

A quantum Fredkin gate

Raj B. Patel,^{1,*} Joseph Ho,¹ Franck Ferreyrol,^{1,2} Timothy C. Ralph,³
& Geoff J. Pryde,^{1,*}

¹CQC2T and Centre for Quantum Dynamics, Griffith University,
Brisbane 4111, Australia

² Laboratoire Photonique, Numerique et Nanosciences, Institut d'Optique,
CNRS and Université de Bordeaux, Talence, France

³ CQC2T and School of Mathematics and Physics, University of Queensland,
Brisbane 4072, Australia

*To whom correspondence should be addressed; E-mail: r.patel@griffith.edu.au
or g.pryde@griffith.edu.au

Key to realising quantum computers is minimising the resources required to build logic gates into useful processing circuits. While the salient features of a quantum computer have been shown in proof-of-principle experiments, difficulties in scaling quantum systems have made more complex operations intractable. This is exemplified in the classical Fredkin (controlled-SWAP) gate for which, despite theoretical proposals, no quantum analogue has been realised. By adding control to the SWAP unitary, we use photonic qubit logic to demonstrate the first quantum Fredkin gate, which promises many applications in quantum information and measurement. We implement example algorithms and generate the highest-fidelity three-photon GHZ states to-date. The technique we use allows one to add a control operation to a black-box unitary, something impossible in the standard circuit model. Our experiment represents the first use of this technique to control a two-qubit operation and paves the way for larger controlled circuits to be realised efficiently.

Introduction

One of the greatest challenges in modern science is the realisation of quantum computers (*1–3*) which, as they increase in scale, will allow enhanced performance of tasks in secure networking, simulations, distributed computing and other key tasks where exponential speedups are available. Processing circuits to realise these applications are built up from logic gates that harness quantum effects such as superposition and entanglement. At present, even small-scale and medium-scale quantum computer circuits are hard to realise because of the requirement to control enough quantum systems sufficiently well in order to chain together many gates into circuits. One example of this is the quantum Fredkin gate, which requires at least five two-qubit gates (*4*) to be implemented in the standard circuit model. Thus, despite featuring prominently in schemes for quantum computation (*5–7*), error-correction (*8, 9*), cryptography (*10–12*), and measurement (*13, 14*), no such gate has been realised to date.

The quantum Fredkin gate, shown in Fig. 1A, is a three-qubit gate whereby, conditioned on the state of the control qubit, the quantum states of the two target qubits are swapped. The original, classical version of the gate first proposed by Fredkin (*15*) also serves as one of the first examples of a reversible logic operation where the number of bits are conserved and no energy is dissipated as a result of erasure. In the framework of universal quantum computation, gates are also reversible, so it may seem

natural to ask whether it is possible to construct a quantum version of the Fredkin gate. The first design of the quantum Fredkin gate was proposed by Milburn (*16*) and was to use single photons as qubits and cross-Kerr nonlinearities to produce the necessary coherent interactions. Further schemes utilising linear optics developed these ideas further (*4, 17–20*) by using ancilla photons, interference, and multiple two-qubit (*21, 22*) and single-qubit gates. However concatenating multiple probabilistic gates in this fashion typically leads to a multiplicative reduction in the overall probability of success of $< 1/100$. Hence it would be desirable to be able to construct a quantum Fredkin gate directly without decomposition and avoid the associated resource overhead.

We begin by describing the concept of our experiment. We perform the controlled-SWAP operation by adding control to the SWAP unitary U_{SWAP} applying the technique in Zhou *et al.* (*23*), to greatly reduce the complexity of quantum circuits. The notion of adding control to a black-box unitary is forbidden or difficult in many architectures (*24, 25*) – optics lends itself well to this approach because the optical implementation of the unitary leaves the vacuum state unchanged. Here we utilise this method to simplify a controlled multi-qubit operation. A key idea in our demonstration is to use entanglement in a non-qubit degree of freedom (we use the photon's path mode) to drive the operation of the gate. This path entanglement can be produced in different ways. In our demonstration (Fig. 1B), it is generated

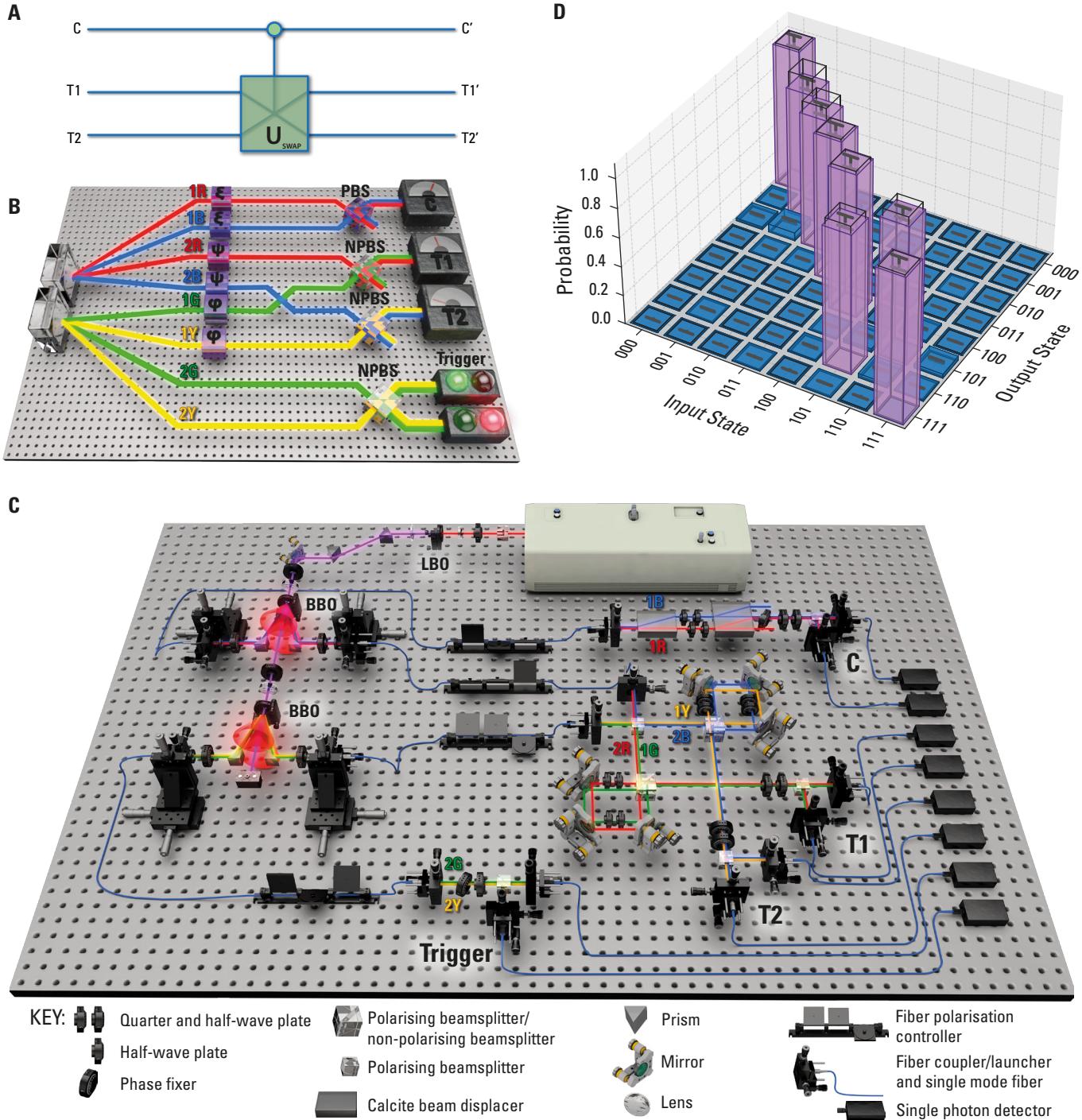


Fig. 1. Experimental arrangement and truth table measurements. **A**, The quantum Fredkin gate circuit. The states of the target qubits are either swapped or not swapped depending on the state of the control qubit. **B**, Concept of our experiment. Two SPDC photon sources allow production of path entanglement such that modes R and Y are entangled with modes B and G . The SWAP operation is carried out on the path modes, depending on the control photon's state, such that arrival of the control photon indicates a system state of $\alpha|H\rangle^C|\psi\rangle^{T_1}|\varphi\rangle^{T_2} + \beta|V\rangle^C|\varphi\rangle^{T_1}|\psi\rangle^{T_2}$. **C**, The experimental arrangement. Entangled photons are produced via SPDC (see Materials and Methods). Entering the gate via single-mode fiber, the two target photons are sent through a PBS. The path-entangled state in Eq. 1 is produced after each target photon enters a displaced Sagnac interferometer and the which-path information is erased on an NPBS. QWPs and HWPs encode the polarisation state in Eq. 2. The control consists of a polarisation beam displacer interferometer. The desired control state is encoded onto modes $1R$ and $1B$ and coherently recombined. A tilted HWP is used to set the phase of the output state. Successful operation is heralded by four-fold coincidence events between the control, target, and trigger detectors. **D**, Ideal (transparent bars) and measured (solid bars) truth table data for our gate. A total of 620 four-fold events were measured for each of the eight measurements, giving $\langle O \rangle = 96 \pm 4\%$.

from spontaneous parametric down-conversion (SPDC). Given the physical arrangement of the circuit and that we only accept detection events where a single photon is counted at each of the four outputs simultaneously, the optical quantum state produced by SPDC is converted to the required four-photon path-mode entangled state (see Materials and Methods) and has the form

$$(|11\rangle_B|11\rangle_G|00\rangle_R|00\rangle_Y + |00\rangle_B|00\rangle_G|11\rangle_R|11\rangle_Y) / \sqrt{2} \quad (1)$$

where B , R , Y , and G refer to path-modes and, for example, $|11\rangle_B$ indicates a photon occupying mode $1B$ and another occupying $2B$. The path-modes are distributed throughout the circuit such that U_{SWAP} is applied only to the B and G modes. The qubit state is encoded on the polarisation of the photon. Because the photons are in a spatial superposition, polarisation preparation optics must be applied to both path-modes of each photon. Hence, an arbitrary, separable, three-qubit state $|\xi\rangle|\psi\rangle|\varphi\rangle$ can be prepared as an input to the gate. In particular, the control qubit is encoded on modes $1R$ and $1B$, target 1 is encoded on modes $2R$ and $2B$, and target 2 is encoded on modes $1G$ and $1Y$, yielding

$$(|\xi\rangle_{1B}^C|\psi\rangle_{2B}^{T1}|\varphi\rangle_{1G}^{T2}|H\rangle_{2G}^{Tr} + |\xi\rangle_{1R}^C|\psi\rangle_{2R}^{T1}|\varphi\rangle_{1Y}^{T2}|V\rangle_{2Y}^{Tr}) / \sqrt{2} \quad (2)$$

The two control modes $1R$ and $1B$ are mixed on a polarising beam splitter (PBS), whereas a 50:50 non-polarising beam splitter (NPBS) is used to erase the path information in the target and trigger arms. The SWAP is implemented via rearrangement of the path-modes such that the target modes $2B$ and $1G$ are swapped whereas $2R$ and $1Y$ are not. Successful operation of the gate occurs when photons are detected at the control, target 1, and target 2 detectors (simultaneously with a photon detection at either trigger detector). The polarisation state of the three-qubit system, given the required modes are occupied, is $\alpha|H\rangle^C|\psi\rangle^{T1}|\varphi\rangle^{T2} + \beta|V\rangle^C|\varphi\rangle^{T1}|\psi\rangle^{T2}$ as expected from application of the Fredkin gate on the state $|\xi\rangle^C|\psi\rangle^{T1}|\varphi\rangle^{T2}$ where $|\xi\rangle = \alpha|H\rangle + \beta|V\rangle$. Taking into consideration the probability of recording a four-fold coincidence, successful execution of the gate occurs one-sixteenth of the time, on average. This can be increased to one-fourth of the time by collecting the target photons from both NPBS outputs.

Results

The experimental arrangement of the quantum Fredkin gate is shown in Fig. 1C and consists of three interferometers designed to be inherently phase-stable. Pairs of polarisation entangled photons, produced by two SPDC crystals (see Materials and Methods), impinge on a PBS. Two orthogonally polarised photons, one from each source, are sent to separate displaced Sagnac interferometers. Initially, they are incident on a beam splitter where one half of the interface acts as a PBS and the other half acts as an NPBS. Entering at the PBS side, photons may travel along counterpropagating path modes where the polarisation state $|\psi\rangle$ is encoded onto one mode and the state $|\varphi\rangle$ is encoded on the other. The two paths are then recombined on the NPBS side of the beam splitter where the path information is erased (see Methods and Materials), giving the path-mode entangled state in equation 1 whilst the polarisation encoding procedure leads to the state in Eq. 2. The control of the gate is

realised in a polarisation interferometer consisting of two calcite beam displacers. The desired polarisation state of the control is encoded onto modes $1R$ and $1B$, which are coherently recombined in the second beam displacer. Given successful operation (arrival of a photon at the control detector), the preparation of the control photon in $|H\rangle = |1\rangle$ projects the target photons onto path modes $1G$ and $2B$ which undergo SWAP; conversely, preparing $|V\rangle = |0\rangle$ projects the target photons onto path modes $2R$ and $1Y$, which undergo the identity operation. In practice, the trigger arm consists of a half-wave plate (HWP) whose optic axis (OA) is set to 22.5° , producing diagonal $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ or anti-diagonal $|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ polarised photons, and a PBS. Successful operation is heralded by measuring four-fold coincidences across the trigger, control and two target detectors.

The logical operation of the gate was measured by performing eight measurements, one for each of the possible logical inputs. For each input we measure a total of 620 four-fold events distributed across the eight possible output states. Under ideal operation, for a given input, there is a single output. The solid bars in Fig. 1D depict the experimentally measured truth table data, M_{exp} , whereas the transparent bars represent the ideal truth table M_{ideal} . To quantify the mean overlap between M_{exp} and M_{ideal} , we calculate $\langle \mathcal{O} \rangle = Tr(M_{exp}M_{ideal}^T/M_{ideal}M_{ideal}^T) = 96 \pm 4\%$ which confirms excellent performance in the logical basis. The slight reduction in fidelity is most likely due to the imperfect extinction of our polarisation optics.

We demonstrate the full quantum nature of our gate by preparing the control in a superposition $|\xi\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ which places the gate in a superposition of the SWAP and identity operations. Using our gate, we produce four of the eight maximally entangled three-photon Greenberger-Horne-Zeilinger (GHZ) states, namely

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)^C|1\rangle^{T1}|0\rangle^{T2} \rightarrow |GHZ_1^\pm\rangle \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle^C|1\rangle^{T1}|0\rangle^{T2} \pm e^{i(\phi+\theta(\vartheta))}|1\rangle^C|0\rangle^{T1}|1\rangle^{T2}\right) \end{aligned} \quad (3)$$

and,

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)^C|0\rangle^{T1}|1\rangle^{T2} \rightarrow |GHZ_2^\pm\rangle \\ &= \frac{1}{\sqrt{2}}\left(|0\rangle^C|0\rangle^{T1}|1\rangle^{T2} \pm e^{i(\phi+\theta(\vartheta))}|1\rangle^C|1\rangle^{T1}|0\rangle^{T2}\right) \end{aligned} \quad (4)$$

Here ϕ is a phase shift intrinsic to the gate, and $\theta(\vartheta)$ is a corrective phase shift that can be applied by tilting a HWP at OA by an angle ϑ , such that $\phi + \theta(\vartheta) = 2n\pi$ (see Materials and Methods). In doing so, we are able to test the coherent interaction of all three qubits in the gate, which is a key requirement for constructing universal quantum computers. For each of the four states in Eqs. 3 and 4, we perform three-qubit quantum state tomography (QST) to fully characterise the state. The control and target qubits are measured independently in the D/A basis, which we denote as σ_x ; in the R/L basis (σ_y), where $|R\rangle =$

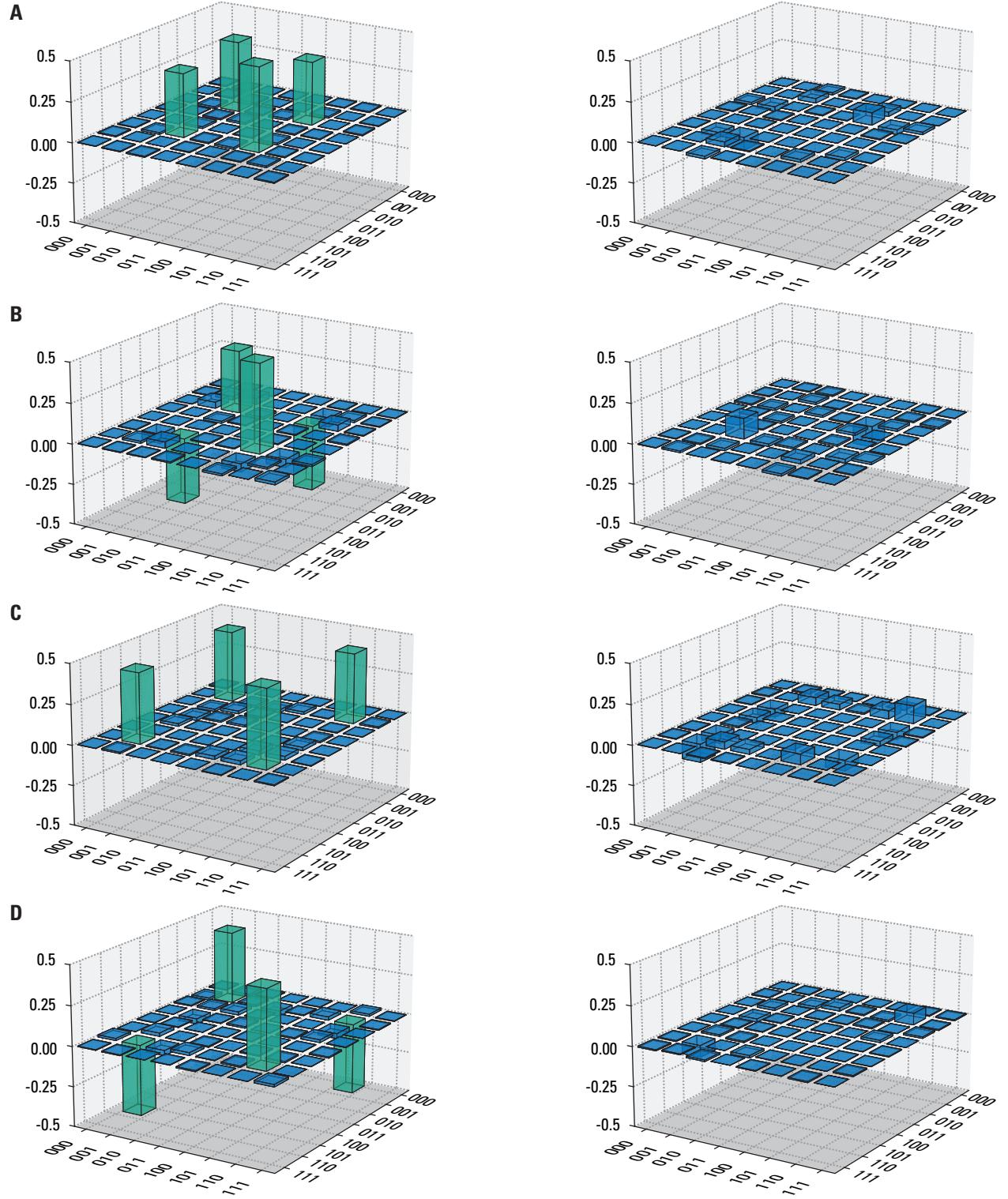


Fig. 2. Real (left) and imaginary (right) parts of the reconstructed density matrices for our four GHZ states. Fidelity and purity were calculated for each state. **A**, $|GHZ_1^+\rangle$: $F = 0.88 \pm 0.01$ and $P = 0.79 \pm 0.02$. **B**, $|GHZ_1^-\rangle$: $F = 0.90 \pm 0.01$ and $P = 0.83 \pm 0.02$. **C**, $|GHZ_2^+\rangle$: $F = 0.93 \pm 0.01$ and $P = 0.87 \pm 0.02$. **D**, $|GHZ_2^-\rangle$: $F = 0.92 \pm 0.01$ and $P = 0.85 \pm 0.02$.

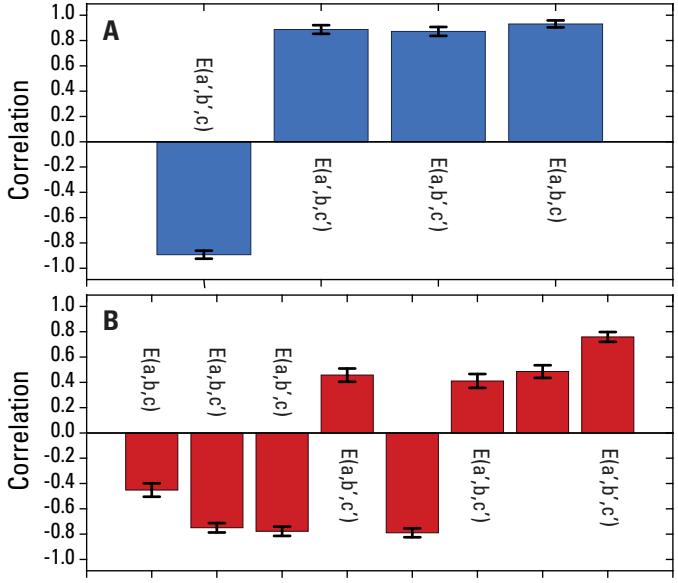


Fig. 3. Measured correlations for violations of Mermin's and Svetlichny's inequalities. **A**, Mermin's inequality resulting in $S_M = 3.58 \pm 0.06$, a violation by 24 standard deviations. **B**, Svetlichny's inequality with $S_{Sv} = 4.88 \pm 0.13$, a violation by 7 standard deviations. Error bars were calculated from Poissonian counting statistics.

$\frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$ and $|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$; and in the H/V basis (σ_z). Therefore full state reconstruction can be carried out by a set of 27 measurements settings ($\sigma_x\sigma_x\sigma_x$, $\sigma_x\sigma_x\sigma_y$...) effectively resulting in an over-complete set of 216 projective measurements as each measurement setting has eight possible outcomes. Figure 2 shows the real (left) and imaginary (right) parts of the reconstructed density matrices of the four GHZ states, each of which was calculated from ~ 5000 four-fold events using a maximum-likelihood algorithm. We measure fidelities and purities of $F = 0.88 \pm 0.01$ and $P = 0.79 \pm 0.02$ for $|GHZ_1^+\rangle$, $F = 0.90 \pm 0.01$ and $P = 0.83 \pm 0.02$ for $|GHZ_1^-\rangle$, $F = 0.93 \pm 0.01$, and $P = 0.87 \pm 0.02$ for $|GHZ_2^+\rangle$, and $F = 0.92 \pm 0.01$ and $P = 0.85 \pm 0.02$ for $|GHZ_2^-\rangle$. The errors were calculated from 500 samples of a Monte-Carlo simulation. These values are most likely limited by imperfect mode overlap at the NPBS in each displaced Sagnac interferometer. Nevertheless, to the best of our knowledge, these values are the highest reported for photonic GHZ states surpassing the previous values reported in Hamel *et al.* (26).

We perform further measurements to characterise the quality of the $|GHZ_2^+\rangle$ state. GHZ states can show a strong contradiction between local hidden-variable theories and quantum mechanics (27). Mermin (28) derived a Bell-like inequality by imposing locality and realism for three particles, which holds for any local hidden-variable theory

$$S_M = |E(a',b,c') + E(a,b',c') + E(a,b,c) - E(a',b',c)| \leq 2 \quad (5)$$

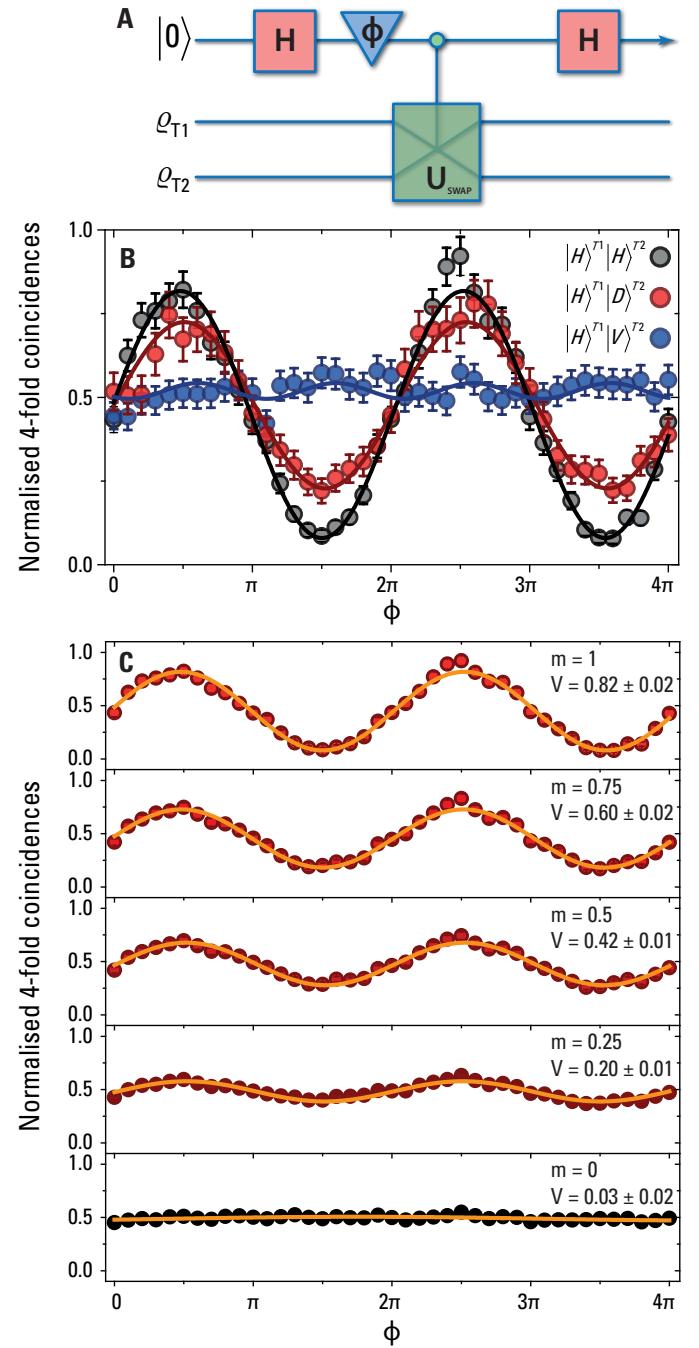


Fig. 4. Estimations of nonlinear functionals of a single-qubit state with the quantum Fredkin gate. **A**, Circuit diagram of the network. **B**, Measurements of the overlap of two single qubit states, $|\langle T1|T2 \rangle|^2$. The fringe visibility or overlap was measured for states $|0\rangle^{T1}|0\rangle^{T2}$ (black), $\frac{1}{\sqrt{2}}(|0\rangle \pm 1)^{T1}|0\rangle^{T2}$ (red), and $|0\rangle^{T1}|1\rangle^{T2}$ (blue) with values 0.82 ± 0.02 , 0.52 ± 0.02 , and 0.05 ± 0.01 , respectively. **C**, Measurements of the state purity. We measure a visibilities ranging from 0.82 ± 0.02 for a pure state to 0.03 ± 0.02 for a maximally mixed state.

This inequality can be violated by performing measurements with settings $a = b = c = \sigma_x$ and $a' = b' = c' = \sigma_y$ with a maximum violation of $S_M = 4$. From the QST of $|GHZ_2^+\rangle$, 747 of the total 5029 four-fold events can be used to calculate the correlation functions E in Eq. 5; these results are shown in

Fig. 3A. This leads to $S_M = 3.58 \pm 0.06$ which is a violation by 24 standard deviations. The implication of using these particular measurement settings is that the state exhibits genuine tripartite entanglement.

An additional test, namely, the violation of Svetlichny's inequality, is required to test whether the state is capable of displaying tripartite non-locality (29, 30). Non-local hidden variable theories cannot be ruled out with Mermin's inequality, as they can be violated for arbitrarily strong correlations between two of the three particles. Svetlichny's inequality takes the form

$$\begin{aligned} S_{Sv} = & |E(a, b, c) + E(a, b, c') + E(a, b', c) - E(a, b', c') \\ & + E(a', b, c) - E(a', b, c') - E(a', b', c) - E(a', b', c')| \\ & \leq 4 \end{aligned} \quad (6)$$

with settings $a = Sv1_{\pm}$ (where $|Sv1_{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm e^{\frac{i3\pi}{4}}|V\rangle)$), $a' = Sv2_{\pm}$ (where $|Sv2_{\pm}\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm e^{\frac{i\pi}{4}}|V\rangle)$), $b' = c = \sigma_x$, and $b = c' = \sigma_y$. The maximum violation allowed by quantum mechanics is $S_{Sv} = 4\sqrt{2}$. Figure 3B shows the correlations calculated from 2348 four-fold events leading to $S_{Sv} = 4.88 \pm 0.13$, which is a violation by 7 standard deviations.

An application of the quantum Fredkin gate is the direct estimation of non-linear functionals (13) of a quantum state, described by a density matrix ρ , without recourse to QST. Here $\rho = \varrho_{T1} \otimes \varrho_{T2}$ is the density matrix of two separable subsystems. The circuit we employ is shown in Fig. 4A, where an interferometer is formed using two Hadamard gates and a variable phase shift $\theta(\vartheta)$. This interferometer is coupled to the controlled-SWAP operation of our quantum Fredkin gate such that measuring the control in the logical basis leads to an interference pattern given by $\text{Tr}[U_{SWAP}\varrho_{T1} \otimes \varrho_{T2}] = \text{Tr}[\varrho_{T1}\varrho_{T2}] = ve^{i\theta(\vartheta)}$. If $\varrho_{T1} \neq \varrho_{T2}$ then measurement of the fringe visibility provides, for pure states, a direct measure of the state overlap $|\langle T1|T2 \rangle|^2$, where $\varrho_{T1} = |T1\rangle\langle T1|$ and $\varrho_{T2} = |T2\rangle\langle T2|$. Conversely, if $\varrho_{T1} = \varrho_{T2}$ then the fringe visibility provides an estimate of the length of the Bloch vector (that is, the purity $P = \text{Tr}[\varrho^2]$). We realise the Hadamard operations in Fig. 4A by setting the quarter wave plate (QWP) and HWP combinations to prepare or measure σ_x .

Figure 4B shows the results of preparing the target qubits in the states $|0\rangle^{T1}|0\rangle^{T2}$, $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)^{T1}|0\rangle^{T2}$, and $|0\rangle^{T1}|1\rangle^{T2}$, corresponding to ideal (measured) overlaps and visibilities of 1 (0.82 ± 0.02), 0.5 (0.52 ± 0.02), and 0 (0.05 ± 0.01), respectively. Although the maximum visibility we are able to measure is limited by the performance of the three interferometers in the circuit, our measurements show a clear reduction in visibility as the single qubit states are made orthogonal. Figure 4C shows the result of setting $\varrho_{T1} = \varrho_{T2}$. As we increase the degree of mixture (see Materials and Methods), we observe a reduction in visibility from 0.82 ± 0.02 for a pure state to 0.03 ± 0.02 for a maximally mixed state.

Discussion

In conclusion, we have used linear optics to perform the first demonstration of the quantum Fredkin gate. This is achieved by

exploiting path-mode entanglement to add control to the SWAP operation. Our implementation has an improved success rate of more than one order of magnitude compared to previous proposals and does not require ancilla photons or decomposition into two-qubit gates. Our gate performs with high accuracy in the logical basis and operates coherently on superposition states. We have used the gate to generate genuine tripartite entanglement with the highest fidelities to date for photonic GHZ states and have implemented a small-scale algorithm to characterise quantum states without QST.

An alternative method for generating the polarisation-path entanglement that drives the gate is the use of C-path gates (23) at the input. Our implementation varies from a fully heralded quantum Fredkin gate (see Materials and Methods), which does not require preexisting entanglement; however it demonstrates the key properties of a quantum Fredkin gate. For completely general quantum circuits that incorporate Fredkin (or similar controlled-arbitrary-unitary) gates at arbitrary circuit locations, the C-path methodology may be necessary at the cost of some additional resources and success probability (see Materials and Methods), though we conjecture that specific circuits comprising multiple Fredkin gates might be optimised using similar techniques to those that allow us to simplify the Fredkin down from a circuit of five two-qubit gates. Nevertheless, for small algorithms or operations and whenever possible, it is significantly favourable to directly generate path entanglement.

The quantum Fredkin gate has many applications across quantum information processing. Our demonstration should stimulate the design and implementation of even more complex quantum logic circuits. Later we became aware of related work carried out by Takeuchi (31).

Materials and Methods

Source

Our source consisted of a 150 fs pulsed Ti-Sapphire laser operating at a rate of 80 MHz and at a wavelength of 780 nm, which was frequency doubled using a 2 mm LBO crystal. Two dispersion-compensating ultrafast prisms spatially filter any residual 780 nm laser light. The frequency-doubled light (with power 100 mW) pumped two 2 mm type-II β barium borate (BBO) crystals in succession. Entangled photons, generated via SPDC, were collected at the intersection of each set of emission cones. They then encountered an HWP with its OA at 45° and an additional 1 mm type-II BBO crystal used to compensate for spatial and temporal walk-offs. The single photons were coupled into single-mode fiber and delivered to the gate. This configuration gave, on average, a four-fold coincidence rate of 2.2 per minute at the output of the gate.

Entangled state preparation

Each SPDC source emitted pairs of entangled photons of the form $|\psi_1^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_{1B}|V\rangle_{2B} + |V\rangle_{1R}|H\rangle_{2R})$ and $|\psi_2^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_{1Y}|V\rangle_{2Y} + |V\rangle_{1G}|H\rangle_{2G})$. Polarisation optics were used to distribute the path-modes throughout the circuit and thus convert this state into the path-entangled states $|\psi_1^+\rangle =$

$\frac{1}{\sqrt{2}}(|1\rangle_{1B}|1\rangle_{2B}|0\rangle_{1R}|0\rangle_{2R} + |0\rangle_{1B}|0\rangle_{2B}|1\rangle_{1R}|1\rangle_{2R})$ and $|\psi_2^+\rangle = \frac{1}{\sqrt{2}}(|1\rangle_{1Y}|1\rangle_{2Y}|0\rangle_{1G}|0\rangle_{2G} + |0\rangle_{1Y}|0\rangle_{2Y}|1\rangle_{1G}|1\rangle_{2G})$. Path modes from $|\psi_1^+\rangle$ and $|\psi_2^+\rangle$ were combined on a PBS (Fig 1C, PBS with outputs $2R$, $1G$, $1Y$, and $2B$); along with post-selection of four-fold coincidence events at the outputs of the control, target, and trigger outputs, this led to Eq. (1) in the main text. Each qubit was encoded using photon polarisation: using Eq. (1), considering that each photon exists in a superposition of path-modes and omitting the unoccupied modes, an arbitrary polarisation state can be encoded onto each qubit by performing a local unitary operation on each mode, giving equation (2). The state encoding was performed inside the beam displacer (control qubit) and displaced Sagnac (target qubits) interferometers.

Tuning the phase

The phase was tuned by tilting an HWP set to its OA. To set the correct phase for each of the four GHZ states, we varied the tilt of the HWP and measured fringes in the four-fold coincidences with our measurement apparatus in the $\sigma_x\sigma_y\sigma_y$ basis. For the $|GHZ_{1,2}^+\rangle$ ($|GHZ_{1,2}^-\rangle$) we set the tilt to maximise (minimise) the occurrence of the $|DRR\rangle$, $|DLL\rangle$, $|ARL\rangle$, and $|ALR\rangle$ events.

Mixed state preparation

The mixed states of the form $\varrho = m|0\rangle\langle 0| + \frac{(1-m)}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$ were obtained by measuring output statistics for a combination of pure input states. The input states of the target were prepared, in varying proportions given by the parameter m , as $0.25(1+m)^2|0\rangle^{T1}|0\rangle^{T2}$, $0.25(1-m^2)|0\rangle^{T1}|1\rangle^{T2}$, $0.25(1-m^2)|1\rangle^{T1}|0\rangle^{T2}$, and $0.25(1-m)^2|1\rangle^{T1}|1\rangle^{T2}$. The aggregated data resulted in a fringe pattern which reflects the purity of the mixed single-qubit state.

Erasing the which-path information

Generation of path-mode entanglement and successful operation of the gate in the quantum regime relied on the erasure of the which-path information in the two displaced Sagnac interferometers. We tested this by performing a Hong-Ou-Mandel (HOM) two-photon interference measurement after each interferometer. After overlapping path modes $2R$ and $1G$ on an NPBS, an HWP with its OA set to 22.5° rotated the polarisation of the photons to $|D\rangle$ and $|A\rangle$, respectively. Sending these photons into the same port of a PBS led to bunching at the output if the path-modes were indistinguishable. Doing the same for modes $2B$ and $1Y$ gave two separate HOM dips (see Materials and Methods) with visibilities of $90 \pm 5\%$ and $91 \pm 6\%$.

Heralding the quantum Fredkin gate

In order to use a quantum Fredkin gate as part of a much larger quantum circuit (with gates in series), it is preferable for the gate to be heralded. Realising our gate in this manner involves adding C-path gates (23) to each input. For the best probability of success $P_{success}$, each C-path gate requires two heralded C-NOT gates (32) which, in turn, require two entangled pair ancillae. Execution of the C-path gate succeeds with $P_{success} = (1/4)^2$

(23, 32). C-path gates are not a necessity at the output if successful execution is heralded by non-detections at the relevant NPBS ports, at an additional probability cost of factor $1/4$.

References

1. P. Kok, K. Nemoto, T. C. Ralph, J. P. Dowling, G. J. Milburn, Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79**, 135-174 (2007).
2. J. L. O'Brien, A. Furusawa, J. Vuckovic, Photonic quantum technologies. *Nature Photon.* **3**, 687-695 (2009).
3. T. D. Ladd, *et al.*, Quantum computers. *Nature* **464**, 45-53 (2010).
4. J. A. Smolin, D. P. DiVincenzo, Five two-bit quantum gates are sufficient to implement the quantum Fredkin gate. *Phys. Rev. A.* **53**, 2855-2856 (1996).
5. L. M. K. Vandersypen, *et al.*, Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883-887 (2001).
6. E. Martin-Lopez, *et al.*, Experimental realization of Shor's quantum factoring algorithm using qubit recycling. *Nature Photon.* **6**, 773-776 (2012).
7. B. Lanyon, *et al.*, Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement. *Phys. Rev. Lett.* **99**, 250505 (2007).
8. I. L. Chuang, Y. Yamamoto, Quantum bit regeneration. *Phys. Rev. Lett.* **76**, 4281-4284 (1996).
9. A. Barenco, *et al.*, Stabilisation of Quantum Computations by Symmetrisation. *SIAM J. Comput.* **25**, 1541 – 1557 (1997).
10. H. Buhrman, R. Cleve, J. Watrous, R. de Wolf, Quantum Fingerprinting. *Phys. Rev. Lett.* **87**, 167902 (2001).
11. R. Horn, S. Babichev, K.-P. Marzlin, A. Lvovsky, B. Sanders, Single-Qubit Optical Quantum Fingerprinting. *Phys. Rev. Lett.* **95**, 150502 (2005).
12. D. Gottesman, I. Chuang, Quantum digital signatures. *arXiv:quant-ph/0105032* (2001).
13. A. Ekert, *et al.*, Direct Estimations of Linear and Nonlinear Functionals of a Quantum State. *Phys. Rev. Lett.* **88**, 217901 (2002).
14. J. Fiurášek, M. Dušek, R. Filip, Universal Measurement Apparatus Controlled by Quantum Software. *Phys. Rev. Lett.* **89**, 190401 (2002).
15. E. Fredkin, T. Toffoli, Conservative Logic. *International Journal of Theoretical Physics* **21**, 219-253 (1982).
16. G. J. Milburn, Quantum Optical Fredkin Gate. *Phys. Rev. Lett.* **62**, 2124-2127 (1989).

17. H. Chau, F. Wilczek, Simple Realization of the Fredkin Gate using a Series of Two-Body Operators. *Phys. Rev. Lett.* **75**, 748-750 (1995).
18. J. Fiurasek, Linear-optics quantum Toffoli and Fredkin gates. *Phys. Rev. A.* **73**, 062313 (2006).
19. J. Fiurasek, Linear optical Fredkin gate based on partial-SWAP gate. *Phys. Rev. A.* **78**, 032317 (2008).
20. Y. X. Gong, G. C. Guo, T. C. Ralph, Methods for a linear optical quantum Fredkin gate. *Phys. Rev. A.* **78**, 012305 (2008).
21. J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, D. Banning, Demonstration of an all-optical quantum controlled-NOT gate. *Nature* **426**, 264-267 (2003).
22. M. A. Pooley, *et al.*, Controlled-NOT gate operating with single photons. *Appl. Phys. Lett.* **100**, 211103 (2012).
23. X. Q. Zhou, *et al.*, Adding control to arbitrary unknown quantum operations. *Nature Commun.* **2** (2011).
24. M. Araújo, A. Feix, F. Costa, v. Brukner, Quantum circuits cannot control unknown operations. *New J. Phys.* **16**, 093026 (2014).
25. J. Thompson, M. Gu, K. Modi, V. Vedral, Quantum computing with black-box subroutines. *arXiv:1310.2927v5* (2013).
26. D. R. Hamel, *et al.*, Direct generation of three-photon polarization entanglement. *Nature Photon.* **8**, 801–807 (2014).
27. J. W. Pan, D. Bouwmeester, M. Daniell, H. Weinfurter, A. Zeilinger, Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. *Nature* **403**, 515-519 (2000).
28. N. D. Mermin, Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.* **65**, 1838-1840 (1990).
29. G. Svetlichny, Distinguishing three-body from two-body nonseparability by a Bell-type inequality. *Phys. Rev. D.* **35**, 3066-3069 (1987).
30. J. Lavoie, R. Kaltenbaek, K. J. Resch, Experimental violation of Svetlichny's inequality. *New J. Phys.* **11**, 073051 (2009).
31. S. Takeuchi. Private communication.
32. T. B. Pittman, B. C. Jacobs, J. D. Franson, Probabilistic quantum logic operations using polarizing beam splitters. *Phys. Rev. A* **64**, 062311 (2001).

Acknowledgements:

We thank Sergei Slussarenko, Allen Boston, and Kavan Modi for useful discussions.

Funding: This work was supported by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Project number CE110001027).

Author Contributions T.C.R., F.F., and G.J.P. conceptualised the scheme. R.B.P., J.H., and F.F. designed and constructed the experiment. R.B.P. and J.H. performed the experiment and data analysis with input from G.J.P. R.B.P. wrote the manuscript with input from all authors. G.J.P. oversaw the work.

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

Data and materials availability: All data needed to evaluate the conclusions in the paper are present in the paper itself and in the Supplementary Materials or are available upon request from the authors.

Supplementary Materials:

Section S1. Erasing the which-path information
 Section S2. Generation of three-photon GHZ states
 Fig. S1. HOM dip measurements

S1. Erasing the which-path information

Generation of path-mode entanglement, and successful operation of the gate in the quantum regime, relies on the erasure of the which-path information in the two displaced Sagnac interferometers. We test this by performing a Hong-Ou-Mandel (HOM) two-photon interference measurement after each interferometer. After overlapping path modes $2R$ and $1G$ on an NPBS a HWP with its OA set to 22.5° rotates the polarisation of the photons to $|D\rangle$ and $|A\rangle$, respectively. Sending these photons into the same port of a PBS leads to bunching at the output if the path-modes are indistinguishable. Doing the same for modes $2B$ and $1Y$ gives two separate HOM dips with visibilities $90\pm5\%$ and $91\pm6\%$. In the main article, the HOM dips were measured simultaneously for each displaced Sagnac interferometer where path modes $2R$ and $1G$, and $2B$ and $1Y$ are overlapped on a non-polarising beamsplitter (NPBS). The temporal delay in arrival times of the photons was varied by scanning the position of the input coupler for path modes $1G$ and $1Y$. The variation in accumulated four-fold events as a function of temporal delay results in a dip with a visibility defined as $V = (C_{max} - C_{min})/C_{max}$, where C_{max} and C_{min} are the maximum and minimum number of four-fold events, respectively. In Fig S1 we measure $V=90\pm5\%$ for modes $2R$ and $1G$ and $V=91\pm6\%$ for modes $2B$ and $1Y$, confirming a high degree of indistinguishability.

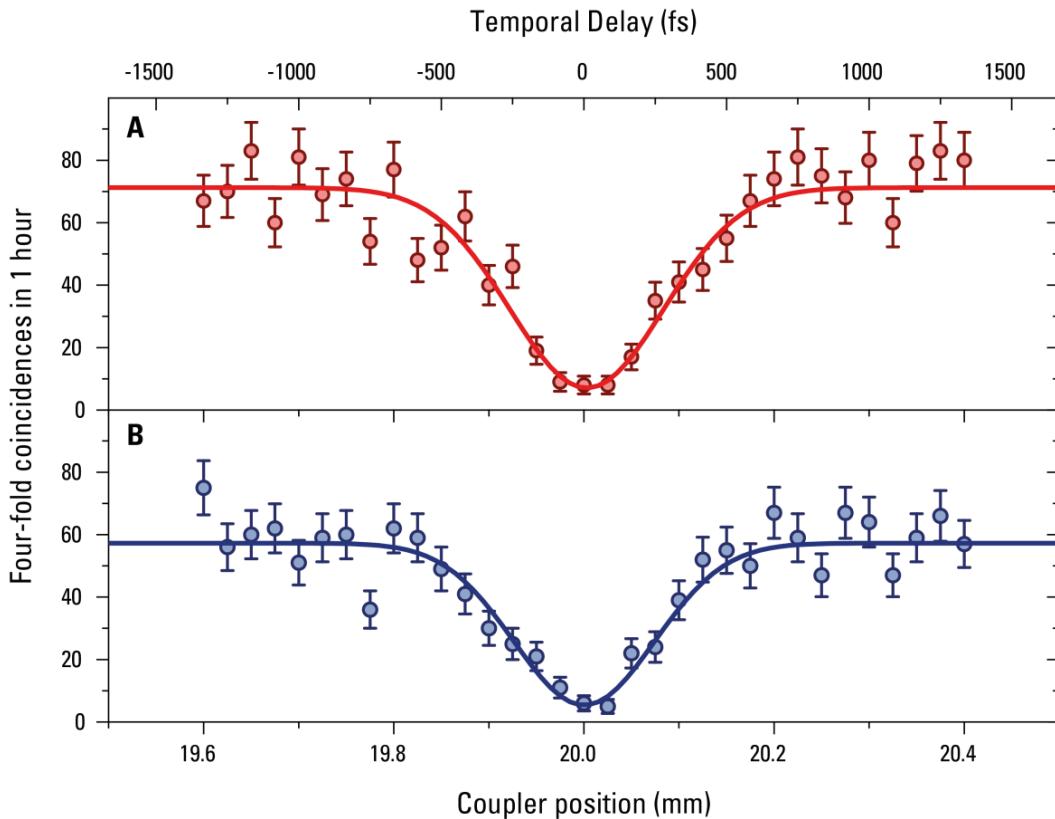


Fig. S1. HOM dip measurements testing the indistinguishability of path-modes after each displaced Sagnac interferometer. (A), Overlap of $2R$ and $1G$ with $V=90\pm5\%$, and (B), overlap of $2B$ and $1Y$ with $V=91\pm6\%$.

S2. Generation of three-photon GHZ states

Here we outline how our quantum Fredkin gate generates four of the eight maximally entangled three-photon GHZ states. The general four-photon state prior to state preparation is

$$\left(\left| \xi \right\rangle_{1B}^C \left| \psi \right\rangle_{2B}^{T1} \left| \phi \right\rangle_{1G}^{T2} \left| H \right\rangle_{2G}^{Tr} + \left| \xi \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| V \right\rangle_{2Y}^{Tr} \right) / \sqrt{2} \quad (\text{S1})$$

The photons in modes $2G$ and $2Y$ pass through a HWP with its OA set to 22.5° and then impinge on a PBS leading to

$$\begin{aligned} & \frac{\left| \xi \right\rangle_{1B}^C \left| \psi \right\rangle_{2B}^{T1} \left| \phi \right\rangle_{1G}^{T2} \left| H \right\rangle_{2G}^{Tr}}{\sqrt{4}} + \frac{\left| \xi \right\rangle_{1B}^C \left| \psi \right\rangle_{2B}^{T1} \left| \phi \right\rangle_{1G}^{T2} \left| V \right\rangle_{2G}^{Tr}}{+} \\ & \frac{\left| \xi \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| H \right\rangle_{2Y}^{Tr}}{\sqrt{4}} - \frac{\left| \xi \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| V \right\rangle_{2Y}^{Tr}}{\sqrt{4}} \end{aligned} \quad (\text{S2})$$

In order to prepare the gate in a superposition of the SWAP and identity operations the control qubit is set to $\left| D \right\rangle^C = \frac{1}{\sqrt{2}} \left(\left| H \right\rangle^C + \left| V \right\rangle^C \right)$ giving

$$\begin{aligned} & \frac{\left| H \right\rangle_{1B}^C \left| \psi \right\rangle_{2B}^{T1} \left| \phi \right\rangle_{1G}^{T2} \left| H \right\rangle_{2G}^{Tr}}{\sqrt{8}} + \frac{\left| V \right\rangle_{1B}^C \left| \psi \right\rangle_{2B}^{T1} \left| \phi \right\rangle_{1G}^{T2} \left| H \right\rangle_{2G}^{Tr}}{\sqrt{8}} \\ & + \frac{\left| H \right\rangle_{1B}^C \left| \psi \right\rangle_{2B}^{T1} \left| \phi \right\rangle_{1G}^{T2} \left| V \right\rangle_{2G}^{Tr}}{\sqrt{8}} + \frac{\left| V \right\rangle_{1B}^C \left| \psi \right\rangle_{2B}^{T1} \left| \phi \right\rangle_{1G}^{T2} \left| V \right\rangle_{2G}^{Tr}}{\sqrt{8}} \\ & + \frac{\left| H \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| H \right\rangle_{2Y}^{Tr}}{\sqrt{8}} + \frac{\left| V \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| H \right\rangle_{2Y}^{Tr}}{\sqrt{8}} \\ & - \frac{\left| H \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| V \right\rangle_{2Y}^{Tr}}{\sqrt{8}} - \frac{\left| V \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| V \right\rangle_{2Y}^{Tr}}{\sqrt{8}} \end{aligned} \quad (\text{S3})$$

In the control arm of our experiment, the interferometer is arranged such that terms with $\left| H \right\rangle_{1B}^C$ or $\left| V \right\rangle_{1R}^C$ in equation (S3) are rejected. Rejecting these terms and swapping modes $2B$ and $1G$ gives

$$\begin{aligned} & \frac{\left| H \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| H \right\rangle_{2Y}^{Tr}}{\sqrt{4}} + \frac{\left| V \right\rangle_{1B}^C \left| \phi \right\rangle_{1G}^{T1} \left| \psi \right\rangle_{2B}^{T2} \left| H \right\rangle_{2G}^{Tr}}{\sqrt{4}} \\ & - \frac{\left| H \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2} \left| V \right\rangle_{2Y}^{Tr}}{\sqrt{4}} + \frac{\left| V \right\rangle_{1B}^C \left| \phi \right\rangle_{1G}^{T1} \left| \psi \right\rangle_{2B}^{T2} \left| V \right\rangle_{2G}^{Tr}}{\sqrt{4}} \end{aligned} \quad (\text{S4})$$

Consequently from equation (S4) detection of a trigger photon in state $\left| H \right\rangle$ or $\left| V \right\rangle$ will result in two states with a relative phase difference of π .

$$\left| H \right\rangle^{Tr} : \frac{\left| H \right\rangle_{1R}^C \left| \psi \right\rangle_{2R}^{T1} \left| \phi \right\rangle_{1Y}^{T2}}{\sqrt{2}} + \frac{\left| V \right\rangle_{1B}^C \left| \phi \right\rangle_{1G}^{T1} \left| \psi \right\rangle_{2B}^{T2}}{\sqrt{2}} \quad (\text{S5})$$

$$|V\rangle^{Tr} \cdot \frac{|H\rangle_{1R}^C |V\rangle_{2R}^{T1} |\varphi\rangle_{1Y}^{T2}}{\sqrt{4}} - \frac{|V\rangle_{1B}^C |\varphi\rangle_{1G}^{T1} |V\rangle_{2B}^{T2}}{\sqrt{2}} \quad (S6)$$

As we detect both polarisations of the trigger photon, it is necessary to perform a classical phase rotation to the coincidence data corresponding to the detection of $|V\rangle^{Tr}$. The two sets of coincidence data are then combined. After erasing the which-path information, setting $|\psi\rangle = |V\rangle$ and $|\varphi\rangle = |H\rangle$ and recalling that $|H\rangle = |1\rangle$ and $|V\rangle = |0\rangle$ we obtain the three-photon GHZ state

$$|GHZ_1^+\rangle = \frac{(|0\rangle^C |1\rangle^{T1} |0\rangle^{T2} + |1\rangle^C |0\rangle^{T1} |1\rangle^{T2})}{\sqrt{2}}. \quad (S7)$$

Alternatively, setting $|\psi\rangle = |H\rangle$ and $|\varphi\rangle = |V\rangle$ produces

$$|GHZ_2^+\rangle = \frac{(|0\rangle^C |0\rangle^{T1} |1\rangle^{T2} + |1\rangle^C |1\rangle^{T1} |0\rangle^{T2})}{\sqrt{2}}. \quad (S8)$$

Preparing the control in $|A\rangle^C = \frac{1}{\sqrt{2}}(|H\rangle^C - |V\rangle^C)$ and setting $|\psi\rangle = |V\rangle$ and $|\varphi\rangle = |H\rangle$ gives

$$|GHZ_1^-\rangle = \frac{(|0\rangle^C |1\rangle^{T1} |0\rangle^{T2} - |1\rangle^C |0\rangle^{T1} |1\rangle^{T2})}{\sqrt{2}} \quad (S9)$$

while for $|\psi\rangle = |H\rangle$ and $|\varphi\rangle = |V\rangle$

$$|GHZ_2^-\rangle = \frac{(|0\rangle^C |0\rangle^{T1} |1\rangle^{T2} - |1\rangle^C |1\rangle^{T1} |0\rangle^{T2})}{\sqrt{2}} \quad (S10)$$