Quantum computing using shortcuts through higher dimensions

B. P. Lanyon[1], M. Barbieri[1], M. P. Almeida[1], T. Jennewein[1,2], T. C. Ralph[1],
K. J. Resch[1,3], G. J. Pryde[1,4], J. L. O'Brien[1,5], A. Gilchrist[1,6] & A. G. White[1]

[1]*Department of Physics and Centre for Quantum Computer Technology,*
University of Queensland, Brisbane 4072, Australia
[2]*Institute for Quantum Optics and Quantum Information,*
Austrian Academy of Sciences, Boltzmanng. 3, A-190 Vienna, Austria
[3]*Institute for Quantum Computing, University of Waterloo, N2L 3G1, Canada*
[4]*Centre for Quantum Dynamics, Griffith University, Brisbane 4111, Australia*
[5]*Centre for Quantum Photonics, University of Bristol, Bristol BS81UB, UK*
[6]*Physics Department, Macquarie University, Sydney 2109, Australia*

Quantum computation offers the potential to solve fundamental yet otherwise intractable problems across a range of active fields of research. Recently, universal quantum-logic gate sets—the building blocks for a quantum computer—have been demonstrated in several physical architectures. A serious obstacle to a full-scale implementation is the sheer number of these gates required to implement even small quantum algorithms. Here we present and demonstrate a general technique that harnesses higher dimensions of quantum systems to significantly reduce this number, allowing the construction of key quantum circuits with existing technology. We are thereby able to present the first implementation of two key quantum circuits: the three-qubit Toffoli and the two-qubit controlled-unitary. The gates are realised in a linear optical architecture, which would otherwise be absolutely infeasible with current technology.

The realisation of a full-scale quantum computer presents one of the most challenging problems facing modern science. Even the implementation of small scale quantum algorithms requires an unprecedented level of control over multiple quantum systems and a deep understanding of quantum mechanics. Recently much progress has been made with demonstrations of universal quantum gates sets - the fundamental building blocks of a quantum computer - in a number of physical architectures including ion-traps[1, 2], linear optics[3, 4], and superconductors[5]. In theory these gates can now be put together to implement any quantum algorithm and build a scalable quantum computer. However, in practice there are many significant obstacles that will require much theoretical and technological development to overcome. One of the most daunting is the sheer number of gates required to implement quantum algorithms.

Most approaches to quantum computing employ qubits—the quantum version of bits—encoded in two-level quantum systems. However, candidate systems for encoding quantum information typically have a far more complex physical structure with many readily accessible degrees of freedom, such as atoms[6], ions[1, 2] or photons[3, 4]. In this paper we show how harnessing these higher dimensions of quantum systems during computation can drastically reduce the number of gates required to implement key quantum circuits. This is based on a recent proposal[7], which we extend and use to build two key quantum logic gates for the first time. The technique has the potential for application in a wide range of physical architectures in combination with existing technology, and offers numerous advantages inherent in a reduced circuit complexity.

One of the most important quantum logic gates that has yet to be realised is the Toffoli—a three-qubit entangling gate that flips the logical state of the 'target' qubit conditional on the logical state of the two 'control' qubits. Famously, Toffoli gates allow universal reversible classical computation. The Toffoli also plays a central role in quantum error correction[8] and fault tolerance[9]. Furthermore, the combination of the Toffoli and the one-qubit Hadamard offers a simple universal quantum gate set[10]. The implementation of this gate requires a new level of coherent control over multiple quantum systems and represents a significant experimental challenge. We note that previous demonstrations in a liquid NMR architecture have since been shown to represent, at best, a classical simulation of quantum logic leading to no computational advantage[11, 12].

The Toffoli-sign (TS) is a three-qubit gate that applies a sign shift to one logical input state and is equivalent to a Toffoli under the action of only a few additional one-qubit gates. The simplest decomposition[13] of a TS gate when restricted to *qubits* throughout the calculation requires five two-qubit gates. If we further restrict ourselves to controlled-z (or CNOT) gates this number climbs to six[13], Fig. 1a. A quantum logic circuit that requires only three two-qubit gates is shown in Fig. 1b[7]. The increased efficiency is achieved by harnessing a third level of one of the information carriers *during* computation—i.e. one carrier becomes a qutrit with logical states **0**, **1** and **2**. The action of the first X_a gate is to move information encoded in the logical **0** state of this qutrit into its third level (**2**), which then bypasses the subsequent two-qubit gates. The final X_a gate *coherently* brings this information back into the **0** state, reconstructing the log-

ical qubit. This shortcut through a higher dimension allows the two-qubit gates to operate on a subspace of the original target qubit and implementation of the TS with a reduced number of gates. Note that standard two-qubit gates are necessary, with only the additional requirement that they apply the identity to information encoded in the logical **2** state of the qutrit. The technique can be generalized to implement higher-order n-control-qubit Toffoli gates (^{n}T) by harnessing a single ($n+1$)-level information carrier during computation and only ($2n-1$) standard two-qubit gates[7] (see supplementary information).

We extend this approach to simplify the construction of another key quantum circuit: the two-qubit controlled-unitary (CU) which applies an arbitrary one-qubit gate (U) to a target qubit conditional on the state of a single control qubit, Fig. 1b. This circuit plays a central role in quantum computing, particularly in the phase estimation algorithm[13] which in turn finds application in quantum simulation and quantum chemistry[14]. Phase estimation also underpins Shor's famous quantum algorithm for factoring numbers[15], the implementation of which would have significant consequence for modern cryptography. Futhermore, the set of CU's alone is sufficient for universal quantum computing; a CU can implement a CNOT and induce any single qubit rotation at the expense of an additional ancilla qubit, for example. Our technique can be generalized to implement higher-order n-control-bit unitary (c^nU) gates using an ($n+1$)-level target and only $2n$ two-qubit gates (see supplementary information). Even more generally, the approach can be used to efficiently add n control-qubits to an arbitrary controlled unitary that operates on k qubits (see supplementary information).

The simplest known decompositions[13] of a ^{n}T and c^nU into two-qubit gates requires ($12n-11$) and ($12n-10$) gates, respectively[‡]. In each case this is achieved by employing an additional overhead of ($n-1$) ancilla qubits. (Note that implementations without ancillas require on the order of n^2 two-qubit gates[13]). By harnessing only higher dimensions of *existing* information carriers we achieve a significant reduction in all cases. For example, a known decomposition[13] of the ^{5}T and c^5U both require 50 two-qubit gates plus 4 ancilla qubits, when restricted to *qubits*. Our technique requires only 9 for the former, 10 for the latter and no ancillary information carriers in either case.

With an abundance of higher dimensions available in most candidate systems for encoding quantum information, our technique has the potential for wide application.

───────

[‡] We note that an architecture-specific decomposition of the ^{n}T has been proposed for implementation in an ion trap[16]. This requires ($2n+1$) qubit-*qutrit* entangling gates.
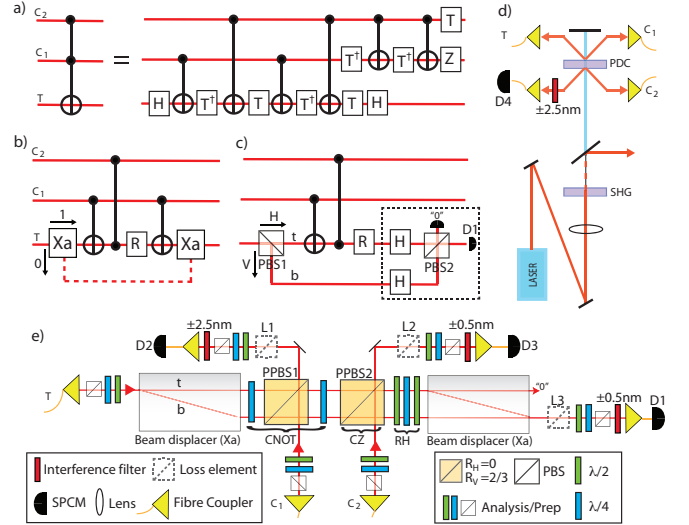

FIG. 1: a) Quantum logic circuit for a three-qubit Toffoli gate requiring six two-qubit CNOT gates when restricted to employing only qubits[13]. Standard symbols are used (see supplementary information). b) Circuit for a Toffoli Sign or controlled-z_θ gate. The Toffoli Sign gate (R=I, the identity) requires only three two-qubit gates (two CNOT's and one CZ). A sign change occurs only on the input $|C_2, C_1, T\rangle = |\mathbf{1,0,1}\rangle$. For the controlled-unitary R=z_θ (imparting an arbitrary phase shift between logical states) the circuit implements a controlled-z_θ between C_1 and T. C_2 and the gate it controls are redundant in this case. X_a expands the Hilbert space of the target (T) from a *qubit* to a *qutrit*. Its action is defined by: $X_a|\mathbf{0}\rangle = |\mathbf{2}\rangle, X_a|\mathbf{2}\rangle = |\mathbf{0}\rangle, X_a|\mathbf{1}\rangle = |\mathbf{1}\rangle$. The two-qubit gates act on the qubit levels in the usual way[13] and always impart the identity on a qutrit in level **2**. c) Conceptual logic circuit for our linear-optic implementation. The final CNOT in b) has been replaced by a non-deterministic recombination of the target qubit (dashed box). d) Layout of our photon source. Forward and backward photons pairs are produced via parametric downconversion (PDC) of a frequency-doubled mode-locked Ti:Saph laser (820 nm →410 nm, $\Delta\tau$=80 fs at 82 MHz repetition rate) through a Type I PDC 2 mm BiB$_3$O$_6$ crystal. The photons are collected into four single-mode optical fibres and detected using fibre-coupled single photon counting modules. e) Experimental implementation of the conceptual circuit shown in c). A successful run of the TS (CU) is flagged by a four-fold (two-fold) coincident measurement at D1-4 (D1-2). We employ an inherently stable Jamin-Lebedev interferometer using two calcite beam-displacers[3] to coherently expand the dimension of T from a polarisation qubit to a four-level system distributed across polarisation and spatial-mode. We spectrally filter using unblocked interference filters centered at 820 nm (bandwidths as shown) and realise an arbitrary one-qubit gate (RH) using a quarter-half-quarter waveplate combination.

A clear example is the photon, which has a large number of degrees of freedom including polarisation, transverse spatial-mode, arrival-time, photon number, and frequency. Coherent control over and between many of these dimensions has already been demonstrated and shown to offer significant advantages in a range of applications such as quantum communication and measurement[17, 18].

Trapped ions also offer a range of higher dimensions that can be readily exploited, including additional electronic and vibrational energy levels. Indeed, these levels are routinely used for read-out and to coherently implement individual logic gates[16, 19]. An immediate benefit of a significant reduction in the number of two-qubit gates required for quantum circuits is an equally significant speed-up in processing time. This has particular advantages for the many architectures where short coherence times are an obstacle in the path to scalability.

Here we present an implementation using photons to encode information and linear optics to construct quantum gates. Such gates are high performing, well characterised and offer fast gate speeds. Linear optics provide an excellent test-bed for studying quantum information science, and has several known paths to scalable quantum computing[20, 21]. Without the resource saving technique that we present here linear optic implementations of these gates is *absolutely* infeasible with current technology. We note that our resource saving scheme is fundamentally different from and potentially complementary to schemes for reducing the overhead associated with generating a universal resource[22, 23, 24]; here we are concerned with reducing the amount of that resource required to implement algorithms.

Fig. 1c shows a conceptual circuit of our implementation of the TS and CU. Key steps are the expansion of the Hilbert space of the target qubit (T), effected by the first polarising beamsplitter (PBS1), and contraction back into the original space, effected by the components in the dashed box. Before PBS1 we have a two-level system in the target rail with logical states $\mathbf{H}=\mathbf{0}$ and $\mathbf{V}=\mathbf{1}$ (a polarisation qubit). PBS1 then moves information encoded in the logical $\mathbf{H}$ state into a separate spatial mode. After PBS1 we have access to a *four-level* system; two levels in the top rail ($\mathbf{t}$) and two in the bottom rail ($\mathbf{b}$), with logical basis states $|\mathbf{H},\mathbf{t}\rangle, |\mathbf{V},\mathbf{t}\rangle, |\mathbf{H},\mathbf{b}\rangle$ and $|\mathbf{V},\mathbf{b}\rangle$, respectively. While we only need to use one of the additional levels in the bottom rail, we use both in our experiment simply to balance optical path-lengths. The contraction back into the original two-level polarisation qubit is performed non-deterministically, i.e. given deterministic two-qubit gates measurement of a single photon at D1 heralds a successful run of the gate. This allows for a demonstration without the last CNOT gate of Fig. 1b, thereby making an implementation feasible with recent developments in linear optics quantum gates[25].

In the case where R is the identity, the circuit in Fig. 1c implements a TS gate between carriers C_2, C_1 and T, applying a sign shift to the $|C_2, C_1, T\rangle = |\mathbf{1}, \mathbf{0}, \mathbf{1}\rangle$ term. It is of no consequence which state receives the sign shift; all cases are equivalent to a Toffoli under the action of additional one-qubit gates. For polarisation encoding, such gates are trivial to implement with standard birefringent waveplates. In the case where R is Z_θ the circuit implements a controlled-Z_θ (CZ_θ) between C_1 and T. Z_θ
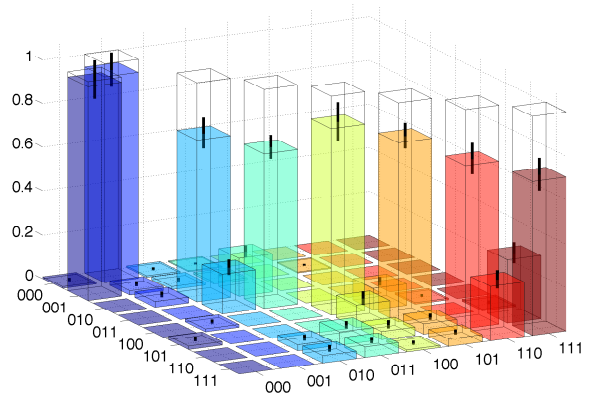

FIG. 2: Experimentally reconstructed truth-table for our Toffoli gate. Axis labels are written in the order $|C_2, C_1, T\rangle$. Ideally a flip of the logical state of the target qubit (T) occurs only when both control qubits (C_2 and C_1) are in the logical $|\mathbf{0}\rangle$ state. The overlap of ideal and measured truth tables is $I = 0.81 \pm 0.03$. The ideal case is shown as a wire grid. Error bars are shown representing one standard deviation, calculated from Poissonian photon counting statistics. The Inquisition ($\mathcal{I}$) is defined as the average logical state fidelity of a truth table $\bar{\mathcal{I}} = \mathrm{Tr}(\mathrm{M_{exp}M_{ideal}})/d$, where $\mathrm{M_{exp}}$ and $\mathrm{M_{ideal}}$ are the measured and ideal truth tables, and d is the table dimension. We define the logical flipping contrast as $\mathcal{C} = 1/2\{1 + (\mathrm{P_{ideal}} - \mathrm{P_{flip}})/(\mathrm{P_{ideal}} + \mathrm{P_{flip}})\}$ where $\mathrm{P_{ideal}}$ is the probability of obtaining the ideal output state and $\mathrm{P_{flip}}$ is the probability of obtaining the output state where the ideal target qubit output state has been flipped.

imparts an arbitrary phase between the logical states, i.e. the operation $\mathrm{Z}_\theta|\mathbf{0}\rangle \to |\mathbf{0}\rangle, \mathrm{Z}_\theta|\mathbf{1}\rangle \to e^{i\theta}|\mathbf{1}\rangle$. It is straightforward to show that such a gate is locally equivalent to a CU, under the action of additional one-qubit gates (see supplementary material).

Figs. 1d-e show the layout of our optical source and logic circuit in the laboratory, respectively. Our photons are generated via spontaneous parametric down conversion (SPDC), spatially filtered via single-mode optical fiber and spectrally filtered using interference filters, as detailed in the figure caption. Two-qubit linear optic gates are realised by combining one-qubit gates (waveplates) and controlled-Z ($\mathrm{CZ}=\mathrm{CZ}_\pi$) gates based on nonclassical interference at partially-polarising beamsplitters; the gates are nondeterministic and employ a measurement induced non-linearity[26, 27, 28]. Rather than chaining the gates to implement the required sequence for our implementation of the Toffoli (Fig. 1c) we employed a recently developed three-qubit quantum logic gate[25]. Ideal operation of the two-qubit gates requires non-classical interference between indistinguishable photons at the PPBS's (Fig. 1e). Dependent photons generated from the first pass of the PDC source interfere non-classically at PPBS1. One photon then goes on to interfere with a third, independent photon from the second pass, at PPBS2. We measure relative non-classical two-photon interference visibilities between vertically po-
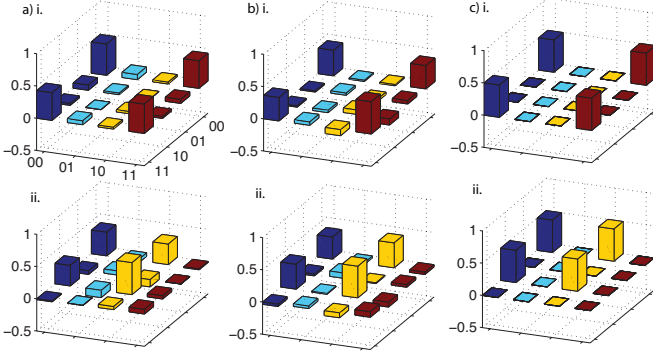
FIG. 3: a) Measured output states of qubits C_1 and T for Toffoli gate inputs; i) $|\mathbf{0},(\mathbf{0}+\mathbf{1}),\mathbf{0}\rangle/\sqrt{2}$; and ii) $|\mathbf{1},(\mathbf{0}+\mathbf{1}),\mathbf{0}\rangle/\sqrt{2}$. We observe fidelities with the ideal states, linear entropies and tangles[30] of i) {0.90±0.04, 0.21±0.08, 0.68±0.10} and ii) {0.75±0.06, 0.47±10, 0.04±0.06}, respectively. b) As for a) but where the roles of C_1 and C_2 have been swapped. We now observe i) {0.81±0.02, 0.39±0.05, 0.53±0.07} and ii) {0.80±0.03, 0.40±0.05, 0.01±0.01}. The decrease in tangle in the i) cases reflects the difference between dependent and independent photon interference, as discussed in the text. c) ideal density matrices. Note in all cases only real parts are shown, imaginary parts are negligible. The fidelity between two matrices (either two states or two processes) is $\mathrm{F}(\rho,\sigma)\equiv\{\mathrm{Tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\}^2$; Linear entropy is $\mathrm{S_L}\equiv d(1-\mathrm{Tr}[\rho^2])/(d-1)$, where d is the state dimension.

larised photons of $V_r=100\pm1\%$ and $V_r=92\pm4\%$ (where $V_r=V_{\mathrm{meas}}/V_{\mathrm{ideal}}$ and $V_{ideal}=80\%$), for the dependent and independent interferences respectively. The difference in these visibilities reflects the difficulty of achieving perfectly indistinguishable photons generated from independent sources[29]. For our experimental implementation we include the additional one-qubit gates required to convert the TS in Fig. 1c to the Toffoli. In both implementations our imperfectly manufactured beamsplitters impart systematic unitary operations on the optical modes. For simplicity we corrected for these effects numerically. Alternatively such unitaries could be corrected with standard waveplates.

For our implementation of a Toffoli we use photons from both passes of the PDC crystal and set R to the identity (Fig. 1e). A four-fold coincident measurement at detectors D1-4 signals a successful run of the gate. In linear optics implementations of two-qubit quantum gates, state dependent loss is used to rebalance amplitudes[26, 27, 28]. When incorporating loss elements L1-3 the gate operates with a success probability of 1/72. Alternatively, to combat low count rates, correct balance can be achieved by removing additional loss elements and pre-biasing the input polarisation states during gate characterisation[26, 27, 28]. Under these con-

ditions we measure a four-fold coincidence rate of approximately $10\,\mathrm{mHz}$ when running at full pump laser power. While this is not sufficient to perform a full process tomography[31] of the gate over a practical time period, we are able to to demonstrate all the key aspects of its behavior.

To demonstrate the classical action of our Toffoli we first reconstruct a logical truth-table (Fig. 2). In the ideal case of our implementation the target (T) undergoes a logical flip if, and only if, both control qubits are in the logical $\mathbf{0}$ state. The inquisition, $\mathcal{I}$, is the overlap between the ideal and measured truth tables[30]: for our three-qubit gate we measure $\mathcal{I}=0.81\pm0.03$, compared to $\mathcal{I}=0.85\pm0.01$ achieved for optical implementations of two-qubit gates[28]. Significant deviations from the ideal correspond to unwanted flips of the target qubit which can be understood with reference to the non-classical interferences required for correct operation in each case. In order to gauge our gates ability to apply the correct operation to a subset of logical input states we employ the flipping contrast, $\mathcal{C}$. (See Fig. 2). For inputs $|C_2,C_1\rangle=|\mathbf{0},\mathbf{0}\rangle$, no non-classical interference is required for correct operation and we measure $\mathcal{C}=0.99\pm0.01$, averaged over both target logical input states. Inputs $|C_2,C_1\rangle=|\mathbf{0},\mathbf{1}\rangle$ require perfect non-classical interference between *dependent* photons C_1 and T, for ideal operation. As discussed previously we achieve a near perfect interference visibility between vertical photons in this case. However, the full process suffers from the presence of higher-order PDC terms which are not observed in the visibility measurement due to higher-order interference processes[32]. This is reflected in an average of $\mathcal{C}=0.95\pm0.02$. Inputs $|C_2,C_1\rangle=|\mathbf{1},\mathbf{0}\rangle$ require perfect non-classical interference between *independent* photons C_2 and T, for ideal operation. This process is limited not only by higher-order terms but by inherent distinguishability of these photons[29], reflected in an average of $\mathcal{C}=0.80\pm0.02$. Inputs $|C_2,C_1\rangle=|\mathbf{1},\mathbf{1}\rangle$ require perfect non-classical interference between both dependent and independent photons, and are therefore the most challenging cases. Here we observe an average of $\mathcal{C}=0.73\pm0.05$.

To demonstrate the quantum action of our Toffoli we test its ability to *coherently* control an entangling process. With an input state of $|\mathbf{0},(\mathbf{0}+\mathbf{1}),\mathbf{0}\rangle/\sqrt{2}$ our Toffoli will produce the entangled state $|\mathbf{0},\Psi_+\rangle$, where $|\Psi_+\rangle$ is the maximally entangled Bell state[13] $(|\mathbf{0},\mathbf{0}\rangle+|\mathbf{1},\mathbf{1}\rangle)/\sqrt{2}$. With an input state of $|C_2,C_1,T\rangle=|\mathbf{1},(\mathbf{0}+\mathbf{1}),\mathbf{0}\rangle/\sqrt{2}$, it will produce the separable output state $|\mathbf{1},(\mathbf{0}+\mathbf{1}),\mathbf{0}\rangle/\sqrt{2}$. In the former (latter) case the entangling operation between C_1 and T is coherently turned on (off) by C_2. We then swap the roles of the control qubits and repeat the test. These processes require coherent interaction between all three qubits. We perform over-complete full state tomography to reconstruct the density matrix of two-qubit output states, requiring 36 separate measurements[26]. Our

tomography employs convex optimisation and Monte-Carlo simulation for error analysis[25]. Measurements sets are taken iteratively, whereby multiple sets—each taking around 1 hr to complete—are recorded. This reduces the effect of optical source power fluctuations.

Fig. 3 shows experimentally reconstructed density matrices representing the state of a control and target qubit, at the output of our Toffoli gate. We achieve a high fidelity[30] with the ideal states in all cases, as detailed in the figure caption. The entangling process required to achieve Fig. 3a)i relies on interference between dependent photons. The process required to achieve Fig. 3b)i, relies on both dependent and independent interference. This leads to the reduced fidelity and increased linear entropy[30] observed in the latter case. These processes demonstrate the coherent action of our Toffoli gate.

Higher order PDC terms are caused when more than one pair of photons is created simultaneously in a single PDC pass (Fig. 1d). It is straightforward to show that the ratio of double to single photon-pair emission is proportional to the pump power. Thus reducing the power by a factor of 4 should in turn reduce these higher-order contributions from each pass by a factor of 4. Under these conditions we observe a four-fold rate at the output of the Toffoli gate of only $\sim$0.1 mHz and repeat measurement of the average flipping contrast for the most challenging logical inputs $|C_2, C_1\rangle = |\mathbf{1}, \mathbf{1}\rangle$. We observe a clear improvement from $\mathcal{C} = 0.73 \pm 0.05$ to $\mathcal{C} = 0.83 \pm 0.04$.

For our implementation of the CU circuit we inject only dependent qubits C_1 and T into the circuit, from the forward pass through the PDC crystal (Figs 1d-e). When incorporating loss element L1 (Fig. 1e) the gate operates with a success probability of 1/18. For our demonstration this was optimised by removing L1 and pre-biasing only the C_1 input state[26, 27, 28]. A two-fold coincident measurement at detectors D1-2 signals a successful run of the gate. When running at 1/4 power we observe a two-fold rate at the output of our circuit of around 100 Hz. This is more than sufficient to perform a full process tomography[31] of the CU on a timescale of the order of 2 hrs, whilst retaining the advantages of a lower power.

As a demonstration, we report the implementation of four distinct CU gates that apply Z_θ rotations of $\pi/4$ (CT), $\pi/2$ (CJ), $3\pi/4$ (CL) and π (CZ) to the target (T) conditional on the control (C_1), respectively. Three of these are of fundamental importance to quantum computing[13]. We fully characterise these gates via quantum process tomography[31]: Fig. 4 shows the experimentally reconstructed process matrices. We achieve the highest reported two-qubit logic gate process fidelities, in any architecture, as detailed in the figure caption. The origins of the small deviations from ideal operation are thought to lie in residual higher order PDC emissions, imperfect mode matching and manufactured optics[29, 32]. The overriding source of error in our
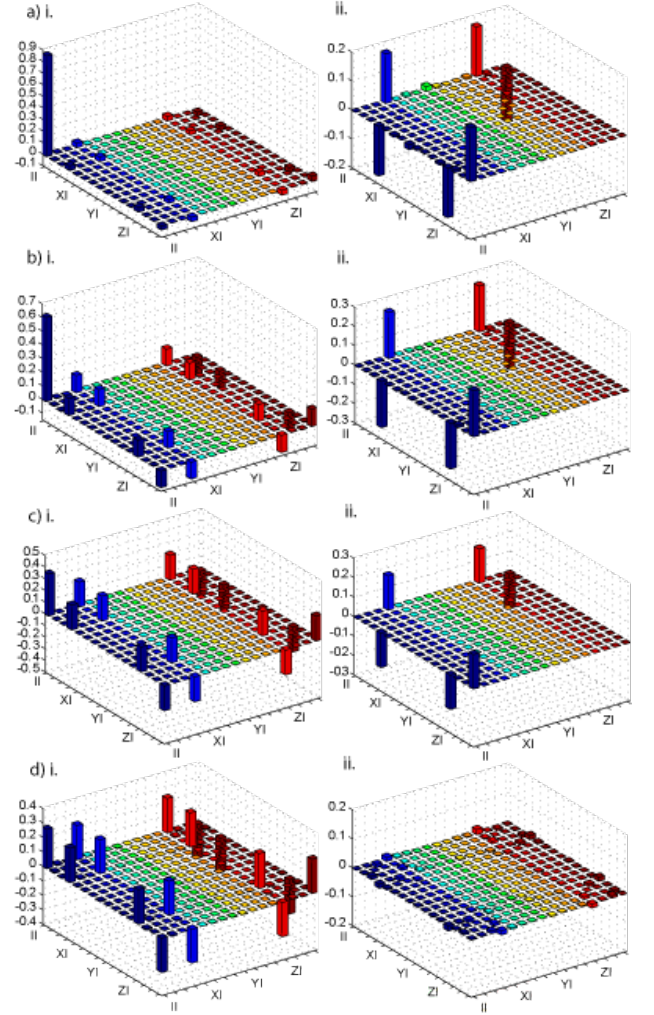

FIG. 4: Experimentally reconstructed process matrices[31] for four demonstrations of our controlled-unitary gate (CU), for U=Z_θ and: a) $\theta = \pi/4$ (CT); b) $\theta = \pi/2$, (CJ); c) $\theta = 3\pi/4$, (CL); and d) $\theta = \pi$, (CZ). (i) Real and (ii) imaginary parts are shown. We observe high process fidelities[31] with the ideal {0.982$\pm$0.003, 0.977$\pm$0.004, 0.940$\pm$0.006, 0.956$\pm$0.003} and low average output-state linear entropies {0.036$\pm$0.004, 0.047$\pm$0.004, 0.091$\pm$0.005, 0.086$\pm$0.006}, respectively. Matrices are presented in the standard Pauli basis[31].

experiments lies in our imperfect photon source. Current developments in source technology promise significant improvements in the near future. The combination of this with recently developed photon-number resolving detectors offers a path to a deterministic and scalable implementation of our gates.

We have demonstrated a new technique that harnesses the power of readily available higher dimensional quantum systems to drastically simplify the construction of key quantum circuits. As we have shown, the technique is particularly relevant to the current state of experimental quantum computing and can be integrated with *ex-*

isting technology to realise new quantum circuits. The demonstration of these circuits represents a crucial test of the practicality of quantum computing, raises many important questions that have yet to be solved and immediately offers valuable new tools with which to study quantum interactions.

---

[1] Schmidt-Kaler, F. *et al.* Realization of the cirac-zoller controlled-not quantum gate. *Nature* **422**, 408–411 (2003).

[2] Leibfried, D. *et al.* Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate. *Nature* **422**, 412–415 (2003).

[3] O'Brien, J. L., Pryde, G. J., White, A. G., Ralph, T. C. & Branning, D. Demonstration of an all-optical quantum controlled-not gate. *Nature* **426**, 264–267 (2003).

[4] Gasparoni, S., Pan, J.-W., Walther, P., Rudolph, T. & Zeilinger, A. Realization of a photonic controlled-not gate sufficient for quantum computation. *Physical Review Letters* **93**, 020504 (2004).

[5] Plantenberg, J. H., de Groot, P. C., Harmans, C. J. P. M. & Mooij, J. E. Demonstration of controlled-not quantum gates on a pair of superconducting quantum bits. *Nature* **447**, 836–839 (2007).

[6] Mandel, O. *et al.* Controlled collisions for multi-particle entanglement of optically trapped atoms. *Nature* **425**, 937–940 (2003).

[7] Ralph, T. C., Resch, K. J. & Gilchrist, A. Efficient toffoli gates using qudits. *Physical Review A* **75**, 022313 (2007).

[8] Cory, D. G. *et al.* Experimental quantum error correction. *Phys. Rev. Lett.* **81**, 2152–2155 (1998).

[9] Dennis, E. Toward fault-tolerant quantum computation without concatenation. *Phys. Rev. A* **63**, 052314 (2001).

[10] Shi, Y. Both toffoli and controlled-not need little help to do universal quantum computation. *Quantum Information and Computation* **3(1)**, 84–92 (2003).

[11] Braunstein, S. L. *et al.* Separability of very noisy mixed states and implications for nmr quantum computing. *Phys. Rev. Lett.* **83**, 1054–1057 (1999).

[12] Menicucci, N. C. & Caves, C. M. Local realistic model for the dynamics of bulk-ensemble nmr information processing. *Phys. Rev. Lett.* **88**, 167901 (2002).

[13] Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[14] Aspuru-Guzik, A., Dutoi, A. D., Love, P. J. & Head-Gordon, M. Simulated Quantum Computation of Molecular Energies. *Science* **309**, 1704–1707 (2005).

[15] Shor, P. In *Proc. 35th Ann. Symp. Found. Comp. Sci.* *124* (IEEE Comp. Soc. Press, Los Alamitos, California, 1994).

[16] Cirac, J. I. & Zoller, P. Quantum computations with cold trapped ions. *Phys. Rev. Lett.* **74**, 4091–4094 (1995).

[17] Kwiat, P., Mitchell, J. R., Schwindt, P. & White, A. Grover's search algorithm: an optical approach. *Journal of Modern Optics* **47**, 257–266 (2000).

[18] Schuck, C., Huber, G., Kurtsiefer, C. & Weinfurter, H. Complete deterministic linear optics bell state analysis. *Physical Review Letters* **96**, 190501 (2006).

[19] Roos, C. F. *et al.* Control and measurement of three-qubit entangled states. *Science* **304**, 1478–1480 (2004).

[20] Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46–52 (2001).

[21] Nielsen, M. A. Optical quantum computation using cluster states. *Physical Review Letters* **93**, 040503 (2004).

[22] Yoran, N. & Reznik, B. Deterministic linear optics quantum computation with single photon qubits. *Phys. Rev. Lett.* **91**, 037903 (2003).

[23] Ralph, T. C., Hayes, A. J. F. & Gilchrist, A. Loss-tolerant optical qubits. *Phys. Rev. Lett.* **95**, 100501 (2005).

[24] Browne, D. E. & Rudolph, T. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.* **95**, 010501 (2005).

[25] Lanyon, B. P. *et al.* Experimental demonstration of Shor's algorithm with quantum entanglement. *Physical Review Letters, to appear* (2007).

[26] Langford, N. K. *et al.* Demonstration of a simple entangling optical gate and its use in bell-state analysis. *Physical Review Letters* **95**, 210504 (2005).

[27] Kiesel, N., Schmid, C., Weber, U., Ursin, R. & Weinfurter, H. Linear optics controlled-phase gate made simple. *Physical Review Letters* **95**, 210505 (2005).

[28] Okamoto, R., Hofmann, H. F., Takeuchi, S. & Sasaki, K. Demonstration of an optical quantum controlled-not gate without path interference. *Physical Review Letters* **95**, 210506 (2005).

[29] Rarity, J., Tapster, P. & Loudon, R. *Quantum Interferometry* (VCH, Weinheim, 1996).

[30] White, A. G. *et al.* Measuring two-qubit gates. *J. Opt. Soc. Am. B* **24**, 172–183 (2007).

[31] O'Brien, J. L. *et al.* Quantum process tomography of a controlled-[NOT] gate. *Phys. Rev. Lett.* **93**, 080502 (2004).

[32] Weinhold, T. J. *et al.* Error budgets for quantum logic gates: the road to fault tolerance (2007).

Supplementary material.

Our technique can be extended to multiple-control gates, e.g. ^{n}T and C^{n}U. Figure 5 gives an implementation of ^{3}T and C^{2}U. Fig. 6 shows a more general application of our technique; adding n control qubits to an arbitrary k qubit unitary.

Correspondence.

Correspondence and requests for materials should be addressed to BPL (lanyon@physics.uq.edu.au).
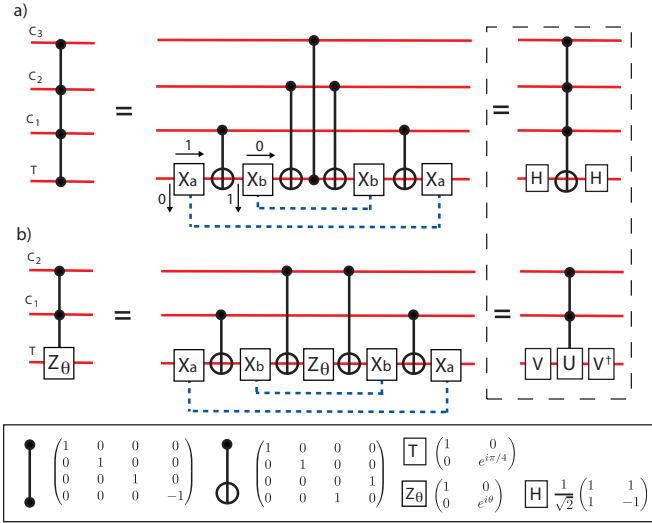
FIG. 5: Implementation of the next level of encoding of our technique required to realise **a** a 3-control-qubit Toffoli Sign gate (^{3}TS) and **b** 2-control-qubit unitary $\mathrm{C}^2\mathrm{Z}_\theta$. The X_a gate flips information between the logical **0** and **2** state of the target. The X_b gate flips infomation between the logical **1** and **3** state of the target. Thus we require access to a four-level information carrier in the target; two levels in the original red rail and one in each of the dashed-blue rails. The dashed box shows the 1-qubit gates required to interconvert the TS^3 and $\mathrm{C}^2\mathrm{U}$ to the Toffoli and controlled-unitary equivalents, respectively. $VZ_\theta V^\dagger$ is the spectral decomposition of U, up to a trivial global phase factor. All other gates operate as usual (on the qubit subspace: levels **0** and **1**) and their operations are shown, including some used in Fig. 1 of the main text. In **a** the control operation occurs if $|C_3, C_2, C_1\rangle=|\mathbf{1,1,0}\rangle$. In **b** the control operation occurs if $|C_2, C_1\rangle=|\mathbf{1,0}\rangle$. a) is based on Fig. 2 of Ref. 3 in the main text.
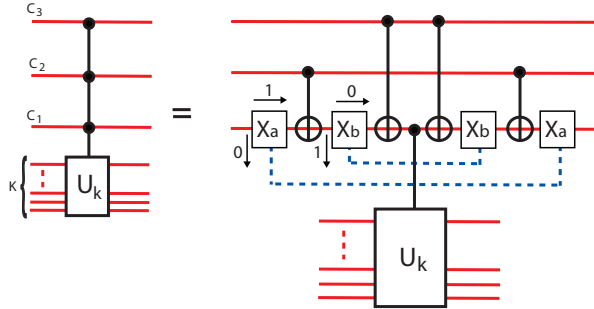

FIG. 6: Circuit for implementation of a 3-control-qubit unitary acting on k qubits, $\mathrm{C}^3(\mathrm{U}_k)$. Given the ability to perform a single instance of a $\mathrm{C}^1(\mathrm{U}_k)$ n additional control qubits can be added at a cost of an extra $2n$ two-qubit gates and an additional n dimensions in C_1. The X_j perform as described in the caption of Fig. 1.