AFRL-RI-RS-TR-2012-304

CLUSTER STATE QUANTUM COMPUTING

DECEMBER 2012

INTERIM 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-2012-304 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE DIRECTOR:

/ S /

STEVEN T. JOHNS, Chief
Trusted Systems Branch
Computing & Communications Division

/ S /

RICHARD MICHALAK
Acting Tech 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

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
DECEMBER 2012	INTERIM TECHNICAL REPORT	NOV 2010 – OCT 2012

4. TITLE AND SUBTITLE
CLUSTER STATE QUANTUM COMPUTING

5a. CONTRACT NUMBER
IN-HOUSE

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
62788F

6. AUTHOR(S)
Paul Alsing, Michael Fanto and A. Matthew Smith

5d. PROJECT NUMBER
T2QC

5e. TASK NUMBER
IN

5f. WORK UNIT NUMBER
HO

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

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFRL-RI-RS-TR-2012-304

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited. PA# 88ABW-2012-6581
Date Cleared: 18 December 2012

13. SUPPLEMENTARY NOTES

14. ABSTRACT
Experimental, theoretical and numerical investigations of quantum computation using photon-based qubits were conducted to explore the Cluster State (or one-way) Quantum Computing paradigm. This report describes research on a unique type II SPDC source (Schioedtei) design that can generate up to six pairs of entangled photons per pass through the type II crystal assembly. This source is currently being used as the entangled photon source to create photon-based qubit cluster states. Under this project we developed a new detector design architecture that turns the single photon detector into a number-resolving detector by means of a novel three dimensional architecture that utilizes spatial multiplexing. We have studied the CNOT gate, as an archetypical quantum linear optical gate, and found several interesting features in the both the ideal and the realistic case of implementation with imperfect (non-unit) fidelity. We have conducted a theoretical investigation of the limitations of quantum correlations under the physically imposed constraint of no-signaling (no faster than light communication). We discuss our ongoing work of quantum algorithm development.

15. SUBJECT TERMS
Quantum information processing, quantum entanglement, quantum computing, measurement based quantum computation, cluster states, photonic qubits

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			**PAUL M. ALSING**
U	U	U	SAR	51	19b. TELEPONE NUMBER (*Include area code*) **NA**

TABLE OF CONTENTS

LIST OF FIGURES

1.0 SUMMARY

Experimental, theoretical and numerical investigations of quantum computation using photon-based qubits (Quantum Bits) were conducted to explore the Cluster State (or one-way) Quantum Computing paradigm. This report describes research on a unique type II SPDC (Spontaneous Parametric Down Conversion) source ("Schioedtei") design that can generate up to six pairs of entangled photons per pass through the type II crystal assembly. This source is currently being used as the entangled photon source to create photon-based qubit cluster states. Under this project we developed a new detector design architecture that turns the single photon detector into a number-resolving detector by means of a novel three-dimensional architecture that utilizes spatial multiplexing. We have studied the CNOT gate, as an archetypical quantum linear optical gate, and found several interesting features in the both the ideal and the realistic case of implementation with imperfect (non-unit) fidelity. We have conducted a theoretical investigation of the limitations of quantum correlations under the physically imposed constraint of no-signaling (i.e. no faster than light communication). Finally, we discuss our ongoing work of quantum algorithm development utilizing the measurement-based quantum computation approach, and compare and contrast it with the standard quantum circuit model approach in the case of an unstructured search.

2.0 INTRODUCTION

Under this AFRL/RI in-house project we continued research and development of a novel multi-qubit entangled photon source, begun under the AFRL/RI in-house project "Quantum Information Science (QIS)," (AFRL-RI-RS-TR-2012-073), and begun investigations into the measurement-based cluster state quantum computation paradigm utilizing photon-based qubits. These investigations included: (i) the development and characterization of a new multipli-entangled photon source that increased the usable number of photon pairs by a factor of six over conventional entangled photon sources, (ii) design of multi-layer superconducting number-resolving photon detector, (iii) a theoretical and experimental investigation into the requirements of imperfect (non-unit fidelity) two-qubit linear optical photonic gates, and (iv) a theoretical investigation of entanglement and nonlocality addressing the issue of why nature does not take advantage of the algebraically allowed maximum correlations amongst collections of qubits. In addition, this report discusses upgrades to our in-house AFRL/RI Quantum Computing Laboratory under the current project and our thrust to transition our development of quantum gates/circuits in bulk optics to an on chip integrated waveguide implementation. Finally, this report briefly discusses research we initiated, and is currently ongoing, in the area of cluster state quantum algorithm development.

Cluster State Quantum Computation Background

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 a 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 (MBQC) [Briegel09]. The appeal of MBQC is that deterministic quantum computation is possible based on (i) the preparation of an initial entangled cluster state, followed by (ii) a temporally ordered pattern 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.

In the OWQC approach a 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 gate operations 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 - bases, 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].

Experimental Research:

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 begun under the in-house Quantum Information Science project focused on (i) developing a 6-qubit capable photon-based quantum information testbed and (ii) initial development of 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. This latter direction of research was continued and expanded upon in the current in-house project Cluster State Quantum Computing.

Number resolving photon counting at the single photon level, i.e. distinguishing 1, 2 or 3 photons is an important experimental ability. While experiments can be performed without number resolving detectors such as the APD (Avalanche Photo Diode) we are currently using, a significant number of interesting experiments require the number resolving ability. Therefore we considered a known single photon detector (click or no-click) and have developed a new detector design architecture that turns the single photon detector into a number-resolving detector. This is done through spatial multiplexing. The architecture we have developed allows for higher density of detection elements and larger number of detector elements then the current state of the art. This leads to faster repetition times, and most importantly, superior number resolution.

Theory/Numerical Research:
The creation of single photons is most often performed by non-linear processes such as SPDC. However to create cluster states from these resource photons requires linear optics, such as the CNOT or CZ gates. Numerous implementation methods have been suggested for these gates in theory, but in practice any implementation will be imperfect. Therefore it is important to be able to characterize and optimize imperfect, i.e. fidelity less than 1, linear optical gates and state transformations. We have studied the CNOT gate, as an archetypical linear optical gate and found several interesting features in the both the ideal case and the realistic case of imperfect fidelity. In particular we find that the success rate can be increased as the fidelity decreases. This trade off in fidelity for success opens several interesting possibilities in the field of linear optics. We also found that the CNOT gate has a high degree of symmetry that simplifies its physical implementation in both cases and proposed a practical experiment to test our theories. Such studies can and have been carried over to other gates and state transformation with relative ease.

The ultimate goal of MBQC is to execute quantum algorithms with a speedup over their corresponding classical algorithm counterparts. Under this project we began an investigation of Grover's search algorithm (GSA) on an unsorted list of elements in the MBQC paradigm, and its comparison/contrast with the usual QCM approach. GSA serves as an important prototypical benchmark for many numerical simulations of quantum algorithms [Grover97, Walther05]. Our preliminary results (which are currently being written up for journal submission) indicate that the MBQC implementation of Grover's algorithm is faster than even Grover's quantum algorithm (with its quadratic speedup over a brute force search).

In brief, 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. Under the previous in-house QIS project, 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.

3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

3.1. Multipli-entangled photons from a spontaneous parametric down-conversion source

Photon based quantum computation, with single or entangled photons, is a heavily researched area. This is in part due to many desirable properties of photons such as (i) room temperature

operation, (ii) immunity from the environment and (iii) superior mode quality. Spontaneous parametric down conversion has proven to be the most reliable method of generating entangled photon pairs. Type I sources spontaneously convert one linearly polarized parent photon into two daughters, each having a polarization orthogonal to the parent. The spontaneous nature of parametric down conversion produces a ring pattern where each diametric photon pair shares the same parent photon. The type I process produces two photons of the same polarization which are path entangled. That is, detecting a photon (signal) in path A implies that its sister (idler) can be found in the diametrically opposite spot [Dragoman01]. This implies that in the polarization basis a mixed state $|H\rangle_1|H\rangle_2$ or $|V\rangle_1|V\rangle_2$ will be produced. Many experiments that require photon pairs, but not entangled pairs, use the output of a type I crystal as input to a more sophisticated experiment. Type I crystals are inherently birefringent, but the walk-off associated with these crystals is mitigated by the fact that the down converted photons are the same polarization; the delays that the signal and idler photons experience are the same. Type I sources have been used for many years in harmonic generation (SHG, THG) systems as frequency converters.

Kwiat first described a feasible source for SPDC-generated entangled pairs using type I β-BBO [Kwiat99] (beta-Barium borate, BaB_2O_4). This consisted of a stacked pair of type I crystals rotated 90° relative to each other (Figure 1). This allows for the generation of two orthogonally polarized cones that overlap in space. Each crystal can only be excited by a certain linear polarization. The stack must be pumped by a beam made up of components that excite each crystal equally. That is, if the stack consists of an optic axis that is vertical in the first crystal, and horizontal in the second, the pump beam polarization must be oriented at 45°. The resulting superposition state is $|H\rangle_1|H\rangle_2 \pm e^{i\theta}|V\rangle_1|V\rangle_2$. It is important to note that there is a temporal delay associated with the down converted states due to the crystal's birefringence. Compensation depends on the wave packet of the pump photon.

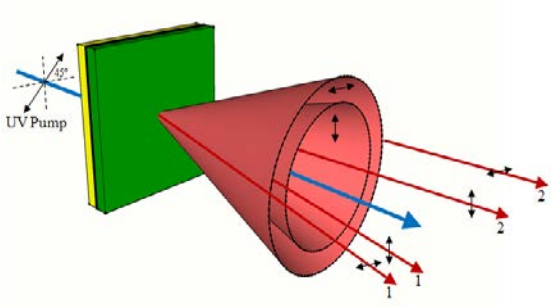


Figure 1. Kwiat's type I pair. Each crystal will spontaneously down convert a linearly polarized photon pair orthogonal to its pump photon. When specifically oriented, these down converted rings can overlap and create a polarization entangled pair.

Type II sources [Kwiat95] down convert a linearly polarized parent photon into two orthogonally polarized daughters making them particularly interesting because the crystal is birefringent. One daughter photon will walk off faster than the other and lead to a noticeable spatial separation, and thus there are two intersecting cones (Figure 2). The walk off of type II crystals limits the length of the crystal because the extraordinary index of refraction will quickly bend light out of the crystal. Indistinguishable photons are produced in the intersections of the two cones. These two points form a superposition state of polarization ($|H\rangle_1|V\rangle_2 \pm e^{i\theta}|V\rangle_1|H\rangle_2$) and have been

exhaustively studied and used as inputs to more complex photonic systems. Figure 3 shows the evolution of the rings of entangled photons produced from SPDC crystals under type I and II phase matching conditions.

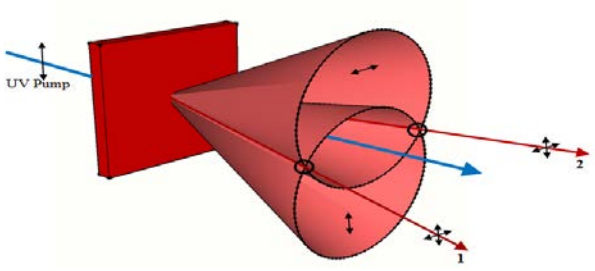


Figure 2. Standard type II down conversion. A linear pump beam spontaneously down converts to two photons, one of which has the same polarization as the pump. The other is orthogonal. The familiar double ring pattern is a product of the crystal's birefringence.

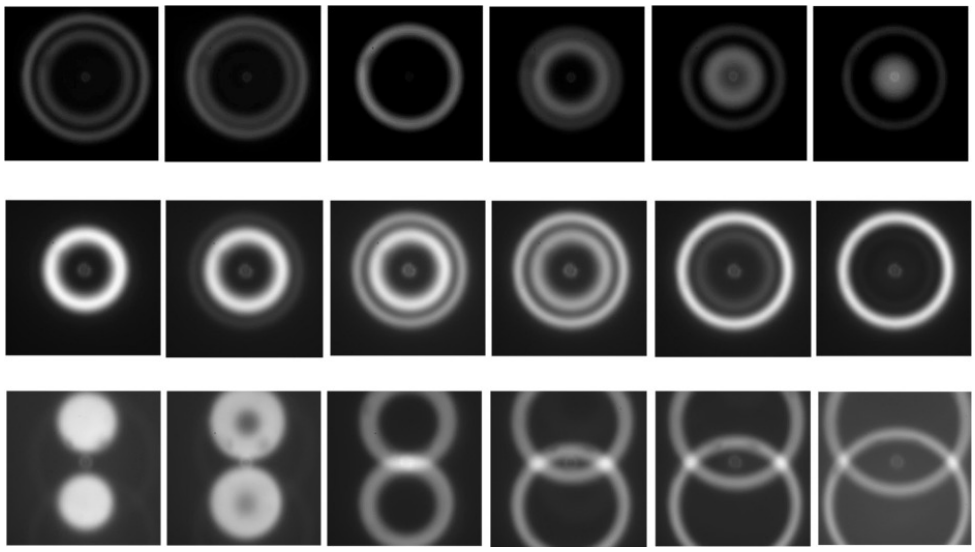


Figure 3: Imaging of the down-converted light for three different configurations. First row: type-I SPDC as a function of the tilt of one crystal. Second row: type-I SPDC rings of different diameters as a function of the polarization of the pump beam (horizontal on the left and vertical on the right). Third row: type-II SPDC rings as a function of the tilt of the crystal. All cases involve the CW pump laser beam.

In a similar fashion to Kwiat's type I stack, Bitton et al. [Bitton01] described a type II stack comprised of two crystals rotated 180° relative to each other (Figure 4). This allows the linear pump scheme to remain unchanged and yields one set of rings from either crystal. The set of rings entirely overlap each other and thus can yield an entangled photon pair of the same state as standard type II. Addressing the compensation is a necessary requirement with any birefringent crystals. A standard type II stacked configuration allows for greater pair production and more useable detection area. In this source as well as a type I stack, the fundamental size of the

collection apertures become the limiting factor in the number of entangled pairs that can be collected.

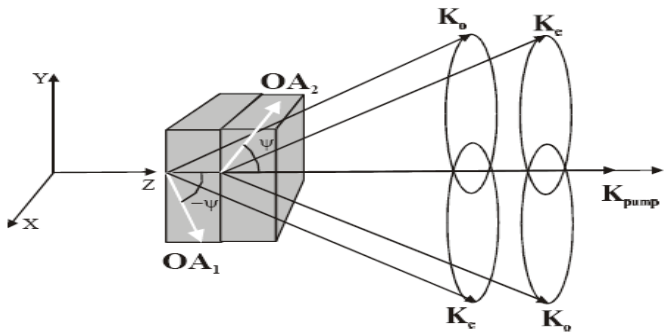


Figure 4. Type II crystal assembly as described by [Bittion01]. The second crystal is rotated 180° relative to the first, resulting in two overlapping sets of cones with orthogonal polarization.

U'ren et al. [U'ren06] described a type II crystal assembly (Figure 5a) that is designed for group velocity matching (GVM) of the pump and signal/idler wave packets, thereby removing any spectral distinguishability of the down converted photons. The assembly consists of a successive stack of nonlinear crystals (β-BBO, BiBO (Bismuth Borate, BiB_3O_6)) separated by a thin layer of compensating crystal (calcite ($CaCO_3$), α-BBO). This slowly compensates different components (pump and down converted wave packets) such that by the end of the stack there is no spectral walk off. The need to spectrally filter post down conversion is mitigated by the symmetry of their joint spectral function (Figure 5b). Removing this requirement typically increases the useable count rate and overall efficiency.

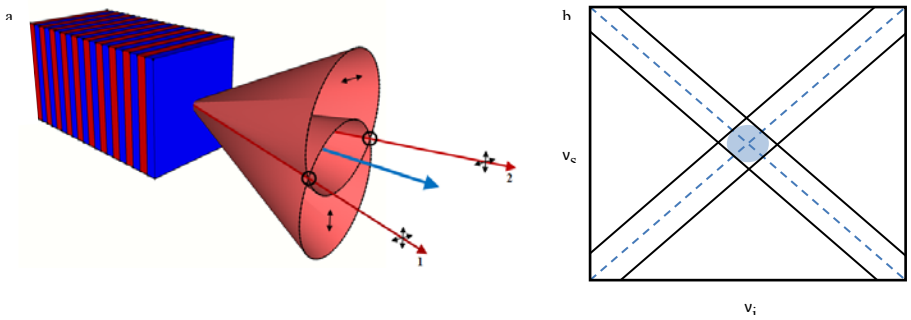


Figure 5. (a) Type II custom assembly showing alternating layers of β-BBO (red) and calcite (blue). (b) Joint spectral function of down converted wavepacket. This implies a maximally separable state.

Type I and II crystals are still governed by their spontaneous nature, and this becomes problematic when large numbers of entangled photons are required. In a typical configuration for the generation of greater than four photons a cascaded apparatus is used. For this setup either multiple crystals are used in succession, or multiple passes through a single crystal (Figure 6). This implies an overall increase in footprint size. Hyper-entanglement has been considered to mitigate the spontaneous nature of down conversion by adding entanglement various degrees of

freedom, not just polarization [Ceccarelli09]. While this is effective it requires larger physical hardware requirements and more complicated analysis processes.

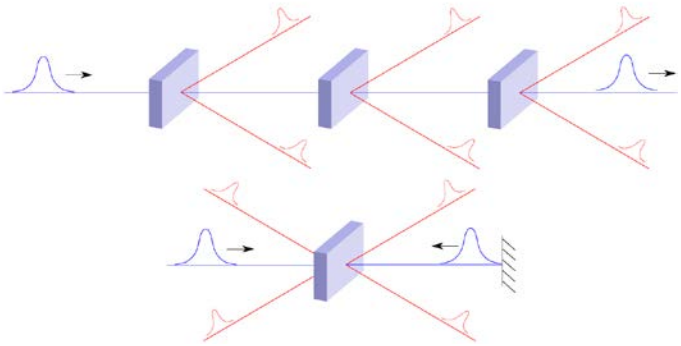


Figure 6. Cascaded and multi-pass crystal configurations for the generation of cluster states [Lu07].

In recent years there has been a paradigm shift in quantum computation with the need to migrate toward schemes that require only single qubit measurements. One-way quantum computation (cluster state) has facilitated this shift. Cluster state computation allows a predetermined sequence of single qubit measurements to determine the algorithm being evaluated [Walther05]. This protocol requires a highly entangled cluster state [Raussendorf01] generated from a resource of qubits. Such a cluster state can be constructed by preparing each of the qubits into a state, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and applying controlled-phase gates to link the required qubits. Computation proceeds with a sequence of single qubit measurements whose results will classically feed forward to control the basis required for future measurements [Nielson05]. Cluster state computation allows for a practical resource reduction in qubits and hardware compared to other quantum computing methods. That being said, the fundamental requirement for larger numbers of qubits still exists. The source we have developed produces larger qubits numbers than that of a typical type II SPDC source.

SPDC custom crystal assembly

Our custom two-crystal assembly (designated as "Schioedtei" henceforth) design consists of a pair of type II non-collinear phase-matched SPDC crystals cut for degenerate down-conversion whose optic axes are rotated orthogonal with respect to one another. The pair of crystals is optically contacted with one another and a dual band (405/810 nm) anti-reflection coating applied to the two exterior faces of the assembly. Any type II material can be used to create an equivalent device. Our particular version that will be discussed here was constructed from two 8x8x2 mm type II beta-Barium borate (β-BBO, BaB_2O_4) crystals phase matched (at angles of theta = 41.9°, phi = 30°) for 810 nm spontaneous parametric down-conversion.

Exciting Schioedtei with an incident 45° polarized pump beam produces one pair of rings 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 Figure 7, the indicated points marked 5, 6 (Bell pair #1 from crystal #1) and 7, 8 (Bell pair #2 from crystal #2) are the typical Bell states, $|\psi\rangle_{5,6(7,8)} = \frac{1}{\sqrt{2}}(|HV\rangle_{5,6(7,8)} \pm e^{i\varphi}|VH\rangle_{5,6(7,8)})$. The

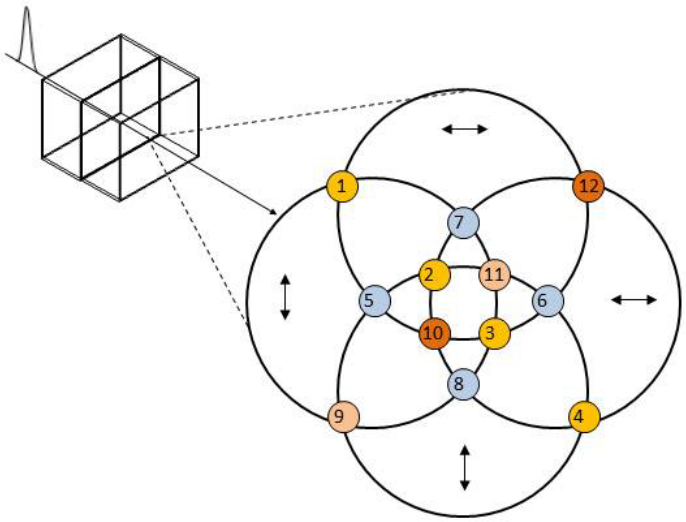


Figure 7. Type-II SPDC Schioedtei source. See text for discussion of the intersection points of the overlapping rings.

points indicated by 1, 2, 3, 4 are the product of two bell states, $|\psi\rangle_{1,2,3,4} = \frac{1}{2}(|HV\rangle_{1,4} \pm e^{-i\varphi}|VH\rangle_{1,4})(|HV\rangle_{2,3} \pm e^{-i\varphi}|VH\rangle_{2,3})$, produced from photons from both crystal 1 and 2 concurrently. Points 9, 11 and 10, 12 are $|VV\rangle_{9,11}$ and $|HH\rangle_{10,12}$ states produced from photons from crystal 1 and 2 concurrently. Further analysis and experimental results of Schioedtei are covered in section 4.1.

3.2 A multi-layer three dimensional superconducting nanowire photon detector

Construction of photon-counting devices with high counting efficiency, high number resolution and short reset times, is highly desirable for a wide array of applications, such as quantum key distribution [Xu08], quantum communication [O'Brein09], quantum computing [Knill01], [Uskov10], [Knill02] among others [Hadfield09], [Smith11]. Here we describe and perform some simple analyses of a proposed detector design that uses multiple short sections of superconducting nanowires to construct a new superconducting nanowire single photon detector (SNSPD). We refer to these short sections of nanowire as pixels and arrange them in a two dimensional grid in analogy with a standard CCD camera. We will discuss the potential advantages of such a system and the difficulties of the design.

When an incident photon strikes a Niobium nitride (NbN) nanowire, or other superconducting material such as NbTiN or a-W_xSi_{1-x} developed recently at NIST, it creates a resistive hot spot [Nam11]. This hot spot causes the current in the superconductor to deflect around the spot, thus increasing the current density in the wire. This increased current density leads to an increase in

the temperature of a small section of the wire. If the nanowire is held just below the critical current for superconduction, then the increase in heat will break the superconducting condition and the resistance of the wire will spike upward for a short time. This resistance spike creates a measurable current in the external resistance load and a photon is counted.

Present superconducting nanowire systems, such as NbN, have reasonably good counting efficiency [Dauler10], [Marsili11], by which we mean the probability of an incident photon being detected is over 25%. However, a significant problem exists with the number resolution, relaxation time, and fill factors [Gurevich87], [Dauler10], [Marsili11]. A detector consisting of a single wire can be made to cover a significant detection area by creating a meander. Usually this means folding the nanowire back and forth across the desired area of approximately 10 μm x 10 μm [Dauler10], [Marsili11]. This however is not a number resolving detector. All that the detector can feel is the loss of the superconducting condition somewhere in the nanowire. Should two photons strike the wire simultaneously in two different locations the current drop is very similar. One suggested solution to this lack of number resolving capability is to increase the number of wires in the meander. This has been done experimentally by Dauler et al [Dauler10]. While this approach improves on the single wire meander it still consists of long wires each of which occupies a significant portion of the active detection area (i.e. each nanowire in a 4 nanowire meander takes approximately 25% of the active area). In order to have a high probability of correctly detecting n number of photons one would need significantly more than n wires.

We proposed a detector design using short sections of wire, which we will refer to as pixels, that are arranged in a 2D grid to create the detection area. Such a design would use a large number of pixels thus giving high number resolution and the small size of the pixels gives short relaxation times. We call this configuration a multi-layer superconducting number-resolving photon detector. A significant problem with creating a two dimensional array of nanowire pixels is the question of how to attach the leads to each pixel, as the leads are of a similar size as the pixels themselves. One could simply move the pixels farther and farther apart to fit in all the necessary connections but this is impractical as the space between pixels does not detect photons and the device's overall efficiency would decrease below useful levels. Ideally the pixels will be packed as closely as possible, while still avoiding cross talk. This will maximize the so called fill factor, the ratio of the photon sensitive area to the non-sensitive area within the "active" area of the detector. We therefore propose moving away from the two dimensional approaches used to date

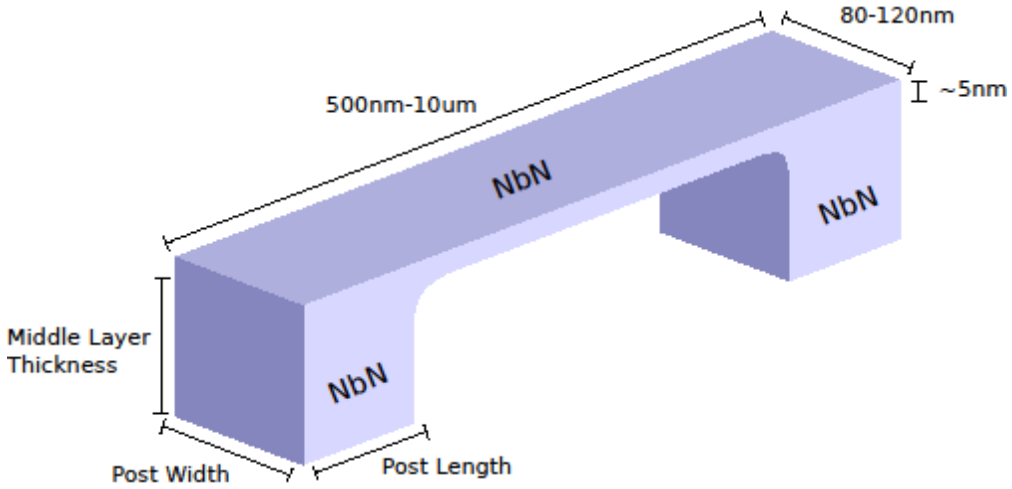


Figure 8. A single superconducting nanowire "pixel" bridge.

and instead suggest a multilayer, three dimensional architecture. In this scheme the non-superconducting leads are allowed to pass under the active detector pixels. To create this effect we shape the pixels like small bridges as seen in Figure 8. This shape was chosen because of its relatively simple design and in order to maximize the fill factor.

This creates a three layer design, with the bottom layer containing the leads, an insulating middle layer, and the active detection layer on top. We now show a bird's eye view (plan view) of the final device with all three layers aligned on top of each other, Figure 9. The black arrows show the movement of the current throughout the device.

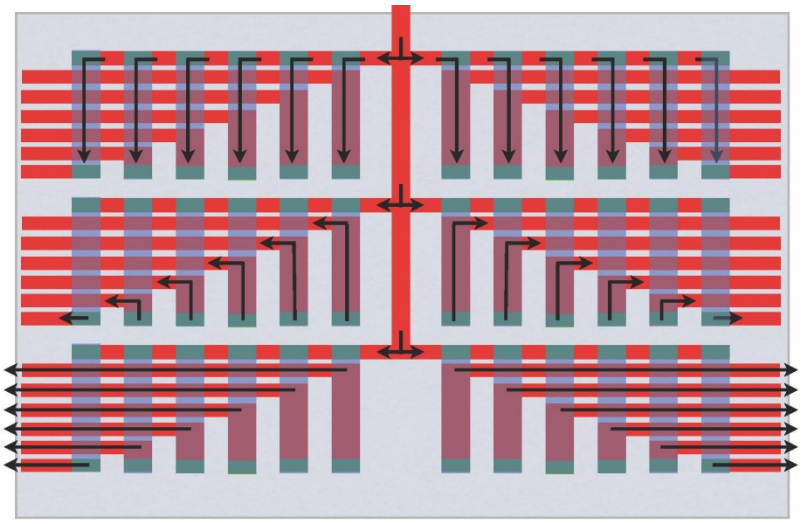


Figure 9. Plan view of final device with all three layers aligned on top of each other.

The current enters the detector in the bottom layer (red) through the shared input lead (center of figure). Current then moves up through the middle layer connections, called “posts" (green), to the top/detection layer. Once in the top layer it moves along the surface of the bridge (purple). This is the area in which an incident photon will form a resistance blockage. The current then moves back down to the bottom layer and is channeled out of the device by the output leads (red). Note that the leads (red) pass under the pixel bridges, between the posts and that the input/output leads are all on the same layer. The external detection electronics would then be similar industry standards. As a final aside each pixel can be wired as a completely independent circuit, but the number of leads will increase and counting simultaneous events between elements can become difficult.

3.3 Theory/experimental requirements of imperfect two-qubit linear optical photonic gates

Knill, Laflamme, and Milburn (KLM) significantly advanced the prospect of single-photon quantum computing in their seminal paper [Knill01], in which they overcame the need for nonlinear interactions by using the inherent nonlinearity of photon measurements. In this scheme, the computational system is combined with ancillary modes, and the gate operation is performed on the enlarged state space. The ancilla modes are measured with photon-number-resolving detectors, such as those described above leaving the computational modes undisturbed and in the desired output state provided the measurement is successful. In our previous work [Uskov10, Uskov09, Smith11], we have shown that a combination of analytical and numerical techniques may be used to design optimal linear optical transformations implementing two- and three-qubit entangling gates. Here we show results for non-ideal gates and suggest an experiment to test them.

The probabilistic nature of quantum measurement implies a trade-off between the success rate of the operation (the probability of obtaining the desired measurement outcome for the ancillary modes) and the fidelity (the overlap between the actual and desired states of the computational system when the ancilla measurement is successful). Previously, solutions were obtained that have the maximum possible ancilla measurement success probability given the constraint of perfect fidelity for a specified transformation [Uskov10, Uskov09]. In practical implementations, however, the goal of perfect fidelity may not always be desirable or even attainable. We have therefore generalized our previous techniques to the case of imperfect fidelity, and investigated the above-mentioned trade-off between the fidelity and success of the linear optical transformations. It was found that for sufficiently small deviations from perfect fidelity, a single optimization parameter determines the relationship between fidelity and optimal success rate [Smith11].

The input state to the experiment $|\Psi^{comp}\rangle x |\Psi^{ancilla}\rangle$ is a product of the computational state containing Mc photons in Nc modes, and an ancilla state containing Ma photons in Na modes. The Nc computational modes are those on which the actual gate is intended to act. Assuming dual-rail encoding, each qubit is represented by one and only one photon in two computational modes, so we have Mc = Nc=2. The ancilla state may in general be separable, entangled, or a maximally entangled or ebit state carrying spatially distributed entanglement [Wilde09], though

here we propose using only a product state of single-photon and zero-photon ancillas, which are relatively simple to produce in an experimental setting.

The linear optical device transforms the creation operator $a_i^{(in)\dagger}$ associated with each input mode i to a sum of creation operators $\sum_j U_{i,j} a_j^{(out)\dagger}$. Here U, which contains all physical properties of the device, is an N x N matrix, where N = Nc + Na is the total number of modes. The total input state may be written as a superposition of Fock states $|\Psi>=|n_1, n_{12}, \dots, n_N>$, where n_i is the occupation number of the i-th input mode, and $\sum n_i = M_c + M_a = M$ is the total number of photons. The input state is transformed as

$$|\Psi_{out}> = \Omega|\Psi_{out}>= \prod_{i=1}^{N} \frac{1}{\sqrt{n_i!}} \left(\sum_{j=i}^{N} U_{i,j}\, a_j^{(out)\dagger}\right)^{n_i}. \quad (1)$$

We note that Ω is a multivariate polynomial of degree M in the elements $U_{i,j}$. Once the transformation is complete, a measurement is applied to the Na ancillary modes. In the case of a number-resolving photon-counting measurement, $\langle\Psi_{measured}| = \langle K_{N_c+1}, K_{N_c+2}, \dots, K_N|$, where K_i is the number of photons measured in the i-th mode of the ancilla. The resulting transformation of the computational state is a contraction quantum map $|\Psi_{in}^{comp}\rangle = A|\Psi_{in}^{comp}\rangle / \||A|\Psi_{in}^{comp}\rangle\|$ [Kraus83], where A = A(U) is defined by,

$$A|\Psi_{in}^{comp}\rangle = \langle K_{N_c+1}, K_{N_c+2}, \dots, K_N|\Omega|\Psi_{in}\rangle. \quad (2)$$

The linear operator A, which maps computational input states to computational output states, contains all the information of relevance to the transformation. We define the fidelity as the probability that the desired target gate A^{Tar} has been faithfully implemented on the computational modes given a successful measurement of the ancilla modes:

$$F(A) = \frac{\left|Tr(A^\dagger A^{Tar})\right|^2}{2^{M_c} Tr(A^\dagger A)}, \quad (3)$$

since Tr $(A^{Tar\dagger}A^{Tar})=2^{M_c}$ for a properly normalized target gate. As we are interested in deviations from perfect fidelity, we define δ =1-F as our main parameter [Smith11].

We define the success rate of the ancilla measurement to be given by an average over all computational input states,

$$S(A) = \frac{Tr(A^\dagger A^{Tar})}{2^{M_c}\|U\|^{2M}}, \quad (4)$$

for general complex U. Note that U need not be unitary, as any matrix can be made unitary via the unitary dilation technique by adding vacuum modes [Knill02, uskov09]. We also note that the Hilbert-Schmidt norm $\langle A|A\rangle = Tr\,(A^\dagger A)/2^{M_c}$, used in our definition of S, is bounded above by the square of the operator norm, $\|A\|^2 = (\|A\|^{max})^2 = Max\left(\langle\Psi_{in}^{comp}|A^{Tar\dagger}A|\Psi_{in}^{comp}\rangle\right)$ and below by $(\|A\|^{min})^2 = Min\left(\langle\Psi_{in}^{comp}|A^{Tar\dagger}A|\Psi_{in}^{comp}\rangle\right)$ where the maximum and minimum are

taken over the set of properly normalized input states. In the limit F $\longrightarrow$1, $\|A\|^{max}/\|A\|^{min}\longrightarrow$1, and all definitions of the success rate coincide.

3.4 Nonlocality, entanglement witnesses and supra-correlations

While entanglement is believed to underlie the power of quantum computation and communication, it is not generally well understood for multipartite systems. Recently, it has been appreciated that there exists proper no-signaling probability distributions derivable from operators that do not represent valid quantum states. Such systems exhibit *supra-correlations* that are stronger than allowed by quantum mechanics, but less than the algebraically allowed maximum in Bell-inequalities (in the bipartite case). Some of these probability distributions are derivable from an entanglement witness *W*, which is a non-positive Hermitian operator constructed such that its expectation value with a separable quantum state (positive density matrix) ρ_{sep} is non-negative (so that Tr[$W\ \rho$]< 0 indicates entanglement in quantum state ρ). In the bipartite case, it is known that by a modification of the local no-signaling measurements by spacelike separated parties *A* and *B*, the supra-correlations exhibited by any *W* can be modeled as derivable from a physically realizable quantum state ρ. However, this result does not generalize to the *n*-partite case for $n>2$. Supra-correlations can also be exhibited in 2- and 3-qubit systems by explicitly constructing "states" *O* (not necessarily positive quantum states) that exhibit PR correlations for a fixed, but arbitrary number, of measurements available to each party. In this area of research we examined the structure of "states" that exhibit supra-correlations. In addition, we examined the affect upon the distribution of the correlations amongst the parties involved when constraints of positivity and purity are imposed. We investigated circumstances in which such "states" do and do not represent valid quantum states.

Physics imposes limits on the correlations that can be observed by distant (i.e. spacelike separated) parties. In particular, special relativity (SR) implies the principle of no-signaling (NS), that is, correlations cannot lead to any sort of instantaneous communication between spacelike separated observers. Quantum correlations may be stronger than classical, and their violation of Bell inequalities (BI) [Bell64] suggests that quantum mechanics (QM) cannot be regarded as a local realism theory. Tsirelson [Tsirelson80] showed that there is an upper bound to the violation of BI, which implies that the amount of non-locality allowed by QM is limited. Popescu and Rohrlich (PR) showed [Popescu94] that there exists a broad class of no-signaling theories which allow stronger-than-quantum or supra-quantum correlations. PR developed a valid joint probability distribution whose violations of the BI lie above those of physical quantum correlations and below the allowed algebraic maximum of the BI (the latter are called PR-Boxes). Thus, the principle of NS imposed by SR does not single out QM from these other post-quantum NS theories [Masanes06] (PQNS).

These PQNS have much in common with QM such as no-cloning, information-disturbance tradeoffs, security for key distribution, and others. Recently, van Dam [van Dam05] showed that PR-Boxes make communication complexity trivial, which is not the case within QM. Other researchers have shown that PQNS theories would lead to implausible simplification of distributed computational tasks (see [Pawlowski09] and references therein). It is now widely believed that theories in which communication/computational complexity is trivial are very unlikely to exist. It is therefore important to understand the structure of the PQNS and ultimately

to find physical and informational principles that rule them out. In this area of research we took steps in that direction by investigating the structure of PR correlations by forming operators which reproduce these PR probability distributions. We investigated circumstances in which they do and do not represent valid quantum states.

Bell Inequalities (BI)

Nonlocality is expressed by means of violations of Bell inequalities[1] (BI) which set upper bounds for classical correlations arising from local-realistic theories. For bipartite systems, the most well know BI is the Clauser-Horne-Shimony-Holt (CHSH) inequality[7] defined as follows. Consider a bipartite system A⊗B, for Alice and Bob, each possessing measurement directions A,B =A and C,D =B taking measurement values $a,b,c,d = \{\pm 1\}$. We define the correlation $E(AC)$ between A=A and C=B as

$$\begin{aligned} E(AC) &\equiv \langle AC \rangle = \sum_{a,c=\{\pm 1\}} a\,c\,P(a,c \mid A,C) \\ &= P(+,+ \mid A,C) + P(-,- \mid A,C) - P(+,- \mid A,C) - P(-,+ \mid A,C) \end{aligned} \tag{5}$$

In (5), we define $P(a,c|A,C)$ as the joint probability that given the (input) measurement directions A for Alice and C for Bob, Alice obtains the (output) measurement result a and Bob obtains the value b, subject to the normalization condition $\sum_{a,c=\{\pm 1\}} P(a,c \mid A,C) = 1,\ \forall A,C.$ Finally, we define the following CHSH correlation parameter S by

$$S \equiv E(AC) + E(BC) + E(BD) - E(AD). \tag{6}$$

S has been cleverly constructed as the expectation value of the quantity Arg≡$A(C\text{-}D) + B(C+D)$. If A,B,C,D are classical random variables taking values ± 1 then it can be readily seen that if (i) $C=D$, then |Arg| = $|B(2C)| = 2$ and if (ii) $C=\text{-}D$, |Arg| = $|A(2D)| = 2$. Thus, for classical correlation we have the CHSH inequality

$$\text{CHSH inequality:}\quad |\, S = E(AC) + E(BC) + E(BD) - E(AD) \,| \le S_{Cl} = 2 \tag{7}$$

(where the subscript "Cl" denotes "classical"). For a large class of measurement directions (but not all), quantum states can violate the CHSH inequality (i.e. |S|>2) up to a maximum value shown by Tsirelson [Tsirelson80] to be $S_Q = 2\sqrt{2}$. Here, a *quantum state* is defined as a positive (i.e. non-negative eigenvalues) Hermitian matrix with unit trace denoted by the symbol ρ. The archetypical example is the singlet (Bell) state

$$\rho_{\text{singlet}} = \left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right)/\sqrt{2} \equiv \left(|01\rangle - |10\rangle\right)/\sqrt{2} \tag{8}$$

with measurement directions in the x-y plane: $A = \hat{x}, B = \hat{y}, C = (\hat{x}+\hat{y})/\sqrt{2}, D = (\hat{x}-\hat{y})/\sqrt{2}$ that saturates the Tsirelson bound with $S = -S_Q = -2\sqrt{2}$. This is a manifestation of the stronger than classical correlations that can be exhibited by quantum states. (Note: quantum states with measurement

directions such that the CHSH inequality is satisfied, i.e. $S \leq 2$, are not distinguishable from classical states by the correlation parameter S).

It is instructive to note that the CHSH inequality in (7) can be derived [Schumacher91] as a statement of a classical quadrilateral inequality for the *correlation metric* $\Delta(AC) = 1 - E(AC) = P(+,-|A,C) + P(-,+|A,C) \geq 0$. Substituting this expression into (7) yields $\Delta(AC) + \Delta(BC) + \Delta(BD) \geq \Delta(AD) \Rightarrow S \equiv E(AC) + E(BC) + E(BD) - E(AD) \leq +2$ (see Figure 10). Thus, the

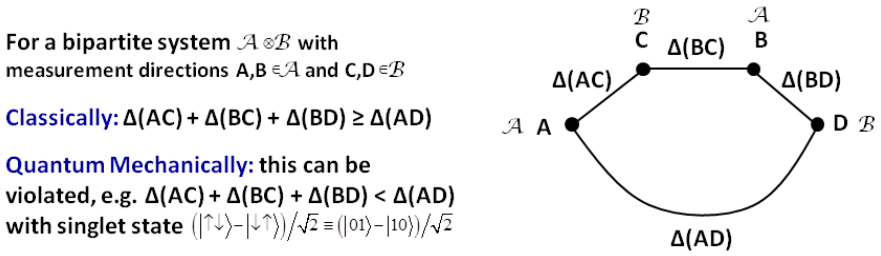


Figure 10. CHSH inequality derived as a violation of the classical quadrilateral inequality.

violation of the CHSH inequality by quantum states can be interpreted as a violation of the classical quadrilateral inequality which, for certian measurement directions, yields the distance $\Delta(AD)$ via the direct path *A-D* to be *smaller* than the sum of the distances around the indirect path *A-C-B-D*.

Returning to the CHSH inequality (7), one notes that it is bounded by the algebraic maximum $|S| \leq S_{AM}=4$. This follows from the fact that the correlations E are bounded by $|E| \leq 1$. This latter result can be inferred by writing $E = P_{++} + P_{--} - (P_{+-} + P_{-+}) = 2(P_{++} + P_{--}) - 1 = 1 - 2(P_{+-} + P_{-+})$, where $= P_{++} + P_{--} + P_{+-} + P_{-+} = 1$ has been used. Using the fact that $0 \leq P_{++} + P_{--} \leq 1$ and $0 \leq P_{+-} + P_{-+} \leq 1$ in the previous two expressions for E, yields the desired bound $|E| \leq 1$. Therefore, if the first three correlations in (7) take the value ± 1 and the last correlation takes the value ∓ 1, we obtain $S = \pm 4$. The implication of this observation is that the regime $2\sqrt{2} \leq S \leq 4$ represents *supra-correlations* that are stronger than quantum, yet are unphysical by Tsirelson's bound, i.e. cannot be realized by any physical quantum state. The salient question to study is what 'natural' principles determine the exclusion of such supra-correlations. As a first hypothesis, one might surmise that the principle of *no-signaling* from special relativity (i.e. that information cannot be instantaneously broadcast between spacelike separated observers) might exclude supra-correlations. Surprisingly, this is *not* the case. In 1994, Popescu and Rohrlich (PR) [Popescu94] were able to construct a valid joint probability distribution between a pair of spacelike separated observers that (i) satisfies the non-signaling principle, and (ii) yields the algebraic maximum correlations allowed by the CHSH inequality. Here the adjective 'valid' implies that the joint probability distribution, and all its derived marginal probability distributions, obtain values between 0 and 1, and satisfy the appropriated normalization requirements (i.e. the joint and all marginal probability distributions summed over all outcomes for any measurement settings yields unity). These correlations are now called *PR correlations*, which we describe in the next section.

No Signaling (NS) Theories and PR Correlations

We wish to consider correlations between n spacelike separated parties (observers) $A_1,\ldots,A_n$, who can perform m possible measurements $x_1,\ldots,x_n$ ($x_i=\{0,1,\ldots,m\text{-}1\}$), with r possible outcomes $a_1,\ldots,a_n$ ($a_i=\{0,1,\ldots,r\text{-}1\}$) The observed correlations will be described by the joint probability distribution $P(a_1,a_2,\ldots,a_n \mid x_1,\ldots,x_n)$ giving the probability that the parties obtain the measurement values (outputs) $a_1,\ldots,a_n$ when their local measurement apparatuses (inputs) are set to $x_1,\ldots,x_n$. The joint probability distribution is constrained only by the conditions $0 \le P(a_1,a_2,\ldots,a_n \mid x_1,\ldots,x_n) \le 1$ and the normalization condition $\sum_{a_1,\ldots,a_n} P(a_1,a_2,\ldots,a_n \mid x_1,\ldots,x_n) = 1$ for all measurement settings $x_1,\ldots,x_n$.

Imposing the no-signaling (NS) constraint, i.e. adherence to the requirement from special relativity that spacelike separated measurements should not influence each other due to the finite speed of light (communication), requires that the marginal probability distributions satisfy the additional condition

$$\text{No Signaling: } P(a_1,a_2,\ldots,a_k \mid x_1,\ldots,x_n) \equiv \sum_{a_{k+1},\ldots,a_n \in \{0,1\}} P(a_1,\ldots,a_n \mid x_1,\ldots,x_n) = P(a_1,a_2,\ldots,a_k \mid x_1,\ldots,x_k). \quad (9)$$

Here, the first equality in (9) formally defines the marginal probability distribution describing the measurement outcomes of the first k parties, when the last n-k outcomes are un-observed and hence summed over. Note, this marginal probability distribution $P(a_1,a_2,\ldots,a_k \mid x_1,\ldots,x_n)$ formally depends on all n measurement settings. The last equality in (9) imposes the NS constraint requiring that the marginal probability depends *only* upon the k measurement settings of the parties participating in the joint measurement (and not on the remaining n-k measurement setting of the unobserved outcomes).

As first pointed out by Pospescu and Rohrlich [Popescu94], the NS constraint (9) by itself does not single out classical and quantum theories, i.e. $|S| \le S_Q$. PR proposed the following joint probability distribution for two parties (Alice and Bob) with two measurement settings (inputs) $x,y = \{0,1\}$, and two measurement outcomes (outputs) $a,b = \{0,1\}$ given by

$$\text{PR Box: } P(a,b \mid x,y) = \begin{cases} 1/2 & \text{if } a \oplus b = x \cdot y \\ 0 & \text{otherwise} \end{cases}. \quad (10)$$

By considering all possible inputs and outputs, it is straightforward to show that PR correlations of (10) satisfy all the requirements for a NS theory as follows: normalization (total probability)

$$
\begin{aligned}
&\sum_{a,b=\{0,1\}} P(a,b\,|\,x,y) \\
&= \underbrace{P(0,0\,|\,x,y)+P(1,1\,|\,x,y)}_{a\oplus b=0}\ \underbrace{+P(0,1\,|\,x,y)+P(1,0\,|\,x,y)}_{a\oplus b=1}, \\
&= \quad (1/2 \ + \ 1/2)\ \delta_{0,x\cdot y} + (1/2 \ + \ 1/2)\ \delta_{1,x\cdot y}, \\
&= \quad \delta_{0,x\cdot y} + \ \delta_{1,x\cdot y}, \\
&= \quad 1 \quad \forall x,y,
\end{aligned}
\tag{11}
$$

and the NS constraint

$$
\begin{aligned}
&P(a\,|\,x,y) \equiv \sum_{b=\{0,1\}} P(a,b\,|\,x,y) \\
&= \ \underbrace{P(a,0\,|\,x,y)}_{a\oplus b=a\oplus 0=a} \ + \ \underbrace{P(a,1\,|\,x,y)}_{a\oplus b=a\oplus 1\equiv \bar{a}} \\
&= \quad 1/2\ \delta_{a,\,x\cdot y} + 1/2\ \delta_{\bar{a},\,x\cdot y}, \\
&= \quad \begin{cases} 1/2+0 \ (\text{if } a=0 \,\&\, x\cdot y=0),\ 0+1/2\,(\text{if } a=0 \,\&\, x\cdot y=1) \\ 0+1/2 \ (\text{if } a=1 \,\&\, x\cdot y=0),\ 1/2+0\,(\text{if } a=1 \,\&\, x\cdot y=1) \end{cases}, \\
&= \quad 1/2 \quad \forall a,x,y, \\
&= \quad P(a\,|\,x)\ \forall a,x \quad (\Rightarrow \textit{Isotropic}, \text{ i.e. } P(a\,|\,x)=1/2 \text{ indep of } a,\, x).
\end{aligned}
\tag{12}
$$

With the PR Box define above in (10) we can compute correlations as

$$
\begin{aligned}
E(a,b\,|\,x,y) &= \underbrace{P(0,0\,|\,x,y)+P(1,1\,|\,x,y)}_{a\oplus b=0}\ \underbrace{-P(0,1\,|\,x,y)-P(1,0\,|\,x,y)}_{a\oplus b=1}, \\
&= \quad (1/2 \ + \ 1/2)\ \delta_{0,x\cdot y} - (1/2 \ + \ 1/2)\ \delta_{1,x\cdot y}, \\
&= \begin{cases} +1 \ \text{ if } \ x\cdot y=0, \ \text{i.e.}(x,y)\in\{(0,0),\,(0,1),\,(1,0)\}, \\ -1 \ \text{ if } \ x\cdot y=1, \ \text{i.e.}(x,y)=(1,1), \end{cases}
\end{aligned}
\tag{13}
$$

where we have used $E(a,b\,|\,x,y)=\sum_{a',b'\in\{\pm1\}} a',b'\,P(a,b\,|\,x,y)$, where $a'=1-2a$ $(b'=1-2b)$ associates the measurement values $a'(b')\in\{+1,-1\}$ with the measurement value labels (bits) $a\,(b)\in\{0,1\}$, respectively. Therefore, in Figure 10, assigning Alice's measurement directions *A,B* =A the bit labels x_A=1 and x_B=0, and Bob's measurement directions *C,D* =B the bit labels y_C=0 and y_D=1, and using (6) yields the algebraic maximum S_M=4 of the CHSH inequality, as illustrated in Figure 11.

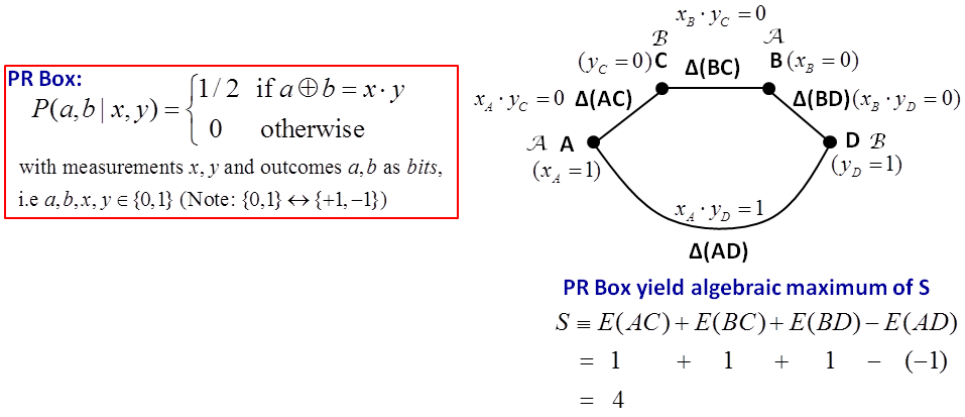


Figure 11. PR Box with joint probability distribution achieving the algebraic maximum S_M=4 of the CHSH inequality.

Since S_M=4>S_Q=2√2, no quantum (i.e. physically realizable) state can reproduce the above PR probability (10). However, the following "state" [Acin10] $O=\alpha_+\left|\Phi^+\right\rangle\left\langle\Phi^+\right|+\alpha_-\left|\Phi^-\right\rangle\left\langle\Phi^-\right|$ with $\alpha_\pm=(1\pm\sqrt{2})/2$ and Bell states $\left|\Phi^\pm\right\rangle=(\left|00\right\rangle\pm\left|11\right\rangle)/\sqrt{2}$, yields the PR probability (10) through the usual trace rule $P_{PR}(a,b\,|\,x,y)=Tr[O\,M_a^x\otimes M_b^y]$ with $\{M_a^{x_A},M_a^{x_B}\}=\{\sigma_2,\sigma_1\}$ and $\{M_b^{x_C},M_b^{x_D}\}=\{(\sigma_1+\sigma_2)/\sqrt{2},(\sigma_1-\sigma_2)/\sqrt{2}\}$, where $\{\sigma_i\}_{i\in\{1,2,3\}}$ are the usual Pauli matrices. Note that the form of the joint measurement between Alice and Bob written as a pure tensor product of local observables $M_a^x\otimes M_b^y$, ensures the locality of the spacelike separated measurements, which cannot increase entanglement between the parties. A measurement involving the sum of pure tensor products, such as $M_a^x\otimes M_b^y+M_a'^x\otimes M_b'^y$ which might possibly create entanglement, would involve non-local measurements between the parties, which could only be physically realized if the parties were brought together. The important point is that *O* does not represent a physical quantum state since it is non-positive, i.e. it possesses the negative eigenvalue $\alpha_-=(1-\sqrt{2})/2$. Henceforth, we shall refer to non-positive, unit trace Hermitian operators *O* capable of producing NS probability distributions as "states," and reserve the specific term "quantum state" or "q-state" for the physically realizable positive, unit trace Hermitian operators denoted as ρ≥0, (i.e. density matrix).

Following Acin *et al*. [Acin10] we desired to investigate all sets of *n*-party spacelike correlations in terms of local quantum observables (measurements) $M_{\text{non-sig}}=M_{a_1}^{x_1}\otimes\cdots\otimes M_{a_n}^{x_n}$ that ensure NS. These correlations can be written in the form

$$P_O\equiv P_O(a_1,\ldots,a_n\,|\,x_1,\ldots,x_n)=Tr[O\,M_{a_1}^{x_1}\otimes\cdots\otimes M_{a_n}^{x_n}]. \tag{14}$$

Without loss of generality, we can take the local measurement operators $M_a^x=\Pi_a^x=\left|a\right\rangle_x\left\langle a\right|$ to be the projection operators onto "spin-component" *a* in the "direction" *x*. Requiring that proper probabilities be derived from *all* local quantum measurements imposes the condition that O be positive on *all* product states. This implies that *O*=*W* is an entanglement witness (EW, see

[Guhne09]) with the property $\langle \alpha, \beta, \ldots | W | \alpha, \beta, \ldots \rangle \geq 0.$ Here some definition are helpful. A q-state is separable (contains only classical correlations) if it is of the form $\rho^{sep} = \sum_i p_i \rho_i^{A_1} \otimes \rho_i^{A_2} \otimes \cdots \otimes \rho_i^{A_N}$ where each $\rho_i^{A_1}$ is a local density matrix and $\sum_i p_i = 1.$ (If a q-state is not separable, it is entangled). Each local density matrix has a (non-unique) ensemble decomposition $\rho_i^{A_k} = \sum_j p_{ij}^k \left| \psi_{ij}^k \right\rangle \left\langle \psi_{ij}^k \right|$ where $\sum_j p_{ij}^k = 1.$ The requirement that W is positive on all product states $\langle \alpha, \beta, \ldots | W | \alpha, \beta, \ldots \rangle \geq 0$ ensures that $Tr[\rho^{sep} W] \geq 0$ from the form of ρ^{sep}. A q-state ρ such that $Tr[\rho W] < 0$ is then entangled (since it is not separable), and *W* is said to "witness" (or exhibit) the entanglement of ρ. Note that *W* is in general a non-positive Hermitian operator. In the context of (10), we now consider $O \rightarrow W$ as a state (not necessarily a q-state) from which to derive NS correlations through the joint probability distributions

$$P_W \equiv P(a_1, \ldots, a_N \mid x_1, \ldots, x_n) = Tr[W M_{a_1}^{x_1} \otimes \cdots \otimes M_{a_n}^{x_n}] \geq 0. \tag{15}$$

The correlations (4) are termed *Gleason correlations* by Acin *et al*. [Acin10].

The subtle distinction between (14) and (15) is that the latter produces positive probabilities for *all* local NS measurements, while the former may produce non-negative probabilities on only a *subset* of NS measurements. This distinction is important since it has been shown [Guhne09, Barnum10] that for bipartite systems *n*=2, any Gleason correlation $P(a_1, a_2 \mid x_1, x_2) = Tr[W M_{a_1}^{x_1} \otimes M_{a_2}^{x_2}] \geq 0$ can be converted to a probability distribution derived from a q-state $\rho_{|\Phi_{PB}\rangle} = \left| \Phi_{PB} \right\rangle \left\langle \Phi_{PB} \right|$ with modified measurements $P(a_1, a_2 \mid x_1, x_2) = Tr[W M_{a_1}^{x_1} \otimes M_{a_2}^{x_2}]$ $= Tr[\rho_{|\Phi_{PB}\rangle} M_{a_1}^{x_1} \otimes \bar{M}_{a_2}^{x_2}] \geq 0.$ Here $|\Phi_{PB}\rangle$ is any pure bipartite state (not necessarily maximally entangled). The proof relies on the explicit use of the Choi-Jamiolkowski isomorphism (CJI) [Guhne09, Barnum10, Vedral97] which allows any bipartite (*n*=2) witness *W* to be written as $W^{(n=2)} \equiv (I \otimes \Lambda)(\rho_{|\Phi_{PB}\rangle})$, where Λ is a positive trace preserving map. In the above, $\bar{M}_{a_2}^{x_2} = \Lambda^*(M_{a_2}^{x_2})$ where Λ^* is the adjoint of the map Λ, i.e. $\mathrm{Tr}[\mathrm{A}\,\Lambda(B)] = \mathrm{Tr}[\Lambda^*(A)\,B].$ The proof then follows directly as

$$\begin{aligned} &P_W(a,b \mid x,y) = Tr[W M_a^x \otimes M_b^y] = Tr[(I \otimes \Lambda)(\rho_{|\Phi_{BP}\rangle}) M_a^x \otimes M_b^y] \\ &= Tr[M_a^x \otimes M_b^y (I \otimes \Lambda)(\rho_{|\Phi_{BP}\rangle})] = Tr[M_a^x \otimes \Lambda^*(M_b^y)\, \rho_{|\Phi_{BP}\rangle}] = Tr[\rho_{|\Phi_{BP}\rangle} M_a^x \otimes \bar{M}_b^y)], \end{aligned} \tag{16}$$

where the second equality uses the CJI, the third equality uses the cyclic property of the trace, the fourth inequality utilizes $I \otimes \Lambda$ acting to the left on the tensor product measurements $M_a^x \otimes M_b^y$ thereby introducing the adjoint Λ^* operation and the modified local measurement operation $\bar{M}_{a_2}^{x_2} = \Lambda^*(M_{a_2}^{x_2})$ in the last equality. Acin *et al*. [Acin10] point out that the CJI decomposition $W^{(N=2)} \equiv (I \otimes \Lambda)(\rho_{|\Phi_{PB}\rangle})$ in general fails for *n*>2 (which they demonstrate by a specific example). Thus, the Gleason correlations (4) are strictly larger ($|S| > S_Q$) than quantum correlations for n>2

(and equivalent only for $n \leq 2$). The state $O = \alpha_+ \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \alpha_- \left|\Phi^-\right\rangle\left\langle\Phi^-\right|$ used in the example of PR correlations in the discussion after Figure 11 is *not* an EW since it can produce negative probabilities for measurements other than those considered (it would be an EW if it produced positive probabilities for *all* measurement choices). Acin *et al.* [Acin10] classify the distributions $P(a_1,\ldots,a_n \mid x_1,\ldots,x_n)$ as (i) *No-Signaling* if and only if *P* can be written in the form of (14), (ii) *Quantum* whenever *O* is positive ($O \geq 0$), and (iii) *Local* if and only if *O* corresponds to a separable quantum state. In the following, we investigate the NS correlations of (10) and the conditions for which they become either Gleason, or Quantum correlations.

4.0 RESULTS AND DISCUSSION

4.1 Multipli-entangled photons from a spontaneous parametric down-conversion source

Experimental analysis and testing apparatuses for Schioedtei are very similar to that for any SPDC source. With the more complex ring pattern generated though there are modifications one must do to the standard detection scheme. The experimental configuration for Schioedtei is shown in Figure 12. The testbed consists of a violet (405 nm) femtosecond pulsed pump source (Millenia PRO 15sJ > Tsunami 3960-15HP > Inspire Blue FM) with an average power of ~1.4 W, ~100 femtosecond pulses and a repetition rate of 80 MHz. The 405 nm pulses first pass through a ~12.5 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 before entering Schioedtei. Proper alignment of the crystal was accomplished with live images from a cooled CCD camera (Princeton Instruments Pixis 1024BR). The photons were collected in free space collimators located 1.5 meters behind Schioedtei. This distance is the minimum amount required to obtain the useable spatial separation required for detector access to the middle blue diamond of intersection points (5, 6, 7, and 8). The post-compensating crystals, inserted in the down-converted photon paths, are 8x8x1 mm type II phase matched β-BBO (at angles of $\theta = 41.9°$ and $\varphi = 30°$) as Schioedtei's orientation is non-collinear and there is no interaction between the pump and the compensators. 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. Photon collection was accomplished via fiber coupled collimators immediately

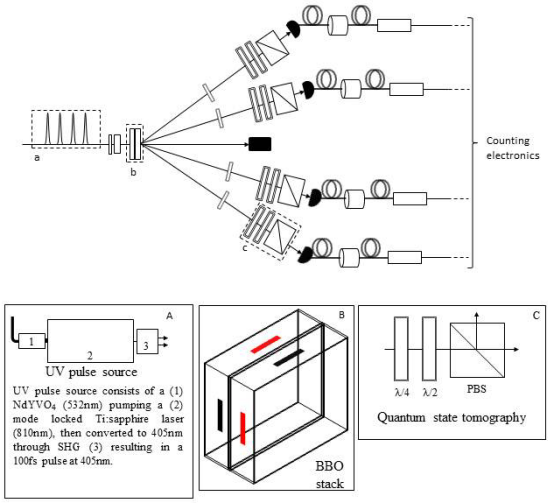


Figure 12. Experimental testbed to analyze the Schioedtei source.

followed by 2 nm bandpass filters. The output of the bandpass filter was routed directly into fiber-coupled single photon counting avalanche photodiodes (APDs) (Perkin Elmer SPCM-AQ4C). Coincidence detection was accomplished by a four channel coincidence counting module (CCM) [Branning11].

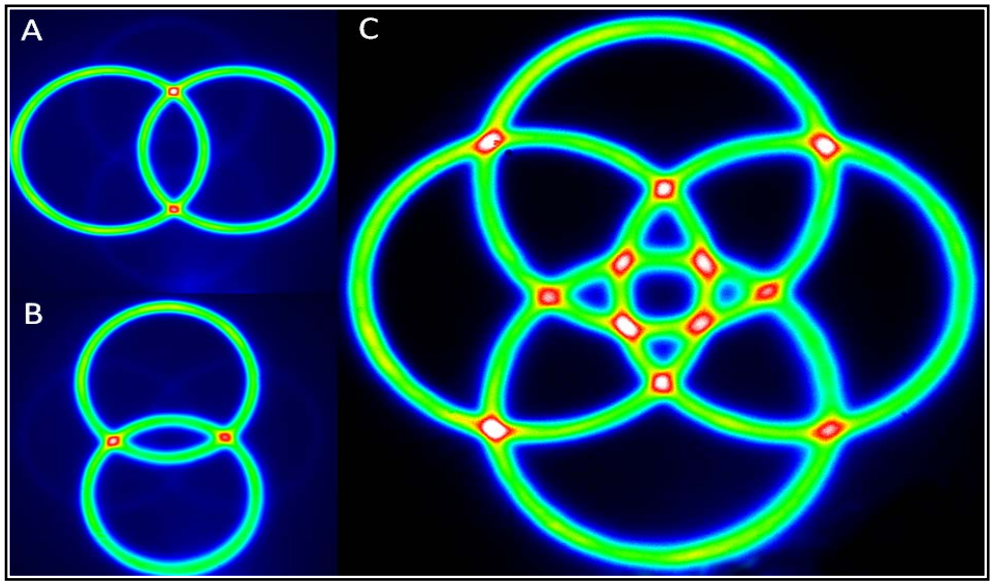


Figure 13. False color CCD images of custom crystal assembly (1 sec exposure). A,B are the type II non-collinear outputs from each individual crystal. C is the combined output from the crystal stack.

A trio of false color CCD camera images of Schioedtei output is shown in Figure 13. 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 alignment image in Figure 13 is

utilized for aligning the proper orientation of the rings while a back propagated beam shown in Figure 14 aligns the collimators to the intersection points.

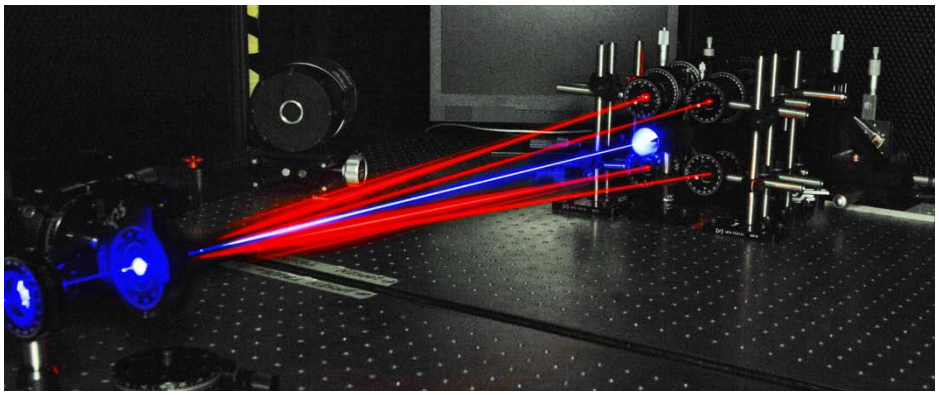


Figure 14. Alignment image of the Schioedtei crystal stack.

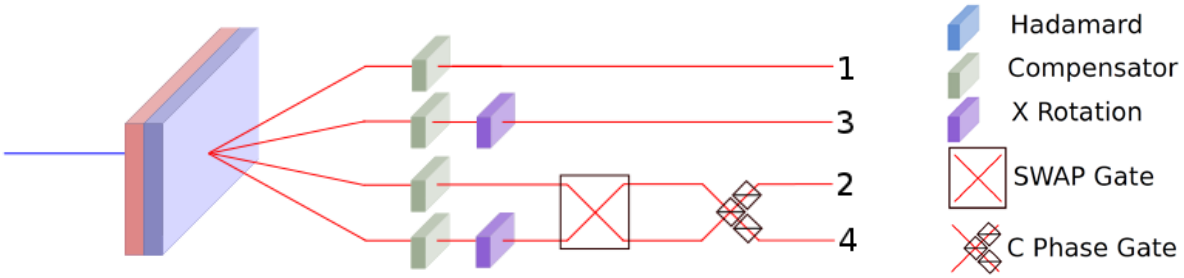
As stated, Schioedtei was constructed from β-BBO though any type II material can be used. Materials such as BiBO (Bismuth Borate, BiB_3O_6) have been shown to have a higher photon generation rate than β-BBO [Rangarajan09] and this will be the next step for Schioedtei. Secondly, increasing the useable photon count rate in Schioedtei can be accomplished by factoring the GVM phase matching constraint [U'Ren06] into the crystal construction. A GVM-matched configuration [Fanto10] is possible by alternating reduced thickness Schioedtei and α-BBO layers. α-BBO can be used as a compensator since there is no second order nonlinear effect in α-BBO crystal due to the centric symmetry in its crystal structure. Such a GVM source would provide the same up to six spatially separate entangled pairs as Schioedtei, while alleviating 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.

Schioedtei source uses and applications

Another applicable area of extreme interest is in the generation of photon-based cluster states. Cluster states play a central role in the measurement-based one-way quantum computation approach [Walther05, Raussendorf01]. In this scheme, the entanglement resource is provided in advance through an initial, highly entangled multi-qubit 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]. Figure 15 illustrates a scheme for utilizing the output of Schioedtei to generate a four photon cluster state, $|C\rangle_4$ [Schmid07]. This particular example employs the spots 1,2,3,4 and requires insertion of two half-wave plates, a SWAP gate 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.

More complex cluster states can be constructed from Schioedtei with additional hardware. This includes, but is not limited to, the construction of box cluster states [Prevedel07, Walther05]. In

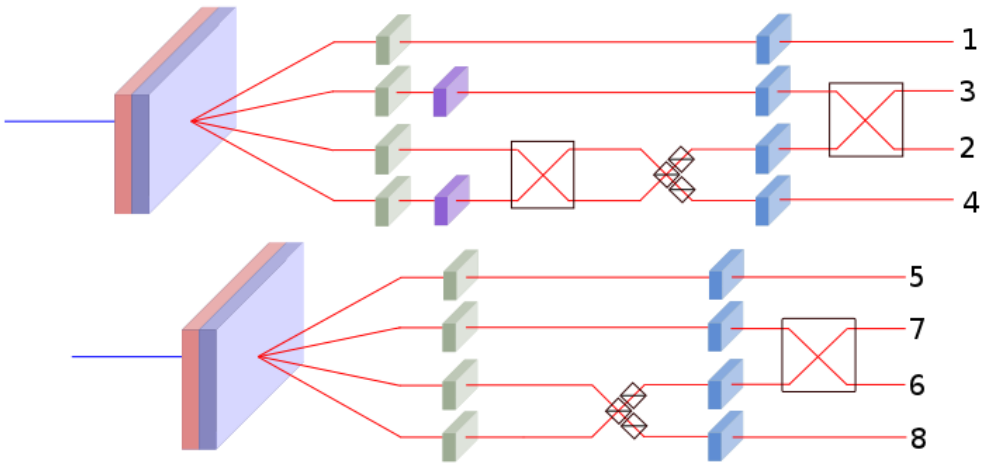
fact Schioedtei is capable of producing two 4-qubit box states simultaneously by using eight of the spots: 1,2,3,4 and 5,6,7,8. As the states Schioedtei outputs at these two sets of spots are different,



$|C\rangle_4 = \frac{1}{2}(|HHHH\rangle_{1,2,3,4} + |HHVV\rangle_{1,2,3,4} + |VVHH\rangle_{1,2,3,4} - |VVVV\rangle_{1,2,3,4})$

Figure 15. Experimental setup for 4-qubit cluster state generation utilizing Schioedtei.

slightly different preparation methods are required for the two boxes, as shown in Figure 16. After the preparation is complete the two box states are completely equivalent. With additional preparation and resource photons these states can be used as the building blocks of larger states such as the 6-qubit butterfly network [Ma10, Soeda10].



$|\psi\rangle_{BOX} = \mathrm{Swap}_{2,3}\ \mathrm{H}_1\mathrm{H}_2\mathrm{H}_3\mathrm{H}_4\ \mathrm{CZ}_{2,4}\ \mathrm{Swap}_{2,4}\ \mathrm{X}_3\mathrm{X}_4|\psi\rangle_{1,2,3,4}$

$|\psi\rangle_{BOX} = \mathrm{Swap}_{6,7}\ \mathrm{H}_5\mathrm{H}_6\mathrm{H}_7\mathrm{H}_8\ \mathrm{CZ}_{6,8}|\psi\rangle_{5,6,7,8}$

Figure 16. Experimental construction of a 4-qubit box cluster state utilizing Schioedtei.

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 $|HV\rangle \pm e^{i\varphi}|VH\rangle$ along with the generation of the state $|HH\rangle \pm e^{i\varphi}|VV\rangle$ with the addition of a half-wave plate. In addition, separable states such as $|HV\rangle \pm e^{i\varphi}|VV\rangle$ or $|HV\rangle \pm e^{i\varphi}|HH\rangle$ can also be

directly generated with clever combinations of the twelve output intersections and proper compensation.

4.2 A multi-layer three dimensional superconducting nanowire photon detector

General amplitude amplification

We now take a closer look at the minimum three layers needed to create the device, shown in Figure 17. The bottom layer 17a, consists of non-superconducting leads (red)placed on an

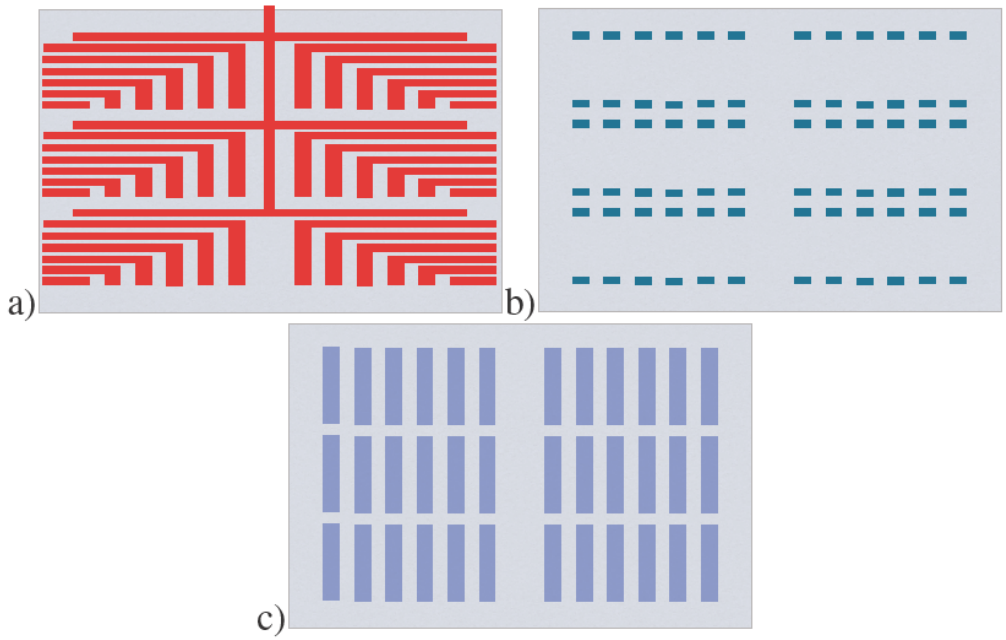


Figure 17 A plain view of the three layers in the multilayer design.

insulating substrate (gray), such as R-plane sapphire, MgO or Si. Note that there is no complete circuit on this level, so the current will be forced to move up to the next level. The optimal minimal spacing will depend on the insulating ability of the substrate to prevent leakage and crosstalk, mainly between the input and output channels but also with the superconducting nanowires passing above. Over the bottom layer will be a second layer of deposited substrate 17b. This layer will then have vias, i.e. holes (green), which pass completely through it (gray) at predetermined locations so as to hit the input/output leads in the bottom layer. These vias are filled with superconducting material (in practice it may be advantageous to use non-superconducting material here, if the pixels are long enough to avoid the latching condition) thus completing the middle layer of the device. Alignment will be a very important, but not insurmountable issue, as these structures are on the scale of approximately 100 nm in width and current alignment techniques can achieve results on the order of 1 nm [Anderson04]. Finally the detection layer Figure 17c, will be deposited on top of the middle layer. Alignment of the superconducting bridges with the vertical “posts” in the middle layer will be important for the overall detection efficiency [Kerman07].

The device will have significantly higher number resolution, while maintaining a useful detection area. It has several parameters which can control the reset time to avoid latching while still minimizing the rest time. An array of pixels of arbitrary number, size and shape is possible. Most of the detector will remain active after a single photon is absorbed as opposed to small number or single meander detectors which are effectively blinded by a single photon. The active area of the detector can be tuned by changing the number or the shapes of the pixels. These advantages are compelling theoretical evidence for the construction and testing of multi-layer superconducting number-resolving photon detectors.

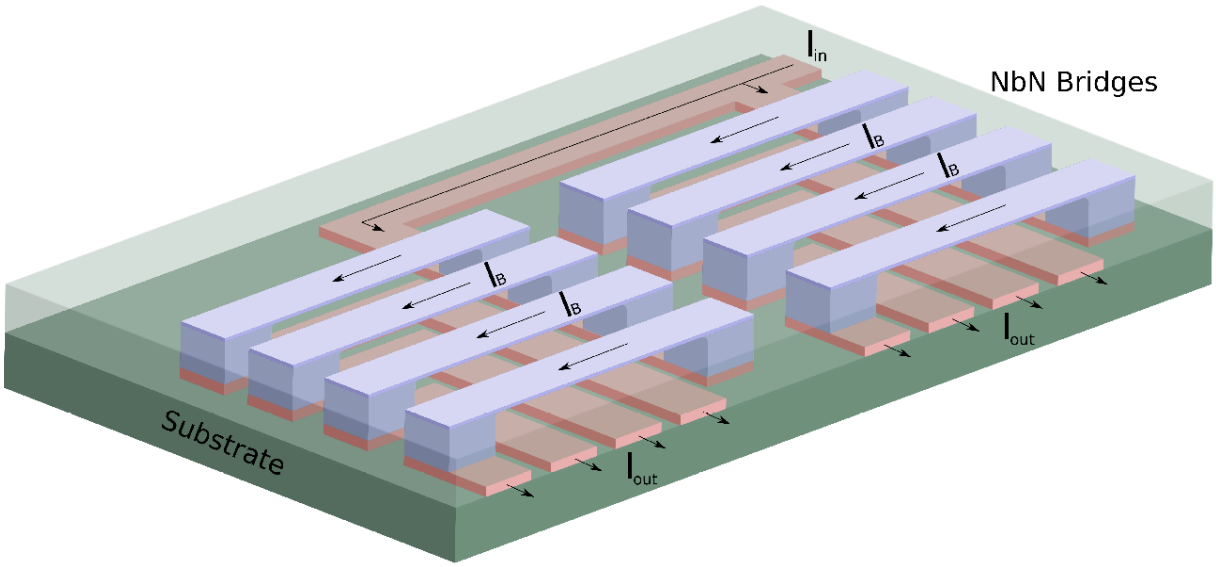


Figure 18 A toy model of a multi-layer SNSPD.

Figure 18 shows a toy model of a working multi-layer SNSPD. For clarity only the super-cooled part of the chip is shown. The dark green substrate and red leads are similar to the grey substrate and red leads in Figure 17a. The blue vertical posts are shown in a semi-transparent middle layer similar to Figure 17b for clarity. The blue superconducting pixels on the surface are similar to Figure 17c. The development of this design has resulted in two patents filled by the AFRL JAG officer with the U.S. patent office.

4.3 Laboratory upgrade and ongoing research in integrated waveguide quantum circuits

The Quantum Information Science Laboratory originally located in lab 18 in Bldg. 104 was relocated to a larger facility in Bldg. 3 Suite I5. The transition to the new facility allowed for the addition of 2 more optical tables, multiple work benches and equipment storage cabinets. The facility is partitioned in two separate work areas defined by laser curtains allowing separate experiments to be conducted concurrently with lasers of class 4 or lower. During this period the Ti:Sapphire laser was upgraded from a femtosecond 1.5 W system to a femto/picosecond 3.5-4 W system. Additionally installed were both femtosecond and picosecond second harmonic generation units (SHG) were added to the system to generate powers greater than 1 W in the blue/violet regime. These additions completed the upgrade to the entangled photon generation testbed.

Further effort has been placed to reduce the footprint size of quantum gates/circuits built from bulk optical components. This added research focuses on the use of integrated optical waveguides to construct the quantum gates/circuits. The direction of the research exploits two arenas: (i) world class domestic researchers at Rome Research Site and WPAFB along with universities such as Columbia, MIT and RIT, and (ii) and world class international researchers through EOARD at universities such as Bristol, Oxford and Vienna. Expanding the ongoing research in optical waveguides was a necessary step and made possible in-house with the acquisition of an optical wafer probe station. The probe station along with multiple table top probe stations will be utilized for the testing and integration of quantum photonic integrated circuits (QPIC). The entangled photons generated by the existing generation testbed are routed into the QPICs to validate the chips functionality. The acquisition of a second Ti:Sapphire laser and optical parametric oscillator (OPO) expanded the testbed's available wavelength range from the original span of 600-1000 nm to a span of 340-2500 nm. The OPO greatly increases the diversity of materials that the QPICs can be constructed from. The upgraded components have arrived and the full testbed is under construction.

4.4 Theory/experimental requirements of imperfect two-qubit linear optical photonic gates

The optimization method we have developed maximizes the success probability S for a given target transformation A^{Tar}, for given ancilla resources, and for a given fidelity level $F \leq 1$. This is mathematically equivalent to unconstrained maximization of the function $S+F/\epsilon$ in the space of all matrices U, where $1/\epsilon$ is a Lagrange multiplier. Here $\epsilon \longrightarrow 0^+$ corresponds to maximizing the success probability while requiring perfect fidelity (F = 1). As ϵ is increased, the maximum of $S + F/\epsilon$ yields linear optics transformations that maximize the success S as a function of the fidelity F. Given one transformation U that (locally or globally) maximizes success S for a given fidelity F, ϵ may be continuously varied to obtain a one-parameter family of optimal transformations, tracing out a curve in success-fidelity space. Note that in general the members of these families need not be all unitary, however for some gates of interest, including the CZ gate, all members of the family are unitary. Figure 20 shows optimal results for the CZ gate. Here each point corresponds to a unique unitary mode transformation U. As previously reported we find an interesting feature of these unitary matrices. The optimal solution with fidelity F = 1 was found by Knill to have a surprising form [Knill02], which we have dubbed the "Knill Form" [Uskov09], where one mode of each qubit is non-interacting, e.g., in the CZ case U acts as the identity on modes 1 and 3 (or equivalently 1&4, 2&3, or 2&4). This form has been found to hold for the CZ gate and for the TS Toffoli Sign gate (CNOT and Toffoli respectively are equivalent to these up to local rotations).

We now propose an experiment that will test the results shown in Figure 19. Reck et al. have shown that any discrete N x N unitary transformation U can be implemented as a multi-port device consisting only of variable transmittance beamsplitters and phase shifters [Reck94]. Their method is a decomposition in which each unitary matrix element below the diagonal is transformed into zero by a 2 x 2 rotation matrix embedded in an N x N matrix which is otherwise equal to the identity. For example, the 2 x 2 rotation acting on modes N and N-1, which eliminates the element $U_{N,N-1}$, takes the form $T_{N,N-1}$shown in Figure 19.

$$T_{N,N-1} = \begin{pmatrix} 1 & \cdots & \cdots & 0 \\ \vdots & \ddots & e^{i\phi}\sin(\omega) & e^{i\phi}\sin(\omega) \\ 0 & \cdots & e^{i\phi}\sin(\omega) & e^{i\phi}\sin(\omega) \end{pmatrix}$$

Figure 19. Rotation matrix for modes N -1 and N.

The method is recursive and requires one iteration for each pair of modes. Finally, we obtain $U(N)T_{N,N-1}T_{N,N-2}\ldots T_{2,1}D = I$ where D is a diagonal matrix of phases. The desired transformation U is then decomposable as $U(N) = D^{-1}T_{2,1}^{-1}T_{3,1}^{-1}\ldots T_{N,N-1}^{-1}$. Physically, each NxN transformation $T_{i,j}^{-1}$ is implemented as a variable transmittance beamsplitter with a phase plate on one input mode, while D^{-1} corresponds physically to a phase shift on each output mode [Reck94]. Thus a generic two-qubit operation, which needs at least N = 7 modes (Nc = 4 computational modes and Na = 3 ancillas) requires a minimum of 21 beamsplitters and 28 phase shifters. A controlled unitary gate (N = Nc+Na = 4+2 = 6) requires at least 15 beamsplitters and 21 phase shifters. If unitary dilation is required (as is often the case) the number of optical elements increases rapidly. However our experiment does not require unitary dilation and furthermore as noted by Reck et al., if an element of the unitary matrix is already zero, then no transformation is required. The element is skipped.

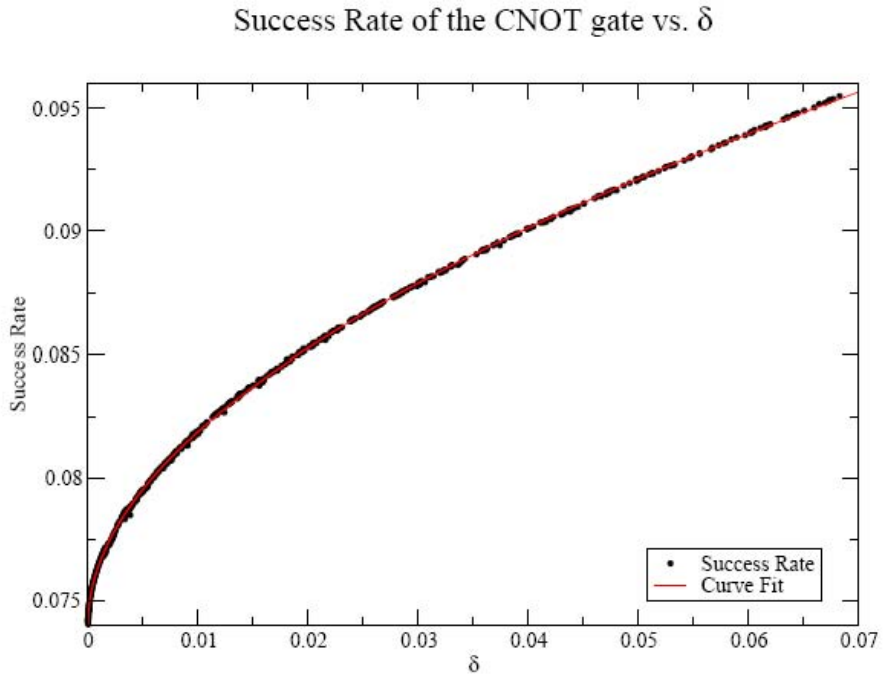


Figure 20. Improved success rates for compromised δ.

Here we return to the “Knill Form," where in the case of CZ we find that nine of the elements below the diagonal are already zero. Therefore the unitary transform can be implemented with

only six beamsplitters and ten phase shifters. We can perform this decomposition for each data point in Figure 20, and find the rotation angles $\omega_{i,j}$ and phases $\phi_{i,j}$ in each case. Surprisingly we find numerically that all of the phase shifts, $\phi_{i,j}$, are constant along the entire length of the curve in Figure 20. Therefore only the six beamsplitter rotation angles $\omega_{i,j}$ out of a total of 36 possible variables need to be modified to vary , making the experiment much more physically realizable. To be specific, the transformation only requires beamsplitters acting on the following mode pairs: (i; j) = (6; 5); (6; 4); (6; 2); (5; 4); (5; 2); (4; 2). Figure 21 shows that the six beamsplitter rotation angles change smoothly with δ. Implementing such rotations and constant phase shifters will recreate the unitary matrices from Figure 20.

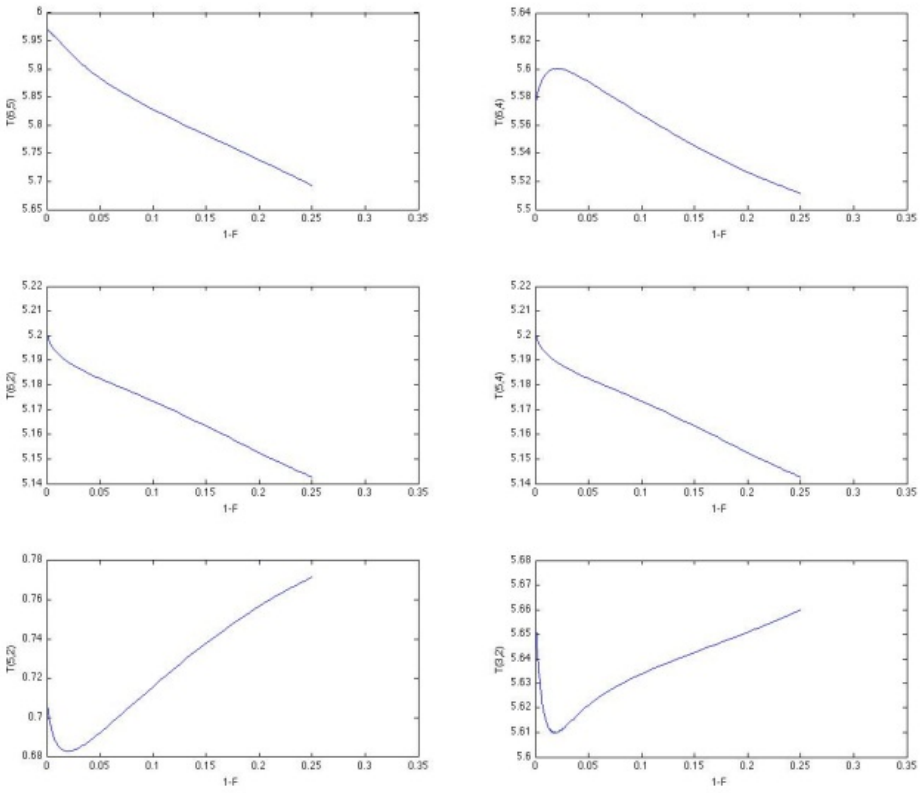


Figure 21. Beamspliter transitivities

This system lends itself to being implemented with 2 x 2 Mach-Zehnder interferometers (MZI) in place of standard beamsplitters. The transmittance of the MZI is controlled dynamically by adjusting the phase difference, without having to alter the physical system. These interferometers have already been put on optical chips by Thompson et al. [Sohma94] among others. Indeed, significantly larger electro-optical matrix switches have been proposed and built for broadband optical communication networks [Sohma94, Drever83]. Figure 22 shows a multi-port device that mixes seven input/output modes (thin lines) using 2 x 2 variable transmittance beamsplitters (rectangles), each of which has a phase shifter on one of its input modes (ellipses). An additional phase shifter is placed on each device output mode. The thick line is a simple mirror. J. L.

O'Brien recently proposed a similar 7 x 7 single-chip MZI-based device made from lithium niobate waveguides [Sohma94]. The intended purpose of this chip was to be able to perform any two-qubit unitary operation, i.e. any transformation in SU(4). However, such a device would also be capable of performing the experiment described above.

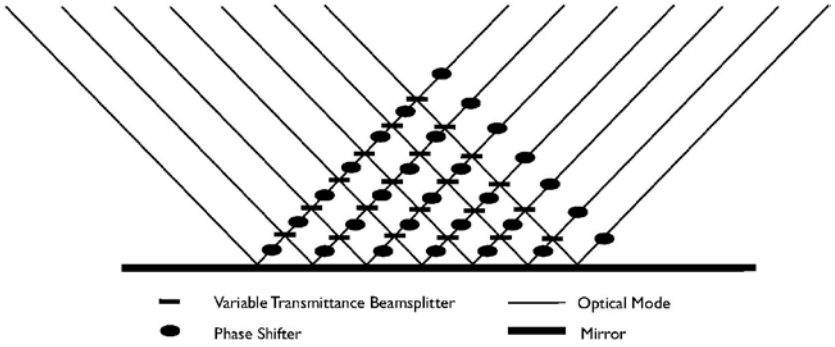


Figure 22. General multiport device schematic.

4.5 Nonlocality, entanglement witnesses and supra-correlations

No Signaling (NS) Correlations: 2-Qubits

Following Acin *et al*. [Acin10] we define an *n*-partite probability distribution $P(a_1,\ldots,a_n \mid x_1,\ldots,x_n)$ as being NS if and only if there exists local quantum measurements $M_{a_i}^{x_i}$ and a Hermitian operator *O* of unit trace such that (3) holds. It is important to note that *O* need not produce positive probabilities for other measurements outside this set. Acin *et al*. [Acin10] give a prescription for the formal construction of *O* given the set of measurements $M_{a_i}^{x_i}$. In the following we present an explicit construction for *O* for the case of *n*=2 qubits (*r*=2 outputs, i.e. *a,b* = {0,1}) and arbitrary number *m* of measurement inputs (*x,y* = {0,1,…,*m*-1}). Later, we extend this to the case of *n*=3 for qubits.

As stated in Section 3.4, without loss of generality we can take the local Hermitian measurement operators to be the projection operators onto "spin-component" *a* in the "direction" *x,* $M_a^x = \Pi_a^x = |a\rangle_x \langle a|$. For each *x*, the completeness of the measurement operators give $\sum_{a=0}^{r-1} M_a^x \equiv I_{r\times r}$ where $I_{r\times r} \equiv I$ is the $r\times r$ identity matrix. This allows us to write the *a=r-1* measurement operator as $M_{a=r-1}^x \equiv I_{r\times r} - \sum_{a=0}^{r-2} M_a^x$. One defines the (tilde) Hermitian matrices $\tilde{M}_a^x$ dual to M_a^x through the inner product $Tr[M_a^x \tilde{M}_{a'}^{x'}] = \delta_{x,x'}\delta_{a,a'}$. For the bipartite case *n*=2, with in general *m* measurement settings with *r* measurement outcomes, one has

$$O = \sum_{a,b=0}^{r-2} \sum_{x,y=0}^{m-1} P(a,b \mid x,y) \tilde{M}_a^x \otimes \tilde{M}_b^y + \sum_{a=0}^{r-2} \sum_{x=0}^{m-1} P(a \mid x) \tilde{M}_a^x \otimes \tilde{I} + \sum_{b=0}^{r-2} \sum_{y}^{m-1} P(b \mid y) \tilde{I} \otimes \tilde{M}_b^y + \tilde{I} \otimes \tilde{I}, \quad (17)$$

where $\tilde{I}$ is the tilde matrix dual to the $r \times r$ identity matrix I, with the additional orthogonality conditions defined by $Tr[I\,\tilde{I}] = Tr[\tilde{I}] = 1,\ Tr[M_a^x \tilde{I}] = 0,$ and $Tr[I\,\tilde{M}_{a'}^{x'}] = Tr[\tilde{M}_{a'}^{x'}] = 0.$ The conditions

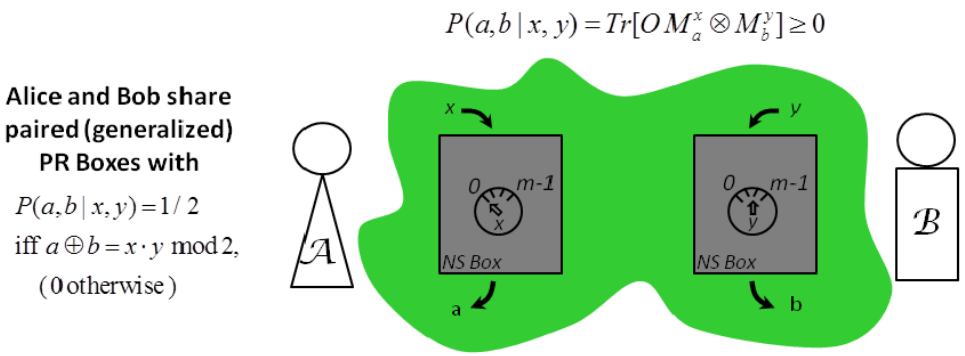


Figure 23. PR Box shared between Alice and Bob.

ensure that O is Hermitian, Tr[O]=1 and probabilities are given by the trace formulas $P(a,b\,|\,x,y) = Tr[OM_a^x \otimes M_b^y]$, $P(a\,|\,x) = Tr[O\,M_a^x \otimes I]$ and $P(b\,|\,y) = Tr[O\,I \otimes M_b^y]$. This is illustrated in Figure 23 where Alice and Bob share PR correlations by means of, what are termed in the literature, a pair of *PR boxes* (or NS {non-signaling} boxes).

In the following we specialize to the case of qubits (r=2, a,b = {0,1}) with arbitrary number m of measurement inputs (x,y = {0,1,…,m-1}) . In this case the measurement operators $M_{a=0}^x$ are given as projection operators for "spin-up" along the directions $x \to \vec{m}_x$ on the Bloch sphere. The $M_{a=0}^x$ are just density matrices on the Bloch sphere written as

$$M_{a=0}^x = |0\rangle_x \langle 0| = 1/2\,(I + \vec{m}_x \cdot \vec{\sigma}),\ \ \vec{m}_x = m_x(\sin\theta_x \cos\phi_x, \sin\theta_x \cos\phi_x, \cos\theta_x)$$
$$|\vec{m}_x| \leq 1,\ \text{(density matrix on Bloch Sphere)}, \qquad (18)$$

where $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ is the vector of single qubit Pauli matrices. Although not required for the case of qubits, the projection onto "spin-down" along x is given by $M_{a=1}^x = |1\rangle_x \langle 1| = 1/2\,(I - \vec{m}_x \cdot \vec{\sigma}) = I - M_{a=0}^x$, with I the 2×2 identity matrix. Equation (17) now simplifies to the form

$$O = \sum_{x,y=0}^{m-1} P(a=0,b=0\,|\,x,y)\tilde{M}_0^x \otimes \tilde{M}_0^y + \sum_{x=0}^{m-1} P(a=0\,|\,x)\tilde{M}_0^x \otimes \tilde{I} + \sum_{y=0}^{m-1} P(b=0\,|\,y)\tilde{I} \otimes \tilde{M}_0^y + \tilde{I} \otimes \tilde{I}. \qquad (19)$$

We simplify the notation by defining $\{I, M_{a=0}^x; x = 0, \cdots, m-1\} \equiv \{M_{-1} \equiv I, \{M_{i\geq 0}\} = \{M_{-1}, M_0, M_1, \ldots\}\}$ $= \{M_{\alpha=\{-1,i\geq 0\}}\}$ (a set of m+1 linear independent matrices) with duals $\{\tilde{M}_{\beta=\{-1,j\geq 0\}}\} \equiv \{\tilde{M}_{-1} \equiv \tilde{I}, \tilde{M}_0, \tilde{M}_1 \ldots\}$

satisfying the trace orthogonality conditions $\mathrm{Tr}[M_\alpha \tilde{M}_\beta]=\delta_{\alpha,\beta}$, and similarly for $\left\{I,\{M^{y}_{j\geq 0}\}\right\}\rightarrow\{N_{\beta=\{-1,j\geq 0\}}\}$. We therefore write (19) as

$$O=\sum_{i,j=0}^{m-1}P^{0,0}_{i,j}\tilde{M}_i\otimes\tilde{N}_j+\sum_{i=0}^{m-1}P^{0,\bullet}_{i}\tilde{M}_i\otimes\tilde{I}+\sum_{j=0}^{m-1}P^{\bullet,0}_{j}\tilde{I}\otimes\tilde{N}_j+\tilde{I}\otimes\tilde{I}, \tag{20}$$

using the abbreviations $P^{0,0}_{i,j}=P(a=0,b=0\,|\,x=i,y=j)$, $P^{0,\bullet}_{i}=P(a=0\,|\,x=i)$ and $P^{\bullet,0}_{j}=P(b=0\,|\,y=j).$ For the measurement matrices $M_{-1}=I\equiv I_{2\times 2}$, and $M_{i\geq 0}=1/2\,(I+\vec{m}_i\cdot\vec{\sigma}),\ |\vec{m}_i|\leq 1,$ the dual matrices are given explicitly by $\tilde{M}_{-1}\equiv\tilde{I}=1/2\,(I-\sum_{i\geq 0}\underset{\sim}{\vec{m}}_i\cdot\vec{\sigma})\equiv 1/2\,(I-\underset{\sim}{\vec{m}}\cdot\vec{\sigma}),$ and $\tilde{M}_i=\underset{\sim}{\vec{m}}_i\cdot\vec{\sigma}$ where $\vec{m}_i\cdot\underset{\sim}{\vec{m}}_j=\delta_{i,j}$, $|\underset{\sim}{\vec{m}}_i|\geq 1,$ with the orthogonality relations $Tr[\tilde{I}]=1,\ Tr[\tilde{M}_j]=0, Tr[M_i\tilde{I}]=0,$ and $Tr[M_i\tilde{M}_j]=\delta_{ij}$. Using the relationship $Tr[X\otimes Y]=Tr[X]Tr[Y]$ it is straightforward to verify that Tr[O]=1 and, for example, $P^{0,0}_{i,j}=Tr[O\,M_i\otimes N_j]$ which picks out the term $\tilde{M}_i\otimes\tilde{N}_j$ in (20). Other probabilities are obtained for example as $P^{0,1}_{i,j}=Tr[O\,M_i\otimes(I-N_j)]=Tr[O\,M_i\otimes I]-Tr[O\,M_i\otimes N_j]=P^{0,\bullet}_{i}-P^{0,0}_{i,j}=\sum_{b=\{0,1\}}P^{0,b}_{i,j}-P^{0,0}_{i,j}$ $=P^{0,1}_{i,j}=P(a=0,b=1\,|\,x=i,y=j).$ Substituting the explicit expressions for the dual matrices into (20) yields the general expression for O in terms of products of Pauli matrices

$$\begin{aligned}O=\frac{1}{4}\Big[&\sum_{i,j=0}^{m-1}(4P^{0,0}_{i,j}-2(P^{0,\bullet}_{i}+P^{\bullet,0}_{j})+1)(\underset{\sim}{\vec{m}}_i\cdot\vec{\sigma})\otimes(\underset{\sim}{\vec{n}}_j\cdot\vec{\sigma})\\&+\sum_{i=0}^{m-1}(2P^{0,\bullet}_{i}-1)\,(\underset{\sim}{\vec{m}}_i\cdot\vec{\sigma})\otimes I+\sum_{j=0}^{m-1}(2P^{\bullet,0}_{j}-1)\,I\otimes(\underset{\sim}{\vec{n}}_j\cdot\vec{\sigma})+I\otimes I\ \Big].\end{aligned} \tag{21}$$

Specializing to the PR correlations in (10) given by $P(a,b\,|\,x=i,y=j)=1/2\ \delta_{a\oplus b,\ i\cdot j\bmod 2}$ $\Rightarrow P^{0,0}_{i,j}=1/2\,\delta_{0,\ i\cdot j\bmod 2}$ with marginals $P^{0,\bullet}_{i}=P^{\bullet,0}_{j}=1/2\,\forall i,j,$ yields the expression for the NSPR operator

$$\begin{aligned}&O_{PR}=\frac{1}{4}\Big[\ (\underset{\sim}{\vec{m}}_e\cdot\vec{\sigma})\otimes(\underset{\sim}{\vec{n}}_e\cdot\vec{\sigma})+(\underset{\sim}{\vec{m}}_e\cdot\vec{\sigma})\otimes(\underset{\sim}{\vec{n}}_o\cdot\vec{\sigma})+(\underset{\sim}{\vec{m}}_o\cdot\vec{\sigma})\otimes(\underset{\sim}{\vec{n}}_e\cdot\vec{\sigma})-(\underset{\sim}{\vec{m}}_o\cdot\vec{\sigma})\otimes(\underset{\sim}{\vec{n}}_o\cdot\vec{\sigma})+I\otimes I\ \Big],\\&\text{where }\underset{\sim}{\vec{m}}_e=\sum_{i=0,1,2,\ldots}\underset{\sim}{\vec{m}}_{2i},\quad\underset{\sim}{\vec{m}}_o=\sum_{i=0,1,2,\ldots}\underset{\sim}{\vec{m}}_{2i+1},\quad\underset{\sim}{\vec{n}}_e=\sum_{j=0,1,2,\ldots}\underset{\sim}{\vec{n}}_{2j},\quad\underset{\sim}{\vec{n}}_o=\sum_{j=0,1,2,\ldots}\underset{\sim}{\vec{n}}_{2j+1}.\end{aligned} \tag{22}$$

In (22) the subscripts {e,o} denote {even,odd} for the summation over even and odd dual measurement vectors. Note that in (22) the "single-σ" terms $\sigma_i\otimes I$ and $I\otimes\sigma_j$ (representing measurements by Alice or Bob alone, respectively) have dropped out since the marginal distributions $P(a|x)=P(b|y)=1/2$ are independent of a,b,x,y. This leaves only the solely two-party correlation terms $\sigma_i\otimes\sigma_j$ and the maximally mixed term $(I\otimes I)/4$. For the bipartite case n=2 often considered in the literature for two qubits, each with two measurement directions $x\in\{\vec{m}_0,\vec{m}_1\}$ for Alice and $y=\{\vec{n}_0,\vec{n}_1\}$ for Bob (i.e. $a,b,x,y=\{0,1\}$) we obtain the simplified form

$$O'_{PR} = \frac{1}{4}[\ (\underset{\sim}{\vec{m}}_0 \cdot \vec{\sigma}) \otimes (\underset{\sim}{\vec{n}}_0 \cdot \vec{\sigma}) + (\underset{\sim}{\vec{m}}_0 \cdot \vec{\sigma}) \otimes (\underset{\sim}{\vec{n}}_1 \cdot \vec{\sigma}) + (\underset{\sim}{\vec{m}}_1 \cdot \vec{\sigma}) \otimes (\underset{\sim}{\vec{n}}_0 \cdot \vec{\sigma}) - (\underset{\sim}{\vec{m}}_1 \cdot \vec{\sigma}) \otimes (\underset{\sim}{\vec{n}}_1 \cdot \vec{\sigma}) + I \otimes I\ ]. \quad (23)$$

Using the procedure for calculating probabilities discussed after equation (4) , the following probabilities can be computed from

$$\begin{array}{ccccc} \vec{n}_0 \quad \vec{n}_1 & \vec{n}_0 \quad \vec{n}_1 & \vec{n}_0 \quad \vec{n}_1 & \vec{n}_0 \quad \vec{n}_1 & \vec{n}_0 \quad \vec{n}_1 \\ \vec{m}_0 \begin{bmatrix} 1/2 & 1/2 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 1/2 & 1/2 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 0 & 0 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 0 & 0 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 1 & 1 \end{bmatrix} \\ \vec{m}_1 \begin{bmatrix} 1/2 & 0 \end{bmatrix} & \vec{m}_1 \begin{bmatrix} 1/2 & 0 \end{bmatrix} & \vec{m}_1 \begin{bmatrix} 0 & 1/2 \end{bmatrix} & \vec{m}_1 \begin{bmatrix} 0 & 1/2 \end{bmatrix} & \vec{m}_1 \begin{bmatrix} 1 & -1 \end{bmatrix} \end{array} \quad (24)$$

$$\begin{array}{ccccc} P(a{=}0,b{=}0 \mid x{=}\vec{m}_i, y{=}\vec{n}_j), & P(a=1,b=1 \mid \vec{m}_i,\vec{n}_j), & P(a=0,b=1 \mid \vec{m}_i,\vec{n}_j), & P(a=1,b=0 \mid \vec{m}_i,\vec{n}_j), & E(\vec{m}_i,\vec{n}_j) \\ a \oplus b = 0, & & a \oplus b = 1, & & \\ \Rightarrow P = 1/2 \text{ for } (x,y) \in \{(0,0),(0,1),(1,0)\}, & & \Rightarrow P = 1/2 \text{ for } (x,y) \in \{(1,1)\}. & & \end{array}$$

Here, the correlations in (8) are computed as (see (5))

$$E(\vec{m}_i,\vec{n}_j)_{i,\,j\in\{0,1\}} = P(a{=}0,b{=}0 \mid x{=}\vec{m}_i, y{=}\vec{n}_j) + P(a=1,b=1 \mid \vec{m}_i,\vec{n}_j) - P(a=0,b=1 \mid \vec{m}_i,\vec{n}_j) - P(a=1,b=0 \mid \vec{m}_i,\vec{n}_j), \quad (25)$$

with corresponding *S* parameter (see (5))

$$S = E(\vec{m}_0,\vec{n}_0) + E(\vec{m}_0,\vec{n}_1) + E(\vec{m}_1,\vec{n}_0) - E(\vec{m}_1,\vec{n}_1) = 4 = S_{AM}, \quad (26)$$

achieving the algebraic maximum value $S_{AM} = 4.$

For the case of two qubits with *m*=3 measurement vectors $x \in \{\vec{m}_0,\vec{m}_1,\vec{m}_3\}$ for Alice and $y = \{\vec{n}_0,\vec{n}_1,\vec{n}_2\}$ for Bob (i.e. *a*,*b* = {0,1}, with *x*,*y* = {0,1,2}) we obtain from (22) the probabilities and correlations

$$\begin{array}{ccccc} \vec{n}_0 \quad \vec{n}_1 \quad \vec{n}_2 & \vec{n}_0 \quad \vec{n}_1 \quad \vec{n}_2 & \vec{n}_0 \quad \vec{n}_1 \quad \vec{n}_2 & \vec{n}_0 \quad \vec{n}_1 \quad \vec{n}_2 & \vec{n}_0 \quad \vec{n}_1 \quad \vec{n}_2 \\ \vec{m}_0 \begin{bmatrix} 1/2 & 1/2 & 1/2 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 1/2 & 1/2 & 1/2 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}, & \vec{m}_0 \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \\ \vec{m}_1 \begin{bmatrix} 1/2 & 0 & 1/2 \end{bmatrix}, & \vec{m}_1 \begin{bmatrix} 1/2 & 0 & 1/2 \end{bmatrix}, & \vec{m}_1 \begin{bmatrix} 0 & 1/2 & 0 \end{bmatrix}, & \vec{m}_1 \begin{bmatrix} 0 & 1/2 & 0 \end{bmatrix}, & \vec{m}_1 \begin{bmatrix} 1 & -1 & 1 \end{bmatrix} \\ \vec{m}_2 \begin{bmatrix} 1/2 & 1/2 & 1/2 \end{bmatrix} & \vec{m}_2 \begin{bmatrix} 1/2 & 1/2 & 1/2 \end{bmatrix} & \vec{m}_2 \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} & \vec{m}_2 \begin{bmatrix} 0 & 0 & 0 \end{bmatrix} & \vec{m}_2 \begin{bmatrix} 1 & 1 & 1 \end{bmatrix} \end{array} \quad (27)$$

$$\begin{array}{ccccc} P(a{=}0,b{=}0 \mid x{=}\vec{m}_i, y{=}\vec{n}_j), & P(a=1,b=1 \mid \vec{m}_i,\vec{n}_j), & P(a=0,b=0 \mid \vec{m}_i,\vec{n}_j), & P(a=1,b=0 \mid \vec{m}_i,\vec{n}_j), & E(\vec{m}_i,\vec{n}_j) \\ a \oplus b = 0, & & a \oplus b = 1, & & \\ \Rightarrow P = 1/2 \text{ for } (x,y) \in \{(e,e),(e,o),(o,e)\}, & & \Rightarrow P = 1/2 \text{ for } (x,y) \in \{(o,o)\}. & & \end{array}$$

In (27) *e* = {0,2} denotes even indices of the measurement directions while *o* = {1} denotes odd indices. We achieve the algebraic maximum for the S parameter, generalizing (26) defined as

$$S = E(\vec{m}_e,\vec{n}_e) + E(\vec{m}_e,\vec{n}_o) + E(\vec{m}_0,\vec{n}_e) - E(\vec{m}_o,\vec{n}_o) = 4 = S_{AM}. \quad (28)$$

Note that the dimension of the measurement vectors $\vec{m}_i$ is set by the dimension $D = d^2 - 1$ of the Hilbert space of the observer, which simply states that any $(D+1)\times(D+1)$ matrix can be written in term of the $(D+1)\times(D+1)$ identity matrix and the D generators of $su(d)$. For qubits, D=3 and the three generators of $su(2)$ are the usual Pauli matrices $\vec{\sigma}$. For a given set of m measurement 3-vectors $\{\vec{m}_i\}$ (vectors in the Bloch sphere, $|\vec{m}_i| \le 1$) one needs to solve for the correspond dual measurement vectors $\{\vec{\underset{\sim}{m}}_j\}$ satisfying $\vec{m}_i \cdot \vec{\underset{\sim}{m}}_j = \delta_{i,j}$. We write these equations as the matrix equation $\mathbf{M}_{m\times 3}\tilde{\mathbf{M}}_{3\times m} = \mathbf{I}_{m\times m}$ where the ith row (i = {0,1,…,m-1}) of (the known coefficient matrix) $\mathbf{M}_{m\times 3}$ is $\vec{m}_i$, and the jth column of (unknowns) $\tilde{\mathbf{M}}_{3\times m}$ is $\vec{\underset{\sim}{m}}_j$. By linear algebra, there exists a right inverse of $\mathbf{M}_{m\times 3}$ via $\tilde{\mathbf{M}}_{Right\ Inv} = \mathbf{M}^T(\mathbf{M}\mathbf{M}^T)^{-1}$ (if $(\mathbf{M}\mathbf{M}^T)^{-1}$ exists) if the columns of $\mathbf{M}_{m\times 3}$ span R^m, which can only occur for $m \le D$=3. The systems of equations is under-determined and there exists at least one solution (typically and infinite number due to undetermined free parameters). This is the situation for probabilities and correlations shown in (24) and (27) for the case m=2 and m=3 measurement vectors, respectively. For the $m > D$=3, there exists at most one, unique solution (if any). This is the least squares (LS) solution using the pseudo-inverse $\mathbf{M}_{m\times 3}$ given by $\tilde{\mathbf{M}}_{LS} = (\mathbf{M}^T\mathbf{M})^{-1}\mathbf{M}^T$ (if $(\mathbf{M}^T\mathbf{M})^{-1}$ exits). In general, the LS solution has non-zero residual errors given by $\mathbf{Err} = \mathbf{M}_{m\times 3}\tilde{\mathbf{M}}_{LS(3\times m)} - \mathbf{I}_{m\times m}$, corresponding to joint probabilities that may be negative for some measurements but still satisfy the (total probability) normalization condition $\sum_{a,b} P(a,b \mid x,y) = 1,\ \forall x,y$. Nonetheless, it is instructive to perform numerical searches in the case of m>3 of random measurement vectors to seek solutions which yield all joint probabilities in the range $0 \le P(a,b|x,y) \le 1$, for all pairs of measurement vectors $\vec{m}_i, \vec{n}_j$ for Alice and Bob that still yield supra-correlations, i.e. $0 < S\text{-}S_Q \le 4\text{-}2\sqrt{2} = 1.172$.

For the case m=4, a particular solution is shown in (29) that yields $S\text{-}S_Q = 0.102$ (for brevity, we only show $P(a{=}0, b{=}0 \mid x{=}\vec{m}_i, y{=}\vec{n}_j)$ and the correlations $E(\vec{m}_i, \vec{n}_j)$). In general, the even/odd structure of the correlations $E(\vec{m}_i, \vec{n}_j)$

$$
\begin{array}{c} \\ \vec{m}_0 \\ \vec{m}_1 \\ \vec{m}_2 \\ \vec{m}_3 \end{array}
\begin{array}{c}
\begin{array}{cccc} \vec{n}_0 & \vec{n}_1 & \vec{n}_2 & \vec{n}_3 \end{array} \\
\begin{bmatrix} 0.237 & 0.395 & 0.072 & 0.406 \\ 0.162 & 0.018 & 0.381 & 0.004 \\ 0.469 & 0.449 & 0.341 & 0.457 \\ 0.249 & 0.038 & 0.481 & 0.024 \end{bmatrix} \\
P(a{=}0, b{=}0 \mid x{=}\vec{m}_i, y{=}\vec{n}_j),
\end{array}
\quad
\begin{array}{c} \\ \vec{m}_0 \\ \vec{m}_1 \\ \vec{m}_2 \\ \vec{m}_3 \end{array}
\begin{array}{c}
\begin{array}{cccc} \vec{n}_0 & \vec{n}_1 & \vec{n}_2 & \vec{n}_3 \end{array} \\
\begin{bmatrix} -0.052 & 0.581 & -0.710 & 0.623 \\ -0.350 & -0.927 & 0.522 & -0.982 \\ 0.875 & 0.796 & 0.365 & 0.829 \\ -0.004 & -0.847 & 0.923 & -0.905 \end{bmatrix} \\
E(\vec{m}_i, \vec{n}_j)
\end{array}
\qquad (29)
$$

exhibited in the cases $m \le 3$ ((24) and (27)) is destroyed, yet they still produce supra-correlations $S\text{-}S_Q \ge 0$. For each value of m in Figure 24 (left) we searched 10^5 random trials of the

measurement vectors $\{\vec{m}_i, \vec{n}_j\}_{i,j\in\{0,1,\ldots,m-1\}}$ and plot the value of S-S_Q for the first solution encountered in which (i) we find proper joint probability distributions $0\leq P(a,b\,|\,x=\vec{m}_i, y=\vec{n}_j)\leq 1$ for all measurement vectors, and (ii) which produce supra-correlations, S-$S_Q \geq 0$. In Figure 24 (middle), we plot the minimum

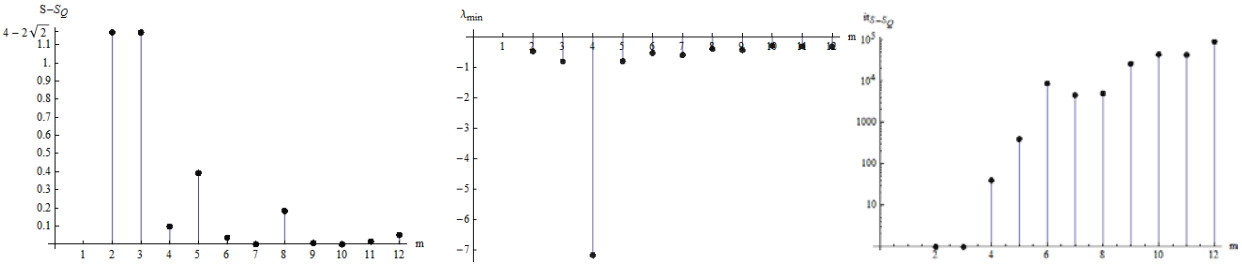


Figure 24. Numerical simulations for m={2,3,4,…,12} measurement vectors.

eigenvalue $\lambda_{\min}$ of the matrix O in (22). The negative value of $\lambda_{\min}$ indicates that O is not realized by a proper quantum state (i.e. a positive, Hermitian operator, $\rho\geq 0$). The rightmost plot in Figure 24 is the iteration number at which the first set of measurement vectors was found which produced supra-correlations. For the values of $13 \leq m \leq 20$ numerically explored, no supra-correlations solutions were found within 10^5 trials (the plot indicates that it becomes exponentially hard to find such a solution).

No Signaling (NS) Correlations: 3-Qubits

The bipartite results of the previous section for n=2-qubits are straightforwardly extended to the tripartite case of n=3-qubits with similar implications. Here the generalization of the bipartite CHSH nonlocality parameter S is given by the Svetlichny [Svetlichny87] inequality (SI) relating correlations $E(a,b,c|x,y,c)$ between three spacelike separated parties *A, B, C*

$$\begin{aligned} S \equiv\, & E(a,b,c\,|\,0,0,0)+E(a,b,c\,|\,0,1,0)+E(a,b,c\,|\,1,0,0)-E(a,b,c\,|\,1,1,0) \\ & +E(a,b,c\,|\,0,0,1)-E(a,b,c\,|\,0,1,1)-E(a,b,c\,|\,1,0,1)-E(a,b,c\,|\,1,1,1). \end{aligned} \tag{30}$$

The SI has the bounds (i) $|S|\leq S_C = 4$ for classical correlations, (ii) $|S|\leq S_Q = 4\sqrt{2}$ for quantum correlations, with (iii) the algebraic upper bound given by $|S|\leq S_{AM} = 8,$ achieved when the correlations in (14) take the values E=1 if they are preceded by a plus sign, and E=-1 if they are preceded by a minus sign. The generalization of the PR correlations of (30) is given by [Xiang11]

$$\text{TPR Box:}\quad P(a,b,c\,|\,x,y,z)=\begin{cases} 1/4 & \text{if } a\oplus b\oplus c = x\cdot y\oplus y\cdot z\oplus x\cdot z \\ 0 & \text{otherwise} \end{cases}, \tag{31}$$

often referred to as a tripartite PR (TPR) box. The marginal distributions of (15) are again isotropic and satisfy the NS constraint, i.e. $P(a,b|x,y,z) = P(a,b|x,y)=1/4$ for all a,b,x,y,z and $P(a,|x,y)=P(a|x)=1/2$ for all a,x,y, and similarly for all other marginal probability distributions.

For the case of n=3 qubits (r=2 output measurement values) a,b,c ={0,1), with m possible measurement vectors for each observer, x,y,z ={0,1,…,m-1) we again find that only the highest (three party) correlations term and the maximally mixed term are non-zero in the expression for O_{TPR}

$$O_{TPR} = \frac{1}{8}[\ \{(\vec{\tilde{m}}_e\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_e\cdot\vec{\sigma})+(\vec{\tilde{m}}_e\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_o\cdot\vec{\sigma})+(\vec{\tilde{m}}_o\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_e\cdot\vec{\sigma})-(\vec{\tilde{m}}_o\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_o\cdot\vec{\sigma})\}\otimes(\vec{\tilde{r}}_e\cdot\vec{\sigma})$$
$$-\{(\vec{\tilde{m}}_o\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_o\cdot\vec{\sigma})+(\vec{\tilde{m}}_o\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_e\cdot\vec{\sigma})+(\vec{\tilde{m}}_e\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_o\cdot\vec{\sigma})-(\vec{\tilde{m}}_e\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_e\cdot\vec{\sigma})\}\otimes(\vec{\tilde{r}}_o\cdot\vec{\sigma})+I\otimes I\otimes I],\quad(32)$$

where $\vec{\tilde{q}}_e = \sum_{i=0,1,2,\ldots}\vec{\tilde{q}}_{2i}$, $\vec{\tilde{q}}_o = \sum_{i=0,1,2,\ldots}\vec{\tilde{q}}_{2i+1}$, $\vec{\tilde{q}} = \{\vec{\tilde{m}}, \vec{\tilde{n}}, \vec{\tilde{r}}\}$.

The regular, even/odd (mod 2) structure of O_{TPR} in (32) reflects the non-zero structure of the TRP probabilities in (31), and can be seen as an additional single qubit generalization of O_{PR} in (22). That is, the 2-qubit term in the first curly brackets in (32) $\{(\vec{\tilde{m}}_e\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_e\cdot\vec{\sigma})+(\vec{\tilde{m}}_e\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_o\cdot\vec{\sigma})+(\vec{\tilde{m}}_o\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_e\cdot\vec{\sigma})-(\vec{\tilde{m}}_o\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_o\cdot\vec{\sigma})\}$ tensor-producted with the remaining "even" qubit term $(\vec{\tilde{r}}_e\cdot\vec{\sigma})$, is precisely two-party correlation term that appears in O_{PR} in (22). Similarly, the term in the second curly bracket in (32) $\{(\vec{\tilde{m}}_o\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_o\cdot\vec{\sigma})+(\vec{\tilde{m}}_o\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_e\cdot\vec{\sigma})$ $+(\vec{\tilde{m}}_e\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_o\cdot\vec{\sigma})-(\vec{\tilde{m}}_e\cdot\vec{\sigma})\otimes(\vec{\tilde{n}}_e\cdot\vec{\sigma})\}$ tensor-producted with the remaining "odd" qubit term $(\vec{\tilde{r}}_o\cdot\vec{\sigma})$ (with the accompanying minus sign) is just the bit flip ($e\leftrightarrow o$) of the previous two-party correlation term. Again, we can achieve the algebraic maximum S_{AM}=8 when each party has (for the case of qubits) at most m=3 measurement vectors (for exactly the same linear algebraic reason for the n=2 bipartite case). Further, as in the bipartite case, we can find particular NS supra-correlation solutions $0<S\text{-}S_Q\leq 4\text{-}2\sqrt{2}$ for $m>3$, but which become increasingly hard to find the larger the value of m.

4.6 Ongoing cluster state algorithm research

As part of our theoretical research goals for this project, we have been investigating quantum algorithm development in the cluster state paradigm. In almost every implementation of quantum computing one of the first algorithms that people have developed and tested is an unstructured quantum search algorithm. In the photonic circuit model of quantum computing [DiVincenzo00] this algorithm is structurally very similar to that first proposed by Grover and as such is called Grover's algorithm [Grover97]. Since the development of MBQC, and particularly in the photonic implementation of MBQC, also called the cluster state model, parallels have been drawn between the photonic circuit model and MBQC model. This includes comparing the circuit model of Grover's algorithm to a cluster state model of a four element quantum search [Walther05]. Given the difficulty of creating large cluster states this four element search is the

largest that has been performed to date. The, $2^n=2^2=4$ element search requires $n^2=2^2=4$ qubits arranged in a square or ``box" cluster state [Walther05]. The next larger $2^3=8$ element search requires a significantly more difficult to produce 3 x 3 square cluster state and so on.

Using the 4-qubit box state, as illustrated in Figure 25, the measurement based quantum search appears to be very similar to that of Grover. The input state is similar, the desired output state is

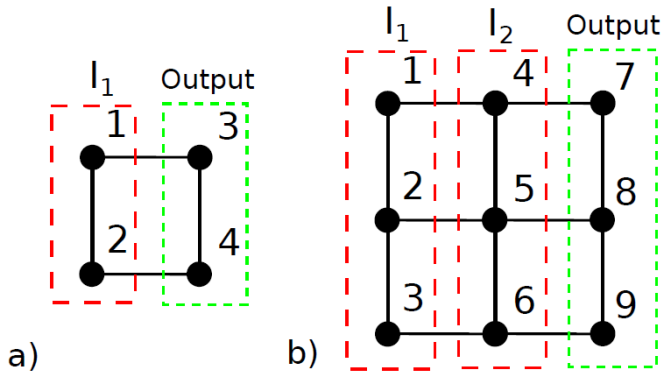


Figure 25. Square cluster states (a) (n=2) 4-element "box," (b) (n=3) 9-element.

similar, the number of iterations is the same and the oracle's tagging operation appears similar. This has led many people to call the MBQC quantum search, Grover's algorithm [Grover97]. However, there is often a small caveat that is overlooked. As Zeilinger *et al.* wrote "Remarkably, the inversion-about-the-mean process is `hard-wired' into the structure of the cluster state and is automatically implemented" [Walther05]. We found this automatic implementation of an inversion about a mean, or equivalently amplitude amplification (when combined with tagging), to be an imprecise claim and as such have investigated the measurement based quantum search algorithm numerically for larger systems. We have found that a significant number of non-trivial differences exist between the standard description of Grover's algorithm and its implementation in the circuit model and the MBQC search algorithm for larger systems. This leads us to question whether the MBQC search algorithm is some variant of Grover's algorithm, or rather a different search algorithm all together.

Two cluster-states able to perform an unsorted search for a) the (n=2) $2^2=4$ element search on $|\Psi_{box}\rangle$ and b) the (n=3) $2^3=8$ element search on $|C9\rangle$ are shown in Figure 25. Each circle is a single qubit initialized in the $|+\rangle$ state. The solid lines connecting the circles indicate the action of a CZ gate between these qubits, i.e. entanglement between the qubits. Logical qubits are arranged in rows of the grid, initially: (1,3) and (2,4) for $|\Psi_{box}\rangle$, and (1,4,7), (2,5,8), and (3,6,9) for $|C9\rangle$. Figure 25(a) shows the trivial MBQC measurements using one application of an iterator I_1 (large red dashes acting on columns of qubits) on the 4-qubit box state. Figure 25(b) Shows the two iterations for the eight element search I_1, I_2. All of the measurements in an iterator I_j can be

implemented simultaneously. The outcomes of each I_j determine the basis of the next iteration I_{j+1}. (Equivalently I_j determines the Pauli correction factors that can be applied latter in post-processing). The output state (small green dashes) holds the logical state at the end of the algorithm. The effective logical qubits after the first iteration I_1 are (3) and (4) (the output states) for $|\Psi_{box}\rangle$, and (4,7), (5,8), and (6,9) for $|C9\rangle$.

Measurement Sequence ($\mathcal{I}_1$; $\mathcal{I}_2$)	Search Element i	Output State $\|\Psi_{out,i}\rangle$
(0,0,0 ; 0,0,0)	1	(1,0,0,0,0,0,0,0)
(0,0,π ; 0,π,0)	2	(0,1,0,0,0,0,0,0)
(0,0,0 ; 0,0,π)	3	(0,0,1,0,0,0,0,0)
(0,0,π ; 0,π,π)	4	(0,0,0,1,0,0,0,0)
(0,0,π ; 0,0,0)	5	(0,0,0,0,1,0,0,0)
(0,0,0 ; 0,π,0)	6	(0,0,0,0,0,1,0,0)
(0,0,π ; 0,0,π)	7	(0,0,0,0,0,0,1,0)
(0,0,0 ; 0,π,π)	8	(0,0,0,0,0,0,0,1)

Figure 26. Measurement patterns and resulting output for 8-element MBQC search.

Here we pause to note something rather undesirable. If we consider the measurement of the vertical columns to be a "step" in the iteration (i.e. 1,2,3 or 4,5,6 from Figure 25(b)), then the MBQC algorithm does not have a fixed, constant iterator. The iterator will in general vary between steps and it is neither sequential nor random as can be seen from the first column of Figure 26. The various iterators must be carefully chosen by the oracle at each step. This appears very different from Grover's iterator. In Grover's algorithm the iterator is chosen by the oracle at the start of the calculation and then remains a constant regardless of the number of iteration steps. Figure 26 shows measurement settings for the 6-qubit measurements that result in each of the eight possible outputs of the MBQC search. Note the output state is corrected for overall phase, so the tags are not unique. In addition, all measurements presented are presumed to have given the "correct" output (i.e. only entries in section 1 of $|\Psi_{out}\rangle$ are populated), thus negating the need for trivial feed forward corrections typical in MBQC. We have found a way of modifying the MBQC search algorithm such that the iterator is a constant not only between steps, but is also constant for any desired output. This work an ongoing project for FY13, and the research results are being written up for submission to Physical Review A.

5.0 CONCLUSIONS

Multipli-entangled photons from a spontaneous parametric down-conversion source

This report describes research on the Schioedtei source, a unique type II SPDC source design for which additional in-depth information can be obtained through our previously published papers [Fanto11, Peters12]. Schioedtei generates up to six pairs of entangled photons per pass through the type II crystal assembly. This configuration surpasses the typical single entangled pair generated per pass found in standard type II SPDC sources. Concurrently Schioedtei generates a variety of states atypical of being produced from a single photon source. Useable photon generation rates (two and four photon) have been observed, thus showing its feasibility as a

direct generation source of entangled photons for quantum optics/entanglement experiments. The six pairs of photons produced are directly applicable to the generation of linear, box, butterfly and a multitude of other cluster states. The utility of the Schioedtei source is (i) its reduced experimental footprint compared to standard multi-crystal/multi-pass experiments, (ii) it generates a variety of entangled/separable states, and (iii) generated states are amenable towards cluster state generation. Furthermore, the generated photons from Schioedtei are the input states for our bulk optical gates and QPICs.

A multi-layer three dimensional superconducting nanowire photon detector

The multilayer superconducting number-resolving photon detector represents a significant improvement on current single layer meander devices. The device will have significantly higher number resolution, while maintaining a useful detection area. It has several parameters which can control the reset time to avoid latching while still minimizing the rest time. An array of pixels of arbitrary number, size and shape is possible. The active area of the detector can be tuned by changing the number or the shapes of the pixels. The fill factor of the detector should be at least equal to that of current nanowire meanders and given the potential reduction of the current crowding effect significantly higher. As a final note we will point out that the multi-layer superconducting number-resolving photon detector can also give a rough spatial distribution of the incident photons. These advantages are compelling evidence for the construction and testing of multi-layer superconducting number-resolving photon detectors.

Theory/experimental requirements of imperfect two-qubit linear optical photonic gates

We have shown the theoretical basis and interest for this experiment. At this time it is the only apparent means of experimentally confirming the numerical data presented above, which quantifies the trade-off between fidelity and success, for the CZ or CNOT gate. The experimental setup may naturally be extended to explore the behavior of other quantum gates of interest. The components needed for the execution of the experiment are well within the means of many experimental groups. The main stumbling block is the expense of purchasing number-resolving detectors. However, any group already possessing these detectors should be able to implement this scheme with relative ease.

Nonlocality, entanglement witnesses and supra-correlations

In this area of research we have examined the structure of supra-correlations that are stronger than quantum and hence not realizable by a physical (positive) quantum state $\rho \geq 0$. The supra-correlations are intriguing because they arise from valid probability distributions, first put forth by Popescu and Rohrlich (PR), that satisfy the no-signaling principle of special relativity as well as all the usual normalization condition on the joint and marginal distributions. Thus, the fact that nature is not able to realize these supra-correlations points to hidden structure underlying how quantum correlations can be distributed amongst spacelike separated parties. Our work has examined the structure and distribution of PR correlations in 2- and 3-qubit systems by explicitly constructing "states" (not necessarily positive quantum states) that exhibit supra-correlations for a fixed, but arbitrary number, of measurements available to each party. We have shown that the PR correlations involve only solely *n*-party correlations amongst the *n* observers. We have extended this study to include *n*-party correlations that capture the essential features of the PR

correlations and do not rely on predetermined measurements between the *n* participants. Additionally, by constructing constraints based on the positivity and purity of an arbitrary *n*-qubit state we have shown the "unreasonableness" of the PR correlations in that they encode more correlations than are physically allowed by nature [see details in Alsing12]. In future work we will couple this approach of studying how correlations are distributed amongst the *n* parties to the study of quantum entanglement. The study of entanglement [Horodecki09] is an important, but difficult field, only well understood for the case of two qubits (both pure and mixed), and to a lesser degree, for pure 3-qubit systems. A fruitful area to investigate next are pure 3-qubit systems, where a generalized (though non-unique) Schmidt decomposition holds [Acin00]. We purport that an examination of the distribution of correlations, bounded by physically imposed constraints on e.g. positivity and purity, coupled with the description of entanglement in terms of the tangle, as initiated in this work, can shed further light on the classification of pure tripartite systems.

6.0 REFERENCES

[Acin00] A. Acin, A. Andrianov, L. Costa, E. Jane, J.I. Latorre and R. Tarrach, "Generalized Schmidt decomposition and classification of three-quantum-bit states," Phys. Rev. Lett. **85**, 1560 (2000).

[Acin10] A. Acin, R. Augsiak, D. Cavalcanti, C. Hadley, J.K. Korbicz, M. Lewenstein, L. Masanes and M. Piani, "Unified framework for correlations in terms of local quantum observables," Phys. Rev. Lett. **104**, 140404, (2010); arxiv:0911.3606.

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

[Alsing12] P.M. Alsing and J.R. McDonald, "Nonlocality, Entanglement Witnesses and Supra-correlations," Proc. of SPIE **8400**, 84000Y (2012).

[Anderson04] E. H. Anderson, D. Ha, J. A. Liddle, "Sub-pixel alignment for direct write electron beam lithography," Microelectronic Eng. **73-74**, 74-79 (2004).

[Barnum10] H. Barnum, S. Beigi, S. Boixo, M.B. Elliot and S. Wehner., "Local quantum measurement and no-signaling imply quantum correlations," Phys. Rev. Lett. **104**, 140401 (2010); arxiv:0910.3952.

[Bell64] J.S. Bell, "On the Einstein Podolsky Rosen paradox," Physics **1**, 195 (1964).

[Bitton01] G.Bitton, *et al*., "Novel Cascaded Ultra Bright Pulsed Source of Polarization Entangled Photons", arXiv:quant-ph/0106122v1, (2001).

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

[Ceccarelli09] R. Ceccarelli, *et al.*, "Experimental Entanglement and Nonlocality of a Two-Photon Six-Qubit Cluster State", Phys. Rev. Lett. **103**, 160401 (2009).

[Clauser69] J.F. Clauser, "Proposed experimental tests to local hidden-variable theories,"Phys. Rev. Lett. **23**, 880 (1969).

[Clem11] J. R. Clem and K. K. Berggen "Geometry-dependent critical currents in superconducting nanocircuits," arXiv:1109.4881v1 (2009).

[Dauler08] E. A. Dauler et al., "Photon-number-resolution with sub-30-ps timing using multi-element superconducting nanowire single photon detectors," Journal of Modern Optics **56**, pp. 364-373 (2008).

[DiVincenzo00] D.P. DiVincenzo, "The physical implementation of quantum computation," Fortschr. Phys. **48**, 771 (2000).

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

[Drever83] Drever R. W. et al. "Laser phase and frequency stabilization using an optical resonator," Appl. Phys. B **31**, 97-105 (1983).

[Fanto10] M.L. Fanto *et al.*, "Compensated crystal assemblies for type-II entangled photon generation in quantum cluster states", SPIE Vol. **7702**, 77020H (2010).

[Fanto11] M.L. Fanto *et al.*, "Multipli-entangled photons from a spontaneous parametric down-conversion source", SPIE **8057**, 805705 (2011).

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

[Guhne09] O. Guhne and G. Toth, "Entanglement detection," Phys. Reports **474**, 1-75 (2009).

[Gurevich87] A.V. Gurevich and R.G. Mint, "Self-heating in normal metals and superconductors," Rev. Mod. Phys. **59**, 941 (1987).

[Hadfield09] R. H. Hadfield "Single-photon detecors for optical quantum information applications," Nat. Photonics 3 Dec. (2009) doi:10.1038/nphoton.2009.230.

[Horodecki09] R. Horodecki, P. Horodecki, M. Horodecki and K. Horodecki, "Quantum entanglement," Rev. Mod. Phys. 81, 865-942 (2009); arxiv:quant-ph/0702225.

[Kerman07] A. J. Kerman et al. ,"Constriction-limited detection efficiency of superconducting nanowire single-photon detectors," Appl. Phys. Lett. **90**, 101110 (2007).

[Knill01] E. Knill E., R. Laflamme and G.J. Milburn, "A scheme for efficient quantum computation with linear optics," Nature **409**, 46 (2001).

[Knill02] E. Knill, "Quantum gates using linear optics and postselection," Phys. Rev. A **66**, 052306 (2002).

[Kraus83] Kraus K. "Lecture Notes: States, Effects and Operations: Fundamental Notions of Quantum Theory" (Springer, New York, 1983).

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

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

[Lu07] C.Y. Lu *et al.*, "Experimental entanglement of six photons in graph states", Nature Physics, **3**, 91 (2007).

[Ma10] S.Y. Ma, *et al.*, "Probabilistic quantum network coding of M-qudit states over the butterfly network", Opt. Comm. **283**, 497-501 (2010).

[Marsili11] F. Marsili et al., "Single-Photon Detector based on Ultranarrow Superconducting Nanowires," Nano Let. **11**, 2048-2053 (2011).

[Masanes06] L. Masanes, A. Acin and N. Gisin, "General properties of nonsignaling theories," Phys. Rev. Lett. **73**, 012112 (2006); arxiv:quant-ph/0508016.

[Nam11] B. Baek, A. E. Lita, V. Verma and S. W.Nam, "Superconducting a-W_xSi_{1-x} nanowire single-photon detector with saturated internal quantum efficiency from visible to 1850 nm," Appl. Phys. Lett. **98**, 251105 (2011).

[Nielsen05] M.A. Nielson, "Cluster-Sate Quantum Computation", arxiv 0504097v2, (2005).

[O'Brine07] J.L. O'Brien, *et al.*, "Optical quantum computing", Science **318**, 1567 (2007).

[O'Brein09] J. L. O'Brein, A. Furusawa, J. Vuchovic, "Photonic quantum technologies," Nat. Photonics 3 Dec. (2009) doi:10.1038/nphoton.2009.229.

[Pawlowski09] M. Pawlowski, T. Paterek, D. Kaszilkowski, V. Scarani, A. Winter and M. Zukowski, "Information causality as a physical principle," Nature Letters **461,** 1101 (2009).

[Peters12] C.J. Peters *et al.*, "A Multipli-entangled Photon Source for Cluster State Generation," SPIE **8400**, 84000Z (2012).

[Popescu94] S. Popescu and D. Rohrlich, "Quantum nonlocality as an axiom," Found. Phys. **24**, 379 (1994).

[Prevedel07] R. Prevedel, *et al.*, "Experimental realization of a quantum game on a one-way quantum computer", New J. Phys. **9**, (2007).

[Rangarajan09] R. Rangarajan, *et al.*, "Optimizing type-I polarization-entangled photons", Optics Express **17**, 18920 (2009).

[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); *ibid*, "Persistent entanglement in arrays of interacting particles," Phys. Rev. Lett. **85**, 910–913, (2001); R. Raussendorf, D.E. Browne and H.J. Briegel, "Measurement-based quantum computation using cluster states," Phys. Rev. Lett. **68**, 022312 (2003).

[Reck94] Reck M., Zeilinger A., Bernstein H. J., and Bertani P. "Experimental realization of any discrete unitary operator". Phys. Rev. Lett. **73**, 58-61 (1994).

[Schumacher91] B.W. Schumacher, "Information and quantum nonseparability," Phys. Rev. A **44**, 7047 (1991).

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

[Soeda10] A. Soeda *et al.*, "Quantum computation over the butterfly network", Phys. Rev. A **84**, 012333 (2010).

[Sohma94] S. Sohma *et al.* "Silica-based PLC Type 32x32 Optical Matrix Switch," Euro. Conference on Optical Communication, 1-2 (2006).

[Smith11] A. M. Smith, D. B. Uskov , L. H. Ying, and Kaplan L., "Imperfect linear optical photonic gates with number-resolving photodetection," Phys. Rev. A **84**, 032341 (2011).

[Svetlichny87] G. Svetlichny, "Distinguishing three-body from two-body nonseparability by a Bell-type inequality," Phys. Rev. D **35**, 3006 (1987).

[Tsirelson80] B. Tsirelson, "Quantum Generalizations of Bell's Inequality," Lett. Math. Phys. **4**, 93 (1980).

[U'ren06] A.B. U'Ren *et al.*, "Generation of two-photon states with an arbitrary degree of entanglement via nonlinear crystal super lattices", Phys. Rev. Lett. **97**, 223602 (2006).

[Uskov09]Uskov D.~B., Kaplan L., Smith A. M., Huver S. D., and Dowling J. P. "Maximal success probabilities of linear-optical quantum gates". Phys. Rev. A **79**, 042326 (2009).

[Uskov10] D. B. Uskov, A. M. Smith, and L. Kaplan, "Generic two-qubit photonic gates implemented by number-resolving photodetection," Phys. Rev. A **81**, 012303 (2010).

[Vallone10] G. Vallone *et al.*, "Six-qubit two-photon hyperentangled cluster states: Characterization and application to quantum computation", Phys. Rev. A. **81**, 052301 (2010).

[van Dam05] W. van Dam, "Implausible consequences of superstrong nonlocality," quant-ph/0501159 (2005).

[Vedral97] V. Vedral, M.B. Plenio, M.A. Rippin and P.L. Knight, "Quantifying Entanglement," Phys. Rev. Lett. 78, 2275 (1997); V. Vedral, "Introduction to quantum information science", Oxford, N.Y. (2006).

[Walther05] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer and A. Zeilinger, "Experimental one-way quantum computing," Nature **434**, 169 (2005).

[Wilde09] Wilde M.M. and Uskov D.B. "Linear-optical hyperentanglement-assisted quantum error-correcting code". Phys. Rev. A 79, 022305 (2009).

[Xiang11] Y. Xiang and W. Ren, "Bound on genuine multipartite correlations from the principle of information causality," Quantum Information & Computation. **11**, 948 (2011); arxiv:1101.2971.

[Xu08] F. Xu, Z. Han, and G. Guo, "Improvements of QKD with practical photonnumber resolving detectors," Proc. SPIE **7278**, 72780Y (2008).

7.0 LIST OF SYMBOLS, ABBREVIATIONS, AND ACRONYMS

2D	2 Dimensional
3D	3 Dimensional
α-BBO	Alpha barium borate
AFRL	Air Force Research laboratory
APD	Avalanche photodiode
a-W_xSi_{1-x}	Amorphous Tungsten Silicon
ß-BBO	Beta barium borate
BiBO	Bismuth borate
BI	Bell Inequality
CCD	Charged coupled device
CCM	Coincidence counting module
CHSH	Clauser-Horne-Shimony-Holt
CJI	Choi-Jamiolkowski isomorphism
CNOT	Controlled NOT (gate)
CW	Continuous wave
CZ	Controlled Z (gate)
fs	femtosecond
GVM	Group velocity matching
HP	High power
JAG	Judge Advocate General
LS	Least squares
MBQC	Measurement based quantum computing
MgO	Magnesium Oxide
MHz	megahertz
mm	millimeter

NbN	Niobium Nitride
NbTiN	Niobium Titanium Nitride
NIST	National Institute for Standards and Technology
nm	nanometer
NS	No-signaling
OPO	Optical Parametric Oscillator
PQNS	Post Quantum No-signaling
PR	Popescu-Rohrlich
QM	Quantum Mechanics
QIS	Quantum Information Science
QPIC	Quantum Photonic Integrated Circuit
SHG	Second harmonic generation
Si	Silicon
Si-APD	Silicon avalanche photodiode
SI	Svetlichny Inequality
SNSPD	Superconducting Nanowire Single Photon Detector
SPCM	Single photon counting module
SPDC	Spontaneous parametric downconversion
SR	Special Relativity
THG	Third harmonic generation
TPR	Tripartite Popescu-Rohrlich
UV	Ultraviolet