

Calculating unknown eigenvalues with a quantum algorithm

Xiao-Qi Zhou¹, Pruet Kalasuwan^{1,2}, Timothy C. Ralph³ and Jeremy L. O'Brien^{1*}

A quantum algorithm solves computational tasks using fewer physical resources than the best-known classical algorithm. Of most interest are those for which an exponential reduction is achieved. The key example is the phase estimation algorithm, which provides the quantum speedup in Shor's factoring algorithm and quantum simulation algorithms. To date, fully quantum experiments of this type have demonstrated only the read-out stage of quantum algorithms, but not the steps in which input data is read in and processed to calculate the final quantum state. Indeed, knowing the answer beforehand was essential. We present a photonic demonstration of a full quantum algorithm—the iterative phase estimation algorithm (IPEA)—without knowing the answer in advance. This result suggests practical applications of the phase estimation algorithm, including quantum simulations and quantum metrology in the near term, and factoring in the long term.

Many quantum computations can be roughly broken down into two stages: read-in and processing of the input data; and processing and read-out of the solution. In the first phase, the initial data are read into a quantum register and processed with quantum gates, sometimes multiple times. This produces a quantum state in which the solution is encoded. In the second phase the quantum state may be subjected to further processing followed by measurement, producing a classical data string containing the solution. Even though quantum computers are currently limited to a small number of qubits, there is considerable interest in the small-scale demonstration of quantum algorithms, even if the size of the problems solved means that they remain easily tractable with classical techniques. Such demonstrations remain challenging, even for small numbers of qubits, as they typically require the sequential application of a large number of quantum gates¹. Note we are making a distinction here between quantum algorithms and direct quantum simulation (Supplementary Section S1).

In recent years there have been a number of elegant demonstrations of the read-out phase of Shor's factoring algorithm^{2–5} and a quantum chemistry simulation algorithm^{6–8}. In these demonstrations, quantum gates have been used to produce the quantum state corresponding to a particular solution of the algorithm. It was then shown that the corresponding solution could be read out with high fidelity from this state. However, in each case, the method for producing the quantum state explicitly required the solution to be already known from a classical calculation. That is, the solution was put into the quantum state by hand, before being read out through further processing and measurement. It is clearly important to go beyond this restriction and demonstrate both stages of a quantum algorithm.

Phase estimation algorithm

First, we briefly review the standard phase estimation algorithm¹. Given a unitary U and one of its eigenstates $|\psi\rangle$ that fulfil the equation

$$U|\psi\rangle = e^{i2\pi\varphi}|\psi\rangle \quad (1)$$

the task is to find what the corresponding eigenvalue is—in other words, find the value of φ . As shown in Fig. 1a, m ancillary qubits act as controls, where each qubit is prepared in $|0\rangle$, and the target is the given eigenstate $|\psi\rangle$. After applying a Hadamard gate to each of the control qubits, we obtain the state $|+\rangle^{\otimes m} \otimes |\psi\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. This state can also be represented as

$$\sum_{x=0}^{2^{m+1}-1} |x\rangle \otimes |\psi\rangle \quad (2)$$

A series of controlled-unitary gates are then applied on the state, as shown in Fig. 1a, and thus convert it to

$$\sum_{x=0}^{2^{m+1}-1} |x\rangle \otimes U^x |\psi\rangle = \left(\sum_{x=0}^{2^{m+1}-1} e^{i2\pi\varphi x} |x\rangle \right) \otimes |\psi\rangle \quad (3)$$

The target state is intact and all the information about φ is contained in the state of the control qubits. The m qubits of the control register then undergo an inverse quantum Fourier transform (QFT^{-1}), and the control qubits are converted to $|\tilde{\varphi}_1\rangle \otimes |\tilde{\varphi}_2\rangle \dots \otimes |\tilde{\varphi}_m\rangle$, where $\tilde{\varphi}_i$ ($1 \leq i \leq m$) is an estimated bit equal to 0 or 1. By measuring the control qubits in the computational basis, one obtains the values of $\tilde{\varphi}_1, \tilde{\varphi}_2 \dots \tilde{\varphi}_m$ and the estimated phase in binary expansion:

$$\tilde{\varphi} = 0.\tilde{\varphi}_1\tilde{\varphi}_2\dots\tilde{\varphi}_m \quad (4)$$

As the inverse quantum Fourier transform can be scalably realized in a semiclassical way⁹ where no entangling gates are needed, the circuit with m ancillary qubits in Fig. 1a can be simplified to an m -round iterative single ancillary qubit circuit. This simplified version is called the iterative phase estimation algorithm (IPEA)¹⁰. Figure 1b shows the IPEA at the k th iteration. At the end of this iteration, a measurement of the ancillary qubit in the computational basis is performed, yielding the result 0 or 1, which is the estimate of the k th bit of φ in the binary expansion. Note that in the IPEA

¹Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, Bristol BS8 1UB, UK, ²Department of Materials Science and Technology, Faculty of Science, Prince of Songkla University, Hat-Yai, Songkla 90112, Thailand, ³Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane 4072, Australia.

*e-mail: jeremy.obrien@bristol.ac.uk

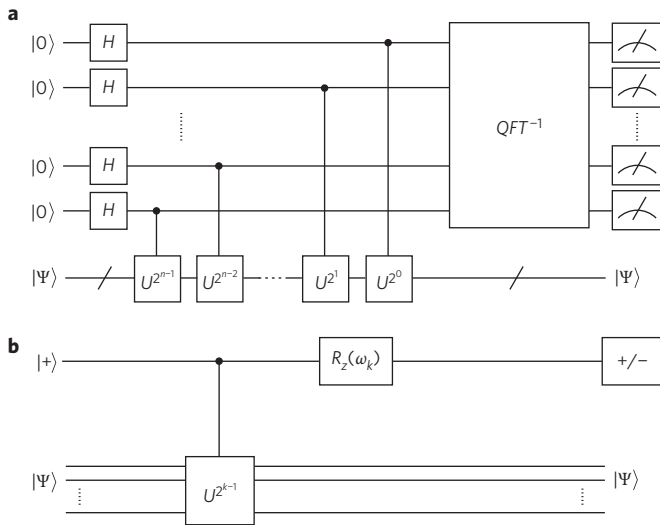


Figure 1 | The phase estimation algorithm. **a**, The standard quantum circuit for phase estimation, where H is the standard Hadamard gate and QFT^{-1} is the inverse quantum Fourier transform. The measurements are all implemented in computational basis. **b**, The k th iteration of the iterative phase estimation algorithm (IPEA). The algorithm is iterated m times to get an m -bit $\tilde{\varphi}$ (equation (4)), which is the approximation to the phase of the eigenstate φ (equation (1)). The measurement is implemented in $+/-$ basis, where $|+/-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Each iteration obtains one estimated bit $\tilde{\varphi}_k$; starting from the least significant ($\tilde{\varphi}_m$), k is iterated backwards from m to 1. The feedback angle ω_k depends on the previously measured bits as $\omega_k = -2\pi\xi_k$, where $\xi_k = 0.0\tilde{\varphi}_{k+1}\tilde{\varphi}_{k+2}\dots\tilde{\varphi}_m$ in binary expansion and $\omega_m = 0$.

scheme the least significant bits are evaluated first (that is, k is iterated backwards from m to 1) and the information obtained is used to improve the estimation of the more significant bits. This information transfer between iterations is realized via a single qubit rotation $R_z(\omega_k)$, whose angle is determined by all previously measured bits, as described in the caption of Fig. 1b.

In the case where the phase φ has exactly m bits in binary expansion, a perfect implementation of m iterations of the algorithm will deterministically extract the exact phase, which means $\tilde{\varphi} = \varphi$. When φ has a binary expansion of more than m bits, it has been proven that a perfect implementation of the algorithm achieves a precision of $\pm 2^{-m}$ with an error probability less than 19%, which is independent of m (ref. 10). This error can always be eliminated by simply repeating each IPEA iteration several times and choosing the most frequently observed result as the corresponding estimated bit. Note that this procedure is scalable.

Entanglement-based controlled unitary gates

From the description of the IPEA above, it is clear that implementing a sequence of controlled unitary gates is essential to this algorithm, where the unitaries are typically non-diagonal ones. Recently the IPEA was implemented⁶ using a simplified construction of controlled-unitary gates^{11,12}. However, the method of constructing the controlled-unitary gate in refs 11 and 12 is based on eigenvalue decomposition—decomposing the single-qubit unitary U to the product of $T, R_z(\alpha)$ and T^{-1} , where T and T^{-1} are two complementary unitary gates and $R_z(\alpha)$ is a phase-shift gate with α phase shift in the computational basis (Supplementary Section S2). For the application of the phase (eigenvalue) estimation of a unitary, this eigenvalue decomposition is of course unknown, otherwise the eigenvalue could be directly extracted from the eigenvalue decomposition.

Thus, to realize the phase estimation algorithm generally, control qubits should be added to the unitary without already knowing

the eigenvalue decomposition of the unitary. To circumvent this problem, we access a higher-dimensional Hilbert space to build the required controlled-unitary gates¹³ to construct the IPEA. As shown in Fig. 2a, the initial state is $\frac{1}{\sqrt{2}}(|H\rangle \otimes |\psi\rangle_r + |V\rangle \otimes |\psi\rangle_b)$, where $|H\rangle$ and $|V\rangle$ denote horizontal and vertical polarization respectively, $|\psi\rangle$ denotes the given (eigen)state encoded in n polarization qubits, and r and b denote the red and blue spatial modes respectively.

The blue modes of the target pass through the unitary $U^{2^{k-1}}$ and thus the state is converted to

$$\frac{1}{\sqrt{2}}(|H\rangle \otimes |\psi\rangle_r + |V\rangle \otimes U^{2^{k-1}}|\psi\rangle_b) \quad (5)$$

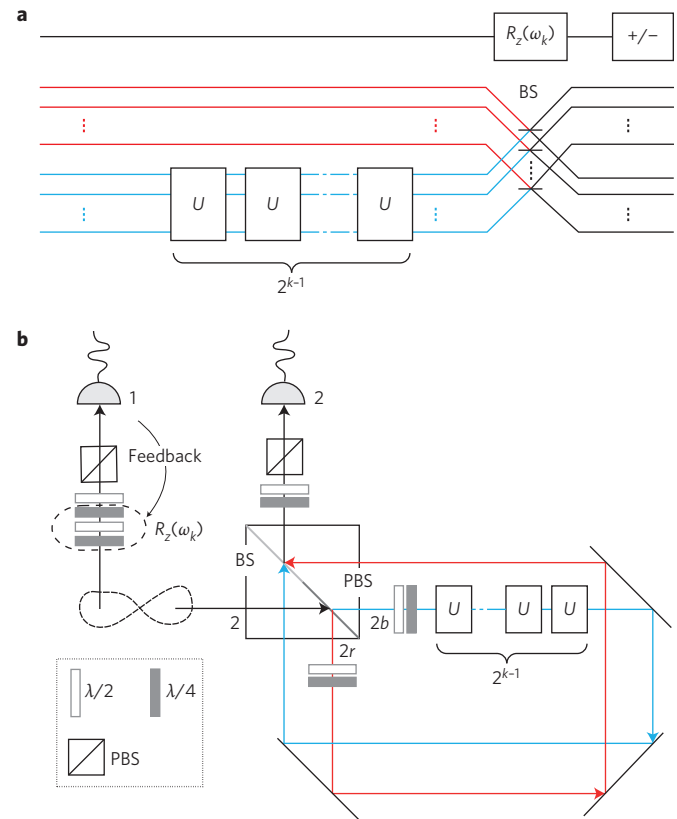


Figure 2 | Optical implementation of the phase estimation algorithm.

a, Simplified entanglement-based circuit for $C-U^{2^{k-1}}$ gate. The initial input state is $\frac{1}{\sqrt{2}}(|H\rangle \otimes |\psi\rangle_r + |V\rangle \otimes |\psi\rangle_b)$, where $|\psi\rangle$ is a multi-qubit polarization-encoded state and red r and blue b denote different spatial modes of the photons. After the blue mode passes through the unitary gate $U^{2^{k-1}}$, which is realized by cascading 2^{k-1} copies of U , the red and blue modes of each target qubit are mixed on beamsplitters (BS). By retaining the case where an even number of target photons arrives in lower spatial modes, $C-U^{2^{k-1}}$ is realized for the input state $|+\rangle \oplus |\psi\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$. The rotation $R_z(\omega_k)$ and the measurement in $+/-$ basis are then used to extract $\tilde{\varphi}_k$ —the estimate of the k th bit of the phase φ . **b**, Experimental set-up for the k th iteration of the two-qubit iterative phase estimation algorithm (IPEA). A 60 mW continuous-wave laser beam with a central wavelength of 404 nm is focused onto a type-II BBO crystal to create the polarization entangled photon pairs. The PBS part of the BS/PBS cube and the following waveplates convert the two photons to the desired polarization-spatial entangled state (equation (7)). Based on this state, the $C-U^{2^{k-1}}$ gate is effectively realized, where U is the unitary whose eigenvalue is to be estimated. The rotation gate $R_z(\omega_k)$ (for the value of ω_k , see the caption of Fig. 1b) is implemented by three waveplates—two quarter-waveplates with a HWP in between. The displaced-Sagnac structure makes the phase between modes $2r$ and $2b$ inherently stable.

The red and blue modes of each target qubit are then mixed on non-polarizing beamsplitters (BS) to remove the path information and the state is now changed to

$$\sum_{p \in P} \frac{1}{\sqrt{2^{n+1}}} (|H\rangle \otimes |\psi\rangle_p + |V\rangle \otimes U^{2^{k-1}} |\psi\rangle_p) + \sum_{q \in Q} \frac{1}{\sqrt{2^{n+1}}} (|H\rangle \otimes |\psi\rangle_q - |V\rangle \otimes U^{2^{k-1}} |\psi\rangle_q) \quad (6)$$

where P (Q) denotes the cases where an even (odd) number of target photons arrive in the lower spatial modes. By retaining any case in P , the desired state $\frac{1}{\sqrt{2}}(|H\rangle \otimes |\psi\rangle + |V\rangle \otimes U^{2^{k-1}} |\psi\rangle)$ is obtained with a $(1/2)^n$ probability of success. There are 2^{n-1} such cases in P where the total probability of success is $1/2$, regardless of the size of the unitary gate U . Here $U^{2^{k-1}}$ is implemented by simply placing 2^{k-1} copies of the unitary U into the path of the blue mode ($U^{2^{k-1}}$ could alternatively be realized by 2^{k-1} passes through U ; ref. 14). Finally, to finish the iteration, the first qubit passes through the rotation $R_z(\omega_k)$ and is measured in $+/-$ basis to extract $\tilde{\varphi}_k$ —the estimate k th bit of the phase φ . There is another $1/2$ probability that one of the cases in Q occurs, which means the state $\frac{1}{\sqrt{2}}(|H\rangle \otimes |\psi\rangle - |V\rangle \otimes U^{2^{k-1}} |\psi\rangle)$ is obtained. Using the same procedures will extract the same $\tilde{\varphi}_k$ as long as the measurement result of $+(-)$ is redefined as $1(0)$. In this way, the circuit shown in Fig. 2a can be used to implement the IPEA deterministically—that is, with probability 1. Note that no information about the unitary U needs to be known at all for implementing the above circuits.

Experimental demonstration

By using the entanglement-based controlled-unitary gates described above, we implement the IPEA without having to already know the value of the phase φ —that is, without already knowing the answer to the algorithm. The experimental set-up is shown in Fig. 2b. A 60 mW 404 nm continuous-wave laser is focused on a barium borate (BBO) crystal cut for type-II spontaneous parametric down-conversion (SPDC) to create a two-photon polarization-entangled state $\frac{1}{\sqrt{2}}(|H\rangle_1 \otimes |V\rangle_2 + |V\rangle_1 \otimes |H\rangle_2)$, where 1 and 2 denote the control and target photons, respectively. A special beamsplitter cube, which on one half is a non-polarizing beamsplitter (BS) and the other half is polarizing beamsplitter (PBS)¹⁵, is used as shown to build a displaced-Sagnac structure to increase the inherent phase stability of the setup. Photon 2 passes through the PBS part of the BS/PBS cube and thus the two-photon state is converted to $\frac{1}{\sqrt{2}}(|H\rangle_1 \otimes |V\rangle_{2r} + |V\rangle_1 \otimes |H\rangle_{2b})$. Waveplates are used in the path of $2r$ and $2b$ to prepare the required polarization-spatial entangled state

$$\frac{1}{\sqrt{2}}(|H\rangle_1 \otimes |\psi\rangle_{2r} + |V\rangle_1 \otimes |\psi\rangle_{2b}) \quad (7)$$

where $|\psi\rangle$ is the eigenstate of the target unitary U ; that is, $U|\psi\rangle = e^{i\varphi}|\psi\rangle$. Then, after the blue mode passes through the unitary $U^{2^{k-1}}$, the two modes of photon 2 are combined at the BS side of the BS/PBS cube (Fig. 2b). For experimental simplicity, we retain only the cases where photon 2 exits at port 2 and thus get the desired two-photon state $\frac{1}{\sqrt{2}}(|H\rangle_1 \otimes |\psi\rangle_2 + |V\rangle_1 \otimes U^{2^{k-1}} |\psi\rangle_2)$, which can be written as $\frac{1}{\sqrt{2}}(|H\rangle_1 + e^{i2\pi\varphi 2^{k-1}} |V\rangle_1) \otimes |\psi\rangle_2$. To finish the k th iteration, photon 1 passes through the $R_z(\omega_k)$ gate (ω_k is set to an angle determined by all previously measured bits; see Fig. 1b caption) and is then measured in the $+/-$ basis to obtain the k th bit of the estimated phase.

We implemented three iterations of the IPEA to estimate the value of the phase φ to three bits of precision. The unitaries U^4 , U^2 and U are used in the first, second and third iterations, and

U^4 and U^2 are realized by four and two consecutive U gates, respectively. The U gate is implemented by two consecutive half-waveplates (HWP). A convenient feature of this unitary is that $|R\rangle$ and $|L\rangle$ are always eigenstates, where $|R/L\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm i|V\rangle)$. This can be understood by considering the following fact: a HWP always converts the states $|R\rangle \leftrightarrow |L\rangle$ no matter what the angle of the HWP is. Two consecutive HWPs therefore leave $|R\rangle$ and $|L\rangle$ unchanged, up to a phase factor; that is, $|R\rangle$ and $|L\rangle$ are the eigenstates of this unitary U . We therefore choose $|R\rangle$ as the input eigenstate $|\psi\rangle$. We fixed the angle of the first HWP to 0° and changed the angle of the second HWP, θ , to various values to realize a number of different unitaries. For each of these unitaries, we get a 3-bit estimate of the phase $\tilde{\varphi}$ in binary expansion. The results are shown in Fig. 3. We see that φ is non-trivially related to θ ; that is, θ appears in a non-diagonal representation of U which must be diagonalized to extract φ ; in principle, a third party could prepare the waveplates without revealing θ , and the experimenter would still be able to successfully extract φ . There is no limitation on choosing unitaries to be estimated in this protocol. Here we chose unitaries composed of two consecutive HWPs because for these unitaries we know that $|R\rangle$ and $|L\rangle$ are eigenstates of the unitary, but the unitary itself and its eigenvalue are unknown (an alternative would be for a third party to provide both an unknown unitary and an eigenstate of it to us, and for us to then determine the eigenvalue). In this way, we can show the key feature of our scheme, that estimating the phase requires no knowledge of the unitary at all.

Eigenstate generator

It has been shown¹⁶ that the phase estimation algorithm still works even when the input target state is not the eigenstate of U (provided the iterations are coherent). Assume the input state is $\alpha|\psi_a\rangle + \beta|\psi_b\rangle$, where $|\psi_a\rangle$ and $|\psi_b\rangle$ are the eigenstates of U with distinctive eigenvalues $e^{2\pi\varphi_a}$ and $e^{2\pi\varphi_b}$, respectively. By passing the control and the target through the same circuit as shown in Fig. 1a, the state $\alpha|\tilde{\varphi}_a\rangle \otimes |\psi_a\rangle + \beta|\tilde{\varphi}_b\rangle \otimes |\psi_b\rangle$ would be obtained at the output, where $\tilde{\varphi}_a$ and $\tilde{\varphi}_b$ are the estimates of φ_a and φ_b , respectively. When the number of control qubits is sufficiently large to make $\tilde{\varphi}_a$ and $\tilde{\varphi}_b$ distinguishable, measuring the control qubits in the computational basis yields either $\tilde{\varphi}_a$, which means the estimated eigenvalue is $e^{2\pi\tilde{\varphi}_a}$ and the target state automatically collapses to the corresponding eigenstate $|\psi_a\rangle$, or $\tilde{\varphi}_b$, which means the estimated eigenvalue is $e^{2\pi\tilde{\varphi}_b}$ and the target state collapses to the state $|\psi_b\rangle$. In this way, the phase estimation circuit can be regarded as an eigenvalue measuring device or as an eigenstate generator.

We performed an experiment to show this eigenstate generation feature of the phase estimation algorithm. We used a similar experimental set-up, as shown in Fig. 2b. The U gate, whose eigenvalue is the target to be estimated, is implemented by a single HWP. Two HWPs oriented at the same angle realize an identity operator, which means $U^2 = I$. Based on this fact, one can deduce that, for $k \geq 2$, all the gates $C - U^{2^{k-1}}$ are equal to identity operators. No iterations are required and we implement the only non-trivial circuit $C - U$ (corresponds to $k = 1$). We set the initial target state to $|H\rangle$ and measure the control photon in the $+/-$ basis. When the result is $+$ or $-$, the target qubit collapses to the eigenstate of U with eigenvalue $+1$ or -1 , respectively. To evaluate this process, we perform state tomography on the output target state and compare the result with the theoretical prediction. The results are shown in Fig. 4a–f. The output target state, which is only determined by the measurement result of the control qubit, is not affected by changing the initial target state. We verify this feature by changing the initial target state to $|V\rangle$ and performing the state tomography on the output target state. The results are shown in Fig. 4g–i.

The non-unit fidelities observed above arise primarily due to two effects: the partial distinguishability of the photons generated in the

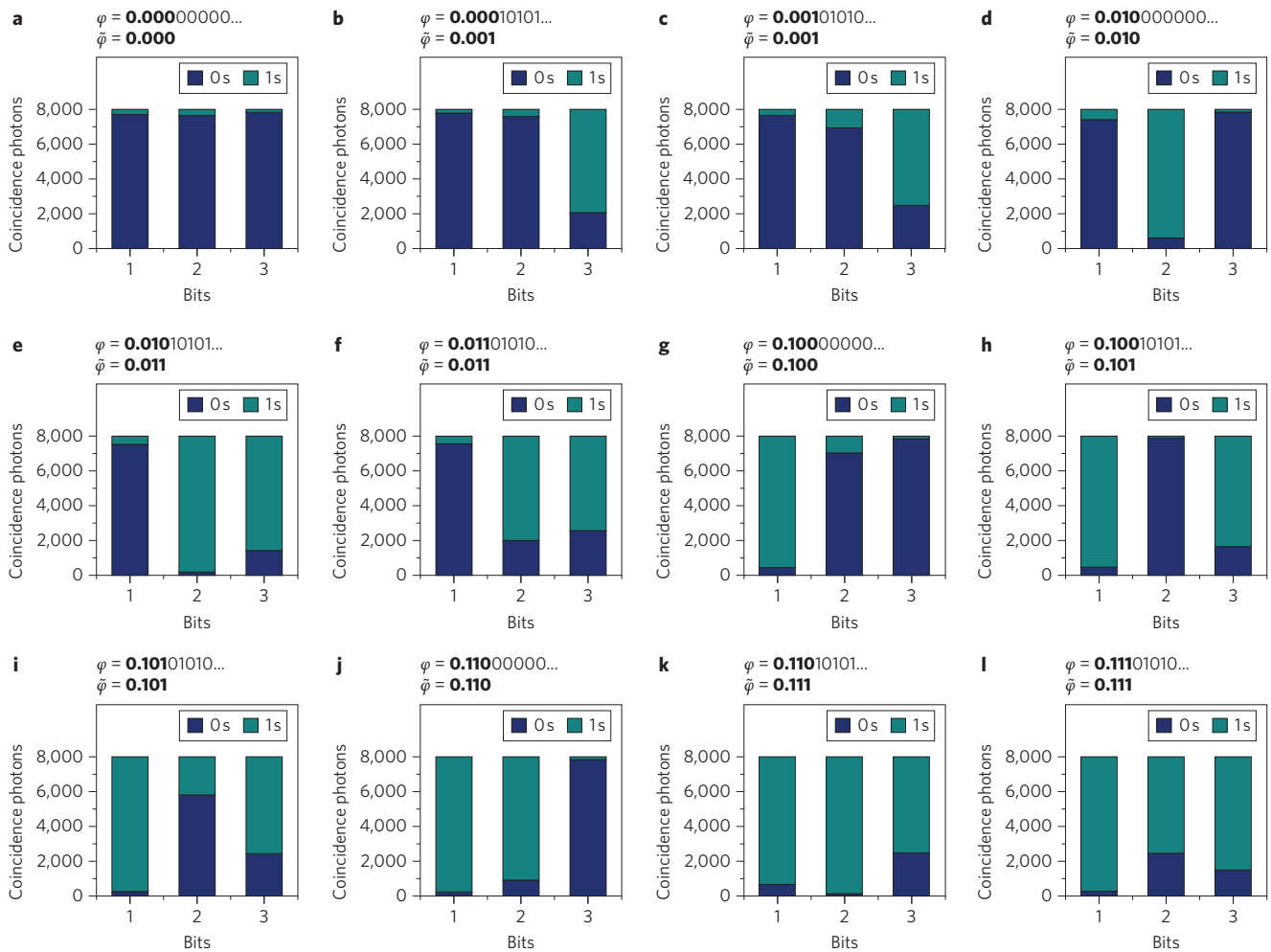


Figure 3 | Phase estimation data for 12 different U s. a–l, Each U is composed of two HWPs. The first is set to 0° , the second HWP is oriented at 0° (a), 15° (b), 30° (c), 45° (d), 60° (e), 75° (f), 90° (g), 105° (h), 120° (i), 135° (j), 150° (k) and 165° (l). For each U , three iterations of the algorithm are implemented and thus a three-digit estimated phase $\tilde{\varphi}$ is obtained. Compared with the phase φ the error in $\tilde{\varphi}$ is always less than 0.0001 in binary, which is consistent with theoretical prediction.

SPDC source, which results in some incoherent mixture, and the imperfect optical components, including the settings of waveplate angles. In the case of the eigenstate generation results (Fig. 4), the fidelities of the output states range from 84.83% to 98.96%, which is, in part, due to the varying overlap between the input state $|H\rangle$ and the output states. This results in a large difference in the output count rates. The total counts of the output are $\sim 600 \text{ s}^{-1}$ in Fig. 4a and $\sim 2,200 \text{ s}^{-1}$ in Fig. 4c, for example, and the error counts of the output are similar in both cases.

Discussion

Both the IPEA and eigenstate generation experiments shown above need sub-wavelength phase stability, which is realized here by using a displaced Sagnac loop interferometer. However, as the system size grows, it would become harder to maintain the phase stability with the bulk optics set-up. A straightforward solution would be to adopt the integrated photonics approach^{5,17–19} to implement this scheme, as the monolithic nature of integrated circuits inherently guarantees the phase stability. With the development of waveguide-based photon source technology^{20,21}, the entangled photon pairs can be directly generated inside the integrated circuits so as to avoid sending entangled photon pairs into the chip that can introduce phase instability in the interface.

In these two experiments, the given eigenstate is encoded in an initial entangled state. We note that the use of an entangled initial

state does not reduce the generality of the central result: implementing the phase estimation algorithm without any pre-knowledge about the unitary. It applies to any unitary and is scalable to a larger number of qubits. To perform the standard phase estimation algorithm on an unknown unitary where an eigenstate is given, it is not necessary to encode in a one-qubit state, and our implementation is valid and efficient. In other applications, by involving coherent interactions where the eigenstate is not given, such as Shor's algorithm, it is possible to use a single qubit encoded state using teleportation techniques and off-line entanglement to create the required initial entangled state, or the gate techniques described in ref. 13. We exploit particular properties of the unitary in the eigenstate generation experiment.

The ability to construct quantum algorithms without the need to know the answer in advance is clearly essential to their practical application. In the case of the phase estimation algorithm this requires that the controlled unitaries $C-U^{2^{k-1}}$ are realized without already knowing the eigenvalues of U . The approach demonstrated here achieves this efficiently and opens the way to practical applications of quantum simulation algorithms (for calculating molecular properties⁶ for example), and metrology applications¹⁴ for enhanced measurement precision, in the near term, and factoring in the long term. For Shor's factoring algorithm, coherent iterations are required²², which can be realized by employing the path entangling gates of ref. 13. Although current

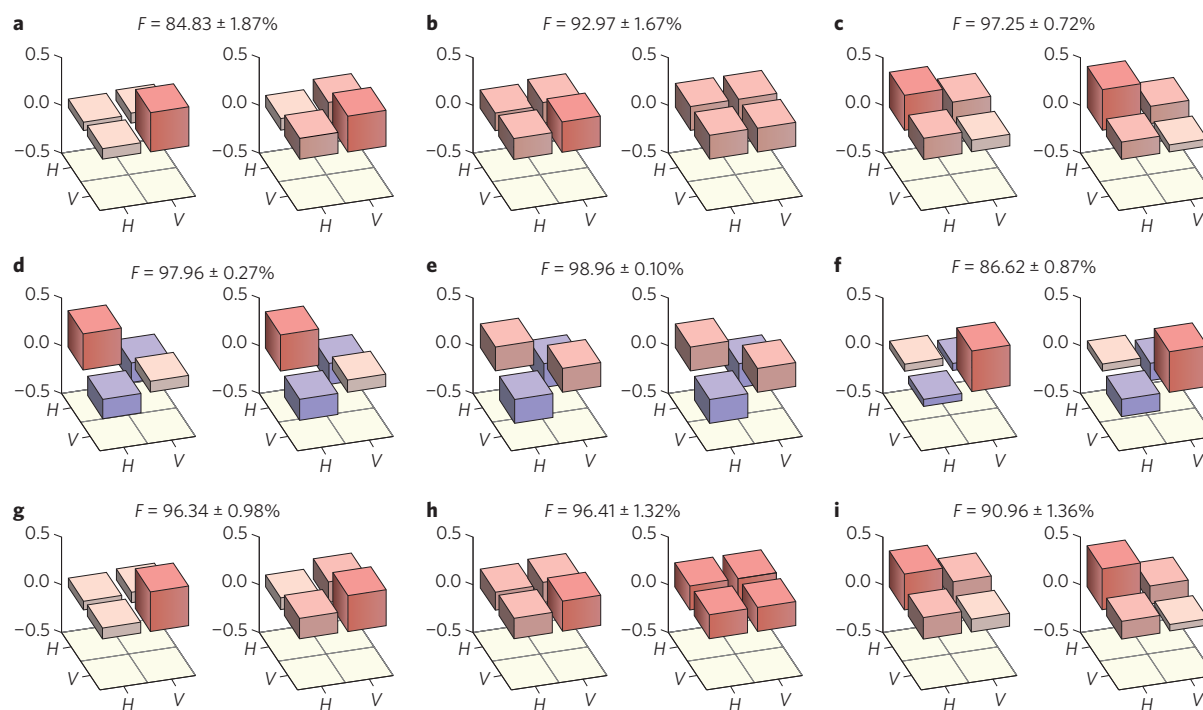


Figure 4 | Using the phase estimation algorithm to generate the eigenstates of U . **a–i**, The density matrix of the target output: (L) experimental, (R) ideal. Unitaries U_1 , U_2 and U_3 are implemented with a single HWP set to 30° , 45° and 67.5° , respectively. **a–c**, The case where the unitary is U_1 , U_2 , U_3 , the initial target state is $|H\rangle$ and the measurement outcome of the control qubit is 1. **d–f**, The case where the unitary is U_1 , U_2 , U_3 , the initial target state is $|H\rangle$ and the measurement result of the control qubit is 0. The output target state is determined only by the measurement result of the control qubit and not affected by changing the initial target state, as verified by the similarity between matrices **a** and **g**, **b** and **h**, **c** and **i**. State tomography and maximum-likelihood are used for the reconstruction of the density matrices. The fidelities of the reconstructed density matrices with the ideal case are shown. The error estimates are obtained by performing many reconstructions with random noise added to the raw data in each case.

single-photon source and detector efficiencies preclude scaling beyond an order of magnitude, rapid progress is being made in improving these efficiencies^{23,24}.

These technical issues aside, we note that the approach taken here is scalable. The IPEA is itself scalable, and the scheme of Fig. 2a works deterministically, provided U can be performed and the entangled input state can be prepared. The realization of controlled unitaries is scalable to multi-qubit unitaries and applicable to any physical implementation where a higher-dimensional Hilbert space is accessible, which typically is the case. Trapped-ion systems, for example, offer a large number of precisely controllable internal electronic and external vibrational degrees of freedom. For photons, path degrees of freedom, as used here, are ideal, and the required entangled input state can be efficiently prepared using the 'KLM'²⁵ or derivative approaches to linear optical quantum computing. For other architectures this entangled input may be directly prepared using deterministic entangling gates, and the BS operations (Fig. 2a) would correspond to single qudit operations.

Received 21 May 2012; accepted 20 December 2012;
published online 24 February 2013

References

- Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
- Vandersypen, L. M. K. *et al.* Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883–887 (2001).
- Lu, C.-Y., Browne, D. E., Yang, T., & Pan, J.-W. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.* **99**, 250504 (2007).
- Lanyon, B. P. *et al.* Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. *Phys. Rev. Lett.* **99**, 250505 (2007).
- Politi, A., Matthews, J. C. F. & O'Brien, J. L. Shor's quantum factoring algorithm on a photonic chip. *Science* **325**, 1221 (2009).
- Lanyon, B. P. *et al.* Towards quantum chemistry on a quantum computer. *Nature Chem.* **2**, 106–111 (2010).
- Du, J. *et al.* NMR implementation of a molecular hydrogen quantum simulation with adiabatic state preparation. *Phys. Rev. Lett.* **104**, 030502 (2010).
- Li, Z. *et al.* Solving quantum ground-state problems with nuclear magnetic resonance. *Sci. Rep.* **1**, 88 (2011).
- Griffiths, R. B. & Niu, C.-S. Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.* **76**, 3228–3231 (1996).
- Dobšiček, M., Johansson, G., Shumeiko, V., & Wendin, G. Arbitrary accuracy iterative quantum phase estimation algorithm using a single ancillary qubit: a two-qubit benchmark. *Phys. Rev. A* **76**, 030306 (2007).
- Ralph, T. C., Resch, K. J. & Gilchrist, A. Efficient Toffoli gates using qudits. *Phys. Rev. A* **75**, 022313 (2007).
- Lanyon, B. P. *et al.* Simplifying quantum logic using higher-dimensional Hilbert spaces. *Nature Phys.* **5**, 134–140 (2009).
- Zhou, X.-Q. *et al.* Adding control to arbitrary unknown quantum operations. *Nature Commun.* **2**, 413 (2011).
- Higgins, B. L., Berry, D. W., Bartlett, S. D., Wiseman, H. M. & Pryde, G. J. Entanglement-free Heisenberg-limited phase estimation. *Nature* **450**, 393–396 (2007).
- Gao, W. *et al.* Experimental demonstration of a hyper-entangled ten-qubit Schrödinger cat state. *Nature Phys.* **6**, 331–335 (2010).
- Abrams, D. S. & Lloyd, S. Quantum algorithm providing exponential speed increase for finding eigenvalues and eigenvectors. *Phys. Rev. Lett.* **83**, 5162–5165 (1999).
- Politi, A., Cryan, M. J., Rarity, J. G., Yu, S., & O'Brien, J. L. Silica-on-silicon waveguide quantum circuits. *Science* **320**, 646–649 (2008).
- Matthews, J. C. F., Politi, A., Stefanov, A., & O'Brien, J. L. Manipulation of multiphoton entanglement in waveguide quantum circuits. *Nature Photon.* **3**, 346–350 (2009).
- Shadbolt, P. *et al.* Generating, manipulating and measuring entanglement and mixture with a reconfigurable photonic circuit. *Nature Photon.* **6**, 45–49 (2011).

20. Lobino, M. *et al.* Correlated photon-pair generation in a periodically poled MgO doped stoichiometric lithium tantalate reverse proton exchanged waveguide. *Appl. Phys. Lett.* **99**, 081110 (2011).
21. Engin, E. *et al.* Photon pair generation in silicon microring resonator and enhancement via reverse bias. Preprint at <http://arXiv.org/abs/1204.4922> (2012).
22. Parker, S., & Plenio, M. B. Efficient factorization with a single pure qubit and $\log N$ mixed qubits. *Phys. Rev. Lett.* **85**, 3049–3052 (2000).
23. Shields, A. J. Semiconductor quantum light sources. *Nature Photon.* **1**, 215–223 (2007).
24. Hadfield, R. Single-photon detectors for optical quantum information applications. *Nature Photon.* **3**, 696–705 (2009).
25. Knill, E., Laflamme, R., & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46–52 (2001).

Acknowledgements

The authors thank P.J. Shadbolt for writing the quantum process tomography code and J.C.F. Matthews, A. Peruzzo, G.J. Pryde and P. Zhang for helpful discussions. This work was supported by the Engineering and Physical Sciences Research Council (EPSRC), the European Research Council (ERC), PHORBITECH, Quantum Interfaces, Sensors, and

Communication based on Entanglement (QESSENCE) and the Centre for Nanoscience and Quantum Information (NSQI). J.O'B. acknowledges a Royal Society Wolfson Merit Award.

Author contributions

The theory was developed by X.-Q.Z. and T.C.R. The theory was mapped to the experimental circuit by X.-Q.Z., P.K., T.C.R. and J.O.B. Experiments were performed by X.-Q.Z. and P.K. Data were analysed by X.-Q.Z., P.K., T.C.R. and J.O.B. The manuscript was written by X.-Q.Z., P.K., T.C.R. and J.O.B. The project was supervised by X.-Q.Z. and J.O.B.

Additional information

Supplementary information is available in the online version of the paper. Reprints and permissions information is available online at www.nature.com/reprints. Correspondence and requests for materials should be addressed to J.L.O.

Competing financial interests

The authors declare no competing financial interests.

Supplementary Information

Xiao-Qi Zhou,¹ Pruet Kalasuwan,¹ Timothy C. Ralph,² and Jeremy L. O'Brien¹

¹Centre for Quantum Photonics, H. H. Wills Physics Laboratory & Department of Electrical and Electronic Engineering, University of Bristol, BS8 1UB, United Kingdom

²Centre for Quantum Computation and Communication Technology, School of Mathematics and Physics, University of Queensland, Brisbane 4072, Australia

We provide here supplementary materials for our Article to explain the distinction between quantum algorithms and direct quantum simulations and the limitation of previous demonstrations of quantum algorithms.

Distinction between quantum algorithms and direct quantum simulations

There is a distinction between quantum algorithms and direct quantum simulations. In the latter case the aim is to mimic directly the time evolution of some quantum system of interest in the lab. There has been considerable progress in direct quantum simulation in recent years^{1–3}. In contrast, quantum algorithms, the subject of this paper, calculate specific mathematical properties - some of which can be useful for the mathematical simulation of physical systems.

Limitation of previous demonstrations of quantum algorithms

Refs 4–7 are demonstrations of Shor's factoring algorithm⁸ which is effectively the order-finding algorithm. However, all of them are compiled demonstrations, which means the unitaries are not the true modular exponentiation operations. Building these compiled unitaries needs the knowledge of the order of the modular exponentiation function which is already the solution of the Shor's algorithm. Refs 9–11 are demonstrations of Kitaev's phase estimation algorithm (PEA). As mentioned in the main text, the demonstration of IPEA in ref 9 requires the diagonalization of the unitary to be known from the outset—i.e. the eigenvalues are known (the answer is known) before one can implement the algorithm. The method used for implementing the controlled unitaries in refs 10 and 11 is only valid for a very special and symmetric Hamiltonian. This class of Hamiltonians has a symmetry that means that the sub-Hamiltonians commute—something that is not generally true—enabling separate applications, without the need for Trotterisation.

¹ Lanyon, B. *et al.* Universal digital quantum simulation with trapped ions. *Science* **334**, 57–61 (2011).

² Gerritsma, R. *et al.* Quantum simulation of the Klein paradox with trapped ions. *Phys. Rev. Lett.* **106**, 060503 (2011).

³ Islam, R. *et al.* Onset of a quantum phase transition with a trapped ion quantum simulator. *Nature Commun.* **2**, 377 (2011).

⁴ Vandersypen, L. M. K. *et al.* Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature* **414**, 883–887 (2001).

⁵ Lu, C.-Y., Browne, D. E., Yang, T. & Pan, J.-W. Demonstration of a compiled version of Shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.* **99**, 250504 (2007).

⁶ Lanyon, B. P. *et al.* Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. *Phys. Rev. Lett.* **99**, 250505 (2007).

⁷ Politi, A., Matthews, J. C. F. & O'Brien, J. L. Shor's Quantum Factoring Algorithm on a Photonic Chip. *Science* **325**, 1221 (2009).

⁸ Shor, P. W. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science* (ed. Goldwasser, S.) 124–134 (IEEE Computer Society Press, 1994).

⁹ Lanyon, B. P. *et al.* Towards quantum chemistry on a quantum computer. *Nature Chem.* **2**, 106–111 (2010).

¹⁰ Du, J. *et al.* NMR implementation of a molecular hydrogen quantum simulation with adiabatic state preparation. *Phys. Rev. Lett.* **104**, 030502 (2010).

¹¹ Li, Z. *et al.* Solving quantum ground-state problems with nuclear magnetic resonance. *Sci. Rep.* **1**, 88 (2011).