Experimental one-way quantum computing

P. Walther[1], **K. J. Resch**[1], **T. Rudolph**[2], **E. Schenck**[1*], **H. Weinfurter**[3,4], **V. Vedral**[1,5,6], **M. Aspelmeyer**[1] **& A. Zeilinger**[1,7]

[1] *Institute of Experimental Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*
[2] *QOLS, Blackett Laboratory, Imperial College London, London SW7 2BW, UK*
[3] *Department of Physics, Ludwig Maximilians University, D-80799 Munich, Germany*
[4] *Max Planck Institute for Quantum Optics, D-85741 Garching, Germany*
[5] *The Erwin Schrödinger Institute for Mathematical Physics, Boltzmanngasse 9, 1090 Vienna, Austria*
[6] *The School of Physics and Astronomy, University of Leeds, Leeds LS2 9JT, UK*
[7] *IQOQI, Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*

* Permanent address: Ecole normale supérieure, 45, rue d'Ulm, 75005 Paris, France

Standard quantum computation is based on sequences of unitary quantum logic gates that process qubits. The one-way quantum computer proposed by Raussendorf and Briegel is entirely different. It has changed our understanding of the requirements for quantum computation and more generally how we think about quantum physics. This new model requires qubits to be initialized in a highly entangled cluster state. From this point, the quantum computation proceeds by a sequence of single-qubit measurements with classical feedforward of their outcomes. Because of the essential role of measurement, a one-way quantum computer is irreversible. In the one-way quantum computer, the order and choices of measurements determine the algorithm computed. We have experimentally realized four-qubit cluster states encoded into the polarization state of four photons. We characterize the quantum state fully by implementing experimental four-qubit quantum state tomography. Using this cluster state, we demonstrate the feasibility of one-way quantum computing through a universal set of one- and two-qubit operations. Finally, our implementation of Grover's search algorithm demonstrates that one-way quantum computation is ideally suited for such tasks.

The quantum computer[1,2] is a powerful application of the laws of quantum physics. Such a device will be far more efficient at factoring[3] or database searches[4] compared to its classical counterparts[5]. Considerable effort has been directed towards understanding the role of measurement and entanglement in quantum computation[6–12]. A significant step forward in our understanding was the introduction of the one-way quantum computer[13–17], which highlights the importance of both measurement and entanglement in a striking way. In this model, all of the entanglement is provided in advance through a highly entangled multiparticle cluster state[13]. The quantum computation on the cluster state proceeds via local, single-qubit projective measurements with the outcomes potentially affecting those measurement settings that follow. It is a strength of the cluster state model that the intrinsic randomness of quantum measurement results creates specific types of errors that can be corrected through this classical feedforward. Most importantly, feedforward makes cluster state quantum computation deterministic. In the present proof-of-principle experiment, we perform measurements using fixed single-port polarizers, making our computations probabilistic. Different algorithms require only a different pattern of adapted single-qubit operations on a sufficiently large cluster state. As it is entirely based on single-particle measurements instead of unitary evolution, the computation is inherently not time-reversible—it is one-way. Most importantly, cluster state quantum computation is universal[14,17] in that any quantum circuit can be implemented on a suitable cluster state. Open theoretical questions remain about the scalability under realistic noise conditions required for fault-tolerant one-way quantum computation. Although a threshold has been proved to exist[18], it is unknown whether cluster state quantum computation will be more or less sensitive to noise than the standard model.

The one-way quantum computer does not perform quantum logic on the individual qubits of the cluster state. In order to describe the computational circuit, we need to distinguish between the physical qubits (in our case, the polarization state of photons), which make up the cluster state and on which actual measurements are carried out, and encoded qubits, on which the computation is actually taking place. Owing to the specific entanglement of the cluster state, no individual physical qubit carries any information about an input state. Instead, each encoded qubit is written on the cluster state non-locally; that is, the information is carried by the correlations between the physical qubits. As the quantum computation proceeds, the encoded input qubits are processed in the imprinted circuit, whose output is finally transferred onto physical readout qubits. Interestingly, whereas the entanglement between the physical qubits in general decreases as a result of the measurement sequence, the entanglement between encoded qubits may increase.

A cluster state can be thought of as emerging from an array of equally prepared independent qubits, which then interact via controlled-phase ('CPhase') gates with their nearest (connected) neighbours. Specifically, a cluster state can be built up as follows: a large number of physical qubits are each prepared in the superposition state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, where $|0\rangle$ and $|1\rangle$ are the computational basis of the physical qubits. A CPhase operation $|j\rangle|k\rangle \rightarrow (-1)^{jk}|j\rangle|k\rangle$, with $(j,k \in 0,1)$, is then applied between pairs of neighbouring, connected qubits and effectively generates entanglement between them. The choice of which physical qubit neighbours are entangled by the CPhase operations, drawn as connecting 'bonds' (Fig. 1), determines the structure of the cluster state, which defines the basic type quantum circuit it can implement. This construction provides an intuitive understanding of the graphical representation of cluster states as connected arrays of physical qubits, in which each line corresponds to a previous nearest-neighbour interaction. We will later demonstrate how the highly entangled cluster states can be generated in a different way—directly from nonlinear optical processes.

Given a cluster state, two basic types of single-particle measurements suffice to operate the one-way quantum computer. Measurements in the computational basis $\{|0\rangle_j, |1\rangle_j\}$ have the effect of disentangling, that is, removing, the physical qubit j from the cluster, leaving a smaller cluster state. Such operations can be used to modify the structure of the cluster and thus the imprinted circuit. The measurements that perform the actual quantum information processing are made in the basis $B_j(\alpha) = \{|+\alpha\rangle_j, |-\alpha\rangle_j\}$, where $|\pm\alpha\rangle_j = (|0\rangle_j \pm e^{i\alpha}|1\rangle_j)/\sqrt{2}$ (α is a real number). The choice of measurement basis determines the single-qubit rotation, $R_z(\alpha) = \exp(-i\alpha\sigma_z/2)$, followed by a Hadamard operation, $H = (\sigma_x + \sigma_z)/\sqrt{2}$, on encoded qubits in the cluster ($\sigma_x, \sigma_y, \sigma_z$ being the usual Pauli matrices). Combinations of rotations about the z axis and Hadamard operations can implement $R_x(\alpha) = \exp(-i\alpha\sigma_x/2)$ rotations through the matrix identity $R_x(\alpha) = HR_z(\alpha)H$. General quantum logic operations can be carried out by the correct choice of $B_j(\alpha)$ on a sufficiently large cluster state. We define the outcome s_j of a measurement on the physical qubit j as 0 if the measurement outcome is $|+\alpha\rangle_j$, and as 1 if the outcome is $|-\alpha\rangle_j$. In those cases where the 0 outcome is found, the computation proceeds as desired. However, in those cases where the 1 outcome is found, a well-defined Pauli error is introduced. Feedforward, such that the output controls future measurement, compensates for these known errors.

For the implementations of single- and two-qubit quantum logic, we post-select only those cases where the 0 outcome is found. In these cases the computation proceeds error-free and requires no feedforward. In the final section, where we report the implementation of Grover's search algorithm, the feedforward determines the final, classical, measurement. There we measured all possible combinations of the measurement results individually, and applied the feedforward relation in such a way that the earlier

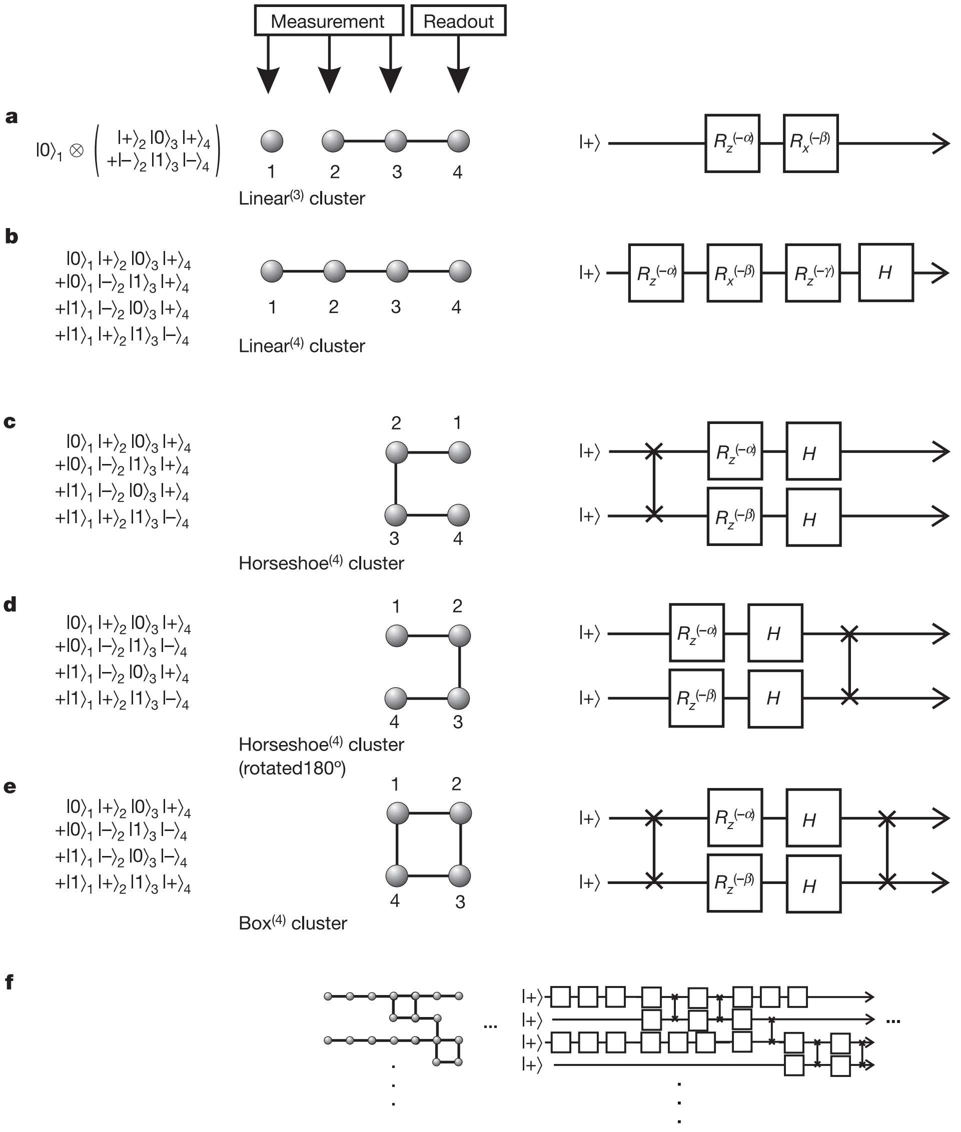
Measurement
Readout
a
$|0\rangle_1 \otimes \begin{pmatrix} |+\rangle_2|0\rangle_3|+\rangle_4 \\ +|-\rangle_2|1\rangle_3|-\rangle_4 \end{pmatrix}$
1
2
3
4
Linear$^{(3)}$ cluster
$|+\rangle$
$R_z^{(-\alpha)}$
$R_x^{(-\beta)}$
b
$|0\rangle_1|+\rangle_2|0\rangle_3|+\rangle_4$
$+|0\rangle_1|-\rangle_2|1\rangle_3|+\rangle_4$
$+|1\rangle_1|-\rangle_2|0\rangle_3|+\rangle_4$
$+|1\rangle_1|+\rangle_2|1\rangle_3|-\rangle_4$
1
2
3
4
Linear$^{(4)}$ cluster
$|+\rangle$
$R_z^{(-\alpha)}$
$R_x^{(-\beta)}$
$R_z^{(-\gamma)}$
H
c
$|0\rangle_1|+\rangle_2|0\rangle_3|+\rangle_4$
$+|0\rangle_1|-\rangle_2|1\rangle_3|+\rangle_4$
$+|1\rangle_1|-\rangle_2|0\rangle_3|+\rangle_4$
$+|1\rangle_1|+\rangle_2|1\rangle_3|-\rangle_4$
2
1
3
4
Horseshoe$^{(4)}$ cluster
$|+\rangle$
$|+\rangle$
$R_z^{(-\alpha)}$
$R_z^{(-\beta)}$
H
H
d
$|0\rangle_1|+\rangle_2|0\rangle_3|+\rangle_4$
$+|0\rangle_1|-\rangle_2|1\rangle_3|-\rangle_4$
$+|1\rangle_1|-\rangle_2|0\rangle_3|+\rangle_4$
$+|1\rangle_1|+\rangle_2|1\rangle_3|-\rangle_4$
1
2
4
3
Horseshoe$^{(4)}$ cluster
(rotated180°)
$|+\rangle$
$|+\rangle$
$R_z^{(-\alpha)}$
$R_z^{(-\beta)}$
H
H
e
$|0\rangle_1|+\rangle_2|0\rangle_3|+\rangle_4$
$+|0\rangle_1|-\rangle_2|1\rangle_3|-\rangle_4$
$+|1\rangle_1|-\rangle_2|0\rangle_3|-\rangle_4$
$+|1\rangle_1|+\rangle_2|1\rangle_3|+\rangle_4$
1
2
4
3
Box$^{(4)}$ cluster
$|+\rangle$
$|+\rangle$
$R_z^{(-\alpha)}$
$R_z^{(-\beta)}$
H
H
f
$|+\rangle$
$|+\rangle$
$|+\rangle$
$|+\rangle$

Figure 1 Few-qubit cluster states and the quantum circuits they implement. For each three- and four-qubit cluster, its quantum state and the computation carried out in the one-way quantum computer model are shown. For the case of the linear clusters $|\Phi_{\text{lin}3}\rangle$ (**a**) and $|\Phi_{\text{lin}4}\rangle$ (**b**), consecutive measurements on the qubits 1, 2 and 3 will perform a computation as a series of one-qubit rotation gates. The encoded input state undergoes single-qubit rotations with controllable angles, and the output is left on physical qubit 4. In contrast, the horseshoe clusters $|\Phi_{\subset 4}\rangle$ (**c**) and $|\Phi_{\sqsupset 4}\rangle$ (**d**) and the box cluster $|\Phi_{\Box 4}\rangle$ (**e**) form more complex circuits containing both single-qubit and two-qubit gates, both of which are necessary to form a universal set of logic gates for quantum computation. In particular, measurements on two of the physical qubits (2 and 3 in the case of $|\Phi_{\subset 4}\rangle$, and 1 and 4 in the case of $|\Phi_{\sqsupset 4}\rangle$ or $|\Phi_{\Box 4}\rangle$) will perform the circuit defined by the particular cluster and transfer the logical output onto the remaining two physical qubits (1 and 4 in the case of $|\Phi_{\subset 4}\rangle$, and 2 and 3 in the case of $|\Phi_{\sqsupset 4}\rangle$ or $|\Phi_{\Box 4}\rangle$). When these cluster states are not a part of a larger cluster, the encoded input states are always $|\Psi_{\text{in}}\rangle = |+\rangle_{1\text{E}}$ for the one-qubit gates and $|\Psi_{\text{in}}\rangle = |+\rangle_{1\text{E}}|+\rangle_{2\text{E}}$ for the two-qubit gates. **f**, General input states can be prepared and processed through these operations when these clusters are subunits of larger clusters.

measurement outcomes define the meaning of the final ones.

Even a small cluster state suffices to demonstrate all the essential features of one-way quantum computing. Each of the three- and four-particle cluster states shown in Fig. 1 can implement the quantum circuit shown to its right that consists of a series of single- and two-qubit quantum gates. The computation proceeds via single-particle measurements carried out from the left side of the cluster to the right side, where the final readout takes place. The important feature of the quantum circuits is that the output of one circuit can be fed into the input of a subsequent one if their cluster states are bonded together by CPhase operations. Thus these small circuits, which form a universal set of logic gates, can be used as subunits for a fully functional quantum computer.

As an example, consider the four-particle box cluster state $|\Phi_{\square 4}\rangle$ on a two-dimensional lattice (Fig. 1e). The encoded input to the two-qubit quantum circuit is the product state $|\Psi_{\rm in}\rangle = |+\rangle_{1\rm E}|+\rangle_{2\rm E}$, where the numerical subscript labels the qubit and the subscript E is used to distinguish encoded qubits from physical qubits. The circuit processes this pair of encoded qubits through a sequence beginning with a CPhase gate, followed by single-qubit rotations $R_z(-\alpha)$ and $R_z(-\beta)$ on encoded qubits 1 and 2, then a Hadamard operation, H, on both qubits, ending with a second CPhase operation. The values for α and β of the rotation gates are set by the choice of measurement bases $B_1(\alpha)$ and $B_4(\beta)$ on the physical qubits 1 and 4 respectively. The output of the quantum computation is transferred onto physical qubits 2 and 3. This kind of two-qubit quantum gate is essential for universal quantum computation, as it can generate entanglement between the encoded qubits.

On the other hand, by changing the geometry of the cluster state to the one-dimensional cluster $|\Phi_{\rm lin4}\rangle$ (Fig. 1b), it now results in a different quantum circuit corresponding to a set of single-qubit rotations on one encoded qubit. Consecutive measurements $B_1(\alpha)$, $B_2(\beta)$ and $B_3(\gamma)$ on the physical qubits 1, 2 and 3 transform the input state, in our case $|\Psi_{\rm in}\rangle = |+\rangle_{1\rm E}$, to $|\Psi_{\rm out}\rangle = HR_z(-\gamma)R_x(-\beta)R_z(-\alpha)|\Psi_{\rm in}\rangle$ and store the output on qubit 4.

In order to demonstrate all the circuits shown in Fig. 1a–e, it is sufficient to produce first a linear cluster state of four qubits. The particular circuit implemented is then determined by the order of the measurements performed. Specifically, the one-dimensional linear structure (Fig. 1a and b) is implemented by sequentially measuring qubits 1, 2 and 3, with the final result then being available at qubit 4. The two-dimensional 'horseshoe' structures (Fig. 1c and d) are implemented by measuring either qubits 2 and 3 or 1 and 4, with the final result then being available at qubits 1 and 4 or 2 and 3, respectively. The four-qubit box cluster (Fig. 1e) can be obtained from the four-qubit linear cluster by Hadamard rotations and by swapping (that is, relabelling) the physical qubits 2 and 3. This will be described in more detail in the next section, and in the section 'Two-qubit gates'.

The difficulty of one-way quantum computing lies with the cluster state preparation. Cluster states arise naturally in spin chains or spin lattices by way of nearest-neighbour Ising interaction[13], a well-known interaction model in solid-state physics. The first proposals to achieve cluster states were based on analogues of dipole–dipole coupling between atoms in optical lattices[15,19]. Although photon–photon interactions are negligible, recent proposals have nevertheless shown that optical systems may be well suited for implementing the cluster state model. These schemes use sequences of probabilistic quantum-logic gates[8,20–23] based on linear optical elements to construct large photonic cluster states[24,25]. These optical one-way quantum computation proposals are less demanding of resources than the comparable optical implementation in the standard model[8].

In the present work, we have used nonlinear optics to directly produce four-photon cluster states. This method exploits a mode- and polarization-entangled four-photon state[26] produced in pulsed-pump spontaneous parametric down-conversion (SPDC) (see Methods). We reconstructed the density matrix of the four-qubit cluster state using quantum state tomography, and studied the state's entanglement properties relevant for quantum computation. We then implemented all of the quantum circuits shown in Fig. 1a–e, and demonstrated a two-qubit quantum search algorithm. In doing so, we have demonstrated the first universal set of gates and an important algorithm in a one-way quantum computer.

Creation and characterization of the cluster state

Our cluster state is produced experimentally using the mode- and polarization-entangled output of nonlinear spontaneous parametric down-conversion and linear optical elements, as described in detail in the Methods section. When four photons are emitted into the output modes of the polarizing beam-splitters 1, 2, 3 and 4, they are in the highly entangled cluster state

$$|\Phi_{\rm cluster}\rangle = \frac{1}{2}\big(|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 + |H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4 + |V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 - |V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4\big) \quad (1)$$

where $|H\rangle$ and $|V\rangle$ represent respectively horizontally and vertically polarized photon states, and the subscript labels the spatial mode. This state, $|\Phi_{\rm cluster}\rangle$, is equivalent to the four-qubit linear cluster, $|\Phi_{\rm lin4}\rangle$, and the horseshoe cluster states, $|\Phi_{\subset 4}\rangle$ and $|\Phi_{\supset 4}\rangle$ (Fig. 1) under the local unitary operation $H_1 \otimes I_2 \otimes I_3 \otimes H_4$ on the physical qubits, where H_i (I_i) is a Hadamard (identity) operation on qubit i. The four-qubit linear cluster can easily be reduced to a three-qubit linear cluster by measuring qubit 1 in the computational basis of the cluster and thus disentangling it from the rest. The state, $|\Phi_{\rm cluster}\rangle$, can be converted to the box cluster state (Fig. 1e) by the local unitary operation $H_1 \otimes H_2 \otimes H_3 \otimes H_4$ and a swap (or relabelling) of qubits 2 and 3. Note that the four-qubit cluster state thus realized is also the smallest cluster state that represents a new kind of entanglement[27], while the two-qubit and three-qubit cluster states are locally equivalent to a maximally entangled Bell state and the three-qubit Greenberger–Horne–Zeilinger (GHZ) state, respectively.

State tomography

We have completely characterized our state via quantum-state tomography (which is a method for extracting the density matrix of a quantum state) from a discrete set of experimental measurements. Although quantum process and state tomography has been performed with up to three qubits[28,29] this is, to our knowledge, the first time that a four-qubit density matrix has been determined from a complete, experimentally obtained density matrix. For a four-photon polarization state, like our cluster state, the full density matrix, ρ, is a 16×16 dimensional object that can be reconstructed by linear combinations of 256 linearly independent four-photon polarization projections. We performed each of these 256 measurements for 600 s using all combinations of $\{|H\rangle, |V\rangle, |+\rangle, |R\rangle\}$, where $|+\rangle = \big(|H\rangle + |V\rangle\big)/\sqrt{2}$ and $|R\rangle = \big(|H\rangle - i|V\rangle\big)/\sqrt{2}$. A maximum of 127 fourfold coincidence counts in 600 s were measured in the case of the setting $|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$. Instead of a direct linear combination of measurement results, which can lead to unphysical density matrices owing to experimental noise, we use a maximum-likelihood reconstruction technique[30–32]. The resulting density matrix is shown in Fig. 2. The dominant diagonal elements represent the four components $|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4$, $|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$, $|V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4$ and $|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$ as expected from equation (1), while off-diagonal elements indicate strong coherences between them. The negative coherences are due to the required π phase shift in the amplitude for the $|V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$ term. Our reconstructed state is in good qualitative agreement with the target state, $|\Phi_{\rm cluster}\rangle$. This can be quantified by the state fidelity $F = \langle\Phi_{\rm cluster}|\rho|\Phi_{\rm cluster}\rangle = (0.63 \pm 0.02)$, which is the state vector overlap with the ideal state $|\Phi_{\mathrm{cluster}}\rangle$. At present, no theoretical results exist concerning the fidelity requirements in cluster state quantum computation, so the full implications of the value that we found for the fidelity are unclear. Nevertheless, it has been proved that bi-separable four-qubit states cannot have a fidelity greater than 0.5 with our target cluster state. Our measured fidelity is clearly above this threshold, and therefore the observed fidelity is proof of the fact that the state contains the required four-particle entanglement[33] to a significant degree. Our cluster state is a coherent superposition of four different terms, each from a different physical origin (see Methods). The fidelity of our state is not perfect, because of partial distinguishability of these terms and because of imperfect phase stability in our set-up. We expect that achieving high fidelity with the target state will become rapidly more difficult as the size of the Hilbert space is increased. However, the acceptable amount of noise per qubit is independent of the size of the cluster, whereas it becomes exponentially small for GHZ states[34]. Thus the problem of noise does not increase for larger clusters[34].

Entanglement properties

One-way cluster state quantum computation is based entirely on the entanglement properties of the physical qubits of the initial cluster state. For three-qubit states, there are only two classes of entanglement typified by the GHZ state[35], $|\mathrm{GHZ}\rangle = \big(|H\rangle_1|H\rangle_2|H\rangle_3 + |V\rangle_1|V\rangle_2|V\rangle_3\big)/\sqrt{2}$, and by the W state[36,37], $|W\rangle = \big(|V\rangle_1|H\rangle_2|H\rangle_3 + |H\rangle_1|V\rangle_2|H\rangle_3 + |H\rangle_1|H\rangle_2|V\rangle_3\big)/\sqrt{3}$. As such, the three-qubit cluster state cannot represent a fundamentally different class of state and is, in fact, a GHZ state. On the other hand, our four-qubit cluster state cannot be converted via local unitary operations to either the four-qubit generalizations of the GHZ or the W state, but combines important characteristics of both.

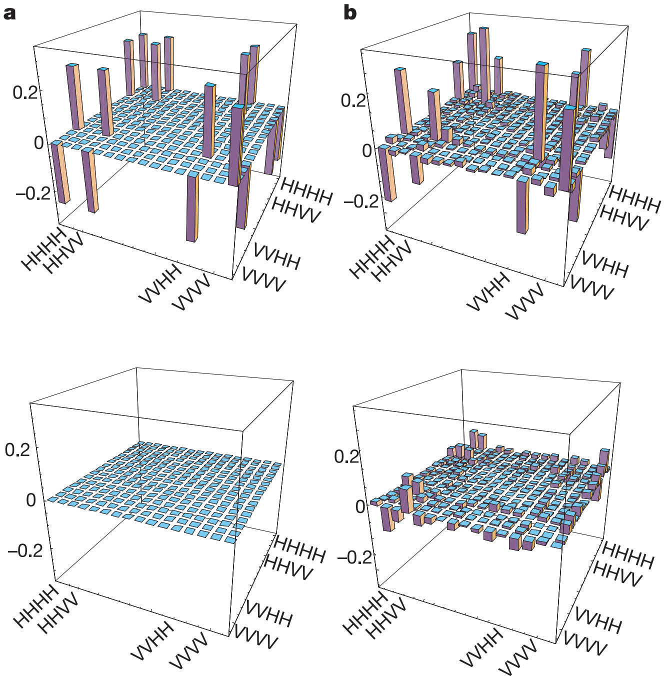

Figure 2 Density matrix of the four-qubit cluster state in the laboratory basis. Shown are the real (top) and imaginary (bottom) parts of the density matrix for the ideal case (**a**) and the reconstruction from the experimental four-photon tomography data (**b**). In both cases, there are four large diagonal components corresponding to HHHH, HHVV, VVHH and VVVV. The coherences between each of these diagonal elements show up as off-diagonal contributions, and are necessary for quantum entanglement. The real density matrix was reconstructed by way of a maximum likelihood method using four-photon coincidence rates obtained in 256 polarization projections.

As in a four-qubit GHZ state, we can make local measurements on one or two of the qubits and, with only classical communication, leave the remaining qubits in a three-qubit GHZ state or in a two-qubit Bell state, both of which can serve as an entanglement resource for quantum communication. For an explicit example, we reconstructed the density matrix of qubits 2, 3 and 4 by considering only the subset of our full tomographic measurements where qubit 1 was successfully measured in the state $|+\rangle_1$. Its fidelity compared to an ideal three-photon GHZ state was (0.60 ± 0.02), which is above the local realism threshold[38] of 0.56.

Whereas the loss of one qubit in a GHZ state is already sufficient to completely disentangle the state, $N/2$ particles have to be removed from an N-particle cluster state in order to leave a separable state. The cluster states share this persistency of entanglement[13] with the W states, which show an even stronger robustness against such decoherence. We demonstrate this property by considering the reduced density matrix of qubits 2, 3 and 4, $\rho^{\mathrm{red}}_{2,3,4}$, after ignoring qubit 1—that is, after tracing out the first qubit. This trace has been implemented by summing the two subsets of our tomographic measurements in which the first qubit was measured in the state $|H\rangle_1$ or $|V\rangle_1$. To test for entanglement in the remaining three-qubit state, we used the entanglement-witness operator $W=\frac{1}{4}I^{\otimes 3}-\frac{1}{2}\big(|H\rangle_2\langle H|_2\otimes|\Phi^+\rangle_{3,4}\langle\Phi^+|_{3,4}+|V\rangle_2\langle V|_2\otimes|\Phi^-\rangle_{3,4}\langle\Phi^-|_{3,4}\big)$, where $\mathrm{Tr}(W\rho) \geq 0$ for all separable states, but is negative for some entangled states. Our state gives a value of (−0.115 ± 0.007), which is negative by 16σ and thus proves that entanglement in qubits 2, 3 and 4 persists even after 'loss' of qubit 1. This remaining entanglement is between qubits 3 and 4. The loss of another particle destroys all entanglement and leaves a separable two-qubit state. We test this by calculating the eigenvalues of the partial transpose reduced density matrix of qubits 3 and 4, which are λ_1=0.49, λ_2=0.45, λ_3=0.05 and λ_4=0.008. These values are all positive, and thus fulfil the necessary and sufficient conditions for separability in two-particle systems[39,40].

A one-way quantum computer

Given a cluster state, quantum gates are implemented on the encoded qubits using only a series of single-qubit measurements and classical feedforward. In this section, we demonstrate the essentials of cluster-state quantum computation. In the present experiment, we created a cluster state and performed fixed polarization measurements, that is, projections onto the state $|+\alpha\rangle_j$ in the bases, $B_j(\alpha)$, which require no feedforward or subsequent

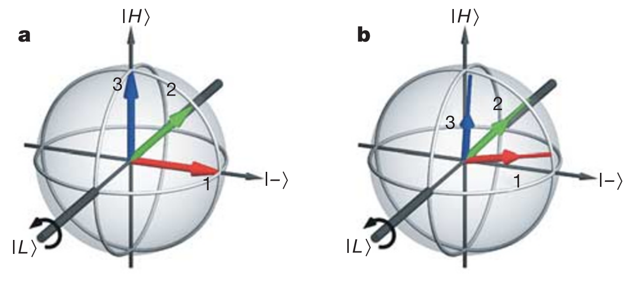

Figure 3 Output Bloch vectors from single qubit rotations using a three-qubit linear cluster $|\Phi_{\mathrm{lin3}}\rangle$. The results of the ideal rotations (**a**) are compared with the results of the measured rotations (**b**) on the encoded input state $|+\rangle_{1E}$ for three different choices of measurement bases $B_2(\alpha)$. The output state is written in the laboratory basis. The measurement basis $B_3(\beta)$ for qubit 3 was fixed at $\beta = \pi/2$. The angle α is set to $\pi/2$, $\pi/4$ and 0 for the Bloch vectors labelled 1, 2 and 3 respectively. These different choices of α result in different rotations about the $|L\rangle$ axis. The sense of the rotation is shown for decreasing α. Our final states, extracted from measured single-qubit tomography, had fidelities of (0.86 ± 0.03), (0.85 ± 0.04) and (0.83 ± 0.03) with respect to the ideal output states. Fidelities of outputs for other choices of angles and hence other rotations are shown in Supplementary Table 1b.

corrections given a successful measurement. This reduces the success rate of the computation by a factor of two for every measurement as compared to ideal, deterministic gate operations, but it certainly suffices as a proof of principle. An important challenge for future work is to implement the fast active switching and logic requirements for one-way quantum computation with feedforward. We have realized a universal set of quantum logic operations in the form of single-qubit rotations and non-trivial two-qubit gates. In the following sections we characterize the quality of each quantum computation by comparing the measured output state to the ideal using the state fidelity. Interesting avenues for study include full quantum gate characterization using quantum process tomography[41,42] or related measures[43].

Single-qubit rotations

We start with the one-dimensional four-qubit linear cluster state, $|\Phi_{\text{lin4}}\rangle$, which implements an arbitrary single-qubit rotation gate (Fig. 1b). In particular, we perform $B_1(\alpha)$, $B_2(\beta)$ and $B_3(\gamma)$ on the physical qubits in the linear cluster basis. The parameters α, β and γ are sufficient to rotate the input qubit to anywhere on the Bloch sphere, or more generally to implement an arbitrary SU(2) single-qubit rotation. This computation rotates the encoded input qubit $|\Psi_{\text{in}}\rangle = |+\rangle_{1\text{E}}$ to the output state $|\Psi_{\text{out}}\rangle = HR_z(-\gamma)R_x(-\beta)R_z(-\alpha)|\Psi_{\text{in}}\rangle$, while the output of this computation is left in the quantum state of qubit 4. We finally characterize physical qubit 4 to verify the performance of the computation using single-qubit quantum state tomography (see Supplementary Table 1a).

The three-qubit linear cluster state $|\Phi_{\text{lin3}}\rangle$ is generated from $|\Phi_{\text{lin4}}\rangle$ by disentangling physical qubit 1 from the cluster. This is achieved by measuring physical qubit 1 in the computational basis for the linear cluster, that is, $\{|+\rangle_1, |-\rangle_2\}$ in the laboratory basis. We consider only those cases where we find the '+' outcome. This resulting cluster state implements the quantum circuit in Fig. 1a, which is a simpler single-qubit rotation gate with rotations determined by the measurements $B_2(\alpha)$ and $B_3(\beta)$ of the second and the third qubit. This rotates the encoded input qubit $|\Psi_{\text{in}}\rangle = |+\rangle_{1\text{E}}$ to the final state, $|\Psi_{\text{out}}\rangle = R_x(-\beta)R_z(-\alpha)|\Psi_{\text{in}}\rangle$, which is again left on physical qubit 4. The computation is directly implemented by performing single-particle measurements on qubits 1, 2 and 3. The single-qubit output stored on qubit 4 is completely characterized by single-qubit tomography. We compare this single output qubit with both the theoretically expected output and the predicted output from our reconstructed four-particle cluster state density matrix. Figure 3 shows the state of qubit 4 on the Bloch sphere in the laboratory basis in the ideal (left-hand side) and measured (right-hand side) case for three different measurement settings. These measurement settings were chosen to clearly show the effect of changing a single measurement basis. For the three state vectors shown as 1, 2 and 3, α was set to $\pi/2$, $\pi/4$ and 0, respectively, while β was fixed to $-\pi/2$. The state fidelities of these and other measurement settings compared to the ideal gate action are shown in Supplementary Table 1b.

Two-qubit gates

In order to perform universal quantum computation, non-trivial two-qubit quantum-logic gates[4] are required in addition to single-qubit rotations. Well-known examples of such gates are the controlled-NOT (CNOT) or CPhase operations. The crucial trait of these gates is that they can change the entanglement between qubits. Gates of this type can be implemented with a two-dimensional cluster. In Fig. 1, we show two-dimensional cluster states—the horseshoe cluster states (Fig. 1c and d) and the box cluster state (Fig. 1e)—that satisfy this condition for two-qubit quantum logic. Both of their quantum circuits comprise single-qubit rotations and CPhase operations that can generate entanglement between two

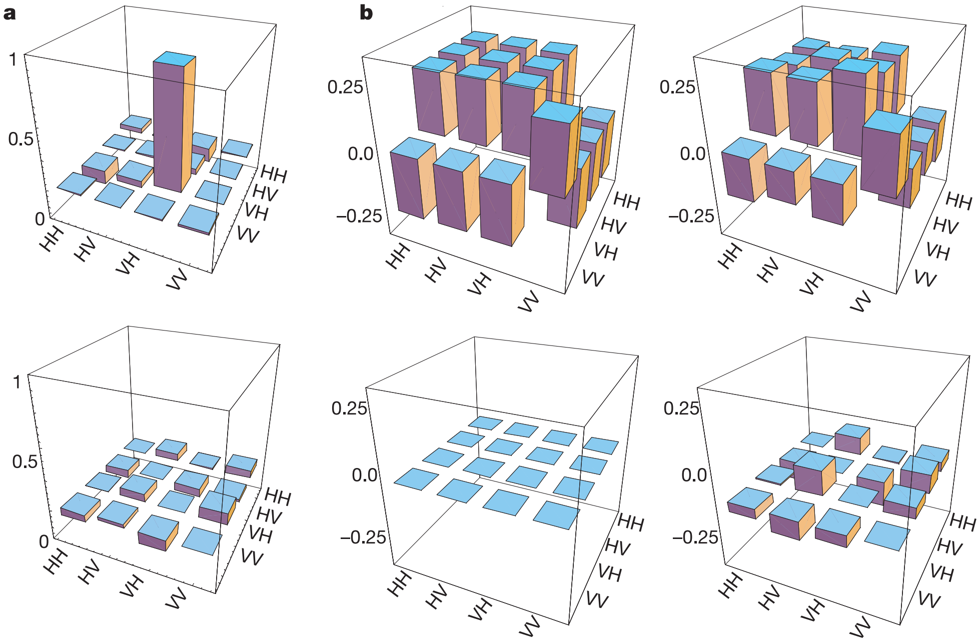

Figure 4 The output density matrices from two different two-qubit computations. Each density matrix is shown as two bar charts, with the upper bar chart depicting the real part of the matrix and the lower chart depicting the imaginary part. In case **a**, single-qubit measurements were made on qubits 1 and 4 in the box cluster state $|\Phi_{\square 4}\rangle$. The measurement settings were $B_1(\pi)$ and $B_4(0)$, which results in the expected output state $|V\rangle_2|H\rangle_3$ in the laboratory basis. The measured density matrix has (0.93 ± 0.01) fidelity with this state and no entanglement. In case **b**, single-qubit measurements in $B_2(0)$ and $B_3(0)$ were made on the horseshoe cluster state $|\Phi_{\subset 4}\rangle$. In this case, the expected output density matrix (left-hand side) and the experimentally measured density matrix (right-hand side) are both shown in the laboratory basis. The measured and expected density matrices are in good agreement and this is reflected in the fidelity (0.84 ± 0.03). We extracted the tangle, a measure of entanglement, from the experimentally measured density matrix as τ=(0.65 ± 0.11). This conclusively demonstrates that our cluster state quantum computer can generate the quantum entanglement necessary for universal quantum computation.

initially separable encoded qubits. Whether or not entanglement is generated depends on the specific circuit and the initial states. We will give a specific example of a two-qubit quantum computation that does not generate entanglement (in the box cluster) and a second computation that does generate entanglement (in the horseshoe cluster).

The box cluster transforms the two-qubit encoded input state according to

$$|\Psi_{\mathrm{out}}\rangle = \mathrm{CPhase}(H_1 \otimes H_2)[R_z(-\alpha)\otimes R_z(-\beta)]\mathrm{CPhase}|\Psi_{\mathrm{in}}\rangle \quad (2)$$

where α and β are determined by measurements $B_1(\alpha)$ and $B_4(\beta)$ on qubits 1 and 4, respectively. For the isolated box (or horseshoe) cluster state, the encoded qubit input state is the product state $|\Psi_{\mathrm{in}}\rangle = |+\rangle_{1\mathrm{E}}|+\rangle_{2\mathrm{E}}$. Consider the case where photons 1 and 4 are measured to be $|V\rangle_1$ and $|H\rangle_4$ in the laboratory basis. For the box cluster, this corresponds to measuring the '0' outcome of $B_1(\pi)$ and $B_4(0)$ respectively on physical qubits 1 and 4. According to the box quantum circuit, this should perform the computation $|+\rangle_{1\mathrm{E}}|+\rangle_{2\mathrm{E}} \rightarrow |+\rangle_{1\mathrm{E}}|-\rangle_{2\mathrm{E}}$ with the resulting product state outcome left on qubits 2 and 3. The experimentally measured final state of qubits 2 and 3, in the laboratory basis, are shown as a two-qubit density matrix in Fig. 4a. The state has a single dominant diagonal element corresponding to the state $|V\rangle_2|H\rangle_3$ and no off-diagonal elements. Recall that the conversion from the box basis to the laboratory basis requires a swap of qubits 2 and 3 and the application of a Hadamard on each qubit. This converts $|+\rangle_{1\mathrm{E}}|-\rangle_{2\mathrm{E}}$ to $|V\rangle_{1\mathrm{E}}|H\rangle_{2\mathrm{E}}$, in agreement with our measured density matrix. The fidelity of this measured density matrix of qubits 2 and 3 with the ideal output is (0.93 ± 0.01). We can quantify the entanglement in the output state using the tangle[44] defined as $\tau = \left[\mathrm{Max}\left(0, \sqrt{\lambda_1} - \sqrt{\lambda_2} - \sqrt{\lambda_3} - \sqrt{\lambda_4}\right)\right]^2$, where λ_i are the eigenvalues of the matrix $\rho\Sigma\rho^T\Sigma$ and $\Sigma = \sigma_y \otimes \sigma_y$, and are decreasingly ordered with λ_1 being the largest. The tangle can range from 0 for separable states to 1 for maximally entangled states. The tangle of our measured density matrix is (0.01 ± 0.01), in agreement with the expected value of 0—no entanglement has been generated in this case. The fidelities of other quantum computations in the box cluster are shown in Supplementary Table 2a, including an example where entanglement is generated.

Encoded two-qubit operations are crucial for cluster state quantum computation as they can generate entanglement. The horseshoe cluster state of Fig. 1c performs the following quantum circuit:

$$|\Psi_{\mathrm{out}}\rangle = (H_1 \otimes H_2)[R_z(-\alpha)\otimes R_z(-\beta)]\mathrm{CPhase}|\Psi_{\mathrm{in}}\rangle \quad (3)$$

For our input state $|\Psi_{\mathrm{in}}\rangle = |+\rangle_{1\mathrm{E}}|+\rangle_{2\mathrm{E}}$, this circuit always generates maximal entanglement. Consider the case where photons 2 and 3 are both measured in the state $|+\rangle$. This measurement corresponds to the '0' outcome of $B_2(0)$ and $B_3(0)$ on physical qubits 2 and 3, and should perform the transformation $|+\rangle_{1\mathrm{E}}|+\rangle_{2\mathrm{E}} \rightarrow \frac{1}{\sqrt{2}}\left(|0\rangle_{1\mathrm{E}}|+\rangle_{2\mathrm{E}} + |1\rangle_{1\mathrm{E}}|-\rangle_{2\mathrm{E}}\right)$, where the output is maximally entangled. The experimentally measured output density matrix of photons 2 and 3 is shown in Fig. 4b (right-hand side). For

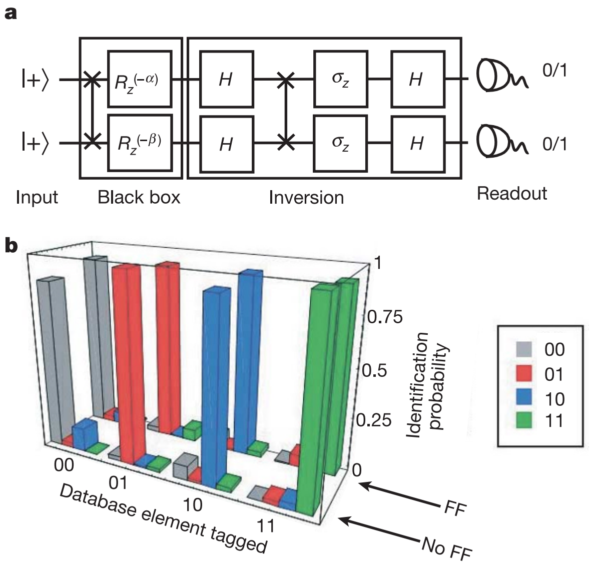

Figure 5 Grover's algorithm in a cluster state quantum computer. **a**, The quantum circuit implementing Grover's search algorithm for two qubits. The box cluster state implements the quantum circuit shown in Fig. 1e. These two circuits perform the equivalent computation when the readout measurements on physical qubits 2 and 3 in the box cluster are carried out in the bases $B_{2,3}(\pi)$. The rotations, and hence black-box function, are fixed by the measurement settings $B_1(\alpha)$ and $B_4(\beta)$ on physical qubits 1 and 4. The circuit implements one of the four black boxes in the search algorithm, and processes the output through an inversion-about-the-mean operation. The output, which is the final states of physical qubits 2 and 3, reveals which black box was applied. **b**, The experimentally measured outputs of this quantum computation. The data labelled 'no FF' show the computational outputs $\{s_2, s_3\}$ in those cases where the measurements in the black box found the '0' outcome. The data labelled 'FF' show the outputs for all individually measured outcomes from the black box to which the feedforward relation $\{s_2 \oplus s_4, s_3 \oplus s_1\}$ has been applied to the output results. The probability for successful identification of the function is approximately 90% in all cases.

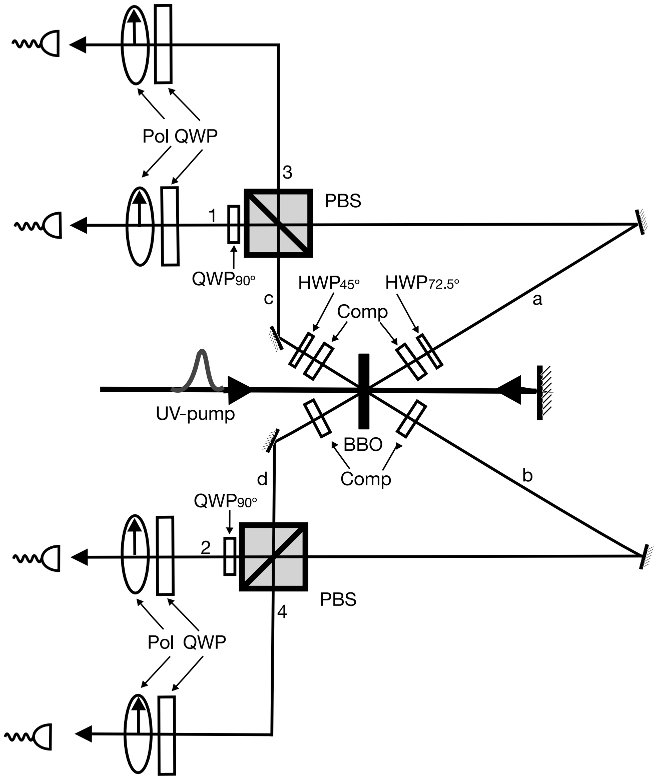

Figure 6 The experimental set-up to produce and measure cluster states. An ultraviolet laser pulse makes two passes through a nonlinear crystal (BBO), which is aligned to produce entangled photon pairs $|\Phi^-\rangle_{a,b}$ in the forward direction in modes a and b, and $|\Phi^+\rangle_{c,d}$ in the backward direction in modes c and d. Compensators (Comp), consisting of a half-wave plate (HWP) and an extra BBO crystal, are placed in each path to counter walk-off effects. Including the possibility of double-pair emission and the action of the polarizing beam-splitters (PBSs), the four components of the cluster state can be prepared. The incorrect phase on the HHVV amplitude can easily be changed by using a HWP in mode a. The amplitudes can be equalized by adjusting the relative coupling efficiency of those photon pairs produced in the backward pass as compared to the forward pass. Polarization measurements were carried out in modes 1 to 4 using quarter-wave plates (QWPs) and linear polarizers (Pol) followed by single-mode fibre-coupled single-photon counting detectors behind 3-nm interference filters.

comparison, the ideal output density matrix is also shown in Fig. 4b (left-hand side). The two density matrices are qualitatively very similar and, indeed, the state fidelity of our measured state with the ideal state is (0.84 ± 0.03). The tangle of this output state is τ=(0.65 ± 0.11), confirming the generation of entanglement between the logical qubits as a result of the quantum computation. Furthermore, this experimentally measured density matrix implies a maximum Clauser–Horne–Shimony–Holt (CHSH) Bell parameter[45] of S=(2.47 ± 0.08), which is well above the S=2 upper limit for local realistic theories. The fidelities of other quantum computations in the horseshoe cluster are shown in Supplementary Table 2b.

Grover's search algorithm

The excitement over quantum computation is based on just a few algorithms, the most well known being Shor's factorization algorithm[3] and Grover's search algorithm[6]. The latter is extremely important, both from a fundamental standpoint, as it is provably more efficient than the best classical algorithm, and from a practical standpoint, because fast searching is central to solving difficult problems. Grover's algorithm has been implemented under the standard model[46,47] both in NMR[48,49] and in optical experiments[47]. Here, we demonstrate a two-qubit implementation of Grover's fast quantum search using the cluster state model.

The goal of a search is to identify one out of N elements of a database. Formally, one could consider the database as a black box that labels one of N possible inputs leaving all others unchanged. The challenge, then, is to find that labelled state. The best classical strategy chooses the inputs randomly one by one and checks for the label; it takes, on average, about N/2 calculations to find the special input. Quantum parallelism in Grover's algorithm allows for all inputs to be processed simultaneously in superposition, while interference enhances the probability of finding the desired outcome in only $O\left(\sqrt{N}\right)$ calculations of the function. In the case of a two-bit function (N=4), the difference is even more dramatic, as Grover's algorithm needs only one calculation of the function, whereas classically three evaluations are needed in the worst case, and 2.25 evaluations are needed on average.

The quantum circuit for the two-qubit Grover algorithm is shown in Fig. 5a. Two input qubits, 1 and 2, are prepared in the state $|+\rangle_1|+\rangle_2$. This is a superposition of all four computational basis states $|0\rangle|0\rangle$, $|0\rangle|1\rangle$, $|1\rangle|0\rangle$ and $|1\rangle|1\rangle$. As one of four possibilities, the black box could label the state $|0\rangle|1\rangle \rightarrow -|0\rangle|1\rangle$ by changing its sign and leaving all other states unchanged. Note that the change of sign is equivalent to a bit flip on an ancillary qubit. Any of the four possibilities can be set by proper choices of the rotation angles α and β. The output from the black box is processed by an operation that inverts the amplitudes for each computational state about the mean value. This process amplifies the labelled amplitude and reduces the rest. In the two-qubit case, theory predicts that after a single application of this inversion, the computer outputs the labelled state with probability 1.

We can compare this circuit for the two-qubit Grover algorithm to that implemented by the box cluster state in Fig. 1e. The Grover algorithm circuit contains extra fixed single-qubit operations (a σ_z followed by a Hadamard transformation, H) on each qubit before the readout in the computational basis. Measurement of a final physical qubit in the computational basis after a σ_z followed by H is equivalent to direct measurement of those qubits in the basis $B(\pi)$, that is, we can absorb these additional fixed single-qubit operations into the readout stage. The quantum circuit implemented by the box cluster can be seen as precisely that one required for Grover's algorithm provided that the final readout measurements are made in $B_{2,3}(\pi)$ on physical qubits 2 and 3.

The cluster state computation proceeds as follows. The encoded qubits begin in the state $|+\rangle_1|+\rangle_2$. Setting the measurement angles, $\alpha\beta$, to $\pi\pi$, $\pi 0$, 0π and 00 determines the black-box settings 00, 01, 10 and 11, respectively. In principle, these settings remain hidden. The result of a measurement of physical qubit i is s_i, which is 0 (1) for a measurement of $|+\alpha\rangle$ $\left(|-\alpha\rangle\right)$. For the computation to proceed deterministically, the black box must provide the measurement outcomes for feedforward. The encoded qubits are transferred non-locally to the remaining physical qubits in the cluster. Remarkably, the inversion-about-the-mean process is already 'hard-wired' into the structure of the cluster state and is automatically implemented. The output of the computation, including feedforward (FF), are two bits $\{s_2 \oplus s_4, s_3 \oplus s_1\}$ identifying the black box.

In Fig. 5b, we show the experimental outcomes of the quantum computation. As in the previous computations, measurements were made using quarter-wave plates and polarizers. The 'no FF' data are the computational outputs obtained when the black-box outcomes, s_1 and s_4, were 0, which requires no feedforward but reduces the success rate to 1/4. In addition, we have measured individually all possible correlations between the measurement results from the black box and the readout. This enables us to implement the simplest feedforward possible, where the earlier measurement determines the meaning of the final readout. Thus, when the black-box measurement outcomes are other than s_1=0 and s_4=0, it is necessary to reinterpret the readout via the bitwise addition shown above; the 'FF' row of data in Fig 5b shows the sum of the readouts interpreted in this way. In either case, the probability of the quantum computer determining the correct outcome is about 90%. These high-fidelity results (Fig. 5b) constitute, to our knowledge, the first demonstration of a quantum algorithm in a cluster state quantum computer.

Discussion

We have generated a four-qubit cluster state, and characterized that state and its entanglement features. With that cluster, and taking advantage of a curious equivalence of a number of cluster states, we have demonstrated a universal set of single-qubit and non-trivial two-qubit quantum logic gates in a one-way quantum computer. Our final realization of the Grover algorithm strongly underlines the basic simplicity of the cluster state approach. Given the various alternatives for their creation, such as linear optics, ion traps and optical lattices, and the recent advances in the preparation of multiparticle entangled states, cluster states are promising for inclusion in future implementations of quantum computation. The most important challenges for the optical approach presented here are (1) realization of cluster states on demand, (2) generating cluster states with more qubits and (3) implementation of fast feedforward where earlier measurement outcomes actually change the setting of a future measurement in real time. □

Methods

Experimental preparation of cluster states

In our experiment, entangled photons are created by using type-II parametric down-conversion[50]. A frequency-doubled laser pulse at 795 nm makes two passes through a β-barium borate (BBO) crystal, which emits highly entangled photons into the forward pair of modes a and b and the backward pair of modes c and d (Fig. 6). To counter the effect of birefringence in the BBO crystal, the polarization in each mode is rotated by 90° and the photons pass through compensation crystals that erase transverse and longitudinal walk-off. Final half-wave plates (HWPs), one for each photon pair, and the tilt of the compensation crystals allow for the production of any of the four Bell states. The modes of the forward emitted pairs a and b and the modes of the backward emitted pairs c and d are coherently combined at polarizing beam-splitters (PBSs) by adjusting the position of the delay mirror for the ultraviolet pump. The preparation of the cluster state is based on the simultaneous emission of four photons. The construction of the set-up allows for four photon events to come from either two entangled pairs, one forward and one backward, or from double-pair emission into the modes a and b, and c and d[26].

Proposed methods for producing cluster states are based on series of two-qubit gates, such as the CPhase or CNOT. In our case, the four-photon cluster state is generated directly from parametric down-conversion. Because of its intrinsically probabilistic nature, the down-conversion process becomes exponentially inefficient for generating larger cluster states. Our way of generating the cluster states furthermore exploits the properties of PBSs and uses post-selection. A PBS is an optical device that transmits horizontally polarized light and reflects vertically polarized light. Considering the two-photon case, where after the PBS in each mode one photon has to be detected, both incoming photons must have the same polarization when they come from different input modes, or they must have orthogonal polarizations when entering along the same input mode. If the source produces simultaneously a $|\Phi^-\rangle_{a,b}$ state into the forward pair of modes, and backwards a $|\Phi^+\rangle_{c,d}$ state, only the state $|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 - |V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$ results in a four-photon coincidence. However, there exists also the case where a four-photon emission into the two modes on either side results in a fourfold coincidence. The state must be in this case $-|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$ coming from the $|\Phi^-\rangle_{a,b}$ setting and $+|V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4$ coming from the $|\Phi^+\rangle_{c,d}$ setting. The final emerging state is a superposition of all four terms.

In order to produce a cluster state, the phase of the $-|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$ term has to be shifted by π. This can be done using a HWP in one mode, where a polarization rotation of an angle ϕ causes the state after the PBSs to evolve to $-\cos(2\phi)|H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4$. Thus any HWP rotation larger than 22.5° results in a sign flip. At the same time, the Bell state is converted to $\cos(\phi)|\Phi^-\rangle_{a,b} + \sin(\phi)|\Psi^+\rangle_{a,b}$, where the amount of the wanted $|\Phi^-\rangle_{a,b}$ state is decreased by a factor of $\cos(\phi)$. Owing to the properties of the PBS, only the amplitudes for the $|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 - |V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4$ terms are affected, while the $|\Psi^+\rangle_{1,2}$ Bell state does not contribute to any fourfold coincidence.

Note that after each PBS a quarter-wave plate (QWP) was placed to compensate for birefringence effects. For each measurement, the phase of the back-reflected pair or four-photon was kept fixed and verified for each measurement setting. Taking into account the emission rates of the source for the entangled pairs (28,000 s^{-1} two-photon coincidences for the forward-emitted pair, and 18,000 s^{-1} coincidences for the backward-emitted pair), theoretical calculations show that a HWP rotation by 27.5° results in the maximally entangled cluster state of the form $|\Phi_{cluster}\rangle = \frac{1}{2}(|H\rangle_1|H\rangle_2|H\rangle_3|H\rangle_4 + |H\rangle_1|H\rangle_2|V\rangle_3|V\rangle_4 + |V\rangle_1|V\rangle_2|H\rangle_3|H\rangle_4 - |V\rangle_1|V\rangle_2|V\rangle_3|V\rangle_4)$. Thus, a HWP in mode a has been rotated to prepare this state. Fine-tuning has been done by short measurements to obtain approximately equal count rates for each component.

Received 7 October 2004; accepted 11 January 2005; doi:10.1038/nature03347.

1. Deutsch, D. & Ekert, E. Quantum computation. *Phys. World* **11,** 47–52 (1998).
2. Braunstein, S. L. & Lo, H.-K. (eds) Experimental proposals for quantum computation. *Fortschr. Phys.* **48** (special focus issue 9–11), 767–1138 (2000).
3. Shor, P. W. in *Proc. 35th Annu. Symp. Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE Computer Society Press, Los Alamitos, 1994).
4. Grover, L. K. Quantum mechanics helps in search for a needle in a haystack. *Phys. Rev. Lett.* **79,** 325–328 (1997).
5. Bennett, C. & DiVicenzo, D. Quantum information and computation. *Nature* **404,** 247–255 (2000).
6. Ekert, A. & Josza, R. Quantum algorithms: entanglement enhanced information processing. *Phil. Trans. R. Soc. Lond. A* **356,** 1769–1782 (1998).
7. Gottesman, D. & Chuang, I. L. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature* **402,** 390–393 (1999).
8. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409,** 46–52 (2001).
9. Linden, N. & Popescu, S. Good dynamics versus bad kinematics: Is entanglement needed for quantum computation? *Phys. Rev. Lett.* **87,** 047901 (2001).
10. Josza, R. & Linden, N. On the role of the entanglement in quantum computational speed-up. *Proc. R. Soc. Lond. A* **459,** 2011–2032 (2003).
11. Nielsen, M. A. Quantum computation by measurement and quantum memory. *Phys. Lett. A* **308,** 96–100 (2003).
12. Biham, E., Brassard, G., Kenigsberg, D. & Mor, T. Quantum computing without entanglement. *Theor. Comput. Sci.* **320,** 15–33 (2004).
13. Briegel, H. J. & Raussendorf, R. Persistent entanglement in arrays of interacting particles. *Phys. Rev. Lett.* **86,** 910–913 (2001).
14. Raussendorf, R. & Briegel, H. J. A one-way quantum computer. *Phys. Rev. Lett.* **86,** 5188–5191 (2001).
15. Raussendorf, R. & Briegel, H. J. Computational model underlying the one-way quantum computer. *Quant. Inform. Comput.* **2,** 344–386 (2002).
16. Raussendorf, R., Brown, D. E. & Briegel, H. J. The one-way quantum computer—a non-network model of quantum computation. *J. Mod. Opt.* **49,** 1299–1306 (2002).
17. Raussendorf, R., Brown, D. E. & Briegel, H. J. Measurement-based quantum computation on cluster states. *Phys. Rev. A* **68,** 022312 (2003).
18. Nielsen, M. & Dawson, C. M. Fault-tolerant quantum computation with cluster states. Preprint at ⟨http://arXiv.org/quant-ph/0405134⟩ (2004).
19. Mandel, O. *et al.* Controlled collisions for multiparticle entanglement of optically trapped ions. *Nature* **425,** 937–940 (2003).
20. 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).
21. Pittman, T. B., Fitch, M. J., Jacobs, B. C. & Franson, J. D. Experimental controlled-not logic gate of single photons in the coincidence basis. *Phys. Rev. A.* **68,** 032316 (2003).
22. Gasparoni, S., Pan, J.-W., Walther, P., Rudolph, T. & Zeilinger, A. Realization of a photonic controlled-NOT gate sufficient for quantum computation. *Phys. Rev. Lett.* **92,** 020504 (2004).
23. Sanaka, K., Jennewein, T., Pan, J.-W., Resch, K. & Zeilinger, A. Experimental nonlinear sign-shift for linear optics quantum computation. *Phys. Rev. Lett.* **92,** 017902 (2004).
24. Nielsen, M. A. Optical quantum computation using cluster states. *Phys. Rev. Lett.* **93,** 040503 (2004).
25. Brown, D. E. & Rudolph, T. Efficient linear optical quantum computation. Preprint at ⟨http://arXiv.org/quant-ph/0405157⟩ (2004).
26. Walther, P. *et al.* De Broglie wavelength of a non-local four-photon state. *Nature* **429,** 158–161 (2004).
27. Hein, M., Eisert, J. & Briegel, H.-J. Multi-party entanglement in graph states. *Phys. Rev. A* **69,** 062311 (2004).
28. Roos, C. F. *et al.* Control and measurement of three-qubit entangled states. *Science* **304,** 1478–1480 (2004).
29. Weinstein, Y. *et al.* Quantum process tomography of the quantum Fourier transform. *J. Chem. Phys.* **121,** 6117–6133 (2004).
30. Hradil, Z. Quantum-state estimation. *Phys. Rev. A* **55,** R1561–R1564 (1997).
31. Banaszek, K., Ariano, A., Paris, M. & Sacchi, M. Maximum-likelihood estimation of the density matrix. *Phys. Rev. A* **61,** 010304 (1999).
32. James, D., Kwiat, P., Munro, W. & White, A. Measurement of qubits. *Phys. Rev. A* **64,** 052312 (2001).
33. Toth, G. & Guehne, O. Detecting genuine multipartite entanglement with two local measurements. Preprint at ⟨http://arXiv.org/quant-ph/0405165⟩ (2004).
34. Dür, W. & Briegel, H.-J. Stability of macroscopic entanglement under decoherence. *Phys. Rev. Lett.* **92,** 180403 (2004).
35. Greenberger, D. M., Horne, M. A. & Zeilinger, A. in *Bell's Theorem, Quantum Theory and Concepts of the Universe* (ed. Kafatos, M.) (Kluwer, Dordrecht, 1989).
36. Zeilinger, A., Horne, M. & Greenberger, D. in *Squeezed States and Quantum Uncertainty* (eds Han, D., Kim, Y. S. & Zachary, W. W.) (NASA Conference Publication 3135, NASA, College Park, 1992).
37. Dür, W., Vidal, G. & Cirac, J. I. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A* **62,** 62314–62325 (2000).
38. SenDe, A., Sen, U., Wiesniak, M., Kaszlikowski, D. & Zukowski, M. Multi-qubit W states lead to stronger nonclassicality than Greenberger-Horne-Zeilinger states. *Phys. Rev. A* **68,** 623306 (2003).
39. Horodecki, M., Horodecki, P. & Horodecki, R. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A* **223,** 1–8 (1996).
40. Peres, A. Separability criterion for density matrices. *Phys. Rev. Lett.* **77,** 1413–1415 (1996).
41. Chuang, I. L. & Nielsen, M. A. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.* **44,** 2455–2467 (1997).
42. Poyatos, J. F., Cirac, J. I. & Zoller, P. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.* **78,** 390–393 (1997).
43. Schumacher, B. Quantum coding. *Phys. Rev. A* **51,** 2738–2747 (1995).
44. Coffman, V., Kundu, J. & Wootters, W. K. Distributed entanglement. *Phys. Rev. A* **61,** 052306 (2000).
45. Horodecki, R., Horodecki, P. & Horodecki, M. Violating Bell inequality by mixed spin-1/2 states: necessary and sufficient condition. *Phys. Lett. A* **200,** 340–344 (1995).
46. Ahn, J., Weinacht, T. C. & Bucksbaum, P. H. Information storage and retrieval through quantum phase. *Science* **287,** 463–465 (2000).
47. Bhattacharya, N., van Linden van den Heuvell, H. B. & Spreeuw, R. J. C. Implementation of quantum search algorithm using classical Fourier optics. *Phys. Rev. Lett.* **88,** 137901 (2002).
48. Chuang, I. L., Gershenfeld, N. & Kubinec, M. Experimental implementation of a fast quantum searching. *Phys. Rev. Lett.* **80,** 3408–3411 (1997).
49. Jones, J. A., Mosca, M. & Hansen, R. H. Implementation of a quantum search algorithm on a quantum computer. *Nature* **393,** 344–346 (1998).
50. Kwiat, P. G. *et al.* New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.* **75,** 4337–4342 (1995).

Supplementary Information accompanies the paper on **www.nature.com/nature**.

Acknowledgements We thank H. J. Briegel, D. Browne and M. Zukowski for theoretical discussions, and C. Först for assistance with graphics. This work was supported by the Austrian Science Foundation (FWF), NSERC, the European Commission under project RAMBOQ, and by the Alexander von Humboldt Foundation.

Competing interests statement The authors declare that they have no competing financial interests.

Correspondence and requests for materials should be addressed to P.W. (pwalther@quantum.at) or A.Z. (zeilinger-office@quantum.at).