. 4: A purification bit-commitment (BC) protocol.](image-url)
minimum 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 orthogonal, two-qutrit projective measurement, and either decodes the bit \( \{|0\rangle_L, |1\rangle_L\} \) 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 Alice-supplied 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 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 \( C_{residual} = 0.27 \) (for \( \lambda = 0.99 \)). 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 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 characterisation 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 only requires 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 DAAD19-03-1-0199. A. G. acknowledges support from the NZ FRST, J. L. O’B. and G. J. P. from the ARC COE CQCT.

[1] See e.g. special issue: Quant. Inform. 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., Quant. Inform. Comp. 4, 093 (2004).
[7] G. Molina-Terriza et al., Opt. Comp. 228, 155 (2003).
[8] A. Mair et al., Nature 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] 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 \( |1\rangle = (|p^+\rangle + i|q^+\rangle) / \sqrt{2} \). Instead they yield Gaussian-mode superpositions, e.g. \( \sum_{i=0}^{\infty} c_i LGV_{i,-1} \), 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 behaviour can be obtained by appropriate normalisation of the Stokes’ parameters used in tomography, i.e. \( S_i = (N_X - N_Y) / (N_X + N_Y) \), where \( \langle j, X, Y \rangle \) is \((1, H, V)\), \((2, D, A)\), or \((3, R, L)\), and \( N_X \) is the number of counts in the \( X \) basis. If exact behaviour is required, then Gaussian holograms should be used.
[16] A. Vaziri et al., J. Opt. B 4, S47 (2002).
[17] Plane-wave holograms do not produce/analyse single Gaussian modes, e.g. \( |LGV_{0,-1}\rangle \). Instead they yield Gaussian-mode superpositions, e.g. \( \sum_{i=0}^{\infty} c_i LGV_{i,-1} \), 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 behaviour can be obtained by appropriate normalisation of the Stokes’ parameters used in tomography, i.e. \( S_i = (N_X - N_Y) / (N_X + N_Y) \), where \( \langle j, X, Y \rangle \) is \((1, H, V)\), \((2, D, A)\), or \((3, R, L)\), and \( N_X \) is the number of counts in the \( X \) basis. If exact behaviour is required, then Gaussian holograms should be used.
[18] A. Vaziri et al., J. Opt. B 4, S47 (2002).
[19] This should not be done for higher-order, \(|l|>1\), modes. Displacing a charge \(|l|>1\) hologram to measure non-degenerate qudit superpositions — as was done in [4, 7] — analyses a superposition of several orders, not just the desired superposition of \( |\zeta = (LGV_{0,1}) + |LGV_{0,\pm1}\rangle / \sqrt{2} \). This is apparent in the output intensity pattern: a displaced charge \(|l|\) hologram produces a mode with a single displaced vortex [5], whereas a hologram for \( |\zeta \rangle \) will produce/analyse a mode with \(|l|\) single-charge vortices [21].
[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 renormalising the remainder appropriately.

[29] Computer-generated, sinusoidal, phase gratings; diffraction angle of $\sim0.28^\circ$ at 670 nm; efficiencies of 20-30%.