Optical and Quantum Communications

RLE Group
Optical and Quantum Communications Group

Academic and Research Staff
Professor Jeffrey H. Shapiro, Dr. Franco N. C. Wong, Dr. Baris I. Erkmen,
Dr. Raúl García-Patrón, Dr. Julien Le Gouët, Dr. Maria Tengner, Dr. Mankei Tsang

Graduate Students
Aman Chawla, Onur Kuzucu, Dheera Venkatraman, Wenbang Xu, Tian Zhong

Undergraduate Student
Bhaskar Mookerji

The central theme of our programs has been to advance the understanding of optical and quantum communication, radar, and sensing systems. Broadly speaking, this has entailed: (1) developing system-analytic models for important propagation, detection, and communication scenarios; (2) using these models to derive the fundamental limits on system performance; and (3) identifying, and establishing through experimentation the feasibility of, techniques and devices which can be used to approach these performance limits.

Sponsors
Air Force Research Laboratory Contract FA8750-06-2-0069
Air Force Research Laboratory Contract FA8750-07-C-0206
Army Research Office – Grant W911NF-05-1-0197
NIST - Grant 70NANB7H6186
Office of Naval Research - Contract N00014-02-1-0717
U.S. Department of Interior Contract NBCHC00671
W. M. Keck Foundation Center for Extreme Quantum Information Theory

We are embarked on research in the area of quantum information technology whose goal is to enable the quantum-mechanical information transmission, storage, and processing needed for future applications in quantum computing and quantum communication. Our theoretical work is currently focused on the fundamental limits on classical information transmission that are due to the quantum noise of bosonic channels, and on the use of quantum resources in precision measurement and imaging applications. Our main experimental work is focused on generation and application of entanglement sources with high brightness and wavelength tunability. In addition, we are interested in novel entanglement sources and their applications in quantum logic gates, enhanced quantum measurements, quantum imaging, quantum protocols for entanglement distillation, and quantum cryptography.

Reverse Coherent Information Shannon proved that sending classical information through a noisy classical channel can be achieved with vanishingly small error probability in the limit of many channel uses subject to two conditions: (1) the information rate is less than the channel's capacity; and (2) appropriate error-correction coding is employed [1,2]. Quantum information theory is a generalization of Shannon's work that treats both classical and quantum information transmission over noisy quantum-mechanical channels. In recent years we have devoted a great deal of our attention to classical information transmission over bosonic channels [3-7], because the vast majority of today's communication carriage employs fiber-optic systems to convey classical information. During the past year, however, we turned to questions of quantum

information transmission and entanglement distribution. The quantum communication capacity $Q(\Lambda)$ of a channel governed by the trace-preserving completely positive map Λ is found from the coherent information, $I(\Lambda^{\otimes n}, \rho_A)$, for n channel uses with density operator ρ_A as follows [8,9]

$$Q(\Lambda) = \lim_{n\to\infty} \frac{1}{n} \max_{\rho} I(\Lambda^{\otimes n}, \rho_A).$$

The necessity of including multiple-letter (n>1) encoding arises from the fact that quantum channels need not be additive.

Unlike the case for classical channels, for which feedback does not increase channel capacity, having access to a classical communication channel between Alice (the quantum transmitter) and Bob (the quantum receiver) can increase quantum communication capacity. Indeed, one can define three new quantum communication capacities according whether the classical communication is one-way forward between Alice and Bob ($Q_{\rightarrow}$), one-way backward between Bob and Alice ($Q_{\leftarrow}$), or two way ($Q_{\leftarrow}$).

Entanglement is the cornerstone of quantum information science. Hence its distribution is of critical importance for many applications, and so the entanglement-distribution capacities of quantum channels — without classical-communication assistance (E) and with such assistance in either one-way forward ($E_{\rightarrow}$), one-way backward ($E_{\leftarrow}$), or two way ($E_{\leftrightarrow}$) — are of considerable interest. We summarize the known relationships between the preceding quantum and entanglement-distribution capacities in Fig. 1.

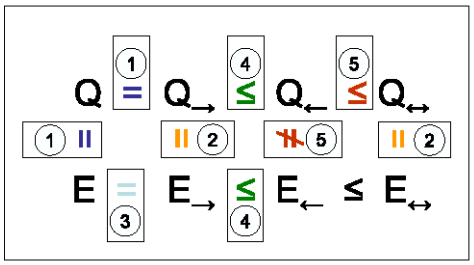

Figure 1. Relations between the quantum communication and entanglement-distribution capacities. The notes in this figure refer to the following. (1) The equality $E = Q = Q_{\rightarrow}$ was shown in [10]. (2) Any entanglement-distribution protocol can be transformed into a quantum communication protocol by appending teleportation to it. (3) This relation results from combining 1 and 2. (4) This result follows from combining 1, and 3, with the fact that increasing the feedback resources available cannot decrease capacity. (5) It is easy to prove that $E_{\leftarrow} = Q_{\leftrightarrow}$ for the erasure channel [11,12]. In [12] it was shown that the erasure channel satisfies the strict inequality $Q_{\leftarrow} < Q_{\leftrightarrow}$, which gives $E_{\leftarrow} \neq Q_{\leftarrow}$.

The coherent information can be expressed as $I(\rho_{RB})$, where $|\psi\rangle_{RA}$ is a purification of Alice's density operator obtained by adjoining a reference system *R*, and

$$I(\rho_{RB}) = S(\rho_B) - S(\rho_{RB})$$

with $S(\rho) \equiv -\mathrm{tr}[\rho \ln(\rho)]$ being the von Neumann entropy of density operator ρ. We have given operational meaning to the reverse coherent information,

$$I_R(\rho_{RB}) = S(\rho_R) - S(\rho_{RB}),$$

by showing that its maximum, over single-letter density operators for Alice, leads to a reverse coherent information capacity for entanglement distribution assisted by classical feedback that can exceed the unassisted capacity for the amplitude-damping channel and the generalized amplitude-damping channel [13].

Nonlinear Waveguide Polarization Entanglement Source The capability to efficiently generate high-quality entangled photons is key to many applications of photonic quantum information processing, such as quantum key distribution and linear optics quantum computing. In recent years most entanglement sources have been based on spontaneous parametric downconversion (SPDC) in a noncollinearly propagating, angle phase-matched crystal, such as beta barium borate (BBO) [14]. We have taken a different approach to entanglement generation that takes advantage of advances in nonlinear materials and utilizes standard techniques in nonlinear optics. We have employed the method of quasi-phase matching in periodically-poled potassium titanyl phosphate (PPKTP) or periodically-poled lithium niobate (PPLN) bulk crystals to enable efficient downconversion at user-specified wavelengths. During the past year we have developed a source of high quality polarization-entangled photons generated from a PPKTP waveguide that promises to be more efficient and compact than bulk-crystal sources. Additionally, the single spatial mode nature of the waveguide output can, in principle, be efficiently extracted into a single-mode fiber for easy transport and manipulation.

SPDC generation efficiency in bulk crystals is typically in the range of 10^{-12} to 10^{-8}, depending on the type of crystal, the crystal length, collection angle and bandwidth. Moreover, in a bulk crystal the total output flux from a bulk crystal is linearly proportional to the pump power and is not dependent on pump focusing. Nonlinear waveguides, on the other hand, have been shown to have a significantly higher SPDC efficiency. Fiorentino *et al*. made a direct comparison between the outputs from a waveguide on PPKTP and a bulk PPKTP crystal, showing a 50-fold enhancement in the case of the waveguide and in agreement with a semiclassical model based on the density of states of guided mode fields [15]. We have developed an alternative theoretical model for waveguide SPDC generation by taking into account the transverse index profile of a nonlinear crystal waveguide that imposes an effective transverse momentum on the phase-matching conditions. We find that the effective transversal grating leads to a broader transverse spatial bandwidth of the signal and idler outputs, which in turn explains the much higher spectral brightness of a waveguide SPDC source compared with a bulk-crystal SPDC source [16]. Our model gives essentially the same result as the model based on density of states, suggesting that the higher density of states comes from a larger transverse bandwidth due to the presence of the waveguide. The signal spectral brightness is given by

$$\frac{dP_s}{d\lambda_s} = \frac{16\pi^3 h\, d_{eff}^2 L^2 c P_p}{\varepsilon_0 n_s n_i n_p \lambda_s^4 \lambda_i} \frac{1}{A_{wg}} \mathrm{sinc}^2(\Delta k_z L/2),$$

where P_s is the signal power at wavelength λ_s, L is the length of the waveguide with a cross-sectional area A_{wg}. P_p is the pump power, λ_i is the idler wavelength, d_{eff} is the nonlinear coefficient, Δk_z is the momentum mismatch along the propagation z axis, and h is the reduction factor to account for focused beams. The waveguide cross section A_{wg} factor is what yields the large enhancement in generation efficiency over SPDC in bulk crystals.

The 16-mm long fiber-coupled Rb-indiffused PPKTP waveguide was fabricated by AdvR, Inc. for type-II phase matching with orthogonally polarized degenerate outputs at 1316 nm. We obtained a pair production rate of 2 x 10^7/s/mW of pump power in a 1.08-nm bandwidth, in good agreement with our theoretical estimate. Figure 2 shows the Hong-Ou-Mandel (HOM) quantum interference setup for measuring the indistinguishability of the signal and idler photons from the fiber-coupled PPKTP waveguide source. The orthogonally-polarized signal and idler were separated using a polarizing beam splitter (PBS), and a polarization controller in one of the output

paths was used to match the polarizations of both photons for interference measurements at the fiber 50/50 beam splitter. By blocking the residual pump light to eliminate any pump-induced fluorescence that might originate from downstream optical components and by using a tunable narrowband filter, we obtained an HOM quantum-interference visibility of 98.2% after subtraction of accidental coincidences (caused by the InGaAs avalanche photodiodes), as shown in Fig. 3, representing the highest reported value for a waveguide-based photon-pair source [16].

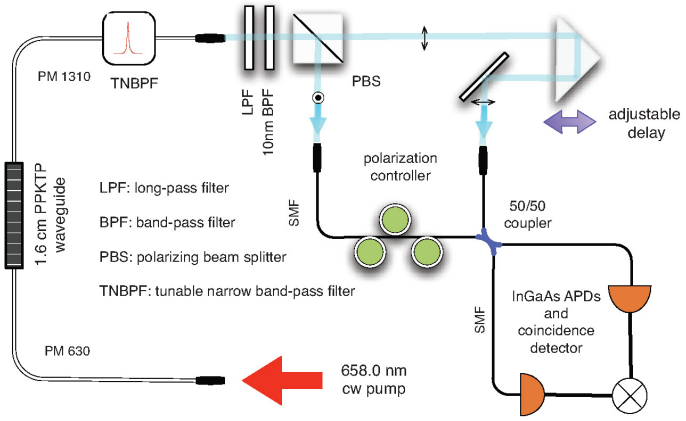

Figure 2. Schematic of experimental setup for Hong-Ou-Mandel two-photon quantum interference measurement. Three different types of spectral filters were used to eliminate residual pump light and out-of-band fluorescence to yield more accurate characterization of the PPKTP waveguide SPDC source.

The high HOM visibility of the waveguide device suggests that it is a suitable source for many quantum information processing applications that require compactness, high spectral brightness, and a high degree of indistinguishability. We took advantage of the high quality waveguide source to generate polarization-entangled photons at 1316 nm and collaborated with Professor Karl Berggren to demonstrate remote detection of entangled photons using his superconducting nanowire single-photon detector (SNSPD). SNSPDs are much better than InGaAs detectors for single-photon detection at telecom wavelengths because of low dark counts, high speed, and better detection efficiency [17]. See the chapter Quantum Nanostructures and Nanofabrication in this Report for details of the design, fabrication, and characteristics of SNSPDs.

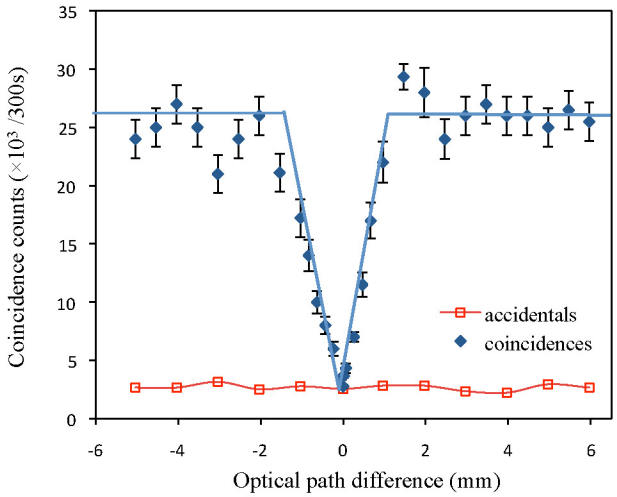

Figure 3. Measured HOM coincidences and accidentals counts in 300-s time intervals as function of the optical path difference between the signal and idler arms, yielding an HOM visibility of 98.2% with accidentals subtracted [16].

Figure 4 shows the experimental setup for polarization entanglement generation and a novel time-multiplexed scheme for two-photon coincidence detection using a single SNSPD. After separating the orthogonally polarized outputs from the PPKTP waveguide, we applied a relative time delay between the two photons to compensate for the birefringence imposed on them in the waveguide, thereby eliminating any temporal distinguishability between the two photons. We then combined the orthogonally polarized photons at a 50/50 fiber splitter, and a postselected polarization-entangled state was generated when there was one photon in each of the output paths of the 50/50 fiber splitter. This can be verified by two-photon coincidence measurements using a single SNSPD located in a separate laboratory and linked by two 200-m single-mode optical fibers. Each of the two entangled photons from the 50/50 coupler (labeled 1 and 2) was polarization analyzed with a half-wave plate and PBS and then sent through the optical fibers to the remote SNSPD location. Photon 2 had a 125-ns optical delay and the two photons were combined with a fiber coupler and sent to the fiber-coupled SNSPD. The time separation was larger than the reset time of the detector and therefore a single SNSPD was capable of performing coincidence measurements between the time-separated photons. Figure 5 shows the two-photon quantum-interference of polarization-entangled photons generated by the PPKTP waveguide. We obtained a quantum-interference visibility of 98.7% in the horizontal-vertical (*H*-*V*) basis and 96.2% in the antidiagonal-diagonal (*A*-*D*) basis, after subtraction of accidental coincidences [18].

The PPKTP waveguide source of photon pairs scores high on two key performance metrics, namely the spectral brightness and the degree of indistinguishability for the generated photon pairs. Our waveguide source has a ~40x greater pair generation efficiency compared with a bulk PPKTP crystal [19], yielding a pair production rate of 2 x 10^7/s/mW of pump power in a 1.1 nm bandwidth. The high visibility of the HOM quantum interference enabled us to produce polarization-entangled photons showing high-visibility two-photon quantum interference. We believe the compact nonlinear waveguide source with its high-quality single-spatial mode outputs will play an increasing role in future photonic sources for quantum information science such as linear optics quantum computing.

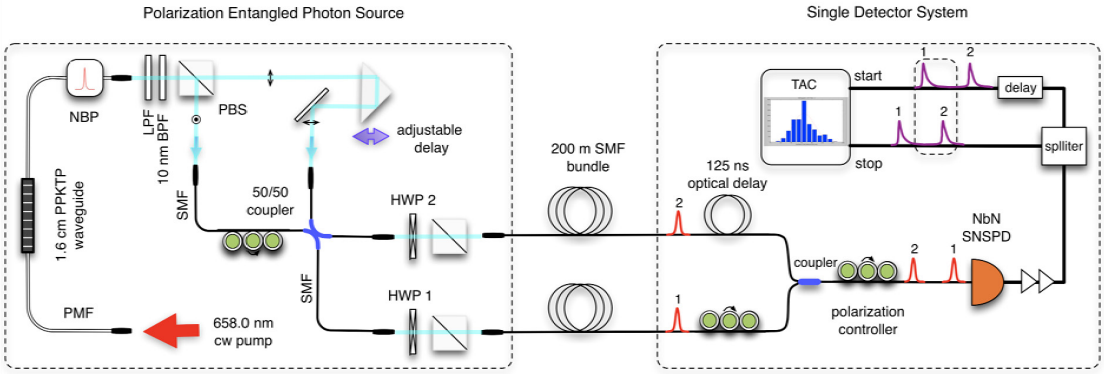

Figure 4. Schematic of experimental setup for polarization entanglement generation in PPKTP waveguide and time-multiplexed two-photon coincidence detection with a single SNSPD.

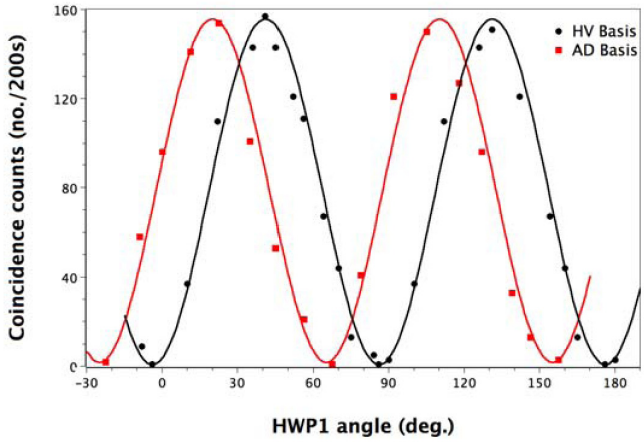

Figure 5. Two-photon quantum interference of polarization-entangled photons generated from a fiber-coupled PPKTP waveguide and detected by a single SNSPD in a time-multiplexed measurement scheme, showing visibilities of 98.7% and 96.2% in the H-V and A-D bases, respectively.

Imaging with Phase-Sensitive Light We have been exploring the use of phase-sensitive light in a variety of imaging scenarios in both quantum and quantum-mimetic imaging scenarios. A pair of Gaussian-state light beams that possess a phase-sensitive cross-correlation can be produced by continuous-wave (cw) spontaneous parametric downconversion (SPDC) with vacuum-state signal and idler inputs [19-21]. The low-flux limit of cw SPDC can then be approximated by a vacuum state plus a frequency-entangled biphoton. Many quantum imaging scenarios have been characterized — both theoretically and experimentally — in terms of post-selected biphoton detection, e.g., quantum optical coherence tomography [22,23], ghost imaging [24], and two-photon imaging [25,26]. The primary objective of our work has been to clearly delineate the boundary between classical and quantum behavior in these and other imaging scenarios and to use this understanding to develop new, and more robust imaging schemes that offer advantages over classical techniques. What follows is a brief summary of our recent results on optical coherence tomography. Our recent work on ghost imaging will be described in the section to follow.

Optical coherence tomography (OCT) produces 3-D imagery through focused-beam scanning (for transverse resolution) and interference measurements (for axial resolution). Conventional OCT (C-OCT) uses classical-state signal and reference beams, with a phase-insensitive cross-correlation, and measures their second-order interference in a Michelson interferometer [27]. Quantum OCT (Q-OCT) employs signal and reference beams in an entangled biphoton state, and measures their fourth-order interference in a Hong-Ou-Mandel (HOM) interferometer [22,23]. In comparison to C-OCT, Q-OCT offers the advantages of a two-fold improvement in axial resolution and even-order dispersion cancellation. Q-OCT's advantages have been ascribed to the non-classical nature of the entangled biphoton state, but we have shown that it is the phase-sensitive cross-correlation between the signal and reference fields, rather than non-classical behavior *per se*, that provides the axial resolution improvement and even-order dispersion cancellation [28]. Based on this understanding, we proposed a new OCT configuration — phase-conjugate OCT (PC-OCT) — which can exploit classical signal and reference beams with phase-sensitive cross-correlation to achieve the factor-of-two axial resolution improvement and the even-order dispersion cancellation reaped by Q-OCT. PC-OCT, shown schematically in Fig. 6, employs a double-pass interrogation of the sample being imaged — with a conjugate amplifier sandwiched in between these interrogations — followed by a Michelson interferometer measurement module as used in C-OCT. The conjugate amplifier converts the phase-sensitive cross-correlation between signal and reference into a phase-insensitive cross-correlation that can be sensed with the Michelson (second-order) interferometer. Q-OCT, on the other hand, needs a Hong-Ou-Mandel (fourth-order) interferometer, in order to measure phase-sensitive cross-correlation.

Unlike Q-OCT, PC-OCT can use strong fields, hence it may be applicable to standoff sensing as well as microscopy.

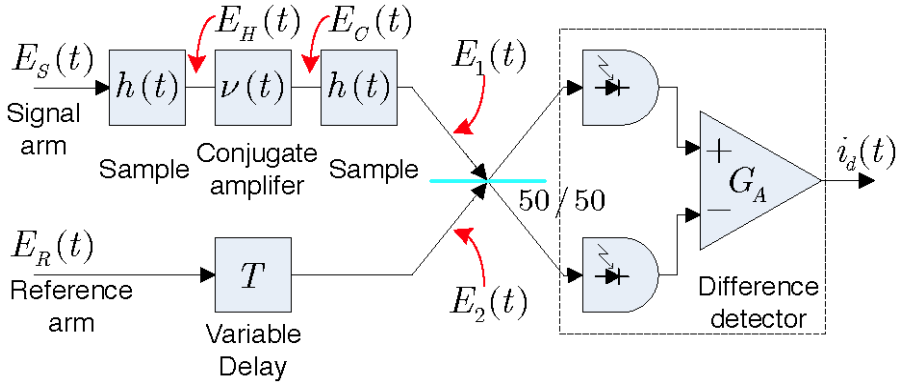

Figure 6. Schematic for phase-conjugate optical coherence tomography. The signal and reference are broadband light beams with a phase-sensitive cross correlation. The signal is transmitted to a target represented by a linear time-invariant filter $h(t)$ — shown here in transmission, but in the real application it would be seen in reflection — and then phase conjugated upon its return in a parametric device with impulse response $\nu(t)$. The conjugate beam re-interrogates the target after which it is interfered with the delayed reference in a Michelson interferometer. Axial information is derived from the location of peak fringe visibility.

Two key components necessary for implementing PC-OCT are a classical source of phase-sensitive cross-correlated signal and reference beams and a phase-conjugate amplifier, which can be realized with a strongly-driven parametric downconverter. We have developed a pulsed source of single-mode broadband amplified spontaneous parametric downconversion based on a strongly pumped type-0 phase-matched periodically poled MgO-doped lithium niobate (PP-MgO:LN) crystal [29]. Ultrabroadband SPDC was obtained with a 20-mm long crystal yielding a phase-matching bandwidth of 132 nm centered at 1560 nm, and we chose to evaluate the performance of amplified SPDC in two narrow spectral output regions at 1550 and 1570 nm. The pulsed pump was a frequency-doubled narrowband mode-locked fiber laser at 780 nm with 50-ps pulses, an average output power greater than 2 W, and a repetition rate of 31 MHz. By optimally focusing the pump into the PP-MgO:LN crystal, we were able to concentrate ~70% of the typically multimode downconverted output into a single spatial mode, of which 82% was coupled into a single-mode fiber. High peak powers of the pump laser in the kW range permitted us to drive the downconverter into the nonlinear regime in which amplification of the spontaneously emitted output occurred. Figure 7 shows the single-mode SPDC output power per nm of bandwidth as a function of the average pump power, showing clearly exponential growth due to parametric amplification of parametric fluorescence for pump powers greater than 0.5 W. At a spectral brightness level of 1 nW/nW and a bandwidth of 5 nm, each fiber-coupled output pulse contained ~600 photon pairs that could be easily detectable by a high-sensitivity InGaAs pin photodetector.

We have also operated a second strongly pumped PP-MgO:LN crystal as an optical parametric amplifier (OPA) that served as the phase-conjugate amplifier for PC-OCT [29]. For a continuous-wave (cw) input at 1570 nm to the OPA we measured the output power at 1550 nm and obtained the parametric gain G of the OPA as a function of the average pump power, as shown in Fig. 8. More relevant to PC-OCT was to input the 1570-nm signal from our pulsed SPDC into the OPA. At 1.3 W pump power, we obtain a parametric gain of ~14 dB and the amplified conjugate output at 1550 nm had a pulse width of 50 ps. The observed pulse width, shown in Fig. 9, is narrower than one would expect from the linear convolution of the input signal pulse (25 ps) and the pump pulse (50 ps). The conjugate idler pulse narrowing was due to the strong pump power, such that the OPA gain is higher at the center of the idler pulse than in its wings.

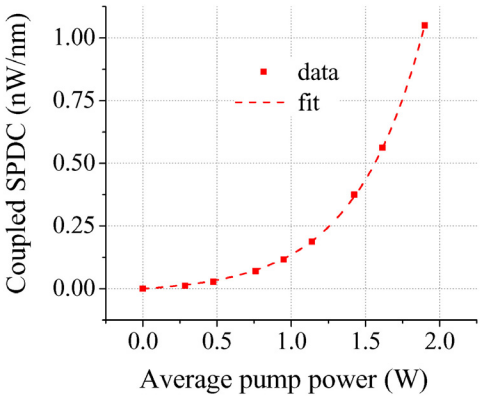

Figure 7. Spectral brightness of parametric fluorescence measured at the output of a single-mode fiber as a function of average pump power. Dashed line shows exponential fit. The spectral brightness level in the linear regime is 46 pW/nm/W.

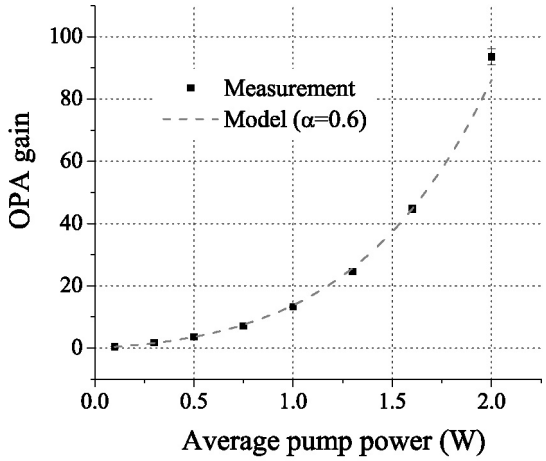

Figure 8. Measured OPA gain (solid squares) and theoretical values (dashed line) as functions of the average pulsed pump power. The theoretical model uses a fitting factor of 0.6 to account for the temporal mismatch between the pulsed pump and the cw signal input.

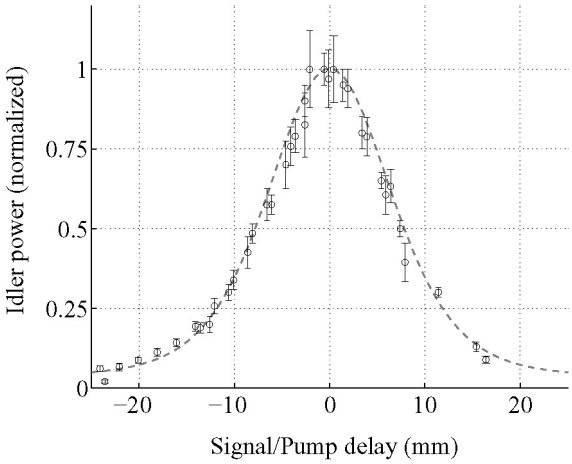

Figure 9. Normalized idler power of OPA as a function of the pump-signal spatial delay and theoretical values (dashed curve). The idler power envelope width (full width at half maximum) is 15 mm (50 ps).

Figure 10 is a schematic of our experimental setup for demonstrating that axial resolution is improved by a factor of two with dispersion cancellation in PC-OCT. The output from the pulsed SPDC source was spectrally separated with a coarse wavelength division multiplexer (CWDM) into a signal channel at 1570 nm and a reference channel at 1550 nm. The signal light was sent through a 50-m single-mode fiber (SMF-28) to a reflective target whose relative position was to be determined. The returned signal light was directed to the high-gain OPA to generate the phase-conjugate signal at 1550 nm and the OPA also provided gain to overcome transmission losses in our laboratory setup. The amplified conjugate beam at 1550 nm was then sent to the target one more time, through the 50-m fiber, and collected via a second CWDM for input to a fiber-optic Michelson interferometer. We used an interference filter with a 5.9-nm bandwidth centered at 1550 nm to set the operating bandwidth of the PC-OCT experiment, and hence the effective pulse width of the signal and reference channels was ~0.7 ps. The roundtrip passage through the 50-m SMF-28 fiber and additional fibers in the setup would have broadened the pulse to ~15 ps due to dispersion (17 ps/km/nm) if there were no dispersion cancellation. For the reference path, we used a dispersion-shifted LEAF fiber (4.2 ps/km/nm) to replace most of the reference fiber length, so that the reference pulse was broadened to ~5 ps. Dispersion cancellation due to phase conjugation of the signal was expected to reduce the dispersive broadening in the signal channel significantly (but not to zero, because of residual fiber lengths that were uncompensated). Interferometric measurements between the returned beam and the reference beam then yielded the relative location of the target as the target was translated.

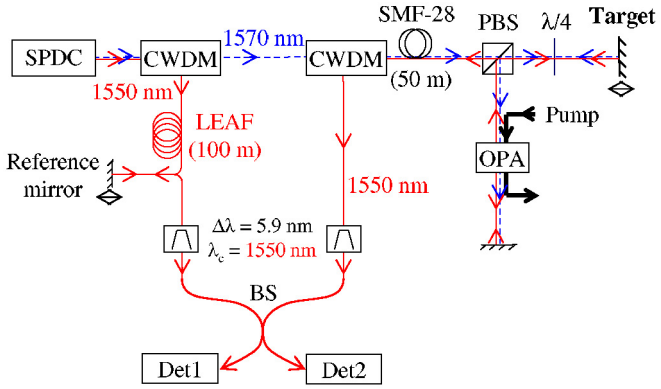

Figure 10. Schematic for phase-conjugate optical coherence tomography experimental setup.

At each target position, we scanned the reference mirror to tune the relative delay between the reference pulse and the return pulse. The interferometric signal was measured with a high-sensitivity InGaAs pin photodetector and the interference envelope amplitude was recorded for each reference mirror position and each target location, as shown in Fig. 11 for three different target locations. Adjacent target positions were separated by a distance of 450 μm. Compared with a classical OCT measurement (such as in Fig. 10 by not interrogating the target mirror twice), the shift in the reference mirror was twice as large as the target positional shift. For the same envelope width, this implies a factor-of-two better axial resolution because the signal (reference mirror shift) to noise (envelope width) ratio is twice as large in the double-pass PC-OCT configuration. We measured an interference envelope width of 890 ± 30 μm, or 6 ± 0.2 ps in time after doubling the spatial delay to account for the double-pass configuration. The 6-ps width was in line with our expectation that it was primarily due to the small amount of LEAF-fiber dispersion in the reference channel (5 ps) plus some small residual dispersion in the signal channel. More importantly, the measured envelope width was a clear indication that dispersion in the reference channel was cancelled by the PC-OCT's phase-conjugation technique. The results of 2x axial resolution and dispersion cancellation that can be achieved by Q-OCT and a completely classical technique of PC-OCT confirms that the origin of these results comes from the phase-sensitive cross correlation of the signal and reference beams.

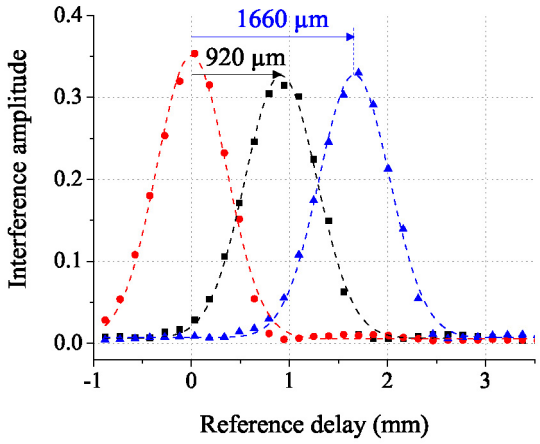

Figure 11. Interference envelope amplitudes for three target positions with adjacent separation of 450 μm. Envelope width was measured to be 890 ± 30 μm, caused mainly by dispersion in the reference channel.

Ghost Imaging Ghost imaging is the acquisition of the transmittance pattern of an object through intensity correlation measurements, and it has been demonstrated with both thermal (classical) light and biphoton (quantum) light [24,30-32]. We have used our coherence theory [33] for Gaussian-state sources — which encompasses both thermal light and biphoton-state light as special cases — to show that almost all the characteristics of quantum ghost imaging are due to the phase-sensitive cross correlation between the signal and reference beams [34]. The particular ghost-imaging setup that we considered is shown in Fig. 12. For this arrangement we showed that thermal light, classical phase-sensitive light, and quantum phase-sensitive light all yield ghost images in both near-field and far-field operation. The same image inversion that has been seen in the quantum phase-sensitive light case, but not the thermal light case, turns out to be present for ghost imaging with classical phase-sensitive light. If the ghost-imager's source fields are constrained to have specific phase-insensitive auto-correlations, then quantum light offers a spatial resolution advantage in the source's near field and improved field-of-view in the far field. The principal advantage of quantum ghost imaging, however, comes from the near-absence of any background term in the ghost image. During the past year we have completed a comprehensive analysis of the signal-to-noise ratio behavior obtained with thermal light, classical phase-sensitive light, and quantum phase-sensitive light [35], as well as conceiving two new configurations for ghost imaging [36], as summarized below.

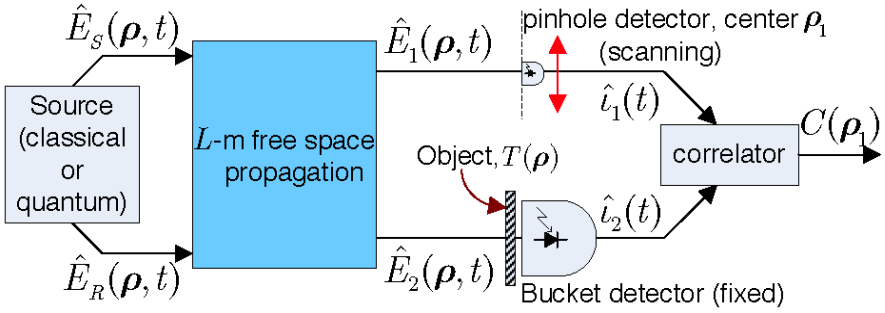

Figure 12. Schematic for ghost imaging. The signal and reference are broadband light beams with either a phase-insensitive or phase-sensitive cross correlation. After propagation over an *L*-m-long free space path, the signal beam illuminates a scanning pinhole detector and the reference illuminates an object transmittance mask followed by a large-area (bucket) detector. Cross correlating the resulting (shot-noise limited) photocurrents as the pinhole detector is scanned yields the ghost image.

Figure 13 compares the signal-to-ratios (SNRs) of quantum-state (left panel) and thermal-state (right panel) ghost imagers as functions of the brightness of the fields arriving at the object

transmittance mask for various values of the time-bandwidth product, i.e., the source coherence time multiplied by the photodetector's electrical bandwidth [35]. Because quantum-state (SPDC) sources are inherently broadband, whereas pseudothermal (laser light passed through a rotating ground-glass diffuser) are inherently narrowband, with respect to typical photodetector bandwidths, the $\Omega_B T_0$ values we have chosen are different for the two sources. In both cases, however, there is a high-brightness asymptote that is due to speckle fluctuations, and in both cases there is a low-brightness asymptote that is set by photon-flux limitations.

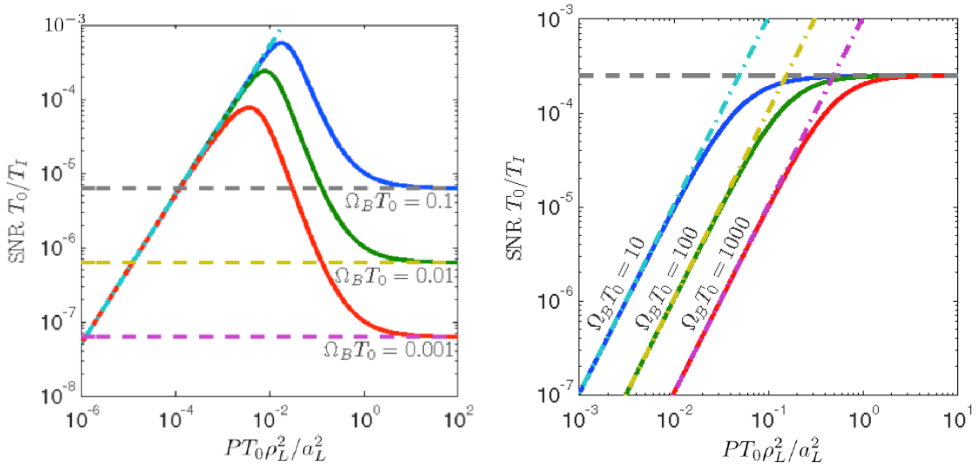

Figure 13. Ghost imaging SNR behavior for far-field propagation of a quantum-state source (left panel) or a thermal-state source (right panel) versus the source brightness at the object transmittance plane. T_0 and T_I are the source coherence time and ghost-imaging integration time, respectively, and Ω_B is the photodetector's electrical bandwidth. In both cases, the high-brightness asymptote represents speckle-noise limited SNR. In both cases the low-brightness asymptotes represent flux-limited SNR.

Our SNR analysis permits, for the first time, a meaningful comparison between quantum-state and thermal-state ghost imaging performance with respect to their image acquisition time. i.e., the integration time required to achieve a desired SNR value for the image. For the important case of far-field broadband entangled-state imaging versus far-field narrowband thermal-state imaging we find that neither one enjoys a universal advantage, viz., depending on the parameter values involved either the quantum or the classical-state system may have the shorter image acquisition time [35].

The correlation-based theory we have developed for ghost imaging has recently led us to conceive two novel configurations for ghost imaging: spatial-light modulator (SLM) ghost imaging and computational ghost imaging [36], as shown in Fig. 14 and 15, respectively. In SLM ghost imaging we transmit a cw laser beam through a spatial-light modulator that imposes an independent deterministic phase shift on each pixel such that the output field mimics a source of low spatial coherence. The rest of the setup is the same as a thermal-light lensless ghost imager. Our analysis shows that this arrangement yields a far-field ghost image with the essentially the same field-of-view and spatial resolution characteristics as found previously for thermal-state ghost imaging. In particular, the field of view is inversely proportional to the effective coherence length at the output of the SLM and the spatial resolution in inversely proportional to the beam size at the output of the SLM.

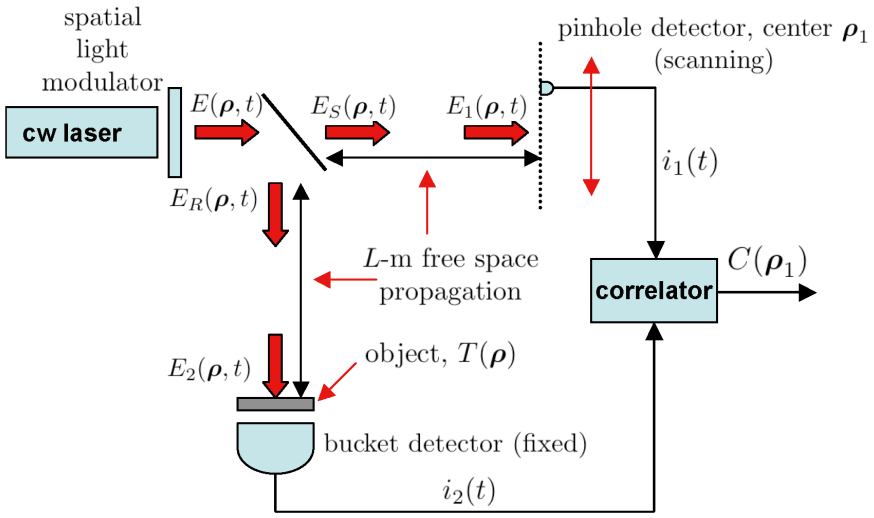

Figure 14. Configuration for spatial-light modulator ghost imaging. The output from a cw laser is passed through a spatial light modulator driven by deterministic waveforms that impose different phase shifts on each pixel such that the output field mimics a source of low spatial coherence. The remainder of the setup is the same as a thermal-light lensless ghost imager.

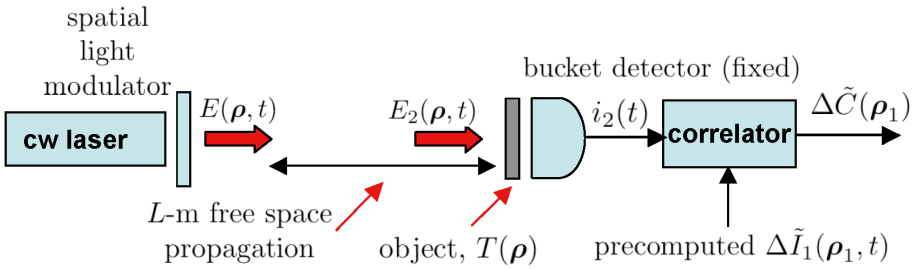

Figure 15. Configuration for computational ghost imaging. The output from a cw laser is passed through a spatial light modulator driven by deterministic waveforms that impose different phase shifts on each pixel such that the output field mimics a source of low spatial coherence. The remainder of the setup is the same as a thermal-light lensless ghost imager except that the reference path is derived by computing the free-space diffraction integral of the output field obtained from the spatial light modulator.

The transition from SLM ghost imaging to computational ghost imaging arises from the realization that we can precompute the reference field arriving at the high-resolution detector, in this case, because it is due to free-space diffraction of the deterministic light field obtained from passing the cw laser beam through the spatial light modulator. Aside from eliminating the need for a high spatial-resolution reference-path detector, computational ghost imaging allows the reference field to be precomputed for a range of path lengths, hence by correlating the bucket detector's output with these precomputed quantities permits range sectioning to be performed using a single data collection, something that is not possible in conventional ghost imaging. In this regard it is worth noting that proof-of-principle experiments have already demonstrated the basic features we predicted for computational ghost imaging [37].

Physical Simulation of the Asymmetric Cloning BB84 Attack The Bennett-Brassard 1984 quantum key distribution (BB84 QKD) protocol is the most mature application in quantum information processing and is poised for deployment in the near future. The BB84 protocol is a technique to securely distribute secret keys for one-time pad encryption and is considered to be unconditionally secure by the laws of physics under a specified set of operating conditions. It is, useful, however, to verify its security by attacking the BB84 system. Previously we have demonstrated a physical simulation of the entangling-probe attack on BB84 [38,39] using single-

photon two-qubit (SPTQ) quantum logic [40]. Eve uses a controlled-NOT (CNOT) gate to interact her probe qubit with Alice's qubit in a unitary manner, then sends Alice's qubit to Bob, and performs a positive operator-valued measurement on her probe qubit. The CNOT gate interaction allows Eve to obtain some information on Alice's qubit, but it also disturbs Alice's qubit and produces an error that Alice and Bob can detect and discard. Our SPTQ implementation, which utilizes both momentum and polarization degrees of freedom of a single photon, is both efficient and deterministic. Our experimental results agree with theoretical predictions; however, the experiment is only a physical simulation because with SPTQ implementation it is necessary for Eve to share the detection apparatus with Bob in order to measure both qubits of a single photon.

The entangling-probe method is the most powerful individual-qubit attack for a BB84 protocol that discards the errors. However, it has been pointed out that for error-correcting protocols the entangling-probe attack is not optimal [41]. Indeed, the optimal attack for BB84 with error-correcting post processing is the asymmetric Fourier-covariant cloning machine (AFCCM) attack [42], which optimally and uniformly copies the states in the computational and incompatible bases. Here, “asymmetric” denotes the fact that the two copies of the input state — the one Eve sends to Bob and the one she retains — have different fidelities. This fidelity inequality enables the tradeoff between the amount of information that Eve gleans versus the quantum bit error rate (QBER) she creates.

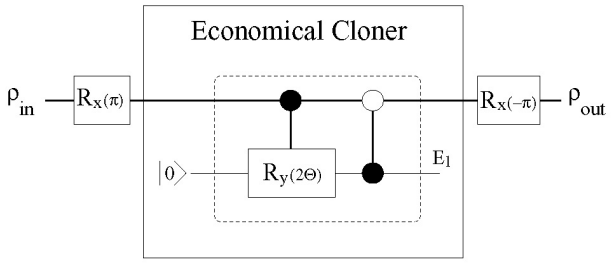

Figure 16. In the economical cloner Eve prepares her ancilla in the $|0\rangle$ state, which interacts with Alice's state through a controlled rotation about the *y*-axis of the Bloch sphere, followed by a CNOT gate. A π rotation about the *x*-axis before and after the economical cloner is required to put Alice's qubit in the proper frame of reference in Eve's Bloch sphere.

For BB84, a simpler version of the AFCCM attack can be implemented by taking advantage of the fact that the four states which are involved in BB84, namely *H*, *V*, *D* (+45°) and *A* (-45°), all reside on an equatorial plane of the Bloch sphere. Figure 16 shows a circuit diagram of this economical phase-covariant cloning attack, so called because it requires only one ancilla qubit to accomplish the cloning task. More interestingly is that the economical cloning attack can also be physically simulated with SPTQ quantum logic gates, such as CNOT [43] and SWAP [44] gates. The amount of information Eve obtains about Alice's qubit is determined by the controlled rotation ($R_y(2\theta)$) which can be implemented easily using two half-wave plates. A major difference between the entangling-probe and the economical cloning attacks is that in the cloning attack Eve must measure her ancilla qubit in the same basis as that used by Alice and Bob.

Figure 17 shows a quantum circuit diagram for our SPTQ implementation of the economical cloner. Alice's qubit at the input is in one of four linear polarization states *H*, *V*, *D*, *A* that are first mapped into *RC*, *LC*, *D*, *A* by a rotation R to simplify the SPTQ implementation, where *RC* and *LC* denote right-circular and left-circular polarization, respectively. This initial mapping is accomplished by use of a quarter-wave plate (QWP) with its fast and slow axes aligned with the *D* and *A* polarization axes, as shown in the left panel of Fig. 18. After the initial mapping, the main step of the economical cloner is a controlled rotation $R_y(2\theta)$ of Eve's qubit. A linear rotation $R_y(2\theta)$ about the y-axis of the Bloch sphere with an arbitrary angle θ for any linear polarization is more easily accomplished in the polarization space than in the momentum space. We therefore

apply a SWAP between the Alice's polarization qubit and Eve's momentum qubit of the same photon so that the controlled rotation of Eve's qubit (now in polarization) can be done with a half-wave plate (HWP), as shown in the right panel of Fig. 18. After the controlled rotation, Alice and Eve's qubits are swapped again, each to its original polarization and momentum space, respectively. Finally, the inverse rotation R^{-1} is applied to map the final state of Alice's qubit back to the *H*, *V*, *D*, *A* states before sending it to Bob for measurements.

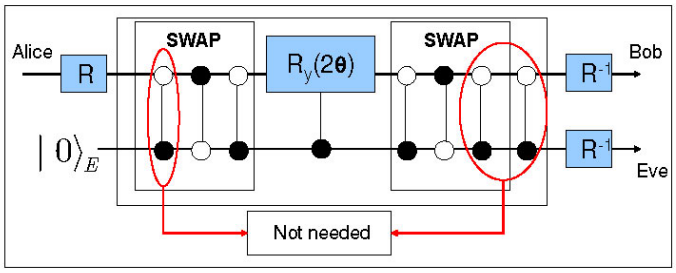

Figure 17. Quantum circuit diagram for SPTQ implementation of the economical cloner. Polarization and momentum qubits are represented by the upper and lower rails, respectively. Initial rotation R of Alice's qubit puts it on the equator of the Bloch sphere, while a subsequent inverse rotation R^{-1} restores the original orientation. The economical cloner is implemented using two SWAP gates and a controlled rotation $R_y(2\theta)$. The initial momentum-controlled NOT (M-CNOT) gate is not needed because Eve's input is in the state $|0\rangle$, and the last two M-CNOT gates cancel each other.

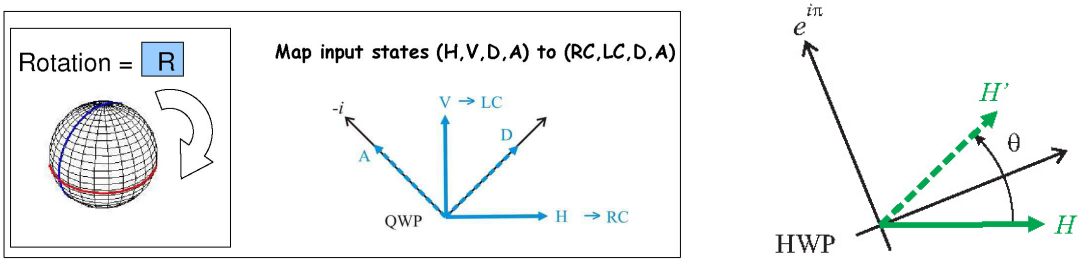

Figure 18. Left: The π rotation about the Bloch-sphere's x axis uses a QWP with its slow axis aligned with the antidiagonal (*A*) polarization to transform the states *H*, *V*, *D*, *A* into *RC*, *LC*, *D*, *A*. The inverse rotation R^{-1} is accomplished by aligning the QWP's slow axis with the diagonal (*D*) polarization. Right: For an initial state along *H*, the controlled rotation $R_y(2\theta)$ is implemented using a HWP with its fast axis aligned at an angle $\theta/2$ from the *H* polarization axis, thus rotating it by an angle θ.

The relatively simple SPTQ implementation of the economical cloner in Fig. 17 using previously demonstrated SPTQ logic gates suggests that a physical simulation can be realized using realistic sources and SPTQ gates. The economical cloner uses more SPTQ gates than the previously demonstrated entangling-probe (CNOT gate) attack. It is therefore our expectation that implementing the economical cloner using SPTQ gates is feasible but perhaps more difficult than the entangling-probe attack. The ability to implement optimal individual attacks such as the economical cloner should provide the QKD community with experimentally realistic data for testing BB84 eavesdropping vulnerability and learning about the interplay between security and post-processing protocols.

Quantum Illumination Loss and noise can quickly destroy entanglement, so it has commonly been thought that there is little reason to employ entangled light sources in such scenarios. Lloyd [47], however, showed that "quantum illumination" can reap substantial benefits, from the use of entanglement in target detection, despite the presence of loss-destroying loss and noise. In

Lloyd's quantum-illumination paradigm, a photonic source creates *d*-mode maximally entangled signal and ancilla beams each containing a single photon. The signal beam irradiates a target region containing a very weak thermal-noise bath — with an average of $b << 1$ photons per mode — in which a low-reflectivity object might be embedded. The light received from this region — together with the retained ancilla beam — is then used to decide whether the object is present or absent. Lloyd showed that quantum illumination, with the optimum joint measurement on the received light and the ancilla, achieves a much higher signal-to-background ratio than that realized by optimum quantum reception of light received in response to transmission of a single unentangled photon.

The analysis in [47] was confined, primarily, to the vacuum plus single-photon manifold, wherein at most one photon arrives at the receiver during the measurement interval regardless of whether the object of interest in absent or present in the target region. During the past year we remedied that deficiency by providing a full Gaussian-state treatment of quantum-illumination target detection [48]. We employed the exact quantum statistical model for the entangled signal and idler beams obtained from continuous-wave (cw) spontaneous parametric downconversion (SPDC) in the absence of pump depletion [16] in conjunction with the standard model for the lossy, bosonic channel [4]. We showed that in a very lossy, very noisy environment, a low-brightness quantum-illumination system enjoys a substantial improvement in the effective signal-to-background ratio — which translates into a very large reduction in the target-detection error probability — in comparison to that achieved by a coherent-state transmitter of the same average photon number. Just as Lloyd found in [47], the SPDC quantum illumination advantage that we have derived accrues despite there being no entanglement between the light that is received from the target region and the retained idler. Quantum illumination is thus the first example of an entanglement-based performance gain, in a full bosonic-channel setting, that survives entanglement-killing loss and noise.

Figure 19 summarized the results that we have found for target detection using bosonic quantum illumination [47]. Here we have plotted error-probability bounds on optimum receivers for coherent-state and quantum-illumination systems of the same average transmitted photon number. In both cases N_S is the average number of transmitted photons per mode, N_B is the average number of received background photons per mode, κ is the roundtrip (transmitter-to-target-to-receiver) channel transmissivity, and M is the number of modes employed. The solid curves are the Chernoff bound and the Bhattacharyya bound, respectively, on the error probabilities of the optimum quantum receivers for coherent-state and quantum-illumination transmitters. The former is an exponentially-tight upper bound, whereas the latter, in this case, is approximately so. The dashed curve is a lower bound, which in general is loose, on the error probability of the coherent-state system. Figure 18 shows that for M sufficiently large quantum illumination has an error probability that can be much smaller than that of the coherent-state system. Moreover, we have shown that the lower bound in this figure also applies to all classical-state transmitters, revealing that entangled-state quantum illumination achieves performance beyond that of any such conventional target-detection system.

Additional Theoretical Work In addition to the research accomplishments detailed above, our group has also made significant progress in several other theoretical areas. These include the theory of quantum temporal phase and instantaneous frequency [48,49]. Here we have built a general theory — guided by classical estimation theory — that leads to optimal designs for homodyne phase-locked loops in both input-output and state-variable forms. We have also shown two ways in which quantum resources can allow images to be obtained whose resolutions exceed classical diffraction limits [50,51]. We are presently planning proof-of-principle experiments to demonstrate some of these quantum-enhanced capabilities.

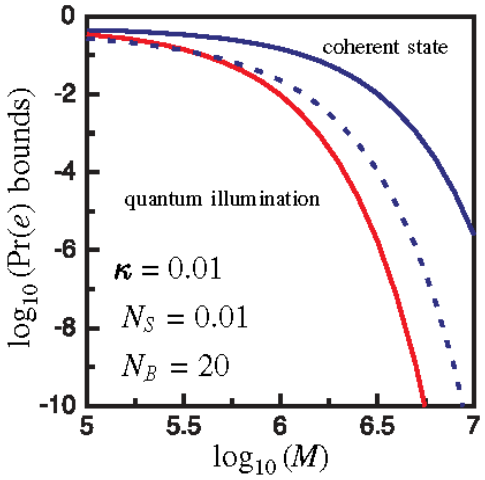

Figure 19. Upper bounds (solid curves) on the target-detection error probabilities for coherent-state (Chernoff bound) and quantum-illumination (Bhattacharyya bound) transmitters with *M* transmitted modes. Also shown is the lower bound (dashed curve) for the coherent-state case, which applies to all classical-state transmitters with the same total average transmitted photon number. For large *M*, the classical-state lower bound exceed the quantum-illumination upper bound

References

1. C. E. Shannon, "A Mathematical Theory of Communication, Part I," *Bell Syst. Tech. J*. 27, 379-423 (1948).

2. C. E. Shannon, "A Mathematical Theory of Communication, Part II," *Bell Syst. Tech. J*. 27, 623-656 (1948).

3. V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, "Classical Capacity of the Lossy Bosonic Channel: the Exact Solution," *Phys. Rev. Lett*. 92, 027902 (2004).

4. V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, B. J. Yen, and H. P. Yuen, "Classical Capacity of Free-Space Optical Communication," in *Quantum Information, Statistics, Probability* ed. O. Hirota (Rinton Press, New Jersey, 2004).

5. B. J. Yen and J. H. Shapiro, "Multiple-Access Bosonic Communications," *Phys. Rev. A* 72, 062312 (2005).

6. S. Guha, J. H. Shapiro, and B. I. Erkmen, "Classical Capacity of Bosonic Broadcast Communication and a Minimum Output Entropy Conjecture," *Phys. Rev. A* 76, 032303 (2007).

7. S. Guha, J. H. Shapiro, and B. I. Erkmen, "Capacity of the Bosonic Wiretap Channel and the Entropy Photon-Number Inequality," *Digest of the 2008 International Symposium on Information Theory*, Toronto, Canada, July 6-11, 2008.

8. S. Lloyd, "Capacity of the Noisy Quantum Channel," *Phys. Rev. A* 55, 1613-1622 (1997).

9. I. Devetak, "The Private Classical Capacity and the Quantum Capacity of a Quantum Channel," *IEEE Trans. Inform. Theory* 51, 44-55 (2005).

10. V. Giovannetti and R. Fazio, “Information-Capacity Description of Spin-Chain Correlation,” *Phys. Rev. A* 71, 032314 (2005).

11. H. Barnum, E. Knill, and M. A. Nielsen, “On Quantum Fidelities and Channel Capacities,” *IEEE Trans. Inform. Theory* 46, 1317-1329 (2000).

12. D. Leung, J. Lim, and P. W. Shor, *Phys. Rev. Lett*. (to be published).

13. R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, “Reverse Coherent Information,” *Phys. Rev. Lett*. 102, 210501 (2009).

14. P. G. Kwiat, E. Waks, A. G. White, I. Appelbaum, and P. H. Eberhard, “Ultrabright Source of Polarization-Entangled Photons,” *Phys. Rev. A* 60, R773-R776 (1999).

15. M. Fiorentino, S. M. Spillane, R. G. Beausoleil, T. D. Roberts, P. Battle, and M. W. Munro, “Spontaneous Parametric Down-Conversion in Periodically Poled KTP Waveguides and Bulk Crystals,” *Opt. Express* 15, 7479-7488 (2007).

16. T. Zhong, F. N. C. Wong, T. D. Roberts, and P. Battle, "High Performance Photon-Pair Source based on a Fiber-coupled Periodically Poled $KTiOPO_4$ Waveguide," *Opt. Express* 17, 12019-12030 (2009).

17. K. M. Rosfjord, J. K. W. Yang, E. A. Dauler, A. J. Kerman, V. Anant, B. M. Voronov, G. N. Gol'tsman, and K. K. Berggren, “Nanowire Single-Photon Detector with an Integrated Optical Cavity and Anti-Reflection Coating,” *Opt. Express* 14, 527-534 (2006).

18. T. Zhong, X. Hu, F. N. C. Wong, C. Herder, F. Najafi, K. Berggren, T. D. Roberts, and P. Battle, “Towards High Quality Photonic Polarization Entanglement Distribution at 1.3-μm Telecom Wavelength,” Postdeadline paper, *International Quantum Electronics Conference*, Baltimore, MD, May 31 - June 5, 2009.

19. F. N. C. Wong, J. H. Shapiro, and T. Kim, “Efficient Generation of Polarization-Entangled Photons in a Nonlinear Crystal,” *Laser Phys.* 16, 1517-1524 (2006).

20. J. H. Shapiro and N. C. Wong, “An Ultrabright Narrowband Source of Polarization-Entangled Photon Pairs,” *J. Opt. B: Quantum Semiclass*. *Opt*. 2, L1-L4 (2000).

21. J. H. Shapiro and K.-X. Sun, “Semiclassical versus Quantum Behavior in Fourth-Order Interference,” *J. Opt. Soc. Am. B* 11, 1130-1141 (1994).

22. A. F. Abouraddy, M. B. Nasr, B. E. A. Saleh, A. V. Sergienko, and M. C. Teich, “Quantum Optical Coherence Tomography with Dispersion Cancellation,” *Phys. Rev. A* 65 053817 (2002).

23. M. B. Nasr, B. E. A. Saleh, A. V. Sergienko, and M. C. Teich, “Demonstration of Dispersion-Canceled Quantum-Optical Coherence Tomography,” *Phys. Rev. Lett*. 91, 083601 (2003).

24. T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, “Optical Imaging by Means of Two-Photon Quantum Entanglement,” *Phys. Rev. A* 52, R3429-R3432 (1995).

25. M. D’Angelo, M. V. Chekhova, and Y. Shih, ``Two-Photon Diffraction and Quantum Lithography,” *Phys. Rev. Lett*. 87, 013602 (2001).

26. Y. Shih, “Quantum Imaging,” *IEEE J. Sel. Top. Quantum Electron*. 13, 1016-1030 (2007).

27. J. M. Schmitt, “Optical Coherence Tomography: A Review,” *J. Sel. Top. In Quantum Electron*. 5, 1205-1215 (1999).

28. B. I. Erkmen and J. H. Shapiro, “Phase-Conjugate Optical Coherence Tomography,” *Phys. Rev. A* 74, 041601(R) (2006).

29. J. Le Gouët, D. Venkatraman, F. N. C. Wong, and J. H. Shapiro, “Classical Low-Coherence Interferometry based on Broadband Parametric Fluorescence and Amplification,” *Opt. Express* 17, 17874-17887 (2009).

30. F. Ferri, D. Magatti, A Gatti, M. Bache, E. Brambilla, and L. A. Lugiato, “High Resolution Ghost Image and Ghost Diffraction Experiments with Thermal Light,” *Phys. Rev. Lett*. 94, 183602 (2005).

31. G. Scarcelli, V. Berardi, and Y. Shih, “Can Two-Photon Correlation of Chaotic Light Be Considered as Correlation of Intensity Fluctuations?,” *Phys. Rev. Lett*. 96, 063602 (2006).

32. R. Meyers, K. Deacon, and Y. Shih, “Ghost-imaging Experiment by Measuring Reflected Photons,” *Phys. Rev. A* 77, 041801(R) (2008).

33. B. I. Erkmen and J. H. Shapiro, “Optical Coherence Theory for Phase-Sensitive Light,” *Proc. SPIE* 6305, 6305G (2006).

34. B. I. Erkmen and J. H. Shapiro, “Unified Theory of Ghost Imaging with Gaussian-State Light,” *Phys. Rev. A* 77, 043809 (2008).

35. B. I. Erkmen and J. H. Shapiro, “Signal-to-Noise Ratio of Gaussian-State Ghost Imaging,” *Phys. Rev. A* 79 023833 (2009).

36. J. H. Shapiro, “Computational Ghost Imaging,” *Phys. Rev. A* 78, 061802(R) (2008).

37. Y Bromberg, O. Katz, and Y. Silberberg, “Ghost Imaging with a Single Detector,” *Phys. Rev. A* 79, 053840 (2009).

38. H. E. Brandt, “Quantum-Cryptographic Entangling Probe,” *Phys. Rev. A* 71, 042312 (2005).

39. J. H. Shapiro and F. N. C. Wong, “Attacking Quantum Key Distribution with Single-Photon Two-Qubit Quantum Logic,” *Phys. Rev. A* 73, 012315 (2006).

40. T. Kim, I. Stork genannt Wersborg, F. N. C. Wong, and J. H. Shapiro, “Complete Physical Simulation of the Entangling-Probe Attack on the Bennett-Brassard 1984 Protocol,” *Phys. Rev. A* 75, 042327 (2007).

41. I. M. Herbauts, S. Bettelli, H. Hübel, and M. Peev, “On the Optimality of Individual Entangling-Probe Attacks against BB84 Quantum Key Distribution,” *Eur. Phys. J. D* 46, 395-406 (2008).

42. C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, “Optimal Eavesdropping in Quantum Cryptography. I. Information Bound and Optimal Strategy,” *Phys. Rev. A* 56, 1163 (1997).

43. M. Fiorentino and F. N. C. Wong, “Deterministic Controlled-NOT Gate for Single-Photon Two-Qubit Quantum Logic,” *Phys. Rev. Lett.* 93, 070502 (2004).

44. M. Fiorentino, T. Kim, and F. N. C. Wong, “Single-Photon Two-Qubit SWAP Gate for Entanglement Manipulation,” *Phys. Rev. A* 72, 012318 (2005).

45. B. I. Erkmen and J. H. Shapiro, “Unified Theory of Ghost Imaging with Gaussian-State Light,” *Phys. Rev. A* 77, 043809 (2008).

46. B. I. Erkmen and J. H. Shapiro, “Gaussian-State Theory of Two-Photon Imaging,” *Phys. Rev. A* 78, 023835 (2008).

47. S. Lloyd, “Enhanced Sensitivity of Photodetection via Quantum Illumination,” *Science* 312, 1463-1465 (2008).

48. M. Tsang, J. H. Shapiro, and S. Lloyd, “Quantum Theory of Optical Temporal Phase and Instantaneous Frequency,” *Phys. Rev. A* 78, 053820 (2008).

49. M. Tsang, J. H. Shapiro, and S. Lloyd, “Quantum Theory of Optical Temporal Phase and Instantaneous Frequency. II. Continuous-Time Limit and State-Variable Approach to Phase-Locked Loop Design” *Phys. Rev. A* 79, 053843 (2009).

50. V. Giovannetti, S. Lloyd, L. Maccone, and J. H. Shapiro, “Sub-Rayleigh-Diffraction-Bound Quantum Imaging,” *Phys. Rev. A* 79, 013827 (2009).

51. M. Tsang, “Quantum Imaging Beyond the Diffraction Limit by Optical Centroid Measurements,” *Phys. Rev. Lett*. 102, 253601 (2009).

Publications

Journal Articles, Published

O. Kuzucu, F. N. C. Wong, S. Kurimura, and S. Tovstonog, “Time-Resolved Single-Photon Detection by Femtosecond Upconversion,” *Opt. Lett.* 33, 2257-2259 (2008).

O. Kuzucu, F. N. C. Wong, S. Kurimura, and S. Tovstonog, “Joint Temporal Density Measurements for Two-Photon State Characterization,” *Phys. Rev. Lett.* 101, 153602 (2008).

M. Tsang, “Fundamental Quantum Limit to the Multiphoton Absorption Rate for Monochromatic Light,” *Phys. Rev. Lett*. 101, 033602 (1008).

M. Tsang, J. H. Shapiro, and S. Lloyd, “Quantum Theory of Optical Temporal Phase and Instantaneous Frequency,” *Phys. Rev. A* 78, 053820 (2008).

S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, “Quantum Illumination with Gaussian States,” *Phys. Rev. Lett*. 101, 253601 (2008).

J. H. Shapiro, “Computational Ghost Imaging,” *Phys. Rev. A* 78, 061802(R) (2008).

V. Giovannetti, S. Lloyd, L. Maccone, and J. H. Shapiro, “Sub-Rayleigh-Diffraction-Bound Quantum Imaging,” *Phys. Rev. A* 79, 013827 (2009).

B. I. Erkmen and J. H. Shapiro, “Signal-to-Noise Ratio of Gaussian-State Ghost Imaging,” *Phys. Rev. A* 79 023833 (2009).

M. Tsang, J. H. Shapiro, and S. Lloyd, “Quantum Theory of Optical Temporal Phase and Instantaneous Frequency. II. Continuous-Time Limit and State-Variable Approach to Phase-Locked Loop Design” *Phys. Rev. A* 79, 053843 (2009).

S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, “Direct and Reverse Secret-Key Capacities of a Quantum Channel,” *Phys. Rev. Lett*. 102 050503 (2009).

R. García-Patrón and N. J. Cerf, “Continuous-Variable Quantum Key Distribution Protocols over Noisy Channels,” *Phys. Rev. Lett*. 102, 130501 (2009).

R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, “Reverse Coherent Information,” *Phys. Rev. Lett*. 102, 210501 (2009).

M. Tsang, “Quantum Imaging Beyond the Diffraction Limit by Optical Centroid Measurements,” *Phys. Rev. Lett*. 102, 253601 (2009).

T. Zhong, F. N. C. Wong, T. D. Roberts, and P. Battle, “High Performance Photon-Pair Source based on a Fiber-coupled Periodically Poled $KTiOPO_4$ Waveguide,” *Opt. Express* 17, 12019-12030 (2009).

A. H. Nejadmalayeri, F. N. C. Wong, T. D. Roberts, P. Battle, and F. X. Kärtner, “Guided Wave Optics in Periodically Poled KTP: Quadratic Nonlinearity and Prospects for Attosecond Jitter Characterization,” *Opt. Lett.* 34, 2522-2524 (2009).

J. Le Gouët, D. Venkatraman, F. N. C. Wong, and J. H. Shapiro, “Classical Low-Coherence Interferometry based on Broadband Parametric Fluorescence and Amplification,” *Opt. Express* 17, 17874-17887 (2009).

Journal Articles, Accepted for Publication

J. H. Shapiro, “Quantum Theory of Optical Communications,” *IEEE J. Sel. Topics Quantum Electron*. Forthcoming (2009).

Journal Articles, Submitted for Publication

X. Hu, J. E. White, T. Zhong, E. A. Dauler, F. Najafi, C. H. Herder, F. N. C. Wong, and K. K. Berggren, “Fiber-coupled Nanowire Photon-Counter at 1550 nm with 24% System Detection Efficiency,” submitted to *Opt. Lett*.

Meeting Papers, Published

F. N. C. Wong, T. Kim, J. H. Shapiro, and R. García-Patrón “Physical Simulation of Individual Attacks against BB84 using Single-Photon Two-Qubit Quantum Logic,” *17th International Laser Physics Workshop*, Trondheim, Norway, June 30 - July 4, 2008.

J. H. Shapiro and B. I. Erkmen, “Imaging with Phase-Sensitive Light: What is Quantum and What is Not,” *17th International Laser Physics Workshop*, Trondheim, Norway, June 30 - July 4, 2008.

S. Guha, J. H. Shapiro, and B. I. Erkmen, “Capacity of the Bosonic Wiretap Channel and the Entropy Photon-Number Inequality,” *Digest of the 2008 International Symposium on Information Theory*, Toronto, Canada, July 6-11, 2008.

R. García-Patrón, F. N. C. Wong, and J. H. Shapiro, “Optimal Individual Attacks against BB84,” *Digest of 3rd International Conference on Quantum Information*, Boston, MA, July 13 - 16, 2008.

S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, “Quantum Illumination: Enhanced Background-Limited Target Detection by Means of Entanglement,” *Digest of 3rd International Conference on Quantum Information*, Boston, MA, July 13 - 16, 2008.

O. Kuzucu and F. N. C. Wong, “Two-Photon Joint Temporal Density Measurement via Time-resolved Upconversion,” *Proceedings of the Ninth International Conference on Quantum Communication, Measurement and Computing*, Calgary, Canada, August 19 - 24, 2008.

Z. Dutton and J. H. Shapiro, "LADAR Resolution Improvement using Squeezed-Vacuum Injection," *Proceedings of the Ninth International Conference on Quantum Communication, Measurement and Computing*, Calgary, Canada, August 19 - 24, 2008.

J. H. Shapiro and B. I. Erkmen, "Ghost Imaging: From Quantum to Classical to Computational," *Proceedings of the Ninth International Conference on Quantum Communication, Measurement and Computing*, Calgary, Canada, August 19 - 24, 2008.

A. Lapidoth, J. H. Shapiro, V. Venkatesan, and L. Wang, "The Poisson Channel at Low Input Powers," *Proceedings 25th IEEE Convention of Electrical & Electronics Engineers in Israel*, Eilat Israel, December 3-5, 2008

O. Kuzucu, F. N. C. Wong, S. Kurimura, and S. Tovstonog, "Two-Photon Joint Temporal Density Measurements via Ultrafast Single-Photon Upconversion," *Digest of International Quantum Electronics Conference*, Baltimore, MD, May 31 - June 5, 2009.

A. H. Nejadmalayeri, F. N. C. Wong, T. D. Roberts, and F. X. Kärtner, "Efficient Second Harmonic Generation in the Optical Telecom S-Band Non-Segmented PPKTP Waveguides," *Digest of Conference on Lasers and Electro-Optics*, Baltimore, MD, May 31 - June 5, 2009.

M. Tsang, J. H. Shapiro, and S. Lloyd, "Quantum Optical Temporal Phase Estimation by Homodyne Phase-Locked Loops," *Digest of International Quantum Electronics Conference*, Baltimore, MD, May 31 - June 5, 2009.

P. Zerom, G. Piredda, R. W. Boyd, and J. H. Shapiro, "Optical Coherence Tomography Based on Intensity Correlations of Quasi-Thermal Light," *Digest of International Quantum Electronics Conference*, Baltimore, MD, May 31 - June 5, 2009.

B. I. Erkmen and J. H. Shapiro, "Signal-to-Noise Ratio of Gaussian-State Ghost Imaging," *Digest of International Quantum Electronics Conference*, Baltimore, MD, May 31 - June 5, 2009.

J. Le Gouët, D. Venkatraman, F. N. C. Wong, and J. H. Shapiro, "Phase-Conjugate Optical Coherence Tomography," Postdeadline paper, *International Quantum Electronics Conference*, Baltimore, MD, May 31 - June 5, 2009.

T. Zhong, X. Hu, F. N. C. Wong, C. Herder, F. Najafi, K. Berggren, T. D. Roberts, and P. Battle, "Towards High Quality Photonic Polarization Entanglement Distribution at 1.3-μm Telecom Wavelength," Postdeadline paper, *International Quantum Electronics Conference*, Baltimore, MD, May 31 - June 5, 2009.

Theses

T. Kim, "Applications of Single-Photon Two-Qubit Quantum Logic to Quantum Information Science," Ph.D. thesis, Department of Physics, MIT 2008; also Res. Lab. Electron. Technical Rep. 724.

O. O. Kuzucu, "Ultrafast Source of Entangled Photons for Quantum Information Processing," Ph.D. thesis, Department of Electrical Engineering and Computer Science, MIT 2008; also Res. Lab. Electron. Technical Rep. 725.