THE UNIVERSITY
OF QUEENSLAND
AUSTRALIA

Optical Quantum Information: New States, Gates and Algorithms

By

Benjamin Peter Lanyon
M.Phil., The University of Warwick
B.Sc.(Hons I), The University of Warwick

A thesis submitted for the degree of Doctor of Philosophy at
The University of Queensland in February 2009
School of Physical Sciences

Principal Advisor: *Prof. Andrew G. White*
Associate Advisors: *Dr. Marcelo P. Almeida, Dr. Marco Barbieri,* and
Assoc. Prof. Geoff J. Pryde.

Produced in LaTeX 2$_\varepsilon$.

Mandatory declaration by the author

This thesis is composed of my original work, and contains no material previously published or written by another person except where due reference has been made in the text. I have clearly stated the contribution by others to jointly-authored works that I have included in my thesis. I have clearly stated the contribution of others to my thesis as a whole, including statistical assistance, survey design, data analysis, significant technical procedures, professional editorial advice, and any other original research work used or reported in my thesis. The content of my thesis is the result of work I have carried out since the commencement of my research higher degree candidature and does not include a substantial part of work that has been submitted to qualify for the award of any other degree or diploma in any university or other tertiary institution. I have clearly stated which parts of my thesis, if any, have been submitted to qualify for another award. I acknowledge that an electronic copy of my thesis must be lodged with the University Library and, subject to the General Award Rules of The University of Queensland, immediately made available for research and study in accordance with the Copyright Act 1968. I acknowledge that copyright of all material contained in my thesis resides with the copyright holder(s) of that material.

Statement of contributions to jointly authored works contained in the thesis.
This thesis presents six jointly authored works that have been published by, or submitted to, peer-reviews scientific journals. Each is presented as a Chapter in this thesis. Following each is a detailed contribution statement.

Statement of contributions by others to the thesis as a whole.
No contributions by others.

Statement of Parts of the Thesis Submitted to Qualify for the Award of Another Degree.
None.

Published Works by the Author Incorporated into the Thesis

1. B. P. Lanyon, T. J. Weinhold, N. K. Langford, K. J. Resch, J. L. O'Brien, A. Gilchrist and A. G. White. Manipulating biphotonic qutrits. *Phys. Rev. Lett.*, 100, 060504, 2008. [DOI: 10.1103/PhysRevLett.100.060504]. [e-print arXiv:quant-ph/0707.2880]. Incorporated as Chapter 5 of this thesis.

2. B. P. Lanyon, T. J. Weinhold, N. K. Langford, J. L. O'Brien, K. J. Resch, A. Gilchrist and A. G. White. Experimental demonstration of Shor's algorithm with quantum entanglement. *Phys. Rev. Lett.*, 100, 060504, 2008. [DOI: 10.1103/PhysRevLett.99.250505]. [e-print arXiv:quant-ph/0707.2880]. Incorporated as Chapter 2 of this thesis.

3. B. P. Lanyon, M. Barbieri, M. P. Almeida and A. G. White. Experimental Quantum Computing without Entanglement. *Phys. Rev. Lett.*, 101, 200501, 2008. [DOI: 10.1103/PhysRevLett.101.200501]. [e-print arXiv:quant-ph/0807.0668]. Incorporated as Chapter 4 of this thesis.

4. B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist and A. G. White. Simplifying quantum logic using higher-dimensional Hilbert spaces. *Nat. Phys.*, 5, 134, 2008. [DOI: 10.1038/nphys1150]. [e-print arXiv:quant-ph/0804.0272]. Incorporated as Chapter 1 of this thesis.

5. B. P. Lanyon, N. K. Langford Experimentally generating and tuning robust entanglement between photonic qubits. *New. J. Phys.*, 11, 013008, 2009. [DOI: 10.1088/1367-2630/11/1/013008]. [e-print arXiv:quant-ph/0802.3161]. Incorporated as Chapter 6 of this thesis.

6. B. P. Lanyon, J. D. Whiteld, G. G. Gillet, M. E. Goggin, M. P. Almeida, I. Kassal, J. D. Biamonte, M. Mohseni, B. J. Powell, M. Barbieri, A. Aspuru-Guzik and A. G. White. Molecular energy calculation on a prototype optical quantum computer. under review, 2009. Incorporated as Chapter 3 of this thesis.

Additional Published Works by the Author Relevant to the Thesis but not Forming Part of it

1. K. J. Resch, J. L. O'Brien, T. J. Weinhold, K. Sanaka, B. P. Lanyon, N. K. Langford and A. G. White. Entanglement Generation by Fock-State Filtration. *Phys. Rev. Lett.*, 98, 203602, 2007. [DOI: 10.1103/PhysRevLett.98.203602].

2. M. Barbieri, T. J. Weinhold, B. P. Lanyon, A. Gilchrist, K. J. Resch, M. P. Almeida and A. G. White. Parametric downconversion and optical quantum logic gates: two's company, four's a crowd. *J. Mod. Optics.*, 56, Nos. 2-3, 209-214, 2009. [DOI: 10.1080/09500340802337374].

3. R. B. Rohan, G. G. Gillet, M. P. Almeida, M. Barbieri, B. P. Lanyon, G. J. Pryde, J. L. O'Brien, K. J. Resch, A. G. White and S. D. Barlett. Experimental quantum control of a single photonic qubit. in progress, 2009.

4. M. E. Goggin, M. P. Almeida, M. Barbieri, B. P. Lanyon, J. L. O'Brien, A. G. White, G. J. Pryde. Does a photon have a definite polarization in between two measurements? in progress, 2009.

Acknowledgements

First and foremost I would like to thank my wife, Nia, for all her support throughout my studies. There were few weekends over the last three years when I wasn't thinking about matters relating to this research project. Thank you so much for waiting patiently for them and putting up with me in the meantime. I would also like to thank my supervisor Andrew White, who never lost his temper with me (at least in my presence) despite much provocation. Also, thanks for writing all those grants and always having an open door—which are some of the best things that a supervisor can do.

I owe a big debt of gratitude to my associate supervisor Geoff Pryde. In my first year I was fortunate enough to work closely with Geoff in the Lab. During this time Geoff, very patiently, taught me the experimental skills that I have needed for my PhD. Thank you also for so often giving really useful feedback on my work. Also a big thank you to my other associate supervisors Marco Barbieri and Marcelo Almeida for years of blood, sweat and tears. An Italian, brazilian and englishman walk into a lab...

Throughout my PhD I made thorough use of the expertise at hand within the UQ physics department, which basically means that I went door knocking with my problems a lot. Consequently, I am very grateful to Andrew Doherty and Alexei Gilchrist for putting down what they were doing and sharing their knowledge, and especially to Guifre Vidal, whose problem solving skills and physical intuition are inspirational.

In one way or another, almost all of the research presented in this thesis is built upon work done by Tim Ralph, whose creative brilliance I could not have done without: thank you Tim, please keep it up.

Finally, thank you to my fellow Ph.D. students, especially Nathan Langford, Geoff Gillet, Austin Lund, Till Weinhold, Rohan Dalton, Mark Dowling, Nick Menicucci, Peter Rhode and Brendon Higgins.

Abstract

One of the current hot topics in physics is *quantum information*, which, broadly speaking, is concerned with exploring the information-processing and storing tasks that can be performed in quantum mechanical systems. Besides driving forward our experimental control and understanding of quantum systems, the field is also in the early stages of developing revolutionary new technology of far reaching implication.

As part of these endeavors, this thesis presents some results in *experimental* quantum information. Specifically, we develop several new tools for performing quantum information processing in optical quantum systems, and use them to explore a number of applications and novel physical phenomena. A central theme, and one of the most sought after applications of quantum information, is the pursuit of a programmable *quantum computer*. This thesis is divided into 3 parts.

In Part I we develop some new optical quantum logic gates, which are tools for manipulating quantum information and the fundamental building blocks of a quantum computer. We also develop a new technique for simplifying the construction of quantum logic circuits, by exploiting multi-level quantum systems, that has the potential for application in any physical encoding of quantum information.

In Part II we use these tools to perform some of the first demonstrations of quantum algorithms. Each of these could, in principle, efficiently solve an important problem that is thought to be fundamentally intractable using conventional 'classical' techniques. Firstly we implement a simplified version of the quantum algorithm for factoring numbers, and demonstrate the core processes, coherent control, and resultant entangled states required for a full-scale implementation. Secondly we implement an algorithm for calculating the energy of many-body quantum systems. Specifically, we calculate the energy spectrum of the Hydrogen molecule, in a minimal basis. Finally we demonstrate an algorithm for a novel model of quantum computing that uses mixed states. Here we perform the first characterisation of intrinsically non-classical correlations between fully separable quantum systems, captured by the 'discord'—a measure of quantum correlations in mixed states that goes beyond entanglement.

Part III presents a technique that extends experimental control over biphotons—the novel quantum information carriers formed by the polarisation of two photons in the same

spatial and temporal mode. We also generate and explore new forms of entanglement: producing the first instance of *qubit-qutrit* entanglement, by entangling the polarisation of a photon and a biphoton, and developing a technique that enables full control over the level of 'W-class' of multi-partite entanglement between the polarisation of three photons.

Keywords & Australian and New Zealand Standard Research Classifcations (ANZSRC)

Keywords

Quantum Information, Quantum Computing, Linear Optical Quantum Computing, Quantum Optics, Pulsed Parametric Down-conversion.

ANZSR codes

80% 020603 Quantum Information, Computation and Communication
20% 020604 Quantum Optics

Contents

List of Figures

Introduction

Almost all of the different ways that information is stored and processed in the world today have something in common—the information is encoded into degrees of freedom of physical systems that are accurately described by classical physics. For example: hard drives typically use the orientation of macroscopic magnetic domains; computer processors use the state of transistor switches or the charge on a capacitor; even performing a calculation by hand uses chalk markings on a blackboard, or ink on paper. Even though some of these systems, like the modern transistor, certainly employ quantum effects in their operation, the degrees of freedom in which the information is encoded can be described by classical physics, to a high degree of approximation.

We said 'almost all' because in several laboratories around the world, physicists and engineers are starting to try something fundamentally different—to store and process information encoded into degrees of freedom of physical systems that must be described using *quantum mechanics*. This is the experimental arm of the very broad research field of *quantum information*, which studies the limits and capabilities of information processing and storage in quantum systems.

An important consequence of moving to encode information into quantum systems is that they can exist in a *superposition* of all possible states. This is in contrast to classical information carriers, which at any instant are in only one of their available states, representing either a '1' or a '0', an 'a' or 'b', but not both at the same time. The ability to be in a superposition is a precursor to a uniquely quantum mechanical phenomena called *entanglement*. Multiple quantum systems can exist in a superposition of their joint states that cannot be written as a product of states of the individual systems—the individuals have no identity on their own and can only be defined in terms of their joint properties, hence they are 'entangled'. Entanglement has been the subject of immense volumes of research and debate for almost a century, culminating in experimental results which imply that we must rethink our concepts of locality (that things going on in one location are somehow separate from things going on at another at the same time) and reality (that physical systems have well defined individual properties independent of observation).

Another fundamental physical difference lies in the effect of *measurement*. While, in principle, classical systems can be measured to reveal their past and future states

without consequence, measuring a quantum system seems to irredeemably alter the system itself. Access to the physical phenomena of *superposition*, *entanglement* and *quantum measurement* represent the major changes to the rules of information processing, when moving to encode information in quantum systems. It is also useful to think of these phenomena as new *resources* for information technology.

Over the last 20 years or so, a range of powerful and exciting applications for quantum information have been proposed that exploit these resources. These include protocols for unconditionally secure information transfer, and the use of highly non-classical states to enable ultra-high resolution measurement. Probably the most established, far-reaching and sought-after application is *quantum computation*, where the vision is to build a quantum version of the programmable classical computer.

There is much excitement associated with this prospect, largely due to the discovery that such a device could offer dramatic speed-ups in the computational time required to solve a number of important problems. The most well known of these is the factoring problem, i.e. finding the prime factors of composite numbers. Besides being of fundamental interest to mathematicians and computer scientists, the difficulty of solving this problem using conventional 'classical computers' is the basis for one of the most widely used encryption protocols in the world. Consequently, the speed-up offered by the quantum factoring algorithm, discovered by Peter Shor [Sho94], is of immense importance to governments, large companies and other major funding bodies for scientific research.

Another example is the discovery that quantum computers offer a dramatic improvement over classical computers when it comes to the simulation of quantum systems themselves [Fey82, Llo96, AL97, AGDLHG05]. The difficulty of solving this problem classically represents a significant obstacle to scientific research in a range of fields involving many-body quantum mechanics, such as solid state physics and quantum chemistry. In this way, a quantum computer would provide an invaluable tool for the development of science itself.

Fortified by these applications, and the desire to develop our understanding of quantum systems, there is currently a world-wide initiative to build a quantum computer, involving many different physical architectures that includes, but is not limited to: large ensembles of nuclear spins; ions in traps; superconducting systems; Bose-Einstein condensates; and, of particular importance to this thesis, photonic systems. While the details of each candidate system are very different, broadly speaking, the challenges are much the same, and equally as daunting: to initialise quantum information carriers into a well defined state: manipulate them in a coherent and arbitrary fashion: read-out information from the systems: overcome sources of error: and to do all this on a large scale.

The first attempts to build a quantum computer were carried out in the 1990s in a bulk NMR architecture [JMH98, CVZ+98]. Researchers even reported experiments involving information encoded in up to 7 quantum systems and their use to implement small-scale quantum algorithms [VSB+01]. However, it is now known that the ability for a system to generate a significant amount of *entanglement* is a prerequisite for any computational advantage over a classical computer, when pursuing the standard pure-state models of quantum computation[1]. In 1999 it was shown that bulk NMR is unable to do this [BCJ+99], and therefore the early experiments represent no more than a classical simulation of a quantum computational device.

Since then the big experimental players have been ion-trap [HRB08] and linear-optic systems [KMN+07]. Both systems can generate a large amount of entanglement and have known theoretical paths to large-scale quantum computation. More recently, several other systems have come 'online', with most notable success coming from super conducting systems [SAB+06, PdGHM07, CW08b]. Today, in any of these architectures, performing a few quantum operations on at most a handful of quantum systems represents the state of the art. Even this takes us to the absolute forefront of our understanding and experimental capabilities, and consequently there is much work to be done.

Besides the end-of-the-road benefits of an operational full-scale device, research and development into quantum computing is also motivated by the journey itself. One of the most exciting things about the subject is how little we know, both in terms of our abstract theoretical understanding and our practical knowledge of how to go about doing it in a physical system. Consequently, there is a lot of new territory to be explored. Often the most profound insights in science come when we develop a method for probing a new regime of nature, and this is exactly what is happening in the pursuit of quantum computing. Physicists are developing an unprecedented level of control over quantum systems in the laboratory.

This thesis presents a series of developments in experimental quantum computing and quantum information. All our experiments are carried out using linear optics to manipulate quantum information encoded into photons. We now give a more detailed summary of these areas, before describing the scope and results of our work.

[1] As we shall emphasize in this thesis, this requirement for entanglement may be avoided, for a subset of problems, by pursuing mixed state quantum computational models, although other highly non-classical correlations between separable states are still required [Vid03].

0.1 Quantum computing

The circuit model of quantum computing was the first to be developed and is the most relevant to the work carried out in this thesis. A detailed introduction to the subject is presented by Nielsen and Chuang [NC01] and therefore we do not reproduce it here. We will assume some familiarity and simply review the main concepts.

The physical stage on which quantum computation is performed are two state quantum systems, commonly called 'qubits' (**qu**antum-**b**inary-dig**its**). The two states are orthogonal. Physically, this means that after measuring the system to be in one state, the probability of an immediate subsequent measurement finding it in the other state is zero. The circuit model of quantum computation is concerned with *pure* state qubits, which can exist in any real or complex *superposition* of their two states, so long as the probabilities for finding the system in each state adds up to one (i.e. the superposition is normalised). Qubits are an abstract concept that could be realised in any physical system with these properties, such as the spin of an electron, the polarisation of single photons, or energy levels of atoms, for example.

Figure 0.1 shows the three stages of a generic circuit model quantum computer algorithm. Firstly, a large number of qubits are each initialised into some simple initial state $|\psi\rangle$. Secondly, the computation itself corresponds to some collective *unitary* evolution (U) of all the qubits. Finally the answer is read out by measuring the logical state of some, or all, of the qubits.

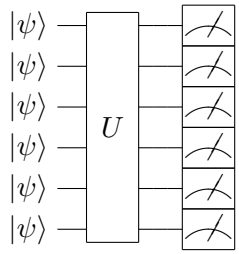


Figure 0.1: **Circuit model of quantum computation**. A large number of qubits are each initialised into some fiducial pure state $|\psi\rangle$, computation then proceeds via a large unitary evolution U and finally the answer is readout via a logical measurement of each qubit.

Since each qubit is initialised into a well defined pure state $|\psi\rangle$, they are not initially entangled. The motivation for this is that it is thought to be easier in practice to prepare such states, than some highly entangled state (and the author can vouch for this when using linear optics). Consequently, the resources required for initialisation can be disregarded. The unitary operation, which is the important part in terms of computational

resource expenditure, can be any of the continuous set of possible unitary operations on n qubits. Which, considering that specifying such a thing requires defining 2^n parameters, is a very large set indeed. Fortunately, any unitary operation can be constructed using only elementary operations, known as gates, from simple and well-understood sets. A gate set with this property is known as *universal*.

Broadly speaking, there are two kinds of universal gate sets; continuous and discrete. Continuous sets can implement any unitary *exactly* with a finite number of gates. Discrete sets can implement an *approximation* to the ideal unitary operation, but with an accuracy that can be made arbitrarily close to, but not exactly, unity. The later is sufficient for practical purposes and makes the construction job far easier—to build a quantum computer, in any particular physical system, we need only demonstrate that we can perform a discrete set of gates. The remaining issue them becomes one of *scalability*. Can we perform enough gates on enough qubits to do anything useful? Another important consideration is that *fault-tolerant* approaches to quantum computing have only been theoretically constructed for discrete gate sets—we don't know how to overcome errors when employing continuous gate sets.

So to recap, the circuit model of quantum computing requires: qubits that can be initialised into simple pure separable state; a discrete universal gate set; the ability to measure the state of each qubit; and to do all this on a large scale. Indeed, this was the wish-list published by David P. Divincenzo [DiV00] in 2000, although he added one more: a qubit coherence time much longer than the time taken to implement a universal gate set. It is also now commonly accepted that the ability to interconvert flying (photonic) and stationary (matter) qubits will also be required.

Other distinct models of quantum computing include 'one-way' [RB01] and 'adiabatic' [FGGS00]. In short, the one-way model involves preparing a very specific highly entangled state of qubits, called a *cluster state*. Universal computation then proceeds via a sequence of 1-qubit measurements (in a basis determined by the outcome of previous measurements). The major resource expenditure for this model occurs in preparing the cluster, specifically the number of elementary operations required (a cluster state can be built from separate qubits using quantum logic gates). The adiabatic model seems very different again. Here, a target Hamiltonian of a quantum system is engineered such that the ground state contains the answer. Computation begins with the system (of qubits, for example) in the ground state of some simple, well understood Hamiltonian, the interactions are then slowly changed towards implementing the target Hamiltonian. If this change is slow enough then the system will end up in ground state of target Hamiltonian—

and the answer can be simply read out. Here, the major resource expenditure is time it takes to move between Hamiltonians. If the energy levels in the target Hamiltonian are very close together, then the evolution has to be very slow to avoid getting wrong answer (an excited state, for example).

The number of computational resources required to implement algorithms (and therefore solve problems) on a computer is the study of complexity theory. In the circuit model of quantum computation the resources are qubits and quantum logic gates, in classical computation they are bits and classical logic gates, with the one-way model its the size of the cluster state and in adiabatic quantum computing it's the time taken to move between Hamiltonians. Fortunately, all of these apparently disparate computational resources can be re-expressed as a computational *time*, i.e. the time taken to implement gates, create clusters, or move between Hamiltonians. The question of central importance is 'for a given algorithm, how does the computational processing time *scale* with the size of the problem'. For example, when factoring, the problem size goes up with each bit in the number to be factored, when searching databases the problem size goes up with the number of entries in the database. The answer to this scaling question determines the *complexity class* of the problem, for a given computational model. Note the complexity of a problem has *nothing* to do with the number of resources required to solve a given instance of a problem, just how that number scales with the problem size.

The most significant distinction is drawn between polynomial and exponential time scaling—from a complexity perspective this is the difference between a problem that is deemed to be computationally 'hard' and one that is 'easy'. An algorithm is also often referred to as 'efficient' if the computational time is polynomial in the problem size. Shor's factoring algorithm was one of the first examples of an algorithm for a quantum computer that takes a problem that is thought to be hard on a classical computer and makes it easy, hence all the excitement.

The powers of different computational models are considered to be the same if for any algorithm in one model, there is an equivalent algorithm in the other model that uses at most a polynomial multiple of the processing time. The good news from the not-getting-a-head-ache point of view is that the circuit, one-way and adiabatic models are equivalent in terms of their computational power [RB01, AvK$^+$07]. However, the great thing about having different options is that one model or another—or some hybrid—may ultimately turn out to be easier to implement in practice.

It is important to be aware that scaling results for algorithms typically only give *upper* bounds on complexity. For example, we can say with certainty that factoring is an easy

problem on a quantum computer. However, we cannot be sure that it is hard on a classical computer. Although it seems unlikely, it is possible that an algorithm may yet be found that makes factoring an easy problem on a classical computer.

Unfortunately, we can say with certainty that a quantum computer *cannot* make all computational problems easy. In 1995 Manny Knill showed that almost all possible quantum algorithms require an exponentially increasing number of logic gates to be implemented (discrete or continuous), with the problem size [Kni95]. Consequently, it is the hope of quantum computing that it will take *some* problems that are irrevocably hard to do on a classical computer and make them easy. For a comprehensive treatment of classical computational complexity theory, see [Pap94]. A good reference for quantum complexity theory is [BV97].

Broadly speaking, there are three known classes of quantum algorithms that offer an improvement over the best classical alternatives. There are those, like Shor's algorithm, that are based on the *quantum Fourier transform*. These algorithms all take problems thought to be hard on a classical computer and make them easy. There are those, like Grover's algorithm [Gro96], that are concerned with solving *searching* problems. Algorithms in this class only offer a quadratic speedup over the best classical approaches, but due to the wide application of these problems, they receive considerable interest. Finally there are algorithms associated with *simulating quantum systems*. Like the quantum Fourier transform algorithms, quantum simulation algorithms are thought to make classically-hard problems easy. A detailed review of each of these algorithm classes is provided by Nielsen and Chuang [NC01].

0.2 Quantum computing with photons and linear optics

A detailed review of linear optical quantum computing (LOQC) is presented by Kok *et al* [KMN$^+$07]. We now provide a summary of important results for this thesis.

Photonic systems play a substantial role in quantum information experiments because they make excellent quantum information carriers in many respects. Photons are extremely well isolated systems and are essentially unperturbed by thermal noise, even at room temperature. Consequently, photonic qubits have very long coherence times, without the need for extensive cooling or high quality vacuum apparatus (unlike matter encodings of quantum information). There are a range of established techniques and relatively inexpensive technologies available for photon generation, detection and individual

manipulation. Photons also allow quantum information to be moved around at the speed of light which makes them of central importance to field of *quantum communication*, for example. All of these properties make photonic systems an ideal test-bed in which to explore quantum information.

Photonic systems were not initially considered as candidates for a quantum computing architecture, due to the absence of a natural photon-photon interaction (or sufficiently strong mediated interaction) required to generate entanglement and implement universal quantum logic. However, in 2001 Knill, Laflamme and Milburn [KLM01] (KLM) showed that efficient quantum computation with photons and linear optics is possible. The essence of their technique contains two results: firstly, the inherent non-linearity of the measurement process can to be harnessed to implement *non-deterministic* linear optic quantum logic gates (gates that don't work all the time, but only with some probability); secondly, that these gates can be made arbitrarily close to deterministic using teleportation, a vast number of additional 'ancilla' photons[2] and error-correction. An important caveat is the requirement for single photon sources and photon number resolving detectors[3]. This result showed, for the first time, that photonic systems are not only a useful test-bed in which to explore quantum information, but also offer a legitimate candidacy for a scalable quantum computing architecture.

Since then several other schemes have been proposed that improve on the KLM scheme in terms of the resources required for universal quantum computation. There is the one-way model, which has particular advantages for optical quantum computing [Nie04]. Here, non-determinisitc logic-gates can be used offline to prepare the highly entangled clusters states. Indeed, proof-of-principle demonstrations of the generation of optical cluster states, and their use to simulate a circuit model universal gate set, have already been demonstrated, see [WRR$^+$05, VPM$^+$07, LZG$^+$07] for example. There have also been proposals to amplify weak photon-photon interactions by coupling single photons to bright coherent states of light [NM04] and, very recently, to encode qubits into coherent states themselves [LRH08].

In the last 5 years there have been a number of proposals for, and demonstrations of, KLM inspired non-deterministic 2-qubit linear optic quantum logic gates [RWMM01, Kni02, PFJF03, PJF02, RLBW02, HT02, OHTS05, LWP$^+$05, OPG$^+$04, OPW$^+$03, GPW$^+$04, ZZC$^+$05, BCZ$^+$07]. These demonstrations represent some of the earliest successful quantum logic experiments in any physical system. When coupled with established techniques for implementing deterministic arbitrary 1-qubit gates, these gates form a universal linear

[2]But not exponentially growing with the desired accuracy.

[3]To be more specific; detectors that can distinguish between one and more than one photon.

optic gate set. Of particular importance to this thesis are the two-qubit 'controlled-Z' gates[4] based on partially polarising beamsplitters (PPBS), which where first developed in 2005 [LWP+05]. The operational principles of these gates are well described in the original publication and more so in colleagues' recent theses (Till J. Weinhold [Wei08] and Nathan K. Langford [Lan07]). However, we will now review some key features.

Firstly, perfect gate operation requires indistinguishable single photons to be injected into each optical input mode, and measurement of a single photon in each output mode. This measurement is often refereed to as 'post-selection' and is currently performed destructively i.e. the presence of a photon is determined by measuring the information carrying photons directly using a photodetector, for example. In the experiments performed so far (and in this thesis) true single photon sources and photon-number resolving detectors were not available[5]. Therefore, a photo-detector 'click' at an output mode could be the result of more than one photon. However, the only way for this to occur, and all the detectors at each output fire, is if more than one photon was injected into an input mode. In the case where the probability of this occurring is small, and conditioning on simultaneous firing of all detectors (i.e. the observation of 'coincident' detector clicks, within some time window), the gates can perform quite well.

As a consequence of the requirement to post-select, these gates cannot be 'chained' i.e. two gates cannot operate sequentially on the same photons, as shown in Fig. 0.2. If this is done then measurement of a photon in each output mode of the final gate does not guarantee successful operation of the previous gate (in fact it most likely did not work). See Fig. 0.3 for more details. However, with some significant development in optical source and detector technology it would be possible to perform this measurement non-destructively. One way to do this is described in the final section of Chapter 1. Of course, once these gates are non-destructively heralded, the non-determinism must still be overcome if they are to be part of a path to scalable linear optic quantum computing. This is where the KLM, one-way or other scheme comes in.

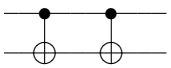


Figure 0.2: Chained CNOT gates.

Linear optic logic gates are clearly at a very early stage in their development, and much progress is required before they can be used to build a scalable quantum computer. However, the realisation of non-deterministic, post-selected gates is an important step

[4]Where Z is the standard σ_z operation [NC01].

[5]Although much progress is being made, see [GSV04, MD04] for example.

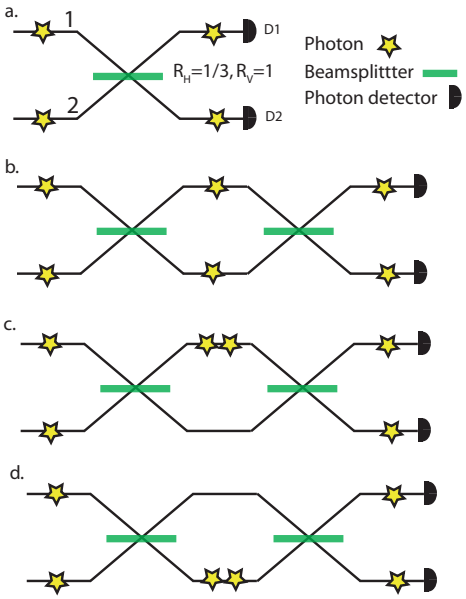


Figure 0.3: **Chaining errors in linear optic 2-qubit gates based on partially polarising beamsplitters**. **a**. The heart of the operation of one gate: single photons injected into input modes 1 and 2 meet at a polarising beamsplitter. Successful gate operation is heralded by measurement of a single photon in each output mode (shown here being performed destructively). See [Lan07] and [Wei08] for more details on these gates. **b-d**. 3 possible photons paths when two gates are chained. Clearly, successful measurement of single photons in the final output modes does not guarantee successful operation of either gate (in **c** and **d** the second gate will also fail because single photons were not injected into each input mode). To succeed in chaining, photon number measurements must be made after each individual gate. See Section 1.5 for an example of how this can be achieved non-destructively.

and has already enabled a significant amount of new research in the fields of quantum computation and quantum information. For example, they have been used to construct the first cluster states for one-way quantum computation [WRR$^+$05], explore quantum non-demolition measurements [POW$^+$04, RBO$^+$06], perform Bell-state analysis [LWP$^+$05] and investigate quantum weak values [POW$^+$05] (to name a few). Clearly there is much to do with, and learn, from these devices on the way to building a scalable optical quantum computer.

So, at the beginning of this research project (early 2006), the state of the art in the field experimental LOQC was the demonstration of these proof-of-principle universal gate sets, and their application to some novel quantum information applications. Key scientific questions facing the field at this point were: how can we scale-up linear optic quantum information technology and construct more complex multi-qubit devices?: what quantum

information applications can this technology be used for?: what are the factors limiting the performance of these circuits and their applications?: and what, therefore, are the next important steps for the field? These are some of the issues that this thesis will address.

0.3 This thesis

This is not a traditional thesis, but a thesis by publication, which means that it consists of a series of research papers in the original format in which they have been published, or submitted for publication. There are 6 Chapters, each of which presents a paper for which I am the leading author, and a small amount of additional material added for the purpose of this thesis. The papers in Chapters 1, 2, 4, 5 and 6 have been published and are presented unaltered in the journal format in which they were published. The paper in Chapter 3 has not been published, but is currently under review at a journal. Each paper is immediately followed by a contribution statement.

The chapters are divided into three parts. Part I presents, amongst other things, the development of new linear optic quantum logic gates. This work directly addresses the scientific question of how to scale up linear optic quantum computation technology, from a past of simple gates, to a future of complex multi-qubit devices. It also provides some clear answers to the question: what are the current limiting factors on further complexity jumps? Part II presents the use of these tools to implement three small-scale quantum computer algorithms. This work directly explores the question of what LOQC technology can be used for and what challenges, and guidelines for future work, that these applications present. The relevance of this work goes beyond LOQC, as we perform some of the first experimental implementations of the respective quantum algorithms in any physical architecture and present bench marks for future work in this direction. Part III presents some developments in optical quantum state engineering and manipulation, relevant to the more general field of quantum information. This work addresses some specific open questions that are discussed below.

Each article in this thesis contains its own introduction and definition of mathematical and technical terms, and so we do not attempt to reproduce them here. We now give a more detailed overview of their content and context. Note that the papers are not presented in chronological order.

Part I contains Chapter 1, which presents a technique for the simplification of quantum logic circuits, and its use to construct two new linear optic quantum logic gates: the

3-qubit Toffoli and 2-qubit controlled-unitary [NC01]. We build these well-studied gates piecewise from a universal set of 2-qubit CNOT and 1-qubit gates [NC01]. This is the 'joint-first' time that either of these gates have been demonstrated in any quantum computing architecture: during the completion of our work we became aware of an parallel implementation of the Toffoli gate in an ion-trap [MKH$^+$09].

The simplification technique itself exploits quantum information carriers with more orthogonal states than the canonical qubit. The availability of these additional states allows the number of elemental logic gates required to build a certain range of logic circuits (of which the Toffoli and controlled-unitary are first-order examples) to be reduced. It is this reduction that enables us to implement the new gates, which would otherwise be infeasible with current technology. Photons have many degrees of freedom in which quantum information can be encoded, allowing the technique to be readily employed. In our experiments we exploit both photon polarisation and longitudinal spatial mode to construct multi-state quantum information carriers. While our experiments are performed with photons, the simplification technique is independent of the physical encoding of quantum information and therefore potentially of interest to the more general quantum computing community.

Part II contains Chapters 2, 3 and 4, which each present a different small-scale implementation of a quantum algorithm. Specifically, Shor's factoring, a quantum simulation and the normalised-trace estimation algorithms, respectively. The run-time of each of these algorithms scales polynomially with the problem size, unlike the best known classical algorithms, which have an exponential scaling. Consequently, they are all examples of powerful quantum algorithms that are thought to make classically hard problems easy.

The implementations are all proof-of-principle and the reader should not expect to see an improvement over the ability of a classical computer to solve the particular instances of problems considered. It is the *way* that we solve the problems that is important: using qubits and quantum logic gates. Our demonstrations of these algorithms are some of the first in any quantum computing architecture and bring us to the edge of what is possible with current technology.

Chapter 2 contains our demonstration of Shor's quantum factoring algorithm, where we find the prime factors of 15—the smallest non-trivial example. An important feature of our experiment is that we show that our circuits generate entanglement, which is a necessary requirement for this pure state algorithm to offer a speedup over a classical approach [Vid03]. The only previous demonstration of Shor's algorithm was performed in 2001 in a bulk NMR architecture [VSB$^+$01]. However, as previously discussed, it has been

shown that bulk NMR systems cannot support entanglement, implying that this result was, at best, a classical simulation [BCJ+99].

Choosing to factor 15 brings our implementation within the realms of possibility with current technology (given the developments of Chapter 1), since part of the algorithm simplifies in this case. Specifically the multi-qubit gates in the quantum Fourier transform become redundant. However, as we demonstrate in Chapter 3, this part of the algorithm can always be performed in a classical manner [GN96], and is not therefore an essential part of the quantum algorithm. In order to explore a second, more complicated implementation we do make a simplification to the quantum routine, which is described in the paper.

A feature of one of our two Shor's algorithm implementations is that it required building a new linear optic quantum logic circuit—specfically concatenating two CNOT gates, as shown in Fig. 0.4.

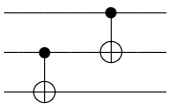


Figure 0.4: Two concatenated CNOT gates.

This is the first time that a linear optic quantum logic circuit has been built that involves more than one 2-qubit gate. Furthermore, this particular type of concatenation is the pattern required to generate a cluster state for the one-way model of computation. In our implementation we use this circuit to generate the maximally entangled 3-qubit Greenberger-Horne-Zeilinger (GHZ) state, which is locally equivalent to a 3-qubit cluster state. Furthermore, to the authors' knowledge, this is the first time that a GHZ state has been generated between photons initially in a separable state (at least their polarisation was separable, which is the degree of freedom that we used to encode our qubits). Previous experiments began with some significant level of preexisting entanglement between the photonic qubits [RWZ05, WRZ05], generated in the process through which they were created (polarisation entangled spontaneous parametric downconversion). It seems that the ability to take initially *separable* photonic qubits and entangle them into a GHZ state represents a new degree of experimental control.

During completion of this work we became aware of another linear optics implementation of Shor's algorithm by the group of Jian Wei Pan in Hefei, China [LBYP07]. Both of our papers where subsequently published back-to-back in Physical Review Letters.

Chapter 3 presents an implementation of a quantum simulation algorithm, where we calculate the energy spectrum of a molecule. Specifically, we encode the quantum

state of the hydrogen molecule (H_2) into photonic qubits, simulate the time-evolution operator using quantum logic gates, and extract the energy levels of the molecule using the iterative phase estimation algorithm. This represents one of the first demonstrations of the use of a quantum computer to simulate quantum systems *and* extract key properties of interest. The specific problem of molecular energy calculation is of particular importance in quantum chemistry, since this quantity determines a range of physical properties.

In order to bring this within reach of our current gate technology (given the developments of Chapter 1) the simulation and subsequent energy calculation is performed in a minimal basis for the molecular Hilbert space (specifically, we consider only a single electronic orbital around each of the two nuclei). This allows the wavefunction to be encoded in as few qubits as possible, but reduces the accuracy. However, this is not unreasonable—any full scale implementation will also have to choose some truncated finite basis, since an exact solution requires an infinite basis. Hence this is not a simplification of the algorithmic process, we are just turning the accuracy knob down. We are certainly not aiming to achieve the accuracy required for practical quantum chemistry applications here, simply demonstrate the algorithmic principles in practice.

However, we do make an important simplification. Due to the small-size of the problem, we are able to implement the molecular time evolution operator (generated by the corresponding Hamiltonian) *exactly*, using a small number of quantum logic gates. For larger implementations this will not be possible and consequently this part of our implementation does not scale efficiently. However, we extensively detail how the evolution operator can be implemented efficiently, using an *approximation* technique, in the additional supporting material. Demonstrating this technique is currently way beyond the reach of our available technology as it requires far more logic gates than we can currently perform.

The algorithms of Chapters 3 and 4 were all implemented using the circuit model of quantum computing. As we have said, the power of this model is computationally equivalent to the adiabatic and one-way models. Another thing that these models have in common is that they all employ information carriers in *pure states*. In this case we know that they must generate a large amount of entanglement in order to offer a speed-up over a classical computer [Vid03].

The algorithm demonstrated in Chapter 4 employs a very different model of quantum computing called 'deterministic quantum computation with one pure qubit' (DQC1) [KL98]. DQC1 is identical to the circuit model except in the qubit initialisation stage, where the initial state is replaced by only one qubit in a pure state, and the rest in the completely

mixed state, as shown in Figure 0.5. A fascinating aspect of this model is that its computational power is thought to lie somewhere in between that of universal pure state quantum computing and classical computing [KL98, DFC05].

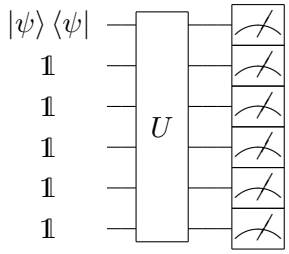


Figure 0.5: **Deterministic quantum computation with 1 pure qubit**. One of a large register of qubits is initialised in pure state $|\Psi\rangle$, while the rest are initialised in the fully mixed state $\mathbb{1}$. Computation then proceeds via a large unitary evolution U and finally the answer is readout via a logical measurement of each qubit.

Most of our understanding of DQC1 is derived from the single algorithm that has been developed for it: estimating the normalised trace of a unitary matrix. Somewhat surprisingly, the ability to perform this task efficiently enables the solution of a range of interesting problems, as described in our paper. DQC1 is only 1 pure qubit away from being very easy to simulate classicaly (i.e. if the top qubit was fully mixed then the output state would be the same as the input state!). Consequently it is surprising that the addition of only one qubit can enable such an increase in power. Another fascinating aspect of this model is that it does not appear to generate a significant amount of entanglement. Instead, it has been proposed that the computational power is reliant on the generation of other intrinsically non-classical correlations, and that these can be captured by a quantity called 'discord' [DSC08, OZ01].

In our paper we present a first-order implementation of the normalised trace estimation algorithm (by first order we mean that the matrix whose trace is to be calculated is 2×2). Furthermore, we observe the absence of entanglement and generation of a significant amount of discord by our circuits. This represents the first experimental measurement of this physical phenomena. The normalised trace-estimation algorithm was first demonstrated in a bulk NMR architecture some time ago [REP+05]. However, they did not explore the underlying correlations, and it may even be possible to show that this architecture is also not capable of supporting any discord[6].

Part III begins with Chapter 5, which presents work on an alternative encoding of photonic quantum information. Specifically, the three-state system provided by the po-

[6]Private communication with Carl Caves, University of New Mexico.

larisation of two photons in the same spatial and temporal mode, or 'biphotonic qutrits'. Consequently, these offer a larger Hilbert space in which to encode quantum information. The results of Chapter 1 add to several others, referenced in this paper, that show how information carriers with greater dimension than the canonical qubit offer advantages for quantum information applications. Biphotons in particular have been the focus of a some research and experimental development, as referenced in our paper. However, a problem with these systems is that the level of control of individual biphoton states is severely limited with standard techniques (waveplates). In our paper we present and demonstrate a technique for extending this level of control. Specifically, we exploit an ancillary photon, and the non-linearity of measurement, to perform highly non-trivial biphoton operations. Furthermore, we demonstrate the first instance of qutrit-qubit entanglement by entangling a biphoton and a single photon.

Chapter 6 presents results concerned with extending our ability to generate and control entanglement in the laboratory. While there is clearly a connection between improving experimental control over entanglement and developing powerful quantum information technology, a separate motivation for this work is to explore the rich structure of entanglement in many-body systems and its physical characteristics. In our experiment we design and implement a technique for generating 3-qubit states within the W-class of entanglement. By changing a single experimental parameter we are able to directly control the level of this kind of entanglement in the output state. The generated states also display the fascinating property of retaining an underlying bipartite entanglement configuration (qubit-qubit) that seems to be optimally robust against qubit loss (i.e they retain the maximum amount of bipartite entanglement after loosing one qubit to the environment, for example). Note that, from conceptualisation to publication, this work was carried out by myself and fellow PhD student Nathan Langford.

Finally, in the *discussion and outlook* we review what we have learned from the developments presented in this thesis and discuss where this research may lead in the future.

Part I

Building optical quantum logic gates

Chapter 1

Simplifying quantum logic using higher-dimensional Hilbert spaces

ARTICLES
PUBLISHED ONLINE: 7 DECEMBER 2008 | DOI: 10.1038/NPHYS1150
nature physics

Simplifying quantum logic using higher-dimensional Hilbert spaces

Benjamin P. Lanyon[1]*, Marco Barbieri[1], Marcelo P. Almeida[1], Thomas Jennewein[1,2], Timothy C. Ralph[1], Kevin J. Resch[1,3], Geoff J. Pryde[1,4], Jeremy L. O'Brien[1,5], Alexei Gilchrist[1,6] and Andrew G. White[1]

Quantum computation promises to solve fundamental, yet otherwise intractable, problems across a range of active fields of research. Recently, universal quantum logic-gate sets—the elemental building blocks for a quantum computer—have been demonstrated in several physical architectures. A serious obstacle to a full-scale implementation is the large number of these gates required to build even small quantum circuits. Here, we present and demonstrate a general technique that harnesses multi-level information carriers to significantly reduce this number, enabling the construction of key quantum circuits with existing technology. We present implementations of two key quantum circuits: the three-qubit Toffoli gate and the general two-qubit controlled-unitary gate. Although our experiment is carried out in a photonic architecture, the technique is independent of the particular physical encoding of quantum information, and has the potential for wider application.

The realization of a full-scale quantum computer presents one of the most challenging problems facing modern science. Even implementing small-scale quantum algorithms requires a high level of control over multiple quantum systems. Recently, much progress has been made with demonstrations of universal quantum gate sets in a number of physical architectures including ion traps[1,2], linear optics[3–6], superconductors[7,8] and atoms[9,10]. In theory, these gates can now be put together to implement any quantum circuit and build a scalable quantum computer. In practice, there are many significant obstacles that will require both theoretical and technological developments to overcome. One is the sheer number of elemental gates required to build quantum logic circuits.

Most approaches to quantum computing use qubits—the quantum version of bits. A qubit is a two-level quantum system that can be represented mathematically by a vector in a two-dimensional Hilbert space. Realizing qubits typically requires enforcing a two-level structure on systems that are naturally far more complex and which have many readily accessible degrees of freedom, such as atoms, ions or photons. Here, we show how harnessing these extra levels during computation significantly reduces the number of elemental gates required to build key quantum circuits. Because the technique is independent of the physical encoding of quantum information and the way in which the elemental gates are themselves constructed, it has the potential to be used in conjunction with existing gate technology in a wide variety of architectures. Our technique extends a recent proposal[11], and we use it to demonstrate two key quantum logic circuits: the Toffoli and controlled-unitary[12] gates. We first outline the technique in a general context, then present an experimental realization in a linear optic architecture: without our resource-saving technique, linear optic implementations of these gates are infeasible with current technology.

Simplifying the Toffoli gate

One of the most important quantum logic gates is the Toffoli[12]—a three-qubit entangling gate that flips the logical state of the 'target' qubit conditional on the logical state of the two 'control' qubits. Famously, these gates enable universal reversible classical computation, and have a central role in quantum error correction[13] and fault tolerance[14]. Furthermore, the combination of the Toffoli and the one-qubit Hadamard offers a simple universal quantum gate set[15]. The simplest known decomposition of a Toffoli when restricted to operating on qubits throughout the calculation is a circuit that requires five two-qubit gates[12]. If we further restrict ourselves to controlled-z (or CNOT) gates, this number climbs to six[12] (Fig. 1a). A decomposition that requires only three two-qubit gates[11] is shown in Fig. 1b. The increased efficiency is achieved by harnessing a third level of the target information carrier—the target is actually a qutrit with logical states $|\mathbf{0}\rangle$, $|\mathbf{1}\rangle$ and $|\mathbf{2}\rangle$.

At the input and output of the circuit, information is encoded only in the bottom two (qubit) levels of the target. The action of the first X_a gate is to move information from the logical $|\mathbf{0}\rangle$ state of the target into the third level ($|\mathbf{2}\rangle$), which then bypasses the subsequent two-qubit gates. The final X_a gate then coherently brings this information back into the $|\mathbf{0}\rangle$ state, reconstructing the logical qubit. By temporarily storing part of the information in this third level, we are effectively removing it from the calculation—enabling the subsequent two-qubit gates to operate on a subspace of the target. This enables an implementation of the Toffoli with a significantly reduced number of gates. Note that only standard two-qubit gates are necessary, with the extra requirement that they act only trivially on (that is, apply the identity to) level $|\mathbf{2}\rangle$ of the qutrit. As such, it is not necessary to develop a universal set of gates for qutrits.

This technique can be readily generalized to implement higher-order n-control-qubit Toffoli gates (${}^n\mathrm{T}$) by harnessing a single $(n+1)$-level information carrier during computation and

[1]Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane 4072, Australia, [2]Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Boltzmanng. 3, A-1090 Vienna, Austria, [3]Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, N2L 3G1, Canada, [4]Centre for Quantum Dynamics, Griffith University, Brisbane 4111, Australia, [5]Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Merchant Venturers Building, Woodland Road, Bristol BS8 1UB, UK, [6]Physics Department, Macquarie University, Sydney 2109, Australia. *e-mail: lanyon@physics.uq.edu.au.

NATURE PHYSICS DOI: 10.1038/NPHYS1150

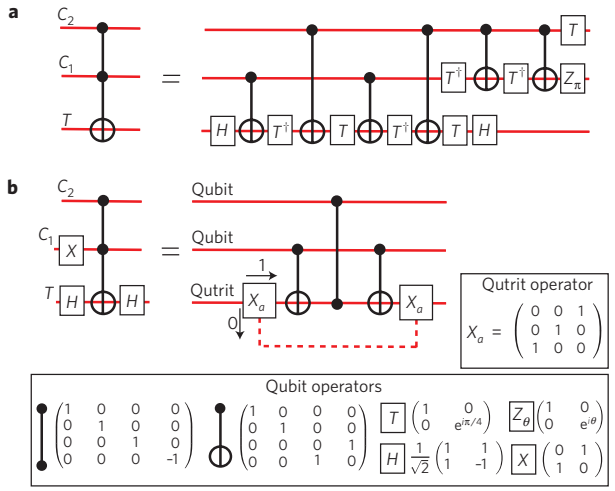


Figure 1 | Simplifying the Toffoli gate. a, Most efficient known decomposition into the universal gate set CNOT + arbitrary one-qubit gate, when restricted to operating on qubits[12]. **b**, Our decomposition requiring only three two-qubit gates[11]. Here, the target is a three-level 'qutrit' with logical states $|\mathbf{0}\rangle$, $|\mathbf{1}\rangle$ and $|\mathbf{2}\rangle$. Initially and finally, all of the quantum information is encoded in the $|\mathbf{0}\rangle$ and $|\mathbf{1}\rangle$ levels of each information carrier. The action of the X_a gates is to swap information between the logical $|\mathbf{0}\rangle$ and $|\mathbf{2}\rangle$ states of the target. The target undergoes a sign shift only for the input term $|C_2, C_1, T\rangle = |\mathbf{1}, \mathbf{0}, \mathbf{1}\rangle$. This operation is equivalent to the Toffoli under the action of only three one-qubit gates, as shown. The second gate in the decomposition is a CZ and is equivalent to a CNOT under the action of two one-qubit Hadamard (H) gates.

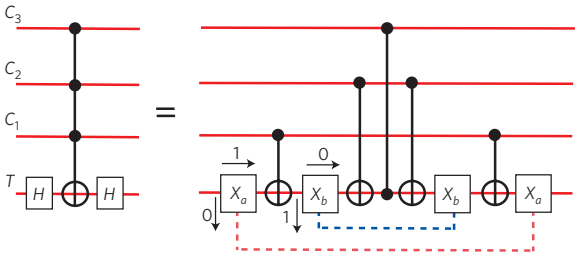


Figure 2 | Simplifying higher-order Toffoli gates. Three-control-qubit Toffoli[11]. The X_a gate swaps information between the logical $|\mathbf{0}\rangle$ and $|\mathbf{2}\rangle$ states of the target. The X_b gate flips information between the logical $|\mathbf{1}\rangle$ and $|\mathbf{3}\rangle$ state of the target. Thus, we require access to a four-level target information carrier: two levels in the original rail and one in each of the dashed rails. The target undergoes a sign shift only for the input term $|C_3, C_2, C_1, T\rangle = |\mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}\rangle$. This operation is equivalent to the Toffoli under the action of only two one-qubit gates, as shown. See Fig. 1 for gate operations.

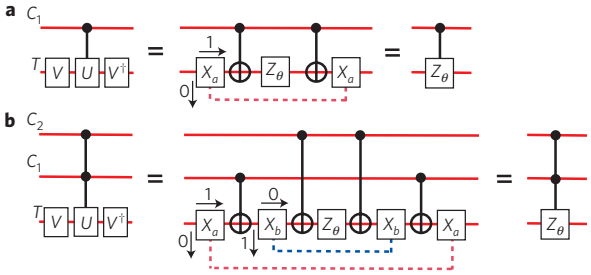


Figure 3 | Simplifying controlled-unitary gates. a, One control qubit (we implement a simplified version, see Fig. 5): the control operation occurs if $|C_1\rangle = |\mathbf{0}\rangle$. **b**, Two control qubits: the control operation occurs if $|C_2, C_1\rangle = |\mathbf{1}, \mathbf{1}\rangle$. $VZ_\theta V^\dagger$ is the spectral decomposition of U, up to a global phase factor. See Fig. 1 for gate operations.

only $2n-1$ standard two-qubit gates[11]; that is, with each extra control qubit we need an extra level in the target carrier (see Fig. 2). Compare this with the previous best known scheme, which requires $12n-11$ two-qubit gates and an extra overhead of $n-1$ extra ancilla qubits[12]. When restrained from using ancilla, this scheme requires of the order of n^2 two-qubit gates. In either case, we achieve a significant resource reduction, by harnessing only higher levels of existing information carriers. For example, the simplest known decomposition of the ^{5}T requires 50 two-qubit gates and four ancilla qubits, when restricted to operating on qubits[12]. Our technique requires only nine two-qubit gates and no ancillary information carriers.

Extension to more general quantum circuits

Figure 3 shows an extension to simplify the construction of another key quantum circuit: the n-control-qubit unitary gate ($C^n U$), which applies an arbitrary one-qubit gate (U) to a target conditional on the state of n control qubits. These circuits have a central role in quantum computing, particularly in the phase-estimation algorithm[12]. Phase estimation underpins many important applications of quantum computing including quantum simulation[16] and Shor's famous algorithm for factoring[17]. Furthermore, the set of $C^1 U$ gates alone is sufficient for universal quantum computing; a $C^1 U$ can implement a CNOT and induce any single-qubit rotation at the expense of an ancilla qubit. Our technique can implement a $C^n U$ using an $(n+1)$-level target and only $2n$ two-qubit gates. This is a similar improvement, over schemes limited to qubits, to that achieved for the Toffoli[12]. Figure 4 shows a further generalization to efficiently add control qubits to an arbitrary controlled-unitary that operates on k qubits.

Potential for application

The technique that we describe is independent of the particular physical system used to encode quantum information and the way in which the elemental gates are realized. Consequently, it has the potential for application in many architectures, yielding the same resource savings. The only physical requirements are access to multi-level systems and the ability to coherently swap information between these levels, that is, implement the generalized X_a gates (Fig. 2).

Fortunately, most of the candidate systems for encoding quantum information naturally offer multi-level structures that are readily accessible. For example, the photon has a large number of degrees of freedom including polarization, transverse spatial mode, arrival time, photon number and frequency. Coherent control over and between many of these dimensions has already been demonstrated and shown to offer significant advantages in a range of applications such as quantum communication and measurement[18,19]. Trapped ions also offer readily accessible levels including multiple electronic and vibrational modes. Indeed, both linear optic[20] and trapped-ion[21,22] quantum computing architectures already routinely use multi-level systems to implement two-qubit gates and realize universal gate sets. Clearly the tools are available to exploit our technique, the benefits of which lie at the next level of construction—building large quantum circuits.

An immediate benefit of a significant reduction in the number of two-qubit gates required for quantum circuits is an equally significant speed-up in processing time. This has particular advantages in the many cases where short coherence times are an obstacle in the path to scalability. Furthermore, as we illustrate in the next section, our technique brings a whole range of logic circuits

ARTICLES NATURE PHYSICS DOI: 10.1038/NPHYS1150

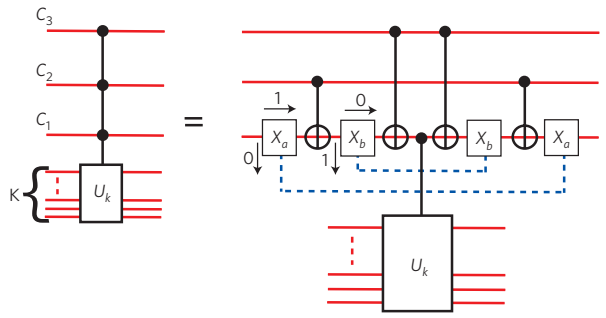


Figure 4 | Efficiently adding control qubits to an arbitrary controlled circuit. Circuit for a three-control-qubit unitary acting on k qubits, c^3u_k. Given the ability to carry out a single instance of a c^1u_k, n extra control qubits can be added at a cost of an extra $2n$ two-qubit gates and an extra n levels in C_1. The X_j perform as described in the caption of Fig. 2. The control operation occurs if $|C_3, C_2, C_1\rangle = |\mathbf{1},\mathbf{1},\mathbf{1}\rangle$.

within reach of current technology, enabling the implementation and exploration of new circuits in the laboratory.

Demonstration in a linear optical architecture

Here, we present an implementation of the Toffoli and the c^1u, using photons to encode information and linear optics to construct the component quantum logic gates (see the Methods section). We acknowledge previous demonstrations of a Toffoli gate in liquid state NMR, which do not exploit our resource-saving technique[13,23–26]. Our demonstration uses two-qubit gates, the successful operation of which is indicated by detection of one photon in each of the spatial output modes[3,27–30]. Such gates are high performing, well characterized, offer fast gate speeds and have several known paths to scalable quantum computing[20,31–33]. We note that our resource-saving technique is fundamentally different from and potentially complementary to the numerous linear optics schemes for reducing the overhead associated with generating a universal resource[34–36]; here, we are concerned with reducing the amount of that resource required to build circuits.

Figure 5 shows schematic diagrams of our experiment (see the Methods section). Key steps are the expansion of the Hilbert space of the target information carrier (T), effected by the first polarizing beamsplitter (PBS1), and contraction back into the original space, effected by the components in the dashed rectangle. Before PBS1, we have a two-level system in the target rail with logical states $|\mathbf{H}\rangle = |0\rangle$ and $|\mathbf{V}\rangle = |1\rangle$ (horizontal and vertical photon polarization). PBS1 then moves information encoded in the logical $|\mathbf{H}\rangle$ state into a separate spatial mode, which bypasses the subsequent two-qubit gates. After PBS1, we have access to a four-level system; two levels in the top rail (t) and two in the bottom rail (b), with logical basis states $|\mathbf{H},\mathbf{t}\rangle$, $|\mathbf{V},\mathbf{t}\rangle$, $|\mathbf{H},\mathbf{b}\rangle$ and $|\mathbf{V},\mathbf{b}\rangle$, respectively. Although we need to use only one of the extra levels in the bottom rail to enact our technique, we use both in our experiment simply to balance optical path lengths. The contraction back into the original two-level polarization qubit is carried out non-deterministically, that is, given deterministic two-qubit gates, measurement of a single photon at D1 heralds a successful run of the gate. This enables a demonstration of the Toffoli and c^1u without the last CNOT in

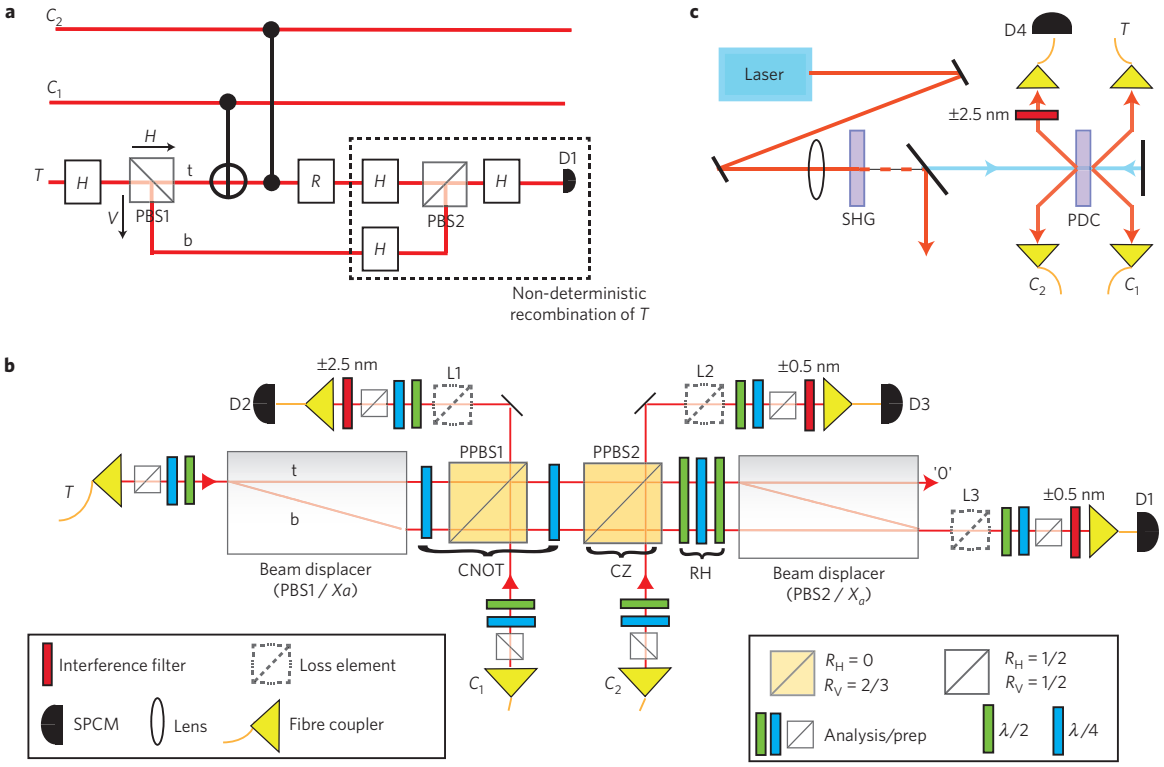


Figure 5 | Toffoli and controlled-unitary experimental layout. a, Conceptual logic circuit. A polarizing beam splitter temporarily expands the Hilbert space of the target information carrier, from a polarization-encoded photonic qubit to a multi-level system distributed across polarization and longitudinal spatial mode. Information in the bottom rail (b) bypasses the two-qubit gates. Detection of a photon at D1 heralds a successful implementation. R = I (the identity) implements a Toffoli. R = Z_θ (see Fig. 1) implements a c^1u between C_1 and T (in this case, no photon is injected into C_2). **b**,**c**, Experimental circuit and optical source (see the Methods section). We use an inherently stable polarization interferometer using two calcite beam displacers[3]. PPBS, partially polarizing beam splitter; SPCM, single-photon counting module; PDC, parametric downconversion; SHG, second-harmonic generation.

NATURE PHYSICS DOI: 10.1038/NPHYS1150

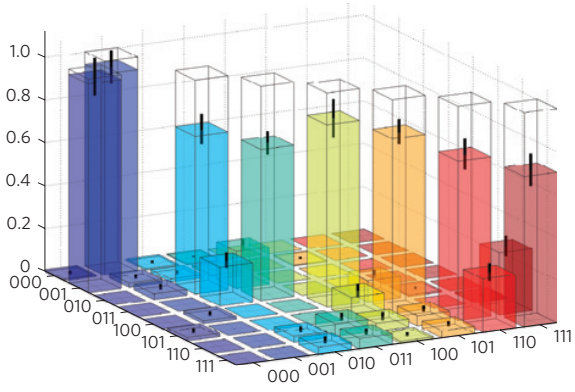


Figure 6 | Experimentally constructed Toffoli logical truth table. The labels on the *x* and *y* axes identify the state $|C_2, C_1, T\rangle$. Ideally, a flip of the logical state of the target qubit (T) occurs only when both control qubits (C_2 and C_1) are in the logical $|\mathbf{0}\rangle$ state. The ideal case is shown as a wire grid and the overlap is $\mathcal{I} = 0.81\pm0.03$ (see the Methods section). Error bars are shown representing one standard deviation, calculated from Poissonian photon-counting statistics. The table required four days of measurement.

Figs 1b and 3a, thereby making an implementation feasible with recent developments in linear optic quantum gates[37,38].

For our implementation of the Toffoli, we require four photons. We observe a fourfold coincidence rate at the output of our circuit of approximately 100 mHz when running at full pump laser power. Although this is not sufficient to carry out a full process tomography[27] of the gate over a practical time period, we are able to demonstrate all of the key aspects of its behaviour. The first step in our characterization is to test the classical action of the gate, that is, the ability to apply the correct operation to all eight logical input states. Figure 6 shows the experimentally reconstructed logical truth table. In the ideal case of our implementation, the target (T) undergoes a logical flip if, and only if, both control qubits are in the logical $|\mathbf{0}\rangle$ state. We measure a good overlap between the ideal and measured truth tables[39] of $\mathcal{I}=0.81\pm0.03$, compared with 0.84 and 0.85 achieved for the original optical implementations of two-qubit gates[3,30]. This is a comprehensive test of the classical action of our gate.

The next step is to test the quantum action of the gate, that is, the ability to apply the correct operation to input superposition states. At our count rates, we are not able to test a tomographically complete set required for a full process characterization, over a practical time period. Our concession is to test the most experimentally challenging and functionally important cases. They are challenging because they require coherent interaction between all three qubits and, in two cases, ideally generate maximally entangled Bell states[12]. They are functionally important because they demonstrate the gates ability to generate and control a large amount of entanglement. This is of fundamental importance to the advantages offered by a universal quantum computer[40] and is a standard figure of merit[3–6]. In the ideal case: with an input state of $|\mathbf{0}, (\mathbf{0}+\mathbf{1}), \mathbf{0}\rangle/\sqrt{2}$, our Toffoli will produce the entangled state $|\mathbf{0}, \Psi_+\rangle$, where $|\Psi_+\rangle$ is the maximally entangled Bell state[12] $(|\mathbf{0},\mathbf{0}\rangle+|\mathbf{1},\mathbf{1}\rangle)/\sqrt{2}$; with an input state of $|C_2, C_1, T\rangle=|\mathbf{1}, (\mathbf{0}+\mathbf{1}), \mathbf{0}\rangle/\sqrt{2}$, it will produce the separable output state $|\mathbf{1}, (\mathbf{0}+\mathbf{1}), \mathbf{0}\rangle/\sqrt{2}$. In the former (latter) case, the entangling operation between C_1 and T is coherently turned on (off) by C_2. We then swap the roles of the control qubits and repeat the test. We carry out over-complete full state tomography to reconstruct the density matrix of two-qubit output states, while projecting the remaining qubit into its input state (see the Methods section).

Figure 7 shows the experimentally reconstructed density matrices representing the state of a control and target qubit, at

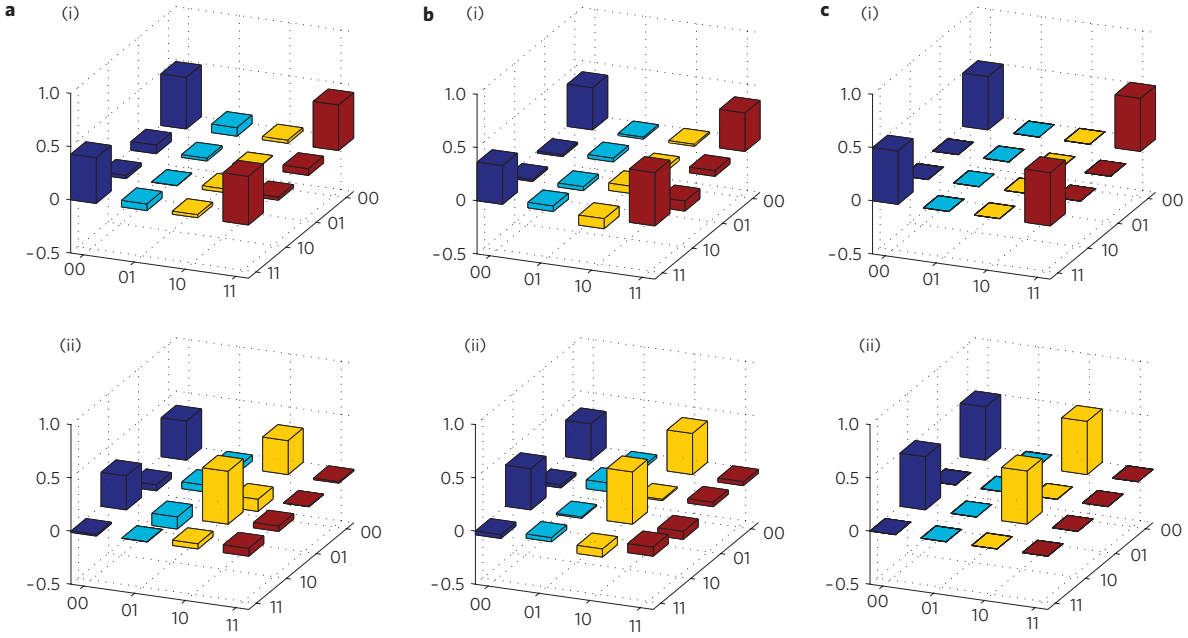


Figure 7 | Experimentally reconstructed Toffoli output density matrices. a, Measured output states of qubits C_1 and T for Toffoli gate inputs; (i) $|\mathbf{0}, (\mathbf{0}+\mathbf{1}), \mathbf{0}\rangle/\sqrt{2}$; and (ii) $|\mathbf{1}, (\mathbf{0}+\mathbf{1}), \mathbf{0}\rangle/\sqrt{2}$. We observe fidelities with the ideal states, linear entropies and tangles[39] of (i) {0.90±0.04, 0.21±0.08, 0.68±0.10} and (ii) {0.75±0.06, 0.47±10, 0.04±0.06}, respectively. **b**, As for **a**, but where the roles of C_1 and C_2 have been swapped. We now observe (i) {0.81±0.02, 0.39±0.05, 0.53±0.07} and (ii) {0.80±0.03, 0.40±0.05, 0.01±0.01}. The decrease in tangle in the (i) cases reflects the difference between dependent and independent photon interference, as discussed in the text. **c**, Ideal density matrices. Note, in all cases only real parts are shown; imaginary parts are small. Each density matrix requires 36 separate measurements[28] and takes approximately three days to complete.

ARTICLES NATURE PHYSICS DOI: 10.1038/NPHYS1150

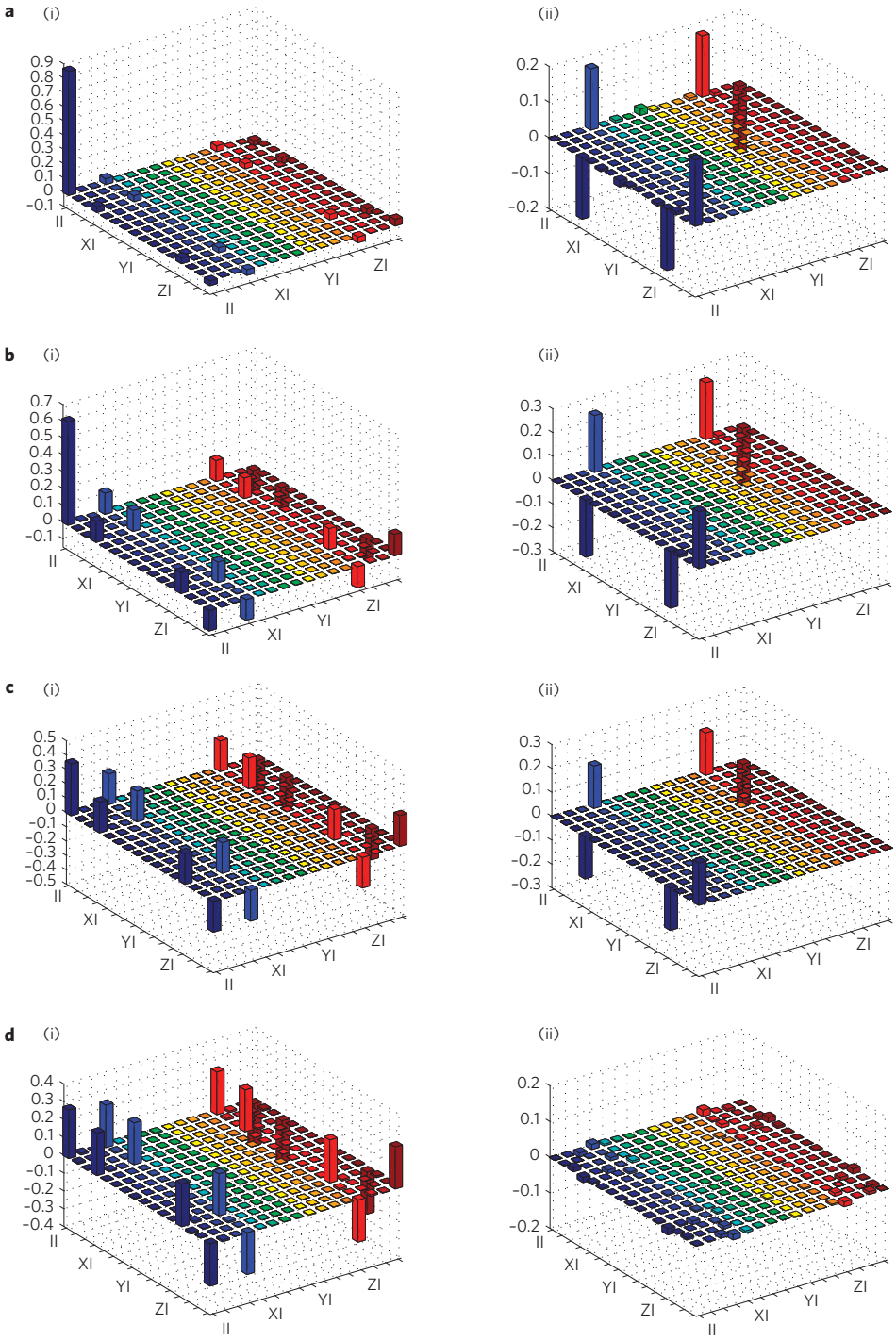


Figure 8 | Experimentally reconstructed controlled-unitary gate process matrices. a–d, $u=Z_\theta$ and $\theta=\pi/4$ (CT) (**a**), $\theta=\pi/2$ (CJ) (**b**), $\theta=3\pi/4$ (CL) (**c**) and $\theta=\pi$ (CZ) (**d**). (i) Real and (ii) imaginary parts are shown. We observe high process fidelities[27] with the ideal {0.982±0.003, 0.977±0.004, 0.940±0.006, 0.956±0.003} and low average output-state linear entropies {0.036±0.004, 0.047±0.004, 0.091±0.005, 0.086±0.006}, respectively. Matrices are presented in the standard Pauli basis[27].

the output of our Toffoli gate. We achieve a high fidelity[39] with the ideal states and a high level of entanglement, as detailed in the figure caption. The results show that the Toffoli carries out its most important and experimentally challenging quantum operations with high fidelity and entanglement.

To discuss sources of experimental imperfection, we look at the details of our linear optic implementation. A key requirement for correct operation of each component two-qubit gate is perfect relative non-classical interference visibility (V_r) between two photons. This in turn requires perfectly indistinguishable single photons. We measure $V_r=100\pm1\%$ and $V_r=92\pm4\%$ for the first and second two-qubit gates shown in Fig. 5, respectively (where $V_r=V_{meas}/V_{ideal}$, $V_{ideal}=80\%$ and results are for vertically polarized photons). The difference can be understood

by considering that the former operates on a 'dependent' pair of photons generated from the same pass of our optical source, whereas the latter uses 'independent' photons from different passes (Fig. 5c). Photons generated from different passes are intrinsically more distinguishable[41,42]. Another contribution to experimental imperfection are the cases when more than one pair of photons is created simultaneously in a single pass of our optical source. Although these 'higher-order terms' occur with very low probability, and do not significantly affect the visibility measurement due to higher-order interference processes, they can introduce a significant error in the gate operation[42].

In general, imperfections in the measured Toffoli truth table correspond to unwanted flips of the target qubit (Fig. 6). These can be understood with reference to the non-classical interferences required for correct operation in each case. To better illuminate these effects, we define a standard contrast $\mathcal{C}$ (see the Methods section), which gauges our gate's ability to apply the correct operation to a subset of logical input states. For inputs $|C_2, C_1\rangle = |\mathbf{0}, \mathbf{0}\rangle$, no non-classical interference is required for correct operation and we measure $\mathcal{C} = 0.99 \pm 0.01$, averaged over both target logical input states. Inputs $|C_2, C_1\rangle = |\mathbf{0}, \mathbf{1}\rangle$ require perfect non-classical interference between dependent photons C_1 and T, for ideal operation. We achieve a near-perfect interference visibility between vertical photons in this case. However, the full process suffers from the higher-order photon terms. This is reflected in an average of $\mathcal{C} = 0.95 \pm 0.02$. Inputs $|C_2, C_1\rangle = |\mathbf{1}, \mathbf{0}\rangle$ require perfect non-classical interference between independent photons C_2 and T, for ideal operation, reflected in an average of $\mathcal{C} = 0.80 \pm 0.02$. Inputs $|C_2, C_1\rangle = |\mathbf{1}, \mathbf{1}\rangle$ require perfect non-classical interference between both dependent and independent photons, and are therefore the most challenging cases. Here, we observe an average of $\mathcal{C} = 0.73 \pm 0.05$.

It is straightforward to show that the ratio of single to double photon-pair emission is proportional to the pump power. Thus, reducing the power by a factor of four should reduce these unwanted higher-order contributions from our source by a factor of four from each pass. Under these conditions, we observe a fourfold rate at the output of the Toffoli gate of only ~1 mHz and repeat measurement of the average contrast for the most challenging logical input $|C_2, C_1\rangle = |\mathbf{1}, \mathbf{1}\rangle$, over a period of five days. We observe a clear improvement from $\mathcal{C} = 0.73 \pm 0.05$ to $\mathcal{C} = 0.83 \pm 0.04$. The effects of photon distinguishability and higher-order terms also cause the imperfections in the state tomographies of Fig. 7. For example, the entangling process required to achieve Fig. 7a(i) relies on interference between dependent photons. The process required to achieve Fig. 7b(i) relies on both dependent and independent photon interference. This leads to the reduced fidelity observed in the latter case. We conclude that the dominant source of experimental error lies in our imperfect photon source.

Our implementation of the $\mathrm{c^1u}$ requires the generation of two photons (Fig. 5). Even when running at 1/4 power, we observe approximately 100 Hz, which is sufficient to carry out full process tomography[27] in ~2 h. As a demonstration, we report the implementation of four distinct $\mathrm{c^1u}$ gates that apply z_θ rotations (Fig. 1) of $\pi/4$ (cT), $\pi/2$ (cJ), $3\pi/4$ (cL) and π (cZ) to the target (T) conditional on the control (C_1), respectively. We fully characterize these gates through quantum process tomography[27]: Fig. 8 shows the experimentally reconstructed process matrices. We achieve exceptionally high process fidelities, as detailed in the figure caption. We attribute the small deviations from ideal operation to residual higher-order emissions, imperfect mode matching and manufactured optics[41,42].

Outlook

A clear implication of our work is that using multi-level quantum systems to encode information, rather than enforcing a two-level structure, can offer significant practical advantages for quantum logic. Although our demonstration enabled new photonic quantum circuits, the resource-saving technique has the potential for application in many other architectures, bringing new circuits within reach of experimental realization. An important path for further research is to look for other practical simplifications to quantum logic that may be possible by enabling simple steps outside the qubit Hilbert space. The overriding sources of error in our demonstrations lie in our imperfect photon source: both the effects of photon distinguishability and the presence of unwanted higher-order emissions from parametric downconversion. Current developments in source technology promise significant improvements in the near future. The combination of this with recently developed photon-number resolving detectors offers paths to deterministic and scalable implementations of our gates. A key result is that it is possible to overcome inherent non-determinism using only a polynomial overhead in resources[20]. Other important next steps are to use our circuits to explore small-scale quantum algorithms, generate new states and test error-correction schemes.

During the preparation of this manuscript, we became aware of a demonstration of the Toffoli gate with trapped ions[43].

Methods

Source. Forward and backward photons pairs are produced through spontaneous parametric downconversion of a frequency-doubled mode-locked Ti:sapphire laser (820 nm → 410 nm, $\Delta\tau = 80$ fs at 82 MHz repetition rate) double passed through a type-I 2 mm BiB_3O_6 crystal (Fig. 5). Photons are collected into four single-mode optical fibres and detected using fibre-coupled non-number-resolving photon-counting modules. We spectrally filter using unblocked interference filters centred at 820 ± 0.5 nm.

Circuit. Photons are injected from single-mode optical fibres into free space and coupled into single-mode fibres at the outputs (Fig. 5). One-qubit gates are realized deterministically using birefringent wave plates. Two-qubit gates are realized non-deterministically using an established technique based on non-classical interference at partially polarizing beamsplitters in combination with coincident measurement[28–30]. Rather than directly chaining the two-qubit gates required for the Toffoli (Fig. 5a), we use a recently developed three-qubit quantum logic gate[37,38]. In linear optics implementations of two-qubit quantum gates, state-dependent loss is used to rebalance amplitudes[28–30]. When incorporating loss elements L1–3 (L1), the Toffoli ($\mathrm{c^1u}$) operates with a success probability of 1/72 (1/18) (Fig. 5). Alternatively, to combat low count rates, we achieve correct balance by removing extra loss elements and pre-biasing the input polarization states during gate characterization[28–30]. For the Toffoli, we use all four outputs from spontaneous parametric downconversion—a fourfold coincident measurement between detectors D1–4 signals a successful run. We measure a fourfold coincidence rate of approximately 100 mHz when running at full pump laser power and 1 mHz at 1/4 power. For the $\mathrm{c^1u}$, we use only outputs C_1 and T. In this case, a twofold coincident measurement between detectors D1–2 signals a successful run. We measure a twofold coincidence rate of approximately 100 Hz when running at 1/4 pump laser power. Our imperfectly manufactured beamsplitters impart systematic unitary operations on the optical modes. For simplicity, we corrected for these effects numerically. Alternatively, such unitaries could be corrected with standard wave plates.

Quality measures and statistics. All error analysis is carried out using a Poissonian distribution to describe the uncertainty in non-number-resolving photon counting. Our state and process tomography uses maximum likelihood estimation to reconstruct physical states and Monte Carlo simulation for error analysis[27,39,44]. Measurements sets are taken iteratively, whereby multiple sets—each taking around 1 h to complete—are recorded. This reduces the effect of optical source power fluctuations. The overlap between two truth tables—or inquisition ($\mathcal{I}$)—is defined as the average logical state fidelity of a truth table $\mathcal{I} = \mathrm{Tr}(\mathrm{M_{exp}M_{ideal}})/d$, where $\mathrm{M_{exp}}$ and $\mathrm{M_{ideal}}$ are the measured and ideal truth tables, and d is the table dimension[39]. The standard fidelity between a mixed (measured) matrix, ρ, and the pure (ideal) matrix (either two states or two processes) is $\mathrm{F} = \langle\Psi|\rho|\Psi\rangle$; linear entropy is $\mathrm{s_L} \equiv d(1-\mathrm{Tr}[\rho^2])/(d-1)$, where d is the state dimension[39]. For the purposes of our error analysis, we define the contrast $\mathcal{C} = 1/2\{1 + (\mathrm{p_{ideal}} - \mathrm{p_{flip}})/(\mathrm{p_{ideal}} + \mathrm{p_{flip}})\}$, where $\mathrm{p_{ideal}}$ is the probability of obtaining the ideal output state and $\mathrm{p_{flip}}$ is the probability of obtaining the output state where the ideal target qubit output state has been flipped. We calculate this property directly from the measured truth table.

ARTICLES NATURE PHYSICS DOI: 10.1038/NPHYS1150

Received 1 February 2008; accepted 27 October 2008; published online 7 December 2008

References

1. Schmidt-Kaler, F. *et al.* Realization of the Cirac–Zoller controlled-NOT quantum gate. *Nature* **422**, 408–411 (2003).
2. Leibfried, D. *et al.* Experimental demonstration of a robust, high-fidelity geometric two ion-qubit phase gate. *Nature* **422**, 412–415 (2003).
3. O'Brien, J. L., Pryde, G. J., White, A. G., Ralph, T. C. & Branning, D. Demonstration of an all-optical quantum controlled-NOT gate. *Nature* **426**, 264–267 (2003).
4. Gasparoni, S., Pan, J.-W., Walther, P., Rudolph, T. & Zeilinger, A. Realization of a photonic controlled-NOT gate sufficient for quantum computation. *Phys. Rev. Lett.* **93**, 020504 (2004).
5. Pittman, T. B., Fitch, M. J., Jacobs, B. C. & Franson, J. D. Experimental controlled-NOT logic gate for single photons in the coincidence basis. *Phys. Rev. A* **68**, 032316 (2003).
6. Bao, X.-H. *et al.* Optical nondestructive controlled-NOT gate without using entangled photons. *Phys. Rev. Lett.* **98**, 170502 (2007).
7. Steffen, M. *et al.* Measurement of the entanglement of two superconducting qubits via state tomography. *Science* **313**, 1423–1425 (2006).
8. Plantenberg, J. H., de Groot, P. C., Harmans, C. J. P. M. & Mooij, J. E. Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits. *Nature* **447**, 836–839 (2007).
9. Mandel, O. *et al.* Controlled collisions for multi-particle entanglement of optically trapped atoms. *Nature* **425**, 937–940 (2003).
10. Anderlini, M. *et al.* Controlled exchange interaction between pairs of neutral atoms in an optical lattice. *Nature* **448**, 452–456 (2007).
11. Ralph, T. C., Resch, K. J. & Gilchrist, A. Efficient Toffoli gates using qudits. *Phys. Rev. A* **75**, 022313 (2007).
12. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge Univ. Press, 2000).
13. Cory, D. G. *et al.* Experimental quantum error correction. *Phys. Rev. Lett.* **81**, 2152–2155 (1998).
14. Dennis, E. Toward fault-tolerant quantum computation without concatenation. *Phys. Rev. A* **63**, 052314 (2001).
15. Shi, Y. Both Toffoli and controlled-NOT need little help to do universal quantum computation. *Quantum Inform. Comput.* **3**, 84–92 (2003).
16. Aspuru-Guzik, A., Dutoi, A. D., Love, P. J. & Head-Gordon, M. Simulated quantum computation of molecular energies. *Science* **309**, 1704–1707 (2005).
17. Shor, P. *Proc. 35th Ann. Symp. Found. Comp. Sci.* 124–134 (IEEE Comp. Soc. Press, 1994).
18. Kwiat, P., Mitchell, J. R., Schwindt, P. & White, A. Grover's search algorithm: An optical approach. *J. Mod. Opt.* **47**, 257–266 (2000).
19. Schuck, C., Huber, G., Kurtsiefer, C. & Weinfurter, H. Complete deterministic linear optics Bell state analysis. *Phys. Rev. Lett.* **96**, 190501 (2006).
20. Knill, E., Laflamme, R. & Milburn, G. J. A scheme for efficient quantum computation with linear optics. *Nature* **409**, 46–52 (2001).
21. Roos, C. F. *et al.* Control and measurement of three-qubit entangled states. *Science* **304**, 1478–1480 (2004).
22. Cirac, J. I. & Zoller, P. Quantum computations with cold trapped ions. *Phys. Rev. Lett.* **74**, 4091–4094 (1995).
23. Cory, D. G., Price, M. D. & Havel, T. F. Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing. *Physica D* **120**, 82–101 (1998).
24. Braunstein, S. L. *et al.* Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.* **83**, 1054–1057 (1999).
25. Menicucci, N. C. & Caves, C. M. Local realistic model for the dynamics of bulk-ensemble NMR information processing. *Phys. Rev. Lett.* **88**, 167901 (2002).
26. Jones, J. NMR quantum computation: A critical evaluation. *Fortschritte der Physik* **48**, 909–924 (2000).
27. O'Brien, J. L. *et al.* Quantum process tomography of a controlled-NOT gate. *Phys. Rev. Lett.* **93**, 080502 (2004).
28. Langford, N. K. *et al.* Demonstration of a simple entangling optical gate and its use in Bell-state analysis. *Phys. Rev. Lett.* **95**, 210504 (2005).
29. Kiesel, N., Schmid, C., Weber, U., Ursin, R. & Weinfurter, H. Linear optics controlled-phase gate made simple. *Phys. Rev. Lett.* **95**, 210505 (2005).
30. Okamoto, R., Hofmann, H. F., Takeuchi, S. & Sasaki, K. Demonstration of an optical quantum controlled-NOT gate without path interference. *Phys. Rev. Lett.* **95**, 210506 (2005).
31. O'Brien, J. L. Optical quantum computing. *Science* **318**, 1567–1570 (2007).
32. Kok, P. *et al.* Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.* **79**, 135–174 (2007).
33. Nielsen, M. A. Optical quantum computation using cluster states. *Phys. Rev. Lett.* **93**, 040503 (2004).
34. Yoran, N. & Reznik, B. Deterministic linear optics quantum computation with single photon qubits. *Phys. Rev. Lett.* **91**, 037903 (2003).
35. Ralph, T. C., Hayes, A. J. F. & Gilchrist, A. Loss-tolerant optical qubits. *Phys. Rev. Lett.* **95**, 100501 (2005).
36. Browne, D. E. & Rudolph, T. Resource-efficient linear optical quantum computation. *Phys. Rev. Lett.* **95**, 010501 (2005).
37. Lanyon, B. P. *et al.* Experimental demonstration of a compiled version of Shor's algorithm with quantum entanglement. *Phys. Rev. Lett.* **99**, 250505 (2007).
38. Ralph, T. C. Scaling of multiple postselected quantum gates in optics. *Phys. Rev. A* **70**, 012312 (2004).
39. White, A. G. *et al.* Measuring two-qubit gates. *J. Opt. Soc. Am. B* **24**, 172–183 (2007).
40. Vidal, G. Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.* **91**, 147902 (2003).
41. Rarity, J., Tapster, P. & Loudon, R. *Quantum Interferometry* (VCH, 1996).
42. Weinhold, T. J. *et al.* Understanding photonic quantum-logic gates: the road to fault tolerance. Preprint at <http://arxiv.org/abs/0808.0794> (2008).
43. Monz, T. *et al.* Realization of the quantum Toffoli gate with trapped ions. Preprint at <http://arxiv.org/abs/0804.0082> (2008).
44. James, D. F. V., Kwiat, P. G., Munro, W. J. & White, A. G. Measurement of qubits. *Phys. Rev. A* **64**, 052312 (2001).

Acknowledgements

We acknowledge discussions with W. Munro and D. Kielpinski, and financial support from the Australian Research Council Discovery and Federation Fellow programmes, the DEST Endeavour Europe and International Linkage programmes, and an IARPA-funded US Army Research Office Contract.

Additional information

Reprints and permissions information is available online at http://npg.nature.com/reprintsandpermissions. Correspondence and requests for materials should be addressed to B.P.L.

1.1 Contribution statement

The author made the following contributions to this work:

- Experimental design and construction of the Toffoli gate
- Design and construction of the controlled-unitary gate (in collaboration with MB, MPA, TJ and KJR)
- Preliminary and final data acquisition (in collaboration with MA and MB)
- Data analysis and interpretation
- Theoretical extensions (summarised in Fig. 3b and Fig. 4 of the paper)
- Figure construction
- Complete first draft of the paper
- Final draft of the paper (in collaboration with all authors)
- Paper submission and corresponding author duties
- Complete first draft of referee replies and corresponding paper revision
- Final revision (in collaboration with all authors)

1.2 Erratum

There are two mistakes in Figure 5b of the paper, which shows the experimental layout. Firstly the reflectivity of the polarising beam splitter (white, solid-line rectangles) is mislabeled in the key and should read R_H=0, R_V=1. Secondly, the colour of the wave plates is the wrong way around in the key. i.e. the half-wave plate ($\lambda/2$) should be blue and the quarter-wave plate ($\lambda/4$) should be green. A corrected version is included in Fig. 1.2 of this thesis.

1.3 Additional experimental details

Due to space limitations, Fig. 5b of the paper shows a single experimental diagram incorporating both the Toffoli and controlled-unitary (CU) gates. While this does contain all the information required to reconstruct each gate, it is a little condensed. To aid in clear understanding, separate representations (conceptual, schematic and photographic) of both gates are shown in Figures 1.2 and 1.3 of this thesis, respectively. Each gate was implemented using a separate optical circuit in the laboratory.

Correct operation of the Toffoli can be confirmed by checking that the conceptual circuit in Fig. 1.2a performs the desired operation on the 8 possible logical input states ($|C1, C2, T\rangle = |000\rangle, |001\rangle, ..., |111\rangle$). Before doing so it is useful to be aware of the identity shown in Fig. 1.1.

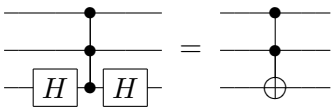


Figure 1.1: Hadamards convert a Toffoli-sign into a Toffoli.

The 3-qubit gate sandwiched between the 1-qubit Hadamard gates, on the left of Figure 1.1, is a 'Toffoli-sign'. In the computational basis the matrix representation of this gate is

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix} \tag{1.1}$$

i.e. the only change is to put a minus sign on the basis state $|111\rangle$. In fact, it does not much matter which basis state gets the minus sign (as long as it is only one basis state) as any case can be converted to a Toffoli-sign by either relabeling the logic or using single qubit bit-flip gates. As a consequence of this identity one can ignore the first and last Hadamards on the target rail (T) of Fig. 1.2a and just check that the circuit in between performs the Toffoli-sign operation, which is much easier. Simple inspection of this part shows that only in the case $|C2, C1, T\rangle = |1, 0, 1\rangle = |V, H, V\rangle$ does a minus sign occur.

Note that Fig. 1.3a shows how to perform an arbitrary controlled-Z_θ operation. This is equivalent to a controlled-unitary with the addition of only two 1-qubit operations, as described in Fig. 3a of the paper. The action of the controlled-Z_θ operation, in the logical basis is

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix} \tag{1.2}$$

i.e. the only change is to put a phase shift $e^{i\theta}$ on the basis state $|11\rangle$. Again, and for the same reasons as before, it does not matter which logical state gets the phase shift. Simple inspection of Fig. 1.3a shows that only the logical basis state $|C1, T\rangle = |1, 0\rangle = |V, H\rangle$ undergoes a phase shift.

Fig. 1.3c shows a series of wave plates implementing the operation $HZ_\theta H$. The way that we did this is worth noting, since it makes the gate far easier to use than might otherwise be possible. We employed a quarter-half-quarter wave plate combination, with the quarter-waveplates set at their optic axes. In this way varying the central half-waveplate corresponds to altering θ directly.

Consider Fig. 1.2. With high probability, successful operation of our Toffoli gate is post-selected when all detectors D1-D4 record a detection event simultaneously (within a 10 ns window). With high probability this selects those cases where only 4 photons were generated by PDC—a pair from each pass of the PDC crystal. These events occur with the same probability as two pairs from one pass and none from the other. However, those events cannot cause all four detectors to fire—hence they do no generate 'false positives' and therefore degrade gate performance (correct gate operation requires a single photon in each input and output mode). The first higher order PDC events that can cause 'false positives' are two pairs in one arm and a single pair in the other (i.e. a six fold event). As discussed in the paper the ratio of 4 to 2 photon events in any one arm can be reduced by reducing the pump power, thereby reducing the probability of 4+2 photon events.

The experimental figures showing the Toffoli and CU in the paper and this section include 'loss elements', and in the Methods section of the paper we talk about 'removing them to improve gate success probability'. We now explain what this means in more detail. Essentially the operation of all of our gate involves a sign change occurring on only logical input state (i.e. $|HH\rangle$, and not $|HV\rangle$, $|VH\rangle$, or $|VV\rangle$). This is achieved, in part, by using a partially polarising beam splitter that is perfectly reflective (or transmissive) for one polarisation, say H, and imperfectly reflective (transmissive) for the other polarisation,

V. This means that the probability of single photons leaving in separate output ports is higher for input states with V polarisation than those with H polairsation i.e. we have an input state dependent gate success probability (when measured in coincidence). In order to balance these out we can include additional partially polarising beam splitters that throw away (filter out) the extra V polarisation to bring everything to balance. Hence, these are called loss elements. If we want these gates to form part of some circuit where the output of one feeds into the other, we don't want a state dependent operation probability. However, for the purposes of characterising these gates on their own, we remove these loss elements , which allows us to characterise the gate operation with greater count rates.

The characterisation technique employed is to 'pre-bias' the input states when necessary. This technique was pioneered by Okamoto *et al* [OHTS05] in 2005. The only purpose of the loss elements is to reduce the amplitude of the vertical component of single photons by $1/\sqrt{3}$ of the original input value, while leaving the horizontal component unchanged. Therefore, we can easily simulate this function by using compensated input state whose vertical component is reduced to $1/\sqrt{3}$. To simulate a general input state $|\psi_{effective}\rangle = c_H |H\rangle + c_V |V\rangle$ we thus use a compensated input state of $|\psi_{comp}\rangle = c_H |H\rangle + c_V/\sqrt{3} |V\rangle$. So, instead of reducing the count rate by throwing away some vertical polarisation away, we balance the states by sending in the equivalent extra horizontal polarisation. This technique can always be used instead of implementing loss elements that are simply at the output of a circuit, but no when the elements are internal in the circuit.

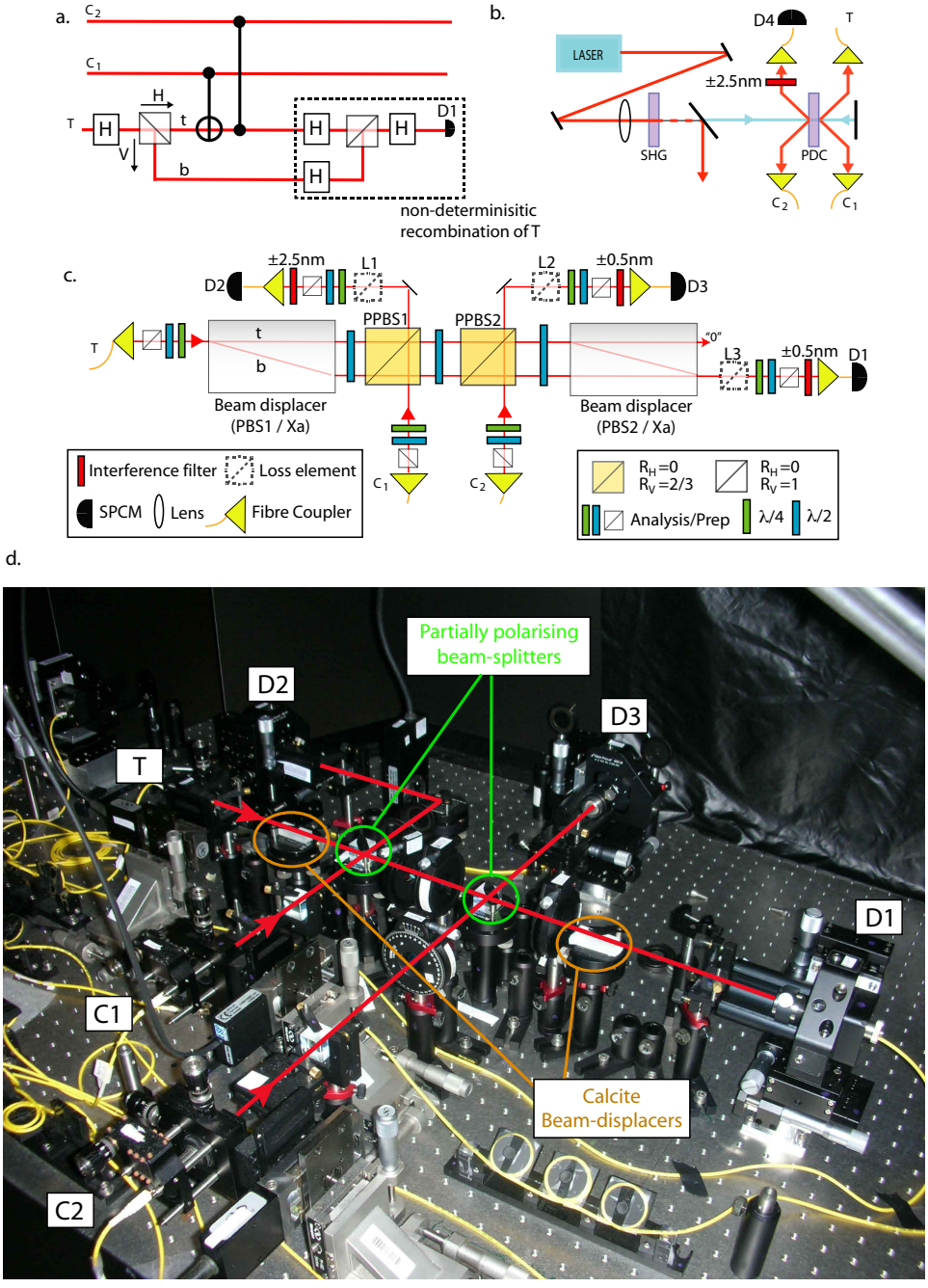


Figure 1.2: **Schematics of the Toffoli gate**. **a**. Conceptual circuit, **b**. Optical source, and **c**. Optical circuit diagrams. **d**. Annotated laboratory photograph of the optical circuit. The tilted waveplate in the gate's centre corrects for birefringent effects in PPBS1, which caused undesirable polarisation rotations. For clearer viewing, many of the preparation/analysis waveplates have been removed. The interference filters are also not shown. Photon detectors (SPCMs) are out of shot, but their corresponding fibre couplers are labelled. For more details see the caption of Fig. 5 in the corresponding paper. Some useful gate operations relevant to this figure are shown in Fig. 1.3 of this thesis. PPBS, partially polarizing beam splitter; SPCM, single-photon counting module; PDC, parametric downconversion; SHG, second-harmonic generation.

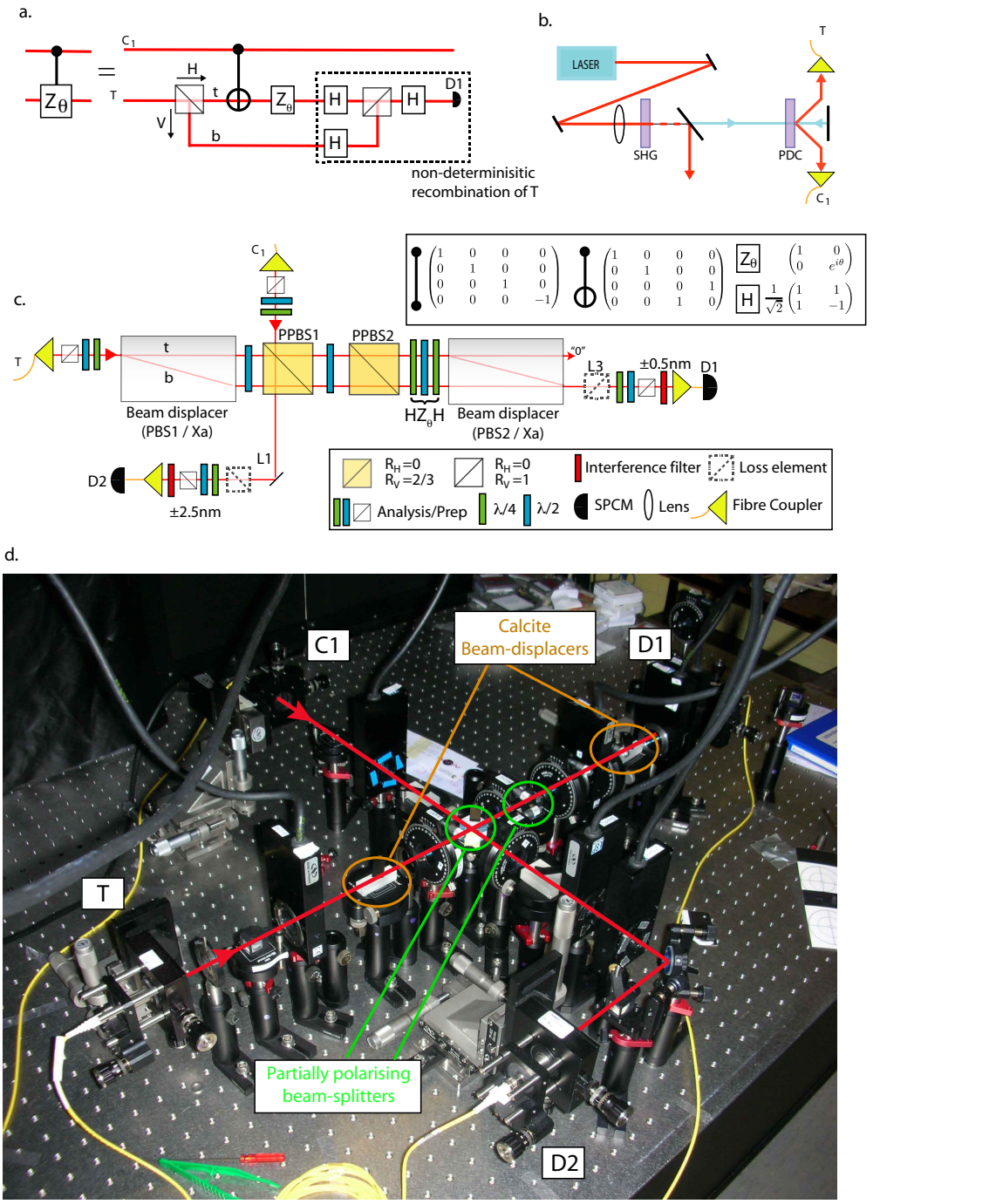


Figure 1.3: **Schematics of the controlled-unitary gate**. **a**. Conceptual circuit diagram. A controlled-Z_θ is equivalent to a controlled-unitary under the action of two 1-qubit gates, as shown in Fig. 3 of the corresponding paper. **b**. Optical source diagram. **c**. Optical circuit diagram. **d**. Annotated laboratory photograph of the optical circuit. Note that for clearer viewing many of the preparation/analysis waveplates have been removed. The interference filters are also not shown. The photon detectors (SPCMs) are out of shot, but their corresponding fibre couplers have been labelled. For more details see the caption of Fig. 5 in the corresponding paper. PPBS, partially polarizing beam splitter; SPCM, single-photon counting module; PDC, parametric downconversion; SHG, second-harmonic generation.

1.4 Unpublished extension

A circuit that turns up frequently in quantum computing consists of a single qubit controlling some unitary evolution on a large number of qubits (a qubit 'register'), as depicted in Fig. 1.4. For example, many instances of this circuit are required to implement the phase estimation algorithm [Kit95, NC01] (PEA), which in-turn is the corner-stone of a range of useful quantum algorithms, like Shor's factoring algorithm [Sho94, NC01].

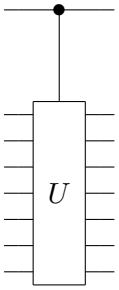


Figure 1.4: A common circuit in quantum computing: unitary operation U is implemented on a qubit register, conditional on the logical state of a single control qubit.

In the circuit model of quantum computing the arbitrary evolution U is implemented by a, usually very large, network of logic gates from a universal set. Given that we have a network that implements U how can we add a single control qubit? One approach is to simply add a control to every gate in the network for U, an example of which is shown in Fig. 1.5.

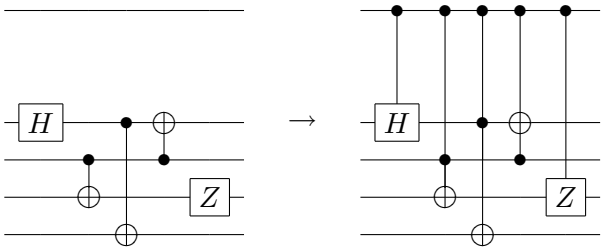


Figure 1.5: Example of how to condition a network of logic gates on the state of a single control qubit: add a control to each gate.

Following this scheme, each of these new controlled gates has to be decomposed into the original universal gate set. Adding a control to a 1-qubit gate (i.e. building a controlled-unitary) requires at least 2 CNOT's and 2 additional 1-qubit gates [NC01]. Adding a control to a CNOT (i.e. building a Toffoli gate) requires at least 6 extra CNOT's and 10 extra 1-qubit gates [NC01], when operating on qubits. Of course, this overhead could be

reduced somewhat by employing qutrits to simplify the Toffoli construction, as described in the published paper.

Figure 1.6 shows a technique that does better. Here, the information carriers in the register are four-level systems, with logical states $|0\rangle$, $|1\rangle$, $|2\rangle$ and $|3\rangle$. The action of a controlled-X_a gate is to move information from the bottom two 'qubit' levels of each carrier to the top two levels (i.e. perform the logical unitary operation $|0\rangle \rightarrow |2\rangle$, $|1\rangle \rightarrow |3\rangle$, $|2\rangle \rightarrow |0\rangle$, $|3\rangle \rightarrow |1\rangle$), conditional on the state of the single qubit. An additional requirement is that the logic gates implementing U apply the identity to the logical states $|2\rangle$ and $|3\rangle$.

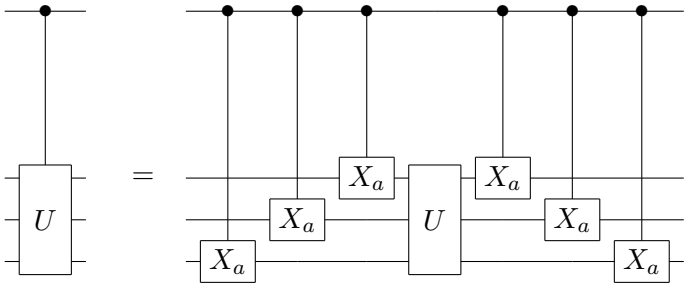


Figure 1.6: Proposed new method to couple an arbitrary circuit U to a single control qubit. The controlled-X_a gates are described in the text.

The result is that U is implemented only when the control qubit is in the logical 0 state, since when this qubit is a 1, all the information in the register is moved into part of the Hilbert space that is not affect by U. The final set of controlled-X gates simply brings the information back into the bottom qubit levels.

A resource count for this technique is simple. Besides access to four-level quantum information carriers, two controlled-X_a gates are required for each qubit involved in the U operation. The overhead is therefore *independent of the depth of* U, i.e. the number of gates that act on a fixed number of qubits. The technique is also independent of the U gate network itself, unlike the approach of adding controls to each gate, which would be different for each circuit.

1.5 Non-destructive photon number measurement.

Correct operation of the gates presented in this Chapter is heralded by a photon number measurement of the output modes. We have performed this measurement destructively. Figure 1.7 shows a way to perform it non-destructively, given two maximally entangled singlet states $|\Psi\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$, photon number resolving detectors D1-4 and the

ability to inject 1 (and only one) photon into each of the two input modes. Measurement of single photons in detectors D1-4 performs two tasks: firstly it guarantees that there was only a single photon in each output mode of the non-determinisitic logic gate (by a simple photon number counting argument); and secondly that the output state of the gate is teleported to the photons in the outer rails (see [BPM+97] for example). The measurements themselves are no different from simple teleportation protocols [BPM+97], but with the added insight that a photon number measurement is performed at the same time. Discounting the gate success probability, the scheme succeeds with a probability of 1/8 (1/4 for each teleportation), further increasing the non-determinism, but without destroying the qubits on successful heralding. Note that KLM [KLM01] proposed teleportation as a means to move the non-determinism 'off-line'. Here it is being used to perform a non-destructive photon number measurement.

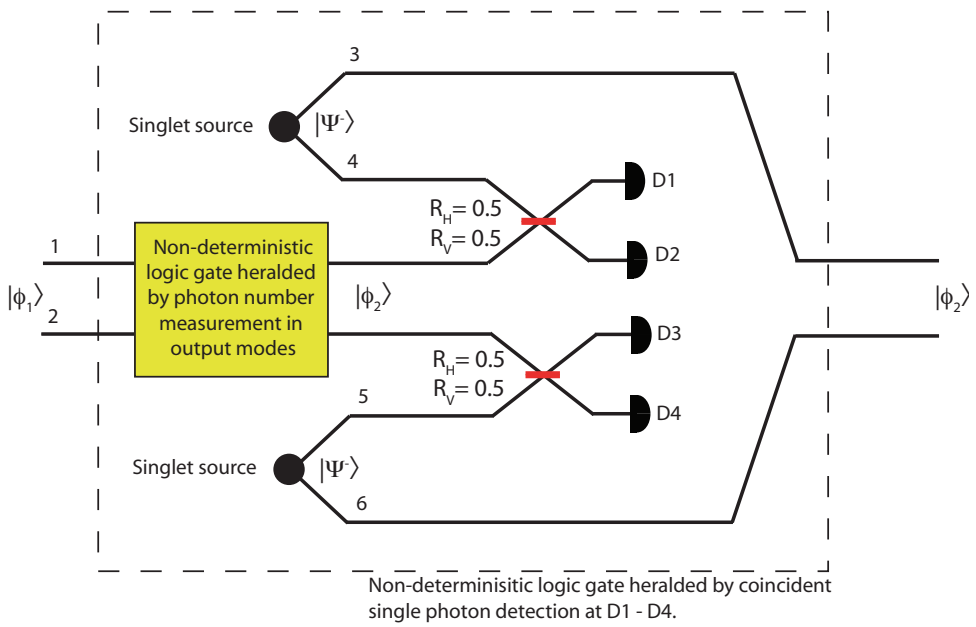


Figure 1.7: **Non-destructive linear optic gate**. Coincident single photon detection at D1-4 heralds a successful photon number measurement, and therefore correct, gate operation, without destroying the output photons. Consider that measurement of single photons at D1 and D2 is equivalent to projecting the photons in rails 1 and 4 into the singlet state, thereby teleporting the state of the photon in rail 1 to rail 3.

Part II

Implementing quantum algorithms

Chapter 2

Experimental demonstration of Shor's factoring algorithm

PRL **99,** 250505 (2007) PHYSICAL REVIEW LETTERS week ending 21 DECEMBER 2007

Experimental Demonstration of a Compiled Version of Shor's Algorithm with Quantum Entanglement

B. P. Lanyon,[1] T. J. Weinhold,[1] N. K. Langford,[1] M. Barbieri,[1] D. F. V. James,[2] A. Gilchrist,[1] and A. G. White[1]

[1]*Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane QLD 4072, Australia*

[2]*Department of Physics and Center for Quantum Information and Quantum Control, University of Toronto, Toronto ON M5S1A7, Canada*

(Received 18 May 2007; published 19 December 2007)

Shor's powerful quantum algorithm for factoring represents a major challenge in quantum computation. Here, we implement a compiled version in a photonic system. For the first time, we demonstrate the core processes, coherent control, and resultant entangled states required in a full-scale implementation. These are necessary steps on the path towards scalable quantum computing. Our results highlight that the algorithm performance is not the same as that of the underlying quantum circuit and stress the importance of developing techniques for characterizing quantum algorithms.

DOI: 10.1103/PhysRevLett.99.250505 PACS numbers: 03.67.Lx, 03.67.−a, 03.67.Mn, 42.50.Dv

As computing technology rapidly approaches the nanoscale, fundamental quantum effects threaten to introduce an inherent and unavoidable source of noise. An alternative approach embraces quantum effects for computation. Algorithms based on quantum mechanics allow tasks impossible with current computers, notably an exponential speedup in solving problems such as factoring [1]. Many current cryptographic protocols rely on the computational difficulty of finding the prime factors of a large number: a small increase in the size of the number leads to an exponential increase in computational resources. Shor's quantum algorithm for factoring composite numbers faces no such limitation, and its realization represents a major challenge in quantum computation.

To date, there have been demonstrations of entangling quantum-logic gates in a range of physical architectures, ranging from trapped ions [2,3], to superconducting circuits [4], to single photons [5–12]. Photon polarization experiences essentially zero decoherence in free space; uniquely, photonic gates have been fully characterized [6], produced the highest entanglement [8], and are the fastest of any architecture [11]. The combination of long decoherence time and fast gate speeds make photonic architectures a promising approach for quantum computation, where large numbers of gates will need to be executed within the coherence time of the qubits.

Shor's algorithm can factor a k-bit number using $72k^3$ elementary quantum gates; e.g., factoring the smallest meaningful number, 15, requires 4608 gates operating on 21 qubits [13]. Recognizing this is well beyond the reach of current technology, Ref. [13] introduced a compiling technique which exploits properties of the number to be factored, allowing exploration of Shor's algorithm with a vastly reduced number of resources. Although the implementation of these compiled algorithms does not directly imply scalability, it does allow the characterization of core processes required in a full-scale implementation of Shor's algorithm. Demonstration of these processes is a necessary step on the path towards scalable quantum computing. These processes include the ability to generate entanglement between qubits by coherent application of a series of quantum gates. In the only demonstration to date, a compiled set of gate operations were implemented in a liquid NMR architecture [14]. However, since the qubits are at all times in a highly mixed state [15], and the dynamics can be fully modeled classically [16], neither the entanglement nor the coherent control at the core of Shor's algorithm can be implemented or verified.

Here, we implement a compiled version of Shor's algorithm, using photonic quantum-logic gates to realize the necessary processes, and verify the resulting entanglement via quantum state and process tomography [17,18]. We use a linear-optical architecture where the required nonlinearity is induced by measurement; current experiments are not scalable, but there are clear paths to a fully scalable quantum architecture [19,20]. Our gates do not require preexisting entanglement, and we encode our qubits into the polarization of up to four photons. Our results highlight that the performance of a quantum algorithm is not the same as performance of the underlying quantum circuit and stress the importance of developing techniques for characterizing quantum algorithms.

Only one step of Shor's algorithm to find the factors of a number N requires a quantum routine. Given a randomly chosen co-prime C (where $1 < C < N$ and the greatest common divisor of C and N is 1), the quantum routine finds the *order* of C modulo N, defined to be the minimum integer r that satisfies $C^r \bmod N = 1$. It is straightforward to find the factors from the order. Consider $N = 15$: if we choose $C = 2$, the quantum routine finds $r = 4$, and the prime factors are given by the nontrivial greatest common divisor of $C^r/^2 \pm 1$ and N, i.e., 3 and 5; similarly, if we choose the next possible co-prime, $C = 4$, we find the order $r = 2$, yielding the same factors.

Figure 1(a) shows a conceptual circuit of the quantum order-finding routine. It consists of three distinct

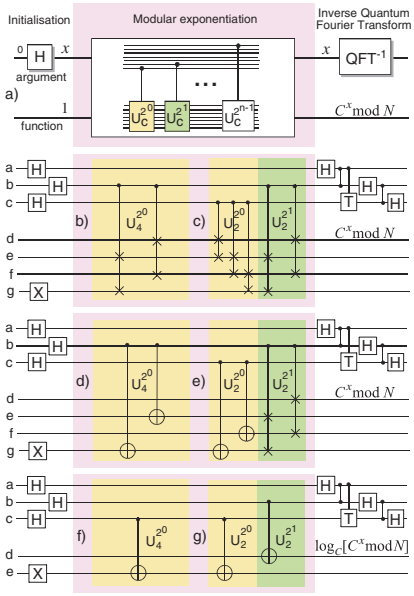


FIG. 1 (color online). (a) Conceptual circuit for the order-finding routine of Shor's algorithm for number N and co-prime C [13]. The argument and function registers are bundles of n and m qubits; the nested order-finding structure uses $U|y\rangle = |Cy \bmod N\rangle$, where the initial function-register state is $|y\rangle = 1$. The algorithm is completed by logical measurement of the argument register, and reversing the order of the argument qubits. (b,c) Implementation of (a) for $N = 15$ and $C = 4$, 2, respectively; the unitaries are decomposed into controlled-swap gates (CSWAP), marked as X; controlled-phase gates are marked by dots; H and T represent Hadamard and $\pi/8$ gates. Many gates are redundant, e.g., the second gate in (b), the first and second gates in (c). (d,e) Partially-compiled circuits of (b,c), replacing CSWAP by controlled-not gates. n.b. (e) is equivalent to the $N = 15$ $C = 7$ circuit in Ref. [14]. (f,g) Fully-compiled circuits of (d,e), by evaluating $\log_C[C^x \bmod N]$ in the function-register.

steps: (i) *register initialization*, $|0\rangle^{\otimes n}|0\rangle^{\otimes m} \rightarrow (|0\rangle + |1\rangle)^{\otimes n}|0\rangle^{\otimes m-1}|1\rangle = \sum_{x=0}^{2^n-1}|x\rangle|0\rangle^{\otimes m-1}|1\rangle$, where the argument-register is prepared in an equal coherent superposition of all possible arguments (normalization omitted by convention); (ii) *modular exponentiation*, which by controlled application of the order-finding function produces the entangled state $\sum_{x=0}^{2^n-1}|x\rangle|C^x \bmod N\rangle$; (iii) the *inverse Quantum Fourier Transform* (QFT) followed by measurement of the argument-register in the logical basis, which with high probability extracts the order r after further classical processing. If the routine is standalone, the inverse QFT can be performed using an approach based on local measurement and feedforward [21]. Note that the inverse QFT in [14] was unnecessary: it is straightforward to show this is true for any order-2^l circuit [22].

Modular exponentiation is the most computationally intensive part of the algorithm [13]. It can be realized by a cascade of controlled unitary operations, U, as shown in the nested inset of Fig. 1(a). It is clear that the registers become highly entangled with each other: since U is a function of C and N, the entangling operation is unique to each problem. Here, we choose to factor 15 with the first two co-primes, $C = 2$ and $C = 4$. In these cases, entire sets of gates are redundant: specifically, $U^{2^n} = I$ when $n > 0$ for $C = 4$, and $U^{2^n} = I$ when $n > 1$ for $C = 2$. Figures 1(b) and 1(c) show the remaining gates for $C = 4$ and $C = 2$, respectively, after decomposition of the unitaries into controlled-swap gates—this level of compiling is equivalent to that introduced in Ref. [14]. Further compilation can always be made since the initial state of the function-register is fixed, allowing the CSWAP gates to be replaced by controlled-not (CNOT) gates as shown in Figs. 1(d) and 1(e) [23].

We implement the order-2-finding circuit, Fig. 1(d). The qubits are realized with simultaneous forward and backward production of photon pairs from parametric down-conversion, Fig. 2(a): the logical states are encoded into the vertical and horizontal polarizations. This circuit requires implementing a recently proposed three-qubit quantum-logic gate, Fig. 2(b), which realizes a cascade of n controlled-z gates with exponentially greater success than chaining n individual gates [24]. The controlled-not gates are realized by combining Hadamards and controlled-z (cz) gates based on partially polarizing beam splitters. The gates are nondeterministic; when fully pre-biased, success probability is $1/4$ [8–10]. A run of each routine is flagged by a fourfold event, where a single photon arrives at each output. Dependent photons from the forward pass interfere nonclassically at the first partial polarizer, Fig. 2(d); one photon then interferes with an independent photon from the backward pass at the second partial polarizer. We measure relative nonclassical visibilities, $V_r \equiv V_{\text{meas}}/V_{\text{ideal}}$, of $98 \pm 2\%$ and $85 \pm 6\%$.

Directly encoding the order-4 finding circuit, Fig. 1(e), requires six photons and at least one three-qubit and five

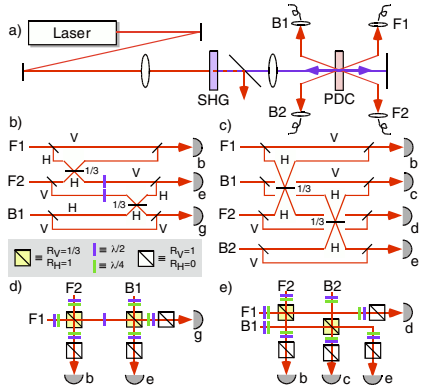


FIG. 2 (color online). Experimental schematic. (a) Forward (F1, F2) and backward (B1,B2) photons pairs are produced via parametric down-conversion [22]. (b,c) Linear-optical circuits for order-2 and order-4 finding algorithms, with inputs from (a) labeled; the letters on the detectors refer to the Fig. 1 qubits. (d,e) Physical optical circuits for (b,c), replacing the classical interferometers with partially polarizing beam splitters.

PRL 99, 250505 (2007) PHYSICAL REVIEW LETTERS week ending 21 DECEMBER 2007

two-qubit gates. This is currently infeasible: the best six-photon rate to date [12] is 30 mHz, which would be reduced by 6 orders of magnitude using nondeterministic gates. To explore an order-4 routine, and the different processes therein, further compilation is necessary. In particular, we can compile circuits 1(d) and 1(e) by evaluating $\log_C[C^x \mathrm{mod} N]$ in the function-register in place of $C^x \mathrm{mod} N$. This requires $\log_2\{\log_C[N]\}$ function qubits, as opposed to $\log_2[N]$; i.e., for $N = 15$, $C = 2$, the function-register reduces from 4 to 2 qubits. Note that this full compilation maintains all the features of the algorithm as originally proposed in Ref. [13]. Thus, the order-4 circuit, Fig. 1(e), reduces to a pair of CNOTS, allowing us to implement the circuit in Fig. 1(g). We use a pair of compact optical gates [8–10], Fig. 2(c) and 2(e), each operating on a dependent pair of photons, resulting in measured visibilities for both of $V_r = 98 \pm 2\%$.

Figure 3 shows the measured density matrices of the argument-register output for both algorithms, sans the redundant top-rail qubit [25]. Ideally, these are maximally-mixed states [22]: in all cases, we measure near-unity fidelities [26,27]. The output of the routines are the logical state probabilities, i.e., the diagonal elements of the matrices. Combining these with the known state of the redundant qubit, and reversing the argument qubits as required, gives the binary outputs of the algorithm which after classical processing yields the prime factors of N. In the order-2 circuits the binary outputs of the algorithm are 00 or 10: the former represents the expected failure mode of this circuit, the latter a successful determination of $r = 2$; failure and success should have equal probabilities; we measure them to be 50% to within error. Thus, half the time the algorithm yields $r = 2$, which gives the factors, 3 and 5. In the order-4 circuit, the binary outputs are 000, 010, 100, and 110: the second and fourth terms yield the order-4 result, the first is a failure mode, and the third yields trivial factors. We measure output probabilities of 25% to within error, as expected. After classical processing half the time, the algorithm finds $r = 4$, again yielding the factors 3 and 5.

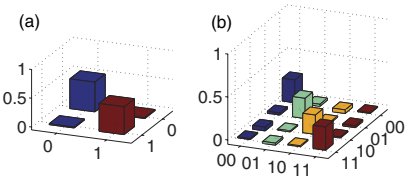


FIG. 3 (color online). Algorithm outputs given by measured argument-register density matrices. The diagonal elements are the logical output probabilities. (a) Order-2 algorithm. The fidelity with the ideal state is $F = 99.9 \pm 0.3\%$, the linear entropy is $S_L = 100 \pm 1\%$ [27]. Combined with the redundant qubit, the logical probabilities are $\{P_{00}, P_{10}\} = \{52, 48\} \pm 3\%$. (b) Order-4 algorithm, $F = 98.5 \pm 0.6\%$ and $S_L = 98.1 \pm 0.8\%$. The logical probabilities are $\{P_{000}, P_{010}, P_{100}, P_{110}\} = \{27, 23, 24, 27\} \pm 2\%$. Real parts shown, imaginary parts are less than 0.6%.

These results show that we have near-ideal algorithm performance, far better than we have any right to expect given the known errors inherent in the logic gates [8,28]. This highlights that the *algorithm* performance is not always an accurate indicator of *circuit* performance since the algorithm produces mixed states. In the absence of the gates, the argument-register qubits would remain pure; as they are mixed, they have become entangled to *something* outside the argument register. From algorithm performance, we cannot distinguish between desired mixture arising from entanglement with the function-register, and undesired mixture due to environmental decoherence. Circuit performance is crucial if it is to be incorporated as a subroutine in a larger algorithm, Fig. 1(a), 1(e), and 1(g). The *joint* state of both registers after modular exponentiation indicates circuit performance; we find entangled states that partially overlap with the expected states, Fig. 4, indicating some environmental decoherence.

Process tomography fully characterizes circuit performance, yielding the χ-matrix, a table of process measurement outcomes and the coherences between them. Measured and ideal χ-matrices can be quantitatively compared using the fidelity [6,27]; we measured process fidelities of $F_p = 85\%$, 89% for the two-qubit gates of the order-4 circuit. It is the easier of the two algorithms to characterize since it consists of two gates acting on inde-

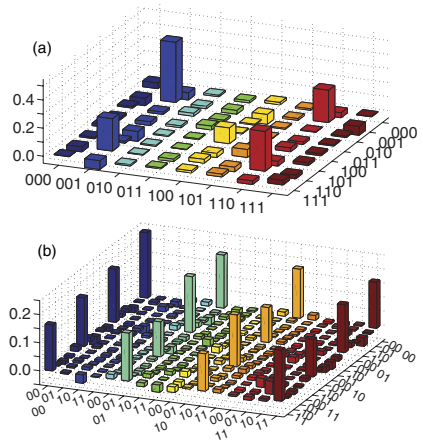


FIG. 4 (color online). Measured density matrices of the state of both registers after modular exponentiation. (a) Order-2 circuit. The ideal state is locally equivalent to a GHZ state: we find $F_{\mathrm{GHZ}} = 59 \pm 4\%$. The state is partially mixed, $S_L = 62\% \pm 4\%$, and entangled, violating the optimal GHZ entanglement witness $W_{\mathrm{GHZ}} = 1/2 - F_{\mathrm{GHZ}} = -9 \pm 4\%$ [31]. (b) Order-4 circuit. Measured fidelity with the ideal state, a tensor product of two Bell-states, is $F = 68 \pm 3\%$. The state is partially mixed, $S_L = 52 \pm 4\%$, and entangled, with tangles of the component Bell-States of $41 \pm 5\%$ and $33 \pm 5\%$. Real parts shown, imaginary parts are, respectively, less than 7% and 4%. The fidelity of the four-qubit state (b) is higher than the three-qubit state (a), chiefly because the latter requires nonclassical interference of photons from independent sources, which suffer higher distinguishability, lowering gate performance [28,32,33].

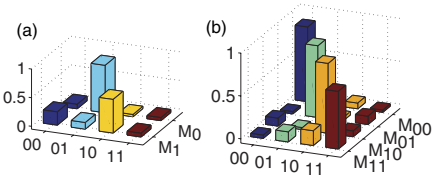


FIG. 5 (color online). Measured function-register probabilities after modular exponentiation, conditioned on logical measurement of the argument-register M_x. There is a high correlation between the registers: (a) Order-2 circuit, $\{P_{01}, P_{10}\} = \{83 \pm 4\%, 59 \pm 5\%\}$; (b) Order-4 circuit, $\{P_{00}, P_{01}, P_{10}, P_{11}\} = \{87 \pm 3\%, 84 \pm 4\%, 82 \pm 5\%, 67 \pm 6\%\}$.

pendent qubit pairs. Consequently, by assuming that only these gates induce error, the order-4 circuit process fidelity is simply the product of the individual gate fidelities [30], $F_p^{bcde} = F_p^{bd} F_p^{ce} = 80\%$. Clearly, this is significantly less than the *algorithm* success rate of 99.7%. The order-2 circuit is harder to characterize, requiring at least 4096 measurements, infeasible with our count rates. Decomposing the three-qubit gate into a pair of two-qubit gates yields process fidelities $F_p = 78\%, 90\%$ (reflecting differing interferences of independent and dependent photons). There is no simple relation between individual cz gate performances and that of the three-qubit gate. However, a bound can be obtained by chaining the gate errors, $F_p \geq 20\%$ [29]. This is not useful, c.f. the fidelity between an ideal cz and doing nothing at all of $F_p = 25\%$ (The bound only becomes practical as $F_p \to 1$). For larger circuits, full tomographic characterization becomes exponentially impractical. The order-finding routine registers contain $k = n + m$ qubits: state and process tomography of a k-qubit system require at least 2^{2k} and 2^{4k} measurements, respectively.

An alternative is to gauge circuit performance via logical correlations *between* the registers. Modular exponentiation produces the entangled state $\sum_{x=0}^{2^n-1} |x\rangle|y\rangle$ where y is respectively $C^x \mathrm{mod} N$ and $\log_C[C^x \mathrm{mod} N]$ for partial and full compilation. For a correctly functioning circuit, measuring the argument in the state x projects the function into y—requiring at most 2^k measurements to check. Figure 5 shows there is a clear correlation between the argument and function registers, 59 to 83% and 67 to 87% for the order-2 and order-4 circuits, respectively. Again, these indicative values of circuit operation are significantly less than the algorithm success rates.

We have experimentally implemented every stage of a small-scale quantum algorithm. Our experiments demonstrate the feasibility of executing complex, multiple-gate quantum circuits involving coherent multiqubit superpositions of data registers. We present two different implementations of the order-finding routine at the heart of Shor's algorithm, characterizing the algorithmic and circuit performances. Order-finding routines are a specific case of phase-estimation routines, which in turn underpin a wide variety of quantum algorithms, such as those in quantum chemistry [30]. Besides providing a proof of the use of quantum entanglement for arithmetic calculations, this work points to a number of interesting avenues for future research—in particular, the advantages of tailoring algorithm design to specific physical architectures, and the urgent need for efficient diagnostic methods of large quantum information circuits.

We wish to thank M. P. de Almeida and E. DeBenedictis for stimulating discussions. This work was supported by the Australian Research Council, Federation Fellow and DEST Endeavour Europe programs, the IARPA-funded U.S. Army Research Office Contract No. W911NF-05-0397, and the Canadian NSERC.

Note added in proof.—By better spectral filtering, we improved the GHZ state to $F = 67 \pm 3\%$, $S_L = 58 \pm 3\%$, and $W_{GHZ} = -17 \pm 3\%$.

[1] P. Shor, *Proc. 35th Ann. Symp. Found. Comp. Sci.* (IEEE Comp. Soc. Press, Los Alamitos, California, 1994), p. 124.
[2] F. Schmidt-Kaler *et al.*, Nature (London) **422**, 408 (2003).
[3] D. Leibfried *et al.*, Nature (London) **422**, 412 (2003).
[4] M. Steffen *et al.*, Science **313**, 1423 (2006).
[5] J. L. O'Brien *et al.*, Nature (London) **426**, 264 (2003).
[6] J. L. O'Brien *et al.*, Phys. Rev. Lett. **93**, 080502 (2004).
[7] P. Walther *et al.*, Nature (London) **434**, 169 (2005).
[8] N. K. Langford *et al.*, Phys. Rev. Lett. **95**, 210504 (2005).
[9] N. Kiesel *et al.*, Phys. Rev. Lett. **95**, 210505 (2005).
[10] R. Okamoto *et al.*, Phys. Rev. Lett. **95**, 210506 (2005).
[11] R. Prevedel *et al.*, Nature (London) **445**, 65 (2007).
[12] C.-Y. Lu *et al.*, Nature Phys. **3**, 91 (2007).
[13] D. Beckman *et al.*, Phys. Rev. A **54**, 1034 (1996).
[14] L. M. K. Vandersypen *et al.*, Nature (London) **414**, 883 (2001).
[15] S. L. Braunstein *et al.*, Phys. Rev. Lett. **83**, 1054 (1999).
[16] N. C. Menicucci *et al.*, Phys. Rev. Lett. **88**, 167901 (2002).
[17] D. F. V. James *et al.*, Phys. Rev. A **64**, 052312 (2001).
[18] J. F. Poyatos *et al.*, Phys. Rev. Lett. **78**, 390 (1997).
[19] E. Knill *et al.*, Nature (London) **409**, 46 (2001).
[20] M. A. Nielsen, Phys. Rev. Lett. **93**, 040503 (2004).
[21] R. B. Griffiths *et al.*, Phys. Rev. Lett. **76**, 3228 (1996).
[22] See EPAPS Document No. E-PRLTAO-99-020750 for supplementary information. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.
[23] Figure 1(e) is equivalent to the order-4 $C = 7$ circuit in Ref. [14]: CSWAP is equivalent to a Toffoli and CNOTS.
[24] T. C. Ralph, Phys. Rev. A **70**, 012312 (2004).
[25] We use convex optimization tomography [M. De Burgh, A. Doherty, and A. Gilchrist (to be published)] and estimate errors via Monte Carlo simulation [6].
[26] Fidelity is $F(\rho, \sigma) \equiv \mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]^2$; linear entropy is $S_L \equiv d(1 - \mathrm{Tr}[\rho^2])/(d-1)$, where d is the state dimension [27].
[27] A. G. White *et al.*, J. Opt. Soc. Am. B **24**, 172 (2007).
[28] T. J. Weinhold *et al.* (to be published).
[29] A. Gilchrist *et al.*, Phys. Rev. A **71**, 062310 (2005).
[30] A. Aspuru-Guzik *et al.*, Science **309**, 1704 (2005).
[31] M. Bourennane *et al.*, Phys. Rev. Lett. **92**, 087902 (2004).
[32] J. G. Rarity *et al.*, J. Opt. B **7**, S171 (2005).
[33] R. Kaltenbaek *et al.*, Phys. Rev. Lett. **96**, 240502 (2006).

Experimental demonstration of Shor's algorithm with quantum entanglement: Additional on-line material

B. P. Lanyon, T. J. Weinhold, N. K. Langford, M. Barbieri, D. F. V. James*, A. Gilchrist, and A. G. White
Centre for Quantum Computer Technology Department of Physics University of Queensland, Brisbane QLD 4072, Australia
**Department of Physics Center for Quantum Information and Control University of Toronto, Toronto ON M5S1A7, Canada*

For all the circuits Fig. 1b)-g), the consecutive Hadamards in the top qubit of the argument-register cancel each other out (since $\mathrm{H}^2=\mathrm{I}$): consequently both this qubit, and the gate(s) controlled by it, are redundant and need not be implemented experimentally. The remaining argument-register qubits are maximally-entangled to the function-register. Since the function-register output is not measured, these argument qubits are maximally-mixed, and the subsequent gates in the inverse QFT are therefore also redundant. Thus the inverse QFT in Ref. [14] was unnecessary: indeed, it is straightforward to show this is true for any order-2^l circuit. After modular exponentiation, the circuit state is $\sum_{x=0}^{2^n-1}|x\rangle|C^x \mathrm{mod} N\rangle$: for any two values x and y that differ by an integer, k number of orders, i.e. $y-x=k\,2^l$, $C^y \mathrm{mod} N=C^x \mathrm{mod} N$, and the state after modular exponentiation becomes $\sum_{k=0}^{2^{n-l}-1}\sum_{a=0}^{2^l-1}|k2^l+a\rangle|C^a \mathrm{mod} N\rangle$. Note that the first $n-l$ qubits of the argument-register (top to bottom) encode the number k, the remaining l qubits encode 2^l distinct values of a: we divide the argument-register accordingly, $\sum_{k,a}|k\rangle|a\rangle|C^a\rangle$. The $|k\rangle$ qubits do not become entangled to the function-register whereas the $|a\rangle$ qubits are maximally-entangled to it—consequently after tracing out the function-register, the $|a\rangle$ qubits are in a maximally-mixed state and any further gates acting on them are redundant. Application of Hadamard gates in the inverse QFT reset the $|k\rangle$ qubits to 0, inhibiting any gates controlled by them, The final step of the inverse QFT is to swap the first and last qubits of the argument register which can be done after measurement. Thus the inverse QFT can be omitted in all cases $r=2^l$.

2.1 Contribution statement

The author made the following contributions to this work:

- Experimental design and construction of the optical circuits (in collaboration with MB and TW)
- Preliminary and final data acquisition (in collaboration with MB, TJW, NKL)
- Data analysis (in collaboration with NKL)
- Complete first draft of the manuscript and subsequent revisions (in collaboration with all authors)
- Referee replies and corresponding manuscript revision (in collaboration with all authors)

2.2 Additional experimental details

Figures 2.1 and 2.2 show various representations of the optical circuits constructed for our implementation of Shor's algorithm. We employ the same qubit labeling used in the paper.

2.3 Improving the GHZ state

As noted at the end of the paper, we were able to improve the quality of the 3-qubit GHZ state produced by the order-2 finding circuit. Specifically, the state Fidelity was increased from $59 \pm 4\%$ to $67 \pm 3\%$. The density matrix of the improved state is shown in Fig. 2.3.

These results where achieved by moving from the filter arrangement shown in Fig. 2.1c, to that employed for the Toffoli gate shown in Fig. 1.2c. One reason why this could have helped is that all of the filters are now at the output of the gate, rather than the input. Perfect gate operation requires that when a photon is detected at the output it is impossible to tell which input mode it came from. If the filters are mismatched in some way (i.e. centre frequency, bandwidth, profile), and located at the input, then this would provide some which-path information and thereby reduce the gate quality.

Another possible reason is that we reduced the bandwidth in two of the filters, from ± 1.5nm to ± 0.5nm. Because photons pairs generated through SPDC are in a frequency

entangled state, the strongest measurement (narrowest filter) will define the spectrum of both photons in a pair. Therefore narrowing one filter will increase the coherence length of both photons in a pair. A longer photon coherence length means that path-length instabilities will have less of an effect on the photon indistinguishability.

Finally we also turned the SPDC pump laser power down, from approximately 400mW to 300mW at 410nm. This reduces the effect of high-order photon number pair emission from SPDC, which are detrimental to gate performance, as describe in a recent paper [BWL$^+$09].

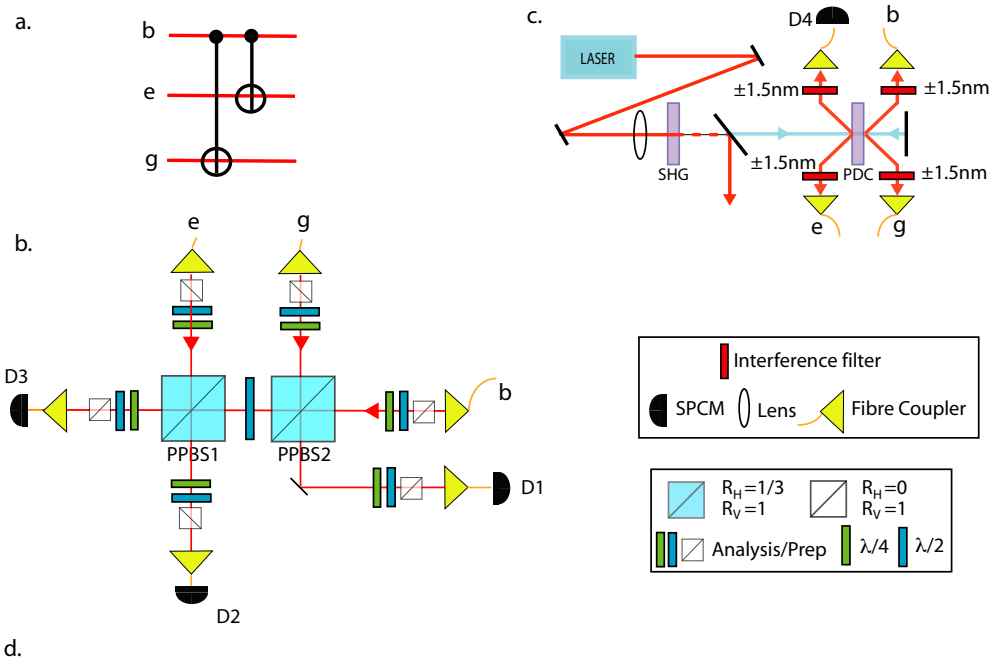


Figure 2.1: **Schematics of concatenated CNOT gates.** This circuit was employed for the order-2 finding Shor's algorithm implementation. **a**. Standard quantum logic circuit notation for concatenated CNOT gates. **b**. Optical circuit diagram. **c**. Optical source diagram. **d**. Annotated laboratory photograph of the optical circuit. Many of the wave plates have been removed to make viewing clearer. The photon detectors (SPCMs) are out of shot, but their corresponding fibre couplers have been labelled. PPBS, partially polarizing beam splitter; SPCM, single-photon counting module; PDC, parametric downconversion; SHG, second-harmonic generation.

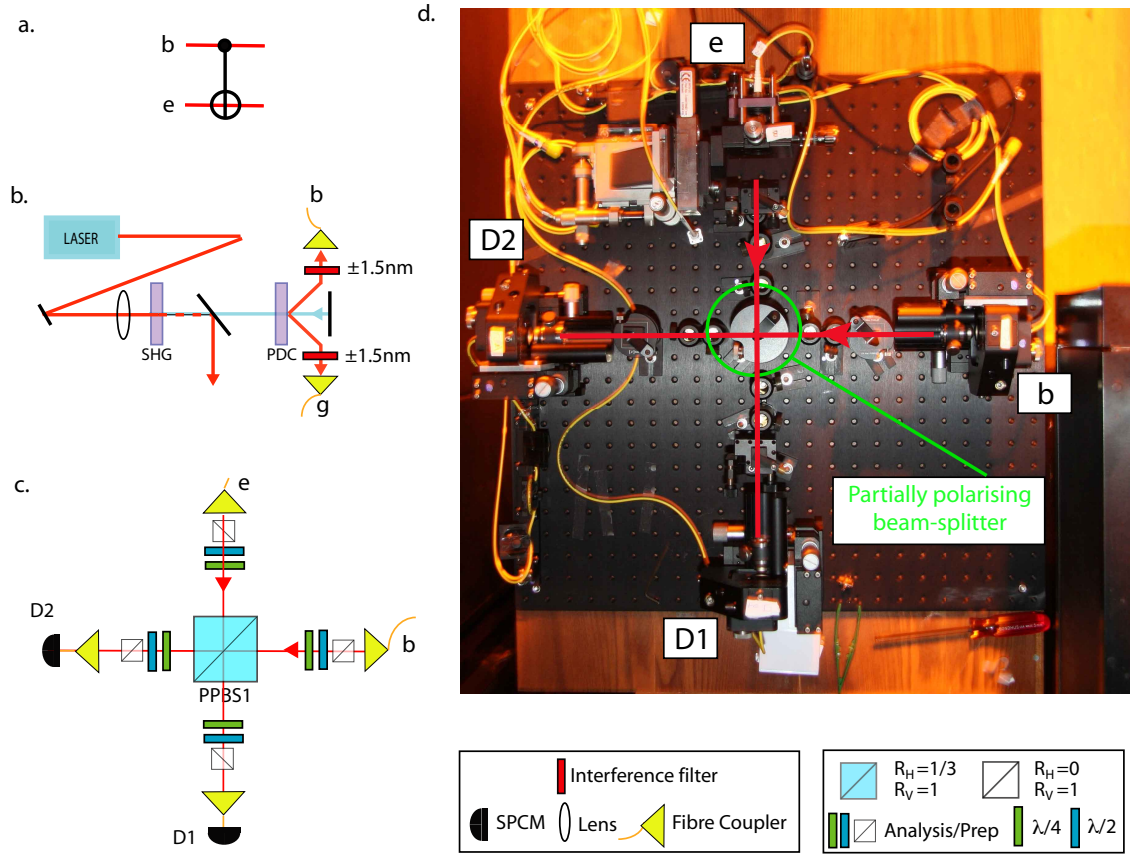


Figure 2.2: **Schematics of one of the CNOT gates employed for the order-4 finding Shor's implementation.** Two CNOTs operating on different pairs of photons where required for the order-4 finding circuit. For the other CNOT we employed the first shown in Fig. 2.1. **a**. Standard quantum logic circuit notation for a CNOT gate. Qubit labels match that of Fig. 1 in the paper. **b**. Optical source diagram. **c**. Optical circuit diagram. **d**. Annotated laboratory photograph of the optical circuit. Many of the wave plates have been removed to make viewing clearer. The photon detectors (SPCMs) are out of shot, but their corresponding fibre couplers have been labelled. PPBS, partially polarizing beam splitter; SPCM, single-photon counting module; PDC, parametric downconversion; SHG, second-harmonic generation.

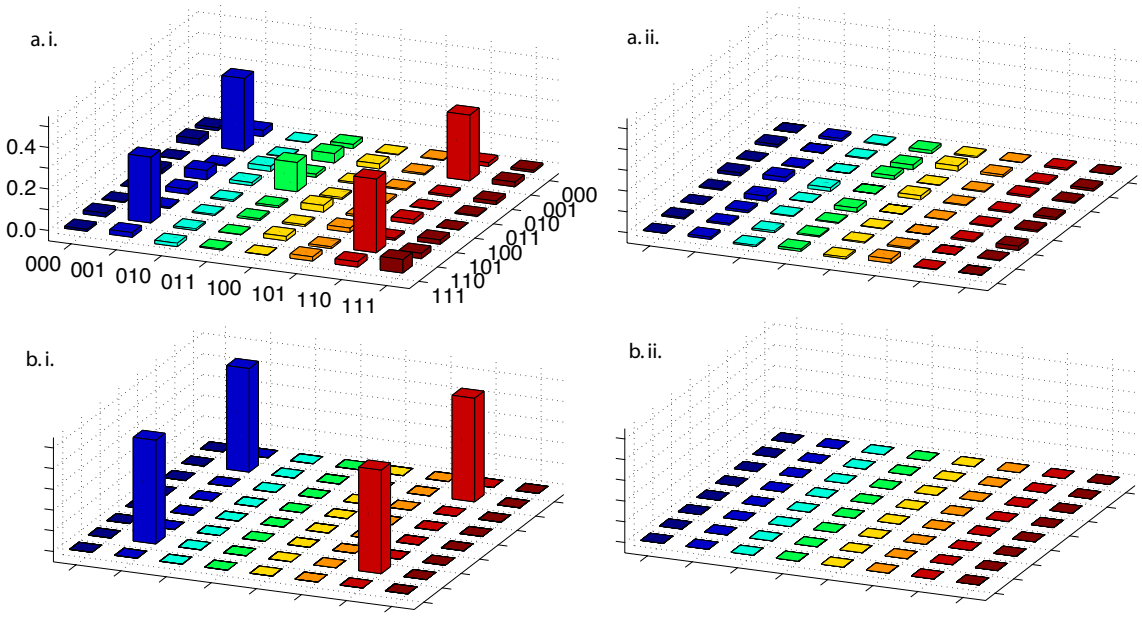


Figure 2.3: **Measured and ideal GHZ density matrices. a.i(ii)** real (imaginary) parts of the experimentally reconstructed density matrix. **b.i(ii)** Real (imaginary) parts of the ideal density matrix. The measured state was generated by the order-2 finding circuit of our Shor's algorithm implementation. The fidelity between the measured and ideal state is $67 \pm 3\%$. The linear entropy of the measured state is $58 \pm 3\%$. Both of these quality measures are defined in the corresponding paper.

Chapter 3

Calculating the energy of H_2 on a prototype optical quantum computer

Implementation of a quantum algorithm for calculating molecular energies using quantum optics

B. P. Lanyon[1], J. D. Whitfield[2], G. G. Gillet[1], M. E. Goggin[1,3], M. P. Almeida[1],
I. Kassal[2], J. D. Biamonte[2,*], M. Mohseni[2], B. J. Powell[4], M. Barbieri[1,†], A. Aspuru-Guzik[2] & A. G. White[1]
[1]*Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane 4072, Australia*
[2]*Department of Chemistry and Chemical Biology, Harvard University, Cambridge, MA 02138, USA*
[3] *Department of Physics, Truman State University, Kirksville, MO 63501, USA*
[4]*Department of Physics and Centre for Organic Photonics & Electronics, University of Queensland, Brisbane 4072, Australia*

One of the most promising applications for a quantum computer is to efficiently simulate and calculate properties of many-body quantum systems. In general, this is believed to be an intractable problem on a conventional computer, yet of enormous importance in a number of research fields. In this paper we present a proof-of-principle demonstration of this application, using optical quantum computational resources. Specifically, we implement the quantum phase estimation algorithm to obtain the energy spectrum of the smallest molecular system—the hydrogen molecule in a minimal basis. Finally, we provide details on the long-term path to large-scale implementations that lie beyond the reach of conventional 'classical' computing, including the gate networks required to simulate an arbitrary molecule, and a resource count for a simple example.

The fundamental problem of quantum chemistry is the calculation of molecular properties, which are of practical importance in fields ranging from materials science to biochemistry. In principle, the total energy of a molecule, as well as most other properties, such as the dipole moment, quadrupole moment, diamagnetic susceptibility, etc., can be calculated by solving the Schrödinger equation. However, the computational time required to obtain exact solutions on a conventional computer, which encodes information in the *classical* state of its constituent parts, generally increases exponentially with the number of atoms involved [1, 2].

This problem could be simplified if one could build a *quantum* computer, which encodes information in the *quantum state* of its constituent parts [1–4]. Such a device could simulate molecular systems, and calculate their energies, to a fixed accuracy using resources that increase only polynomially with the system size [5–8]. Furthermore, recent results show that a quantum computer could also simplify the simulation of chemical reactions and calculation of observables of chemical interest, such as state-to-state transition probabilities and reaction rates [9].

Previous quantum simulation experiments have been performed using various technologies [8, 10–12]. The majority of the experiments have been performed using nuclear-magnetic-resonance–based quantum computers, beginning with simulations of quantum oscillators [10] and leading up to simulations of a pairing Hamiltonian [8, 11]. Recently, using ion-trap quantum computers, the phase transitions of a two-spin quantum magnet were experimentally simulated [12].

Here we report the first quantum simulation of a chemical system and calculation of its energy, using quantum computational resources. Specifically, we present a proof-of-principle demonstration of a quantum algorithm for calculating non-relativistic molecular energies [6] on a small-scale optical quantum computer, obtaining the energy spectrum of the hydrogen molecule (H_2) in a minimal basis. We demonstrate the following key algorithmic steps: encoding of the electronic molecular wavefunction into the polarization of photonic quantum bits (qubits); simulation of the time-evolution operator using optical quantum logic gates; and extraction of the energy using a quantum phase-estimation algorithm. Our demonstration is limited to a proof-of-principle because the small size and high symmetry of the system allows a direct and exact simulation of the molecule, avoiding the need for resource-intensive approximation techniques that are necessary in general. Finally, we discuss how our tech-

*Present address: Oxford University Computing Laboratory, Oxford OX1 3QD, United Kingdom.
†Present address: Laboratoire Ch. Fabry de l'Istitut d'Optique, Palaiseau, France.

nique can be extended to solve large-scale chemical systems. In the Supporting Online Material (SOM), we provide comprehensive details of one of these extensions, the quantum gate networks required to simulate an arbitrary molecule, and a resource count for a simple example.

Molecular energies are the eigenvalues of the associated time-independent Hamiltonian $\hat{H}$ and can be obtained to a fixed accuracy, with quantum computational resources that scale only polynomially with the molecular size [6], using the phase-estimation algorithm [3, 13]. This is a general-purpose quantum algorithm for evaluating the eigenvalues of arbitrary Hermitian or unitary operators. The algorithm can estimate the phase, ϕ, accumulated by a molecular eigenstate, $|\Psi\rangle$, under the action of the time-evolution operator, $\hat{U} = e^{-i\hat{H}t/\hbar}$, i.e.,

$$e^{-i\hat{H}t/\hbar}|\Psi\rangle = e^{-iEt/\hbar}|\Psi\rangle = e^{-i2\pi\phi}|\Psi\rangle \qquad (1)$$

where E is the energy eigenvalue of $|\Psi\rangle$. Therefore, estimating the phase for each eigenstate amounts to estimating the eigenvalues of the Hamiltonian.

In this work, we implement the iterative phase estimation algorithm [6, 14] (IPEA), which reduces the number of qubits and quantum logic gates required. Fig. 1a shows the IPEA at iteration k. Important requirements include the ability to encode a system eigenstate, $|\Psi\rangle$, into a register of qubits and to implement powers of $\hat{U}$ conditional on the state of a single control qubit. The result of a logical measurement of the control qubit after each iteration determines the k^{th} bit of the binary expansion [15] of ϕ. Let m bits of this expansion be $\tilde{\phi} = 0.\phi_1\phi_2...\phi_m$, such that $\phi = \tilde{\phi} + \delta 2^{-m}$ where δ is a remainder $0 \leq \delta < 1$. If ϕ has an exact expansion to m bits ($\delta = 0$) and the circuit implementation is perfect, the algorithm returns all m bits correctly, without error. If $\delta > 0$, m bits can be determined with an accuracy $\pm 2^{-m}$ and error probability [14] $\epsilon \leq 1 - 8/\pi^2 \approx 0.19$, which is independent of m (the bound is saturated for $\delta = 0.5$).

We take the standard approach to quantum-chemical calculations by solving an approximate Hamiltonian created by employing the Born-Oppenheimer approximation (where the electronic Hamiltonian is parameterized by the nuclear configuration) and choosing a suitable truncated basis set in which to describe the non-relativistic electronic system. Typical sets consist of a finite number of single-electron atomic orbitals, which are combined to form antisymmetric multi-electron molecular states (configurations) [17]. Calculating the eigenvalues of the electronic Hamiltonian using all configurations gives the exact energy in the basis set and is referred to as full configuration interaction (FCI). For n orbitals and k electrons there are $\binom{n}{k} \approx n^k/k!$ ways to allocate the electrons among the orbitals. This exponential growth is the handicap of FCI calculations on classical computers.

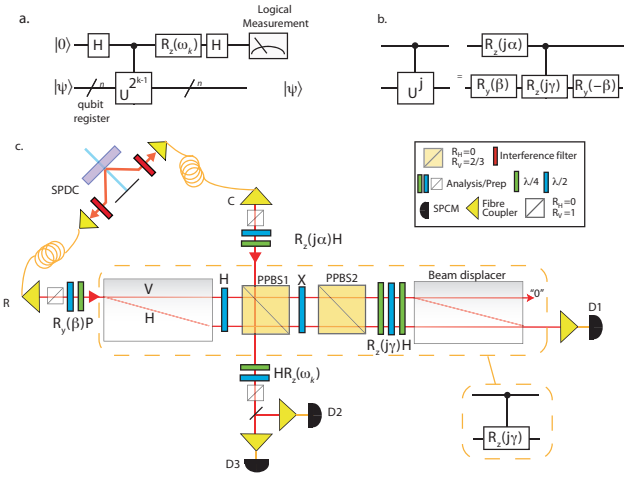


FIG. 1: **Algorithm and experimental implementation.** **(a)** IPEA [6, 14] at iteration k. To produce an m-bit approximation to ϕ the algorithm is iterated m times. Each iteration obtains one bit of ϕ (ϕ_k): starting from the least significant (ϕ_m), k is iterated backwards from m to 1. The angle ω_k depends on all previously measured bits, $\omega_k = -2\pi b$, where b, in the binary expansion, is $b = 0.0\phi_{k+1}\phi_{k+2}...\phi_m$ and $\omega_m = 0$. H is the standard Hadamard gate [15]. **(b)** Our gate network for a two-qubit controlled-$\hat{U}^j$ gate, as discussed in the text. **(c)** Two-qubit optical implementation of (a). Photon pairs are generated by spontaneous parametric down-conversion (SPDC), coupled into single-mode optical fiber and launched into free space optical modes C (control) and R (register). Transmission through a polarizing beamsplitter (PBS) prepares a photonic polarization qubit in the logical state $|0\rangle$, the horizontal polarization. The combination of a PBS with half ($\lambda/2$) and quarter ($\lambda/4$) waveplates allows the preparation (or analysis) of an arbitrary one-qubit pure state. The optical controlled-$\hat{R}_z$ gate, shown in the dashed box, is realized using conditional transformations via spatial degrees of freedom as described by Lanyon [16] *et al.* Coincident detection events (3.1 ns window) between single photon counting modules (SPCM's) D1 and D3 (D2 and D3) herald a successful run of the circuit and result 0 (1) for ϕ_k. Waveplates are labelled with their corresponding operations.

We use the minimal STO-3G basis [18] for H_2, consisting of one $|1s\rangle$-type atomic orbital for each atom. The two basis functions are then combined to form the bonding and antibonding molecular orbitals [19], $|g\rangle$ and $|u\rangle$. Taking into account electron spin, the single-electron molecular spin-orbitals are denoted, $|g\uparrow\rangle$, $|g\downarrow\rangle$, $|u\uparrow\rangle$ and $|u\downarrow\rangle$, where $|\uparrow\rangle$ and $|\downarrow\rangle$ are the electron spin eigenstates. These are combined antisymmetrically to form the six two-electron configurations that form the basis for our simulation: $|\Phi_1\rangle = |g\uparrow, g\downarrow\rangle$, $|\Phi_2\rangle = |g\uparrow, u\uparrow\rangle$,

$|\Phi_3\rangle = |g\uparrow, u\downarrow\rangle$, $|\Phi_4\rangle = |g\downarrow, u\uparrow\rangle$, $|\Phi_5\rangle = |g\downarrow, u\downarrow\rangle$ and $|\Phi_6\rangle = |u\uparrow, u\downarrow\rangle$. Due to symmetry, the Hamiltonian is block-diagonal in this basis, with blocks acting on each of the four subspaces spanned by $\{|\Phi_1\rangle, |\Phi_6\rangle\}$, $\{|\Phi_2\rangle\}$, $\{|\Phi_3\rangle, |\Phi_4\rangle\}$, and $\{|\Phi_5\rangle\}$ (see SOM, section B). Therefore, finding the eigenvalues of the two 2×2 sub-matrices in the Hamiltonian ($\hat{H}^{(1,6)}$ and $\hat{H}^{(3,4)}$) amounts to performing the FCI. Estimating the eigenvalues of 2x2 matrices using the IPEA is the simplest non-trivial case, requiring coherent non-classical interaction between the control and register qubits.

We map the configurations $\{|\Phi_k\rangle\}$ to the computational basis of the qubits for each subspace under consideration. Since the subspaces are two-dimensional, one qubit suffices to represent the wavefunction. The corresponding time-evolution operators, $\hat{U}^{(i,j)} = e^{-i\hat{H}^{(i,j)}t/\hbar}$ (where $(i,j) = (1,6)$ or $(3,4)$), are therefore one-qubit operators. We employ a propagator time step of $t = 1\ \hbar/E_\mathrm{h}$ (the hartree, $E_\mathrm{h} \approx 27.21$ eV, is the atomic unit of energy), chosen so that $0 \leq Et/2\pi\hbar \leq 1$. All necessary molecular integrals are evaluated classically (SOM, section C) using the Hartree-Fock procedure [19]. For our proof-of-principle demonstration, we use these integrals to calculate matrix elements of $\hat{H}$ and $\hat{U}$, then directly decompose each $\hat{U}^{(i,j)}$ operator into a logic gate network. While these steps *do not* scale efficiently with molecular size, we discuss below (and in the SOM) how they can be avoided.

We decompose the two-dimensional $\hat{U}^{(i,j)}$ operators into a global phase and a series of rotations of the one-qubit Hilbert space [15]:

$$\hat{U} = e^{i\alpha}\hat{R}_y(\beta)\hat{R}_z(\gamma)\hat{R}_y(-\beta), \qquad (2)$$

where α, β, and γ, are real angles. In this case, $\hat{U}^j$ is achieved by replacing angles α and γ with $j\alpha$ and $j\gamma$ (while β remains unchanged). Our decomposition of the controlled-$\hat{U}^j$ is shown in Fig. 1b.

Just as classical electronic-structure methods typically require an initial guess of the many-body wavefunction, the IPEA requires that the register qubit be initialized to a state sufficiently close to the eigenstate $|\Psi\rangle$ of $\hat{U}$. For the purpose of our demonstration, we encode exact eigenstates, obtained via a preliminary calculation on a classical computer. This step does not scale efficiently with molecular size, and we return to this later. Note that we show below that perfect encoding of the state is not required.

We implement the IPEA in an all-optical architecture, encoding qubits in the polarization of single photons, Fig. 1c. Two-qubit quantum logic gates are realized using established techniques that combine linear optical elements with projective measurement to achieve the required nonlinear interaction between photons [20, 21]. Consequently these gates are non-deterministic: coincident measurement of single photons in the two output modes signals a successful run, with probability [16] 1/12. Such gates are high-quality, well-characterized, and have several theoretical paths to scalable optical quantum computing [20–25]. Single-qubit gates are performed deterministically using birefringent waveplates.

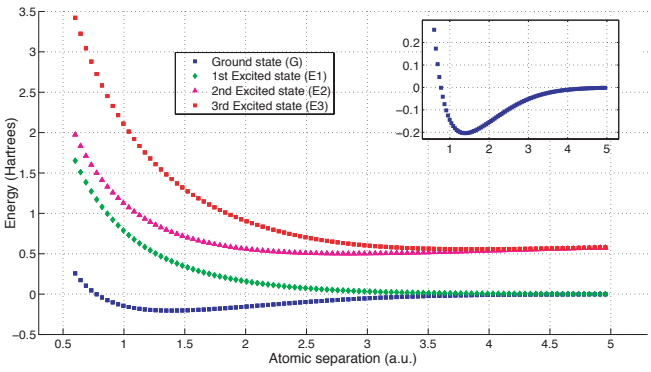


FIG. 2: **Quantum algorithm results: H_2 potential energy curves in a minimal basis**. Each point is calculated using a 20-bit IPEA and employing $n = 31$ samples per bit. Every case was successful, achieving the target precision of $\pm(2^{-20} \times 2\pi)\ E_\mathrm{h} \sim 10^{-5}\ E_\mathrm{h}$. Curve G (E3) is the low (high) eigenvalue of $\hat{H}^{(1,6)}$. Curve E1 is a triply degenerate spin-triplet state, corresponding to the lower eigenvalue of $\hat{H}^{(3,4)}$ as well as the eigenvalues $\hat{H}^{(2)}$ and $\hat{H}^{(5)}$. Curve E2 is the higher (singlet) eigenvalue of $\hat{H}^{(3,4)}$. Measured phases are converted to energies via Eqn. 1 and reported relative to the ground state energy of two hydrogen atoms at infinite separation. **Inset:** Curve G rescaled to highlight the bound state.

Absolute molecular energies must be computed to an accuracy greater than $\approx 10^{-4}E_\mathrm{h}$, to resolve the energy differences relevant to chemical processes[6]. Therefore it is important to demonstrate that the IPEA can achieve the necessary phase precision of ≈ 16 bits (the accuracy of the non-relativistic Born-Oppenheimer energy is then limited only by the choice of basis). In order to decrease errors, each IPEA iteration is repeated n times, yielding n possible values for the corresponding bit; a majority vote of these samples determines the result. Fig. 2 shows our results: H_2 energies calculated over a range of internuclear separations, thus reconstructing the potential energy surfaces. Each point is obtained using a 20-bit IPEA and employing $n = 31$ samples per bit. In every case, the algorithm successfully returned the energy to within the target precision of $\pm(2^{-20}\times 2\pi)\ E_\mathrm{h} \approx 10^{-5}E_\mathrm{h}$. For example, the ground state energy obtained at the equilibrium

bond length, 1.3886 a_0 (where a_0 is the Bohr radius), is -0.20399 ± 0.00001 E_h, which agrees exactly with the result obtained on a classical computer to an uncertainty in the least significant bit.

We use the estimation of this equilibrium energy to study the effect of varying a range of experimental parameters on the IPEA success probability. We define the algorithm success probability as that of obtaining all m bits of the phase to an accuracy of 2^{-m}. Fig. 3a shows the algorithm success probability measured over a range of n, the number of samples used to determine each bit.

The probability of correctly identifying any individual bit with a single sample ($n = 1$) is reduced from unity by both theoretical (δ) and experimental factors (such as imperfect gates). However, as long as it remains above 0.5, repeated sampling and a majority vote will improve the probability of correct identification. The data show that this is achieved and the error probability decreases exponentially with n, in accordance with the Chernoff bound [15]. This technique allows for a significant increase in success probability, at the expense of repeating the experiment a fixed number of times. We note that this simple classical error correction technique can only play a small role when it comes to dealing with errors in large-scale implementations. Here, the numerous errors in very large quantum logic circuits will make achieving a bit success probability over 0.5 a significant challenge, that must be met with quantum error correction techniques.

Fig. 3b shows the algorithm success probability measured as a function of the number of extracted bits (phase precision). By employing $n = 101$ samples per bit we achieve near perfect algorithm success probability up to 47 bits (yielding an energy precision of $\approx 10^{-13} E_\mathrm{h}$), where this limit is imposed only by the machine-level precision used for the classical preprocessing of the Hamiltonians. It is insightful to understand how achieving such high precision will become a far more significant challenge for large-scale implementations: due to the small-scale of our demonstration, we are able to implement each power of $\hat{U}^{(i,j)}$ directly, by re-encoding the same number of gates. Therefore, the probability of error introduced by gate imperfections remains a constant for each bit (and, in our implementation, under 50%). This is the main algorithmic feature that allows the high precision obtained in this experiment. However, as expounded in the SOM (section A), this will not be possible for larger implementations. In general, $\hat{U}$ will not have the same form as $\hat{U}^n$. For each additional digit of precision sought, the gate requirements of the algorithm are roughly doubled.

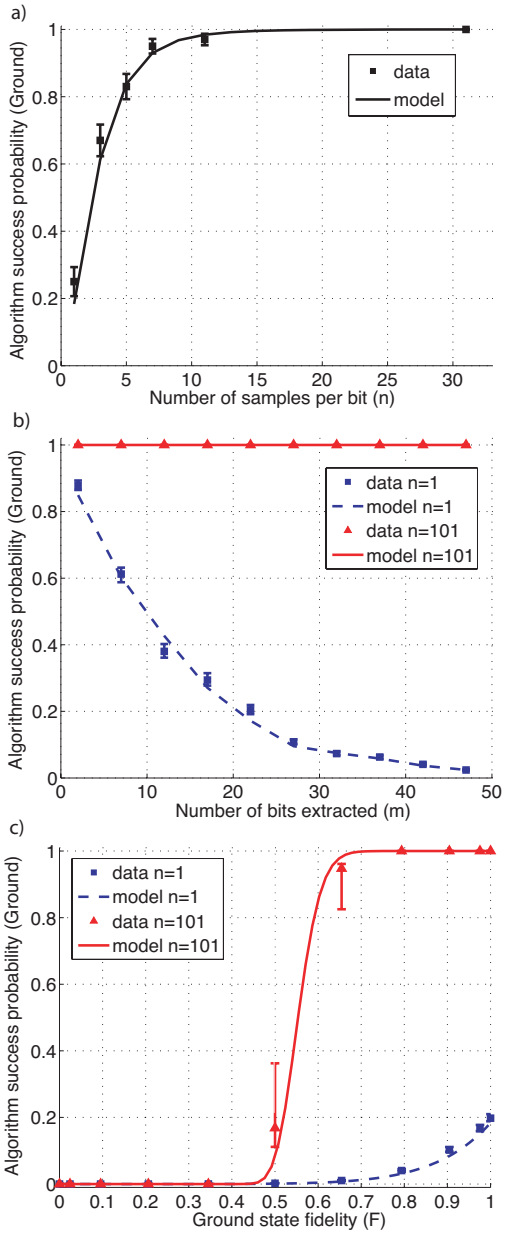


FIG. 3: **IPEA success probability measured over a range of parameters.** Probabilities for obtaining the ground state energy, at the equilibrium bond length 1.3886 a_0, as a function of: **(a)** the number of times each bit is sampled (n); **(b)** the number of extracted bits (m); **(c)** the fidelity between the encoded register state and the ground state (F). The standard fidelity [15] between a measured mixed ρ and ideal pure $|\Psi\rangle$ state is $F{=}\langle\Psi|\rho|\Psi\rangle$. **(a)** & **(b)** employ a ground state fidelity of $F \approx 1$. **(a)** & **(c)** employ a 20-bit IPEA. All lines are calculated using a model that allows for experimental imperfections. This model, as well as the technique used to calculate success probabilities and error bars, are detailed in the SOM (sections D & E).

Fig. 3c shows the algorithm success probability measured as a function of the fidelity F (see caption) between the encoded register state and the ground state. The results show that our implementation is robust for $F \gtrsim 0.5$. Because the probability of correctly obtaining each bit in a single measurement ($n = 1$) is greater than 0.5 in this regime, multiple sampling ($n > 1$) enables the success probability to be amplified arbitrarily close to unity. This is a general feature that will hold for large-scale implementations. However, for $F \lesssim 0.5$, the measured success probabilities are very low.

If we could reuse the register state output after each iteration as the input of the next, then the problem with low eigenstate fidelities could be overcome as the measurement of the control qubit collapses the wave function unfortunately this is not possible in our setup. Any pure encoded register state can be written in the eigenstate basis as $|G\rangle = \sum_i \alpha_i |\lambda_i\rangle$, where $|\alpha_i|^2$ is the fidelity of $|G\rangle$ with eigenstate $|\lambda_i\rangle$. Successful measurement of the m^{th} bit associated with $|\lambda_i\rangle$ will cause the register wavefunction to collapse into a state with a greater fidelity with $|\lambda_i\rangle$—those eigenstates with a low probability of returning the measured bit value will be diminished from the superposition. As more bits are successfully measured, the register state will rapidly collapse to $|\lambda_i\rangle$. In this way, the algorithm will return all the bits associated with $|\lambda_i\rangle$ with probability at least [15] $|\alpha_i|^2(1-\epsilon)$. With current technology, correct operation of our optical circuit requires destructive measurement of both the control and register qubits after each IPEA iteration. Therefore, in our experiment the register state must be re-prepared for each iteration.

The path towards large-scale calculations contains many challenges. There are those associated with scaling up the 'hardware', i.e., achieving more qubits, gates, and longer coherence times. Much progress is being made on developing the necessary technology for a full-scale all-optical quantum computer, including high-quality single-photon sources [26] and efficient photon-number–resolving detectors [27]. In addition the influence of noise is a serious consideration [28] and must be overcome using error correction and fault tolerant constructions [7, 15]. The algorithm we described uses a continuous set of gates rather than a finite universal set of gates. To apply the results of fault tolerant quantum computing, we must approximate each of the gates parameterized by continuous variables in Eqn.2 using gates from a finite set. This can be done efficiently due to the Solovay-Kitaev theorem [15]. For larger implementations, encoding states robustly against decoherence must be done at the cost of additional qubits [15]. Using an ion trap implementation as a case study, Clark *et al.* have carried out a detailed system engineering analysis of the quantum simulation algorithm's performance using error correction using a the quantum logic array method [7]. One of their conclusions is that error correction for quantum simulation is more demanding in terms of additional ancillary quantum bits and gates as quantum factoring. Finding quantum simulation methods that do not suffer from the limitation of Trotter expansions is a fertile research area. The implementation demonstrated in this manuscript does not suffer from these limitations, and therefore we were able to achieve a high accuracy in terms of the number of bits obtained by the phase estimation procedure.

Other challenges are those associated with scaling up of the 'software', i.e., the algorithm itself. Firstly, the efficient preparation of even low fidelity eigenstate approximations is a non-trivial step for molecules much larger than H_2. It has been proposed that in many cases this problem can be overcome using a heuristic adiabatic state preparation algorithm [6, 29–32]. In this way, ground state approximations, for example, can be efficiently obtained provided that the energy gap between the ground state and the excited states is sufficiently large along the path of the adiabatic evolution [33]. Secondly, as previously stated our technique of directly decomposing the molecular evolution operator into logic gates does not scale efficiently with molecular size [2] and an alternative scheme must be employed. The proposed solution exploits the fact that the general molecular Hamiltonian is a sum of fixed-sized one- and two-electron terms that can be efficiently simulated and combined to approximate the global evolution [2, 15]. This allows U to be approximated up to an arbitrarily small (but non zero) error using a number of gates that scales polynomially with molecular size.

We give an overview of this 'operator-splitting' technique in the SOM (section A) and find that the total number of elementary quantum gates required to simulate (without error correction) the evolution of an arbitrary molecule scales as $O(N^5)$, where N is the number of single-particle basis functions used to describe the molecular system. In this scheme, N is also the number of qubits necessary. We also present the quantum logic circuits required to simulate each term in the general molecular Hamiltonian—these are the building blocks of a universal, quantum, molecular simulator. Finally, we count the number of quantum gates required to reproduce our H_2 simulation in this way.

We have performed a proof-of-principle demonstration of an efficient quantum algorithm for the calculation

of molecular energies. Although the small size and high symmetry of the particular molecular system that we consider enabled some simplifications to be made, that are essential given current experimental capabilities, we have demonstrated several key steps of the algorithm. The combination of our demonstration, with the new theoretical results presented in the SOM, provide clear stepping-stones for the next experimental demonstrations, as more and more quantum computing resources become available. Consequently quantum computers with only around 100 qubits are predicted to outperform any classical computational device for the exact first-principles calculation of chemical properties [6, 9]. We note that the techniques presented here can be applied to a very broad class of quantum systems [2, 3] and therefore have the potential for wide application.

Acknowledgments.

We thank A. Perdomo, A. Steinberg, P.J. Love, A.D. Dutoi, G. Vidal, and A. Fedrizzi for discussions. We acknowledge financial support from the Australian Research Council Federation Fellow and Centre of Excellence programs, and the IARPA-funded U.S. Army Research Office Contract No. W911NF-0397. The Harvard team acknowledges support from the Army Research Office under contract W911NF-07-0304. BJP was the recipient of an Australian Research Council Queen Elizabeth II Fellowship (DP0878523) and IK of the Joyce and Zlatko Balokovi´c Scholarship.

Correspondence.

Correspondence and requests for materials should be addressed to BPL (lanyon@physics.uq.edu.au) and AA-G (aspuru@chemistry.harvard.edu).

Competing financial interest statement.

The authors declare no competing financial interests.

[1] R. P. Feynman, *Int. J. Theor. Phys.* **21**, 467 (1982).
[2] S. Lloyd, *Science* **273**, 1073 (1996).
[3] D. Abrams, S. Lloyd, *Phys. Rev. Lett.* **79**, 2586 (1997).
[4] C. Zalka, *Proc. Roy. Soc. Lond. A* **454**, 313 (1998).
[5] D. A. Lidar, H. Wang, *Phys. Rev. E* **59**, 2429 (1999).
[6] A. Aspuru-Guzik, A. Dutoi, P. Love, M. Head-Gordon, *Science* **309**, 1704 (2005).
[7] C. R. Clark, K. R. Brown, T. S. Metodi, S. D. Gasster, *arXiv:0810.5626* (2008).
[8] K. R. Brown, R. J. Clark, I. L. Chuang, *Physical Review Letters* **97**, 050504 (2006).
[9] I. Kassal, S. P. Jordan, P. J. Love, M. Mohseni, A. Aspuru-Guzik, *Proc. Natl. Acad. Sci.* **105**, 18681 (2008).
[10] S. Somaroo, C. H. Tseng, T. F. Havel, R. Laflamme, D. G. Cory, *Phys. Rev. Lett.* **82**, 5381 (1999).
[11] X. Yang, A. M. Wang, F. Xu, J. Du, *Chem. Phys. Lett.* **422**, 20 (2006).
[12] A. Friedenauer, H. Schmitz, J. T. Glueckert, D. Porras, T. Schaetz, *Nature Phys.* **4**, 757 (2008).
[13] A. Kitaev, *arXiv e-print quant-ph/9511026* (1995).
[14] M. Dobsicek, G. Johansson, V. S. Shumeiko, G. Wendin, *Phys. Rev. A* **76** (2007).
[15] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2001).
[16] B. P. Lanyon, *et al.*, *Nature Phys.* **5**, 134 (2009).
[17] T. Helgaker, P. Jorgensen, J. Olsen, *Modern Electronic Structure Theory* (Wiley, 2000).
[18] W. J. Hehre, R. F. Stewart, J. A. Pople, *J. Chem. Phys.* **51**, 2657 (1969).
[19] A. Szabo, N. Ostlund, *Modern Quantum Chemistry: Introduction to Advanced Electronic Structure Theory* (Dover Publications, 1996).
[20] E. Knill, R. Laflamme, G. J. Milburn, *Nature* **409**, 46 (2001).
[21] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, D. Branning, *Nature* **426**, 264 (2003).
[22] J. L. O'Brien, *et al.*, *Phys. Rev. Lett.* **93**, 080502 (2004).
[23] P. Kok, *et al.*, *Rev. Mod. Phys.* **79**, 135 (2007).
[24] M. A. Nielsen, *Phys. Rev. Lett.* **93**, 040503 (2004).
[25] R. Prevedel, *et al.*, *Nature* **445**, 65 (2007).
[26] P. Grangier, B. Sanders, J. Vuckovic, *New J. Phys.* **6** (2004).
[27] A. Migdal, J. Dowling, *J. Mod. Opt.* **51** (2004).
[28] W. Dür, M. J. Bremner, H. J. Briegel, *arXiv:0706.0154* (2007).
[29] L.-A. Wu, M. S. Byrd, D. A. Lidar, *Phys. Rev. Lett.* **89**, 05794 (2002).
[30] S. Oh, *arxiv e-print 0712.0789* (2007).
[31] H. Wang, S. Kais, A. Aspuru-Guzik, M. R. Hoffman, *Phys. Chem. Chem. Phys.* **10**, 5388 (2008).
[32] A. Friedenauer, H. Schmitz, J. T. Glueckert, D. Porras, T. Schaetz, *Nature Phys.* **4**, 757 (2008).
[33] E. Farhi, J. Goldstone, S. Gutmann, M. Sipser, *Science* **292**, 472 (2000).

Molecular energy calculation on a prototype optical quantum computer: Supporting online material

B. P. Lanyon[1], J. D. Whitfield[2], G. G. Gillet[1], M. E. Goggin[1,3], M. P. Almeida[1],
I. Kassal[2], J. D. Biamonte[2,*], M. Mohseni[2], B. J. Powell[4], M. Barbieri[1,†], A. Aspuru-Guzik[2] & A. G. White[1]
[1]*Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane 4072, Australia*
[2]*Department of Chemistry and Chemical Biology, Harvard University, Cambridge, MA 02138, USA*
[3] *Department of Physics, Truman State University, Kirksville, MO 63501, USA*
[4]*Department of Physics and Centre for Organic Photonics & Electronics, University of Queensland, Brisbane 4072, Australia*

A. Efficient simulation of arbitrary molecular time-evolution operators

A fundamental challenge for the quantum simulation of large molecules is the accurate decomposition of the system's time evolution operator, $\hat{U}$. In our experimental demonstration, we exploit the small size and inherent symmetries of the hydrogen molecule Hamiltonian to implement $\hat{U}$ exactly, with only a small number of gates. As the system size grows such a direct decomposition cannot be performed efficiently. However, an efficient first-principles simulation of the propagator is possible for larger chemical systems[1–7].

The key steps of an efficient approach are: (1) expressing the chemical Hamiltonian in second quantized form, (2) transforming each term in the Hamiltonian to a spin representation via the Jordan-Wigner transformation[8], (3) decomposing the overall unitary propagator, via a Trotter-Suzuki expansion[3,9], into a product of the evolution operators for non-commuting Hamiltonian terms, and (4) efficiently simulating the evolution of each term by designing and implementing the corresponding quantum circuit. We note that the first two steps generate a Hamiltonian that can be easily mapped to the states of qubits. The last steps are part of the quantum algorithm for simulating the time-evolution operator, $\hat{U}$, generated by this Hamiltonian. Details of each step are provided as follows:

Step 1. Second-quantized Hamiltonian

The general second-quantized chemical Hamiltonian has $O(N^4)$ terms, where N is the number of single-electron basis functions (i.e. spin-orbitals) used to describe the system[10]. The Hamiltonian can be explicitly written as:

$$\hat{H} = \sum_{p,q} h_{pq} \hat{a}_p^+ \hat{a}_q + \frac{1}{2} \sum_{p,q,r,s} h_{pqrs} \hat{a}_p^+ \hat{a}_q^+ \hat{a}_r \hat{a}_s, \qquad \text{(S1)}$$

where the annihilation and creation operators ($\hat{a}_j$ and $\hat{a}_j^+$ respectively) obey the fermionic anti-commutation relations: $[\hat{a}_i, \hat{a}_j^+]_+ = \delta_{ij}$ and $[\hat{a}_i, \hat{a}_j]_+ = 0$, and the indices p, q, r, and s run over all N single-electron basis functions. The integrals h_{pq} and h_{pqrs} are evaluated during a preliminary Hartree-Fock procedure[11] and are defined as

$$h_{pq} = \int \mathrm{d}\mathbf{x}\, \chi_p^*(\mathbf{x}) \left(-\frac{1}{2}\nabla^2 - \sum_\alpha \frac{Z_\alpha}{r_{\alpha\mathbf{x}}} \right) \chi_q(\mathbf{x})$$

and

$$h_{pqrs} = \int \mathrm{d}\mathbf{x}_1 \mathrm{d}\mathbf{x}_2 \frac{\chi_p^*(\mathbf{x}_1)\chi_q^*(\mathbf{x}_2)\chi_r(\mathbf{x}_2)\chi_s(\mathbf{x}_1)}{r_{12}}$$

where $\chi_q(\mathbf{x})$ are a selected single-particle basis. Here ∇^2 is the Laplacian with respect to the electron spatial coordinates, while $r_{\alpha\mathbf{x}}$ and r_{12} are the distances between the α^{th} nucleus and the electron and the distance between electrons 1 and 2, respectively.

Expressing the Hamiltonian in second-quantized notation allows straightforward mapping of the state space to qubits. The logical states of each qubit are identified with the fermionic occupancy of a single-electron spin-orbital (i.e. $|0\rangle$ = occupied, $|1\rangle$ = unoccupied). Therefore, simulating a system with a total of N single-electron spin-orbitals (e.g., $N = \lambda\kappa$ for a molecule with λ atoms each with κ spin-orbitals) requires only N qubits. Note that the N-qubit Hilbert space allows for any number of electrons (up to N), hence the scaling is *independent* of

*Present address: Oxford University Computing Laboratory, Oxford OX1 3QD, United Kingdom.
†Present address: Laboratoire Ch. Fabry de l'Istitut d'Optique, Palaiseau, France.

the number of electrons present in the system. In practical Gaussian basis-set calculations, the number of spin-orbitals per atom is usually constant for a given row of the periodic table[12]. The use of a double-zeta basis set[12] would require employing ≈ 30 logical qubits per simulated atom. For example, 1800 logical qubits would be required to store the wave function of the fullerene (C_{60}) molecule.

Step 2. Jordan-Wigner transformation of the fermionic operators to spin variables

Starting with the second-quantized Hamiltonian from (S1), the Jordan-Wigner transformation is used to map fermionic creation and annihilation operators into a representation in terms of Pauli spin matrices[8]. This allows for a convenient implementation on a quantum computer[4,5]. The representation is achieved via the following invertible transformations, which are applied to each term in (S1):

$$\hat{a}_j \rightarrow \mathbf{1}^{\otimes j-1} \otimes \hat{\sigma}^+ \otimes (\hat{\sigma}^z)^{\otimes N-j} \quad \text{(S2a)}$$

$$\hat{a}_j^+ \rightarrow \mathbf{1}^{\otimes j-1} \otimes \hat{\sigma}^- \otimes (\hat{\sigma}^z)^{\otimes N-j}, \quad \text{(S2b)}$$

where $\hat{\sigma}^+ \equiv (\hat{\sigma}^x + i\hat{\sigma}^y)/2 = |0\rangle\langle 1|$ and $\hat{\sigma}^- \equiv (\hat{\sigma}^x - i\hat{\sigma}^y)/2 = |1\rangle\langle 0|$. The $\hat{\sigma}^\pm$ operators achieve the desired mapping of occupied (unoccupied) states to the computational basis [i.e., $|1\rangle$ ($|0\rangle$)] while other terms serve to maintain the required anti-symmetrization of the wavefunction in the spin (qubit) representation.

Step 3. Exponentiation of the Hamiltonian

The number of matrix elements in the chemical Hamiltonian (S1) increases exponentially with N. Therefore a direct decomposition of the time-evolution operator, $\hat{U}$, into logic gates is not efficient—requiring a number of logic gates[13] that also increases exponentially with N. However, the Hamiltonian is a sum of one and two-electron terms whose time-evolution operators can each be implemented efficiently—with a number of gates that does not scale with N. However, generally the terms do not commute, thus simple reconstruction of $\hat{U}$ from direct products of the individual operators is not possible. Trotter-Suzuki relations can be used to approximate the full unitary propagator from the individual evolution of non-commuting operators[3,9].

For a Hamiltonian $\hat{H} = \sum_{i=1}^{N} \hat{h}_i$, the first-order Trotter-Suzuki decomposition is expressed as

$$\hat{U}(t) = e^{-i\hat{H}t} = \left(e^{-i\hat{h}_1 dt} e^{-i\hat{h}_2 dt} \cdots e^{-i\hat{h}_N dt}\right)^{\frac{t}{dt}} + O(dt^2). \quad \text{(S3)}$$

The value $T_n = t/dt$ is called the Trotter number[9]. As the Trotter number tends to infinity, or equivalently $dt \rightarrow 0$, the approximation becomes exact. In practice, a compromise between computational effort and accuracy is sought. In numerical computations, such as quantum Monte Carlo simulations[14] successive calculations at different timesteps dt are carried out, and an extrapolation of $dt \rightarrow 0$ gives an estimate of the exact answer. A similar approach can be used for quantum simulation.

We note that, unlike our small-scale experiment, the powers of the system evolution operator, $\hat{U}^j$, required for the IPEA cannot be achieved by simply changing parameters in the gate decomposition for $\hat{U}$. In general $\hat{U}^2$ will take twice as many gates as $\hat{U}$. Intuitively, the system dynamics must be propagated for twice as long leading to twice as many manipulations of the quantum simulator's natural dynamics. The increase in the number of gates required for extra bits will clearly amplify experimental errors, thereby limiting the obtainable precision. Note that although the number of required gates increases exponentially with the number of bits, each additional bit itself provides an exponential increase in precision.

As mentioned previously in the manuscript, quantum algorithms that circumvent the Trotter expansion problem are a fertile area of research. The classification of which quantum Hamiltonians are efficiently simulated without employing Trotter expansions and which ones require them would be a very important development in the field of quantum simulation. For example, Hamiltonians that are diagonal in the computational basis, such as the classical Ising model do not require a Trotter expansion for their accurate simulation[15].

Step 4. Circuit representations of the unitary propagator

Each exponentiated tensor product of Pauli spin variables can then be implemented efficiently by employing a family of quantum circuits. In order to provide an accurate estimation of an upper bound of the number of gates required for the different kinds of second-quantized operators, we carried out analytical gate decompositions. The circuit networks obtained are summarized in Fig. S1. The networks shown realize the unitary operator $\hat{U}(dt)$ for a general molecular Hamiltonian. To realize a controlled unitary, $c-\hat{U}(dt)$, as required by the phase estimation algorithm, only the rotations $\hat{R}_z(\theta)$ must be converted to controlled-$\hat{R}_z(\theta)$ rotations. The number of gates required to simulate each term is linear in the number of intervening qubits due to the product of $\hat{\sigma}_z$ terms resulting from the Jordan-Wigner transformation of Eq. S2. Therefore, the scaling of the number of quantum gates required for simulating a general many-electron chemical

Hamiltonian is $O(N^5)$ without considering the influence of noise[16]. Fault tolerant quantum simulation[13] requires the use of a finite set of gates and the conversion from the continuous set of gates to a discrete set can be accomplished with polylogarithmic penalty[17]. The encoding of robust quantum states will also require several redundant qubits for each logical qubit needed[13]. A more detailed analysis of fault tolerance in the context of quantum simulation can be found in Ref.[15].

Resource count for a simple example.

In order to illustrate this algorithm, we performed numerical simulations for H_2 in the same minimal basis (STO-3G) employed in our experiment. Unlike our experimental mapping, the logical states of each register qubit are now identified with the fermionic occupancy of the four single-electron spin-orbitals (i.e. $|0\rangle$ = occupied, $|1\rangle$ = unoccupied). Therefore, the calculation requires a total of five qubits taking into consideration the single control qubit required for the IPEA. If quantum error correction is needed, the number of qubits will increase according to the scheme used[13]. Fig. S2 shows the error in the ground state energy as a function of the Trotter step. The ground state energies of the approximate unitary propagators were obtained via direct diagonalization on a classical computer. A precision of $\pm 10^{-4} E_h$ is achieved at a Trotter number of 6, which corresponds to 522 gates. Note that this gate count is to construct $\hat{U}^1$ and includes both one- and two-qubit operations. This estimate does not take into consideration error correction for the qubits and it uses a continuous set of gates. In the path to large scale implementations, both will be serious considerations and will increase the complexity of the algorithm and the number of qubits necessary[13,15]. The unitary matrix must be raised to various powers to perform phase estimation. If one desires to maintain a fixed accuracy of 13 bits, about 8.5×10^6 gates must be used for the IPEA estimation procedure. Note that this can be achieved by repeating the 522 gates required for $\hat{U}$ many times. Note that this does not include the resources associated with preparing a system eigenstate. If one uses an adiabatic state preparation techniques[1] the resources are proportional to the gap between the ground state and the excited state along the path of adiabatic evolution[18].

Although the estimates just given exceed the capabilities of current quantum computers, these resource requirements grow only *polynomially* with the size the of system. Consequently, for large enough chemical systems, quantum computers with around 100 qubits are predicted to outperform classical computational devices for the first-principles calculation of chemical properties[1,19].

B. Symmetries in the electronic Hamiltonian of the hydrogen molecule in a minimal basis

The basis for our simulation of H_2 is composed of six two-electron antisymmetric wavefunctions (configurations): $|\Phi_1\rangle = |g\uparrow, g\downarrow\rangle$, $|\Phi_2\rangle = |g\uparrow, u\uparrow\rangle$, $|\Phi_3\rangle = |g\uparrow, u\downarrow\rangle$, $|\Phi_4\rangle = |g\downarrow, u\uparrow\rangle$, $|\Phi_5\rangle = |g\downarrow, u\downarrow\rangle$, and $|\Phi_6\rangle = |u\uparrow, u\downarrow\rangle$. Here $|\uparrow\rangle$ and $|\downarrow\rangle$ are the electron spin eigenstates and $|g\rangle$ and $|u\rangle$ are, respectively, the bonding and antibonding single electron molecular orbitals[11]. Most of the elements of this basis are not mixed by the Hamiltonian. In particular, $|\Phi_1\rangle$ and $|\Phi_6\rangle$ mix only with each other because they have g symmetry while the rest have u symmetry. Of the remaining states only $|\Phi_3\rangle$ and $|\Phi_4\rangle$ mix because they have the same total z-projection of the spin, $m_S = 0$. $|\Phi_2\rangle$ and $|\Phi_5\rangle$ have, respectively, $m_S = 1$ and $m_S = -1$. Therefore, the Hamiltonian is block-diagonal within four subspaces spanned by $\{|\Phi_1\rangle, |\Phi_6\rangle\}$, $\{|\Phi_2\rangle\}$, $\{|\Phi_3\rangle, |\Phi_4\rangle\}$, and $\{|\Phi_5\rangle\}$. There are no approximations involved here, and finding the eigenvalues of the two 2×2 sub-matrices in the Hamiltonian ($\hat{H}^{(1,6)}$ and $\hat{H}^{(3,4)}$) amounts to performing an exact calculation (FCI) in the minimal basis. One should also note that it follows from the requirement that the wave functions are spin eigenstates, that the eigenstates of the subspace $\{|\Phi_3\rangle, |\Phi_4\rangle\}$ will be $(|\Phi_3\rangle \pm |\Phi_4\rangle)/\sqrt{2}$. Additionally, there will be a three-fold degeneracy of the triplet state with angular momentum $S = 1$. That is, the states $|\Phi_2\rangle$, $|\Phi_5\rangle$, and $(|\Phi_3\rangle + |\Phi_4\rangle)/\sqrt{2}$ are degenerate.

C. Details of computational methods

Restricted Hartree-Fock calculations were carried out on a classical computer using the STO-3G basis[20]. The software used was the PyQuante quantum chemistry package[21]. The molecular integrals from the Hartree-Fock procedure are used to evaluate the matrix elements of the Hamiltonians $\hat{H}^{(1,6)}$ and $\hat{H}^{(3,4)}$, described in the main text.

D. Details of experimental methods

1. Count rates

We operate with a low-brightness optical source (spontaneous parametric downconversion pumping power $\approx$ 50 mW) to reduce the effects of unwanted multi-photon-pair emissions (which cannot be distinguished by our

non-photon-number-resolving detectors and introduce error into the circuit operation). This yields about 15 coincident detection events per second at the output of our optical circuit. Therefore each iteration can be repeated 15 times a second. Reconfiguring the circuit for different iterations takes approximately 7 seconds, largely due to the finite time required to rotate standard computer controlled waveplate mounts. Therefore, obtaining a 20-bit estimation of a phase takes about 3 minutes, when using $n = 31$ samples to determine the logical state of each bit (as was employed to achieve the results shown in Fig. 2). Note that approximately 95% of this time is spent rotating waveplates. In future implementations, this time could be reduced significantly using integrated-photonics, e.g. qubit manipulation using an electrooptically-controlled waveguide Mach-Zehnder interferometer[22].

2. How we obtain IPEA success probabilities

Denoting the first m binary bits of a phase ϕ as $\tilde{\phi} = 0.\phi_1\phi_2...\phi_m$, there is, in general, a remainder $0 \leq \delta < 1$, such that $\phi = \tilde{\phi} + \delta 2^{-m}$. To achieve an accuracy of $\pm 2^{-m}$ the IPEA success probability is the sum of the probabilities for obtaining $\tilde{\phi}$ and $\tilde{\phi} + 2^{-m}$. This can be estimated experimentally, for a given phase, by simply repeating the algorithm a large number of times and dividing the number of acceptable results by the total. An estimate with an error less than 10% would require over 100 algorithm repetitions. We calculate the result shown in Fig. 3c in this way. However, using this technique to obtain Fig. 3b-c, and Fig. S3 (described below), would take a long time—the 20 points shown in each would require more than 100 hours of waveplate rotation time alone. Instead, to obtain these results we force the appropriate feedforward trajectory ($R(\omega_k)$) for each accepted phase value and use $n = 301$ samples to estimate the 0/1 probabilities for each bit. Using the binomial cumulative distribution function it is then possible to calculate the majority vote success probability for each bit of each accepted value for a given n (1 and 101 in the figures). The probability for obtaining an accepted phase value is then the product of the majority vote success probabilities for each bit, and the total algorithm success probability is the sum of the probabilities for obtaining each accepted phase. The error bars represent a 68% confidence interval and are obtained from a direct Monte-Carlo simulation of the above process.

Note that forcing the correct feedforward in this way, and taking many samples to estimate the 0/1 probabilities for each bit, simply allows us to accurately estimate the probability that the algorithm will return the correct phase by itself - i.e. without forcing the correct feedforward.

E. Details of Figs. 3 & S3

1. Additional data

For our small scale implementation the system evolution is a 2×2 operator. Therefore any state with a fidelity lower than 0.5 with one eigenstate must have a fidelity greater than 0.5 with the other eigenstate. Consequently, when preparing register states with ground state fidelities below 0.5, multiple sampling will pick out the excited state, as shown in Fig. S3. These results are not an exact mirror of Fig. 3c because they are for obtaining a different phase with a different remainder (δ); unlike Fig. 3c they do not require non-classical interference between photons to achieve and are therefore less prone to our experimental errors.

2. Experimental model

A simple computational model of our experiment produced the lines shown in Figs. 3 and S3. This model allows for two experimental imperfections, which are described below, but otherwise assumes perfect optic element operation. The model consists of a series of operators, representing optical elements and noise sources, acting on a vector space representing both photonic polarisation and longitudinal spatial mode[23]. Firstly the model allows for photon distinguishability, quantified by an imperfect relative non-classical interference visibility of 0.93 (ideal 1), which reduces the quality of our two-qubit logic gate. Secondly the model allows for phase damping of the control qubit, described by the operation elements[13]:

$$\begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\gamma} \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 0 \\ 0 & \sqrt{\gamma} \end{bmatrix}. \tag{S4}$$

Our model employs $\gamma = 0.06$ (ideal 0), which corresponds to $\approx 3\%$ dephasing. These experimental imperfections are attributed to a combination of residual higher-order photon pair emissions from our optical source and circuit alignment drift during long measurement sets.

[1] A. Aspuru-Guzik, A. Dutoi, P. Love, M. Head-Gordon, *Science* **309**, 1704 (2005).

[2] D. Abrams, S. Lloyd, *Phys. Rev. Lett.* **83**, 5162 (1999).

[3] S. Lloyd, *Science* **273**, 1073 (1996).

[4] R. Somma, G. Ortiz, J. E. Gubernatis, E. Knill, R. Laflamme, *Phys. Rev. A* **65**, 042323 (2002).

[5] G. Ortiz, J. Gubernatis, E. Knill, R. Laflamme, *Phys. Rev. A* **64**, 022319 (2001).

[6] E. Ovrum, M. Hjorth-Jensen, *arXiv e-print quant-ph/0705.1928* (2007).

[7] P. Varga, B. Apagyi, *Phys. Rev. A* **78**, 022337 (2008).

[8] P. Jordan, E. Wigner, *Z. Phys. A* **47**, 631 (1928).

[9] N. Hatano, M. Suzuki, *Quantum Annealing and Other Optimization Methods*, Lectures Notes in Physics (Springer, Heidelberg, 2005), chap. Finding Exponential Product Formulas of Higher Orders, p. 37.

[10] T. Helgaker, P. Jorgensen, J. Olsen, *Modern Electronic Structure Theory* (Wiley, 2000).

[11] A. Szabo, N. Ostlund, *Modern Quantum Chemistry: Introduction to Advanced Electronic Structure Theory* (Dover Publications, 1996).

[12] K. L. Schuchardt, *et al.*, *J. Chem. Inf. Model.* **47**, 1042 (2007).

[13] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2001).

[14] A. Aspuru-Guzik, W. A. Lester, Jr., *Comp. Chem.*, C. Le Bris, ed. (Elsevier, Amsterdam, The Netherlands, 2003), vol. X of *Handbook of Numerical Analysis*, p. 485, first edn.

[15] C. R. Clark, K. R. Brown, T. S. Metodi, S. D. Gasster, *arXiv:0810.5626* (2008).

[16] W. Dür, M. J. Bremner, H. J. Briegel, *arXiv:0706.0154* (2007).

[17] A. Y. Kitaev, *Russian Math. Surveys* **52**, 1191 (1997).

[18] E. Farhi, J. Goldstone, S. Gutmann, M. Sipser, *arxiv e-print quant-ph/0001106* (2000).

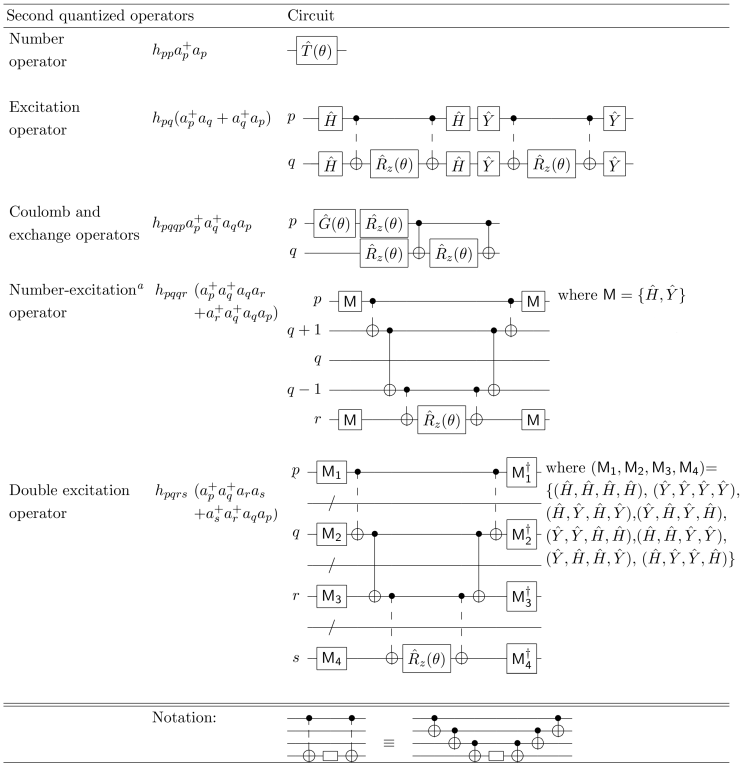
[19] I. Kassal, S. P. Jordan, P. J. Love, M. Mohseni, A. Aspuru-Guzik, *Proc. Natl. Acad. Sci.* **105**, 18681 (2008).

[20] W. J. Hehre, R. F. Stewart, J. A. Pople, *J. Chem. Phys.* **51**, 2657 (1969).

[21] R. P. Muller, Python quantum chemistry (pyquante) program, version 1.6 (2007).

[22] Y. Liao, *et al.*, *Opt. Lett.* **33**, 2281 (2008).

[23] B. P. Lanyon, *et al.*, *Nature Phys.* **5**, 134 (2009).



[a]The spin variable representation of this operator depends on whether q lies in the range p to r or outside of it.

FIG. S1: **The quantum circuits corresponding to evolution of the listed Hermitian second-quantized operators**. Here p, q, r, and s are orbital indices corresponding to qubits such that the population of $|1\rangle$ determines the occupancy of the orbitals. It is assumed that the orbital indices satisfy $p > q > r > s$. These circuits were found by performing the Jordan-Wigner transformation given in (S2b) and (S2a) and then propagating the obtained Pauli spin variables[4]. In each circuit, $\theta = \theta(h)$ where h is the integral preceding the operator. Gate $\hat{T}(\theta)$ is defined by $\hat{T}|0\rangle = |0\rangle$ and $\hat{T}|1\rangle = \exp(-i\theta)|1\rangle$, $\hat{G}$ is the global phase gate given by $\exp(-i\phi)\hat{1}$, and the change-of-basis gate $\hat{Y}$ is defined as $\hat{R}_x(-\pi/2)$. Gate $\hat{H}$ refers to the Hadamard gate. For the number-excitation operator, both $\mathsf{M} = \hat{Y}$ and $\mathsf{M} = \hat{H}$ must be implemented in succession. Similarly, for the double excitation operator each of the 8 quadruplets must be implemented in succession. The global phase gate must be included due to the phase-estimation procedure. Phase estimation requires controlled versions of these operators which can be accomplished by changing all gates with θ-dependence into controlled gates.

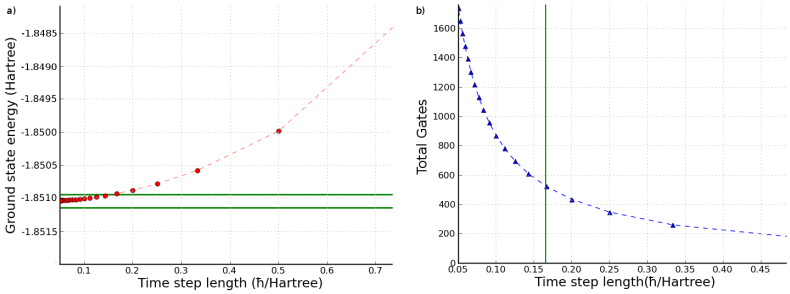


FIG. S2: **Trotter error analysis and resource count for hydrogen molecule using a scalable quantum simulation algorithm**. **(a)** Plot of ground state energy of hydrogen molecule as a function of the length of the time step. As the time step length decreases, the accuracy of the approximation increases in accordance with eqn. (S3). The total time of propagation, t, was unity and this time was split into time steps, dt. The circles are at integer values of the Trotter number, $T_n \equiv t/dt$. Green horizontal lines indicate the bounds for $\pm 10^{-4} E_h$ precision. **(b)** Gates for a single construction of the approximate unitary as a function of time step. As the time step decreases, more gates must be used to construct the propagator. The triangles indicate integer values of the Trotter number and the green vertical line corresponds to the same threshold from graph a. Perfect gate operations are assumed.

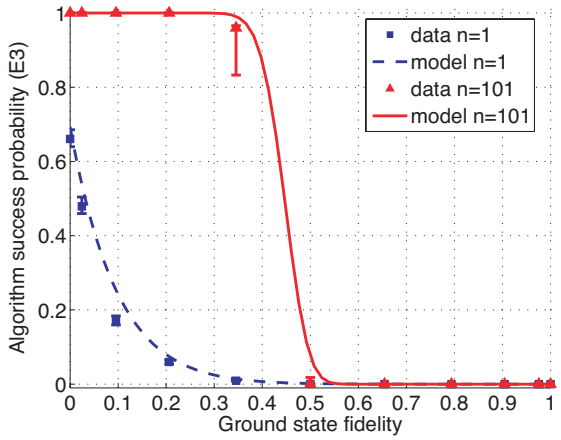


FIG. S3: **Probability of returning the doubly excited state energy**, at 1.3886 a_0 to 20 bits, as a function of the fidelity between the encoded register state and the ground eigenstate. Lines are predictions from a model that allows for experimental imperfections.

3.1 Contribution statement

The author made the following contributions to this work:

- Conceptual development (in collaboration with AAG, MM, JDB, IK, JDW, BJB)
- Design and construction of optical circuits (in collaboration with MPA, MEG, MB)
- Preliminary and final data acquisition (in collaboration with MPA, MEG, GGG)
- Data analysis (in collaboration with GGG)
- Data interpretation
- Complete first draft of the manuscript
- Final draft of the manuscript (in collaboration with all authors)
- Referee replies and corresponding manuscript revision (in collaboration with all authors)

Note that our collaborators from Harvard university derived the gate networks required to simulate each term in the general molecular Hamiltonian and performed the detailed resource count and analysis, which are both presented in the additional online material.

Chapter 4

Experimental quantum computing without entanglement

PRL **101,** 200501 (2008) PHYSICAL REVIEW LETTERS week ending 14 NOVEMBER 2008

Experimental Quantum Computing without Entanglement

B. P. Lanyon,* M. Barbieri,† M. P. Almeida, and A. G. White

Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane 4072, Australia

(Received 15 August 2008; published 13 November 2008)

Deterministic quantum computation with one pure qubit (DQC1) is an efficient model of computation that uses highly mixed states. Unlike pure-state models, its power is not derived from the generation of a large amount of entanglement. Instead it has been proposed that other nonclassical correlations are responsible for the computational speedup, and that these can be captured by the quantum discord. In this Letter we implement DQC1 in an all-optical architecture, and experimentally observe the generated correlations. We find no entanglement, but large amounts of quantum discord—except in three cases where an efficient classical simulation is always possible. Our results show that even fully separable, highly mixed, states can contain intrinsically quantum mechanical correlations and that these could offer a valuable resource for quantum information technologies.

DOI: 10.1103/PhysRevLett.101.200501 PACS numbers: 03.67.Lx, 03.67.Ac

While a great deal of work has been done on the conventional pure-state models of quantum computing [1,2], relatively little is known about computing with mixed states. Deterministic quantum computation with one pure qubit (DQC1) is a model of computation that employs only a single qubit in a pure state, alongside a register of qubits in the fully mixed state [3]. While this model is not universal—it cannot implement any arbitrary algorithm—it can still efficiently solve important problems that are thought to be classically intractable. One of the original applications identified was the simulation of quantum systems [3]. Since then exponential speedups have been identified in estimating the average fidelity decay under quantum maps [4], quadratically signed weight enumerators [5], and the Jones Polynomial in knot theory [6]. DQC1 also affords efficient parameter estimation at the quantum metrology limit [7]. That such a useful tool could be built with only a single pure quantum bit is particularly appealing given the current state of experimental quantum computing, where decoherence is a significant obstacle in the path to large-scale implementations.

Besides its practical applications, DQC1 is also fascinating from a fundamental perspective. Its power is thought to lie somewhere between universal classical and quantum computing—it is strictly less powerful than a universal quantum computer [3] and no efficient classical simulation has been found or thought likely to exist [8,9]. Furthermore its power is thought not to come from the generation of entanglement, which is at most marginally present in DQC1 [9]. This is surprising, as entanglement is widely believed to lie at the heart of the advantages offered by a quantum computer—a belief supported by the discovery that a universal pure-state quantum computer must generate a large amount of entanglement in order to offer any speedup over a classical computer [10,11]. However, no such proof exists for mixed-state models. Instead it has been proposed that DQC1 generates other types of nonclassical correlations and that these are responsible for the computational advantage [8,12–14].

In this Letter we present a small-scale implementation of DQC1 in a linear-optic architecture [15]. We observe and fully characterize the predicted nonclassical correlations. Our results show that while there is no entanglement, other intrinsically quantum mechanical correlations are generated, except in the cases where an efficient classical simulation is always possible. Furthermore, we demonstrate that a small fraction of a single pure quantum bit is enough to implement DQC1 efficiently [9]. This represents the first implementation of DQC1 outside of a liquid-state NMR architecture, in which the question of nonclassical correlations was not addressed [16]. Unlike liquid-state NMR, there are several known paths to scalable linear-optic quantum computing [2,17,18], and there is active development of the necessary technology [19–21].

We perform a first-order implementation of the DQC1 algorithm for estimating the normalized-trace of a unitary matrix [3,8,9,12]. This achieves an exponential speedup over the best known classical approach; i.e., it requires exponentially fewer resources as the size of the unitary increases. It is thought highly unlikely that an efficient, but as yet unknown, classical approach can exist [9]. That DQC1 can perform this task efficiently underpins its ability to solve the range of practical problems listed above.

Figure 1 shows the normalized-trace estimation algorithm. The required input state is separable and consists of a single pure qubit c (control) in the logical state $|0\rangle\langle 0|$, and a register of n qubits in the completely mixed state $I_n/2^n$, where I_n is the n-qubit identity. The circuit consists of the standard Hadamard gate [1] applied to the control qubit, and a unitary (U_n) on the register controlled by qubit c. The state of all $n+1$ qubits at the output of the circuit is

$$\rho_{\mathrm{cr}} = \frac{1}{2N}\begin{bmatrix} I_n & U_n^\dagger \\ U_n & I_n \end{bmatrix}, \tag{1}$$

where $N = 2^n$. The reduced state of qubit c—achieved by

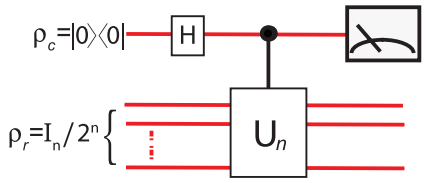


FIG. 1 (color online). Algorithm for estimating the normalized trace of the unitary operator U_n, using deterministic quantum computing with 1-qubit (DQC1). I_n is the n-qubit identity. Repeated running of the circuit and measurement of qubit c in the Pauli X (Y) basis yields an estimate of the corresponding expectation value, from which one can derive the real (imaginary) part of the normalized trace ($\mathrm{Tr}[U_n]/2^n$).

performing a partial trace over the register—is given by

$$\rho_c = \frac{1}{2}\begin{bmatrix} 1 & \mathrm{Tr}[U_n]^\dagger/N \\ \mathrm{Tr}[U_n]/N & 1 \end{bmatrix}. \tag{2}$$

Thus the normalized trace of U_n is encoded in the coherences of qubit c, and can be retrieved by measuring the expectation values of the standard Pauli operators X and Y, since $\langle X\rangle = \mathrm{Re}[\mathrm{Tr}(U_n)/N]$ and $\langle Y\rangle = -\mathrm{Im}[\mathrm{Tr}(U_n)/N]$.

An expectation value is estimated by repeatedly running the circuit. One can achieve a fixed accuracy ϵ in this estimate with a number of runs $L \sim \ln(P_e^{-1})/\epsilon^2$, where P_e is the probability that the estimate is farther from the true value than ϵ [9]. That the accuracy does *not* scale with the size of the unitary, and scales logarithmically with the error probability, means that this is an efficient algorithm for estimating the normalized-trace. In contrast, classical approaches suffer an exponential increase in the required number of resources with the size of the unitary [9]. Note that the algorithm does not efficiently return the full trace $\mathrm{Tr}[U_n]$. This would require multiplying the estimate of the normalized trace by 2^n, thereby amplifying the uncertainty by an amount that is exponential in the size of the unitary.

We implement the first-order ($n = 1$) case for

$$U_1 = Z_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}. \tag{3}$$

In this case $\langle X\rangle = (1 + \cos\theta)/2$ and $\langle Y\rangle = (\sin\theta)/2$. Our implementation is shown in Fig. 2. We encode quantum information in the polarization of single photons. Single qubit gates are realized deterministically using birefringent wave plates. The two-qubit controlled-Z_θ gate is realized nondeterministically using a recently developed technique requiring only one cnot [15]. Measurement of single photons in the two output modes signals a successful run of the algorithm and occurs with probability $1/12$.

Each photonic qubit is passed through a polarization interferometer, allowing the preparation of noisy (mixed) states by introducing a path difference between the two arms, Fig. 2. A path difference greater than the photon coherence length results in a fully decohered—that is, a fully mixed—photonic qubit. By tuning the path difference

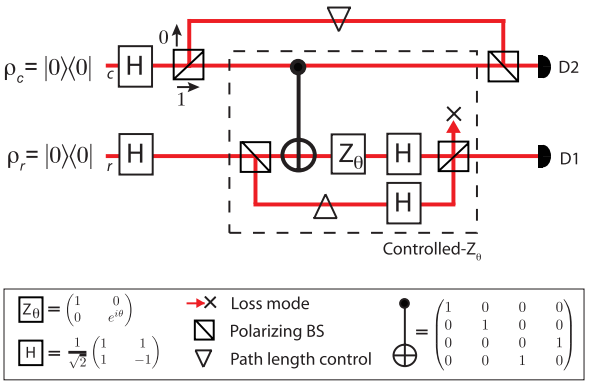


FIG. 2 (color online). Experimental schematic. Qubits at the input and output are encoded in the polarization of single photons ($|0\rangle = |H\rangle$, $|1\rangle = |V\rangle$, horizontal and vertical). Coincident measurement of single photons at fiber-coupled counting modules (D1, D2) signals a successful run of the algorithm. Photons are generated via spontaneous parametric down conversion of a frequency-doubled mode-locked Ti:sapphire laser (820 nm $\rightarrow$ 410 nm, $\Delta\tau = 80$ fs at 82 MHz) pumping a type-I 2 mm BiB_3O_6 crystal; filtered to 820 ± 1.5 nm; collected into two single-mode optical fibers; then injected into free-space modes c and r. With 100 mW at 410 nm, we measure a twofold coincidence rate at the output of the optical circuit of $\approx$100 s^{-1}. Interferometers are realized using calcite beam displacer pairs, rotating one displacer of a pair about an axis perpendicular to the plane defined by the two paths enables relative path length control. The two-qubit gate is realized nondeterministically as described in Ref. [29].

between zero and the photon coherence length we can accurately control the level of mixture in the qubit between zero and maximum, respectively.

We implement the algorithm over the range $-\pi \le \theta \le \pi$ Eq. (3). Figure 3(a) compares the experimentally observed results with the theoretical prediction (calculated assuming perfect circuit operation and measured input states). We observe high correlation between experiment and theory quantified by a reduced χ^2 of 0.7 (real curve) and 1.2 (imaginary curve) [22]. Deviations are due to imperfect circuit operation caused by optical beam steering as θ is varied, interferometric instability and nonclassical interference instability. These effects could be reduced by moving to micro-optic systems [21].

Interestingly, the exponential speedup offered by this algorithm is not compromised by reducing the purity of qubit c [9]. Consider replacing the initial state of this qubit with the mixed state $\frac{1}{2}\{I_1 + \alpha Z\}$, where α now reflects the purity ($p = [1 + \alpha^2]/2$, $0 \le \alpha \le 1$). At the output of the circuit the state is now given by

$$\rho_c = \frac{1}{2}\begin{bmatrix} 1 & \alpha\mathrm{Tr}[U_n]^\dagger/N \\ \alpha\mathrm{Tr}[U_n]/N & 1 \end{bmatrix}. \tag{4}$$

The effect of mixture in qubit c is to reduce $\langle X\rangle$ and $\langle Y\rangle$ by α [Eq. (2)], thereby making it harder to estimate the normalized-trace. To achieve the same fixed accuracy as

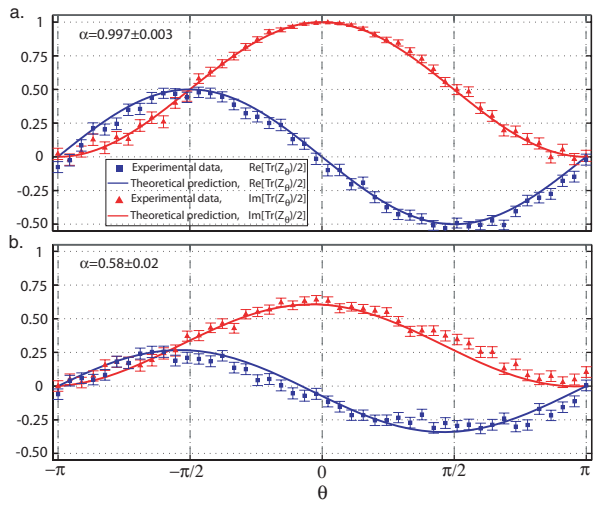


FIG. 3 (color online). Algorithm output. Real (blue or dark gray) and imaginary (red or gray) parts of the normalized-trace measured for two values of α, over a range of θ, Eq. (4). α is the degree of purity of the control qubit as described in the text. $\langle X\rangle$ is estimated by counting the number of coincident photon pairs ($N_\pm$) when projecting qubit c into the states $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, over 10 sec. Then $\langle X\rangle = (N_+ - N_-)/(N_+ + N_-)$. The same technique is used to estimate $\langle Y\rangle$, but in this case we project into the states $|\pm i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$. All error bars are calculated assuming Poissonian uncertainties in the counting statistics. We use the standard definition for a reduced-χ^2 calculation [22], allowing for 3 degrees of freedom [the real and imaginary parts of the trace are simple trigonometric functions defined by an amplitude, frequency and phase, Eq. (3)]. Note that the goal of the algorithm is to return the normalized trace. The full trace is not required for the DQC1 applications mentioned in the introduction.

before requires an increased number of runs $L' \sim L/\alpha^2$. While this clearly adds an additional overhead, as long as α is nonzero, the algorithm still provides an efficient evaluation of the trace. Even access to the tiniest fraction of a single pure qubit is sufficient to achieve an exponential speedup over the best known classical approach.

Figure 3(b) compares the experimentally observed algorithm results with the theoretical predictions (calculated assuming perfect circuit operation and measured input states), for the measured value of $\alpha = 0.58 \pm 0.02$. We observe a high degree of correlation between experiment and theory quantified by a reduced χ^2 of 1.8 (real curve) and 2.0 (imaginary curve). The increased χ^2 in this case [compared to Fig. 3(a)] is due to a less favorable optical alignment, not an intrinsic error associated with initializing c into a mixed state. The additional resource overhead is reflected in the amplitude reduction by a factor of α compared with the results shown in Fig. 3(a). Note that in the limit where the control qubit is completely incoherent, $\alpha = 1$, the entire input state is fully mixed and any unitary evolution leaves the state unchanged—the algorithm does not work. The ability to prepare the control qubit in a superposition state that is at least partially coherent is a necessary condition for a computational speedup. However, as we show later, it is not sufficient.

We analyze the correlations generated by the algorithm by performing tomography of the two-qubit output state, Eq. (1), using 36 (overcomplete) measurement bases. This allows a reconstruction of the density matrix, from which the correlations can be derived. Figure 4 shows two measures of nonclassical correlations—the well-known *tangle* [24,25] and the lesser-known *discord* [12–14]. The tangle is a complete measure of entanglement in two-qubit states, and represents perhaps the most striking divergence from classical behavior. However, entanglement is not the only kind of nonclassical correlation. A far stronger measure, which encompasses entanglement and more, is given by the discord.

The discord is concerned with a fundamental characteristic of classical systems—that their information content is locally accessible and can be obtained without perturbing the state for independent observers [14]. If the discord is zero there exists a local measurement protocol under which all the state information can be revealed, without perturbing the state for observers who do not have access to the measurement results. If the discord is nonzero then no such protocol exists. For pure states, discord is a measure of entanglement—no other nonclassical correlations can be distinguished. However, for mixed states the discord captures more nonclassical correlations than entanglement [12].

The results show that, to within experimental error, our implementation does not give rise to any entanglement. However, in general it does generate quantum discord. We observe a high degree of correlation between the theoretical and measured discord values, quantified by a reduced χ^2 of 1.6. These results are consistent with recent theoretical work [12] which predicts that, although the entanglement is generally zero for arbitrary instances of this algorithm, discord is consistently present.

In our implementation the discord is zero in two distinct cases, $\theta = \{0, \pm\pi\}$, corresponding, respectively, to the controlled-Z_θ gate implementing the identity I and the controlled-sign gate $CZ_{\pm\pi}$. Both of these gates are members of the Clifford group, as is the Hadamard [1]. Thus in these cases the entire state evolution is implemented only by gates from the Clifford group. Further, the algorithm involves preparing the input in a mixture of logical basis states, and measurement of observables in the Pauli group [1]. Under these conditions the Gottesman-Knill theorem states that the entire algorithm can *always*—i.e., for an arbitrary-size implementation—be efficiently simulated on a classical computer [1,26]. In contrast, for all other values of θ the action of the controlled-Z_θ gate is responsible for a non-Clifford-group evolution. There is no known classical method to efficiently simulate an arbitrary-size algorithm that evolves in this way—thereby allowing for a quantum speedup. It is also straightforward to show that an implementation of the algorithm composed entirely of gates from the Clifford group produces a state with zero discord

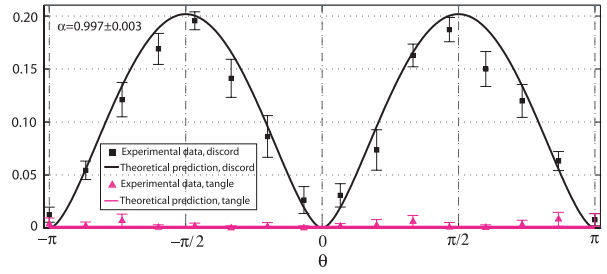


FIG. 4 (color online). Nonclassical correlations generated by our DQC1 algorithm. Discord and tangle are derived from the reconstructed density matrices measured at the algorithm output for $\alpha = 0.997 \pm 0.003$ [Fig. 3(a)]. Discord is calculated by optimizing over all 1-qubit projective measurements on qubit c, Fig. 1 [26]. Theoretical predictions are calculated using measured input states and assuming perfect circuit operation.

(this is true to any order [26]). These results suggest a link between discord and the potential for computational speedup. An important path for further research is to determine whether all DQC1 circuits that do not generate discord can be efficiently simulated on a classical computer. Such a result would provide strong evidence that the discord is a more accurate measure than entanglement of the resources required for a quantum speedup.

Our circuit does not generate entanglement: it takes a mixture of separable states at the input to a different mixture of separable states at the output [26]. Indeed, this is true for an arbitrary-size DQC1 implementation, with respect to the partition between the register and the control [4,9]. In general both the input and output consist of a mixture of 2^n separable states. The key to the computational power is that the mapping between the input and output terms is highly nontrivial: any classical simulation would need to keep track of the evolution of all 2^n state amplitudes. In the case of a Clifford group evolution the mapping is trivial, and a classical simulation is efficient.

We have demonstrated a quantum algorithm that achieves an exponential speedup over the best known classical approach, and yet does not employ entanglement. Instead we observed that the model generates other nonclassical correlations that can exist even in fully separable highly mixed states. Besides the fundamental interest, this could have implications in the many burgeoning quantum computing architectures where environmental decoherence presents a significant obstacle to universal pure-state quantum computing. It is of interest to explore quantum discord in other contexts, such as ''nonlocality without entanglement'' [27,28]—while the two-qubit states of interest in these works are not entangled they have nonzero discord, signifying the presence of quantum correlations.

The authors wish to thank C. Caves, A. Datta, A, Shaji, and G. Vidal for discussions. We acknowledge financial support from the Australian Research Council and the IARPA-funded Army Research Office Contract No. W911NF-05-0397.

*Corresponding author.
lanyon@physics.uq.edu.au
†Present address: Laboratoire C. Fabry, Institut d'Optique, France.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
[3] E. Knill and R. Laflamme, Phys. Rev. Lett. **81**, 5672 (1998).
[4] D. Poulin, R. Blume-Kohout, R. Laflamme, and H. Ollivier, Phys. Rev. Lett. **92**, 177906 (2004).
[5] E. Knill and R. Laflamme, Inf. Proc. Lett. **79**, 173 (2001).
[6] P. W. Shor and S. P. Jordan, Quantum Inf. Comput. **8**, 681 (2008).
[7] S. Boixo and R. D. Somma, Phys. Rev. A **77**, 052320 (2008).
[8] A. Datta and G. Vidal, Phys. Rev. A **75**, 042310 (2007).
[9] A. Datta, S. T. Flammia, and C. M. Caves, Phys. Rev. A **72**, 042316 (2005).
[10] R. Jozsa and N. Linden, Proc. R. Soc. A **459**, 2011 (2003).
[11] G. Vidal, Phys. Rev. Lett. **91**, 147902 (2003).
[12] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).
[13] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
[14] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
[15] B. Lanyon *et al.*, arXiv:0804.0272v1 [Nature Phys. (to be published)].
[16] C. A. Ryan, J. Emerson, D. Poulin, C. Negrevergne, and R. Laflamme, Phys. Rev. Lett. **95**, 250502 (2005).
[17] E. Knill, R. Laflamme, and G. J. Milburn, Nature (London) **409**, 46 (2001).
[18] J. L. O'Brien, Science **318**, 1567 (2007).
[19] Special Issue on Single photons on demand [New J. Phys. **6**, 85 (2004)].
[20] Special Issue on Single-photon: detectors, applications, and measurement [J. Mod. Opt. **51**, 1265 (2004)].
[21] A. Politi *et al.*, Science **320**, 646 (2008).
[22] $\chi^2 = (N - M)^{-1} \sum_1^N (a_i - b_i)^2/\sigma_i^2$ where: N is the number of sample points, $M = 3$ is the number of fitting parameters in our functions; a_i is the ith data point; b_i is the ith theoretical point; and σ_i is the uncertainty in a_i [23].
[23] J. R. Taylor, *An Introduction to Error Analysis* (University Science Books, Sausalito, CA, 1997).
[24] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
[25] A. G. White, D. F. V. James, W. J. Munro, and P. G. Kwiat, Phys. Rev. A **65**, 012301 (2001).
[26] See EPAPS Document No. E-PRLTAO-101-019847 for mathematical details of the proofs cited in the text. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.
[27] C. H. Bennett *et al.*, Phys. Rev. A **59**, 1070 (1999).
[28] G. J. Pryde, J. L. O'Brien, A. G. White, and S. D. Bartlett, Phys. Rev. Lett. **94**, 220406 (2005).
[29] N. K. Langford *et al.*, Phys. Rev. Lett. **95**, 210504 (2005).

Experimental quantum computing without entanglement: supplementary material

B. P. Lanyon, M. Barbieri, M. P. Almeida and A. G. White
Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane 4072, Australia

The Gottesman-Knill theorem for mixed state preparation.
The Gottesman-Knill theorem applies to algorithm input states prepared in the logical basis. In the DQC1 model the input is a mixture of logical basis states [1]. However, it is straightforward to show that such an input state can be prepared from a pure logical state using only a number of additional Clifford group gates and ancilla qubits that is linear in the size of the input state. As such the DQC1 input state satisfies the conditions under which the theorem is valid.

Definition of quantum discord for a two-qubit system.
The definition of the mutual information for a bipartite density matrix is [1, 2],

$$\mathcal{I}(r{:}c)=H(\rho_c)+H(\rho_r)-H(\rho_{cr}), \tag{1}$$

where $H(\rho)$ is the well-known Von Neumann entropy [1] of the state ρ. An alternative definition is given by,

$$\mathcal{J}(r{:}c)=H(\rho_r)-\tilde{H}(\rho_{cr}|c), \tag{2}$$

where $\tilde{H}(\rho_{cr}|c)$ is the extension of the classical conditional entropy to the quantum case [2]. This is obtained by minimising the average entropy of the subsystem r, over all possible projective conditional measurements on c,

$$\tilde{H}(\rho_{cr}|c)=\min_{\{\Pi_i\}}\sum_i p_i H(\rho_{r|\Pi_i}), \tag{3}$$

where $p_i{=}\mathrm{Tr}(\Pi_i\rho_{cr}\Pi_i)$ and $\rho_{r|\Pi_i}{=}\mathrm{Tr}_c(\Pi_i\rho_{cr}\Pi_i)/p_i$. The discord is the difference [2],

$$\mathcal{D}(r,c)=\mathcal{I}(r{:}c)-\mathcal{J}(r{:}c). \tag{4}$$

Notice that $\mathcal{J}(r{:}c)$ is not symmetrical by inversion of c and r, therefore, in general, discord is directional: $\mathcal{D}(r,c)\neq\mathcal{D}(c,r)$; we might not be able to detect quantum correlation when conditioning on measurements of one partition, while they arise when considering the inverse case. It is straightforward to show that states admitting a diagonal representation in a local basis have bidirectionally vanishing discord—they contain only classical correlations.

Proof that DQC1 clifford evolution generates no discord.
The DQC1 input state can be written in the form,

$$\rho_{\mathrm{in}}{=}\frac{1}{2^{n+1}}\left(\mathrm{I}^{\otimes n+1}+\mathrm{Z}\otimes\mathrm{I}^{\otimes n}\right), \tag{5}$$

which is clearly diagonal in the logic basis, hence it has zero discord in both directions. The action of Clifford group gates is to map Pauli matrices into Pauli matrices. If we indicate the unitary action of the circuit by W, the input state ρ_{in} is transformed into,

$$\begin{aligned}\rho_{\mathrm{cr}}&{=}\frac{1}{2^{n+1}}\left(\mathrm{I}^{\otimes n+1}{+}\mathrm{W}(\mathrm{Z}\otimes\mathrm{I}^{\otimes n})\mathrm{W}^\dagger\right)\\&{=}\frac{1}{2^{n+1}}\left(\mathrm{I}^{\otimes n+1}+\bigotimes_{i=1}^{n+1}\sigma_r^{(i)}\right),\end{aligned} \tag{6}$$

where $\sigma_r^{(i)}$ refers to the i-th qubit, and $r{=}\{0,1,2,3\}$ respectively labels the Pauli matrices $\{\mathrm{I},\mathrm{Z},\mathrm{X},\mathrm{Y}\}$. The state (6) is locally equivalent to the state,

$$\rho'{=}\frac{1}{2^{n+1}}\left(\mathrm{I}^{\otimes n+1}+\bigotimes_{i=1}^{n+1}\sigma_s^{(i)}\right), \tag{7}$$

where the index s can take only the values $s{=}\{0,1\}$. Thus ρ' admits a diagonalisation in a local basis: this state is purely classically correlated, and hence its discord is zero. Consequently ρ_{out}, which is obtained from ρ' with local rotations, must have zero discord.

Proof that our circuit generates no entanglement.
Figure (1) in the main text shows the DQC1 algorithm. In our implementation we employ a single register qubit and U is an arbitrary rotation about the logical axis. The initial state of the control and register qubits, after the Hadamard gate, can be written as,

$$\rho_{in}{=}|\Psi_1\rangle\langle\Psi_1|{+}|\Psi_2\rangle\langle\Psi_2|, \tag{8}$$

where $|\Psi_1\rangle{=}|+,0\rangle_{c,r}$, $|\Psi_2\rangle{=}|+,1\rangle_{c,r}$, and $|+\rangle{=}(|0\rangle{+}|1\rangle)/\sqrt{2}$, i.e. the input is a mixture of pure separable states. We can look at the evolution of each of these states through our DQC1 circuit (consisting of a CZ_θ gate) separately,

$$\begin{aligned}\mathrm{CZ}_\theta|\Psi_1\rangle&=\mathrm{CZ}_\theta|+,0\rangle_{c,r}\\&=\mathrm{CZ}_\theta(|0,0\rangle{+}|1,0\rangle)_{c,r}\\&=|0,0\rangle{+}|1,0\rangle_{c,r}\\&=|\Psi_1\rangle\end{aligned} \tag{9}$$

and,

$$\begin{aligned} \mathrm{CZ}_\theta|\Psi_2\rangle &= \mathrm{CZ}_\theta|+,1\rangle_{c,r} \\ &= \mathrm{CZ}_\theta(|0,1\rangle+|1,1\rangle)_{c,r} \\ &= (|0,1\rangle+e^{i\theta}|1,1\rangle)_{c,r} \\ &= |\phi,1\rangle \\ &= |\Psi_2'\rangle. \end{aligned} \tag{10}$$

Therefore the output state is given by a new mixture of separable states—no entanglement is generated,

$$\rho_{out}=|\Psi_1\rangle\langle\Psi_1|+|\Psi_2'\rangle\langle\Psi_2'|. \tag{11}$$

Note that if instead the register qubits where initialised into a superposition with some degree of coherence, then our circuit would generate entanglement (for all values except θ=0). In this sense the absence of coherence in the qubit register is responsible for the absence of entanglement in the output state.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000), ISBN 521635039.

[2] A. Datta, A. Shaji, and C. M. Caves, Phys. Rev. Lett. **100**, 050502 (2008).

4.1 Contribution statement

The author made the following contributions to this work:

- Optical circuit construction (in conjunction with MPA and MB)
- Project initialisation, conceptualisation and development (in conjunction with MB)
- Preliminary and final data acquisition (in conjunction with MB and MPA)
- Data analysis, interpretation and figure construction
- First complete draft of the manuscript
- Final draft of the manuscript (in collaboration with all authors)
- corresponding author duties

Part III

Quantum state engineering

Chapter 5

Manipulating biphotonic qutrits

PRL **100,** 060504 (2008) PHYSICAL REVIEW LETTERS week ending 15 FEBRUARY 2008

Manipulating Biphotonic Qutrits

B. P. Lanyon,[1] T. J. Weinhold,[1] N. K. Langford,[1] J. L. O'Brien,[2] K. J. Resch,[3] A. Gilchrist,[1] and A. G. White[1]

[1]*Department of Physics and Centre for Quantum Computer Technology, University of Queensland, Brisbane, Australia*

[2]*Centre for Quantum Photonics, H. H. Wills Physics Laboratory and Department of Electrical and Electronic Engineering, University of Bristol, Bristol, United Kingdom*

[3]*Institute for Quantum Computing and Department of Physics & Astronomy, University of Waterloo, Waterloo, Canada*

(Received 18 July 2007; published 14 February 2008)

Quantum information carriers with higher dimension than the canonical qubit offer significant advantages. However, manipulating such systems is extremely difficult. We show how measurement-induced nonlinearities can dramatically extend the range of possible transforms on biphotonic qutrits—three-level quantum systems formed by the polarization of two photons in the same spatiotemporal mode. We fully characterize the biphoton-photon entanglement that underpins our technique, thereby realizing the first instance of qubit-qutrit entanglement. We discuss an extension of our technique to generate qutrit-qutrit entanglement and to manipulate any bosonic encoding of quantum information.

DOI: 10.1103/PhysRevLett.100.060504 PACS numbers: 03.67.Mn, 03.65.Ud, 03.65.Wj, 42.50.Dv

Higher dimensional systems offer advantages such as increased security in a range of quantum information protocols [1–7], greater channel capacity for quantum communication [8], novel fundamental tests of quantum mechanics [9,10], and more efficient quantum gates [11]. Optically such systems have been realized using polarization [12] and transverse spatial modes [1,13]. However in each case state transformation techniques have proved difficult to realize. In fact, performing such transformations is a significant problem in a range of physical architectures.

The polarization of two photons in the same spatiotemporal mode represents a three-level bosonic quantum system, a biphotonic qutrit, with symmetric logical basis states: $|0_3\rangle \equiv |2_H, 0_V\rangle$, $|1_3\rangle \equiv (|1_H, 1_V\rangle + |1_V, 1_H\rangle)/\sqrt{2}$, and $|2_3\rangle \equiv |0_H, 2_V\rangle$ [14]. The simple optical tools which allow full control over the polarization of a photonic qubit are insufficient for full control over a biphotonic qutrit [15]. Consequently even simple state transformations required in qutrit generation, processing, and measurement are extremely limited. Significant progress has been made in biphoton state generation. For example, complex arbitrary state preparation techniques that employ multiple nonlinear crystals [12] and nonmaximally entangled states [16] have been developed.

Here we present and demonstrate a technique that dramatically extends the range of biphotonic qutrit transforms, for use in all stages of qutrit manipulation. The technique is based on a Fock-state filter which employs a measurement-induced nonlinearity to conditionally remove photon number (Fock) states from superpositions [17–22]. We first demonstrate the action of the filter as a qutrit polarizer, which can conditionally remove a single logical qutrit state from a superposition. We then combine this nonlinear operation with standard wave plate rotations to demonstrate the dramatically increased range of qutrit transforms it enables. Finally we present the first instance and full characterization of a polarization entangled photon-biphoton state, which underpins the power of our technique. Such qubit-qutrit states have been studied extensively [23–29] and we suggest an extension to generate this type of entanglement.

We generate our qutrits through double-pair emission from spontaneous parametric down-conversion (Fig. 1). Fourfold coincidences between detectors D1–D4 select, with high probability, the cases of double-pair emission into inputs 1 and 2. The biphoton state in mode 1 is passed through a horizontal polarizer to prepare the logical qutrit state $|0_3\rangle$. Input 2 is passed through a 50% beam splitter; detection at D1 indicates a single photon in mode b; after a polarizing beam splitter this prepares the ancilla polarization qubit ($|0_2\rangle \equiv |1_H\rangle$, $|1_2\rangle \equiv |1_V\rangle$) in the logical state $|0_2\rangle$. Thus a qubit and qutrit arrive simultaneously at the central 50% beam splitter.

A Fock filter relies on nonclassical interference effects [30]. When two indistinguishable photons are injected into modes a and b (Fig. 1), the probability of detecting a single photon in mode d is zero; if two or more photons are injected into mode a, then this probability is nonzero. By injecting a single photon into mode b and detecting a single photon in mode d, single photon terms can therefore be removed from any photon number superposition states

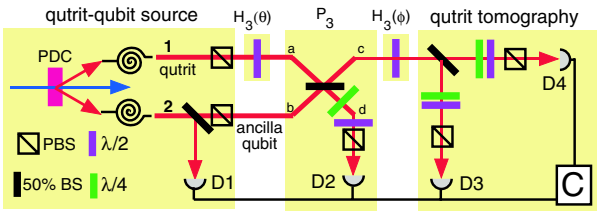


FIG. 1 (color online). Experimental schematic. Emission from a parametric down-conversion (PDC) crystal is coupled into single-mode fiber and injected into modes 1 and 2. Coincident (C) detection of photons at D1–4 selects, with high probability, the cases of double photon-pair emission from the PDC source.

arriving in mode a. By varying the reflectivity of the beam splitter it is possible to conditionally remove any number state from a superposition [21]. This Fock-state filter acts only on light with the same polarization as the ancilla (in our case, horizontal), so by detecting a single horizontal photon in mode d, the logical qutrit state $|1_3\rangle$ is blocked, since it contains a single photon with the same polarization as the ancilla. The remaining logical qutrit states are coherently attenuated.

For a beam splitter of reflectivity 50% the filter acts as a qutrit polarizer described by the operator $\mathbf{P}_3 = |0_3\rangle\langle 0_3| - |2_3\rangle\langle 2_3|$. By varying the polarization of the ancilla, and the reflectivity of the central beam splitter, the operation of our lossy qutrit polarizer can be tuned to preferentially remove the $|0_3\rangle$, $|1_3\rangle$, or $|2_3\rangle$ states. We choose to demonstrate removal of the $|1_3\rangle$ state and include the general operation of the filter for an arbitrary beam splitter reflectivity [31].

The qutrit polarizer offers a powerful tool for transforming between qutrit states. For example, consider the initial qutrit state $|0_3\rangle$ injected into input 1, the red dot of Fig. 2. The black ring shows the limited range of qutrit states, with real coefficients, that are accessible using wave plates [32]. By including the qutrit polarizer the range is dramatically extended to the closed sphere in Fig. 2; the transformation to any real state is possible.

We measure our qutrits by passing mode c through a 50% beam splitter and performing polarization analysis of the two outputs in coincidence, as shown in Fig. 1. This nondeterministically discriminates the logical states $|0_3\rangle$, $|1_3\rangle$, and $|2_3\rangle$ with probabilities $p(0_3) = \frac{1}{2}$, $p(1_3) = \frac{1}{4}$, and $p(2_3) = \frac{1}{2}$. Combining it with single qubit rotations after the beam splitter allows us to perform full qutrit state tomography of mode c. Complete qutrit tomography requires nine independent measurements, which we construct from logical basis states and two-part superpositions [1]. Our method differs from that of Refs. [14,15]. We use convex optimization to reconstruct the qutrit density matrix and Monte Carlo simulations for error analysis [33,34].

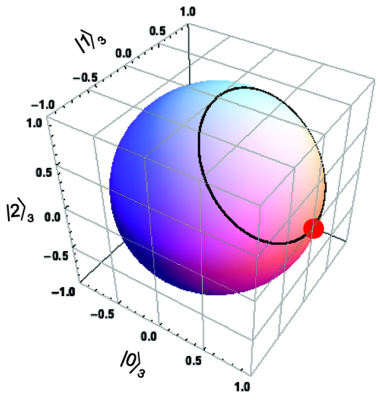


FIG. 2 (color online). Comparison of the range of linearly polarized qutrit states achievable by transforming the state $|0_3\rangle$ (red dot); when using only wave plate operations (black ring); by incorporating our qutrit polarizer, $\mathbf{Q}_3(\alpha)\mathbf{H}_3(\phi)\mathbf{P}_3(\sqrt{0.5})\mathbf{H}_3(\theta)|0_3\rangle$ (sphere) [31,32].

Ideally both the central and tomography beam splitters reflect 50% of both polarizations. In practice, we found that they deviate by a few percent and impart undesired unitary rotations on the optical modes. For the tomography beam splitter, these imperfections modified the nine measured qutrit states; we characterized this effect and incorporated it into the tomographic reconstruction. We found that the effect of the imperfect central beam splitter on the performance of the qutrit polarizer was negligible.

A frequency-doubled mode-locked Ti:Sapphire laser (820 nm $\rightarrow$ 410 nm, $\Delta\tau = 80$ fs at 82 MHz repetition rate) is used to produce photon pairs via parametric down-conversion from a Type I phase-matched 2 mm Bismuth Borate (BiBO) crystal, filtered by blocked interference filters (820 ± 1.5 nm). We collect the down-conversion into single-mode optical fibers. Photons are detected using fiber-coupled single photon counting modules and coincidences measured using a Labview (National Instruments) interfaced quad-logic card (ORTEC CO4020). When directly coupled into detectors the source yielded twofolds at 60 kHz and singles rates at 220 kHz. At the output of the complete circuit we observed fourfold coincidence rates at approximately 1 Hz.

The quality of the nonclassical interference underpinning the qutrit polarizer can be measured directly [21]. Reference [22] relates nonclassical visibilities to a Fock-state filter's ability to block single photon terms. We set all input states and measurement settings to horizontal. Twofold coincidence counts between D2 and D4 show interference between two single photons with visibility $V_{11} = 97 \pm 1\%$. Fourfolds between detectors D1–D4 detect the interference between a photon and a biphoton with visibility $V_{12} = 68 \pm 4\%$. From these visibilities we predict an extinction ratio of $5(\pm 2)$:1 [22]; i.e., our qutrit polarizer will pass the logical $|0_3\rangle$ and $|2_3\rangle$ states at 5 times the rate it passes the logical $|1_3\rangle$ state.

To demonstrate the qutrit polarizer we include a half wave plate in mode a set to $\theta = \frac{\pi}{8}$ to generate the superposition qutrit state [32]:

$$\mathbf{H}_3(\theta)|0_3\rangle = \cos^2 2\theta|0_3\rangle + \sin^2 2\theta|2_3\rangle + \sin 4\theta|1_3\rangle/\sqrt{2}. \quad (1)$$

We measure the output state in mode c without applying the qutrit polarizer. This is achieved by blocking the ancilla photon in mode b and performing qutrit tomography of mode c in twofold coincidence between D3 and D4. The experimentally reconstructed density matrix is shown in Fig. 3(a) and has a near perfect fidelity between the measured and ideal states, $F = 97 \pm 1\%$, and a low linear entropy, $S_L = 6 \pm 7\%$ [35,36]. We then prepare the output state by unblocking the ancilla and, as in all further cases, perform tomography of mode c in fourfold coincidence between D1–D4. The qutrit polarizer is now "on" and we expect the absorption of the logical $|1_3\rangle$ state. The recon-

structed density matrix is shown in Fig. 3(b) and has a lower fidelity with the ideal, $F = 78 \pm 8\%$, and linear entropy $S_L = 47 \pm 14\%$. The relative reduction in the logical $|1_3\rangle$ state probability, when the filter is turned on, yields an extinction ratio of 6.80($\pm$0.07):1, consistent with that predicted above.

Measured nonclassical visibilities are significantly limited by higher-order parametric down-conversion photon number terms [37,38]. After removing these effects, as described in Ref. [22], we find a corrected twofold visibility of $V'_{11} = 100 \pm 1\%$, which would be measured given an ideal two-photon source (higher-order effects cannot be distinguished from experimental uncertainty in the fourfold visibility). This corrected visibility can be used to predict the potential performance of our circuit given an ideal source [22]; in this case we predict that the filter would pass the logical $|0_3\rangle$ and $|2_3\rangle$ states at least 24 times the rate it passes the logical $|1_3\rangle$ state. Clearly the performance of our qutrit polarizer is significantly limited by higher-order emissions from our optical source.

Figures 3(c) and 3(d) show experimentally reconstructed density matrices of newly accessible states achieved by incorporating the qutrit polarizer with half wave plate operations applied to the initial state of $|0_3\rangle$; $|1_3\rangle$ and $(|0_3\rangle - |1_3\rangle - |2_3\rangle)/\sqrt{3}$. The fidelities with the ideal are $77 \pm 3\%$ and $83 \pm 7\%$ with linear entropies $51 \pm 7\%$ and $38 \pm 15\%$, respectively. These fidelities exceed the maximum achievable using only linear wave plates (50%) by 9 ± 1 and 5 ± 1 standard deviations, respectively.

The qutrit polarizer employs a measurement-induced nonlinearity whereby the biphoton becomes entangled with the ancilla photon. Instead of detecting the ancilla in a single, fixed polarization state, we can also use tomographic measurements to directly investigate this resultant entangled qubit-qutrit system. Without emphasis to the physical systems involved, such states were first studied by Peres as a special case of his negativity criterion for entanglement; a negativity of 0 (> 0) is conclusive of a

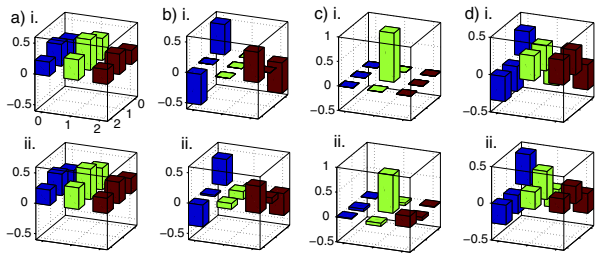


FIG. 3 (color online). Comparison of real parts of (i) ideal and (ii) measured qutrit density matrices. (a) The measured output state with the qutrit polarizer "off" [Eq. (1) for $\theta = \frac{\pi}{8}$]. (b) The output state with the qutrit polarizer "on" showing the removal of the logical $|1_3\rangle$ qutrit state. (c)–(d) Newly accessible qutrit states $|1_3\rangle$ and $(|0_3\rangle - |1_3\rangle - |2_3\rangle)/\sqrt{3}$, respectively. States (b)–(d) all lie on the surface of the sphere of Fig. 2, but not on the ring.

separable (entangled) state [23,39,40]. More recently these states have received a significant amount of attention [23–28] and have been predicted to exhibit novel entanglement sudden death phenomena [29].

On injection of the qutrit state given by Eq. (1) into the Fock filter, we find the following qubit-qutrit joint state of modes c and d:

$$\frac{\cos^2 2\theta|0_2,0_3\rangle + \sin 4\theta|1_2,0_3\rangle + \sin^2 2\theta(\sqrt{2}|1_2,1_3\rangle - |0_2,2_3\rangle)}{N}, \tag{2}$$

where $N = \sqrt{2 - \cos 4\theta}$. By varying θ we can tune the level of entanglement from zero ($\theta = 0$) to near-maximal ($\theta = \frac{\pi}{4}$), with corresponding negativities of 0 to $\sqrt{8/9} \approx 0.94$, respectively. To perform qubit-qutrit state tomography we use 36 independent measurements constructed from all of the combinations of the aforementioned nine qutrit states and four qubit states (H, V, D, R). Figure 4 shows the measured density matrix for the near-maximally entangled case, which corresponds to the preparation of two vertically polarized photons in mode a. There is a high fidelity of $81 \pm 3\%$ with the ideal state and low linear entropy of $17 \pm 5\%$, and the state is highly entangled with a negativity of 0.77 ± 0.05. We note that a maximally entangled state is predicted for $\theta = \frac{\pi}{4}$ and a central beam splitter reflectivity of $R = \sqrt{2}/(\sqrt{2} + 1) \approx 58.6\%$.

Entangling information carriers to ancilla qubits is an extremely powerful technique [41]: such correlations play a central role in the power of the Fock filter to transform biphotonic qutrits. However, the application of our technique is not limited to extending transforms on single qutrits. We propose that the generation of qubit-qutrit entanglement offers a path to realize multiqutrit operations. For example, a pair of entangled qubit-qutrit states could be used to create qutrit-qutrit entanglement by projecting the qubits into an entangled state using well-known techniques. The much anticipated development of high-brightness single photon sources will make such experiments feasible in the near future. We wish to emphasize that our technique is not limited to manipulating biphotons. The Fock filter can be applied to any system where measurement can induce nonlinear effects, that is, any bosonic encoding of quantum information, including bosonic atoms [42] and time-bin, frequency, and orbital angular momentum encoding of photons.

We have shown that measurement-induced nonlinearities offer significant advantages for the manipulation of higher dimensional bosonic information carriers, specifically biphotonic qutrits. We demonstrated a nonlinear qutrit polarizer, capable of conditionally removing a single logical qutrit state from a superposition and greatly extending the range of possible qutrit transforms. Such tools could find application to quickly generate the mutually unbiased basis states required for optimum security in qutrit quantum-key-distribution protocols [5–7] or as a filtering technique to manipulate entanglement in qutrit-

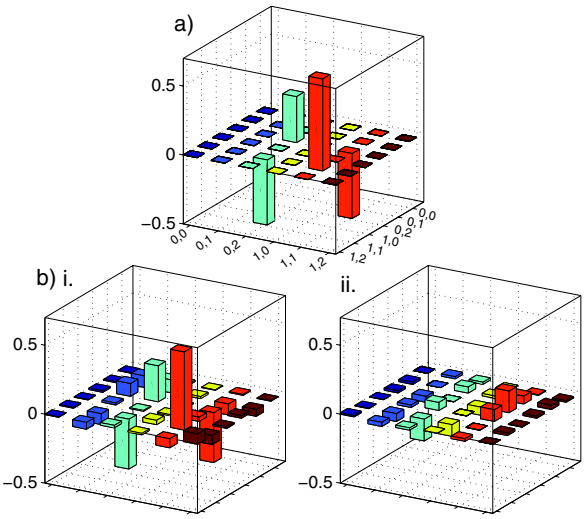


FIG. 4 (color online). Comparison of entangled qubit-qutrit density matrices. (a) Ideal, (b) and (c) measured real and imaginary parts. There is a high fidelity of (81 ± 3%) with the ideal state and low linear entropy (17 ± 5%), and the state is highly entangled with a negativity of 0.77 ± 0.05. The ideal state is given by Eq. (2) for $\theta = \pi/4$. Note the axis label: x,j represents the qubit logical state x and the qutrit logical state j, i.e., $|x_2, j_3\rangle$.

qutrit states. Finally we fully characterized the entangled photon-biphoton state that underpins the power of our technique. This is the first instance of the generation and characterization of entanglement between these distinct physical systems and makes recent theoretical proposals experimentally testable [29]. Besides offering a path to implement novel multiqutrit operations we propose that our technique can be extended to manipulate any bosonic encoding of quantum information.

This work was supported by the Australian Research Council, ARC Discovery Federation, DEST Endeavour Europe programs, and the IARPA-funded U.S. Army Research Office Contract No. W911NF-05-0397.

Note added.—Recently several proposals were presented to which our technique is directly relevant [43–45].

[1] N. K. Langford *et al.*, Phys. Rev. Lett. **93**, 053601 (2004).
[2] R. W. Spekkens and T. Rudolph, Phys. Rev. A **65**, 012310 (2001).
[3] G. Molina-Terriza *et al.*, Phys. Rev. Lett. **92**, 167903 (2004).
[4] S. Gröblacher *et al.*, New J. Phys. **8**, 75 (2006).
[5] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[6] N. J. Cerf *et al.*, Phys. Rev. Lett. **88**, 127902 (2002).
[7] T. Durt *et al.*, Phys. Rev. A **67**, 012311 (2003).
[8] M. Fujiwara *et al.*, Phys. Rev. Lett. **90**, 167906 (2003).
[9] D. Collins *et al.*, Phys. Rev. Lett. **88**, 040404 (2002).
[10] D. Kaszlikowski *et al.*, Phys. Rev. A **65**, 032118 (2002).
[11] T. C. Ralph, K. Resch, A. Gilchrist, Phys. Rev. A **75**, 022313 (2007).
[12] Y. I. Bogdanov *et al.*, Phys. Rev. Lett. **93**, 230503 (2004).
[13] A. Mair *et al.*, Nature (London) **412**, 313 (2001).
[14] Y. Bogdanov *et al.*, arXiv:quant-ph/0411192v1.
[15] Y. I. Bogdanov *et al.*, Phys. Rev. A **70**, 042303 (2004).
[16] G. Vallone *et al.*, Phys. Rev. A **76**, 012319 (2007).
[17] A. Grudka and A. Wojcik, Phys. Rev. A **66**, 064303 (2002).
[18] H. F. Hofmann and S. Takeuchi, Phys. Rev. Lett. **88**, 147901 (2002).
[19] X. Zou, K. Pahlke, and W. Mathis, Phys. Rev. A **66**, 064302 (2002).
[20] K. Sanaka *et al.*, Phys. Rev. Lett. **92**, 017902 (2004).
[21] K. Sanaka, K. J. Resch, and A. Zeilinger, Phys. Rev. Lett. **96**, 083601 (2006).
[22] K. J. Resch *et al.*, Phys. Rev. Lett. **98**, 203602 (2007).
[23] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[24] P. B. Slater, Phys. Rev. A **71**, 052319 (2005).
[25] A. Cabello, A. Feito, and A. Lamas-Linares, Phys. Rev. A **72**, 052112 (2005).
[26] O. Osenda and G. A. Raggio, Phys. Rev. A **72**, 064102 (2005).
[27] S. Jami andM. Sarbishei, arXiv:quant-ph/0606039.
[28] P. B. Slater, arXiv:quant-ph/0702134.
[29] K. Ann and G. Jaeger, arXiv:quant-ph/0707.4485.
[30] C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
[31] For our Fock filter with reflectivity $R = r^2$,

$$\mathbf{P}_3(r) = \begin{bmatrix} r(2-3r^2 & 0 & 0 \\ 0 & r(1-2r^2) & 0 \\ 0 & 0 & -r^3 \end{bmatrix}.$$

[32] From Ref. [15], the wave plate action on a qutrit is

$$\begin{bmatrix} t^2 & \sqrt{2}tr & r^2 \\ -\sqrt{2}tr^* & |t|^2 - |r|^2 & \sqrt{2}t^* r \\ r^{*2} & -\sqrt{2}t^* r^* & t^{*2} \end{bmatrix},$$

where $t = \cos\delta + i\sin\delta\cos 2\theta$, $r = i\sin\delta\sin 2\theta$, and θ is the wave plate angle. For a half wave plate, $\mathbf{H}_3(\theta)$, $\delta = \pi/2$; for a quarter-wave plate, $\mathbf{Q}_3(\theta)$, $\delta = \pi/4$.
[33] A. Doherty and A. Gilchrist (to be published).
[34] J. L. O'Brien *et al.*, Phys. Rev. Lett. **93**, 080502 (2004).
[35] Fidelity is $F(\rho,\sigma) \equiv \{\mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]\}^2$; linear entropy is $S_L \equiv d(1 - \mathrm{Tr}[\rho^2])/(d-1)$, where d is the state dimension.
[36] A. G. White *et al.*, J. Opt. Soc. Am. B **24**, 172 (2007).
[37] J. Fulconis *et al.*, Phys. Rev. Lett. **99**, 120501 (2007).
[38] T. J. Weinhold *et al.*, (to be published).
[39] T. Wei *et al.*, Phys. Rev. A **67**, 022110 (2003).
[40] We define negativity, following [39], as $N = \max\{0, -2 * \sum_i \lambda_i\}$, where λ_i are the negative eigenvalues of the partial transpose of the target density matrix.
[41] E. Knill *et al.*, Nature (London) **409**, 46 (2001).
[42] S. Popescu, Phys. Rev. Lett. **99**, 130503 (2007).
[43] I. Bregman *et al.*, arXiv:quant-ph/0709.3804.
[44] C. Bishop and M. S. Byrd, arXiv:quant-ph/0709.0021.
[45] M. Ali *et al.*, arXiv:0710.2238.

5.1 Contribution statement

The author made the following contributions to this work:

- Preliminary and final data acquisition (in collaboration with NKL, KR and TW)
- Data analysis and interpretation (in collaboration with NKL)
- Figure development and construction
- First complete draft of the manuscript
- Corresponding author duties
- First complete draft of referee replies and manuscript revision
- Final referee replies and manuscript revision (in collaboration with all authors)

5.2 Additional experimental details

Figure 5.1 provides various representations of the optical circuit constructed for this project. Note that the same setup was used for the paper 'Experimentally generating and tuning robust entanglement between photonic qubits' presented in Chapter 6.

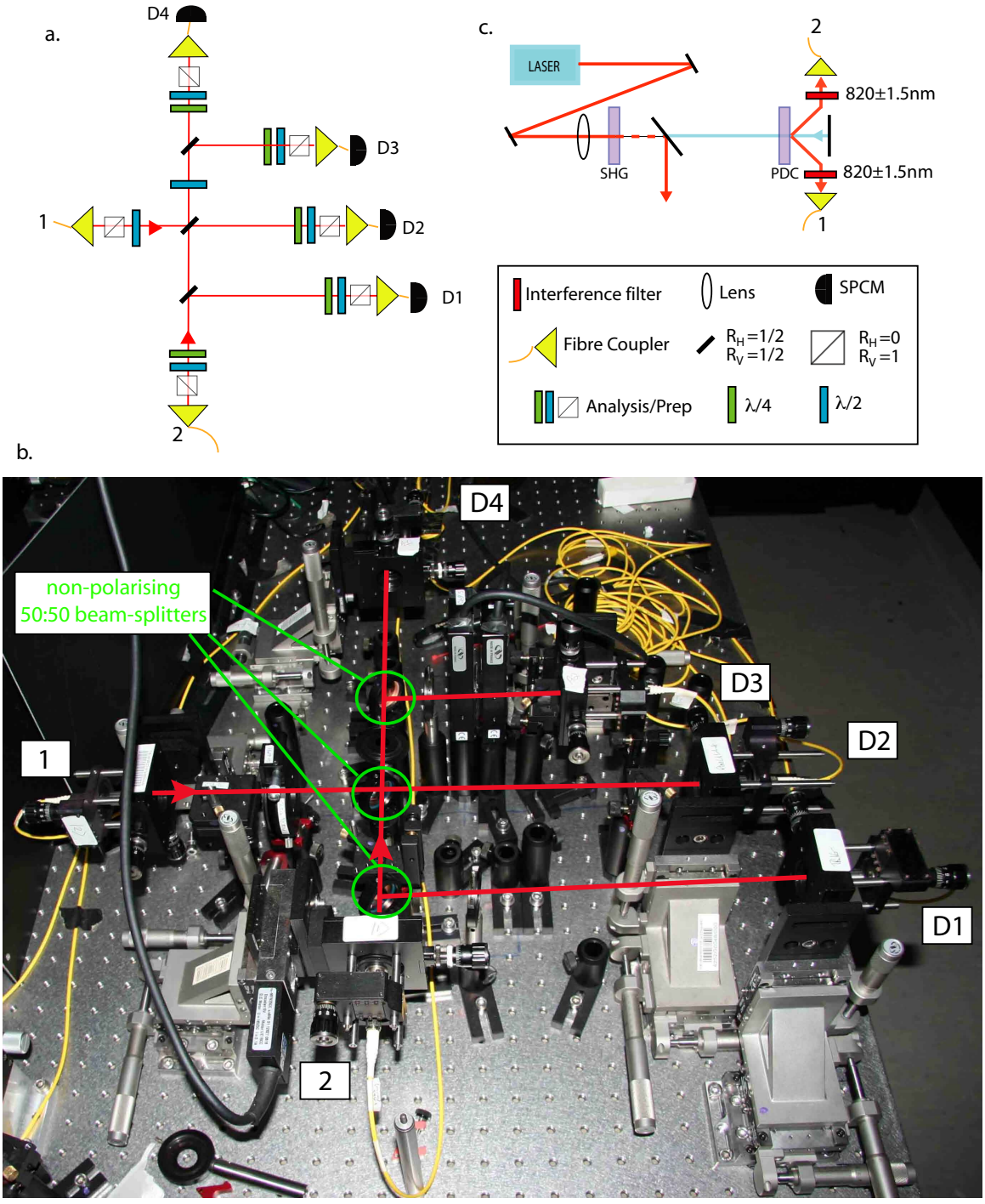


Figure 5.1: **Experimental schematics of the Fock-state filter.** This setup was used for the papers 'Manipulating biphotonic qutrits' (Chapter 5) and 'Experimentally generating and turning robust entanglement between photonic qubits' (Chapter 6). **a.** Optical circuit diagram. **b.** Annotated laboratory photograph of the optical circuit. Many of the wave plates have been removed to make viewing clearer. The photon detectors (SPCMs) are out of shot, but their corresponding fibre couplers have been labelled. **c.** Optical source diagram. SPCM, single-photon counting module; PDC, parametric downconversion; SHG, second-harmonic generation.

Chapter 6

Generating and tuning robust entanglement between three photonic qubits

NJP291111 on 17 November 2008

New Journal of Physics
The open-access journal for physics

Experimentally generating and tuning robust entanglement between photonic qubits

B P Lanyon[1,3] **and N K Langford**[1,2]

[1] Department of Physics and Centre for Quantum Computer Technology, University of Queensland, QLD 4072, Brisbane, Australia
[2] Faculty of Physics, University of Vienna, Boltzmanngasse 5, A-1090 Vienna, Austria
E-mail: lanyon@physics.uq.edu.au

New Journal of Physics **10** (2008) 000000 (9pp)
Received 3 September 2008
Published xx November 2008
Online at http://www.njp.org/
doi:10.1088/1367-2630/9/1/000000

Abstract. We introduce and demonstrate a technique for generating a range of novel multi-photon entangled states. Adjusting a simple experimental parameter allows the preparation of pure states with an arbitrary level of W-class entanglement, from a fully separable state to the maximally robust W state, enabling full control over this entanglement class in our system. Furthermore, the generated states exhibit a highly symmetric entanglement distribution that we show is optimally robust against qubit loss. The ability to prepare entanglement in robust configurations is particularly relevant to many emerging quantum technologies where entanglement is a valuable resource. We achieve a high quality experimental realization for the three-photon case, including a W state fidelity of 0.90 ± 0.03. In addition, we present a new technique for characterizing quantum states in the laboratory in the form of iterative tomography.

Large multipartite entangled states play a central role in many active areas of research including quantum computation, communication and metrology [1]–[3]. However, while entanglement in bipartite quantum systems is well understood, multipartite entanglement is relatively unexplored and offers a far more complex structure; there are various types of entanglement that present significant generation, manipulation and characterization challenges. There has already been much theoretical work devoted to classifying and quantifying to what degree and in which way multipartite states are entangled [4]–[7]. Recently, experimentalists are beginning to achieve the level of control over quantum systems required to generate and study multipartite entanglement [8]–[11].

[3] Author to whom any correspondence should be addressed.

In this paper, we explore robust entanglement between three qubits; the simplest system in which the phenomenon can be observed. This feature is best exemplified by the well-known GHZ and W states:

$$|\mathrm{GHZ}\rangle = (|000\rangle + |111\rangle)/\sqrt{(2)}, \tag{1}$$

$$|\mathrm{W}\rangle = (|001\rangle + |010\rangle + |100\rangle)/\sqrt{(3)}. \tag{2}$$

These states are the canonical examples of the two inequivalent classes of three-qubit entanglement. Specifically, any state possessing genuinely tripartite entanglement can be converted into one, and only one of these states using stochastic local operations and classical communication (SLOCC) [4]. Entanglement in a GHZ state is maximally fragile; loss of information about any single qubit leaves the remaining two in a separable state. Conversely, entanglement in a three-qubit W state is maximally robust [4]; loss of the information in any single qubit leaves the remaining two in an entangled state. The question of entanglement robustness arises naturally in experimental situations from decoherence mechanisms involving loss of qubits or qubit information. This is an important consideration in the many applications where entanglement is a vital resource.

We generate and study the entanglement properties of novel states composed of three polarization-encoded photonic qubits, introducing and experimentally demonstrating a simple scheme for the preparation of pure states with an arbitrary amount of W-class robust entanglement. Furthermore, we show that over the entire range the entanglement remains in a configuration that is optimally robust against qubit loss. We achieve high fidelities with the expected states in all cases.

We generate photons using spontaneous parametric down conversion (SPDC), figure 1. Measurement of a four-fold coincidence between detectors D1–D4 selects, with high probability, the cases where the source emitted two pairs of photons into optical modes 1 and 2. The polarization of two photons in the same spatio-temporal mode represents a three-level quantum system, a biphotonic qutrit [12], with logical basis states: $|\mathbf{0}_3\rangle \equiv |2_\mathrm{H}, 0_\mathrm{V}\rangle$, $|\mathbf{1}_3\rangle \equiv |1_\mathrm{H}, 1_\mathrm{V}\rangle$ and $|\mathbf{2}_3\rangle \equiv |0_\mathrm{H}, 2_\mathrm{V}\rangle$. Passing the two-photon state of mode 1 through a horizontal polarizer prepares the state $|\mathbf{0}_3\rangle$, and we then create a superposition in mode a, using a half-wave plate set at an angle θ, of the form:

$$\cos^2 2\theta |\mathbf{0}_3\rangle + \sqrt{2}\cos 2\theta \sin 2\theta |\mathbf{1}_3\rangle + \sin^2 2\theta |\mathbf{2}_3\rangle. \tag{3}$$

Mode 2 is passed to a 50% beam splitter; detection of a single photon at D1 heralds the presence of a single photon in mode b; which is passed through a polarizing beam splitter to prepare a polarization qubit ($|\mathbf{0}_2\rangle \equiv |1_\mathrm{H}, 0_\mathrm{V}\rangle$, $|\mathbf{1}_2\rangle \equiv |0_\mathrm{H}, 1_\mathrm{V}\rangle$) in the logical state $|\mathbf{0}_2\rangle$. Thus a qubit and qutrit arrive simultaneously at the first 50% beam splitter in our optical circuit.

A successful coincidence measurement heralds the cases where a biphotonic qutrit exits the central splitter in mode d and splits into single photon states in modes e and f after the final 50% beam splitter. At the output of the circuit we find the following three-qubit joint state across modes c, e and f:

$$\frac{\cos^2 2\theta}{4} |\mathbf{0}_2, \mathbf{0}_2, \mathbf{0}_2\rangle + \frac{\cos 2\theta \sin 2\theta}{2} |\mathbf{1}_2, \mathbf{0}_2, \mathbf{0}_2\rangle + \frac{\sin^2 2\theta}{4} (|\mathbf{1}_2, \mathbf{1}_2, \mathbf{0}_2\rangle + |\mathbf{1}_2, \mathbf{0}_2, \mathbf{1}_2\rangle - |\mathbf{0}_2, \mathbf{1}_2, \mathbf{1}_2\rangle). \tag{4}$$

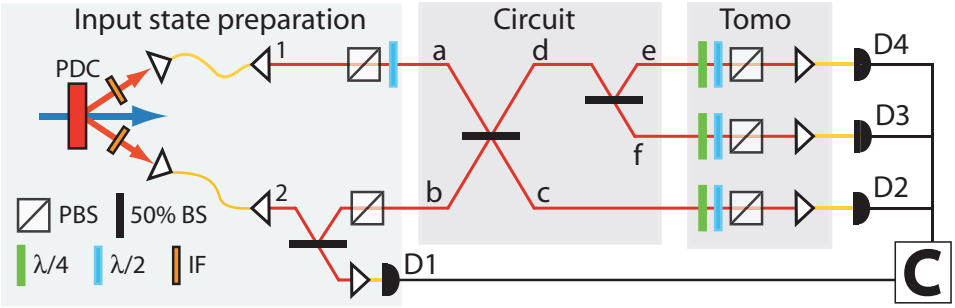


Figure 1. Conceptual experimental layout. Photons are generated via SPDC of a frequency-doubled mode-locked Ti:sapphire laser (820 nm → 410 nm, $\Delta\tau = 80$ fs at 82 MHz) through a type-I 2 mm BiB_3O_6 crystal. Photons are filtered by blocked interference filters (IF) at 820 ± 1.5 nm; collected into two single-mode optical fibres; injected into free-space modes 1 and 2; detected using fibre-coupled single photon counting modules (D1–D4). With 300 mW at 410 nm, we observe a fourfold coincidence rate of 0.1 Hz.

This is a superposition of a separable state (first two terms) and an entangled W state (last three terms). Choosing $\theta = \pi/4$ injects a biphoton in the state $|\mathbf{2}_3\rangle$ into mode a (equation (1)) and results in a three-qubit W state with probability 1/16 (equation (2)). Choosing $\theta = 0$ injects a biphoton in the state $|\mathbf{0}_3\rangle$ and produces a separable state of the form $|\mathbf{0}_2, \mathbf{0}_2, \mathbf{0}_2\rangle$.

Quantifying the amount of genuine tripartite entanglement in a three-qubit pure state is nontrivial. The three-tangle, defined as $\tau_3(\rho_{ABC}) = 4\det\rho_A - C_{AB} - C_{BC}$, where C_{ij} is the concurrence of the reduced state ρ_{ij} [13], quantifies GHZ-class entanglement and, since it is always zero for the W class [4], can be used to distinguish the W and GHZ classes. Following the technique of [4], it is straightforward to show that our ideal output state (equation (2)) belongs to the W class for all θ[4]. An entanglement monotone useful for quantifying W-class entanglement is the tripartite negativity (N_3) [14, 15], defined as $N_3 = (N_{a(bc)}N_{b(ac)}N_{c(ab)})^{1/3}$, where the bipartite negativities are calculated using the standard definition [16]. Using this definition, the three-qubit W state has a near maximal value of $N_3 = 0.94$. Quantifying how robust the entanglement in our three-qubit system is to loss requires a measure of the residual bipartite entanglement left in the two-qubit subsystem after loss of the information contained in qubit k ($\rho_{ij} = \mathrm{Tr}_k(\rho_{ijk})$). We choose to use the tangle (τ_2) [13].

By varying θ between 0 and $\pi/4$ we are able to prepare pure states with any desired amount of W-class entanglement, thereby giving us full control over this class of entanglement in our system. This scheme can be generalized straightforwardly to generate tunable W-class entanglement for any number of qubits. Besides the fundamental interest of how to prepare multiqubit non-maximally entangled states in a given class, we note that, in the case of two qubits, such states have already found important application in fundamental tests of quantum mechanics [17]–[19]. Previous techniques for producing W states [8]–[10] do not enable this control and could not be easily modified to achieve it. Our states also possess another useful and intriguing property. It is straightforward to show that, for all θ, the residual bipartite entanglement remains symmetrically distributed between each pair of qubits,

[4] For all θ, $\tau_3 = 0$ and the state possesses nonzero bipartite entanglement in each bipartite groupings of the three-qubit subsystems.

i.e. $\tau_2(\rho_{ce})=\tau_2(\rho_{cf})=\tau_2(\rho_{fe})=4\sin^4\theta/(\cos 2\theta-2)^2$. As a result, the amount of entanglement left in a two-qubit subsystem is always independent of which qubit is lost. Later, we will show that the entanglement in these states is in fact optimally robust against qubit loss.

We measure three-qubit output states using polarization tomography [20] of modes c, e and f, performing an over-complete set of 216 separate measurements [21] in four-fold coincidence between non-photon-number-resolving detectors D1–D4. With rates of approximately $0.1\,\mathrm{s}^{-1}$, we measure for several days to acquire sufficient counts for an accurate reconstruction. Instead of performing a single measurement set over this time we take many shorter 80 min sets. This *iterative* tomography technique provides many advantages. Most importantly, a complete reconstruction of the density matrix is possible after each iteration, allowing analysis of how our estimates of state properties are developing throughout the measurement process. This allows diagnosis of serious practical problems, such as time-dependant optical misalignment, far earlier than would otherwise be possible. Using many repeated shorter measurement sets also makes the state estimation less prone to errors introduced by certain fluctuations in the optical source brightness, without significantly reducing the total available integration time. After completion we use the data accumulated across all short measurement sets to reconstruct the final state. Our experiment is neither actively stabilized nor realigned between iterative measurement sets. Our beamsplitters impart systematic unitary operations on the optical modes. While the entanglement properties of our ideal or measured states are not affected by these local operations, state fidelities are. For simplicity, we corrected for these effects numerically, but alternatively such unitaries could be corrected using standard waveplates.

Figure 2(a) shows results for $\theta=\pi/4$ (equation (2)). We find a high fidelity with the ideal W state of 0.90 ± 0.03, which violates the entanglement witness for a W state [22] by 7 standard deviations, and a high tripartite negativity of $N_3=0.80\pm0.03$. Note that we use the following standard definition for the fidelity between two mixed states: $F(\rho,\sigma)\equiv\mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]^2$.

Figure 2(b) shows the reduced state of qubits e and f, calculated by numerical application of a partial trace to the state in figure 2(a). We find a high fidelity of $F=0.94\pm0.02$ with the ideal maximally entangled mixed state (MEMS) [16], [23]–[25]. The tangle is $\tau_2=0.27\pm0.03$ (ideal: 4/9), demonstrating the robustness of the entanglement in the three-qubit state to loss. Figure 2(c) shows how our estimates of key properties of the generated states (Figures 2(a) and (b) developed over the iterative measurement process. The asymptotic trends show that we measured for a sufficient period of time such that our reconstructed states are a fair representation of the generated states.

Figure 3(a) shows experimental results for three-qubit states measured over a range of θ (equation (2)). We find high fidelities with the ideal symmetric robust three-qubit states (see caption). The discrepancies in the bipartite tangle seem larger than in the tripartite negativity because tangle is a harsher measure of entanglement [16]. We also measure the reduced two-qubit states *directly* by removing the polarization analysis optics from one qubit output mode at a time and only detecting its presence as a trigger—physically realizing the loss of qubit information. This was repeated for each qubit to test the symmetry of our measured states. Besides offering an unambiguous demonstration of robust entanglement, this approach offers an increased count-rate over that observed when measuring three-qubit states, allowing shorter measurement times that are less prone to experimental drift. We perform over-complete polarization tomography of the remaining two qubits using 36 measurements [29]. Figure 3(b) presents the results plotted on the tangle versus linear entropy plane [23], where the linear entropy [20] is $S_\mathrm{L}\equiv d(1-\mathrm{Tr}[\rho^2])/(d-1)$, and d is the state dimension.

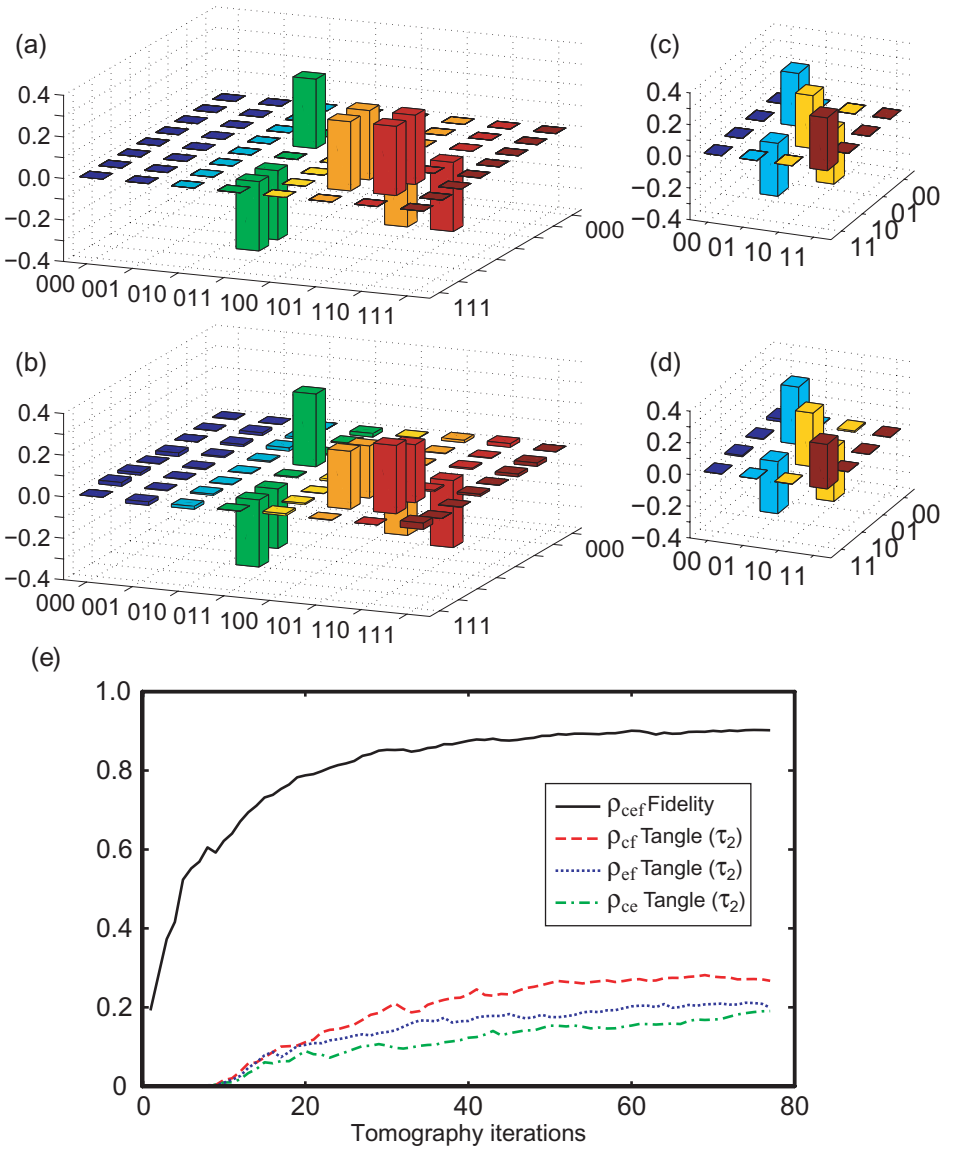


Figure 2. Results for $\theta = \pi/4$ (equation (2)). (a) Ideal and (b) measured three-qubit density matrices. Fidelity $F = 0.90 \pm 0.03$ (with the W state), linear entropy $S_{\mathrm{L}} = 0.20 \pm 0.03$, tripartite negativity $N_3 = 0.80 \pm 0.03$. (c) Ideal and (d) measured reduced state of qubits c and f reconstructed via $\rho_{cf} = \mathrm{Tr}_{\mathrm{e}}(\rho_{cef})$. Fidelity $F = 0.94 \pm 0.02$ (with the MEMS [23, 24]), linear entropy $S_{\mathrm{L}} = 0.61 \pm 0.02$ (ideal 5/9), tangle $\tau_2 = 0.27 \pm 0.03$ (ideal 4/9). (e) Iterative tomography results: we use convex optimization and fixed weight estimation to reconstruct physical density matrices and Monte–Carlo simulations of Poissonian photon-counting fluctuations for error analysis [26]–[28] (see EPAPS material). We use the following standard definitions: the fidelity between two mixed states is $F(\rho, \sigma) \equiv \mathrm{Tr}[\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}]^2$; and the linear entropy [20] is $S_{\mathrm{L}}(\rho) \equiv d(1 - \mathrm{Tr}[\rho^2])/(d-1)$, where d is the system dimension.

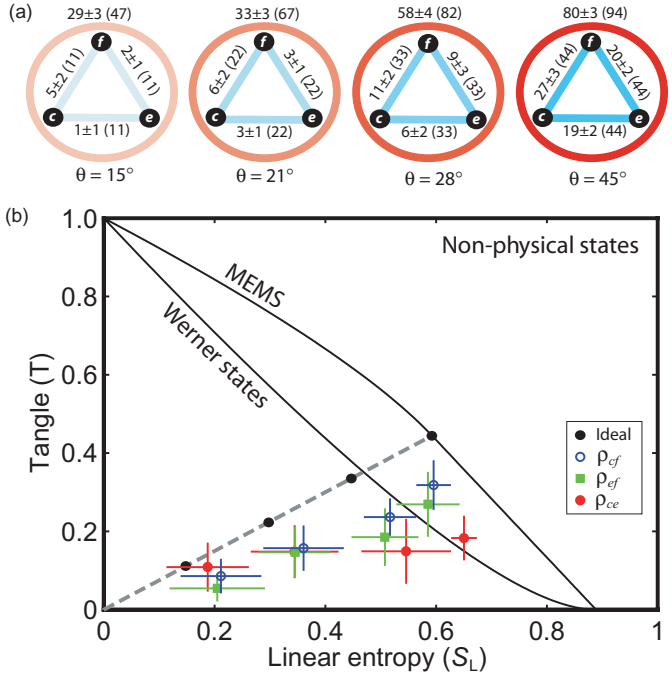


Figure 3. Results for $\theta = \{15^\circ, 21^\circ, 28^\circ, 45^\circ\}$, equation (2). (a) Measured (ideal) entanglement (in %) in three-qubit output states (ρ_{cef}). Black dots are qubits, red circles represent tripartite entanglement (N_3), blue lines represent bipartite (robust) entanglement (τ_2) in reduced states (e.g. line c—e for $\rho_{ce} = \mathrm{Tr}_f\{\rho_{cef}\}$) [14]: high fidelities with ideal configurations, $\{0.90 \pm 0.02,\ 0.84 \pm 0.03,\ 0.84 \pm 0.05,\ 0.90 \pm 0.03\}$, and low linear entropies, $\{0.20 \pm 0.03,\ 0.22 \pm 0.03,\ 0.25 \pm 0.03,\ 0.20 \pm 0.03\}$, respectively. (b) Tangle versus linear entropy plane [23] shows results for reduced two-qubit states measured *directly* by removing the polarization analysis optics of other qubit, and performing two-qubit tomography. The ideal trend (equation (2), dashed), Werner states [30] and MEMS [23, 24] are also shown. The average fidelity with the ideal is 0.97 ± 0.02.

The dashed line shows the path of the ideal reduced states for varying θ (equation (2)); the residual tangle increases linearly with the entropy, with the pure separable state for $\theta = 0$ at the origin, and an MEMS for $\theta = \pi/4$. Due to the symmetry properties of the ideal three-qubit states, this trend does not depend on which qubit is lost. The results show a good correlation with the ideal trend and high fidelities with the expected states (see caption); we can tune the level of robust entanglement in our system.

The reduced entanglement in our results is largely due to optical mode distinguishability caused by alignment drift during the long data runs. The improved bipartite entanglement of figure 3(b) over figure 3(a) reflects a shorter run duration. Another source of error is the higher order emission from SPDC [31]. Both processes introduce extra mixture into the results (there is already mixture in the ideal two-qubit subspaces) and thereby lower the entanglement. The bipartite entanglement is more sensitive to these effects at low θ, because weaker entanglement can be almost completely washed out by extra mixture which would only reduce entanglement

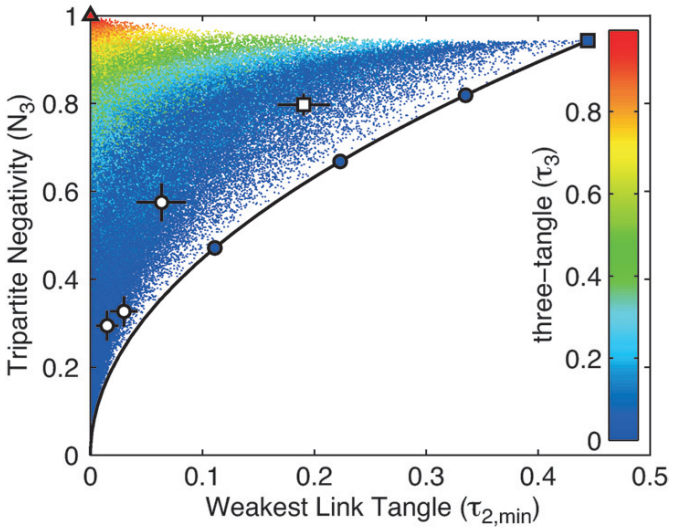


Figure 4. Plot of N_3 versus $\tau_{2,\min}$ (equation (3)) with 300 000 randomly selected pure three-qubit states [34]. Black curve: ideal positions of our states (equation (2)) with $\theta = 0$ (at the origin) to $\pi/4$. The four experimentally measured three-qubit states (white, figure 3(a)) and three-qubit GHZ (red triangle) and W states (blue square) are also shown. The density of states near the boundary (our ideal states) is lower because the set of three-qubit W-class states is of measure zero compared with the set of three-qubit GHZ-class states [4].

in a more strongly entangled state. Important ways to improve entanglement are to increase stability (e.g. by moving to fibre- or micro-optics-based systems [32, 33]) and develop better single photon sources. Beam-splitter reflectivity errors can affect the symmetry of bipartite entanglement. Indeed using our measured values (with deviations $\sim 1\%$) with a simple model predicts that the tangle between qubits c and f will be higher, as observed in our results.

Dür *et al* [4] showed that entanglement in a three-qubit W state is maximally robust in two respects . Firstly, it maximizes the 'weakest link' residual tangle between two-qubit subsystems, namely:

$$\tau_{2,\min}(\Psi_{abc}) = \min\{\tau_2(\rho_{ab}), \tau_2(\rho_{ac}), \tau_2(\rho_{bc})\}, \tag{5}$$

where Ψ_{abc} is any pure three-qubit state and, e.g. $\rho_{ab} = \mathrm{Tr}_c\{\Psi_{abc}\}$. Secondly, it has the highest average residual tangle over the two-qubit subspaces. Figure 4 shows N_3 versus $\tau_{2,\min}$ (equation (3)) for 300 000 pure three-qubit states randomly selected using the Haar measure [34, 35], with the greyscale (colourmap online) representing the three-tangle (τ_3). The black line shows the curve for our ideal states (equation (2)), from the separable state at the origin ($\theta = 0$) to the W state ($\theta = \pi/4$), which reaches the maximum possible $\tau_{2,\min}$ value of 4/9. This line clearly represents a boundary in robust configurations of entanglement: for a given level of genuine pure-state three-qubit entanglement (N_3) the weakest bipartite link between any pair of qubits in our ideal states is of optimal strength. States that are not optimal in this sense have at least one weaker bipartite link: there is a 'linchpin' qubit which, if lost, will leave less bipartite entanglement between the remaining qubits. Figure 4 includes the positions of the four measured states shown in figure 3(a). Note that, even though our measured W state has a fidelity

of over 90% with the ideal, the value of $\tau_{2,\min}$ is less than half of the expected value. Clearly maximizing this property is far more experimentally challenging than achieving a high state fidelity. Similar numerical simulations show that our ideal states are not optimal with respect to the average residual entanglement. However, states that improve on ours in this respect do so at the expense of losing a symmetric distribution of entanglement; they always have at least one weaker bipartite link which is less than (or equal to) the weakest link entanglement in our states.

In conclusion, we have demonstrated and fully characterized a new level of control over multipartite entanglement in the laboratory. Our scheme provides tunable control over the level of W-class entanglement between three or more photonic qubits. Furthermore, as we tune the entanglement, it always remains in a highly symmetric configuration that is optimally robust against information loss—a desirable feature in many experimental situations where entanglement is a valuable resource. We predict that the ability to store, generate or transmit entanglement in such low loss configurations will be important in the emerging field of quantum technology.

Acknowledgments

We are thankful to Guifre Vidal and Andrew White for valuable discussions. This work was supported by the Australian Research Council and DEST Endeavor programs.

References

[1] Nielsen M A and Chuang I L 2000 *Quantum Computation and Quantum Information* (Cambridge: Cambridge University Press)
[2] Giovannetti V, Lloyd S and Maccone L 2004 *Science* **306** 1330
[3] Raussendorf R and Briegel H J 2001 A one-way quantum computer *Phys. Rev. Lett.* **86** 5188–91
[4] Dür W, Vidal G and Cirac J I 2000 *Phys. Rev.* A **62** 062314
[5] Verstraete F *et al* 2002 *Phys. Rev.* A **65** 052112
[6] Bastin T *et al* 2007 arXiv:0710.3720
[7] Kendon V M, Nemoto K and Munro W J 2002 *J. Mod. Opt.* **49** 1709
[8] Eibl M *et al* 2004 *Phys. Rev. Lett.* **92** 077901
[9] Kiesel N *et al* 2007 *Phys. Rev. Lett.* **98** 063604
[10] Walther P, Resch K J and Zeilinger A 2005 *Phys. Rev. Lett.* **94** 240501
[11] Lu C-Y *et al* 2007 *Nat. Phys.* **3** 91
[12] Bogdanov Y I, Krivitsky L A and Kulik S P 2003 *J. Exp. Theor. Phys. Lett.* **78** 352
[13] Coffman V, Kundu J and Wootters W K 2000 *Phys. Rev.* A **61** 052306
[14] Sabin C and Garcia-Alcaine G 2007 arXiv:0707.1780
[15] Love P J e 2007 *Quantum Inform. Process.* **6**
[16] Wei T-C *et al* 2003 *Phys. Rev.* A **67** 022110
[17] Hardy L 1993 *Phys. Rev. Lett.* **71** 1665–8
[18] White A G, James D V, Eberhard P H and Kwiat P G 1993 *Phys. Rev. Lett.* **71** 1665–8
[19] Acén A, Richard G and Gisin N 2005 *Phys. Rev. Lett.* **95** 210402
[20] James D F V *et al* 2001 *Phys. Rev.* A **64** 052312
[21] Lanyon B P *et al* 2007 *Phys. Rev. Lett.* **99** 250505
[22] Bourennane M *et al* 2004 *Phys. Rev. Lett.* **92** 087902
[23] Munro W J *et al* 2001 *Phys. Rev.* A **64** 030302
[24] Peters N A *et al* 2004 *Phys. Rev. Lett.* **92** 133601

[25] Ishizaka S and Hiroshima T 2000 *Phys. Rev.* A **62** 022310
[26] O'Brien J L *et al* 2004 *Phys. Rev. Lett.* **93** 080502
[27] de Burgh M, Doherty A and Gilchrist A 2007 in preparation
[28] Langford N K 2007 PhD Thesis The University of Queensland, Brisbane, QLD, Australia
[29] Langford N K *et al Phys. Rev. Lett.* **95** 210504
[30] Werner R F 1989 *Phys. Rev.* A **40** 4277
[31] Weinhold T J *et al* 2007 in preparation
[32] Politi A *et al* 2008 *Science* **320** 646
[33] Clark A S *et al* 2008 arXiv:0802.1676
[34] Haar A 1993 *Ann. Math.* **34** 147–69
[35] Nemoto K 2000 *J. Phys. A: Math. Gen.* **33** 3493–506

6.1 Contribution statement

The author made the following contributions to this work:

- Project initialisation, conceptualisation and development (in collaboration with NKL)
- Reconstruction of the optical circuit (it was used previously for the work presented in chapter 5)
- Preliminary and final data acquisition
- Data interpretation and analysis (in collaboration with NKL)
- Conceptual, theoretical and coding work behind Fig. 4 in the paper.
- Paper writing (in collaboration with NKL)

6.2 Appendix: Poissonian statistics in photon counting experiments

The following paragraph is a reply to a referee's request for clarification about our use of the Poissonian distribution to describe our photon counting statistics.

The output from a spontaneous parametric down conversion source is a photon number entangled state given by:

$$|\Psi_{dc}\rangle \sim |\mathbf{0},\mathbf{0}\rangle + \alpha|\mathbf{1},\mathbf{1}\rangle + \alpha^2|\mathbf{2},\mathbf{2}\rangle + \alpha^3|\mathbf{3},\mathbf{3}\rangle + ... \tag{6.1}$$

where $|n_1, n_2\rangle$ describes the number of photons in each of the output modes and α is an overall efficiency parameter related to the pump power, the nonlinear coupling constant, and the thickness of the crystal (i.e., the interaction length). In our experiments, we use 4-fold coincidence counts to select only terms which involve two, or more, photon pairs being emitted from the nonlinear crystal (ruling out the $|0,0\rangle$ and $|1,1\rangle$ terms). Because the down-conversion process is relatively weak, the dominant contribution to these counts are made by the $|2,2\rangle$ term. Since we use a pulsed pump laser ($\Delta\tau = 80$fs at 82MHz), this entire process is then repeated many times (once per pulse), and for each pulse we either measure a four-fold coincidence event or not. Therefore, for a given integration time, the count distribution for coincidences is described by a binomial distribution. However,

because the probability per pulse of observing a coincidence is extremely low (low count rates) and the number of repetitions is very large (long integration times and high repetition rate), this binomial distribution reduces to a Poissonian distribution [poi09] (which for practical reasons is much easier to work with in the analysis). Note that the other higher-order terms (e.g., $|3,3\rangle$) also make a contribution to the measured counts, but with a much lower probability determined by the photon number statistics of the two mode squeezed vacuum. However, because their contribution to the count statistics is also Poissonian, they contribute as an error to the measured circuit operation (as discussed in the paper), but they do not change the counting statistics. Therefore we can use a Poissonian distribution to describe the statistics of our coincidence measurements.

6.3 Additional experimental details

Note that the optical circuit constructed for this experiment is the same as that used for the paper 'Manipulating biphotonic qutrits' presented in Chapter 5. A schematic is shown in Fig. 5.1 of that Chapter.

Chapter 7

Discussion and outlook

In this thesis we have presented a range of works that are all linked by the desire to explore, and extend control over, information encoded into quantum mechanical systems. In particular we have developed new tools for the manipulation of optical quantum information, generated new quantum states of light and explored some powerful applications in the form of quantum computer algorithms. In this section we summarise the main results and discuss possible directions for future research.

Important results from Part I, and Chapter 2 of Part II, were the realisation of the three linear optic quantum logic circuits shown symbolically in Fig. 7.1. Notwithstanding previous statements about joint publications, these are the first legitimate demonstrations of these gates in any physical system, and are of particular importance to quantum computation. As we have seen, controlled-unitary gates play a central role in the quantum phase estimation algorithm, which underpins an entire class of quantum algorithms. The Toffoli enables universal reversible classical logic on a quantum computer, and also plays an important role in quantum error correction schemes. The concatenated CNOT gates can be used to create cluster-states—the universal resource for the one-way model of quantum computation. These gates offer a new level of control over photonic qubits in the laboratory that should enable new quantum information experiments.

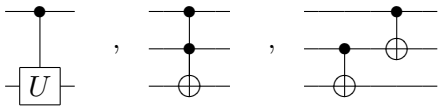


Figure 7.1: New logic circuits implemented in this thesis: controlled-unitary gate, Toffoli gate, two concatenated-CNOT gates, respectively.

We were able to perform a full characterisation of our controlled-unitary gate via a quantum process tomography [OPG+04]. This was not possible for our Toffoli and concatenated-CNOT gates due to a combination of the large number of measurements required and the low brightness of our optical (four-photon) source. Completing the measurement set with enough photon counts to afford a meaningful conclusion would

take an impractical amount of time. A recent discussion with Holger Hoffman, currently of Hiroshima university in Japan, suggested that it should be possible to put a bound on the process fidelity of our Toffoli gate, with the addition of only two more complete truth-tables in a different basis (i.e. the current one is in the logical basis, but another could be repeated in the diagonal/anti-diagonal basis for example). These ideas are presented in several of his recent papers [HOT06b, HOT06a, Hof04], but most concisely in his 2005 PRL [Hof05].

When considering future research paths it is hard to see how these optical circuits can be made any larger with current optical source and detector technology. The requirements of post-selection severely limit the possible elemental gate configurations. Furthermore, the combination of an exponentially decreasing photon generation rate with desired total photon number (when using SPDC), and the exponentially decreasing success probability with every additional multi-qubit gate, is very restrictive. The new gates presented in this thesis have stretched our optical source technology to the limit of its operation, as can be seen by the very low count rate at the output of our Toffoli and concatenated-CNOT gates, and subsequently hampered characterisation process. It is quite surprising that we have managed to get this far, and for that we have the logic-circuit simplification technique presented in Chapter 1 to thank. However, as it stands that technique does not provide a solution to these problems.

Consequently, one of the most important paths for further research is to improve our optical sources, or most likely develop entirely new ones altogether [VBR08, LR08]. The development of the second generation of photonic sources based on periodically poling [HT95, TRT$^+$01] and spontaneous four-wave mixing [LVSK05, FMW05, FAWR07, CLS$^+$09] (SFWM) have advantages for photonic quantum computing. Periodical poling offers a dramatically increased two photon generation rate per unit power and, perhaps most importantly enables high quality experiments to be performed without the need for hugely expensive high powered lasers. SFWM offers in-fiber photon sources which essentially solve the mode-matching problem between sources and circuits. Furthermore, these sources offer greater control over the spectral structure of the generated photon pairs, particularly given the ability to incorporate photonic crystal structures within the fibers to control mode dispersion. Specifically they have proven to offer a dramatic reduction in energy-momentum correlations that are prevalent in the sources used in this thesis, for example. This removes the need for strong, and therefore lossy, spectral filtering. Note that this is also possible with SPDC processes, see [TMCT05] for example. While these developments are undoubtably of great importance, the sources are still highly non-

deterministic and must therefore be supplemented with a scheme for effectively amplifying the success probability.

A important source issue, that has become apparent through this thesis and even more so through that of my colleague Till Weinhold [Wei08], is that of the hugely detrimental affect of higher-order emissions (more than one pair of photons) from spontaneous photon sources on gate performance [BWL$^+$09]. While it has always been known that multiple emissions from these sources exist, it was not known how significant a problem they are. Currently, the only way to generate more than two photons from these sources is to increase the pump laser power—however, this will subsequently increase the rate of unwanted high-emissions. This means that the current approach for increasing the number of photons is fundamentally floored.

I believe that to take experimental photonic quantum computing to the next level the field must aim for a near deterministic source of a least 10 or 12 single photons. I choose these numbers because they are fundamentally well beyond what is possible with existing, non-scalable photon sources, and would therefore represent a significant step forwards. A promising scheme [CDWM03] is to construct large (or smaller more efficient) arrays of non-deterministic sources—so that the probability of at least one source generating a pair is very high. The trick is to then switch one of these photons into a common target mode, conditional on a detection of the other photon from the pair. While the probability of any particular source generating a photon pair can be small, the probability of at least one firing per unit time can be made arbitrarily high by adding a more sources. An obvious challenge is to achieve a high efficiency fast single photon switch. Clearly all this is a substantial wish-list, however I believe that its pursuit is merited given the wide range of potential applications for deterministic photon number sources.

An important next step in gate development, that would become more feasible with the aforementioned source development, is to make their successful operation heralded, without destroying the information-carrying photons. Besides improved source technology, this would also require the introduction and optimisation of newly available photon number resolving detectors [RLMN05, VBR08]. Note that primitive versions of heralded linear optic 2-qubit gates have been demonstrated [GPW$^+$04, BCZ$^+$07, ZZC$^+$05]. From the large and cumbersome circuits constructed in this thesis, it is also clear that circuit miniaturization is an important path to follow in parallel, as pioneered by A. Politi and colleagues [PCR$^+$08]. Of course, this by itself does not overcome the major limitations to scalability imposed by current optical source technology.

In Part I we also presented a technique for simplifying the construction of certain

quantum logic circuits by exploiting multi-level information carriers. This technique has allowed us to greatly simplify complex circuits in the laboratory, thereby enabling the implementation of otherwise infeasible operations. There is also the potential for practical enhancement of circuits in many other architectures, since the technique is independent of the physical encoding of quantum information. More generally, this work has highlighted that there are advantages to exploiting the full physicality of quantum information carriers, rather than imposing an artificial two state structure. And perhaps there may be more significant breakthroughs along these lines of thought in the future. Indeed, at time of writing, our archive publication [LBA+09] has received a number of citations in its first few months. These includes works in the areas of: linear optic quantum logic gates [GGR08, Fiu08]; simplifying quantum logic using graph states [TOK+08]; probabilistic quantum computer simulations [Hof08]; photon source development [CLS+08]; photonic qubit control [TDY+08]; and hyper-entangled photonic state generation [bGLY+08].

The key result of Part II was the implementation of several quantum algorithms. Besides establishing linear optics as a 'mature' quantum computation architecture, the hope is that these proof-of-principle demonstrations will provide essential motivation and inspiration for the further pursuit of quantum computing. A full-scale device will certainly not be built without a significant amount of support from industry, engineers and researchers from other fields, and what better way to encourage this than by providing tangible demonstrations of the potential power, and widespread application, of these devices. We now discuss each implementation separately.

In Chapter 3 we performed a simplified version of Shor's factoring algorithm. For the first time, we demonstrated the basic principles that underly this powerful algorithm, namely the use of quantum superposition and entanglement to perform arithmetic calculations. Furthermore, we demonstrated the feasibility of executing complex, multiple-gate quantum circuits in a linear optic architecture. This is a step towards achieving the level of control over photonic quantum information necessary for large-scale optical quantum computing. It is important to be aware that implementing a full-scale version of this algorithm, even if only to factor 15, would require thousands of gates operating on tens of qubits [BCDP96]. This huge 'buy-in' figure, combined with our state-of-the-art implementation involving only 3 qubits and a handful of gates, shows how very far away we are from practical implementations of this algorithm with current technology.

Chapter 4 presented our demonstration of a molecular energy calculation using a recently proposed quantum algorithm [AGDLHG05]. This involved encoding molecular

eigenstates into photonic qubits, simulating the hamiltonian evolution of the system using logic gates, and reading out the energy using the quantum phase estimation algorithm. This is the first time that an energy calculation, and molecular simulation, have been performed using quantum computational resources. Besides providing the first experimental step, our work also shows a path for future work.

Due to the small size and high symmetry of the molecular system that we solved, we were able to simulate the hamiltonian evolution directly, with only a few of logic gates. This will not be possible for large-scale systems and a resource intensive approximation technique, known as a Trotter decomposition [Llo96], is the proposed solution. An important next step would be to begin exploring this technique experimentally. While it is unlikely that such an exploration is close in a linear optic architecture, an ion-trap scheme is probably capable of performing a sufficient number of operations with available technology [HRB08]. For example, in our paper we show that a 13-bit energy precision can be achieved by simulating the hydrogen molecule using five qubits and 522 logic gates. This number of gates could be significantly reduced by allowing for a lower precision, suggesting that a demonstration with an ion-trap system is within the realms of possibility [HRB08].

In Chapter 5 we demonstrated the normalised-trace estimation algorithm, which is representative of a little-known model of quantum computation entitled DQC1. The are several take-home messages from our results. Firstly, there are correlations that exist between completely separable mixed states that are intrinsically quantum mechanical. Secondly, these correlations are potentially useful for quantum computation and quantum information technology. These results suggest that there is still much to learn even about very simple quantum systems. It is also of interest that it may still be possible to build a powerful computational device, even without fulfilling all the standard criteria for quantum computing [DiV00].

The central results of Part III were the development of two new tools for the manipulation of photonic quantum information, with a specific emphasis on the control and generation of entanglement. In Chapter 6 we developed a technique for extending experimental control over biphotonic qutrits, the three level quantum information carriers formed by the polarisation of two photons in the same spatial and temporal mode. We also generated and characterised a new form of entanglement, specifically that between a qubit and a qutrit. We propose that this provides another way to wrestle control over biphotonic qutrits, given our extensive knowledge of how to manipulate photonic qubits. For example, two of these qubit-qutrit states would enable the creation of qutrit-qutrit entanglement, by projecting their associated qubits into an entangled state (using estab-

lished techniques involving post-selection and a beamsplitter, see Fig. 1.7 for example). Qutrit-qutrit entanglement finds applications in several quantum information protocols, see [GLZ08, FGM01] for example. Although still in its first year of publication, we are encouraged to find that our article has received several citations relating to these results, in the areas of: hidden variable tests in spin-1 systems [KCBS08]; qudit-qudit entanglement dynamics [DŁ08]; optimal qudit discrimination [HB08]; multi-photon entanglement generation [WSK$^+$08]; quantum key distribution with biphotons [BABOE08]; generating four-dimensional states using biphotons [BSS$^+$08]; manipulating photonic spatial qubits [TDY$^+$08]; and defining positivity conditions for qutrits [CW08a].

In Chapter 7 we developed a technique that allows continuous control over the level of W-class entanglement between three photonic polarisation qubits. Furthermore, this is possible by varying only a single experimental parameter. This represents a new level of experimental control over multi-partite entanglement in the laboratory. Using this tool we generated the highest fidelity W-state recorded, and explored a distinct physical property known as entanglement 'robustness'. This feature, specific to the W-class for 3-qubit states, is concerned with the retention of entanglement in the system after loss of some of its constituent parts. We provided evidence that, for any given level of W-class entanglement, our states saturated the bound for the maximal amount of entanglement robustness. It seems likely that the ability to store and transmit entanglement in these low loss configurations will be of use in the future, given entanglement's status as a valuable resource.

This work provided the chance to explore the rich and complex structure of multipartite entanglement. Whilst the recent repackaging of entanglement, as a resource from quantum information technology, represents an important paradigm shift, it is also in danger of oversimplifying things—entanglement is not a single quantifiable thing, like many other physical resources. Instead it comes in a vast variety of fundamentally inequivalent forms [DVC00, VDDV02] that each display distinct physical characteristics.

In terms of future work on multipartite generation, the obvious path is to entangle more photonic qubits. The main obstacles to this are, once again, problems with the standard optical source technology, namely the decreased generation rate with photon number. One way to overcome this is to develop brighter sources, however, as we show in a recent paper [BWL$^+$09], this increases sources of noise, which will subsequently reduce state quality. Consequently, more fundamental source development is required.

Overall, this thesis has developed a number of new tools for experimental quantum information with photons, and provided some of the first demonstrations of quantum

computing algorithms in any physical architecture. We hope that this provides motivation for the continuing pursuit of scalable quantum computation.

References

[AGDLHG05] A. Aspuru-Guzik, A. Dutoi, P. Love, and M. Head-Gordon. Simulated quantum computation of molecular energies. *Science*, 309:1704, 2005.

[AL97] Daniel Abrams and Seth Lloyd. Simulation of many-body fermi systems on a universal quantum computer. *Phys. Rev. Lett.*, 79:2586–2586, 1997.

[AvK+07] Dorit Aharonov, Wim van Dam, Julia Kempe, Zeph Landau, Seth Lloyd, and Oded Regev. Adiabatic quantum computation is equivalent to standard quantum computation. *Siam Journal of Computing*, 37:166, 2007.

[BABOE08] I. Bregman, D. Aharonov, M. Ben-Or, and H. S. Eisenberg. Simple and secure quantum key distribution with biphotons. *Phys. Rev. A.*, 77(5):050301, 2008.

[BCDP96] David Beckman, Amalavoyal N. Chari, Srikrishna Devabhaktuni, and John Preskill. Efficient networks for quantum factoring. *Phys. Rev. A*, 54(2):1034–1063, Aug 1996.

[BCJ+99] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for nmr quantum computing. *Phys. Rev. Lett.*, 83(5):1054–1057, Aug 1999.

[BCZ+07] Xiao-Hui Bao, Teng-Yun Chen, Qiang Zhang, Jian Yang, Han Zhang, Tao Yang, and Jian-Wei Pan. Optical nondestructive controlled-not gate without using entangled photons. *Phys. Rev. Lett.*, 98(17):170502, 2007.

[bGLY+08] Wei bo Gao, Chao-Yang Lu, Xing-Can Yao, Ping Xu, Otfried Guhne, Alexander Goebel, Yu-Ao Chen, Cheng-Zhi Peng, Zeng-Bing Chen, and Jian-Wei Pan. Experimental demonstration of a hyper-entangled ten-qubit schrödinger cat state. arXiv.org:0809.4277, 2008.

[BPM+97] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, and Anton Zeilinger. Experimental quantum teleportation. *Nature*, 390(6660):575–579, 1997.

[BSS+08] So-Young Baek, Stanislav S. Straupe, Alexander P. Shurupov, Sergei P. Kulik, and Yoon-Ho Kim. Preparation and characterization of arbitrary states of four-dimensional qudits based on biphotons. *Phys. Rev. A.*, 78(4):042321, 2008.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *Special issue on Quantum Computation of the Siam Journal of Computing*, Oct 1997.

[BWL+09] M. Barbieri, T. J. Weinhold, B. P. Lanyon, A. Gilchrist, K. J. Resch, M. P. Almeida, and A. G. White. Parametric downconversion and optical quantum gates: two's company, four's a crowd. *Journal of Modern Optics*, *to appear*, 2009.

[CDWM03] S Castelletto, I.P. Degiovanni, Michael Ware, and A. Migdale. Status of mulitplexed single photon on-demand source. In *SPIE Conf on Quantum Information and Computation*, volume 5105, pages 294–302, 2003.

[CLS+08] Offir Cohen, Jeff S. Lundeen, Brian J. Smith, Graciana Puentes, Peter J. Mosley, and Ian A. Walmsley. Tailored photon-pair generation in optical fibers. arXiv.org:0809.0071, 2008.

[CLS+09] Offir Cohen, Jeff S. Lundeen, Brian J. Smith, Graciana Puentes, Peter J. Mosley, and Ian A. Walmsley. Tailored photon-pair generation in optical fibers. *Physical Review Letters*, 102(12):123603, 2009.

[CVZ+98] Isaac L. Chuang, Lieven M. K. Vandersypen, Xinlan Zhou, Debbie W. Leung, and Seth Lloyd. Experimental realization of a quantum algorithm. *Nature*, 393(6681):143–146, 1998.

[CW08a] A. Checinska and K. Wodkiewicz. Analysis of complete positivity conditions for quantum qutrit channels. arXiv.org:0809.3882, 2008.

[CW08b] John Clarke and Frank K. Wilhelm. Superconducting quantum bits. *Nature*, 453(7198):1031–1042, 2008.

[DFC05] Animesh Datta, Steven T. Flammia, and Carlton M. Caves. Entanglement and the power of one qubit. *Phys. Rev. A*, 72(4):042316, 2005.

[DiV00] David P. DiVincenzo. The physical implementation of quantum computation. arXiv:quant-ph/0002077, 2000.

[DŁ08] Jerzy Dajka and Jerzy Łuczka. Origination and survival of qudit-qudit entanglement in open systems. *Phys. Rev. A.*, 77(6):062303, 2008.

[DSC08] Animesh Datta, Anil Shaji, and Carlton M. Caves. Quantum discord and the power of one qubit. *Phys. Rev. Lett.*, 100(5):050502, 2008.

[DVC00] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(6):062314, Nov 2000.

[FAWR07] J Fulconis, O Alibart, W J Wadsworth, and J G Rarity. Quantum interference with photon pairs using two micro-structured fibres. *New Journal of Physics*, 9(8):276, 2007.

[Fey82] R. P. Feynman. Simulating physics with computers. *Int. J. Theor. Phys.*, 21:467, 1982.

[FGGS00] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser. Quantum computation by adiabatic evolution. arXiv.org:quant-ph/0001106, 2000.

[FGM01] Matthias Fitzi, Nicolas Gisin, and Ueli Maurer. Quantum solution to the byzantine agreement problem. *Phys. Rev. Lett.*, 87(21):217901, Nov 2001.

[Fiu08] Jaromir Fiurasek. Linear optical fredkin gate based on partial-swap gate. arXiv.org:0809.3228, 2008.

[FMW05] J. Fan, A. Migdall, and L. J. Wang. Efficient generation of correlated photon pairs in a microstructure fiber. *Opt. Lett.*, 30(24):3368–3370, 2005.

[GGR08] Yan-Xiao Gong, Guang-Can Guo, and Timothy C. Ralph. Methods for a linear optical quantum fredkin gate. *Phys. Rev. A.*, 78(1):012305, 2008.

[GLZ08] Ying Guo, Moonho Lee, and Guihua Zeng. Large-capability quantum key distribution with entangled qutrits. *Optics Communications*, 281(14):3938 – 3942, 2008.

[GN96] Robert B. Griffiths and Chi-Sheng Niu. Semiclassical fourier transform for quantum computation. *Phys. Rev. Lett.*, 76(17):3228–3231, Apr 1996.

[GPW+04] S. Gasparoni, J.-W. Pan, P. Walther, T. Rudolph, and A. Zeilinger. Realization of a photonic controlled-not gate sufficient for quantum computation. *Phys. Rev. Lett.*, 93:020504, 2004.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *STOC '96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, New York, NY, USA, 1996. ACM.

[GSV04] P. Grangier, B. Sanders, and J. Vuckovic. See special issue: Focus on single photons on demand. *New J. Phys.*, 6, 2004.

[HB08] Ulrike Herzog and János A. Bergou. Optimum unambiguous identification of [bold d] unknown pure qudit states. *Phys. Rev. A.*, 78(3):032320, 2008.

[Hof04] Holger F. Hofmann. Efficient tests for experimental quantum gates. arXiv.org:quant-ph/0411011, 2004.

[Hof05] Holger F. Hofmann. Complementary classical fidelities as an efficient criterion for the evaluation of experimentally realized quantum operations. *Phys. Rev. Lett.*, 94(16):160504, 2005.

[Hof08] Holger F. Hofmann. How to simulate a quantum computer using negative probabilities. arXiv.org:0805.0029, 2008.

[HOT06a] Holger F. Hofmann, Ryo Okamoto, and Shigeki Takeuchi. Analysis of an experimental quantum logic gate by complementary classical operations. *Mod. Phys. Lett. A*, 21:1837, 2006.

[HOT06b] Holger F. Hofmann, Ryo Okamoto, and Shigeki Takeuchi. Locally observable conditions for the successful implementation of entangling multi-qubit quantum gates. arXiv.org:quant-ph/0509001, 2006.

[HRB08] H. Haeffner, C. F. Roos, and R. Blatt. Quantum computing with trapped ions. *Physics Reports*, 469:155, 2008.

[HT95] M Houe and P D Townsend. An introduction to methods of periodic poling for second-harmonic generation. *Journal of Physics D: Applied Physics*, 28(9):1747–1763, 1995.

[HT02] Holger F. Hofmann and Shigeki Takeuchi. Quantum phase gate for photonic qubits using only beam splitters and postselection. *Phys. Rev. A*, 66(2):024308, Aug 2002.

[JMH98] Jonathan A. Jones, Michele Mosca, and Rasmus H. Hansen. Implementation of a quantum search algorithm on a quantum computer. *Nature*, 393(6683):344–346, 1998.

[KCBS08] Alexander A. Klyachko, M. Ali Can, Sinem Binicioğlu, and Alexander S. Shumovsky. Simple test for hidden variables in spin-1 systems. *Phys. Rev. Lett.*, 101(2):020403, 2008.

[Kit95] A. Kitaev. Quantum measurements and the abelian stabilizer problem. arXiv:quant-ph/9511026, 1995.

[KL98] E. Knill and R. Laflamme. Power of one bit of quantum information. *Phys. Rev. Lett.*, 81(25):5672–5675, Dec 1998.

[KLM01] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, 2001.

[KMN+07] Pieter Kok, W. J. Munro, Kae Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Reviews of Modern Physics*, 79(1):135, 2007.

[Kni95] E. Knill. Approximation by quantum circuits. arXiv.org:quant-ph/9508006, 1995.

[Kni02] E. Knill. Quantum gates using linear optics and postselection. *Phys. Rev. A*, 66(5):052306, Nov 2002.

[Lan07] N. K. Langford. *Encoding, manipulating and measuring quantum information in optics*. PhD thesis, The University of Queensland, Brisbane, QLD, Australia, 2007.

[LBA+09] B. P. Lanyon, M. Barbieri, M. P. Almeida, T. Jennewein, T. C. Ralph, K. J. Resch, G. J. Pryde, J. L. O'Brien, A. Gilchrist, and A. G. White. Quantum computing using shortcuts through higher dimensions. *Nature Physics*, 5:134 – 140, Feb 2009.

[LBYP07] Chao-Yang Lu, Daniel E. Browne, Tao Yang, and Jian-Wei Pan. Demonstration of a compiled version of shor's quantum factoring algorithm using photonic qubits. *Phys. Rev. Lett.*, 99(25):250504, 2007.

[Llo96] Seth Lloyd. Universal quantum simulators. *Science*, 273:1073–8, Aug 1996.

[LR08] Netanel H. Lindner and Terry Rudolph. A photonic cluster state machine gun. arXiv.org:0810.2587, 2008.

[LRH08] A. P. Lund, T. C. Ralph, and H. L. Haselgrove. Fault-tolerant linear optical quantum computing with small-amplitude coherent states. *Phys. Rev. Lett.*, 100(3):030503, 2008.

[LVSK05] Xiaoying Li, Paul L. Voss, Jay E. Sharping, and Prem Kumar. Optical-fiber source of polarization-entangled photons in the 1550 nm telecom band. *Phys. Rev. Lett.*, 94(5):053601, Feb 2005.

[LWP+05] N. K. Langford, T. J. Weinhold, R. Prevedel, K. J. Resch, A. Gilchrist, J. L. O'Brien, G. J. Pryde, and A. G. White. Demonstration of a simple entangling optical gate and its use in bell-state analysis. *Phys. Rev. Lett.*, 95(21):210504, 2005.

[LZG+07] Chao-Yang Lu, Xiao-Qi Zhou, Otfried Guhne, Wei-Bo Gao, Jin Zhang, Zhen-Sheng Yuan, Alexander Goebel, Tao Yang, and Jian-Wei Pan. Experimental entanglement of six photons in graph states. *Nat. Phys.*, 3(2):91–95, 2007.

[MD04] A. Migdall and J. Dowling. See special issue: Single-photon: detectors, applications, and measurement methods. *J. Mod. Opt.*, 51, 2004.

[MKH+09] T. Monz, K. Kim, W. Hansel, M. Riebe, A. Villar, P. Schindler, M. Chwalla, M. Hennrich, and R. Blatt. Realization of the quantum toffoli gate with trapped ions. *Phys. Rev. Lett.*, 102:040501, 2009.

[NC01] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2001.

[Nie04] Michael A. Nielsen. Optical quantum computation using cluster states. *Phys. Rev. Lett.*, 93(4):040503, 2004.

[NM04] Kae Nemoto and W. J. Munro. Nearly deterministic linear optical controlled-not gate. *Phys. Rev. Lett.*, 93(25):250502, Dec 2004.

[OHTS05] Ryo Okamoto, Holger F. Hofmann, Shigeki Takeuchi, and Keiji Sasaki. Demonstration of an optical quantum controlled-not gate without path interference. *Phys. Rev. Lett.*, 95(21):210506, 2005.

[OPG+04] J. L. O'Brien, G. J. Pryde, A. Gilchrist, D. F. V. James, N. K. Langford, T. C. Ralph, and A. G. White. Quantum process tomography of a controlled-[small-caps not] gate. *Phys. Rev. Lett.*, 93:080502, 2004.

[OPW+03] J. L. O'Brien, G. J. Pryde, A. G. White, T. C. Ralph, and D. Branning. Demonstration of an all-optical quantum controlled-not gate. *Nature*, 426(6964):264–267, 2003.

[OZ01] Harold Ollivier and Wojciech H. Zurek. Quantum discord: A measure of the quantumness of correlations. *Phys. Rev. Lett.*, 88(1):017901, Dec 2001.

[Pap94] C. H. Papdimitriou. *Computatinal Complexity.* Addison-Wesley, Reading, MA, 1994.

[PCR+08] Alberto Politi, Martin J. Cryan, John G. Rarity, Siyuan Yu, and Jeremy L. O'Brien. Silica-on-Silicon Waveguide Quantum Circuits. *Science*, 320(5876):646–649, 2008.

[PdGHM07] J. H. Plantenberg, P. C. de Groot, C. J. P. M. Harmans, and J. E. Mooij. Demonstration of controlled-not quantum gates on a pair of superconducting quantum bits. *Nature*, 447:836–839, 2007.

[PFJF03] T. B. Pittman, M. J. Fitch, B. C Jacobs, and J. D. Franson. Experimental controlled-not logic gate for single photons in the coincidence basis. *Phys. Rev. A*, 68(3):032316, Sep 2003.

[PJF02] T. B. Pittman, B. C. Jacobs, and J. D. Franson. Demonstration of nondeterministic quantum logic operations using linear optical elements. *Phys. Rev. Lett.*, 88(25):257902, Jun 2002.

[poi09] http://en.wikipedia.org/wiki/binomial_distribution, Mar 2009.

[POW+04] G. J. Pryde, J. L. O'Brien, A. G. White, S. D. Bartlett, and T. C. Ralph. Measuring a photonic qubit without destroying it. *Phys. Rev. Lett.*, 92(19):190402, May 2004.

[POW+05] G. J. Pryde, J. L. O'Brien, A. G. White, T. C. Ralph, and H. M. Wiseman. Measurement of quantum weak values of photon polarization. *Phys. Rev. Lett.*, 94(22):220405, 2005.

[RB01] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86(22):5188–5191, May 2001.

[RBO+06] T. C. Ralph, S. D. Bartlett, J. L. O'Brien, G. J. Pryde, and H. M. Wiseman. Quantum nondemolition measurements for quantum information. *Phys. Rev. A.*, 73(1):012113, 2006.

[REP+05] C. A. Ryan, J. Emerson, D. Poulin, C. Negrevergne, and R. Laflamme. Characterization of complex quantum dynamics with a scalable nmr information processor. *Phys. Rev. Lett.*, 95(25):250502, 2005.

[RLBW02] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White. Linear optical controlled-not gate in the coincidence basis. *Phys. Rev. A*, 65(6):062324, Jun 2002.

[RLMN05] Danna Rosenberg, Adriana E. Lita, Aaron J. Miller, and Sae Woo Nam. Noise-free high-efficiency photon-number-resolving detectors. *Phys. Rev. A*, 71(6):061803, Jun 2005.

[RWMM01] T. C. Ralph, A. G. White, W. J. Munro, and G. J. Milburn. Simple scheme for efficient linear optics quantum gates. *Phys. Rev. A*, 65(1):012314, Dec 2001.

[RWZ05] K. J. Resch, P. Walther, and A. Zeilinger. Full characterization of a three-photon greenberger-horne-zeilinger state using quantum state tomography. *Phys. Rev. Lett.*, 94(7):070402, 2005.

[SAB+06] Matthias Steffen, M. Ansmann, Radoslaw C. Bialczak, N. Katz, Erik Lucero, R. McDermott, Matthew Neeley, E. M. Weig, A. N. Cleland, and John M. Martinis. Measurement of the Entanglement of Two Superconducting Qubits via State Tomography. *Science*, 313(5792):1423–1425, 2006.

[Sho94] P. Shor. In *Proc. 35th Ann. Symp. Found. Comp. Sci. 124*. IEEE Comp. Soc. Press, Los Alamitos, California, 1994.

[TDY+08] Gen Taguchi, Tatsuo Dougakiuchi, Nobuaki Yoshimoto, Katsuya Kasai, Masataka Iinuma, Holger F. Hofmann, and Yutaka Kadoya. Measurement and control of spatial qubits generated by passing photons through double slits. *Phys. Rev. A.*, 78(1):012307, 2008.

[TMCT05] Juan P. Torres, Ferran Macià, Silva Carrasco, and Lluis Torner. Engineering the frequency correlations of entangled two-photon statesby achromatic phase matching. *Opt. Lett.*, 30(3):314–316, 2005.

[TOK+08] M. S. Tame, S. K. Ozdemir, M. Koashi, N. Imoto, and M. S. Kim. Compact toffoli gate using weighted graph states. arXiv.org:0809.1513, 2008.

[TRT+01] S. Tanzilli, H. De Riedmatten, W. Tittel, H. Zbinden, P. Baldi, M. De Micheli, D.B. Ostrowsky, and N. Gisin. Highly efficient photon-pair source using periodically poled lithium niobate waveguide. *Electronics Letters*, 37(1):26–28, 2001.

[VBR08] Michael Varnava, Daniel E. Browne, and Terry Rudolph. How good must single photon sources and detectors be for efficient linear optical quantum computation? *Phys. Rev. Lett.*, 100(6):060502, 2008.

[VDDV02] F. Verstraete, J. Dehaene, B. De Moor, and H. Verschelde. Four qubits can be entangled in nine different ways. *Phys. Rev. A*, 65:052112, 2002.

[Vid03] Guifré Vidal. Efficient classical simulation of slightly entangled quantum computations. *Phys. Rev. Lett.*, 91(14):147902, Oct 2003.

[VPM+07] G. Vallone, E. Pomarico, P. Mataloni, F. De Martini, and V. Berardi. Realization and characterization of a two-photon four-qubit linear cluster state. *Phys. Rev. Lett.*, 98:180502, 2007.

[VSB+01] Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, and Isaac L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. *Nature*, 414(6866):883–887, 2001.

[Wei08] T. J. Weinhold. *Stepping stones towards linear optic quantum computing.* PhD thesis, University of Queensland, Nov 2008.

[WRR+05] P. Walther, K. J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger. Experimental one-way quantum computing. *Nature*, 434(7030):169–176, 2005.

[WRZ05] P. Walther, K. J. Resch, and A. Zeilinger. Local conversion of greenberger-horne-zeilinger states to approximate w states. *Phys. Rev. Lett.*, 94:240501, 2005.

[WSK+08] Witlef Wieczorek, Christian Schmid, Nikolai Kiesel, Reinhold Pohlner, Otfried Gühne, and Harald Weinfurter. Experimental observation of an entire family of four-photon entangled states. *Phys. Rev. Lett.*, 101(1):010503, 2008.

[ZZC+05] Zhi Zhao, An-Ning Zhang, Yu-Ao Chen, Han Zhang, Jiang-Feng Du, Tao Yang, and Jian-Wei Pan. Experimental demonstration of a nondestructive controlled-NOT quantum gate for two independent photon qubits. *Phys. Rev. Lett.*, 94(3):030501, 2005.