AFRL-RI-RS-TR-2012-073

QUANTUM INFORMATION SCIENCE

FEBRUARY 2012

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th ABW, Wright-Patterson AFB Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2012-073 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/s/
STEVEN JOHNS
Branch Chief

/s/
PAUL ANTONIK, Technical Advisor
Computing & Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Service, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
FEB 2012	**Final Technical Report**	OCT 2009 – SEP 2011

4. TITLE AND SUBTITLE

QUANTUM INFORMATION SCIENCE

5a. CONTRACT NUMBER
In House

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62702F

6. AUTHOR(S)

Paul M. Alsing
Michael L. Fanto

5d. PROJECT NUMBER
QIS0

5e. TASK NUMBER
PR

5f. WORK UNIT NUMBER
OJ

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/RITA
525 Brooks Road
Rome, NY 13441-4505

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/Information Directorate
Rome Research Site
26 Electronic Parkway
Rome NY 13441

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RI

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2012-073

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. **PA# 88ABW-2012-0892**
Date Cleared: **21 Feb 2012**

13. SUPPLEMENTARY NOTES

14. ABSTRACT
This is the final report for the AFRL/RI in-house project Quantum Information Science. Under this project we constructed a six qubit (quantum bit) capable photon-based experimental testbed for the development of photon-based quantum gates and circuits and performed experimental and theoretical investigations of quantum computation. These investigations included: theoretical/numerical simulation: (i) a hybrid coarse/fine parallel simulation of Grover's quantum search algorithm; (ii) the development of a variant of Grover's algorithm that explicitly searches on one component of a database (iii) the design of quantum optical gates by means of volume holography in photo-thermal refractive glass, and (iv) an investigation of the advantage of utilizing cluster states for a one-way quantum computational paradigm; experimental: (v) the construction and validation of a group velocity matched temporal compensator crystal assembly to increase the usable range of entangled photon sources, and (vi) the development and characterization of a new multipli-entangled photon source that increased the usable number of photon pairs by a factor of six.

15. SUBJECT TERMS

Quantum information processing, quantum entanglement, quantum computing

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					PAUL M. ALSING
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (*Include area code*)
U	U	U	UU	68	N/A

TABLE OF CONTENTS

LIST OF FIGURES

1.0 SUMMARY

Numerical and theoretical investigations of Grover's quantum search algorithm were investigated. The combination of coarse and fine grain parallel resources was explored as a means to utilize current massive multi-processing capabilities typically utilized for large scale graphics rendering purposes. The results, though preliminary, were encouraging for the utilization of a hybrid coarse/fine grain approach for numerical simulation of quantum algorithms. A variant of Grover's algorithm was developed that explicitly searches on one component of a database to find an associated element in the complementary component of the database. An investigation of developing single photon quantum optical gates written into centimeter sized photo-thermal refractive glass as volume holograms was explored. While not a scalable technology in general, this approach was shown to have advantage for small qubit number gates, offering footprint savings over corresponding meter-sized free space gates. A simulation of an entangled Bell state photon pair topologically encoded into a cluster state was carried out to explore the advantages of the measurement-based one-way quantum computation paradigm. The error threshold rates of approximately 5% and 8% that were computed are typically an order of magnitude higher than the most promising error threshold rates obtained by means of the standard quantum circuit model – indicating the potential power of the cluster state quantum computation paradigm. The development of a photon-based quantum information science (QIS) testbed, construction and validation of a group velocity matched (GVM), and a multipli-entangled photon source crystal assembly are described herein. These crystal assemblies are constructed and investigated for the more efficient generation of entangled photons as an input source to quantum computing circuits. The GVM source was shown to increase the useable entangled photon rate by removing the spectral distinguishability, and the multipli-entangled photon sources increased the usable pairs by a factor of six over the single pair typically produced. These two assemblies mitigated the problems inherent in conventionally used sources.

2.0 INTRODUCTION

Under this in-house project we constructed a six *qubit* (quantum bit) capable photon-based experimental testbed and explored topics related to both theoretical/numerical simulation and experimental investigations of quantum computation. These investigations included: ***theoretical/numerical simulation*** – (i) a hybrid coarse/fine parallel simulation of Grover's quantum search algorithm; (ii) the development of a variant of Grover's algorithm that explicitly searches on one component of a database to find an associated element in the complementary component of the database; (iii) the design of quantum optical gates by means of volume holography in photo-thermal refractive (PTR) glass, and (iv) an investigation of the advantage of utilizing cluster states for a one-way quantum computational paradigm; ***experimental*** – (v) the construction of an advanced quantum information science testbed for development of photon-based quantum gates and circuits; (vi) the construction and validation of a group velocity matched (GVM) temporal compensator crystal assembly to increase the usable range of entangled photon sources, and (vii) the development and characterization of a new multipli-entangled photon source that increased the usable number of photon pairs by a factor of six.

Theory/numerical simulations:
Grover's search algorithm (GSA) serves as an important prototypical benchmark for many numerical simulation efforts of quantum algorithms [Grover97, Walther05]. In one of the simulation portions of the research we investigated the use of hybrid coarse and fine grain parallelism to numerically simulate GSA. The goal was to investigate the use of conventional distributed computation utilizing MPI (Message Passing Interface) on a parallel cluster, whose CPUs also had access to multi-core GPU (graphics processor units).

Grover's oracle based unstructured search algorithm is often stated as "given a phone number in a directory, find the associated name." More formally, the problem can be stated as "given as input a unitary black box U_f for computing an unknown function $f:\{0,1\}^n \rightarrow \{0,1\}$ find $x=x_0$ an element of $\{0,1\}^n$ such that $f(x_0)=1$, (and zero otherwise)." The crucial role of the externally supplied oracle U_f (whose inner workings are unknown to the user) is to change the sign of the solution $|x_0\rangle$, while leaving all other states unaltered. Thus, U_f depends on the desired solution x_0. We developed/simulated an amplitude amplification algorithm in which the user encodes the directory (e.g. names and telephone numbers) into an entangled database state, which at a later time can be queried on one supplied component entry (e.g. a given phone number t_0) to find the other associated unknown component (e.g. name x_0). For $N=2^n$ names $|x\rangle$ with N associated phone numbers $|t\rangle$, performing amplitude amplification on a subspace of size N of the total space of size N^2 produces the desired state $|x_0\rangle|t_0\rangle$ in $\sqrt{N}$ steps.

In this in-house project we utilized photon-based qubits for the development of quantum gates and circuits. These qubits propagated in free-space (routed into optical fibers for measurements) and hence the quantum gate/circuit consisted of optical elements (beam splitters, waveplates, etc…) arranged on meter-sized optical tables. In one part of this research we explored the feasibility of using volume holograms to construct simple optical quantum gates in centimeter-sized PTR glass. Volume holography is typically used today for 2D image storage utilizing 394 pixels/μm^2, which consumes only 1% of the theoretical volumetric storage density ($1/\lambda^3$) [Burr01]. This field, first introduced by Dennis Gabor in 1948, has been well established ever since the development of the laser in 1960. As the emulsion of the hologram increases in thickness its angular selectivity, i.e. its ability to differentiate the difference between two planewaves separated by a small angle, increases and it is able under certain well-known conditions to achieve near perfect efficiency [Goodmann05]. A hologram is considered a volume hologram if the emulsion thickness $d >> \Lambda^2/\lambda$ where Λ is the characteristic period of the index of refraction of the grating, and λ is the wavelength of the light. For our purposes, it is important to emphasize that volume holography enables higher storage densities, and under suitable recording configurations can achieve near perfect efficiencies. The goal of this portion of the research was to investigate the possible use of volume holograms in PTR glass to create simple single photon quantum optical gates.

In the standard quantum circuit model (QCM) paradigm, quantum computations are executed by successive unitary operations acting upon an initial quantum state composed of many qubits. These unitary operators create entanglement amongst the qubits through quantum interference. Entanglement is uniquely non-classical property of quantum mechanical systems in which the correlations between sub-systems can be stronger than that allowed by classical (conventional)

computing systems. Recently a new alternative paradigm for quantum computation has emerged called one-way quantum computation (OWQC) [Ruassendorf01]. In the one-way quantum computer, information is processed by sequences of single-qubit measurements. These measurements are performed on a universal resource state—the 2D-cluster state—which does not depend on the algorithm to be implemented. The new approach to quantum computation goes by the collective name measurement-based quantum computation (MQC) [Briegel09]. The appeal of MQC is that deterministic quantum computation is possible based on (i) the preparation of an initial entangled cluster state followed by (ii) a temporally ordered patter of single qubit measurements and feed-forward operations which depend on the outcome of the previously measured qubits [Raussendorf01]. Our interests in OWQC is in the utilization of photon-based cluster states as gates and circuits for quantum computation (see [Vallone08], and references therein). It has been claimed that the use of cluster states can substantially reduce the resource overhead in the standard QCM to photon-based quantum computation.

Experimental:

Photons are particularly desirable for quantum information processing tasks since they are relatively free from environmental decoherence. Hence, they are also essential for any long distance conveyance of quantum information, and do not require cryogenic cooling. Entangled photon sources with the highest mode quality are based on spontaneous parametric down conversion (SPDC). This is a process where laser pump photons are converted into 'signal' and 'idler' entangled pairs in nonlinear (NL) crystals. SPDC in nonlinear crystals has provided the optical sources for groundbreaking foundational and applications work in quantum optics (QO) for the last two decades [O'Brien07].

SPDC is an inherently inefficient process, and work based on it is generally limited by the net signal level or the number of photons that can be entangled in given applications. Photon yield is related to laser power, which cannot be increased beyond the level where higher order NL contributions (multi-photon events) yield errors in quantum processing applications. This point has now been reached in applications that require independent sources of entangled qubits. The work addressed in this in-house project focused on (i) developing a 6-qubit capable photon-based quantum information testbed and (ii) developing new sources of entangled photons that greatly increase process efficiency, without increasing laser power, in a regime where high detection quantum efficiency is available - a highly desirable goal not previously accomplished in the scientific community to date.

Experimental demonstrations of entanglement in photon pairs has more recently become of interest in quantum computational architectures that operate by principles entirely distinct from those based on classical physics. Experiments such as two-photon interference in Hong-Ou-Mandel Interferometers (HOMI) [Hong87] and most quantum cryptography implementations require only single photons, not entangled photons, and hence single crystals. Most other quantum information experiments require multiple crystal sources for entangled photons. It has been found that multi-crystal sources of entangled pairs are not feasible with the continuous wave (CW) pump lasers that were used throughout the original QO developments; short pump pulses are essential for the multiple interference effects to be realized. The temporal-spectral information inherent in pulses however affects and constrains the quantum interference. The effects must be clearly understood to optimize the performance in practical applications. In this

in-house project we directed our efforts to the construction and validation of a group velocity matched (GVM) temporally compensated crystal assembly to increase the usable range of entangled photon sources, and to the development and characterization of a new multipli-entangled photon source crystal assembly that increased the usable number of photon pairs by a factor of six.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1. Hybrid coarse/fine parallel simulation of Grover's quantum search algorithm

Driven primarily by the video gaming industry's need for massive graphics processing, the programmable GPU has evolved into a computational workhorse. With multiple cores driven by very high memory bandwidth, the GPU holds potential for non-graphics processing scientific computing. The main reason for such optimism is that the GPU is specialized for compute-intensive, highly parallel computation (exactly what graphics rendering is about) and therefore is designed such that more transistors are devoted to data processing rather than data caching and flow control.

More specifically, the GPU is especially well-suited to address problems that can be expressed as data-parallel computations – the same program is executed on many data elements in parallel – with high *arithmetic intensity* (the ratio of arithmetic operations to memory operations). Because the same program is executed for each data element, there is a lower requirement for sophisticated flow control; and because it is executed on many data elements and has high arithmetic intensity, the memory access latency can be hidden with calculations instead of big data caches. Data-parallel processing maps data elements to parallel processing threads. Many applications that process large data sets such as arrays can use a data-parallel programming model to speed up the computations.

Currently, AFRL/RI is actively pursuing large scale parallel scientific computing. At the AFRL/RI Naresky High Performance Computing Facility the main computational resource is an AFRL/RI 500 TFLOP (July 2010) integrated HPC system consisting of 2,016 PlayStation3 (cell broadband engine processor) nodes and 84 x86 servers each with an nVidia Tesla C1060 and an nVidia Tesla C2050 GPGPU (general purpose graphical processing unit).

The exploratory codes we developed to simulate Grover's quantum search algorithm utilized a combination of MPI libraries for conventional distributed parallel communication between the host CPUs and CUDA (from the company NVIDIA, (see [CUDA07]) which stands for Compute Unified Device Architecture. CUDA is a new hardware and software architecture for issuing and managing computations on the GPU as a data-parallel computing device without the need of mapping them to a graphics API.

When programmed through CUDA, the GPU is viewed as a *compute device* capable of executing a very high number of threads in parallel. It operates as a coprocessor to the main CPU, or *host*. In other words, data-parallel, compute-intensive portions of applications running on the host are off-loaded onto the device. More precisely, a portion of an application that is executed many times, but independently on different data, can be isolated into a function that is executed on the device as many different threads. To that effect, such a function is compiled to the instruction set

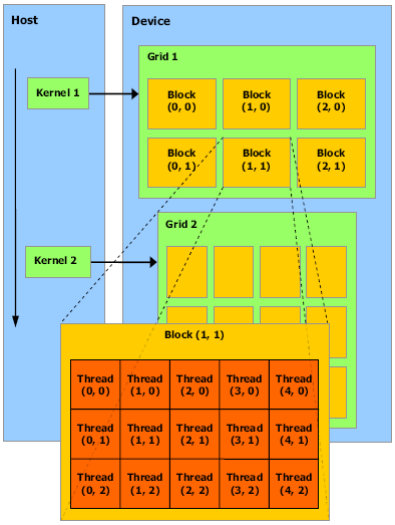


Figure 1. CUDA host/device structure: the host (CPU) issues a succession of kernel invocations to the device (GPU). Each kernel is executed as a batch of threads organized as a grid of thread blocks.

of the device and the resulting program, called a *kernel*, is downloaded to the device. Both the host and the device maintain their own DRAM, referred to as *host memory* and *device memory*, respectively. One can copy data from one DRAM to the other through optimized API calls that utilize the device's high-performance Direct Memory Access (DMA) engines. This is illustrated in Figure 1.

Grover's quantum search algorithm executes an unstructured search on a collection of *n* qubits (quantum bit, e.g. two-level atomic-level quantum system, two-state polarization states of a photon, etc…), which due to the tensor space product nature of composite quantum systems, represents $N=2^n$ cbits (classical bits). This exponential scaling of accessible information *N* with the linear number *n* of the physical qubits is behind the power and lure of quantum computation. Because of the quantum superposition principle, all *N* bits can be searched simultaneously. The unstructured search problem is often colloquially stated as "finding a needle in a haystack," or "given a telephone number, find the associate name in a telephone directory." In a conventional (classical) unstructured search problem, one would need on the order of N/2 queries to an oracle (returning a yes or no answer to question "is this the needle?" or "is this the correct name?") to find the correct solution (e.g. the "needle" or the "name"). Utilizing quantum parallelism, the GSA can find the answer using only on the order of √N queries – a quadratic speedup over the conventional algorithm.

The quantum state $|\psi\rangle$ can be represented as an *N*-dimensional unit vector with complex entries called quantum amplitudes, $|\psi\rangle = \sum_{x=0}^{N-1} c_x |x\rangle$. The entries of the vector $|\psi\rangle$ represent the *N* possible states labeled (decimally) as $|x\rangle = \{0,1,\ldots,N-1\}$. The squared amplitude $|c_x|^2$ gives the

probability that the state $|\psi\rangle$ will be found in ("collapse" to) the component state $|x\rangle$ after the execution of a physical measurement. Quantum operations act upon $|\psi\rangle$ by means of unitary matrices *U*, transforming the system to the new, normalized state $|\psi'\rangle$ via $|\psi'\rangle = U|\psi\rangle$. The unitary operator *U* represents physical operations (e.g. the illumination of atoms/ions by lasers, application of gate voltages to quantum dots/superconducting circuits, passage of light through optical elements, etc…) that must be implemented upon the physical realization of the quantum state vector $|\psi\rangle$. This is called the *quantum circuit model* of quantum computation. For the study of quantum algorithms, we can abstract away concerns of physical realizations and implementations (though this is of intense research interest both experimentally and theoretically).

In Figure 2 illustrates the successive action of Grover unitary iterate $G = U_{inv} U_f$ on an *n*=3 qubit state, corresponding to a search on $N=2^3=8$ bits (adapted from [Yanofsky08]). The goal of the GSA is to apply G successively so that the quantum state $|\psi\rangle$ is steered towards the unknown

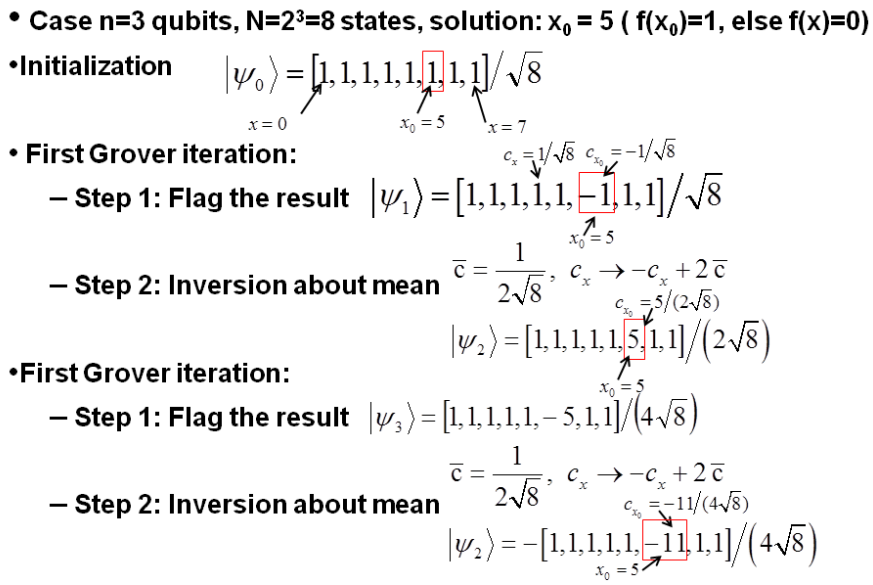


Figure 2. Outline of Grover's search algorithm on n=3 qubits ($N=2^3$ = 8 bits).

"needle" component state labeled $|x_0\rangle$. Queries to an oracle (externally supplied to the questioner) formally answer the yes/no question "is a given *x* equal to x_0 ." In other words, the oracle computes the function $f(x)$ with results $f(x_0)=1$, while $f(x \neq x_0)=0$. In Figure 2, we choose the "needle" to be the state $x_0=5$.

The GSA begins as follows (see Figure 2). We initialize the system to equal-amplitude unbiased state $|\psi_0\rangle$, where, in this example, each amplitude has the value $1/\sqrt{8}$. This implies there is an

equal probability of 1/8 to find the system in any state $|x\rangle$ upon measurement. The Grover iterate G involves two separate unitary operations, applied in right to left order, to the quantum state. The first unitary U_f implements the effective operation $U_f|x\rangle = (-1)^{f(x)}|x\rangle$ on each component state $|x\rangle$, with the net effect of "tagging" the solutions state $|x_0\rangle$ with a minus sign, while leaving all states $|x \neq x_0\rangle$ unchanged. The second unitary U_{inv} of the Grover iterate implements an "inversion about the mean" of all the quantum amplitudes. This implements the operation $c_x \mapsto 2\bar{c} - c_x$ where $\bar{c} = \sum_x c_x / N$ is the average of all the quantum amplitudes c_x.

After one application of G we observe in Figure 2 that the amplitude of the state $|x_0\rangle$ has increased to five times that of all other states, implying that it is 25X more likely ($\left|c_{x_0}/c_x\right|^2$) to be observed upon measurement than the remaining states. After a second implementation of the Grover iterate Figure 2 reveals that this likelihood has increased to 121X ($\left|c_{x_0}/c_x\right|^2$). It can be shown that the optimal number of Grover iterations k to achieve maximum probability to observe the solution state upon measurement is $k \sim \lfloor \pi\sqrt{N}/4 \rfloor$ (where the notation $\lfloor z \rfloor$ denotes *floor(z)*, the nearest integer less than *z*).

3.2 Grover's search algorithm with an entangled database state

Grover's search algorithm [Grover97] is one of the most highly recognized quantum algorithms (next to Shor's factorization algorithm [Shor94]), being widely taught in many texts on quantum computation [Kaye07, Yanofsky08] and serves as a benchmark for nascent physical implementations of quantum computers [Walther05]. Formally, Grover's search algorithm (GSA) considers the following scenario [Boyer96], suppose you have a large table $T[0\ldots N\text{-}1]$ of N entries for which you would like to find some element z_0. More precisely, you wish to find an integer x_0 such that $0 \leq x_0 < N$ and $T[x_0] = z_0$, provided that such an x_0 exists. If the table is sorted the problem can be solved in a time $O(\log N)$. However, in many interesting problems, ordering or structuring the data may not be possible or practical, and one must resort to the brute force method of exhaustively searching through all the data until the result is found (or to determine if it even exists). Classically, there is no algorithm that succeeds with probability greater than ½ without searching through more than half the entries of T. Grover [Grover97] described his algorithm as finding a needle in the haystack, and equivalently as finding the associated name in a telephone book when one is supplied with a given telephone number (in which the telephone book is sorted on the names, but random on the telephone numbers). Grover's quantum unstructured search algorithm can solve this problem on a quantum computer in expected time in $O(\sqrt{N})$. The GSA has also been shown to be optimal [Boyer96], implying that a quantum algorithm cannot achieve faster than a quadratic speedup over its classical counterpart.

The GSA utilizes an *oracle*, which computes a function $f(x)$ of the input x, but whose inner workings are unknown and unavailable to the user. The Grover search problem can be stated formally [Kaye07] as

The Grover Search Problem

Input: A black box (oracle) U_f for computing an unknown function $f: \{0,1\}^n \rightarrow \{0,1\}$.

Problem: Find an input $x_0 \in \{0,1\}^n$ such that $f(x_0) = 1$ and $f(x \neq x_0) = 0$.

In the above, *f* is the classical function which evaluates to "yes" on the needle and "no" on the more abundant pieces of hay in the haystack. U_f is the unitary representation of *f* which acting on *x* encoded into a quantum multi-qubit state $|x\rangle$, performs the reversible operation

$$U_f|x\rangle\otimes|y\rangle=|x\rangle\otimes|y\oplus f(x)\rangle, \tag{1}$$

where $|y\rangle$ is a single auxiliary qubit and $\oplus$ denotes binary (mod 2) addition. (Note: from now on we will often write the tensor products of state $|x\rangle\otimes|y\rangle$ simply as $|x\rangle|y\rangle\equiv|x,y\rangle$).

As is well known, and as will be explicitly illustrated below, U_f requires knowledge of the solution x_0 in order to be explicitly constructed [Yanofsky08]. This is why the oracle U_f is part of the input to the GSA, and it has to be supplied externally to the user performing the search. Recently, there has been interest in developing algorithms that would dispense with the Grover oracle U_f and encode the search list directly into a quantum database state which can be initially constructed (e.g. an encoding of a telephone book), and subsequently searched at a later time (e.g. given a telephone number, find the associated name). Xu *et al.*[Xu08] have designed such an $O(\sqrt{N})$ algorithm based on adiabatic quantum computing (AdQC) and experimentally demonstrated its operation on a two qubit "telephone book" in an NMR quantum computer. In their work, only the names were encoded into the quantum database state, while the telephone numbers were encoded as classical integers. The goal of our work was to enunciate a quantum search algorithm (QSA), analogous in spirit to Xu *et al.*[Xu08], but in the usual quantum circuit model paradigm (i.e. an explicit unitary operator approach vs the Hamiltonian approach of AdQC).

The Grover iteration and the phase kickback or solution tagging operation

The essential operation in Grover's algorithm is the Grover iteration [Kaye07]

$$G=U_{\psi^\perp}U_f \tag{2}$$

composed of two functionally distinct unitary components (i) U_f, the phase kickback (PK) or "solution tagging" operation, and (ii) $U_{\psi^\perp}$, the inversion about the mean (IAM). The phase kickback unitary operation works as follows

$$U_f|x\rangle\otimes|-\rangle=U_f|x\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}=|x\rangle\otimes\frac{|0\oplus f(x)\rangle-|1\oplus f(x)\rangle}{\sqrt{2}}=(-1)^{f(x)}|x\rangle\otimes\frac{|0\rangle-|1\rangle}{\sqrt{2}}=(-1)^{f(x)}|x\rangle\otimes|-\rangle \tag{3}$$

where we have used (1) with $|y\rangle=H|1\rangle\equiv|-\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$ with the Hadamard operator $H=\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\Big/\sqrt{2}$ which also maps $H|0\rangle\equiv|+\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$. In the first equality of (3), U_f acts on both terms of $|y\rangle$ simultaneously (quantum parallelism). Explicitly working out both cases $f(x_0)=1$ and $f(x\neq x_0)=0$ yields two results that can be encapsulated into the single statement given by the rightmost expression. This is the famous phase kickback [Grover97, Kay07, Yanofsky08] in which the evaluation of the function *f* is stored in the quantum phases $e^{i\theta}$ (here, with $\theta\in\{0,\pi\}$). Since the single auxiliary qubit $|y\rangle=|-\rangle$ is returned to its initial state after the PK operation, one often abbreviates (3) to

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle \tag{4}$$

with the understanding that the required auxiliary qubit $|y\rangle$ is implied. The net result of U_f is that the sought after solution state $|x_0\rangle$ is flagged with a -1, while all other states $|x \neq x_0\rangle$ are unchanged. An explicit matrix realization (Yanofsky08) of the unitary operator U_f is shown in Fig. 3 for the case of two qubits with solution state x_0 = 2 in the decimal representation, corresponding to 10 in the binary representation. (From now on we will primarily use the decimal representation x∈{0,1,…,N-1} on *n* qubits, where N=2^n). Figure 3 illustrates the assertion that one needs to know the solution x_0 in order to construct the oracle U_f.

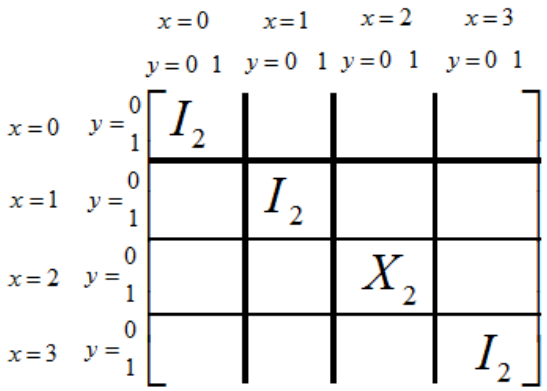


Figure 3. Explicit construction of the unitary phase kickback operator U_f^{xy} for the case of two qubits.

Figure 3 illustrates the explicit construction of the unitary phase kickback operator U_f^{xy} for the case of two qubits labeled by the decimal x∈{0,1,2,3} (↔{00,01,10,11}, binary) representation. In this example, the solution state is x_0 = 2 (binary, 10), X_2 denotes the 2x2 Pauli σ_x bit-flip matrix and I_2 denotes the 2x2 unit matrix. The superscript *xy* on U_f^{xy} denotes that the PK operation acts upon the 3-qubit state $|x\rangle \otimes |y\rangle$, where *y* is a single qubit auxiliary state.

In Fig.3, the x= x_0=2 diagonal block of U_f^{xy} contains the 2x2 Pauli bit-flip matrix denoted as X_2 which flips the single auxiliary *y* qubit. All other x≠x_0 diagonal blocks U_f^{xy} contain the 2x2 identity matrix, denoted as I_2, which leaves the *y* qubit unaltered. The superscript *xy* on U_f^{xy} denotes that the PK operation acts upon the 3-qubit states $|x\rangle \otimes |y\rangle$, and the net effect is to multiply the state $|x_0\rangle \otimes |-\rangle$ by the phase factor -1, leaving all other states unaltered. Since there are *N*=4=2^2 qubits in this example, there are 4 block diagonals in which to place the bit-flip operator X_2. The choice of which specific diagonal block is X_2 placed is determined by the solution state x_0. Formally, the PK operation has the form $U_f^{xy} = |x_0\rangle\langle x_0| \otimes X_2^y + \sum_{x \neq x_0} |x\rangle\langle x| \otimes I_2^y$ that explicitly illustrates this point. Thus, the construction of the PK operator requires knowledge of the solution state x_0. This is the primary reason why U_f^{xy} is given as an "input" to the GSA, and is considered as an *externally provided* oracle.

The inversion about the mean operation

The second unitary in the Grover iterate (2) is the inversion about the mean operation, given by

$$U_{\psi^\perp} = H^{\otimes n} U_{0^\perp} H^{\otimes n} \tag{5}$$

where $H^{\otimes n}$ takes the *n*-qubit initial state $|0\rangle$ to the unbiased, equal amplitude product state $|\psi\rangle = 1/\sqrt{N}\sum_{x=0}^{N-1}|x\rangle \equiv \prod_{i=0}^{N-1} H|0\rangle_i$ (the *n*-fold tensor product of $H|0\rangle_i$ of all qubits). For *n*-qubits, we will denote this for simplicity as

$$H|0\rangle = |\psi\rangle . \tag{6}$$

The operator $U_{0^\perp}$ is defined as

$$\begin{aligned} U_{0^\perp}|0\rangle &= |0\rangle, \\ U_{0^\perp}|x \neq 0\rangle &= -|x \neq 0\rangle. \end{aligned} \tag{7}$$

Note that $U_{0^\perp}$ does not require knowledge of the solution state x_0; it simply flips the sign of all states except the standard initial state x=0. $U_{0^\perp}$ therefore, has the representation $U_{0^\perp} = |0\rangle\langle 0| - |1\rangle\langle 1| - \ldots - |N-1\rangle\langle N-1| = 2|0\rangle\langle 0| - I_N$ where we have used the completeness relation $I_N = \sum_{x=0}^{N-1}|x\rangle\langle x|$, with I_N being the NxN unit matrix. Thus, using (6) we can express $U_{\psi^\perp}$ in (5) as

$$U_{\psi^\perp} = 2|\psi\rangle\langle\psi| - I_N . \tag{8}$$

A straightforward calculation [Kay07,Yanofsky08] reveals that $U_{\psi^\perp}$ maps the amplitudes c_x of arbitrary quantum state $|\varphi\rangle = \sum_x c_x |x\rangle$ according to $c_x \mapsto 2\bar{c} - c_x$ where $\bar{c} = \sum_x c_x / N$ is the average of all the quantum amplitudes c_x. This is easily seen since $\text{Avg} \equiv |\psi\rangle\langle\psi|$ is the matrix with each entry taking the value $1/N$, that maps an arbitrary quantum vector $|\varphi\rangle$ to a vector whose every component is $\bar{c}$. Thus, $U_{\psi^\perp}$ performs an inversion of each quantum amplitude c_x about its mean value $\bar{c}$. It has been shown that after $k \sim \lfloor \pi\sqrt{N}/4 \rfloor$ successive Grover iterations the state $|\psi^{(k)}\rangle = G^k|\psi\rangle$ reaches maximal probability to be in the state $|x_0\rangle$.

3.3 Quantum computing in a piece of glass using volume holograms

Volume holography is used today for 2D image storage utilizing 394 pixels/μm^2, which consumes only 1% of the theoretical volumetric storage density ($1/\lambda^3$) [Burr01] and this field that was first introduced by Dennis Gabor in 1948 has been well established ever since the development of the laser in 1960. As the emulsion of the hologram increases in thickness its angular selectivity, i.e. its ability to differentiate the difference between two planewaves separated by a small angle, increases and it is able under certain well-known conditions to achieve near perfect efficiency [Goodmann05]. A hologram is considered a volume hologram if the emulsion thickness d >> Λ^2/λ where Λ is the characteristic period of the index of refraction of the grating, and λ is the wavelength of the light. It is important for our purposes to emphasize

that volume holography enables higher storage densities, and under suitable recording configurations can achieve near perfect efficiencies.

The transmission volume holograms we consider are formed when a "signal" wave, $\langle \vec{r} | S \rangle = A(\vec{r}) e^{i\Phi(\vec{r})}$ is directed into a holographic emulsion and made to coherently interfere with an oblique "reference" planewave, $\langle \vec{r} | R \rangle$ as illustrated in the left diagram of Fig. 4 for N=3. In the figure the ``signal" wave is a superposition of N planewaves,

$$\langle \vec{r} | S \rangle = \sum_{i=1}^{N} \langle \vec{r} | S_i \rangle \sum_{i=1}^{N} e^{i\alpha_i} e^{i\vec{k}_i \cdot \vec{r}_i}, \tag{9}$$

where α_i are pure phase angles. Here, we only consider planar reference waves, and the signal state as the superposition of planewaves. Ordinarily the signal waves will have variable phase

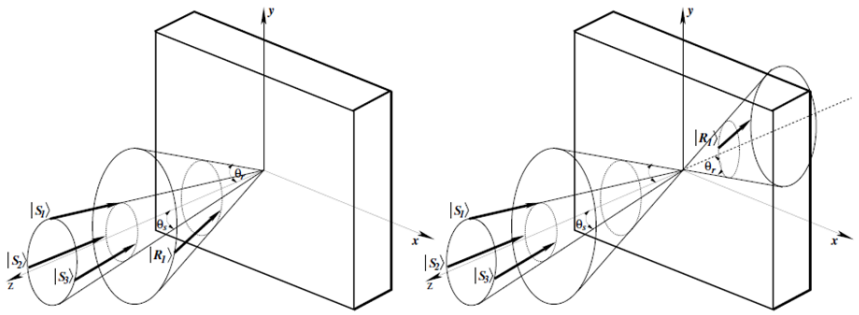


Figure 4. Recording (left) and reconstruction (right) by a volume hologram transmission grating.

and amplitude modulations. After the hologram is developed, and if we direct the identical signal wave $\langle \vec{r} | S \rangle$ into the hologram, then for a perfectly tuned hologram, the reference planewave $\langle \vec{r} | R \rangle$, should emerge as illustrated in the right diagram of Fig. 4. If the photo-thermal refractive (PTR) is not tuned to the correct length, other diffracted orders, e.g. modes parallel to the signal states, may emerge.

In Fig. 4 the left diagram shows a recording of a volume transmission grating by the coherent superposition of a plane reference wave $|R_1\rangle$ and a linear superposition of three signal waves $|S\rangle = e^{i\alpha_1}|S_1\rangle + e^{i\alpha_2}|S_2\rangle + e^{i\alpha_3}|S_3\rangle + e^{i\alpha_4}|S_4\rangle$. On the right we show the function of the hologram. If the identically oriented signal wave $|S\rangle$ is sent into the hologram then the reference wave, $|R_1\rangle$ will be reconstructed in the diffraction. The diffraction pattern will ordinarily consist of higher order diffracted modes parallel to the signal state. However, for a suitably tuned volume hologram perfect efficiency can be achieved, as shown in the right diagram of Fig. 4 [Miller11a,

b]. This is why we constrained the signal wave components to a cone of half angle θ_s centered on the normal to the hologram face.

Recently we have shown [Miller11a] that near perfect efficiencies can be obtained if (1) the hologram thickness is tuned to its optimal thickness, (2) if the each of the signal's Fourier wavevectors have the same projection onto the normal to the hologram surface, i.e. they all lie on a cone with half angle θ_s as shown in Fig. 4 and (3) each of the reference planewaves lie on their own distinct cone concentric with the first, with half angle θ_r and centered on the normal to the hologram face. We have also considered multiplex holograms wherein multiple independent exposures are made within the holographic emulsion before it is developed. We demonstrated using coupled-mode theory that if the signal waves $\{S_i\}_{i=(1,2,\ldots N)}$ form an orthogonal set under the L_2 norm in the plane perpendicular to the waves propagation direction (z), i.e.

$$\left\langle S_i \middle| S_j \right\rangle = \int S_i^*(x,y) S_j(x,y) dxdy = \delta_{ij}, . \tag{10}$$

then perfect efficiency can be achieved for each of the signals [Miller11a].

A volume multiplexed hologram that has achieved perfect efficiency (within coupled-mode theory [Kogelnik69] under the ``3+1" conditions outlined above provides a linear map between signal and reference modes. Physically it represents a projection (or redirection) operator or signal state sorter [Miller11a,b]

$$\hat{P} = \left| R_1 \right\rangle \left\langle S_1 \right| + \left| R_2 \right\rangle \left\langle S_2 \right| + \ldots + \left| R_N \right\rangle \left\langle S_N \right| . \tag{11}$$

uniquely identifying each pair of signal and reference waves. Although the index of refraction within the emulsion can be rather complicated, these devices are strictly linear optical components. Therefore, the diffraction patterns for a beam of photons will correspond exactly to the probability distribution for a single photon in the beam. In our work we assumed that we were dealing with low number Fock states. In section 4.3 we show how this theory can be applied to develop a CNOT gate using stacked holograms in PTR glass.

3.4 Cluster state/one-way quantum computation

As a focus for our experimental efforts in QIS we initiated an investigation into the utility/feasibility of measurement-based quantum computation (MQC) as a computing paradigm [Briegel09]. MQC also goes by the name one-way quantum computation (OWQC) or cluster state quantum computation (CSQC) (see [Ruassendorf01]) because the computation is driven by irreversible measurements performed on a large scale entangled resource state, rather than by a sequence of reversible unitary gates in the usual quantum circuit model (QCM). The initial entanglement resources of the OWQC are called graph states (in general), or cluster states (a graph state arranged as a two or three dimensional regular grid). The appeal of MQC is that deterministic quantum computation is possible based on (i) the preparation of an initial entangled cluster state followed by (ii) a temporally ordered patter of single qubit measurements and feed-forward operations which depend on the outcome of the previously measured qubits

[Raussendorf01]. Our interest in OWQC is in the utilization of photon-based cluster states to develop gates and circuits for quantum computation (see [Vallone08], and references therein).

In contrast to the quantum circuit model, where quantum computations are implemented by unitary operations, in the OWQC approach information is processed by sequences of single-qubit measurements. These measurements are performed on a universal resource state—the 2D-cluster state—which does not depend on the algorithm to be implemented. A one-way quantum computation proceeds as follows: (i) A classical input is provided which specifies the data and the program; (ii) A 2D-cluster state of sufficiently large size is prepared. The cluster state serves as the resource for the computation; (iii) A sequence of adaptive one-qubit measurements is implemented on certain qubits in the cluster. In each step of the computation the measurement bases depend on the specific program under execution and on the outcomes of previous measurements. A simple classical computer is used to compute which measurement directions have to be chosen in every step; (iv) After the measurements the state of the system has the product form $\left|\xi^{\alpha}\right\rangle\left|\psi_{out}^{\alpha}\right\rangle$, where α indexes the collection of measurement outcomes of the different branches of the computation. The states $\left|\psi_{out}^{\alpha}\right\rangle$ in all branches are equal to the desired output state up to a local (Pauli) operation. The measured qubits are in a product state $\left|\xi^{\alpha}\right\rangle$ which also depends on the measurement outcomes. The OWQC is computationally universal, i.e. even though the results of the measurements in every step of the computation are random, any quantum computation can deterministically be realized. Notice that the temporal ordering of the measurements plays an important role and has been formalized as a feed-forward procedure [Raussendorf01].

In realistic physical systems decoherence tends to make quantum systems behave more classically. One could therefore expect that decoherence would threaten any computational advantage possessed by a quantum computer. However, the effects of decoherence can be counteracted by quantum error correction [Shor96]. In fact, arbitrarily large quantum computations can be performed with arbitrary accuracy provided the error level of the elementary components of the quantum computer is below a certain threshold. This important result is called the threshold theorem of quantum computation [Aliferis06].

Fault-tolerant schemes for OWQC using photons have recently been developed [Dawson06, Varnava06]. The dominant sources of error in this setting are photon loss and gate inaccuracies. The constraint of short-range interaction and arrangement of qubits in a 2D lattice—a characteristic feature of the initial one-way quantum computer—is not relevant for photons. In [Dawson06] both photon loss and gate inaccuracies were taken into account yielding a trade-off curve between the two respective thresholds. Fault-tolerant optical computation is possible for a gate error rate of 10^{-4} and photon loss rate of $3\text{x}10^{-3}$. In [Varnava06] the stability against the main error source of photon loss was discussed. With non-unit efficiencies η_S and η_D of photon creation and detection being the only imperfections, the very high threshold of $\eta_S\eta_D > 2/3$ was established. Further, encoding a collection of physical qubits within the 2D cluster state offers a means of topological error protection for the logical qubit. Topologically protected quantum gates are performed by measuring some regions of qubits in the Z-basis, which effectively removes the qubits from the state. The remaining cluster, whose qubits are measured in the X-

and X ±Y -basis, thereby attains a non-trivial topology in which fault-tolerant quantum gates can be encoded. A topological method of fault-tolerance for OWQC can then be achieved [Raussendorf07]. In the work investigated here we numerically studied the evolution and topological protection of a maximally entangled Bell state pair from an initial 2D plane to terminal 2D plane in a 3D rectangular cluster state.

3.5 Quantum information science testbed

To perform quantum information experiments a testbed was constructed to generate photon based quantum bits. These polarization-entangled photons were generated via the process of spontaneous parametric down conversion (SPDC). This involves a source of light with a characteristic higher energy (i.e. "blue" light) spontaneously splitting into two correlated photons of lower energy (i.e. "red" light).

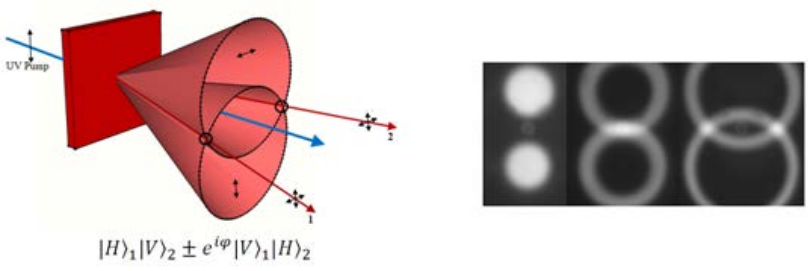


Figure 5. Type-II SPDC photon source (left) and resulting (unnormalized) entangled photon polarization state. In-house laboratory images (right) showing SPDC ring evolution with the variation of the crystal orientation.

Energy and momentum are conserved in the process so the energies and directions of propagation of these photon pairs are correlated. The polarization of the light is an additional parameter that can be correlated. There are two predominant forms of SPDC. In a single type-II crystal, the pair of photons emerges with orthogonal polarizations on two spatially separate cones (Fig. 5) due to the birefringence of the crystal. In a single type-II crystal the photons emerge on a single cone (diametrically opposed) with the same polarization. In practice, two type-I crystals are used to produce two overlapping cones of two distinct polarization (Fig6). For both types of

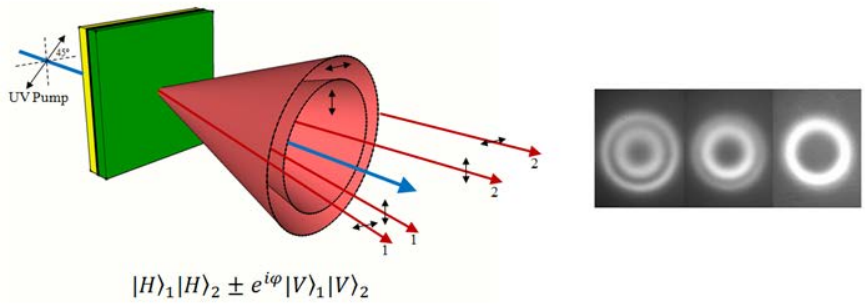


Figure 6. Type-I pair SPDC photon source (left) and resulting (unnormalized) entangled polarization state. In-house laboratory images (right) showing SPDC ring evolution with the variation of the crystal orientation.

SPDC, regions where the cones overlap are potential candidates for extracting polarization-entangled photon pairs. These sources are described in greater detail in the following paragraphs. These bulk crystal based photon sources are the fundamental basis on which the testbed is constructed, with the other main components being the continuous wave (CW) and pulsed pump lasers and the single photon detectors.

High intensity type-II SPDC sources described by Kwiat [Kwiat95] served as the first realizable source for the generation of entangled photons. The output of this source is comprised of two orthogonally-polarized entangled photons (signal & idler) produced upon excitation from a linearly-polarized pump laser beam. Due to the inherent birefringence of the crystal there is noticeable signal, idler walk off which leads to the familiar double ring pattern as illustrated in Fig. 5. The intersections of the two orthogonally-polarized rings are regions of photon indistinguishability where entanglement occurs. Variation of the crystal orientation changes the size and therefore the intersection points of the rings as shown in Fig. 5. The typical operational configuration is collinear or tangential, where the two rings intersect at nearly 90°. This produces a Gaussian-like beam profile which gives a high coupling efficiency into optical fiber.

Type-I crystals have been used for many years as frequency converters for second harmonic generation (SHG). The signal and idler photons produced from type-I down-conversion are both orthogonal with respect to the linear pump beam. The fact that the signal and idler photons both have the same polarization mitigates the walk-off problem due to the birefringence of the crystal. Varying the crystal orientation produces either a single output cone or single beam with respect to the linear pump beam. Kwiat first described the use of type-I crystals as a feasible source for SPDC-generated entangled photons with the development of the type-I pair design [Kwiat99]. This consisted of a pair of type-I crystals rotated with their optic axes orthogonal to each other. This allows for the production of two orthogonally-polarized cones of photons (see Fig. 6) which overlap upon correct rotation of the crystal. The pump must also be changed from purely horizontal or vertical polarization as for a single type-I crystal, to 45° to excite both crystals. Since signal, idler walk-off due to birefringence is not an issue in type-I crystals this source is more efficient than a type-II source. This is due to the longer interaction length in which the photons remain entangled over the crystal length, thus allowing for longer crystals. Further, in a configuration in which the two rings overlap photons along the entire ring are indistinguishable allowing for any diametrically opposite pair to be collected and utilized [Dragoman01]. The fundamental collection limit of this source is governed by the bulk size of the hardware, namely how many apertures can be stationed in front of the ring for collection of the diametric pairs.

Various other schemes have been developed for increasing the useable output of type-II to limits approaching that of type-I. Bitton et. al. describe a type-II pair with each crystal's optical axis rotated 180° with respect to each other; (see Fig. 7) [Bitton01]. This allows the linear pumping scheme to remain unchanged while allowing both crystals to produce one set of rings each with the polarization orientation rotated 180°. In this configuration any selected diametric pair across either ring is indistinguishable and useable, and the size of the collection apertures becomes the limiting factor in the number of diametric pairs that can be collected.

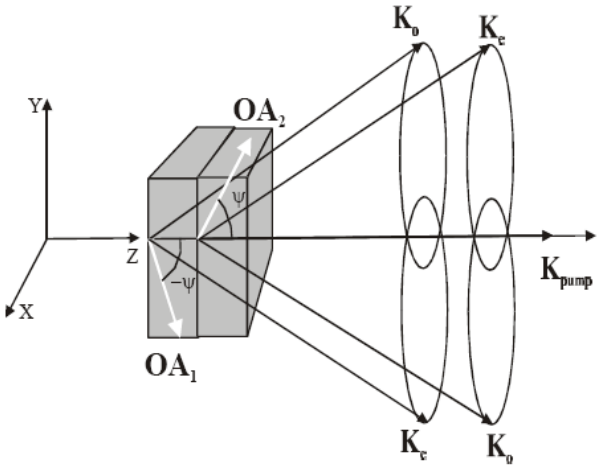


Figure 7. Type-II entangled photon pair as described by Bitton et. al. [4].

U'Ren et al. described a type-II crystal assembly (see Fig. 8) that is designed for group velocity matching (GVM) of the pump and signal/idler wave packets, thereby removing the spectral distinguishability of the photons [U'Ren06]. The symmetric nature of the joint spectral function of the entangled photons produced from this crystal removes the need for spectral filtering of the down-converted photons inherent to all current SPDC sources. This increases the percentage of useable entangled photons produced from a single type-II crystal. This source will be described in greater detail in sections 3.6 and 4.6.

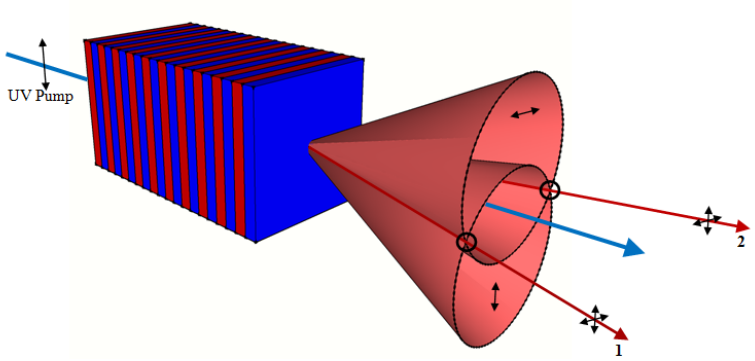


Figure 8. Type-II custom assembly showing alternating BBO (red) and calcite (blue) segments.

With an ever increasing need for larger numbers of entangled photon pairs, new sources must either produce more photons or the efficiency must be increased to compensate for the spontaneous nature of the source. A particular area of interest where larger numbers of photons are desired is photon-based cluster state quantum computing (CSQC). In CSQC individual pairs of photons are entangled together to form larger arrays of entangled photons. Typically, large numbers of single pairs are generated by cascading or multi-passing the excitation beam through SPDC sources as shown in Fig. 9 [Lu07]. In a typical configuration each of these sources produces a single pair of entangled photons. Obtaining a larger photon number requires an increase in the overall footprint size of the experimental setup.

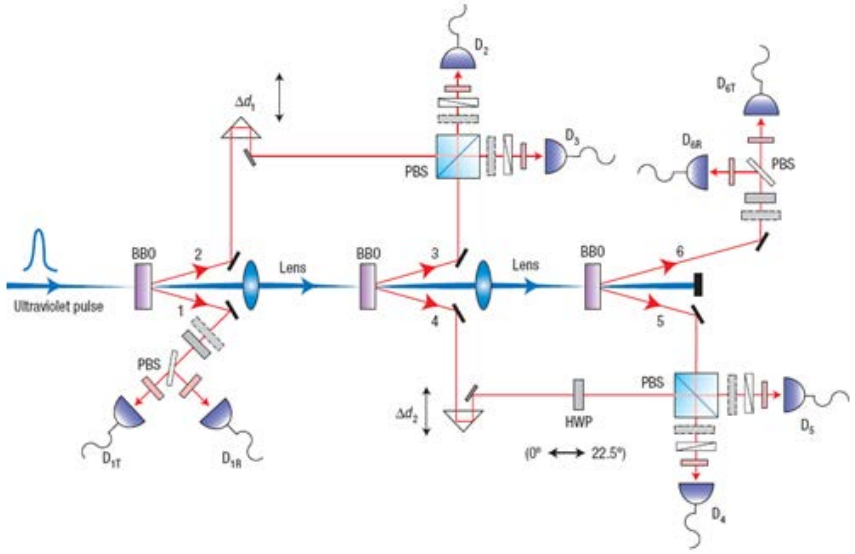
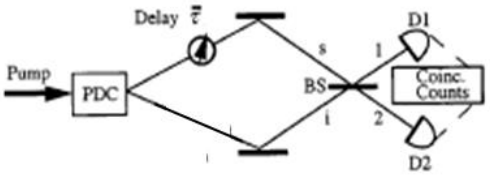


Figure 9. Experimental configuration for the generation of entangled photon cluster states [6].

3.6 Temporally compensated crystal assembly

The outline of this section is as follows: We first describe multi-crystal interference, particularly for type-II SPDC, with key implications for separable quantum states. Next, the significance of group velocity matching (GVM) in such states is discussed. Prototypes of new methods for implementing GVM, designed, and assembled so that initial spectral tests could be performed are discussed. Finally, brief mention is given to how the methods can be generalized to increase control of the SPDC spectral function, to enable applications in regions that have not been accessible with other methods.



Consider amplitudes that yield coincidence counts in the single photon counting detectors (D1,D2); where the events are: a photon with frequency ω_1 *in* $D1$, and a photon with frequency ω_2 *in* $D2$.
Two paths to this event via transmission Tx-Tx OR reflection Rx-Rx are in principle indistinguishable, and exhibit quantum interference by a null in coincidence counts, since the photons always go to same detector.
Note that the high spectral entanglement in frequency yields no distinguishing information to path events.

Figure 10. Hong-Ou-Mandel interferometer single SPDC source.

In an application of photon entanglement it is essential to designate which photon properties (momentum, energy (spectral), polarization, spatial, or temporal etc.) in a given configuration are to be entangled, and to ensure that no others yield information to degrade the desired quality of interference. Quantum interference relies on indistinguishable amplitudes ("Feynman paths") leading to an event. In this case will be photon pair detection in coincidence counting modules. To illustrate consider first the HOMI (Fig. 10) where two photons meet at a beam splitter (BS). If the wave packets of the two photons are coherent with one another, they will always exit the same port of the BS because their probability amplitudes cancel and lead to destructive

interference. Such a simplified single-mode treatment based on a photon's bosonic symmetry is sufficient for conceptual analysis, but not to describe an actual experiment. SPDC photons are far from single mode, even when the pump beam is CW and nearly in a single spectral mode. The photons in SPDC are in fact emitted as wave packets, with finite spectral and temporal bandwidths that can be Fourier transform limited. Each photon can exhibit any spectral value within its envelope. Thus, to explain the HOMI effect with such wave-packets, it must be clear that the spectral properties cannot provide distinguishing information on the Feynman event paths. (Fig. 11)

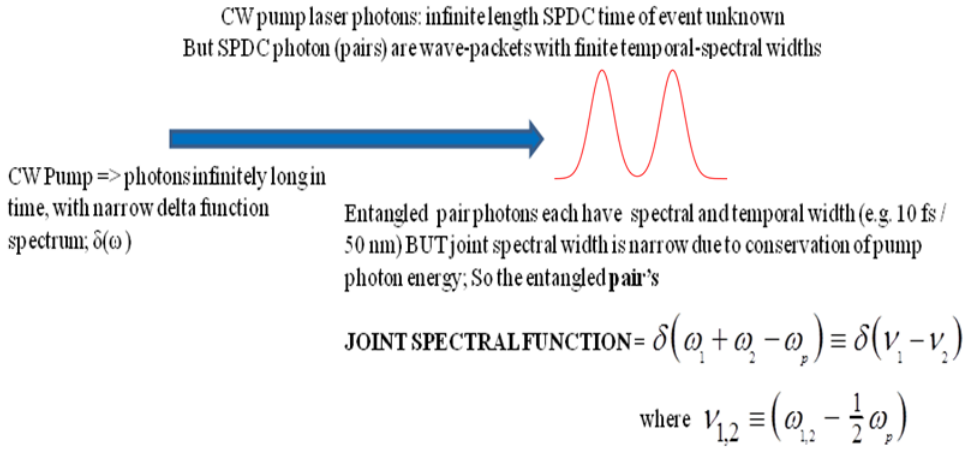
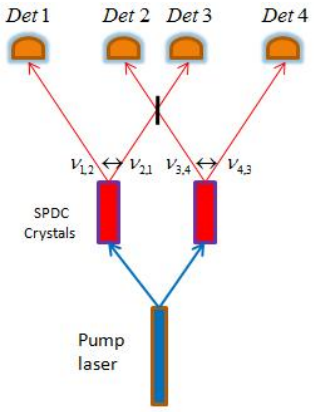


Figure 11. Photon wave-packets generated with CW Pump.

It is emphasized that it is not relevant whether the spectral detections are carried out, it matters only that the measurements could in principle be made; i.e. it is possible events and not actual ones that determine the quantum amplitudes used to calculate (probabilistic) experimental results. Spectrally-resolved single-photon detection is cumbersome and seldom carried out, but it could be done using dispersed arrays of single-photon counters.

We return to the problem of critical interest: how to make use of many independent photon sources, essential to producing more than two entangled photons or two qubits. A possible first step is to replace a CW pump source with short pulses that have a broad spectrum and well defined pair-creation time intervals, which can effectively overlap from many sources. This approach enables, but does not optimize, the process efficiency and purity of quantum interference. An analysis of distinguishing information is required, particularly the photons' spectral state function. To eliminate path distinction, spectral state information regarding one photon state must yield no identifying information regarding the other photon state. This is explicitly shown by Grice [Grice01], when the two-photon state probability distribution is separable into a product state for each photon, i.e. $F(\nu_s, \nu_i) = f(\nu_s)g(\nu_i)$. In that case knowledge of the value of ν_s provides no information on the value of ν_i. This contrasts (Fig. 12) with a CW pump spectral



QUESTION

If photons (ν_1 and ν_2) and (ν_3 and ν_4) are entangled, Can ν_2 and ν_3 be entangled after B.S. as in a HOMI?

New Spectral Function: $\alpha_{pump} = \delta(\nu_1+\nu_2)\delta(\nu_3+\nu_4)$

Problem: In this configuration, the spectral entanglement identifies the source (path) of each photon; such information precludes the quantum path interference.

SOLUTION

A. Eliminate the distinguishing spectral information!
B. Cannot use a CW pump laser; use short pump pulses, having a broad spectrum.
C. Then tailor the source crystal(s) to yield a JOINT SPECTRAL FUNCTION with the required factorizable properties.

$$|\psi\rangle = K\int\int_0^\infty d\nu_s d\nu_i \alpha(\nu_s+\nu_i)\phi(\nu_s,\nu_i)|\nu_s\rangle|\nu_i\rangle$$

Figure 12. Spectral distinguish ability in multi-source entangled photon interference.

function $\delta(\nu_s+\nu_i)$, where knowledge of ν_i determines ν_s exactly; this state is not separable in frequency. Thus, the issue becomes how to generate separable spectral states that can be realized in SPDC. The most direct example would be the product of spectral bandpass filters placed before the detectors, to contribute a spectral response of the form $f(\nu_s)g(\nu_i)$. However this is only realizable in practice if the spectral form contribution of the pump photons and the crystal contributions are neglected since the latter two are, in general, not separable. However if the filters are sufficiently narrowband, their form factor predominates and makes the (separable) Gaussian filter product a good approximation to the experimental distribution.

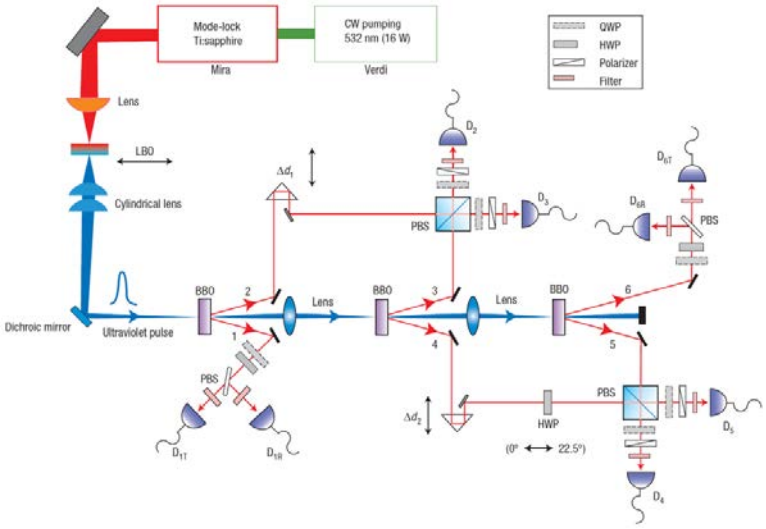


Figure 13. Experimental configuration for the generation of entangled photon cluster states.

This is indeed how nearly every multi-source experiment (Fig. 13) to date has achieved the required separability, sometimes without explicit awareness thereof [Zeilinger05, Pan07]. Unfortunately the vast majority of entangled photons are necessarily discarded in this process. Note: circular symmetry is not related to a separable state. In particular, CIRC ($x^2 + y^2$) is symmetric, but is not factorable.

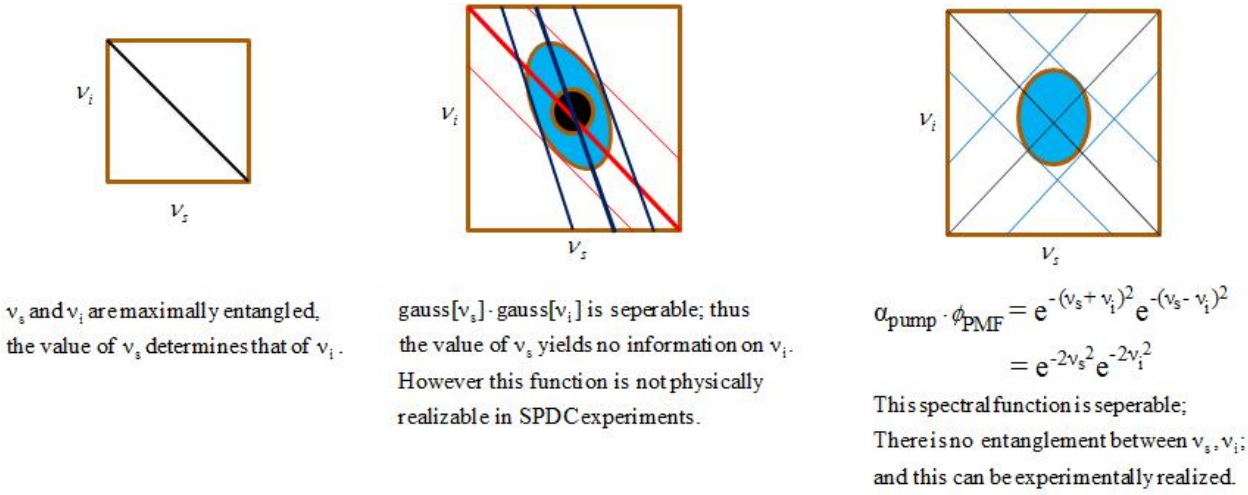


Figure 14. Joint spectral functions for CW pump, and BBO under broadband pump and ideal GVM case.

There is however another way to achieve the desired results without any spectral filtering, and avoid the losses entailed. It was shown in [U'Ren05] that if the crystal spectral function has a particular form then its product with the pump spectral function can become separable, though neither of the two alone meets that condition. A simplified calculation is illustrated (Fig. 14, and Fig. 15).

Gaussian Pulse Pump Function

$$\alpha = e^{-\frac{1}{\sigma}(\nu_i+\nu_s)^2}$$

SPDC Crystal's Phase Matching Function (PMF)

$$j = \mathrm{Sinc}\left[\gamma L^2 \left(\nu_s \cdot (k_p' - k_s') - \nu_i \cdot (k_p' - k_i')\right)\right]$$

Approximate PMF (matching width of Gauss«Sinc)

$$j = e^{-\left[\gamma L^2 \left(\nu_s \cdot (k_p' - k_s') - \nu_i \cdot (k_p' - k_i')\right)\right]}$$

where $k'_{p,s,i}$ are group velocity parameters of crystal for pump, signal, idler photons.

Group Velocity Matched

If we let $k_p' = \frac{1}{2}\left(k_s' + k_i'\right)$

Then $\phi_{GVM} = e^{-K \cdot (\nu_s - \nu_i)^2}$ and the Spectral Function $\alpha \cdot \phi = e^{-q \cdot \nu_s^2} e^{-q \cdot \nu_i^2}$ becomes seperable and symmetric, IF the crystal length L is set such that

$$\frac{1}{\sigma^2} = \frac{1}{4}\left[\gamma L^2 (k_s' - k_i')\right]$$

Figure 15. Joint spectral functions for pump and ideal GVM case.

Rather than the most general case we consider the central one only; the exact group velocity matched case. This means simply that the crystal's dispersive parameters are such that the pump pulse velocity matches that of the (type-II) photon pair's (average) velocity. Several experiments

[Grice01] were able to demonstrate such states with selected nonlinear crystals in the 1.5 um regime. No known crystals enable GVM for applications at ~ 800 nm or shorter wavelengths, where much of the quantum optics work is centered, and where photon detectors exhibit the highest quantum efficiency (>90%) without cryogenic operation. Accordingly, the focus of this work is to demonstrate how GVM crystals at arbitrary wavelength ranges can be "synthesized" by properly combining segments of known crystals. The physical implementation of a GVM matched crystal is described in section 4.6.

3.7 Entangled photon sources

Standard type-I and type-II SPDC crystals are still the leading technology for the production of high mode quality photons used in quantum optics experiments. In these sources entangled photon pairs are emitted as high energy pump photons pass through a nonlinear crystal. Multi-partite states of four or more entangled photons are generated by employing several crystals or multiple passes through a single crystal since typically only one pair is produced per pass. Many groups as well as our in-house are striving to overcome this limitation. Herein will be described our novel, compact multipli-entangled photon source (designated simply as "Schioedtei" henceforth) crystal for type-II SPDC which produces six pairs of photons, surpassing the typical generation of a single pair of entangled photons per pass in conventional SPDC-based sources.

The Schioedtei design is an adaptation of a typical type-II SPDC source. Schioedtei consists of a pair of two type-II non-collinear phase-matched SPDC crystals cut for degenerate down-conversion whose optic axes are rotated orthogonal with respect to one another as in Figure 16.

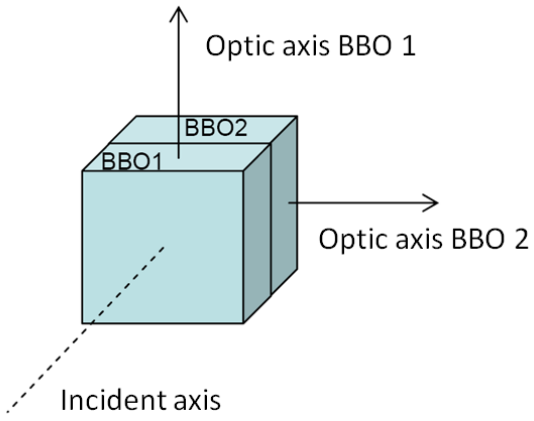


Figure 16. Type-II SPDC Schioedtei crystal assembly.

When the crystal pair is excited with an incident 45° polarized pump beam one pair of rings is produced from each of the type-II crystals. Each pair of rings is orthogonal to the other resulting in 12 intersection points (or simply "points") where indistinguishable photons are produced. Referring to Fig. 17, the indicated points marked 5, 6 and 7, 8 are the typical Bell states, $\left|B\right\rangle_{5,6\,(7,8)} = \frac{1}{\sqrt{2}}\left(\left|HV\right\rangle_{5,6\,(7,8)} \pm \mathrm{e}^{i\varphi}\left|VH\right\rangle_{5,6\,(7,8)}\right)$, with one pair arising from crystal 1, and the second pair produced from crystal 2. The points indicated by 1, 2, 3, 4 are the product of two bell states, $\left|\Psi\right\rangle_{1,2,3,4} = \frac{1}{2}\left(\left|HV\right\rangle_{1,4} + \mathrm{e}^{i\varphi}\left|VH\right\rangle_{1,4}\right)\left(\left|HV\right\rangle_{2,3} + \mathrm{e}^{i\varphi}\left|VH\right\rangle_{2,3}\right)$, produced from independent entangled

photon pairs emerging from crystals 1 and 2 concurrently. Points 9, 11 and 10, 12 are $|VV\rangle_{9,11}$ and $|HH\rangle_{10,12}$ product states produced from photons from crystal 1 and 2 concurrently. The experimental implementation, construction, and results will be described in section 4.7.

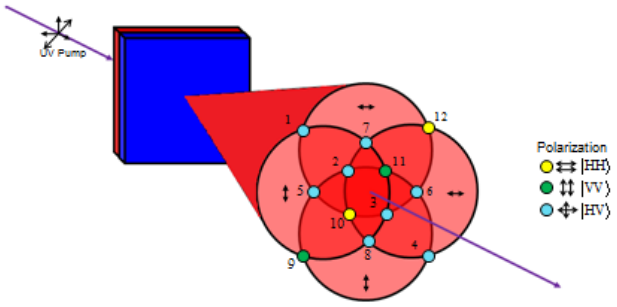


Figure 17. Type-II SPDC Schioedtei source. See text for discussion of the intersection points of the overlapping rings.

4.0 RESULTS AND DISCUSSION

4.1 Grover's quantum search algorithm: simulation

In Fig.18 and Fig. 19 we illustrate the basic utilization of the device GPU compute cores within a parallel MPI code running on the host CPU. In Fig. 20 and Fig. 21 we illustrate how this methodology was employed for a parallel Grover search algorithm (GSA) simulation.

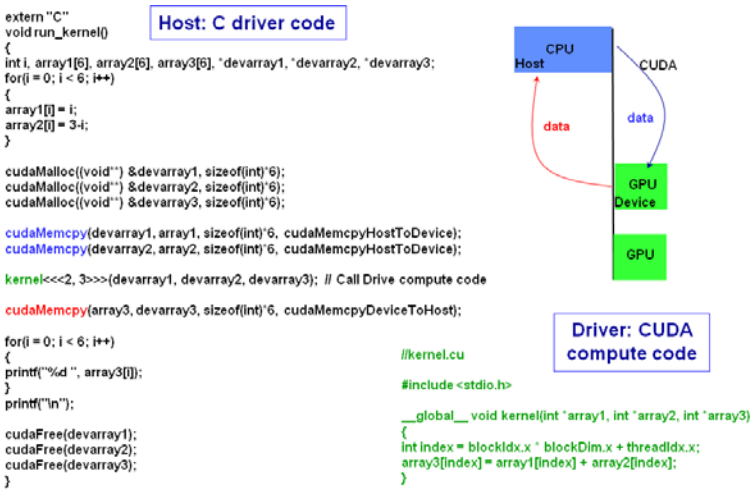


Figure 18. Host C drive code and GPU device compute code.

The example we consider is the addition of two arrays (of length six for purposes of illustration) such that there sum is equal to three for each entry. In Figure 18 the host C code (running on the CPU) creates two arrays *array1* and *array2* with values {0,1,2,3,4,5} and {3,2,1,0,-1,-2}, respectively. Once these arrays are filled, memory for device arrays *devarray1*, *devarray2* and *devarray3* are allocated with the CUDA command *cudaMalloc* (where *devarray3* will hold the

sum of the first two arrays). The command *cudaMemcpy* copies the contents of the host arrays *array1* (*array2*) into the device arrays *devarray1* (*devarray2*) using the directive *cudaMemcpyHostToDevice*. The *kernel* command then calls the device compute code *kernel.cu* running on the GPU. Because our system had two GPUs per CPU, the code kernel<<<2 initiates two invocations of the compute code *kernel.cu*, one on each GPU. Note that *each element* of the arrays array1 and array2 is sent to a single core, where the compute code *kernel.cu* (shown in

Host: MPI wrapper/driver code

```
// mpi.c

#include <mpi.h>

void run_kernel();

int main(int argc, char *argv[])
{
int rank, size;

MPI_Init (&argc, &argv); /* starts MPI */
MPI_Comm_rank (MPI_COMM_WORLD, &rank); /* get current process id */
MPI_Comm_size (MPI_COMM_WORLD, &size); /* get number of processes */

run_kernel(); // Call Host C driver code that will invoke Driver compute code

MPI_Finalize();
return 0;
}
```

Host: MPI output

```
// output
$ mpirun -l -np 10 ./mpicuda
1: 3 3 3 3 3 3
9: 3 3 3 3 3 3
8: 3 3 3 3 3 3
2: 3 3 3 3 3 3
7: 3 3 3 3 3 3
6: 3 3 3 3 3 3
0: 3 3 3 3 3 3
4: 3 3 3 3 3 3
5: 3 3 3 3 3 3
3: 3 3 3 3 3 3
```

Host: MPI/CUDA compilation

```
// compilation with nvcc and mpicc

$ nvcc -c kernel.cu
$ mpicc -o mpicuda mpi.c kernel.o -lcudart  -L /usr/local/cuda/lib  -I/usr/local/cuda/include
```

Figure 19. MPI wrapper/driver code, compilation and output

green in Fig. 18) adds them, and stores them in a *devarray3* (locally named *array3* on the device). That is, there is no sum over the counter *index* in *kernel.cu*. CUDA automatically sends each index of *array1* and *array2* to as many of the (massive number) of device cores on the GPU as are necessary. On each core, operations are performed (here a simple addition) on the single indexed item. This computational methodolgy is in keeping with the spirit of massive multi-core graphics processing for which the GPUs were originally designed. After execution of the device compute code *kernel.cu* the final *cudaMemcpy* copies the contents of *devarray3* back into the host array *array3* this time using the directive *cudaMemcpyDeviceToHost*. The memory for the device arrays is then released.

So far, the code shown in Fig. 18 is serial, running on one CPU. In Fig. 19 we illustrate how this serial code can be embedded in an MPI wrapper to run on many host CPUs. Most of the MPI code simply initiates parallel communication between the set of CPU, by creating the network called MPI_COMM_WORLD, and giving each CPU in the communication network a *rank*, which will be assigned at compilation where the number of processor (CPUs) are stated (*rank*={0,1,…NCPUs-1}). The only non-trivial code portion in Fig. 19 is the command *run_kernel* which executes the serial C code in Fig. 18 separately on each of the NCPU processors. Since there is no parallel communication requested in Fig. 19, the MPI code simply acts as a wrapper for the C-code in Fig. 18, and the output shown (in the upper right hand of the figure) is simply replicated on each processor (the rank is the integer to the left of the ":" and the contents of array3 on each CPU is {3,3,3,3,3,3}). Also shown in Fig. 19 is the joint compilation of the CUDA/MPI code using CUDA compiler *nvcc* and the MPI compiler *mpicc*.

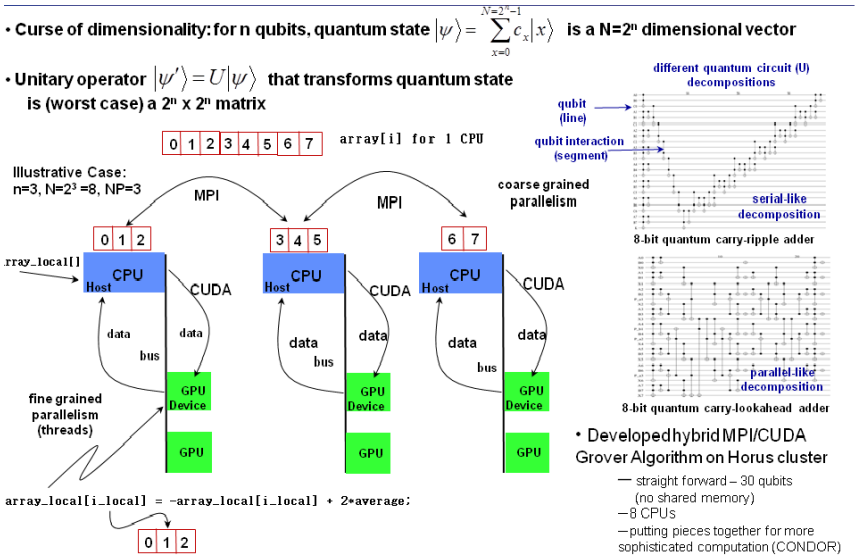


Figure 20. Schematic of hybrid MPI/CUDA parallel simulation.

In Fig. 20 we illustrate the layout of the distributed vector $|\psi\rangle$ of length $N=2^n$ across *Nprocrs* CPUs in an MPI code. As in Section 3.1 we use the simple example of $n=3$ qubits for an $N=8$ bit array, and consider *Nprocrs* =3 CPUs. Each CPU holds *floor*(*N*/*Nprocrs*) elements, with the remaining $R=N-$ *floor*(*N*/*Nprocrs*) < *N* elements being distributed in round robin fashion to the

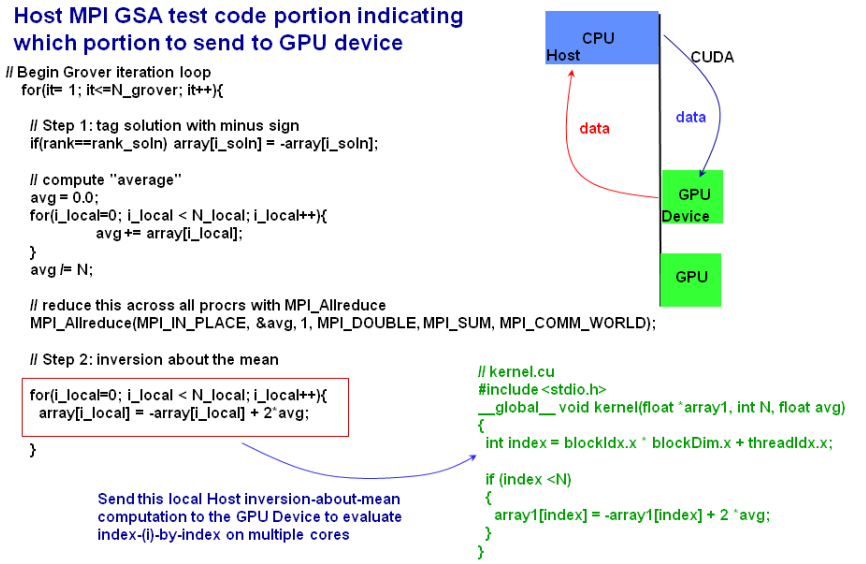


Figure 21. Grover Host C code drive and GPU device compute code.

CPUs with rank 0 thru *R*-1 (here {3,3,2} elements to the three CPUs). The question now arises as to what computation to perform on the host CPUs and what computation warrants the cost of memory copy between the host and device.

The code in the left hand side of Fig. 21 is written purely with MPI in order to perform the U_{inv} unitary of the Grover iterate $G=U_{inv}U_f$. This involves (i) computing the average *avg* of the

quantum amplitudes (the entries of the *array*) and then (ii) performing the inversion about the mean, which sends *array[i_local]* to *–array[i_local] + 2*avg*. Since the full array $|\psi\rangle$ is distributed across all CPUs in the local array *array[*]*, the computation (i) of the average *avg* is best done on the host CPUs using the MPI distributed communication call *MPI_Allreduce*. Each CPU sums all its elements locally and divides the result by the global value N. The MPI call *MPI_Allreduce* with the argument *MPI_SUM*, sums the local values from all the CPUs and then redistributes the result to each processor.

Computation (ii) which uses *avg* computed in (i) to perform the actual inversion about the mean on each local array *array[*]* can be performed index by index. As indicated in the lower right hand corner of Fig. 21, this can be performed on the GPU compute nodes. For each CPU, each array element *array[i_local]* is copied to a core on a GPU where the update *array[i_local]* to *–array[i_local] + 2*avg* is computed, and then returned to the host *array[*]*. In this illustrative example of N=8, the latency cost of copying data between the host CPU and the compute device on the GPU does warrant the small amount of computation performed on the device core. However, for a general GSA calculation with *n* qubits, the array *array[*]* holds on the order of 2^n/*Nprocrs* elements (where *Nprocrs* is the number of CPUs), and the calculation does indeed have high arithmetic intensity, enough to warrant the memory copy latency.

In the numerical studies we performed, we estimated that our local cluster would be able to reach *n=30* qubits, with $N=2^{30} \sim 10^9$ elements. The limiting factor is memory since the addition of every qubit doubles memory storage requirement, so that the addition of 10 more qubits increases the memory requirement by a factor of roughly 10^3. It should be noted that the following represents only the storage of the state vector $|\psi\rangle$ stored in 1-dimensional arrays distributed across all the CPUs. For a quantum computation involving general unitary operations U of size 2^nx2^n the memory requirement are quadratically increased, thereby lowering the effective number of qubits that can be simulated in the quantum computation.

For general quantum computations there is another, more subtle issue to address. As indicated in the right hand side of Fig. 20, the specific decomposition of a general *n*-qubit quantum circuit (a unitary designed to carry out a specific task) into smaller 1-qubit, 2-qubit and 3-qubit operations (which are much easier to implement physically) has a large effect as to whether or not the circuit is amenable to parallel simulation. Each horizontal line represents the time evolution of a qubit. The vertical lines with *k* dots indicate a sub-unitary operation on *k* qubits. Each circuit represents an 8-bit add operation (requiring additional ancilla qubits for intermediate computations). The top diagram represents a decomposition of the circuit as an 8-bit carry-ripple adder. Its V-like horizontal decomposition with only at most two sub-unitary operations per vertical slice forces a serial-like execution. The bottom diagram represents a decomposition of the circuit as an 8-bit carry-lookahead adder. Here, each vertical slice contains many separate sub-unitary operations on different collection of qubits. This latter decomposition is much more amenable to parallel execution. Currently, there is great research interest in the most efficient decomposition of a general *n*-qubit unitary into the fewest number of one, two or three qubit sub-unitary operations. However, the most efficient decomposition may not necessarily be the one most amenable to parallel implementation.

4.2 Grover's quantum search algorithm: theory

General amplitude amplification

It is well known [Boyer96, Kaye07] that the Grover iteration (2) can be extended to the more general case

$$G = U_{\psi^\perp} U_f = A U_{0^\perp} A^\dagger U_f \,, \tag{12}$$

where A is the operator that takes the standard initial state $|0\rangle$ on n qubits to an initial "guess" state, often taken to be the equal amplitude, unbiased state $|\psi\rangle = 1/\sqrt{N}\sum_{x=0}^{N-1}|x\rangle$,

$$A|0\rangle = A\begin{bmatrix}1\\0\\\vdots\\\vdots\\0\end{bmatrix} = \begin{bmatrix}1/\sqrt{N}\\1/\sqrt{N}\\\vdots\\\vdots\\1/\sqrt{N}\end{bmatrix} = |\psi\rangle \quad \Rightarrow \quad A = \begin{bmatrix}\begin{pmatrix}\\|\psi\rangle\\\\\end{pmatrix} & \begin{pmatrix}\\\\\\\end{pmatrix} & \cdots & \begin{pmatrix}\\\\\\\end{pmatrix}\end{bmatrix}. \tag{13}$$

From the left hand side of (13), we see that the initial state $|0\rangle$ picks out the first column of A, which is $|\psi\rangle$. The rest of the columns of A can be chosen arbitrarily, subject only the restriction that A is unitary $AA^\dagger = I_N$, requiring that all columns (and all rows) are mutually orthonormal. Note that in standard Grover iteration (2) $A = H^{\otimes n}$. Further, $A|0\rangle = |\psi\rangle$ ensures that $U_{\psi^\perp} = AU_{0^\perp}A^\dagger = 2|\psi\rangle\langle\psi| - I_N$ is again the inversion about the mean operator (8).

The quantum database state and the subspace phase kickback operation

We developed a quantum database state $|\psi_{db}\rangle$, this time in the quantum circuit model approach in which we explicitly state the unitary evolution operators (vs the AdQC approach, in which the focus is on the constructed Hamiltonians). To describe our approach we again utilize the example of a telephone directory database. We will encode *both* the names and the telephone numbers into quantum states, and illustrate our implementation explicitly with the example utilizing n=2 qubits for the names and n=2 qubits for the telephone numbers, while concurrently developing formulas for an arbitrary number n of qubits. We consider the case of N=2^n (name, telephone number) pairs $\{x_i, t_i\}_{i\in[0,\ldots,N-1]}$. The quantum database state $|\psi_{db}\rangle$ is given by

$$|\psi_{db}\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|x_i\rangle_x \otimes |t_i\rangle_t \,, \tag{14}$$

which is, in general, an entangled state between the name and telephone component states. Note that $|\psi_{db}\rangle$ is an N-dimensional vector in an N^2 dimensional Hilbert space, where the most general state is given by

$$|\Psi\rangle = \frac{1}{\sqrt{N^2}}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} a_{ij}|i\rangle_x \otimes |j\rangle_t \equiv \frac{1}{\sqrt{N^2}}\sum_{k=0}^{N^2-1} b_k |k\rangle_{xt} \in \mathcal{H}_x \otimes \mathcal{H}_t \,, \tag{15}$$

where $\mathcal{H}_x$ and $\mathcal{H}_t$ are the N-dimensional Hilbert spaces of the names and telephone numbers, respectively. In (14) and (15) we use a subscript notation to denote which Hilbert space the ket

belongs $|i\rangle_x \in \mathcal{H}_x, |j\rangle_t \in \mathcal{H}_t$ and $|k\rangle_{xt} \in \mathcal{H}_x \otimes \mathcal{H}_t$. Let us consider the specific example of n=2, N=2^n =4, and utilize the decimal representation of the states (i.e. $\{x_i, t_i\}_{i\in[0,1,2,3]}$). Consider a telephone directory and corresponding database state given by

$$\begin{array}{cc} \text{names} & \text{telephone \#s} \\ 0 & 2 \\ 1 & 3 \\ 2 & 0 \\ 3 & 1 \end{array} \quad \Rightarrow |\psi_{db}\rangle = \frac{1}{\sqrt{4}}\left(|0\rangle_x|2\rangle_t + |1\rangle_x|3\rangle_t + |2\rangle_x|0\rangle_t + |3\rangle_x|1\rangle_t\right) \tag{16}$$

$$= \frac{1}{\sqrt{4}}\left(|2\rangle_{xt} + |7\rangle_{xt} + |8\rangle_{xt} + |13\rangle_{xt}\right), \text{ where } |x_i\rangle_x|t_i\rangle_t \mapsto |Nx_i + t_i\rangle_{xt}.$$

Note, that while we have ordered the names in (16) sequentially, the two lists of names and telephone numbers can in general be chosen as random permutations of the integers [0,1,…,N-1]. Our rationale for constructing the database state $|\psi_{db}\rangle$ is simple. Given the telephone directory (the database) we, as the eventual searcher (database interrogator), can encode this classical information into the quantum state $|\psi_{db}\rangle$ and store it for subsequent interrogation. Suppose at a later time, we select (or are provided with) a random telephone number t^*, and desire to find the associated corresponding name x^*. We can then construct the phase kickback, *telephone number* tagging operator $U_f^{t^*y}$ utilizing the known information of the selected telephone number t^*. For example, if t^*=2, the operator $U_f^{t^*y}$ would have the form given in Fig. 3 (with x now replaced by t^*). Note that $U_{f_{t^*}}^{ty}$ acts on the *ty*-subspace (indicated by the superscript) of telephone numbers t and the auxiliary qubit y, and *not* on the x-subspace of names, on which we are seeking the associated name x^*. Thus, in the full $2N^2$-dimensional Hilbert space of $\mathcal{H}_x^{(N)} \otimes \mathcal{H}_t^{(N)} \otimes \mathcal{H}_y^{(1)}$ (where the superscript denotes the dimension of the Hilbert space) the *telephone number* tagging operator has the following form, and operational PK effect

$$U_{f_{t^*}}^{xty} = I_N^x \otimes U_{f_{t^*}}^{ty} \qquad \text{where} \qquad f_{t^*}(t) = \delta_{t,t^*} = \begin{cases} 1 & t = t^* \\ 0 & t \neq t^* \end{cases},$$

$$I_N^x \otimes U_{f_{t^*}}^{ty}|x\rangle_x \otimes |t\rangle_t \otimes \left(\frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}}\right) = |x\rangle_x \otimes \left\{(-1)^{f_{t^*}(t)}|t\rangle_t \otimes \left(\frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}}\right)\right\} = (-1)^{f_{t^*}(t)}|x\rangle_x \otimes |t\rangle_t \otimes \left(\frac{|0\rangle_y - |1\rangle_y}{\sqrt{2}}\right). \tag{17}$$

Note, that $U_{f_{t^*}}^{ty}$ performs an effective sign flip on states $|x\rangle_x \otimes |t^*\rangle_t$ for *all* values of x. Due to the tensor product nature of the component states, a PK sign flip on $|t^*\rangle_t$ produces an effective PK sign flip on $|x\rangle_x \otimes |t^*\rangle_t$, which includes the sought after state $|x^*\rangle_x \otimes |t^*\rangle_t$. We next describe the construction of the database state and the Grover operator.

Encoding the database into the quantum database state

From (13) we need to construct a unitary operator $A \equiv A^{xt}$ such that $A|0\rangle_x \otimes |0\rangle_t \equiv A|0\rangle_{xt} = |\psi_{db}\rangle_{xt}$.

$$A|0\rangle_x \otimes |0\rangle_t \equiv A|0\rangle_{xt} = |\psi_{db}\rangle_{xt}. \tag{18}$$

This is most easily accomplished if we perform a *relabeling* of the indices of the *xt* component states in the lower, rightmost line of (16) so that we bring them to the first *N* entries of the N^2 database vector, i.e. $|\psi_{db}\rangle = 1/\sqrt{4}\left(|2\rangle_{xt} + |7\rangle_{xt} + |8\rangle_{xt} + |13\rangle_{xt}\right) \rightarrow \quad 1/\sqrt{4}\left(|0'\rangle_{xt} + |1'\rangle_{xt} + |2'\rangle_{xt} + |3'\rangle_{xt}\right) \equiv |\psi'_{db}\rangle$, which we will call the *prime frame*, which we denote by primes on the component values. In the prime frame, the database state has the form $|\psi'_{db}\rangle = 1/\sqrt{4}\,[1,1,1,1,0,\ldots,0]^T$ and we seek a unitary operator A' with the property that $A'|0'\rangle_{xt} = |\psi'_{db}\rangle_{xt}$. Though there is much freedom in choosing such an A', the simplest, most direct (though non-unique) choice that we adopt here, is to choose $A' = H_N \equiv H^{\otimes n}$, the *n*-fold tensor product of 2x2 single quibt Hadamard unitaries. In the prime

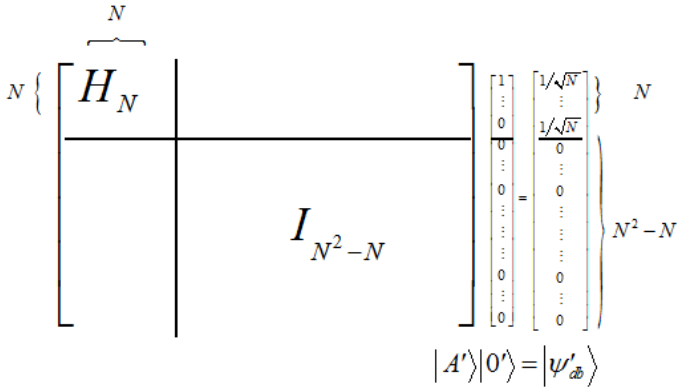


Figure 22. Form of the unitary A' operator, effecting the operation $A'|0'\rangle_{xt} = |\psi'_{db}\rangle_{xt}$, in the *prime index ordering*.

frame A' takes the block diagonal direct sum form,

$$A' = H_N \oplus I_{N^2-N}, \tag{19}$$

(see Fig. 22), in which I_{N^2-N} is the (N^2-N) x (N^2-N) identity matrix acting on those states $|i\rangle_x \otimes |j\rangle_t$ not in $|\psi'_{db}\rangle_{xt}$.

We can transform A' back to the original unprimed frame by a series of N^2 x N^2 unitary operations $S_{i,j} \equiv S^{xt}_{i,j}$ that swaps rows *i* and *j* of any matrix. In our particular example (16) where $|\psi_{db}\rangle = 1/\sqrt{4}\left(|2\rangle_{xt} + |7\rangle_{xt} + |8\rangle_{xt} + |13\rangle_{xt}\right)$ we have

$$\begin{aligned}
|\psi_{db}\rangle &= \frac{1}{\sqrt{4}}\left(|2\rangle_{xt} + |7\rangle_{xt} + |8\rangle_{xt} + |13\rangle_{xt}\right) \equiv \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|k_i\rangle_{xt}; \quad \{k_0,k_1,k_2,k_3\} = \{2,7,8,13\} \\
|\psi'_{db}\rangle &= \frac{1}{\sqrt{4}}\left(|0'\rangle_{xt} + |1'\rangle_{xt} + |2'\rangle_{xt} + |3'\rangle_{xt}\right) \equiv \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i'\rangle_{xt}, \\
\Rightarrow A &= \prod_{i=0}^{N-1} S_{i',k_i} A' = S_{0',2} S_{1',7} S_{2',8} S_{3',13} A', \qquad \left(S_{i,j}\right)_{k,l} = \begin{cases} 1 & (k,l) \in \{(i,j),(j,i)\} \\ 0 & \text{otherwise} \end{cases}
\end{aligned} \tag{20}$$

which is illustrated in Fig. 23. The swap operator $S_{i,j}$ acting on a quantum state vector effectively performs a Pauli bit-flip operation X_2 between the *i*th and *j*th components, and

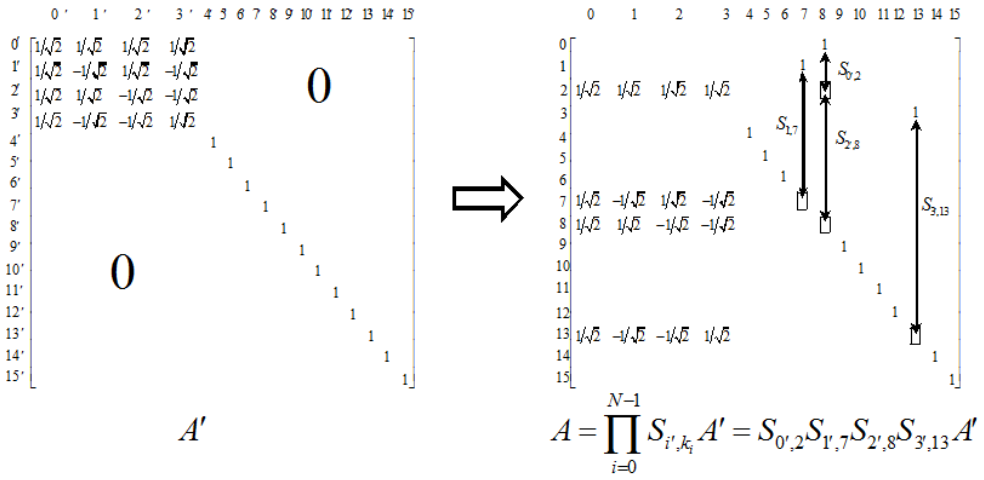


Figure 23. Successive row swapping operations to transform A' in the prime frame to A in the unprimed frame for the specific telephone database example in (20).

therefore, acting on a matrix, $S_{i,j}$ swaps the *i*th and *j*th rows. Note that we perform the row swaps from the prime to the unprimed frame beginning with the largest value of $i' = N$, backwards to smallest value $i' = 0$.

Construction of the Grover iteration

The construction of the Grover iteration is most clearly described in the prime frame (note that in the numerical examples discussed below, the simulations are carried out in the unprimed frame) where it takes the form

$$\begin{aligned} G'^{xt} &= U'^{xt}_{\psi^\perp} U'^{xt}_{f^{t^*}}, \\ &= A'^{xt} U'^{xt}_{0^\perp} A'^{xt\dagger} U'^{xt}_{f^{t^*}}, \\ &= \left(2\left|\psi'_{db}\right\rangle_{xt\ xt}\left\langle\psi'_{db}\right| - I_{N^2}\right)\left(I_N^x \otimes U'^{t}_{f^{t^*}}\right). \end{aligned} \tag{21}$$

Equation (21) is illustrated in Fig. 24 in the prime frame (dropping primes in the figure for visual clarity) acting on $\left|\psi'_{db}\right\rangle_{xt}$.

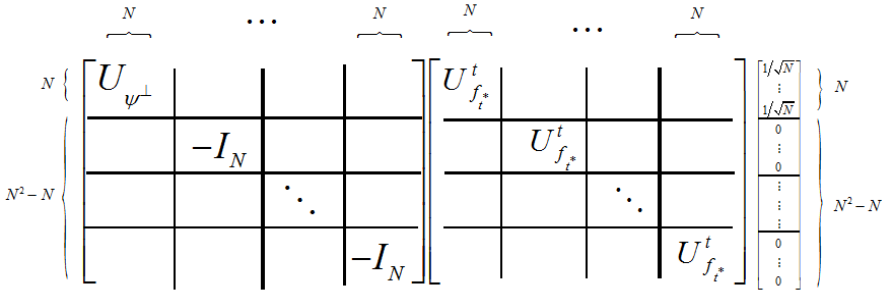


Figure 24. Illustration of the action of the Grover iteration (21) in the primed frame.

Note that in each NxN block $U'^{t}_{f^{t^*}}$ performs a sign flip $U'^{t}_{f^{t^*}}|t\rangle_t = (-1)^{f^{t^*}(t)}|t\rangle_t$ conditioned on the selected telephone number t^*, independent of the value of x. The operator $U'^{(N)}_{\psi^\perp} \equiv 2|\psi'_{db}\rangle_{xt\ xt}\langle\psi'_{db}| - I_N$ (where we have suppressed the subscripts in the figure) performs an inversion about the mean on the N components of $|\psi'_{db}\rangle_{xt}$.

The net effect of (21) is that on the first N components of the primed database state $|\psi'_{db}\rangle_{xt}$, we affect a Grover iteration of the original form in (2). On the later N^2-N components of $|\psi'_{db}\rangle_{xt}$ we perform the operation $|x \neq x^*\rangle_x \otimes |t^*\rangle_t \mapsto -|x \neq x^*\rangle_x \otimes |t^*\rangle_t$ in each N x N block, followed by the multiplication by the N x N identity matrix I_N. However, since the latter N^2-N components of $|\psi'_{db}\rangle_{xt}$ are initially zero (which we will generalize below), they remain zero after the Grover iteration. Thus, after $k \sim \lfloor \pi\sqrt{N}/4 \rfloor$ Grover iterations, the amplitude of the state $|x^*\rangle_x \otimes |t^*\rangle_t$ lying somewhere in the first N (of the N^2) components of $|\psi'_{db}\rangle_{xt}$ will be driven to a magnitude $\sqrt{N-1}/\sqrt{N} \sim O(1)$ with probability $O(1-1/N)$ for detection upon measurement.

Numerical simulations of algorithm

In Fig. 25 we show a simulation for the case of n=3 qubits where a pair of arrays of names and telephones of size N=2^n=8 are chosen as random permutations of [0,1,…,N-1]. In the code, the database state $|\psi_{db}\rangle_{xt} = 1/\sqrt{N}\sum_{k=0}^{N-1}|k\rangle_{xt}$ is constructed in the unprimed frame, and from the specific collection of N indices $\{k\}_{\text{db}}$ in the database state, we construct A in (20) from A', as discussed in (19) and illustrated in Fig. 23. This allows us to construct $U^{xt}_{\psi^\perp}$. We next generate a random telephone number t^* and use it to construct the specific PK telephone tagging operator $U^{xt}_{f^{t^*}}$. Subsequently, we assemble the Grover iteration $G^{xt} = U^{xt}_{\psi^\perp} U^{xt}_{f^{t^*}}$ and apply it for $\lfloor \pi\sqrt{N}/4 \rfloor = 2$. In Fig. 25 note that only N=8 of the total N^2=64 probabilities are non-zero throughout the whole evolution, corresponding to the N=8 non-zero amplitudes of the database state $|\psi_{db}\rangle_{xt}$.

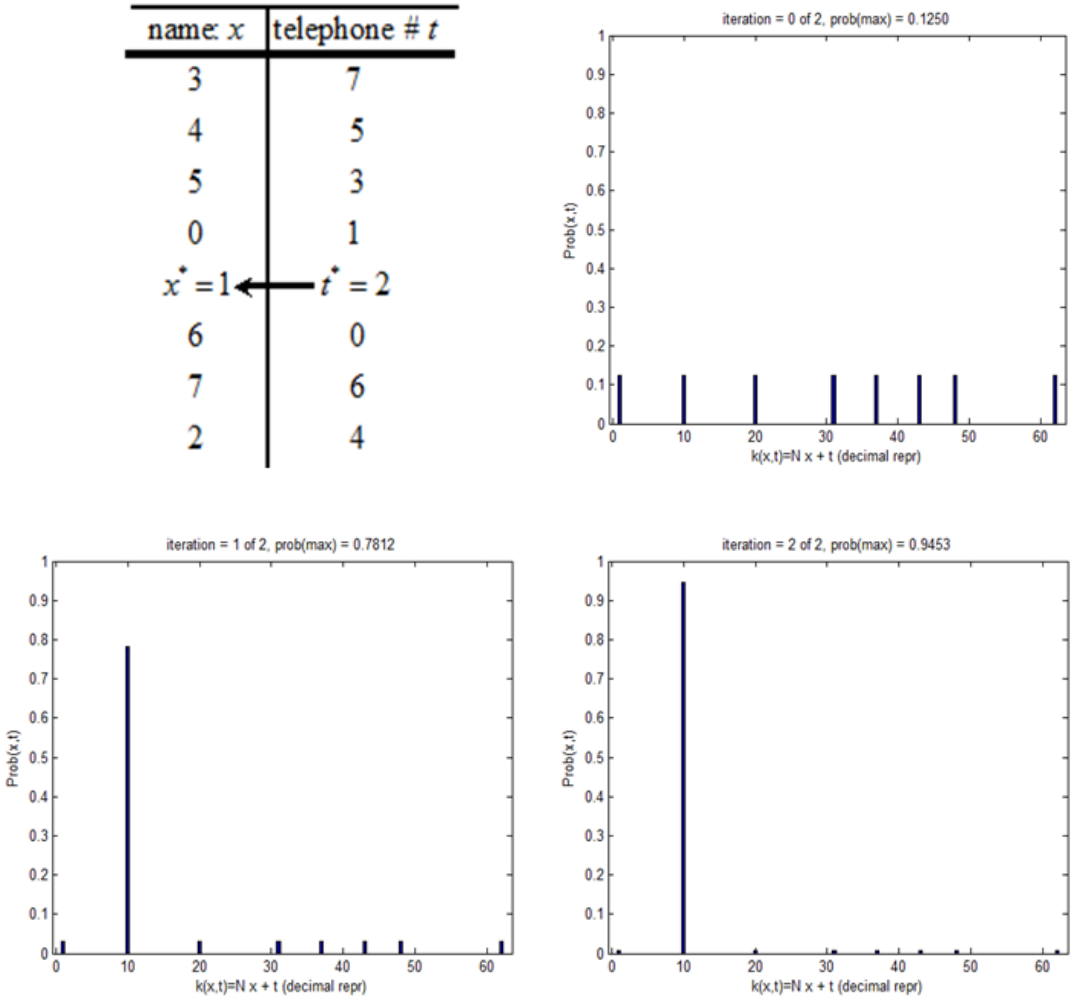


Figure 25. Numerical simulation of Grover iterations (21) for n=3 qubits (N=2^3=8) with a randomly selected telephone number t^*=2 with the initial database state.

Fig. 25 shows a numerical simulation of Grover iterations (21) for n=3 qubits (N=2^3=8) with a randomly selected telephone number t^*=2. The plots (left to right) show the probabilities (amplitude squared) for the $\{0,1,\lfloor \pi\sqrt{N}/4 \rfloor = 2\}$ iterations. The abscissa is the combined xt index k=Nx+t ranging from 0 to N^2-1=63. The Grover iterations act on $|\psi_{db}\rangle_{xt}$ and drive it towards the state $|k^* = 10\rangle = |x^* = 1\rangle_x \otimes |t^* = 2\rangle_t$ with near unit probability. Note that only N=8 of the total N^2=64 probabilities are non-zero throughout the whole evolution, corresponding to the N=8 non-zero amplitudes of the database state $|\psi_{db}\rangle_{xt}$.

Consideration of the initial state

It is illuminating to consider the action of our Grover iteration G^{xt} on initial states $|\psi_{init}\rangle_{xt}$ other than the constructed database state $|\psi_{db}\rangle_{xt}$. In general, the normalized initial state could be written in the form

$$|\psi_{init}\rangle_{xt} = \sqrt{p}\,|\psi_{db}\rangle_{xt} + \sqrt{1-p}\,|\psi_{ndb}\rangle_{xt}, \tag{22}$$

where $|\psi_{ndb}\rangle_{xt}$ denotes a normalized non-database state, i.e. the state formed by all components *not* in the database state $|\psi_{db}\rangle_{xt}$. In (22), $p = |\langle\psi_{db}|\psi_{init}\rangle|^2$ is the probability to find the initial state in the database state. After the $\lfloor \pi\sqrt{N}/4 \rfloor$ of G^{xt} the final state is approximately

$$|\psi_{final}\rangle_{xt} \sim \sqrt{p}\,|x^*\rangle_x |t^*\rangle_t + \sqrt{1-p}\,|\psi_{ndb}\rangle_{xt}, \tag{23}$$

which implies there is only a probability p to detect the sought after solution state $|x^*\rangle_x |t^*\rangle_t$. Thus, as long as p≥1/2, the form of the GSA presented here does better than its classical $O(N/2)$ exhaustive search.

The initial state (22) might occur as an imperfect attempt to construct the desired database state $|\psi_{db}\rangle_{xt}$. A simpler state to form is $|\psi_{N^2}\rangle_{xt} \equiv 1/\sqrt{N^2}\sum_{k=0}^{N^2-1}|k\rangle_{xt} = H_x^{\otimes n} \otimes H_t^{\otimes n}|0\rangle_x \otimes |0\rangle_t$, the N^2 equal

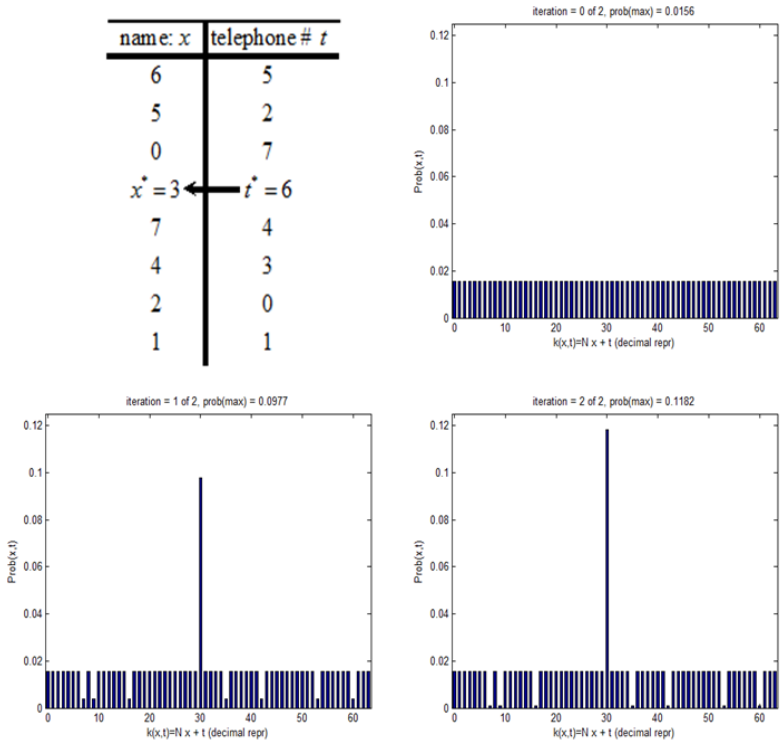


Figure 26. Numerical simulation of Grover iteration (21) for n=3 qubits (N=2^3=8) with a randomly selected telephone number t^*=6 with the unbiased N^2 initial state.

amplitude state, since the last equality shows that we can form this state directly by the application of 2n-fold tensor product of Hadamards $H_x^{\otimes n} \otimes H_t^{\otimes n}$ acting on the tensor product of the n-qubit standard name-state $|0\rangle_x$ and the n-qubit standard telephone-state $|0\rangle_t$. However, from (22) and (23) such an initial state renders the GSA worse than classical exhaustive search since there are N^2-N non-database states each with probability $1/\sqrt{N^2}$ that are unchanged by the Grover iteration G^{xt} for a total probability for the detection of $|\psi_{ndb}\rangle_{xt}$ upon measurement given by 1-1/N. The initial probability of p=1/N to find $|\psi_{N^2}\rangle_{xt}$ in the state $|\psi_{db}\rangle_{xt}$ remains the final probability to find $|\psi_{final}\rangle_{xt}$ in the solution state $|x^*\rangle_x |t^*\rangle_t$. Figure 26 illustrates though that G^{xt} does act only on the N-component state $|\psi_{db}\rangle_{xt}$ buried within N^2 sized initial state $|\psi_{N^2}\rangle_{xt}$.

Fig. 26 shows the numerical simulation of Grover iteration (21) for n=3 qubits (N=2^3=8) with a randomly selected telephone number t^*=6 with initial state $|\psi_{init}\rangle = |\psi_{N^2}\rangle_{xt} \equiv 1/\sqrt{N^2} \sum_{k=0}^{N^2-1} |k\rangle_{xt}$. The plots (left to right) show the probabilities (amplitude squared) for the $\{0,1,\lfloor \pi\sqrt{N}/4 \rfloor = 2\}$ iterations. The abscissa is the combined xt index k=Nx+t ranging from 0 to N2-1=63. The Grover iterations act upon the $|\psi_{db}\rangle_{xt}$ portion of $|\psi_{init}\rangle_{xt} = \sqrt{p}\,|\psi_{db}\rangle_{xt} + \sqrt{1-p}\,|\psi_{ndb}\rangle_{xt}$ where $p = 1/\sqrt{N^2} = 1/N$, and drives it towards the state $|k^* = 30\rangle = |x^* = 3\rangle_x \otimes |t^* = 6\rangle_t$ with probability p=1/8. Note that all N2=64 probabilities are non-zero throughout the whole evolution, but only the N=8 amplitudes of the database state $|\psi_{db}\rangle_{xt}$ are acted upon by Gxt (compare with Fig. 17). Because the amplitudes in $|\psi_{ndb}\rangle_{xt}$ are unchanged by Gxt using the initial state, $|\psi_{init}\rangle = |\psi_{N^2}\rangle_{xt}$ yields inferior performance when compared to classical exhaustive search. Eq.(22) and Eq.(23) argue that one should use p as close to 1 as possible, i.e. the initial state should be as close to $|\psi_{db}\rangle_{xt}$ as is physical realizable.

4.3 CNOT gate in PTR glass: simulation

In our research we considered both multiplexed and stacked volume holograms configurations for constructing quantum gates. In [Miller11b] we detailed the use of multiplexing to simulate quantum teleportation. One alternative to multiplexing is to make single recordings in each of many holograms, and then stack the holograms. In this report, we provide here our design of a quantum CNOT gate compatible with PTR glass. This gate is realized by stacking four

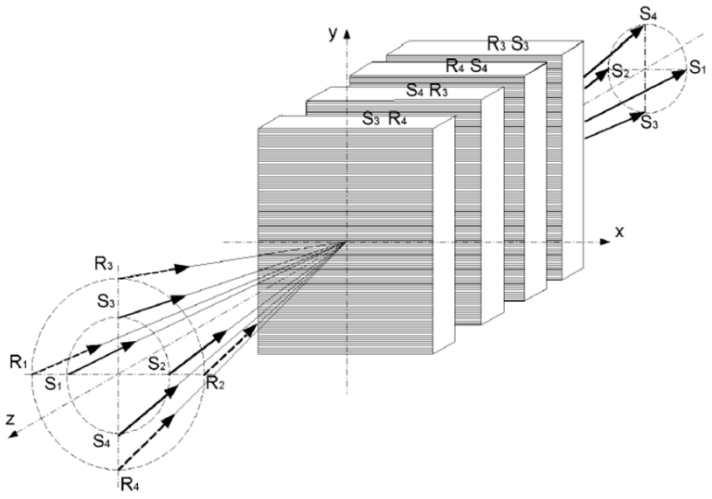


Figure 27. Volume holographic design of 4-dimensional CNOT gate in PTR glass.

holograms, which we describe below. The CNOT gate is a two qubit gate. Therefore the dimension of the state space is 4-dimensional. While this state space can be constructed as a product space of qubits by utilizing the polarization states of two correlated photons, it can also be represented by a single LM photon in a 4-dimensional state space. The CNOT gate can be constructed with a single photon. Following the arguments in Section 3.3, we freely choose four independent plane waves lying on the cone shown in Fig. 27 above.

We associate to these independent transverse LM modes the four orthogonal quantum state vectors $|S_1\rangle$, $|S_2\rangle$, $|S_3\rangle$ and $|S_4\rangle$. Any quantum state vector $|\psi\rangle$, in this 4-dimensional state space can be written as a linear superposition of these states,

$$|\psi\rangle = \alpha|S_1\rangle + \beta|S_2\rangle + \gamma|S_3\rangle + \delta|S_4\rangle, \qquad |\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1. \tag{24}$$

Each of our basis states can be expressed in matrix notation,

$$|S_1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |S_2\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |S_3\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \text{ and } |S_4\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \tag{25}$$

In this computational basis the CNOT gate can be expressed by the following unitary transformation

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{26}$$

If we let the *z*-axis be orthogonal to the face (*x*-*y* plane) of the hologram, the four volume holographic gratings are recorded by a suitable superposition of the set of four signal plane waves,

$$\langle \vec{r} | S_1 \rangle = \exp(i\vec{k}_1 \cdot \vec{r}),\ \langle \vec{r} | S_2 \rangle = \exp(i\vec{k}_2 \cdot \vec{r}),\ \langle \vec{r} | S_3 \rangle = \exp(i\vec{k}_3 \cdot \vec{r}),\ \langle \vec{r} | S_4 \rangle = \exp(i\vec{k}_4 \cdot \vec{r}), \tag{27}$$

and four reference waves

$$\langle \vec{r} | R_1 \rangle = \exp(i\vec{\kappa}_1 \cdot \vec{r}),\ \langle \vec{r} | R_2 \rangle = \exp(i\vec{\kappa}_2 \cdot \vec{r}),\ \langle \vec{r} | R_3 \rangle = \exp(i\vec{\kappa}_3 \cdot \vec{r}),\ \langle \vec{r} | R_4 \rangle = \exp(i\vec{\kappa}_4 \cdot \vec{r}), \tag{28}$$

as shown in Fig. 27.

The hologram is recorded so that each row of the unitary matrix of the CNOT gate is used to generate its own volume holographic grating. For a 2-qubit gate such as the CNOT gate we would ordinarily require four recordings; however, since the first two bits are just an identity matrix we need only two layers to transform the signal states into the desired reference states. In addition to one holographic recording per dimension of the state space, we also require the conjugate of each grating (two in the case of the CNOT gate) in order to transform the diffracted reference waves from the reference waves back into the desired signal states. In particular, the CNOT-gate constructed from four holographic gratings stacked together as is shown in Fig 27:

1. The first grating is recorded with the two coherent plane waves corresponding to states $|S_3\rangle$ and $|R_4\rangle$.
2. The second grating is recorded with the two coherent plane waves corresponding to states $|S_4\rangle$ and $|R_3\rangle$
3. The second grating is recorded with the two coherent plane waves corresponding to states $|R_4\rangle$ and $|S_4\rangle$
4. The second grating is recorded with the two coherent plane waves corresponding to states $|R_3\rangle$ and $|S_3\rangle$.

The four gates will not diffract the first two signal states $|S_1\rangle$ or $|S_2\rangle$. However, the first two gratings redirect the two signal states $|S_3\rangle$ and $|S_4\rangle$ into $|R_3\rangle$ and $|R_4\rangle$ respectively, in accordance with the Pauli X-gate,

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{29}$$

The first hologram is equivalent to the operator,

$$\hat{U}_1 = |S_1\rangle\langle S_1| + |S_2\rangle\langle S_2| + |R_4\rangle\langle S_3| + |S_4\rangle\langle S_4|, \tag{30}$$

and the second hologram recorded with the signal plane wave $\langle \vec{r} | R_4 \rangle$ is equivalent to the operator,

$$\hat{U}_2 = |S_1\rangle\langle S_1| + |S_2\rangle\langle S_2| + |R_4\rangle\langle R_4| + |R_3\rangle\langle S_4|. \tag{31}$$

While these two recordings could have been made in a single multiplexed hologram, we recover the same function by stacking the two together, thereby generating the CNOT operation,

$$\hat{U}'_{CNOT} = \hat{U}_2\hat{U}_1 = |S_1\rangle\langle S_1| + |S_2\rangle\langle S_2| + |R_3\rangle\langle S_4| + |R_4\rangle\langle S_3|. \tag{32}$$

However, the output of these two stacked holograms are the reference states $|R_1\rangle$, $|R_2\rangle$, $|R_3\rangle$, $|R_4\rangle$. In order to redirect these back to the proper signal states, we require the redirection operator similar to Eq. (11). This can be accomplished by recording a third hologram with the states $|R_3\rangle$ and $|S_3\rangle$. The third hologram is equivalent to the operator,

$$\hat{U}_3 = |S_1\rangle\langle S_1| + |S_2\rangle\langle S_2| + |S_3\rangle\langle R_3| + |R_4\rangle\langle R_4|. \tag{33}$$

Similarily, the fourth hologram is recorded with the states $|R_4\rangle$ and $|S_4\rangle$ and is equivalent to the operator,

$$\hat{U}_4 = |S_1\rangle\langle S_1| + |S_2\rangle\langle S_2| + |S_3\rangle\langle S_3| + |S_4\rangle\langle R_4|. \tag{34}$$

Therefore, the combination of the four stacked volume holograms has the desired action -- the CNOT gate,

$$\hat{U}_{CNOT} = \left(\hat{U}_4\hat{U}_3\right)\left(\hat{U}_2\hat{U}_1\right) = |S_1\rangle\langle S_1| + |S_2\rangle\langle S_2| + |S_4\rangle\langle S_3| + |S_3\rangle\langle S_4|. \tag{35}$$

One can apply these principles to design a universal set of quantum gates, as well as simple quantum algorithms such as QT.

The advantage of stacking the holograms is that one can make the hologram thicker, thereby increasing the efficiency; however, achieving and maintaining the proper alignment should be

more problematic. By multiplexing, we would need two holograms, each with two independent recordings in them. The first would be equivalent to the last two holograms in Fig. 27, while the second would be equivalent to the first two and would just redirect the reference beams into their corresponding signal states. The first two recordings are complementary to the second two -- thus in some sense we are recording the "square root" of the CNOT gate.

4.4 Entangled Bell state evolution with topological protection: simulation

In this section we discuss the simulation results of the creation of an entangled Bell state in a 2D cluster state (CS) and its evolution under random depolarized noise errors while undergoing error correction. The end result is that cluster states offer a threshold for Bell state creation/evolution that increases with the 2D lattice size in which it is encoded. The error threshold rates found, 0.052 for a lattice of edge length l=13 and 0.083 for l=29, are significantly higher than the severe 10^{-4} (at best 10^{-3}) single qubit error threshold rates encountered in the usual quantum circuit model. This is an indication of the topological protection resulting from the use of cluster states and measurement based quantum computation. The details of the Bell state creation and error

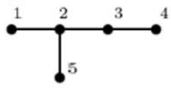
Graph representation	Wavefunction representation	Stabilizer generators
(a) 	$\|\mathcal{G}_a\rangle = CZ_2^1\|++\rangle$ $= (1/\sqrt{2})(\|0+\rangle + \|1-\rangle)$	X_1Z_2, X_2Z_1
(b) 	$\|\mathcal{G}_b\rangle = CZ_2^1CZ_3^2CZ_4^3\|++++\rangle$ $= (1/\sqrt{2})(\|+00+\rangle + \|+01-\rangle$ $\|-10+\rangle + \|-11-\rangle)$	X_1Z_2, $X_2Z_1Z_3$, $X_3Z_2Z_4$, X_4Z_3
(c) 	$\|\mathcal{G}_c\rangle = CZ_2^1CZ_3^2CZ_5^2CZ_4^3\|+++++\rangle$ $= (1/\sqrt{2})(\|+00++\rangle + \|+01-+\rangle$ $+\|-10+-\rangle + \|-11--\rangle)$	X_1Z_2, $X_2Z_1Z_3Z_5$, $X_3Z_2Z_4$, X_4Z_3, X_5Z_2

Figure 28. Simple cluster states, their 1D wavefuntion representations and stabilizer generators.

correction in a 2D and 3D are quite involved. For clarity we illustrate the concepts in the more simple 1D cluster state lattices. It should be recalled that 1D clusters state are not universal for quantum computation, hence our studies took place on 2D and 3D lattices.

Consider the simplest CS, the 1D chain in Fig. 28a consisting of vertices i=1 and j=2 connected by an edge. The preparation of the CS is as follows: each vertex (black dot) represents a qubit-i prepared in the state $|+\rangle_i = (|0\rangle_i + |1\rangle_i)/\sqrt{2}$, the +1 eigenstate of the operator X_i. The edge (black line) represents the Control-Z operation CZ_j^i acting between the qubits i and j. The operator CZ_j^i is a diagonal matrix with entries $\{1,1,1,-1\}$, with rows and columns labeled by the computational

basis states $\{|00\rangle_{ij}, |01\rangle_{ij}, |10\rangle_{ij}, |11\rangle_{ij}\}$, i.e. $CZ_j^i|11\rangle_{ij} = -|11\rangle_{ij}$, while the other three states are unchanged. The cluster $|G_a\rangle$ state in Fig. 28a then given by $|G_a\rangle = CZ_2^1|{+}{+}\rangle_{12} = (|0+\rangle_{12} + |1-\rangle_{12})/\sqrt{2}$, which is easily verified using $|{+}{+}\rangle_{12} = (|00\rangle_{12} + |01\rangle_{12} + |10\rangle_{12} + |11\rangle_{12})/2$, applying $CZ_j^i|11\rangle_{ij} = -|11\rangle_{ij}$ and regrouping terms.

An alternative method called the *stabilizer formalism* (Gottesman97, Nielsen00) more simply defines this state than the above procedure of writing out all (in general 2^n for n qubits) wavefunction components. Using the results $X_i|\pm\rangle_i \equiv X_i(|0\rangle_i \pm |1\rangle_i)/\sqrt{2} = \pm|\pm\rangle_i$, $Z_i|0\rangle_i = |0\rangle_i$ and $Z_i|1\rangle_i = -|1\rangle_i$ it is easy to verify that the state $|G_a\rangle = CZ_2^1|{+}{+}\rangle_{12}$ is the (unique) +1 eigenstate of the operators $\{X_1Z_2, Z_1X_2\}$ (first row, third column of Fig. 28a). These operators are called the *stabilizer generators* of the state $|G_a\rangle$ in that all products of these generators also stabilize $|G_a\rangle$, i.e. return a +1 eigenvalue.

Row (b) of Fig. 28 depicts a 4-qubit CS chain $|G_b\rangle$ created by putting each qubit in the state $|+\rangle_i$ and acting with CZ_{i+1}^i gates between adjacent pairs. Since each CZ gate is diagonal, they all commute, so this operation can be done in parallel – a significant feature of OWQC (or CSQC). The 4-qubit linear chain $|G_b\rangle = CZ_2^1CZ_3^2CZ_4^3|{+}{+}{+}{+}\rangle_{1234}$ is stabilized by the generators (given in the third column) $\{X_1Z_2, Z_1X_2Z_3, Z_2X_3Z_4, Z_3X_4\}$. In general, i.e. not just in 1D, the CS $|G\rangle$ is stabilized by all generators of the form $S_i = X_i\prod_{j\in N_G(i)} Z_j$ where the index i runs over all vertices (qubits) in the graph G and NG(i) represents the *neighborhood of vertex i*, i.e. all vertices connected to vertex i by an edge. The cluster state $|G\rangle$ is then the unique +1 eigenstate of all products of the generators $\{S_i\}$.

We illustrate the construction of a maximally entangled Bell state in a 3-qubit 1D-chain $|G_3\rangle \equiv CZ_2^1CZ_3^2|{+}{+}{+}\rangle_{123} = |0\rangle_2(|00\rangle_{13} + |00\rangle_{13} + |00\rangle_{13} + |00\rangle_{13})/2 + |1\rangle_2(|00\rangle_{13} - |00\rangle_{13} - |00\rangle_{13} + |00\rangle_{13})/2$, where the last equality follows from expanding out $|G_3\rangle$ and factoring out the states $|0\rangle_2$ and $|1\rangle_2$ to the far left. Let us now make a measurement of qubit-2 in the X-basis. When qubit-2 returns a value of ±1, the state $|G_3\rangle$ is projected into the $|\pm\rangle_2$, which we denote as $|G_3\rangle \mapsto |\pm\rangle_2\,{}_2\langle\pm|G_3\rangle$. Projection onto the +1 eigenstate of X_2 returns the state $|+\rangle_2(|00\rangle_{13} + |11\rangle_{13})/\sqrt{2}$ which is the symmetric maximally entangled Bell state $|\beta_{00}\rangle_{13} = (|00\rangle_{13} + |11\rangle_{13})/\sqrt{2}$ on qubits 1 and 3. Projection onto the -1 eigenstate of X_2 returns

$|-\rangle_2 (|01\rangle_{13} + |10\rangle_{13})/\sqrt{2}$, which is a different maximally entangled Bell state on qubits 1 and 3, that can be converted into the previous one, by the application of the operator X_1 (the application of the last operator X_1 is termed *modulo local Pauli corrections*). The result is general for one-dimensional CS chains of *n*-qubits. That is, the measurement of qubits *i*=2 to *i*=n-1 in the *X*-basis returns the symmetric maximally entangled Bell state $|\beta_{00}\rangle_{1n} = (|00\rangle_{1n} + |11\rangle_{1n})/\sqrt{2}$, modulo local Pauli corrections.

We now briefly consider the issue of quantum error correction (QEC) in terms of the stabilizer formalism (for which it was originally intended, see Gottesman97). Suppose we use repetition coding to encode single qubit states into logical states composed of 3-qubits $|0\rangle \mapsto |0\rangle_L \equiv |000\rangle$ and $|1\rangle \mapsto |1\rangle_L \equiv |111\rangle$. A general logical qubit $|\psi\rangle_L = a|0\rangle_L + b|1\rangle_L = a|000\rangle + b|111\rangle$ is stabilized by generators $\{Z_1Z_2, Z_2Z_3\}$. Suppose errors occur as single bit-flips X_i. Consider for example the action of a bit-flip error on the first qubit $|\psi\rangle_L \mapsto X_1|\psi\rangle_L = a|100\rangle + b|011\rangle$. A measurement of the generators on corrupted state $X_1|\psi\rangle_L$ now yields $\{Z_1Z_2, Z_2Z_3\}X_1|\psi\rangle_L = \{-1,+1\}|\psi\rangle_L$. This is called a *syndrome* measurement. Instead of the generators acting on the state, we can find the result of the syndrome by transforming the generators by the general unitary error operator *U* as $U\{Z_1Z_2, Z_2Z_3\}U^\dagger$ (note that $X^\dagger = X$, $Z^\dagger = Z$). Using the result that *XZX*=-*Z* (*ZXZ*=-*X*) and that operators for different qubits commute, we have $X_1\{Z_1Z_2, Z_2Z_3\}X_1 = \{-Z_1Z_2, Z_2Z_3\}$, which again returns $\{-1,+1\}|\psi\rangle_L$ when acting on the corrupted state $X_1|\psi\rangle_L$. In a similar manner we find that a bit flip on the second qubit yields the syndrome $X_2\{Z_1Z_2, Z_2Z_3\}X_2 = \{-Z_1Z_2, -Z_2Z_3\}$, while a bit flip on the third qubit yields the syndrome $X_3\{Z_1Z_2, Z_2Z_3\}X_3 = \{Z_1Z_2, -Z_2Z_3\}$. Of course, the absence of any bit flip error yields $I\{Z_1Z_2, Z_2Z_3\}I = \{Z_1Z_2, Z_2Z_3\}$. Collecting these results, we see in Fig. 29 that the syndrome measurements of the generators of logical qubit $|\psi\rangle_L$ give us

Z_1 Z_2	Z_2 Z_3	Error Type	Corrective Action
+1	+1	no error	no action
-1	+1	bit 1 flipped	flip bit 1 with X_1
-1	-1	bit 2 flipped	flip bit 2 with X_2
+1	-1	bit 3 flipped	flip bit 3 with X_3

Figure 29. Error correction for 3-qubit bit flip code in stabilizer formalism.

a unique signature of which bit was flipped, and what corrective action needs to be performed. Although, this example is fairly simple, it demonstrates the utility of tracking single qubit errors

(the most common error model) on a state in terms of the measurements of the stabilizer of the state. This is particularly important in the general case of *n*-qubit quantum states where the number of stabilizers (to keep track of) scales polynomially as $O(n^2)$, whereas the number quantum amplitudes scales exponentially as $O(2^n)$ [Nielsen00, Campbell09].

We now extend these concepts to a 3D cluster state in the form of rectangular grid and single out the first spatial direction on the cluster as a "simulated time." We consider a perpendicular 2D slice of this cluster into which we encode a logical symmetric Bell state in what is called a *surface code* [Bravyi05]. The qubits in the cluster state are subdivided into code and syndrome qubits. Measurement of the syndrome qubits in the X- basis projects the code qubits into a surface code state. In a 3D cluster consisting of many linked 2D slices, measurement of the code qubits results in teleportation of the encoded state from one slice to the next (plus local Hadamard gates), and measurement of the syndrome qubits amounts to measurement of the surface code stabilizer [Briegel08].

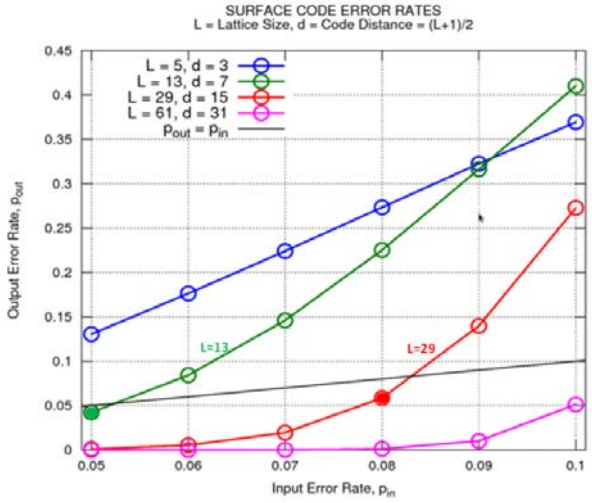


Figure 30. Error rates for the encode Bell state in 3D lattice of size *dx(2d+1)x(2d+1)*.

The simulation results are illustrated in Fig. 30. In the simulation, we have assumed a depolarized noise (DPN) model in which an error is applied with probability p_{in}, yielding an output error with probability p_{out} for the state to be prepared in the Bell state. Fig. 30 illustrates the relationship between the input error rate and the output error rate of a Bell state creation using surface codes for varying lattice sizes. The results are obtained from a Monte-Carlo simulation that uses a DPN channel. In other words, the probabilities of applying a non-ideal Pauli error are all the same and equal to $p_{in}/3$, where the 3 in the denominator refers to X-, Y -, and Z-errors. As is the case with surface codes, the greater the lattice dimension, l (denoted as L in Fig. 30), the higher the distance of the code, d (where a code with distance at least $d=2t+1$ can correct errors on t bits). Specifically, the code distance is directly related to the lattice size by $d = (l+1)/2$. Without including the cost of overhead, codes with higher distances are always more desirable as they relate directly to the number of errors that a code can tolerate without failure.

Figure 30 shows the fidelity curves for logical Bell state preparation in the surface codes with dimensions l of 5, 13, 29, and 61. The black line represents the fault-tolerant threshold line, where the input error rate is equal to the output error rate. Regions of the curves below the threshold line indicate regions where we can perform quantum computations (in this case, create logical Bell states) with asymptotically arbitrary small error using concatenation encoding or larger lattice dimension. In the context of surface codes, lower output error rates p_{out} are achieved via larger lattices as opposed to concatenation. Ideally, the fault tolerant threshold pertains to the ideal, infinite size lattice for which the output error p_{out} is zero for input error p_{in} below threshold, and one for input error above threshold. As particular examples, the simulation results show that the threshold for the Bell pair creation is about 0.052 for the code with lattice size l = 13 (solid green circle in Fig. 30) and 0.083 for the surface code with lattice size l = 29 (solid red circle in Fig. 30). These threshold rates of approximately 5% and 8% are typically an order of magnitude higher than the most promising threshold rates obtained using the standard quantum circuit model.

4.5 Quantum information science testbed

Validation of the testbed was a twofold process, generate entangled photons and analyze the quality of the photons that were produced. The former comprised of exciting the crystal with a pump beam and visualizing the output photon with a single photon CCD camera. The latter was accomplished with a set of measurements that allowed us to map the state of the photon system, called quantum state tomography.

Consider the generation of the entangled photons via SPDC. In the first row of Fig. 31 we show the results of sending the CW laser through the two-crystal down-converter. For this type-I SPDC source there were two concentric rings of orthogonal polarization. Both rings correspond to photons that have the same wavelength of 810 nm with a bandwidth of 10 nm. This was selected by a band-pass filter located in front of the camera. Other filters also placed in front of the camera stopped the part of the pump beam that did not created down-converted light. Each of the rings was generated by one of the crystals of the two-crystal stack. The diameter of each ring (cone) was controlled by the tilt of the corresponding crystal that generated it. The tilt axes of the crystals were orthogonal to each other, and were contained in a plane perpendicular to the input beam axis. This configuration allowed the diameter of the horizontally polarized ring to be controlled by tilt of the crystal about a horizontal axis, and the diameter of the vertically polarized ring by a tilt about the vertical axis.

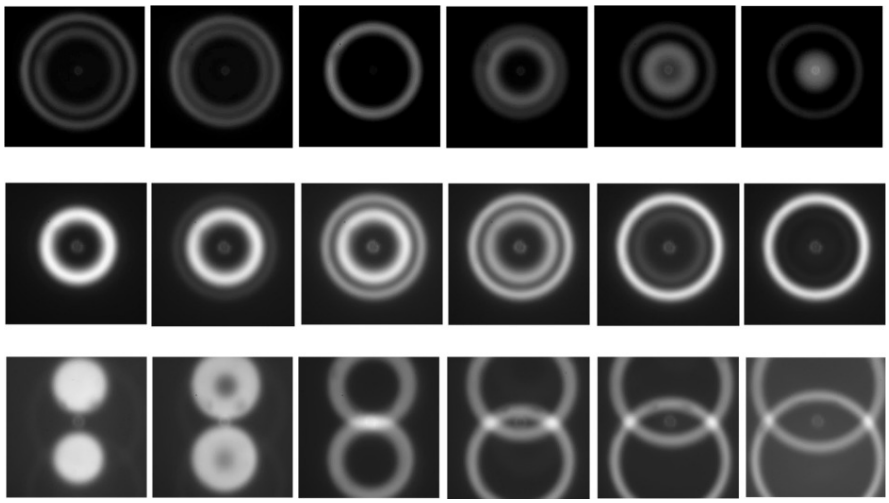


Figure 31: Imaging of the down-converted light for three different configurations. First row: type-I SPDC as a function of the tilt of one crystal. Second row: type-I SPDC rings of different diameters as a function of the polarization of the pump beam (horizontal on the left and vertical on the right). Third row: type-II SPDC rings as a function of the tilt of the crystal. All cases involve the cw pump laser beam.

In the first row of Fig. 31 the tilt about one axis was varied while the other axis remained fixed. From frame to frame we see the diameter of one ring decreasing (from left to right) while the other ring remained at a fixed diameter. The tilt setting for generating polarization-entangled photons is the third image from the left, a case where both rings have the same diameter. The crucial point is that when the overlap of the rings is perfect it is impossible to know from which crystal the light originated. Photons that are partners of each other appear at points diametrically opposite to each other along the ring. If we select two small regions opposite each other, say on a horizontal plane, then it is uncertain whether the photon partners are either both horizontally polarized, or both vertically polarized. The quantum state of the light is said to be entangled in polarization, and given by

$$|\psi\rangle = 1/\sqrt{2}\left(|H_1 H_2\rangle + |V_1 V_2\rangle e^{i\delta}\right), \tag{36}$$

where the subscripts denote the particle labeling, and H and V denote the polarization labeling. The equation is written in the Dirac formalism of quantum mechanics. The variable δ is a phase due to the birefringence of the crystals. It can be adjusted by tilting a wave plate located before the SPDC crystals.

For the case of type-I SPDC entangled photon generation the pump beam has a polarization that is orthogonal to that of the down-converted photons. For example, vertically-polarized photons are produced by the horizontal component of the polarization of the pump beam, and conversely,

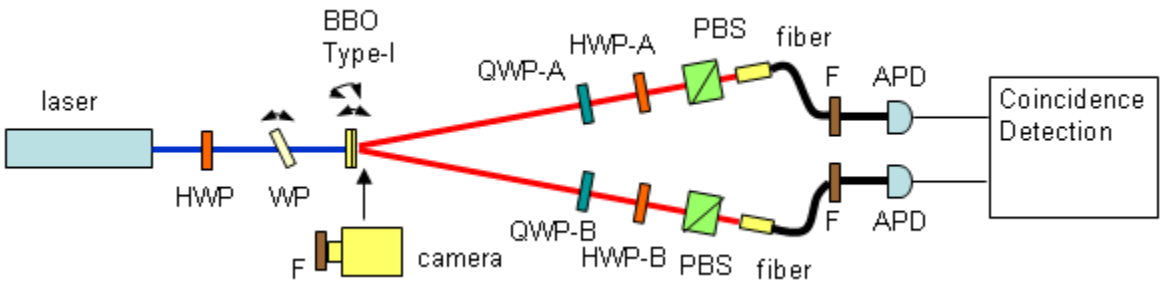


Figure 32. Diagram of the setup to produce and diagnose polarization-entangled photons via type-I SPDC. The components of the figure are: half-wave plates (HWP), quarter-wave plates (QWP) polarizing beam splitter (PBS), Beta-barium-borate SPDC crystals (BBO), wave plate (WP), band-pass filters (F) and avalanche photodiodes (APD).

horizontally-polarized photons are produced by the vertical component of the pump beam. For the frames shown in the top row of Fig. 31 the pump beam had equal intensity on both polarization components. This was achieved by orienting the polarization of the pump beam at an angle of 45° with respect to the horizontal. Since the polarization of the laser is vertical, we rotated it by means of a half-wave plate (HWP), as shown in Fig. 32. A tilted wave plate (WP) was used to adjust δ. The figure also shows the two-crystal system (BBO) and illustrates how the camera was located for generating the images of Fig. 31. For now let us ignore the other elements in the path of the light after the crystal. The sequence of frames in the second row of Fig. 31 corresponds to both crystals having fixed but different tilts so as to produce rings of different diameter. In this sequence of frames we changed the polarization orientation of the pump beam from horizontal on the left to vertical on the right. We saw one ring on the right, which is consistent with down-converted light coming from only one crystal. As the polarization of the pump beam was rotated the second ring of light coming from the second crystal appeared while the first one gradually disappeared. This continued until the last frame where only one ring remained owing to only the single polarization component of the pump beam (vertical) producing down-converted light from only one crystal.

The third row of Fig. 31 shows the images for entangled photon generation via type-II SPDC with a single crystal, for different tilts of the crystal. In this case, rings of differing polarization were non-collinear. At the intersection points of the two rings the photon pair is entangled in polarization. The quantum state of the photon pairs emerging from the intersection points was

$$|\psi\rangle = 1/\sqrt{2}\left(|H_1V_2\rangle + |V_1H_2\rangle e^{i\delta}\right). \tag{37}$$

Adjustment of δ required two additional compensating crystals placed in the path of the light. The third row images of Fig. 31 depict how the rings changed their diameter as a function of the tilt of the crystal. We also investigated a configuration that corresponded to the collinear propagation of the light. This corresponds to the arrangement of the tilt of the crystal that produced the output shown in the third image from the left, where the two rings overlap almost tangentially. Adjustment of these compensators allows for optimization of the states' fidelity. The full analysis of the quantum state can be measured through state tomography.

Quantum state tomography is the process of reconstructing the density matrix of a quantum system from experimental data. Through a series of measurements, dependent upon the degrees of freedom in the system, one can construct a graphical representation of the quantum system's state. For the purpose of this discussion polarization is the only degree of freedom (of several possible) considered. These quantum systems are inherently described by a linear combination of probability amplitudes and eigenstates. Thus, reconstructing the density matrix provides essential information about the composition and quality of the system under experimental investigation.

Although quantum state tomography is well defined and understood in both theory and experiment, there are various practical hurdles that impede its fluid implementation in a laboratory environment. A matrix of 4^n elements (*n* being the number of quantum bits) must be populated to fully characterize a quantum optical signal. In order to alleviate the challenge of performing 4^n calculations each time a density matrix had to be populated with experimental data an automated protocol was developed (in MATLAB). On input this program takes in the 4^n values of predefined measurements [James01] and outputs the various calculations that are needed to analyze the integrity of a quantum system. Values for fidelity, coherence, tangle, and entanglement of formation are calculated and provided in conjunction with a graphical representation of the density matrix (Fig 33a,b). This protocol allows for a readily available analytical tool that is fully reconfigurable and scalable. It requires little computing power and may be executed on the fly in the laboratory.

As we approach the limits of two qubit analysis and move on to higher order state spaces, this tomographic algorithm allows us to easily tailor the calculations to the *n*th order and scale the density matrix accordingly. In a follow on to this in-house project we will investigate the possibility of expanding our state space while limiting the number of measurements needed to populate its density matrix. This can be accomplished through the use of "entanglement witnesses" [Toth05]. This approach utilizes an algorithm similar to our tomographic code while being able to populate density matrices of much larger *n* without measuring all possible 4^n elements individually. In Fig. 33a and Fig. 33b we show a graphical representation of the two

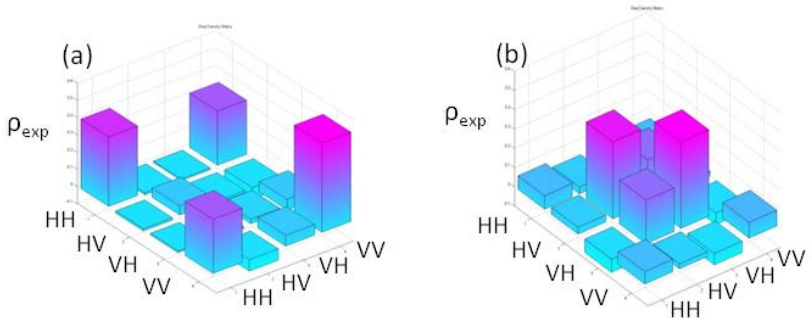


Figure 33: Tomographic reconstruction of density matrix from experimental data.

quantum states (density matrices) given in Eq. (36) and Eq. (37), respectively, produced by SPDC. The density matrices provide a description of the quality of entanglement between the two photons. The diagonal elements the density matrix provide probability information for the system to be in a given computational basis state $\{|HH\rangle,|HV\rangle,|VH\rangle,|VV\rangle\}$. The off-diagonal

elements provide information about the coherence of the system. The entropy and other entanglement measures may also be calculated from these matrices.

4.6 Multi-crystal lattices

Physical implementation of a group velocity matched (GVM) crystal in the 800nm regime is a non-trivial task. Materials do not naturally occur with this property in this particular wavelength regime as they do at the region of 1.5 µm. The design illustration in Fig. 34 bears some resemblance to 'quasi-phase matching' (QPM), but there are important distinctions. In QPM calibrated periodic poling reverses the sign of the nonlinear coefficient such that the periodicity effect can compensate for the phase mismatch in a medium which otherwise could not exhibit 'non-critical' phase-matching. Here, the nonlinear (NL) ß Barium borate (ß-BBO) crystals are already phase matched; it is the group velocities which must be made to match as well. This can be viewed as a generalization of phase matching to include overlap of the photon propagation vectors $\vec{k}_{i,s.p} = \frac{2\pi}{n\lambda}$,where *i,s,p* are idler, signal and pump respectively. The phase is the zero order term in a Taylor expansion of the propagation vector ($\vec{k}_{i,s.p}$), while (inverse) group velocity is the first order term. Unlike QPM however, GVM cannot be synthesized in a single medium; two or more media with proper complementary properties are required for a "compensated assembly" [U'Ren06, Erdmann00]. Though physical difficulties delayed earlier investigations, progress in crystal fabrication has brought the feasibility and cost within a reasonable range (Fig. 34).

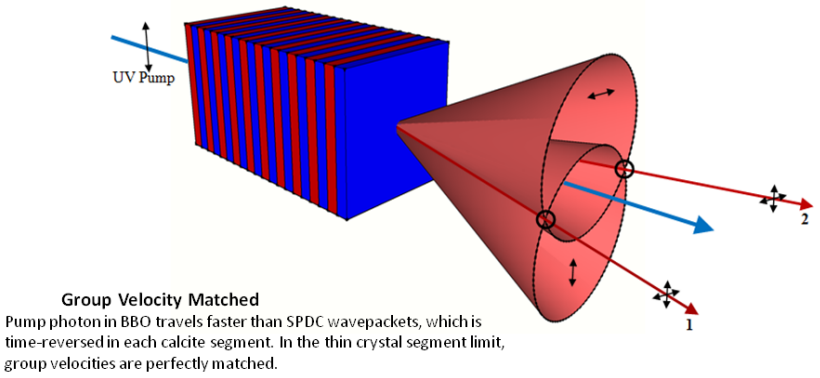


Figure 34. Type-II custom assembly showing alternating BBO (red) and calcite (blue) segments.

The orientation of the crystal phase matching function (PMF) is determined by conservation of momentum for the propagation components along the respective crystal axes. Note that the momentum of a photon in a medium is simply $k' = nk$ where the index of refraction *n* embodies the medium's effect on propagation. The width or spread of the PMF in this case is inversely related to the crystal length and is orthogonal to that of the pump function (which embodies energy conservation). A special case of GVM can be met when the slope of the crystal function becomes exactly orthogonal to that of the pump function and the widths of the pump and crystal functions are engineered to be equal so as to yield a separable (factorizable) state. The more general conditions, illustrated in Fig. 35, involve symmetry about a vertical (or horizontal) axis. Any asymmetry means that a spectral detection of one photon (e.g. signal) provides spectral

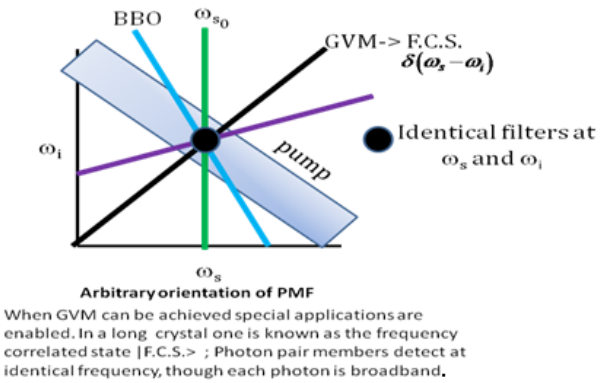


Figure 35. Arbitrary possible orientations of the crystal function with varying BBO-calcite thickness ratios.

information regarding the second (idler) photon. To modify the orientation (or shape) of this distribution one could add optical components (e.g. spectral filters), select a different source, or modify the effective source.

The method we developed in this work made use of custom crystal assemblies (Fig. 34). Each thin (nonlinear) BBO segment is alternated with a (linear) medium, which is also birefringent. The linear medium is not phase matched and hence does not generate SPDC. The effect of the linear medium is to reverse the effect of pump pulse velocity mismatch in BBO compared with that of the SPDC two-photon wave-packet. Calcite has been identified as one of a very few crystals with the requisite properties that exhibit this effect at 800 nm (400 nm pump and shorter). In general, for sufficiently thin segments, GVM is nearly satisfied throughout the assembly, and deviations from the ideal case can be calculated from the actual thickness used. Our initial measurements of the polarization state tomography, illustrated in Fig. 36, deviated

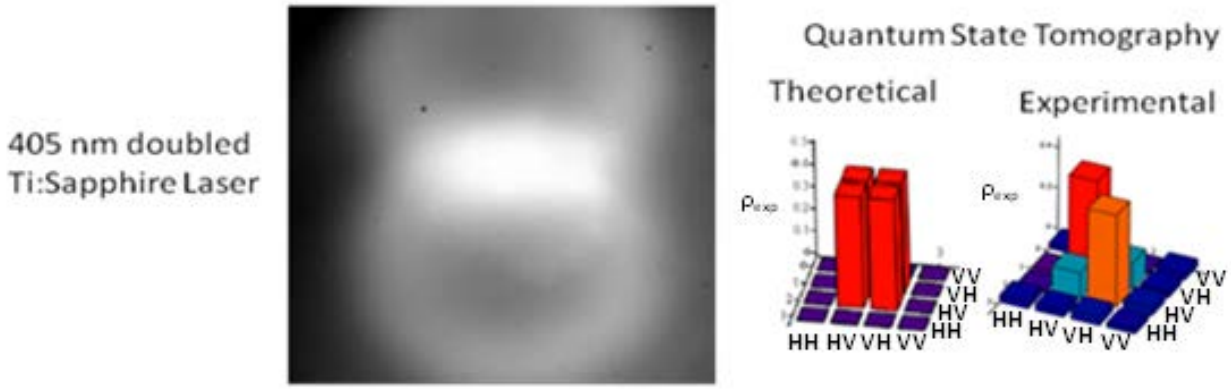


Figure 36. Output entangled rings and tomography for initial custom assembly under broadband pumping.

from the theoretical expectation. Further measurements on these prototype assemblies will be required to resolve this in future work.

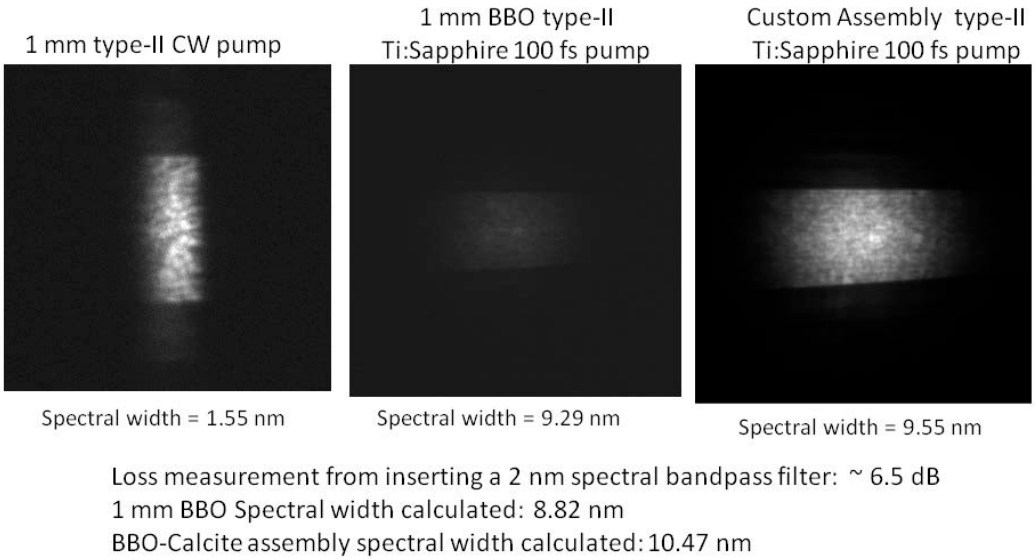


Figure 37. Spectral Images of Type-II polarization entangled photons. Full image widths along x-axes shown are 11, 22, and 14 nm respectively.

Arbitrary control over phase matching function orientation

We focused our efforts on the establishment of GVM because of its wide utility, but the applicability of the segmented method presented above can be also extended to other applications. In particular, this approach can produce arbitrary orientations of the PMF (Fig. 37). In this case we may view the GVM condition as a special case of a spectral function oriented at 45°. Note that pump orientation is always approximately 45°. The PMF orientation can be rotated to any angle by simply adjusting the ratio of segment length between BBO and Calcite, something which cannot be accomplished with other known methods for which special applications have already been identified [U'Ren06, Erdmann00].

4.7 Schioedtei entangled photon crystal source

The multipli-entangled photon source was designed and developed in two stages; a prototype constructed in-house, and second generation (version II) built by an outside vendor. The prototype version of the Schioedtei assembly was constructed from two 8x8x2 mm type-II beta-Barium borate (ß-BBO) crystals phase matched (at angles of theta = 41.9°, phi = 30°) for 810 nm SPDC. Each of the crystals had a dualband AR coating for 405/810 nm on all faces and were placed in physical contact with each other in a constructed housing. Version II of the assembly was constructed by an outside vendor since optically contacting the crystals is not an in-house capability. Version II was dualband AR coated for 405/810 nm only on the exterior faces of the assembly.

The verification and analysis testbed required for testing Schioedtei is shown in Fig. 38. The experimental configuration required for testing with a pulsed pump consisted of a 15 Watt

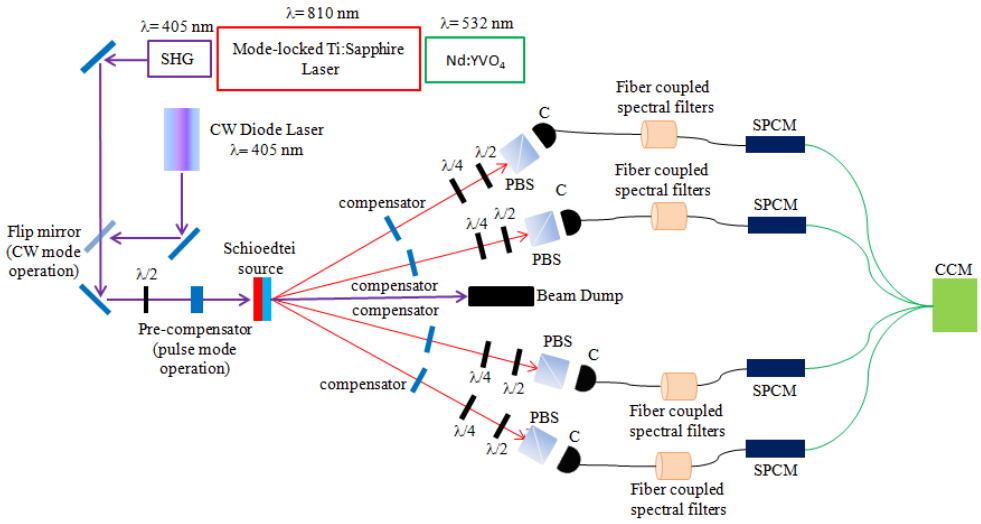


Figure 38. Experimental testbed to analyze the Schioedtei source.

CW Vandate laser operating at 532 nm (Millenia PRO 15sJ) pumping a 3.5 W 100 fs Ti:Sapphire laser operating at 810 nm (Tsunami 3960-15HP), passing through an SHG unit (Inspire Blue FM), to produce ~100 fs pulses at 405 nm with an average power of 1.4 W. The 405 nm pulses served as the input excitation beam for the Schioedtei assembly after first passing through a 6 mm quartz pre-compensator and a half-wave plate set to 22.5° to rotate the input linear polarization to the required 45° for equal excitation of the crystals. This configuration also allowed for CW mode testing in which a 100 mW 405 nm diode laser was inserted into the setup via a flip mirror and the pre-compensator was then removed before the Schioedtei assembly. The residual pump beam was collected in a beam dump, although it could just as easily been redirected with a mirror to pump further crystal stages. The cones of SPDC generated photon pairs then propagated across approximately 0.5 meters of free space to obtain the useable spatial separation required for detector access to the middle square of intersection points (5, 6, 7, 8). Inserted into each of the twelve free space paths were compensators to eliminate the temporal separation between the signal and idler photons due to the birefringence of the Schioedtei assembly. The compensating crystals used for Schioedtei were 8x8x1 mm type-II phase matched ß-BBO (at angles of theta = 41.9° and phi = 30°) aligned orthogonally to their respective counterparts in the Schioedtei crystal pair. These compensators could not be used for compensation of a collinear configuration as they were phase matched for SPDC at 810 nm when exposed to a 405 nm excitation beam.

Detection of the generated entangled photons was accomplished via fiber-coupled single photon counting avalanche photodiodes (APDs) (Perkin Elmer SPCM-AQ4C). Collection apertures consist of fiber-coupled collimators and spectral distinguishability of the photons is removed by fiber-coupled 2 nm bandpass filters centered at 810 nm. Coincidence detection was accomplished by connecting the four detectors to a coincidence counting module (CCM) (Branning, Trinity College) shown in Fig. 39 [Branning11]. This board allowed for up to four fold coincidence detection via four input channels and eight reconfigurable outputs between any of the four input channels.

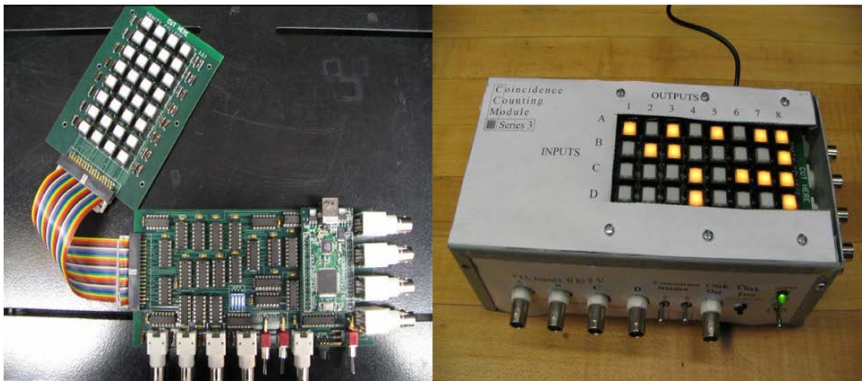


Figure 39. Coincidence counting module (Branning, Trinity College [Branning11]) utilized in the experimental testbed in Fig 38.

A single photon cooled CCD camera (Princeton Instruments Pixis 1024BR) allowed for direct viewing of the SPDC photons produced. Utilizing this camera greatly facilitated alignment of the output of the Schioedtei assembly to the preconfigured collection apertures of the collimators. An alignment grid with pre-determined locations for spots 5,6,7,8 was used to approximately align the Schioedtei assembly to the existing collimators.

A long exposure image from the CCD camera is shown in Fig. 40. The twelve overlap regions are clearly visible and the spatial symmetry of the output should be clearly noted. The orientation of the crystal assembly gives an approximate Gaussian profile on spots 5,6,7,8 and a slightly elongated profile for spots 1,2,3,4,9,10,11,12. The central bright spot shown in the middle of the image is residual 810 nm unfiltered pump beam and fluorescence from the color glass filter used to block the CCD from the 405 nm excitation beam.

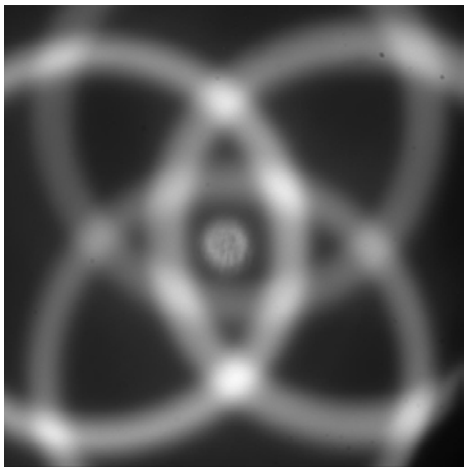


Figure 40. Experimental data from in-house constructed crystal stack.

Once the Schioedtei crystal assembly had been set into the correct orientation via the CCD camera a 630 nm visible laser was back propagated through the collimators to align the faces to the center of the crystal, as shown in Fig. 41. The collimators were reconnected and final alignment was accomplished by optimizing coincidence count rates on the selected channels on the CCM.

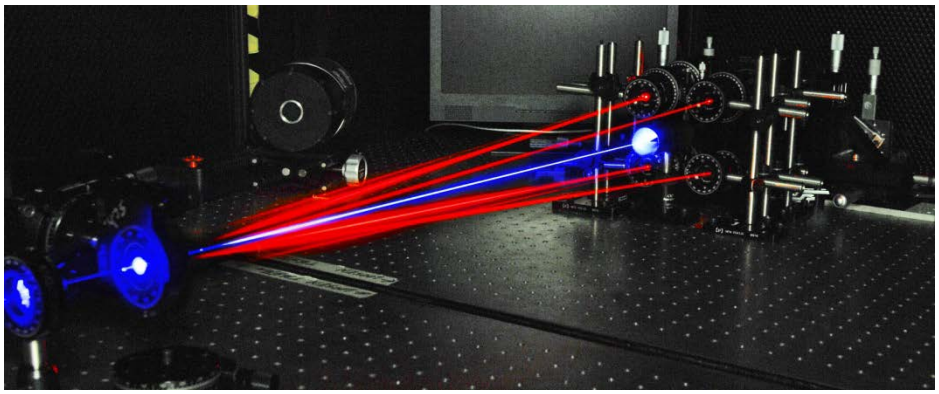


Figure 41. Alignment image of the Schioedtei crystal stack.

The experimental data shown in Fig. 40 is the output of the in-house constructed Schioedtei assembly. The image shows minor levels of scattering which is attributed to the lack of optical contacting between crystal 1 and 2 in the assembly. Scattering is also due to imperfections in the crystal faces and slight angular tilting of the crystal faces with respect to one another in the custom built housing. Overall, the output SPDC rings are well defined and approximately equal in detected intensity on the CCD camera. Single channel count rates detected by the Si-APDs averaged ~20000 counts/sec. Coincidence count rates observed between any pair of spots (1,2,3,4,5,6,7,8) were ~2000 counts/sec with 4 fold coincidence count rates between 1,2,3,4 or 5,6,7,8 in the 5-10 counts/sec range. Upon alignment and optimization of each of these channels a 2-photon quantum state tomography was accomplished on any of the diametric pairs. Since reconfiguration of the collimators was required to observe spot sets 1,2,3,4 (linear arrangement) or 5,6,7,8 (square arrangement) diametric pairs were chosen within each of these sets. Insertion of quarter-wave, half-wave plates and polarizing beamsplitters (in that respective order) into the free-space section following the compensator and preceding the collimators was required for full tomographic analysis of the produced quantum state. The resulting density matrix can be seen in Fig. 42. The resulting quantum state, while mixed and not ideal, was a promising step towards the expected state of $|\psi\rangle = (|\mathrm{HV}\rangle + |\mathrm{VH}\rangle)/\sqrt{2}$ (fidelity: $F = \langle\psi|\rho_{\mathrm{exp}}|\psi\rangle = 0.65$, concurrence: C = 0.53 where $\mathrm{C} = 2(\alpha\delta - \beta\gamma)$ for $|\psi\rangle = \alpha|HH\rangle + \beta|HV\rangle + \gamma|VH\rangle + \delta|VV\rangle$.

$$\rho_{\mathrm{exp}} = \begin{array}{c} \\ \mathrm{HH} \\ \mathrm{HV} \\ \mathrm{VH} \\ \mathrm{VV} \end{array} \begin{array}{c} \begin{array}{cccc} \mathrm{HH} & \mathrm{HV} & \mathrm{VH} & \mathrm{VV} \end{array} \\ \begin{bmatrix} 0.0697 & 0.0354 & -0.0688 & 0.0648 \\ 0.0354 & 0.3994 & 0.2260 & 0.0247 \\ -0.0688 & 0.2260 & 0.4496 & -0.0591 \\ 0.0648 & 0.0247 & -0.0591 & 0.0812 \end{bmatrix} \end{array}$$

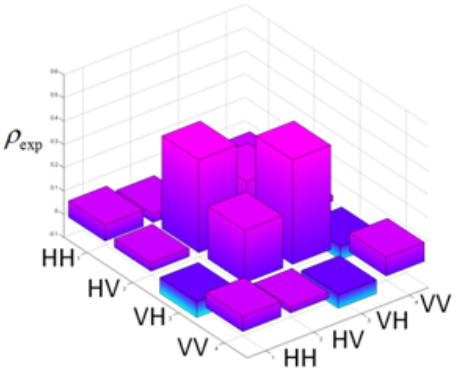


Figure 42. Experimental tomography data (density matrix) from in-house constructed Schioedtei crystal stack.

To improve upon the prototype design, version II was constructed by a commercial vendor with the capability of optically contacting the crystals in the assembly. Optical contacting allowed for the removal of the dual band AR coating layers between the interfaces of crystals 1 and 2. Version II of the Schioedtei assembly was recently delivered, though not yet fully characterized for results to be reported in this report. The initial images from the generated rings are shown in Fig. 43. SPDC rings produced from the in-house designed/commercially-constructed Schioedtei assembly showed greater uniformity in intensity along with a reduction in background scatter.

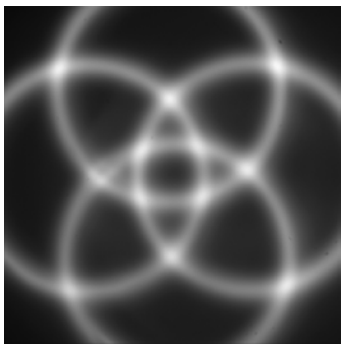
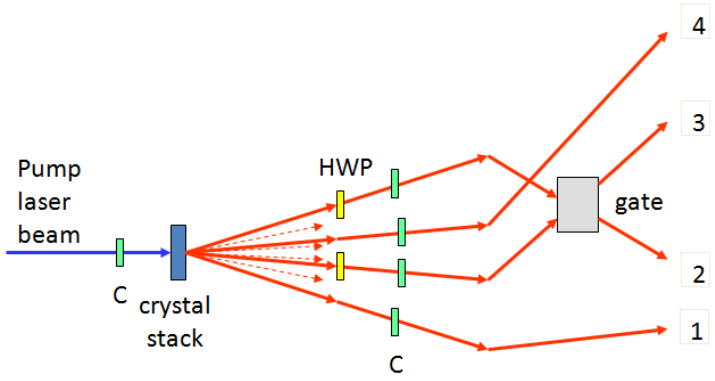


Figure 43. Experimental data from in-house designed, commercially-constructed crystal stack.

The Schioedtei source has immediate and direct implementations for the generation of cluster states. Cluster states play a central role in the measurement-based one-way quantum computation approach [Raussendorf01]. In this scheme, the entanglement resource is provided in advance through an initial, highly entangled multi-particle cluster state, and is consumed during the quantum computation by means of single-particle projective measurements. The feedforward nature of the one-way computation scheme renders the quantum computation deterministic, and removes much of the massive overhead that arises from the error encoding used in the standard quantum circuit computation model [O'Brien07]. Fig. 44 illustrates a scheme for utilizing the output of Schioedtei to generate a four photon cluster state, $|C_4\rangle$ [Schmid07]. This particular



$$|C_4\rangle = \frac{1}{2}\left(|HHHH\rangle_{1,2,3,4} + |HHVV\rangle_{1,2,3,4} + |VVHH\rangle_{1,2,3,4} - |VVVV\rangle_{1,2,3,4}\right)$$

Figure 44. Experimental setup for 4-qubit cluster state generation utilizing Schioedtei crystal source.

example employs the spots 1,2,3,4 and requires insertion of two half-wave plates and a controlled-phase (CPhase) gate. This scheme could be expanded to include the other eight spots to generate even larger cluster states. Such experiments are currently being explored in-house in a follow on project.

An advantage of the Schioedtei configuration is the diversity of states that it is capable of generating. Schioedtei allows for the direct generation of the (unnormalized) state $|\mathrm{HV}\rangle \pm \mathrm{e}^{i\varphi}|\mathrm{VH}\rangle$ as well as the generation of the state $|\mathrm{HH}\rangle \pm \mathrm{e}^{i\varphi}|\mathrm{VV}\rangle$ with the addition of a half-wave plate. In addition, separable states such as $|\mathrm{HV}\rangle \pm \mathrm{e}^{i\varphi}|\mathrm{VV}\rangle$ or $|\mathrm{HV}\rangle \pm \mathrm{e}^{i\varphi}|\mathrm{HH}\rangle$ can also be directly generated with clever combinations of the twelve output intersections and proper compensation.

A path towards increasing the useable photon count rate in Schioedtei is the integration of the GVM phase matching constraint (as discussed in section 4.6, see [U'Ren06]) into the crystal construction. A GVM configuration is possible by alternating reduced thickness Schioedtei and α-BBO layers (α-BBO is used as a compensator; there is no second order nonlinear effect in α-BBO crystal due to the centric symmetry in its crystal structure). A source of this nature would not only provide six spatially separate entangled pairs, but also alleviate the need for spectral filtering of the photons. An increase in useable signal rates of 10X over a typical type-II source is realizable with GVM matching.

5.0 CONCLUSIONS

Grover's quantum search algorithm: simulation

Research conducted under this LRIR indicates that the hybrid coarse grain (distributed MPI)/fine grain (multi-core GPGPUs) approach to numerical simulation of quantum algorithms shows promise. As discussed in Section 4.1, an important item to consider for the applicability of conventional parallel resources is the particular form of the quantum circuit decomposition. The point here is that the most efficient decomposition of a general unitary U into the least number of one and two qubit operations may not necessarily be the one most amenable to the utilization of parallel multi-processor resources. More research in this area is highly warranted.

In general, the utilization of parallel multi-processors to numerical quantum simulation can only increase the number of simulatable qubits by a finite amount (this directly addresses the power of quantum computation over the conventional parallel computation), as the following argument illustrates. The number of qubits n_{serial} that can be simulated on a single (serial) processor can be estimated as $\log_2(N_{serial} = 2^{n_{serial}}) = n_{serial}$. Let the number of parallel processors be given as a power of 2 as $N_{procrs} = 2^{n_{procrs}}$. The number of qubits $n_{parallel}$ that can be simulated by utilizing N_{procrs} is given by solving $n_{serial} = \log_2(N_{parallel} / N_{procrs}) = \log_2(2^{n_{parallel}} / 2^{n_{procrs}})$, with result $n_{parallel} = n_{serial} + n_{processors}$. This means we only get a logarithmic improvement in the number of qubits that can be simulated as we increase the number of processors (e.g. 1024 processors only increases the number of simulatable qubits by 10). However, in practice it would be very

advantageous to simulate the number of qubits in a "small" quantum processor. Using 1 byte = 8bits ~10bits (for order of magnitude estimates) we see that on a serial machine 50 qubits would require $2^{50} \sim (2^{10})^5 \sim (10^3)^5 \sim 10^{14}$ bytes = 100 TB of memory. However, using $1024 = 2^{10}$ parallel processors would require only 100 GB of memory per processor, which though large, is still within reach of today's resources. The use of hybrid coarse/fine grain simulation quantum algorithms/circuits using MPI and CUDA may be of help in this endeavor.

Grover's quantum search algorithm: theory

The focus of the work explored in this LRIR was to illustrate a variant of Grover's algorithm for the case of a k=2 indexed database state of the form $|\psi_{db}\rangle_{xt} = 1/\sqrt{N}\sum_{i=0}^{N-1}|x_i\rangle_x \otimes |t_i\rangle_t$. The rationale behind our approach was to avoid the requirement that the oracle, implementing the phase kickback operation, has to be supplied to the searcher of the database by an external agent (as in the original formulation of the GSA). Instead, our variant of the GSA was designed so that the searcher could initially encode the database state and subsequently search it at a later time, without having to know the sought-for result in order to construct the phase kickback operator.

The variant of the GSA discussed in this work can easily be extended to multi-indexed databases states of the form $|\psi_{db}\rangle_{xtsr\ldots} = 1/\sqrt{N}\sum_{i=0}^{N-1}|x_i\rangle_x \otimes |t_i\rangle_t \otimes |s_i\rangle_s \otimes |r_i\rangle_r \cdots$. If this generalized database state is encoded in the past, then a later time a chosen subspace component (e.g. the t-subspace telephone number as illustrated in this paper) can be searched on through the construction of a phase kickback operation $U_f^t = I_N^x \otimes U_f^t \otimes I_N^s \otimes I_N^r \cdots$ on that subspace, implementing $f(t^*)=1$ and $f(t\neq t^*)=0$ for a given t^*, producing the result $U_f^t |x_i\rangle_x \otimes |t_i\rangle_t \otimes |s_i\rangle_s \otimes |r_i\rangle_r = |x_i\rangle_x \otimes (-|t_i\rangle_t) \otimes |s_i\rangle_s \otimes |r_i\rangle_r$ $= -|x_i\rangle_x \otimes |t_i\rangle_t \otimes |s_i\rangle_s \otimes |r_i\rangle_r$ For a k-component database state (i.e. k different index states $|x_i\rangle_x, |t_i\rangle_t, |s_i\rangle_s, |r_i\rangle_r, \ldots$), general amplitude amplification as given in (12) $G = U_{\psi^\perp} U_f = A U_{0^\perp} A^\dagger U_f$ can be used to perform an $O(\sqrt{N})$ Grover search algorithm in the N dimensional subspace of a general N^k dimensional Hilbert space. Again, A is the unitary operator that takes the standard state $|0\rangle_{xtsr\ldots}$ to the database state $|\psi\rangle_{xtsr\ldots}$. The utility of this approach depends upon the ease and efficiency of constructing the operator A. and hence the quantum database state $|\psi\rangle_{xtsr\ldots}$. Similar work along the lines of a quantum Grover search upon multi-index states has been considered by Pang *et al* [Pang06].

Quantum computing in a piece of glass using volume holograms

For linear optical quantum computing the overarching advantage of constructing simple quantum gates in volume holograms, as opposed to using the standard free-space optical approach, is stability. Often quantum operators, e.g. the simple projection operator given by (11), require a cascade of interferometers where the output of one is the input of the next. Thus, as the dimension of each state space increases it becomes exceedingly hard to stabilize as the number of qubits increases. Other approaches, such as crossed thin gratings, lack the efficiency needed for QIP. The device proposed here can potentially achieve this in a single piece of glass without the problem of misalignment. The technology presented here can potentially replace "fixed" optical components on a broad spectrum of classical and quantum photonics experiments.

The primary limitation of volume holographic QIP is that it is not scalable. Experience shows that multiplexing requires approximately 1mm per recording of the state space to achieve high fidelity, and in QIP applications this scales exponentially with the number of qubits. Secondly, the holograms discussed here are write-once holograms and cannot be erased. Therefore, the algorithm is "fixed" into the holographic emulsion. While there are re-recordable holographic media, none that we know of have the specifications to outperform PTR glass for the applications discussed in this manuscript. Although “static” gates are not the preferable media for a quantum CPU, this technology might be integral to complete QIP systems where smaller d-partite operations are needed on a routine basis, e.g. a quantum memory bus, quantum error correction circuit, or quantum key distribution relay system.

While we have extensively analyzed these volume holographic quantum gates using coupled-mode theory, paraxial wave equation simulations and finite-difference time domain simulations, we have not fully analyzed the engineering particulars of this device. Many important practical questions remain to be explored, for example: (1) how many independent writes of orthogonal states into a holographic emulsion can be made in the PTR glass before cross-talk between the modes becomes a limiting factor? (2) Is it difficult to stack the holograms due to the enhanced angular selectivity of the volume holograms? And (3) what is the maximum number of recordings in a multiplexed PTR hologram that can be reasonably achieved? In this sense, we are well along in understanding these devices from a theoretical prospective. We are, however, at the very beginning experimentally.

Cluster state/one-way quantum computation

The largest obstacle to physically implementing a quantum computer, in any architecture, is decoherence – the unavoidable environmental degradation of quantum interference when one interacts with the quantum computer in order to execute operations or perform measurements. In realistic physical systems decoherence tends to make quantum systems behave more classically, and thereby threatens to mitigate any computational advantage possessed by a quantum computer. However, the effects of decoherence can be counteracted by quantum error correction [Shor96]. In fact, arbitrarily large quantum computations can be performed with arbitrary accuracy, provided the error level of the elementary components of the quantum computer is below a certain threshold. This extremely important and relevant result has been named the threshold theorem of quantum computation [Aliferis06] and allows for the possibility of fault tolerant quantum computation. It is vitally important that the resources involved in performing quantum error correction, before and after each quantum unitary gate, does not grow exponentially, thus again threatening to mitigate the computational advantage of quantum computation over conventional computation. Conventional fault-tolerant schemes for OWQC using photons have recently been developed [Dawson06, Varnava06]. The dominant sources of error in this setting are photon loss and gate inaccuracies. In [Dawson06] both photon loss and gate inaccuracies were taken into account yielding a trade-off curve between the two respective thresholds. Fault-tolerant optical computation is possible for e.g. a gate error (probability) rate of 10^{-4} and photon loss rate of $3\text{x}10^{-3}$.

The OWQC paradigm, utilizing cluster states as the initial fundamental entangled resource, claims to substantially reduce the resources required for both optical quantum gates and for error correction. Further, by encoding a collection of physical qubits within the 2D cluster state,

OWQC offers a means of topological error protection for the logical qubit. The simulations conducted under this in-house project (Fig. 30) show that the threshold for an entangled Bell pair creation is about 0.052 when encoding into a cluster state lattice size l = 13, and 0.083 for the surface code with lattice size l = 29. These threshold rates of approximately 5% and 8% are typically an order of magnitude higher than the most promising threshold rates obtained using the standard quantum circuit model. The encouraging results of this portion of the in-house research was used as motivating factor to develop a follow-on in-house proposal for using photon-based qubits to construct quantum gates and circuits to explore the OWQC cluster state approach to quantum computation.

Quantum information science testbed

The focus of this in-house program was the construction of a 6 qubit capable testbed. The utilization of a high power pulsed laser system allowed pump powers to reach a regime where conducting multi-crystal/multi-stage experiments were feasible. Commonly used down-conversion crystals typically produce a single pair of entangled photons per pass of the pump laser. This limitation typically requires multiple crystals and high power to be used to increase the number of qubits over the standard single pair level. With our in-house testbed the single pair limitation was eliminated with the high power of our pump laser. The pulsed pump laser simultaneously allowed for synchronization of the generated photons from multiple crystals, a requirement when generating multi-qubit photon states. With the addition of the Schioedtei source we have extended the capability of the testbed to 12 qubits while using one pass of the pump laser through a single crystal, as opposed to a single pass through 6 separate crystals [Pan07].

Temporally compensated crystal assembly

We have constructed a GVM compensated crystal assembly in the 800 nm regime. The prototype assembly exhibited increased useable photon generation efficiency greater than that of standard SPDC crystals. When GVM can be achieved in practice other applications are enabled; one such application is known as the frequency correlated state (FCS). In FCS the photon pairs are always detected with identical frequency, although each photon is broadband. Several applications have been identified for use of the FCS [Erdmann00, Wong05]. In the case of type-II SPDC, the GVM crystal must be made relatively long, since the value of crystal length determines the joint spectral width. Single crystal experiments have been performed at 1.55 μm, but none at 800 nm for the reasons mentioned, namely that no such natural crystals exist. The multi-crystal assembly offers an improvement, but to achieve results closer to the theoretical GVM maximum case the number of crystal segments required becomes quite large. In comparison approximately 12 alternating layers have been demonstrated under this project, whereas at least 50 would be needed for a high fidelity GVM, and greater than 100 would be needed for a FCS.

The next version of the crystal will aim to generate a joint spectrum closer to the theoretical maximal GVM case. This requires the alternating layers of ß-BBO and calcite to be reduced in thickness and increased in number. Calcite is brittle and soft, a more robust material has been chosen as our temporal compensator, α-BBO. This will tremendously increase the durability of the crystal stack and allow for a greater ease of construction. The construction of this superlattice can be applied towards any downconversion crystal to remove the need for spectral filtering.

Schioedtei crystal assembly

Here we have described the initial work on a new type-II SPDC source design, designated Schioedtei. Schioedtei allows for the generation of six pairs of entangled photons per pass of the pump laser through the type-II crystal assembly. This configuration surpasses the typical single entangled pair generated per pass found in standard type-II SPDC sources. Useable photon rates resulting in two and four fold coincidence events have been observed from Schioedtei demonstrating its feasibility as a source of entangled photons for QIP. The six pairs of photons produced are directly applicable to the generation of larger entangled states for use in CSQC. The unique and advantageous features of Schioedtei source are (i) the production of a more compact experimental setup compared to conventional multi-stage down-conversion configurations; (ii) generation of additional states beyond those produced in standard SPDC sources, whose variety and number (iii) more easily facilitates the creation of higher-order entangled states.

6.0 REFERENCES

[Aliferis06] P. Aliferis, D. Gottesman, J. Preskill, "Quantum accuracy threshold for concatenated distance-3 codes," Q. Info & Comp. **6**, 97 (2006).

[Alsing11] P.M. Alsing and N. McDonald, "Grover's search algorithm with an entangled database state," Quantum Information and Computation IX, SPIE Defense Security and Sensing Symposium, Paper number 8057-11, 25-29 April (2011).

[Bitton01] Bitton et. al., "Novel Cascaded Ultra Bright Pulsed Source of Polarization Entangled Photons", arXiv:quant-ph/0106122v1.

[Boyer96] Boyer., Brassard, G., Hoyer, P. and Tapp, A., "Tight bounds on quantum searching," arXiv:quant-ph/9605034 (1996).

[Branning11] Branning et. al., "Note: Scalable multiphoton coincidence-counting electronics", Review of Scientific Instruments 82, 016102, (2011).

[Bravyi05] S. Bravyi and A. Kitaev, "Universal quantum computation with ideal Clifford gates and noisy ancillas," Phy. Rev. A **71**, 022316 (2005).

[Briegel09] H.J. Brigel, D.E. Browne, W. Dur, R. Rassendorf and M. Van den Nest, "Measurement-based quantum computation," Nature Physics **5**, 19 (2009).

[Burr01] G. W. Burr, C.M. Jefferson, H. Coufal, M. Jurich, J.A. Hoffnagle, R.M. Macfarlane and R.M. Shleby, "Volume holographic data storage at an areal density of 250 gigapixels/in^2," Optics Letts. **26**, 444 (2001).

[Campbell09] E.T. Campbell and J. Fitzsimons, "An introduction to one-way quantum computing in distributed architectures," arxiv:0906.2725, (Sep, 2009).

[CUDA07] "NVIDA CUDA: Compute unified device architecture," http://developer.download.nvidia.com/compute/cuda/1_1/NVIDIA_CUDA_Programming_Gudide_1.1.pdf

[Dawson06] C.M. Dawson, H.L. Haselgrove and M.A. Nielsen, "Noise thresholds for optical quantum computers," Phys. Rev. Lett. **96**, 020501 (2006); ibid, "Noise thresholds for optical cluster state quantum computations," Phys. Rev. A **73**, 052306 (2006).

[Dragoman01] Dragoman, "Proposal for a three-qubit teleportation experiment", Phys. Lett. A 288, 121-124, (2001).

[Erdmann00] R. Erdmann et.al. Restoring dispersion cancellation for entangled photons produced by ultrashort pulses, PRA **62**, 053810 (2000).

[Fanto10] M. Fanto and R.E. Erdmann, "Compensated crystal assemblies for type-II entangled photon generation in quantum cluster states," Quantum Information and Computation IX, SPIE Defense Security and Sensing Symposium, Paper number 77020H-10, 5-9 April (2010).

[Goodman05] J. W. Goodman, "Introduction to Fourier Optics," Roberts & Co. Publ., Greenwood Village, Third Ed. (2005).

[Gottesman97] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. thesis, California Institute of Technology (1997).

[Grice01] W. Grice et.al. Eliminating frequency and space-time correlations in multi-photon states, PRA 64, 063815, (2001).

[Grover97] Grover, L.K., "Quantum mechanics helps in searching for a needle in a haystack," Phys. Rev. Lett. 79(2), 325-328 (1997).

[GSA Benchmarks05] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Apselmeyer and A. Zeilinger, "Experimental one-way quantum computing," Nature **434**, 169-176 (2005); K.A. Brickman, P.C. Haljan, P.J. Lee, M. Acton, L. Deslauriers, and C. Monroe, "Implementation of Grover's quantum search algorithm in a scalable system," Phys. Rev. A. **72**, 050306(R) (2005); Bhattacharya, N., van Linden van den Heuvell, H. B. & Spreeuw, R. J. C. "Implementation of quantum search algorithm using classical Fourier optics," Phys. Rev. Lett. **88**, 137901 (2002).

[Hong87] C.K Hong et. al, Measurement of subpicosecond time intervals between two photons by interference, Phys. Rev. Lett. 59, (1987).

[James01] D. F. V. James, P. G. Kwiat, W. Munro, A. G. White, Phys. Rev. A **64**, 052312 (2001)

[Kaye07] Kaye, P., Laflamme, R. and Mosca, M., "An Introduction to Quantum Computing", Oxford University Press, New York, 152-178 (2007).

[Kogelnik69] H. Kogelnik, "Coupled wave theory for thick hologram gratings," The Bell System Tech. J. **48**(9), 1, (1969).

[Kwiat95] Kwiat et. al., "New High Intensity Source of Polarization-Entangled Photon Pairs", Phys. Rev. Lett. 75, 4335-4341, 1995.

[Kwiat99] Kwiat et. al., "Ultrabright source of polarization-entangled photons", Phys. Rev. A 60, 773-776, (1999).

[Lu07] Lu et. al., "Experimental entanglement of six photons in graph states", Nature Physics, Vol. 3, (2007).

[Miller 11a] W. A. Miller, "Efficient photon sorter in a high dimensional state space," Quant. Info. and Comm. **11**, 313 (2011).

[Miller11b] W. A. Miller, P. M. Alsing, J.R. McDonald, and C. Tison, "Quantum computing in a piece of glass," in Quantum Information and Computation IX. Paper number 8057-27, SPIE Defense Security and Sensing Symposium, 25-29 April (2011).

[Nielsen00] M.A. Nielsen and I.L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, N.Y. (2000).

[O'Brien07] O'Brien et. al., "Optical quantum computing", Science 318, 1567, 2007.

[Pan07] J.Pan et.al. Six photon six qubit cluster states, nature Physics, (2007) .

[Pang06] Pang, C.Y., Zhou, Z.W. and Guo, G.C. "Quantum discrete cosine transformation for image compression," arXiv:quant-ph/0601043, (2006).

[Raussendorf01] R. Raussendorf and H.J. Briegel, "A one-way quantum computer," Phys. Rev. Lett. **86**, 5188 (2001); *ibid* "Computational model underlying the one-way quantum computer," Q. Info. & Comp. **2**, 443 (2002); R. Raussendorf, D.E. Browne and H.J. Briegel, "Measurement-based quantum computation using cluster states," Phys. Rev. Lett. **68**, 022312 (2003).

[Raussendorf05] R. Rassendorf, S. Bravyi and J. Harrington, "Long-range quantum entanglement in noisy cluster states," Phys. Rev. A **71**, 062313 (2005).

[Raussendorf07] R. Rassendorf and J. Harrington, "Fault-tolerant quantum computation with high threshold in two dimensions," Phys. Rev. Lett. **98**, 190504 (2007).

[Schmid07] Schmid et. al., "The entanglement of the four-photon cluster state", New Journal of Physics 9, 236-246, 2007.

[Shor94] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 124-134 (1994).

[Shor96] P.W. Shor, "Fault-tolerant quantum computation," 37th Symposium on Foundations of Computer Science, IEEE Computer Society Press, 56-65 (1996).

[Toth05] G. Toth and O. Guhne, "Entanglement detection in the stabilizer formalism," Phys. Rev. A **72**, 022340 (2005).

[U'Ren05] A.U'ren et.al. Synthesis of time-bin entangled states via tailored group velocity matching, JMO 52, 2197, 2005

[U'Ren06] A. U'Ren et.al. Generation of two-photon states with an arbitrary degree of entanglement via nonlinear crystal super lattices, PRL 97, 223602, (2006).

[Vallone08] G. Vallone, E. Pmarico, F. De Martini and P. Mataloni, "Active one-way quantum computation with 2-photon 4-qubit cluster states," Phys. Rev. Lett. **100**, 160502 (2008).

[Varnava06) M. Varnava, D.E. Browne and T. Rudolph, "Loss tolerance in one-way quantum computation by counterfactual error correction," Phys. Rev. Lett. **97**, 120501 (2006); ibid, "How

good must single photons sources and detectors be for efficient linear optical quantum computation," Phys. Rev. Lett. **100**, 060502 (208).

[Walther05] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Apselmeyer and A. Zeilinger, "Experimental one-way quantum computing," Nature 434, 169-176 (2005); K.A. Brickman, P.C. Haljan, P.J. Lee, M. Acton, L. Deslauriers, and C. Monroe, "Implementation of Grover's quantum search algorithm in a scalable system," Phys. Rev. A. 72, 050306(R) (2005); Bhattacharya, N., van Linden van den Heuvell, H. B. & Spreeuw, R. J. C. "Implementation of quantum search algorithm using classical Fourier optics," Phys. Rev. Lett. 88, 137901 (2002).

[Wong05] F. Wong et.al. Two-Photon coincident frequency entanglement via extended phase matching, PRL **94,** 083601, (2005)

[Xu2008] Xu, N., Zhu, J., Peng, X., Zhou, X. and Du, J., "A non-oracle quantum search algorithm and its experimental implementation," arXiv:0809.0664 [quant-ph], (2008).

[Yanofsky08] N.S Yanofsky and M.A. Mannucci, "Quantum Computing for Computer Scientists," Cambridge University Press, NY, 194-204 (2008).

[Zeilinger05] A. Zeilinger et.al. Experimental One-way computing Nature 434, 169, (2005).

7.0 LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

AdQC: Adiabatic Quantum Computing

α-BBO: Alpha barium borate

API: Application programming interface

AR: Anti-reflective

ß-BBO: Beta barium borate

Cbit: Classical bit

CCD: Charge coupled device

CCM: Coincidence counting module

CIRC: Circle function

CPU: Central processing unit

CSQC: Cluster state quantum computation

CUDA: Compute Unified Device Architecture

CW: Continuous wave

DMA: Direct Memory Access

DPN: Depolarized noise

DRAM: Direct random access memory

FCS: Frequency correlated state

GPU: Graphics processor unit

GPGPU: General purpose graphics processor unit

GSA: Grover's search algorithm

GVM: Group velocity match

HPCMP: High Performance Computer Modernization Program

HWP: Half wave plate

IAM: Inversion about the mean

JEOM: Joint Education Opportunities for Minorities

MPI: Message passing interface

MQC:	Measurement-based quantum computation
NL:	Nonlinear
OWQC:	One-way quantum computation
PBS:	Polarizing beam splitter
PK:	Phase kickback
PMF:	Phase matching function
PTR:	Photo-thermal refractive
QCM:	Quantum circuit model
QEC:	Quantum error correction
QIP:	Quantum information processing
QIS:	Quantum information science
QPM:	Quasi-phase matching
QSA:	Quantum search algorithm
Qubit:	Quantum bit
QWP:	Quarter wave plate
Si-APD:	Silicon avalanche photodiode
SPDC:	Spontaneous parametric downconversion
WP:	Wave plate