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. Mankei Tsang

Graduate Students
Aman Chawla, Saikat Guha, Taehyun Kim, Onur Kuzucu, Tian Zhong, Dheera Venkatraman

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.

1. Quantum Information and Communication

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
HP-MIT Alliance
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

Project Staff
Professor Jeffrey H. Shapiro, Dr. Franco N. C. Wong, Dr. Baris I. Erkmen,
Dr. Raúl García-Patrón, Dr. Julien Le Gouët, Dr. Mankei Tsang, Aman Chawla, Saikat Guha,
Taehyun Kim, Onur Kuzucu, Dheera Venkatraman, Bhaskar Mookerji

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 protocols for entanglement distillation, and quantum cryptography.

Classical Capacity of Free-Space Optical Communication The past decade has seen several advances in evaluating classical information capacities of several important quantum

communication channels [1-6]. Despite these advances, exact capacity results are not known for many important and practical communication channels. We have been working to advance the line of research aimed at evaluating capacities of bosonic communication channels, which began with the capacity derivation for the input photon-number constrained lossless bosonic channel [3,4]. The capacity of the lossy bosonic channel was found in [5], where it was shown that a modulation scheme using classical light (coherent states) suffices to achieve ultimate communication rates over this channel. Subsequent attempts to evaluate the capacity of the lossy bosonic channel with additive Gaussian noise [6] led to a crucial conjecture on the minimum output entropy of a class of bosonic channels [7]. Proving that conjecture would complete the capacity proof for the bosonic channel with additive Gaussian noise, and it would show that this channel's capacity is achievable with classical-light modulation. Our more recent work has addressed the classical information capacity regions of bosonic multi-user systems. For bosonic multiple-access communication we found [8] that modulation of information using non-classical states of light is necessary to achieve ultimate single-user rates in the multiple-access scenario, although coherent-state light achieves the sum-rate capacity. For bosonic broadcast communication, we found [9] an inner bound on the capacity region that would, in fact, be the capacity region if a new minimum output entropy conjecture were true. For Gaussian-state inputs, we proved that our two minimum output entropy conjectures were equivalent, and we have developed a considerable body of evidence that supports their validity [9,10], but we have yet to obtain a proof for either of them.

During the past year we have turned our attention to the bosonic wiretap channel [11], a study that has led us to formulate the Entropy Photon-Number Inequality (EPnI), as the quantum analog of the Entropy Power Inequality (EPI) of classical information theory. The term "wiretap channel" was coined by Wyner [12] to describe a communication system in which Alice wishes to communicate classical information to Bob over a point-to-point discrete memoryless channel that is subjected to a wiretap by an eavesdropper Eve. Alice's goal is to reliably and securely communicate classical data to Bob, in such a way that Eve gets no information about the message. Wyner used the conditional entropy rate of the signal received by Eve, given Alice's transmitted message, to measure the secrecy level guaranteed by the system. He gave a single-letter characterization of the rate-equivocation region under a limiting assumption, that the signal received by Eve is a degraded version of the one received by Bob. Csiszár and Körner later generalized Wyner's results to the case in which the signal received by Eve is not a degraded versions of the one received by Bob [13]. These classical results were later extended by Devetak [14] to encompass classical transmission over a quantum wiretap channel. We have applied Devetak's results to the noiseless bosonic wiretap channel, by use of a limiting argument that enables those finite-dimensional results to be extended to the infinite-dimensional bosonic channel.

The single-mode form of the noiseless bosonic wiretap channel is governed by the Heisenberg evolutions

$$b = \eta^{1/2} a + (1-\eta)^{1/2} f \qquad \text{and} \qquad e = (1-\eta)^{1/2} a - \eta^{1/2} f, \qquad \text{for } 0 \le \eta \le 1,$$

where a, b, and e are Alice's, Bob's, and Eve's photon annihilation operators, respectively, and f is the photon annihilation operator of a vacuum-state environment mode. Under the same minimum output entropy conjecture that suffices to establish the coherent-state capacity region of the bosonic broadcast channel as the ultimate capacity region of that channel, we have shown [11] that Alice's privacy capacity is given by

$$C_p = g(\eta N) - g((1-\eta)N), \text{ in nats/use}$$

where N is the average photon-number constraint on Alice's transmission and

$$g(x) \equiv (x+1)\ln(x+1) - x\ln(x)$$

is the Shannon entropy of the Bose-Einstein probability distribution with mean N. This C_p value is achievable with coherent-state light, and so, regardless of the truth of the aforementioned minimum output entropy conjecture, it is a lower bound on Alice's privacy capacity.

The expanding importance of the two minimum output entropy conjectures that we have identified has intensified our interest in proving them. Toward that end, we have pursued a quantum mechanical analog of the EPI. The Entropy Power Inequality from classical information theory is widely used in coding theorem converse proofs for Gaussian channels. As a prelude to posing that quantum mechanical analog, let us review the classical inequality from which its inspiration springs.

Suppose that $\mathbf{X}$ and $\mathbf{Y}$ are statistically independent n-dimensional real-valued random vectors that possess differential Shannon entropies $h(\mathbf{X})$ and $h(\mathbf{Y})$, respectively. Because a real-valued, zero-mean Gaussian radon variable U has differential entropy given by $h(U) = \ln(2\pi e\langle U^2\rangle)$, where the means-squared value, $\langle U^2\rangle$, is considered to be the *power* of U, the entropy powers of $\mathbf{X}$ and $\mathbf{Y}$ are taken to be

$$P(\mathbf{X}) \equiv [\exp(h(\mathbf{X})/n)]/2\pi e \qquad \text{and} \qquad P(\mathbf{Y}) \equiv [\exp(h(\mathbf{Y})/n)]/2\pi e.$$

In this way, an n-dimensional, real-valued, random vector $\mathbf{X}'$ comprised of independent, identically distributed (i.i.d.) real-valued, zero-mean, variance-$P(\mathbf{X})$, Gaussian random variables has differential entropy $h(\mathbf{X}') = h(\mathbf{X})$. We can similarly define an i.i.d. Gaussian random vector $\mathbf{Y}'$ with differential entropy $h(\mathbf{Y}') = h(\mathbf{Y})$. We define new random vectors $\mathbf{Z}$ and $\mathbf{Z}'$ by

$$\mathbf{Z} = \eta^{1/2}\mathbf{X} + (1\text{-}\eta)^{1/2}\mathbf{Y} \qquad \text{and} \qquad \mathbf{Z}' = \eta^{1/2}\mathbf{X}' + (1\text{-}\eta)^{1/2}\mathbf{Y}' \quad \text{for } 0 \le \eta \le 1.$$

In term of these new random vectors there are three equivalent forms of the Entropy Power Inequality [15]:

$$P(\mathbf{Z}) \ge \eta P(\mathbf{X}) + (1\text{-}\eta)P(\mathbf{Y})$$
$$h(\mathbf{Z}) \ge \mathrm{h}(\mathbf{Z}')$$
$$h(\mathbf{Z}) \ge \eta \mathrm{h}(\mathbf{X}) + (1\text{-}\eta)\mathrm{h}(\mathbf{Y}).$$

The Entropy Photon-Number Inequality (EPnI) is formulated as follows. Let $(a_1,a_2,\ldots,a_n)$ and $(b_1,b_2,\ldots,b_n)$ be n-dimensional vectors of photon annihilation operators for a collection of $2n$ electromagnetic fields modes whose joint state satisfies $\rho_{ab} = \rho_a\rho_b$. Because the von Neumann entropy, $S(\rho_T)$, of a thermal state, ρ_T, with average photon number N is $g(N)$, we define the entropy photon numbers of the density operators ρ_a and ρ_b as follows:

$$N(\rho_a) = g^{-1}(S(\rho_a)/n) \qquad \text{and} \qquad N(\rho_b) = g^{-1}(S(\rho_b)/n).$$

Thus, if $(a_1',a_2',\ldots,a_n')$ is a vector of annihilation operators whose component modes are in a state $\rho_{a'}$ that is a product of identically-distributed thermal states with average photon number $N(\rho_a)$, then we will have $S(\rho_{a'}) = S(\rho_a)$. Making the corresponding definitions for $(b_1',b_2',\ldots,b_n')$ and $\rho_{b'}$, we have that $S(\rho_{b'}) = S(\rho_b)$. Introducing the new photon annihilation operators $(c_1,c_2,\ldots,c_n)$ and $(c_1',c_2',\ldots,c_n')$ via

$$c_k = \eta^{1/2}a_k + (1\text{-}\eta)^{1/2}b_k \quad \text{and} \quad c_k = \eta^{1/2}a_k' + (1\text{-}\eta)^{1/2}b_k' \quad \text{for } 0 \le \eta \le 1, \text{ and } 1 \le k \le n,$$

we have shown the equivalence of the following two inequalities, which we have dubbed the Entropy Photon-Number Inequality,

$$N(\rho_c) \ge \eta N(\rho_a) + (1\text{-}\eta)N(\rho_b)$$
$$S(\rho_c) \ge S(\rho_{c'}).$$

Assuming the validity of the EPnI, we have obtained immediate proofs of our previous two minimum output entropy conjectures. We have also proven that the EPnI is true for single-mode Gaussian states, but we have yet to obtain its general proof. Although the EPnI is a more general result than our previously conjectured output-entropy statements, its proof might, in fact, be easier, because there is a wealth of information on proving the classical EPI on which to draw. This avenue of research is currently being pursued.

High-Flux Pulsed Polarization Entanglement Source 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) [16]. 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 employ the method of quasi-phase matching in periodically-poled potassium titanyl phosphate (PPKTP) or periodically-poled lithium niobate (PPLN) to enable efficient downconversion at user-specified wavelengths. In addition, collinear propagation of the pump, signal, and idler fields ensure easy manipulation and optimal collection of the output light. Recently we have developed a pulsed version of our bidirectionally pumped polarization Sagnac interferometer (PSI) that yields phase-stable polarization-entangled photons with high brightness and high fidelity [17]. In addition, we have obtained encouraging results from a PPKTP waveguide downconversion source that is highly efficient and we have found that 92% of the unfiltered output photons are indistinguishable.

Figure 1 shows our pulsed Sagnac source setup. The pump for the downconversion source is our previously developed pulsed ultraviolet (UV) laser at 390.35 nm operating at a repetition rate of 31 MHz [18]. The 400-mW narrowband UV pump enters the bidirectionally pumped Sagnac interferometric setup through a dual-wavelength polarizing beam splitter (PBS), which separates the pump light into its horizontal (*H*) and vertical (*V*) polarization components. The relative amplitude and phase between the pump's *H* and *V* components are set by the quarter-wave plate (QWP) and half-wave plate (HWP) to control the downconversion output state. Typically, we set the output to be in a polarization singlet state

$$|\psi\rangle = \left(|H\rangle_1|V\rangle_2 - e^{i\phi}|V\rangle_1|H\rangle_2\right)/\sqrt{2},$$

where the subscripts 1 and 2 refer to the two output ports.

We use a 10-mm long type-II phase-matched PPKTP crystal as the nonlinear medium in a compact configuration that does not require spatial, spectral, or temporal filtering. The PPKTP crystal is set up for frequency-degenerate type-II phase matching with orthogonally polarized signal and idler outputs. The dual-wavelength HWP (DW-HWP) rotates the *V*-polarized pump component to be *H*-polarized, along the crystal's *y* axis. Bidirectional pumping thus effectively creates two identical coherently-driven downconverters. We polarization-rotate the outputs of one of the beams by 90° with the DW-HWP, and combine the two downconverted beams at the dual-wavelength PBS, whose outputs are polarization entangled independent of the output frequencies and propagation directions. We have effectively engineered a decoherence-free subspace in which all output photon pairs are polarization entangled. There is complete indistinguishability (spatially, spectrally, and temporally) at the output. This makes it impossible to tell from which downconverter an output photon originates. Hence the output from the Fig. 1 setup is a coherent superposition of the two downconverted beams [19].

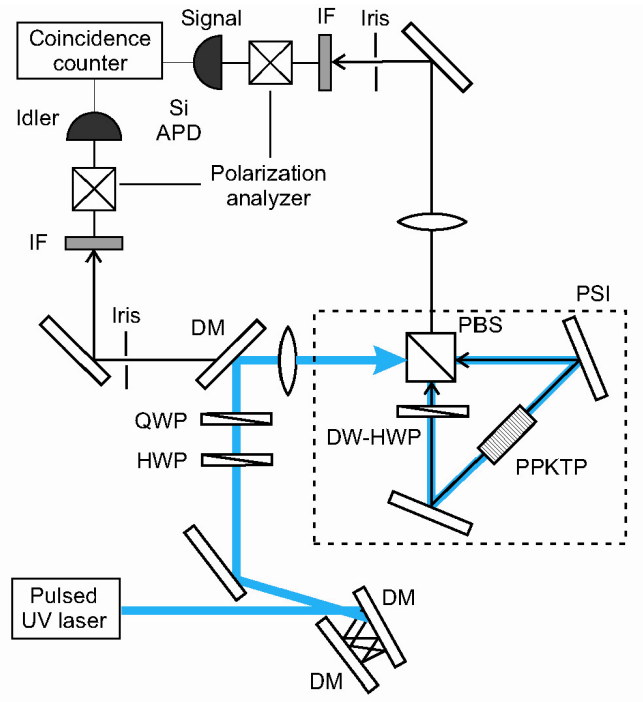

Figure 1. Schematic of pulsed SPDC in a Sagnac interferometer configuration. The dual-wavelength PBS combines the two downconverted outputs to form polarization-entangled signal and idler beams that may have different wavelengths. The relative amplitude and phase of the pump's *H*- and *V*-polarized components are set by the HWP and QWP. HWP, half-wave plate; QWP, quarter-wave plate; PBS, polarizing beam splitter; DM, dichroic mirror; IF, interference filter; PSI, polarization Sagnac interferometer.

We employ three different measurement techniques to assess the quality of the pulsed downconversion source: two-photon quantum interference measurements, Clauser, Horne, Shimony, and Holt (CHSH) form of Bell's inequality violation [20], and quantum state tomography. In two-photon quantum interference the signal polarization is analyzed in the two bases, *H*–*V* and ±45° (*A*–*D*), and the two-photon coincidences are recorded as a function of the idler polarization analysis. For polarization-entangled photons, high quantum-interference visibilities should be observed in both signal bases, as shown in Fig. 2. At low flux, multi-pair events are negligible and we obtain a visibility of 99.8% in the *H*–*V* basis, and 98.1% in the *A*–*D* basis, suggesting a high-quality source of polarization-entangled photons.

The CHSH form of Bell's inequality presents a quantitative measure of how non-classical the photons pairs are. Similar to the quantum-interference measurements, coincidence measurements at various specific polarization analyzer angles for signal and idler are taken to yield the *S* parameter [20]. For the pulsed entanglement source operating at low flux, we obtain a value of 2.739 ± 0.119 for the *S* parameter [17], which is a strong violation of the classical limit of 2 and close to the quantum limit of $2\sqrt{2}$.

The output state can be characterized in more detail by performing quantum state tomography. Through a series of polarization-projective measurements one can reconstruct the density matrix for the two-photon output state using a maximum likelihood algorithm. The real and imaginary parts of the density matrix are plotted in Fig. 3, which yields a 98.85% fidelity for the pulsed singlet-state output. As expected, all three types of measurements are equally effective and useful in characterizing the downconversion output state operating at low flux as highly entangled. This phase-stable pulsed Sagnac source of polarization-entangled photons may prove to be useful for many quantum optical applications, such as quantum key distribution, linear optics quantum computing, and quantum imaging.

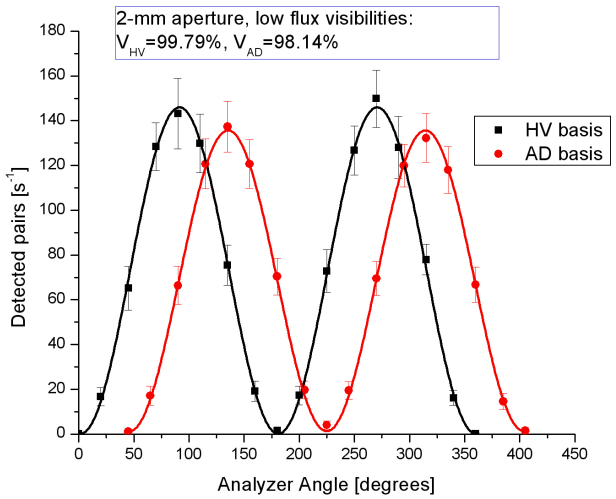

Figure 2. Two-photon quantum interference measurements in the *H*–*V* basis and in the ±45° (*A*–*D*) basis.

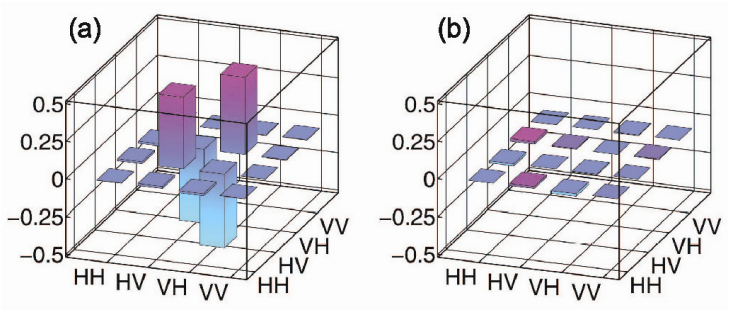

Figure 3. Quantum state tomography of PSI singlet-state output showing (a) real and (b) imaginary parts of the density matrix. Singlet-state fidelity is estimated to be 98.85%.

One of the advantages of a pulsed downconversion source is that it is relatively easy to obtain a high generation probability because the output is temporally confined to within the duration of the pump pulse. For our PSI source the generation probability is 1% per pulse for an average power of 1 mW, representing a new regime of entanglement generation in which we are capable of generating pairs at a significantly higher pair generation rate than continuous-wave (cw) operation. Indeed, the available pump power of as much as 400 mW allows us to increase the generation probability to more than one output pair per pulse, limited only by the potential damage to the PPKTP crystal. At high mean photon-pair generation rates, the Poisson distribution of the parametric downconversion process dictates that multiple-pair events are no longer negligible. These multi-pair events may create errors in quantum information processing and they degrade two-photon quantum interference visibility measurements. Figure 4 displays the two-photon quantum-interference visibility as a function of the mean photon-pair number per pulse, clearly showing the drop in visibility that is due to multi-pair events. We have calculated that the visibility can be approximated by $1 - \alpha$, where α is the mean pair-generation probability per pulse [17]. It is therefore important to keep the generation rate at or below the 1% level for applications that require a high degree of entanglement.

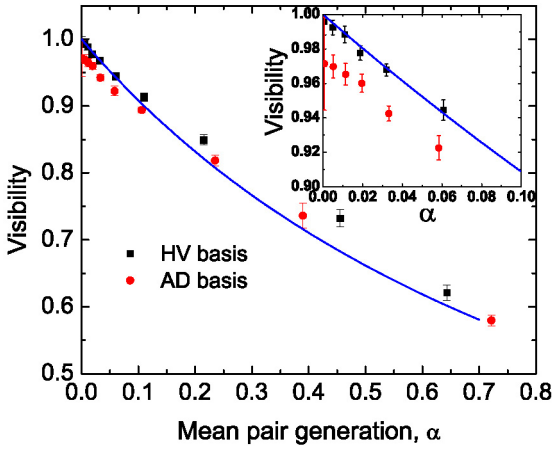

Figure 4. Quantum-interference visibility in the *H-V* (squares) and *A-D* (circles) bases as a function of mean pair-generation number α. The solid curve is computed from a theoretical model [17]. Visibilities in the *A-D* basis are lower than those in the *H-V* basis due to other factors that are unrelated to multi-pair occurrences. Inset shows the linear behavior of the visibility in the low-flux regime (α <0.1).

In addition to using a bulk PPKTP crystal as the nonlinear medium, we have been investigating a downconversion source based on a type-II phase-matched PPKTP waveguide fabricated by our collaborator AdvR, Inc. A nonlinear waveguide confines the interacting fields to a small cross sectional region and is therefore more efficient than a bulk nonlinear crystal. The fiber-pigtailed waveguide is pumped by a cw diode laser at 657 nm and generates orthogonally polarized photon pairs at 1315 nm. We have measured a pair generation efficiency of 2 x 10^7 /mW in an estimated bandwidth of 1 nm, which is about 40x higher than our PPKTP bulk-crystal generation rate. The advantages of the high efficiency and compact footprint of a fiber-pigtailed waveguide can be exploited in applications such as fiber-based quantum key distribution. Preliminary Hong-Ou-Mandel (HOM) quantum-interference measurements suggest that the signal and idler output have a spectral overlap (and hence indistinguishability) of 92% that should yield an HOM visibility of 84% if background counts are subtracted. By passing the outputs through a 1-nm bandpass filter we expect to improve the indistinguishability of the photons in order to generate a high degree of polarization entanglement. Furthermore, future collaboration with Prof. Karl Berggren on using his nanowire superconducting single-photon counters should enable un-gated background-free single-photon detection of the 1315-nm light. The waveguide source and nanowire detector technologies are highly useful in many areas of quantum information science.

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, however, useful to verify its security by attacking the BB84 system. Previously we have demonstrated a physical simulation of the entangling-probe attack on BB84 [21, 22] using single-photon two-qubit (SPTQ) quantum logic [23]. 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 [24]. Indeed, the optimal attack for BB84 with error-correcting post processing is the asymmetric Fourier-covariant cloning machine (AFCCM) attack [25], 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.

For BB84, a simpler version of the AFCCM attack can be implemented by taking advantage that the four states which are involved in BB84, namely *H*, *V*, and ±45°, all reside on an equatorial plane of the Bloch sphere. Figure 5 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 [26] and SWAP [27] gates. The amount of information Eve obtains about Alice's qubit is determined by the controlled rotation (θ) 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. In a real attack this would require that Eve has a quantum memory to temporarily store her ancilla qubit while waiting for the basis information from Alice and Bob. An open question remains: what is the optimal attack if Eve does not have a quantum memory in the case of an error-correcting post-processing BB84 protocol?

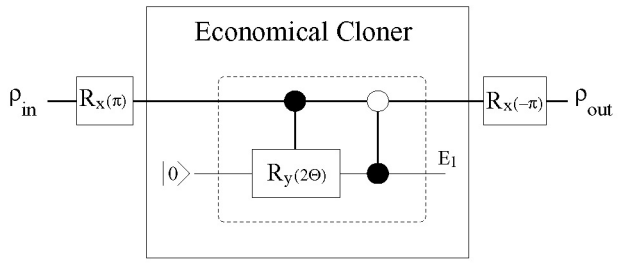

Figure 5. In the economical cloner Eve prepares her ancilla in the $|0\rangle$ state, which interacts with Alice's state through a controlled rotation about the *y*-axis of the Bloch sphere, followed by a CNOT gate. A π rotation about the *x*-axis before and after the economical cloner is required to put Alice's qubit in the proper frame of reference in Eve's Bloch sphere.

Two-Photon Joint Temporal Density Measurement via Time-Resolved Upconversion

Characterizing the spectral and temporal correlations of two-photon states is important in many photonic quantum information processing applications such as linear optics quantum computing. Consider SPDC in which the detection of the idler photon heralds the presence of the conjugate signal photon. The quantum state of the heralded photon, as a pure or mixed state, depends on the shape of the two-photon joint spectral amplitude. By manipulating the joint spectral amplitude through the pump laser spectrum or the crystal's SPDC phase-matching properties, it is possible to create heralded pure states of single photons [28]. A standard tool for measuring the joint spectral distribution relies on tunable narrowband filtering and coincidence detection of the SPDC photon pairs. However, it does not give the whole picture of the two-photon state because it is insensitive to the spectral phase and therefore cannot capture the time-domain dynamics unless the joint state is known to be transform limited. We have developed a new tool for characterizing two-photon correlations by measuring them in the time domain via synchronous single-photon upconversion [29] and coincidence measurements. We utilized this new technique to demonstrate, for the first time, temporal anti-correlation in a special two-photon coincident-frequency entangled state that we previously obtained by tailoring the SPDC phase-matching

function of a type-II phase-matched PPKTP crystal [30]. Furthermore, by varying the SPDC pump spectrum, we were able to manipulate the temporal correlations of the signal and idler, and obtain a nearly unentangled (temporally) two-photon state [31]. This new technique can be used in conjunction with frequency-domain methods to provide a more complete characterization of single and entangled photons.

Figure 6 shows a schematic of our two-photon joint temporal density (JTD) measurement setup. An ultrafast Ti:sapphire laser at 790 nm pumps a type-II phase-matched 10-mm-long PPKTP crystal to create coincident-frequency entangled photon pairs at 1580 nm that we have previous shown to display positive frequency correlation [30]. The same laser pulse train serves to pump two independent single-photon upconverters in a single 1-mm-long periodically poled MgO-doped stoichiometric lithium tantalate (PP-MgO:SLT) crystal that is configured in a noncollinear type-I phase-matched geometry, as shown in the expanded view of Fig. 6. The upconverted outputs at 527 nm are coupled into their respective single-mode optical fibers for detection using Si single-photon counters and for coincidence measurements. This unique synchronous upconversion technique affords continuous detection of infrared photons with a time resolution that is defined by the pump pulse (150 fs), which is much shorter than the single-photon arrival window (~1.3 ps). The upconversion pump functions as an efficient sampling probe to time-stamp individual photon arrivals.

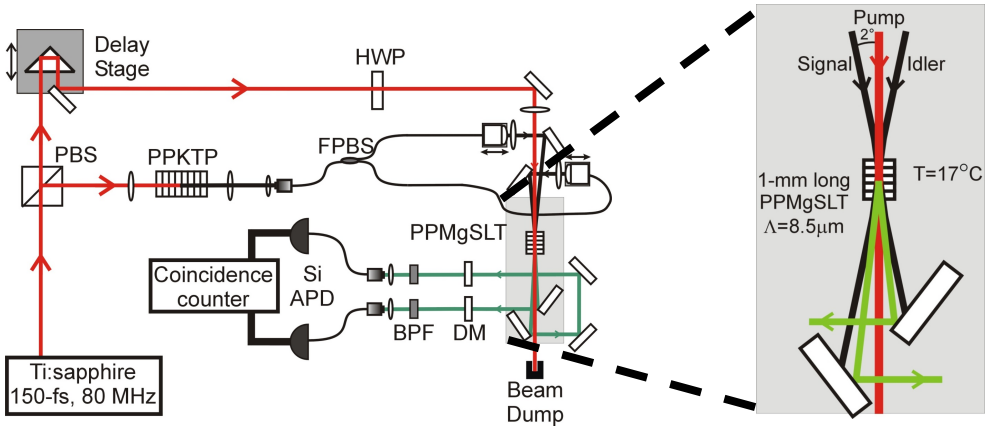

Figure 6. Synchronized upconversion and downconversion experiment driven by the same ultrafast pump. Noncollinear phase-matching geometry is used for single-photon upconversion for both signal and idler outputs. DM, dichroic mirror; FPBS, fiber polarizing beam splitter; HWP, half-wave plate; BPF, 10-nm band-pass filter.

Figure 7 shows the single-photon upconversion measurements of two different gratings of the PPKTP crystal obtained by scanning the pump pulse through the arrival windows of the signal and idler photons. Because the signal, idler, and pump have different group velocities in PPKTP, the location of the histogram therefore reflects where the signal and idler photons are generated within the crystal. For example, if the photon pair is generated at the crystal's exit facet, there is no relative time delay, and the maximum time delay occurs when the photon pair is produced at the entrance facet. In extended phase-matched SPDC the signal-pump and idler-pump time delays are equal with opposite signs [30], and their histograms should be mirror images of each other, as seen in Fig. 7. Moreover, we observe that the histogram shapes are different for the two gratings in the top and bottom panels of Fig. 7, indicating that the generation efficiency along the crystal in each grating channel is not uniform. This newly developed time-resolved measurements offers a simple diagnostic tool to study the grating quality of periodically-poled crystals that is of interest to crystal manufacturers and users of nonlinear crystals. The spatial resolution of ~1.1 mm in this measurement is set by the pulse width of the upconversion pump.

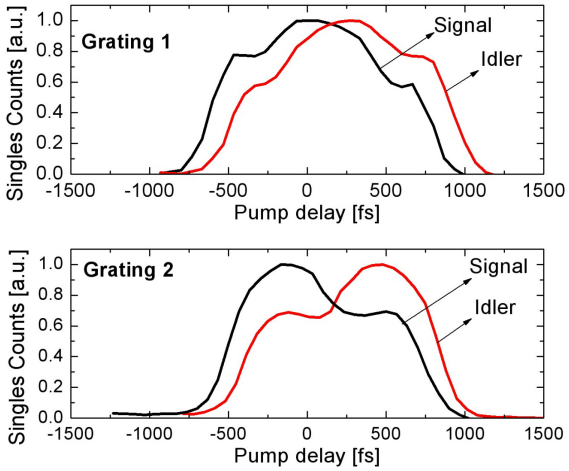

Figure 7. Normalized singles histogram for (top) 46.1 μm and (bottom) 46.0 μm grating of the PPKTP crystal.

For the coincident-frequency entangled two-photon state with a broadband positive frequency correlation and pumped with a 6-nm pump, Fig. 8 (left panel) shows the surface and contour plots of a negative joint temporal correlation (time anti-correlation) that is expected from Fourier duality of the positive frequency correlation. More interesting is how the two-photon state changes when the pump bandwidth is reduced to 1.1 nm, as shown in Fig. 8 (right panel): the JTD profile is nearly symmetric, suggesting a much reduced temporal (and hence spectral) correlation. This symmetric state corresponds to the case of nearly unentangled two-photon state that should yield heralded pure-state single photons.

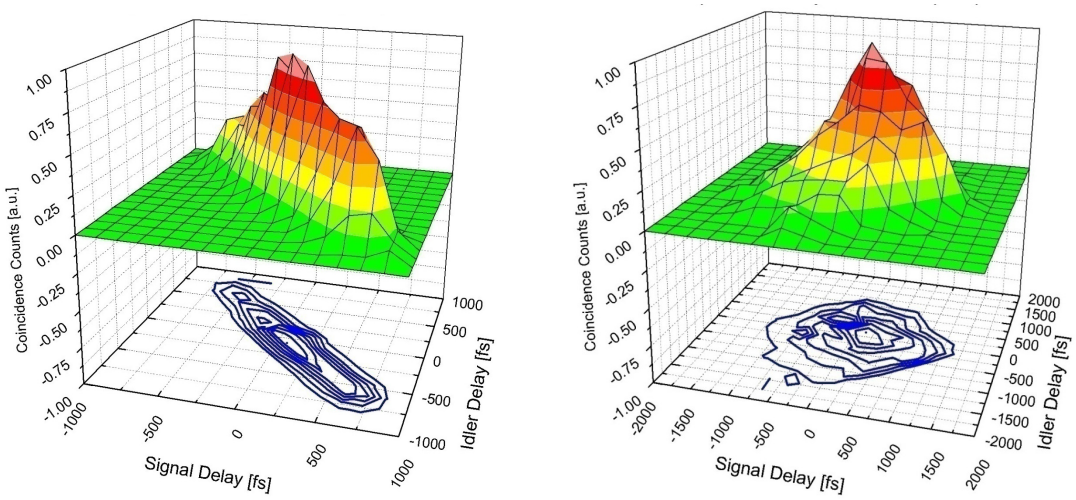

Figure 8. Experimental joint temporal densities for downconversion pump 3-dB bandwidth of (left) 6 nm, and (right) 1.1 nm.

Figure 9 shows good qualitative agreement between the theoretical entropy curves and the entropy values obtained from the joint temporal density distributions at various pump bandwidths. The entanglement entropy corresponding to the experimental JTD profiles lie between the theoretical curves for a Gaussian and a sinc-type phase-matching function. At the lowest value for a 1.1-nm SPDC pump bandwidth, it corresponds to a nearly factorizable two-photon output state, which we estimate to have a purity of 0.88 with respect to a heralded pure-state single photon. This purity value compares well with that of the pure-state single photons generated under SPDC using a different spectral engineering method [29]. We believe that the measured

purity can be further improved if we have a better control of the pump bandwidth and add additional spectral filtering. In comparison, the output for the case of a 6-nm SPDC pump bandwidth yields a purity of 0.38 due to the high degree of coincident-frequency entanglement.

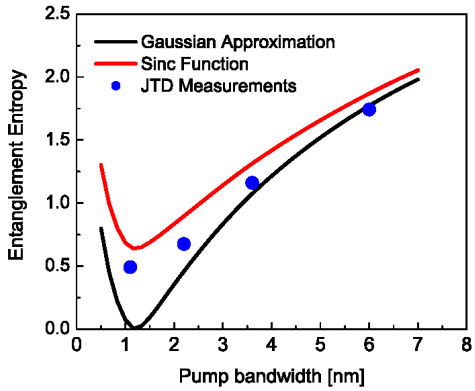

Figure 9. Entanglement entropy values calculated from experimental joint temporal density distributions for various SPDC pump bandwidths. The theoretical entropy values for Gaussian (black) and sinc-type (red) phase-matching functions are given in solid curves.

Entanglement Distillation using Single-Photon Two-Qubit Quantum Logic Entanglement is an essential ingredient for many quantum information processing applications including quantum teleportation, quantum computation, and quantum key distribution. These applications typically require that maximally-entangled qubits are shared by two remote parties, but are often hampered by dissipation and decoherence that occur through interactions with the environment. The need to overcome the loss of entanglement has led to several methods for entanglement restoration. Among various entanglement distillation schemes, the Schmidt projection technique [32] has the interesting property that it can be applied to more than two pairs of entangled qubits at the same time and that the distillation efficiency can approach unity when applied to a large number of initial qubits.

The Schmidt projection protocol is considered very hard to implement because it requires simultaneous measurements of multiple qubits. We overcome this limitation by using hyper-entangled photon pairs that are simultaneously entangled in both polarization and momentum degrees of freedom, and by applying single-photon two-qubit (SPTQ) quantum logic to the photon pairs. Polarization entanglement is created by bidirectionally pumped SPDC in a polarization Sagnac interferometer [33], and the momentum entanglement is obtained by collecting non-collinear and spatially conjugate outputs, labeled left (*L*) and right (*R*), from the same downconverter. We start with an initial product state of two identical pairs of partially-entangled qubits

$$
\begin{aligned}
|\psi\rangle_{in} &= \left(\cos\theta|V\rangle_A|V\rangle_B + \sin\theta|H\rangle_A|H\rangle_B\right)\otimes\left(\cos\theta|L\rangle_A|L\rangle_B + \sin\theta|R\rangle_A|R\rangle_B\right) \\
&= \cos^2\theta|V\rangle_A|L\rangle_A|V\rangle_B|L\rangle_B + \sin^2\theta|H\rangle_A|R\rangle_A|H\rangle_B|R\rangle_B \\
&\quad + \cos\theta\sin\theta\left(|V\rangle_A|R\rangle_A|V\rangle_B|R\rangle_B + |H\rangle_A|L\rangle_A|H\rangle_B|L\rangle_B\right),
\end{aligned}
$$

where θ sets the degree of entanglement for both the polarization and momentum qubits. The Schmidt projection protocol is to extract the maximally entangled term that is proportional to the terms ($\cos\theta\sin\theta$). Figure 10 shows a schematic of the Schmidt projection implementation using SPTQ gates. As indicated in the equation above, the state extraction of the terms *VR* and *HL*, for both Alice and Bob, is achieved with a polarizing beam splitter (PBS) and two half-wave plates (HWPs). To complete the Schmidt projection protocol a polarization controlled NOT (P-CNOT)

gate [26] then combines the two beam paths, each with a different polarization, into a common-path maximally polarization-entangled state.

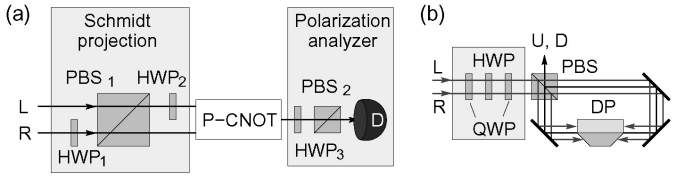

Figure 10. Entanglement distillation scheme for hyperentangled photons. (a) Schmidt projection transmits only the two relevant terms, *VR* and *HL*, of the initial state and a polarization CNOT (P-CNOT) gate combines the two paths *R, L* into a common path for final state extraction and for polarization state analysis. (b) P-CNOT gate with phase compensation. PBS: polarization beam splitter; HWP: half-wave plate; QWP: quarter-wave plate; DP: dove prism.

After Schmidt projection by both Alice and Bob, the resultant photon pairs are analyzed to determine the effectiveness of the protocol. In particular, quantum-state tomography is performed, as shown in Fig. 11 for an initial input state with $\theta = 35.9°$, clearly suggesting that the extracted state is nearly maximally polarization entangled. Figure 12 quantifies the amount of entanglement for different input states θ, demonstrating a visibility of 90% that is primarily limited by the gate fidelity of the P-CNOT gate. The successfully demonstrated Schmidt projection protocol can be applied to other quantum systems such as trapped atoms and trapped ions [34].

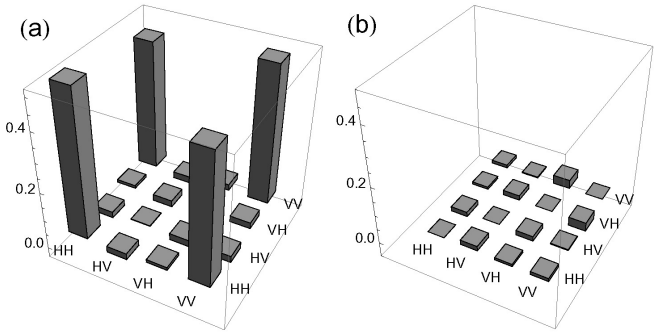

Figure 11. (a) Real, and (b) imaginary part of measured density matrix of the Schmidt projected output state for initial state with $\theta = 35.9°$.

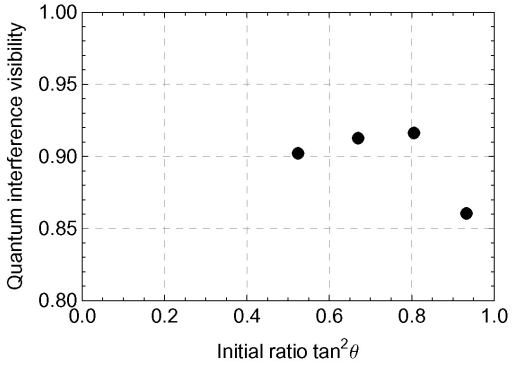

Figure 12. Measured quantum-interference visibilities in the ±45° diagonal basis.

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 [19,35,36]. 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 [37,38], ghost imaging [39], and two-photon imaging [40,41]. 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 results on optical coherence tomography, ghost imaging, and two-photon imaging.

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 [42]. 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 [37,38]. 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 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 [43]. Based on this understanding, we have 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. 13, 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 14 is a schematic of our experimental setup for demonstrating that axial resolution is improved by a factor of two in PC-OCT. A pulsed SPDC source generates a signal output at 1570 nm and a reference beam at 1550 nm. After passing through a coarse wavelength division multiplexer (CWDM) that separates the signal and reference beams, the signal light is sent to a reflective target whose relative position is to be determined. The returned signal light is collected and sent through a high-gain phase conjugate amplifier that we have realized using an optical parametric amplifier (OPA) with a MgO-doped periodically poled lithium niobate crystal. The 20 dB gain available from the OPA is more than sufficient to overcome losses associated with the transmission of the signal and the reflectivity of the target. The amplified conjugate beam at 1550 nm is then sent to the target one more time and collected for input to a fiber-optic Michelson interferometer. Interferometric measurements between the returned beam and the reference beam then yields the relative location of the target as the target is translated. In addition to demonstrating the factor of two improvement in axial resolution, we intend to investigate the dispersion canceling property of PC-OCT, which can be of interest to special situations such as a highly dispersive transmission medium in the optical or microwave regimes.

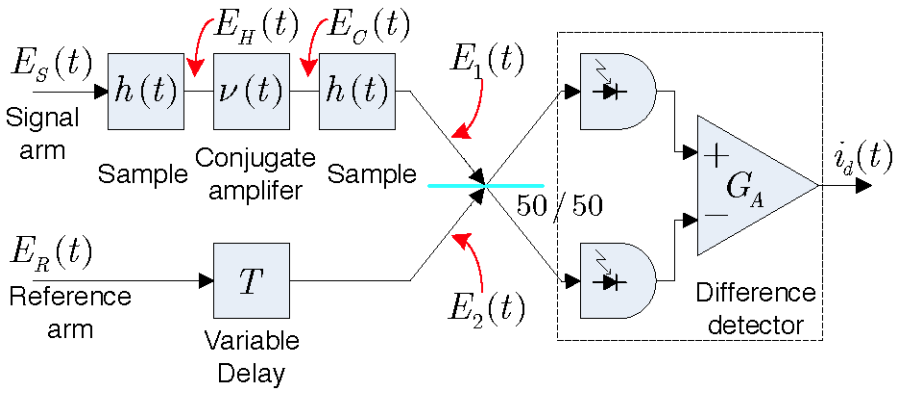

Figure 13. Schematic for phase-conjugate optical coherence tomography. The signal and reference are broadband light beams with a phase-sensitive cross correlation. The signal is transmitted to a target represented by a linear time-invariant filter $h(t)$ — shown here in transmission, but in the real 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.

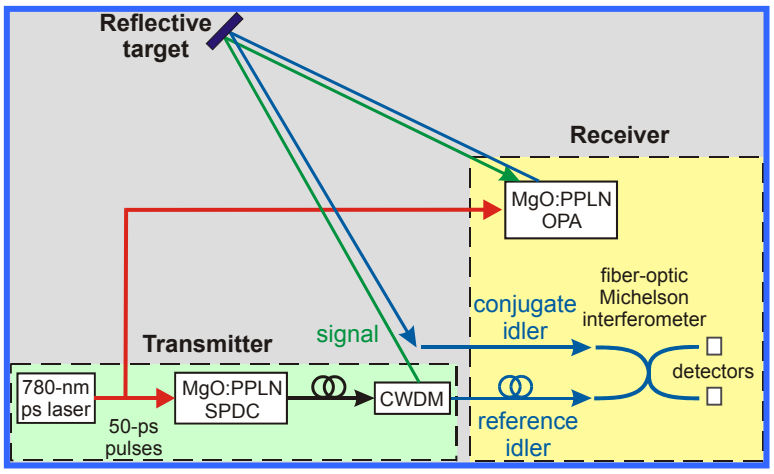

Figure 14. Schematic for phase-conjugate optical coherence tomography experimental setup.

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 [39,44-46]. Recently, we have used our coherence theory [47] 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 [48]. The particular ghost-imaging setup that we considered is shown in Fig. 15. 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. We are presently extending our work on

ghost imaging to include a comprehensive analysis of the signal-to-noise ratio behavior obtained with thermal light, classical phase-sensitive light, and quantum phase-sensitive light.

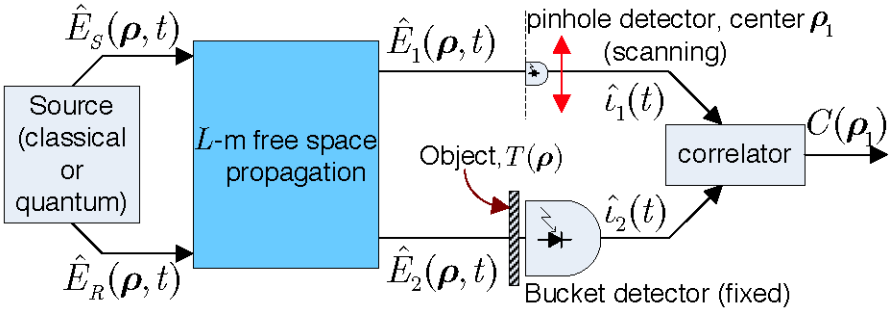

Figure 15. Schematic for ghost imaging. The signal and reference are broadband light beams with either a phase-insensitive or phase-sensitive cross correlation. After propagation over an *L*-m-long free space path, the signal beam illuminates a scanning pinhole detector and the reference illuminates 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.

Recently, we have applied our Gaussian-state framework to two additional biphoton-state quantum imaging scenarios: far-field diffraction-pattern imaging, and broadband thin-lens imaging. Previous theoretical and experimental work has shown that biphoton-state illumination of a transmission mask yields a far-field diffraction (Fourier-plane) pattern that is a factor-of-2 compressed relative to that produced by coherent plane-wave illumination of the mask [40]. In addition, it has been claimed that imaging a transmission mask using broadband, spatially incoherent biphoton-state illumination and a finite-diameter thin lens will yield a point-spread function that is a factor of 2 narrower than that obtained with quasimonochromatic spatially incoherent thermal-state illumination [41]. We used Gaussian-state analysis, together with phase-sensitive coherence propagation theory, to develop a unified — and generalized — understanding of the classical and quantum regimes in these imaging configurations [49]. In particular, we showed that, as we found for the case of Q-OCT, the benefits previously ascribed to entanglement are in fact due to phase-sensitive coherence at the source, and therefore are obtainable with classical-state sources with phase-sensitive coherence. Furthermore, we showed that the narrowing of the point-spread function in the thin-lens imaging configuration is much less than a factor of 2, even at the theoretical upper limit of SPDC bandwidth, and that it is marginal for typical SPDC bandwidths.

2. Nonlinear Optics and Precision Measurements

Sponsor
Office of Naval Research - Contract N00014-02-1-0717

Project Staff
Professor Jeffrey H. Shapiro, Dr. Franco N. C. Wong

In an era that is increasingly technology driven, precision measurements play a key role in many areas of science and commerce, such as the very successful Global Positioning System (GPS). The recent introduction of femtosecond frequency-comb technology bridges the two extremes of time scales: ultrafast optics in the femtosecond regime and optical frequency metrology at the Hertz and sub-Hertz levels. One significant consequence is the functionality and simplicity afforded by femtosecond technology for use in precision measurements, such as the determination of absolute optical frequencies. We are working in collaboration with Professors Erich Ippen and Franz Kärtner to investigate enabling femtosecond-comb technologies with nonlinear optical techniques.

The main focus of our program is to apply nonlinear optical techniques to improve both the signal-to-noise ratio and stability of self-frequency referencing techniques and to facilitate new applications of femtosecond-comb technology for enhanced functionality. The technique of quasi-phase matching and the availability of multiple gratings in a single PPLN crystal offer flexibility in achieving multiple interactions by allowing each nonlinear process to take place in its own grating section. Back-to-back difference-frequency generation in a dual-grating PPLN chip has been used to achieve optical frequency division by 3 [50]. We have also realized self-phase locking in a divide-by-3 optical parametric oscillator (OPO) using a dual-grating PPLN chip in a triply resonant cavity [51].

More recently, we have investigated the use of a type-II phase-matched PPKTP crystal under extended phase matching conditions as a balanced cross correlator and its application to femtosecond timing stabilization in a long optical fiber link [52]. Extended phase matching for PPKTP works in the telecommunication band of 1550 nm with a second-harmonic generation bandwidth that is two orders of magnitude wider than typical phase-matching bandwidths of a few nm [53]. We have demonstrated a 10 fs long-term precision for a 310-m fiber link [52]. However, the relative short length (4 mm) of the bulk crystal in the experiment does not yield a large enough signal-to-noise ratio for use in longer fiber links, and the crystal length cannot be increased without reducing the timing resolution. We have now identified a PPKTP waveguide, also under extended type-II phase matching, that can be utilized to overcome the signal-to-noise problem. In collaboration with AdvR, Inc, we have been investigating with Prof. Kärtner's group the suitability of a PPKTP waveguide for this purpose that potentially offers a significant improvement in fiber-optic distribution of timing signals for precision measurements.

References

1. C. H. Bennett and P. W. Shor, “Quantum Information Theory,” *IEEE Trans. Information Theory* 44, 2724-2742 (1998).

2. M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

3. H. P. Yuen and M. Ozawa, “Ultimate Information Carrying Limit of Quantum Systems,” *Phys. Rev. Lett*. 70, 363-366 (1993).

4. C. M. Caves and P. D. Drummond, “Quantum Limits on Bosonic Communication Rates,” *Rev. Mod. Phys.* 66, 481-537 (1994).

5. 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).

6. 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).

7. V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, “Minimum Output Entropy of Bosonic Channels: a Conjecture,” *Phys. Rev. A* 70, 032315 (2004).

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

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

10. V. Giovennetti, S. Lloyd, L. Maccone, J. H. Shapiro, and B. J. Yen, "Minimum Rényi and Wehrl Entropies at the Output of Bosonic Channels," *Phys. Rev. A* 70, 022328 (2004).

11. 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.

12. A. D. Wyner, "The Wiretap Channel," *Bell Syst. Tech. J*. 54, 1355-1387 (1975).

13. I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Inform. Theory* 23, 339-348 (1978).

14. I. Devetak, "The Private Classical Capacity and Quantum Capacity of a Quantum Channel," eprint arXiv:0304127v6 [quant-ph].

15. O. Rioul, "Information Theoretic Proofs of Entropy Power Inequalities," eprint arXiv:0741751 [cs:IT].

16. 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).

17. O. Kuzucu and F. N. C. Wong, "Pulsed Sagnac Source of Narrow-Band Polarization-Entangled Photons," *Phys. Rev. A* 77, 032314 (2008).

18. O. Kuzucu, F. N. C. Wong, D.E. Zelmon, S.M. Hegde, T.D. Roberts, and P. Battle, "Generation of 250 mW Narrowband Pulsed Ultraviolet Radiation by Frequency Quadrupling of an Amplified Erbium-doped Fiber Laser," *Opt. Lett.* 32, 1290-1292 (2007).

19. 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).

20. J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories," *Phys. Rev. Lett.* 23, 880-884 (1969).

21. H. E. Brandt, "Quantum-Cryptographic Entangling Probe," *Phys. Rev. A* 71, 042312 (2005).

22. 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).

23. 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).

24. 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).

25. 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).

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

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

28. P. J. Mosley, J. S. Lundeen, B. J. Smith, P. Wasylczyk, A. B. U'Ren, C. Silberhorn, and I. A. Walmsley, "Heralded Generation of Ultrafast Single Photons in Pure Quantum States," *Phys. Rev. Lett.* 100, 133601 (2008).

29. 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).

30. O. Kuzucu, M. Fiorentino, M. Albota, F. N. C. Wong, and F. X. Kärtner, "Two-Photon Coincident-Frequency Entanglement via Extended Phase Matching," *Phys. Rev. Lett.* 94, 083601 (2005).

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

32. C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, "Concentrating Partial Entanglement by Local Operations," *Phys. Rev. A* 53, 2046 (1996).

33. T. Kim, M. Fiorentino, and F. N. C. Wong, "Phase-Stable Source of Polarization-Entangled Photons using a Polarization Sagnac Interferometer," *Phys. Rev. A* 73, 012316 (2006).

34. T. Kim and F. N. C. Wong, "Experimental Entanglement Distillation using Schmidt Projection on Multiple Qubits," submitted to *Phys. Rev. A* (2008).

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

36. 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).

37. 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).

38. 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).

39. 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).

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

41. Y. Shih, "Quantum Imaging," *IEEE J. Sel. Top. Quantum Electron*. 13, 1016-1030 (2007).

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

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

44. 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).

45. 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).

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

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

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

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

50. P. T. Nee and N. C. Wong, "Optical Frequency Division by 3 of 532 nm in Periodically Poled Lithium Niobate with a Double Grating," *Opt. Lett.* 23, 46-48 (1998).

51. D. Kolker, A. K. Dmitriyev, P. Gorelik, F. N. C. Wong, and J.-J. Zondy, "Self-Phase Locking in 3-to-1 Triply and Doubly Resonant Optical Parametric Oscillators," *Laser Phys*. 18, 1-6 (2008).

52. J. Kim, J. Chen, Z. Zhang, F. N. C. Wong, F. X. Kärtner, F. Loehl, and H. Schlarb, "Long-term Femtosecond Timing Link Stabilization using a Single-Crystal Balanced Cross Correlator," *Opt. Lett.* 32, 1044-1046 (2007).

53. F. König and F. N. C. Wong, "Extended Phase Matching of Second-Harmonic Generation in Periodically Poled $KTiOPO_4$ with Zero Group-Velocity Mismatch," *Appl. Phys. Lett.* 84, 1644-1646 (2004).

Publications

Journal Articles, Published

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

J. H. Shapiro and F. N. C. Wong, "On-Demand Single-Photon Generation using a Modular Array of Parametric Downconverters with Electro-Optic Polarization Controls," *Opt. Lett.* 32, 2698–2700 (2007).

D. Kolker, A. K. Dmitriyev, P. Gorelik, F. N. C. Wong, and J.-J. Zondy, "Self-Phase Locking in 3-to-1 Triply and Doubly Resonant Optical Parametric Oscillators," *Laser Phys*. 18, 1–6 (2008).

O. Kuzucu and F. N. C. Wong, "Pulsed Sagnac Source of Narrow-Band Polarization-Entangled Photons," *Phys. Rev. A* 77, 032314 (2008).

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

J. H. Shapiro, "Continuous Positive-Operator-Valued Measurement of Photon Polarization," *Phys. Rev. A* 77, 052230 (2008).

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

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).

Journal Articles, Accepted for Publication

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

Journal Articles, Submitted for Publication

Mankei Tsang, Jeffrey H. Shapiro, and Seth Lloyd, "Quantum Theory of Optical Temporal Phase and Instantaneous Frequency," submitted to *Phys. Rev. A*; eprint arXiv:0804.0463 [quant-ph].

V. Giovannetti, S. Lloyd, L. Maccone, and Jeffrey H. Shapiro, "Sub-Rayeigh Quantum Imaging," submitted to *Phys. Rev. Lett*.; eprint arXiv:0804.2875 [quant-ph].

T. Kim and F. N. C. Wong, "Experimental Entanglement Distillation using Schmidt Projection on Multiple Qubits," submitted to *Phys. Rev. A*; eprint arXiv:0808:3270 [quant-ph].

Meeting Papers, Published

F. N. C. Wong and D. Venkatraman, "A High-Flux Source of Single-Mode Fiber-Coupled Nondegenerate Polarization-Entangled Photons," *Proc. SPIE* 6780, 678009 (2007).

F. N. C. Wong and J. H. Shapiro, "Single Photons on Demand using a Modular Array of Parametric Downconverters with Polarization Control," *Single-Photon Workshop*, Torino, Italy, September 25 - 28, 2007.

S. Guha, B. I. Erkmen, and J. H. Shapiro, "The Entropy Photon-Number Inequality and its Consequences," *Digest of 2008 Information Theory and Applications Workshop*, San Diego, CA, January 27 – February 1, 2008.

O. Kuzucu, F. N. C. Wong, S. Kurimura, and S. Tovstonog, "Time-Resolved Single-Photon Upconversion for Entanglement Characterization," *Digest of Quantum Electronics and Laser Science Conference*, San Jose, CA, May 4-8, 2008.

T. Kim and F. N. C. Wong, "Experimental Implementation of Entanglement Concentration using Schmidt Projection," *Digest of Quantum Electronics and Laser Science Conference*, San Jose, CA, May 4-8, 2008.

B. I. Erkmen and J. H. Shapiro, "Gaussian-State Analysis of Biphoton Imaging," *Digest of Quantum Electronics and Laser Science Conference*, San Jose, CA, May 4-8, 2008.

F. N. C. Wong, T. Kim, J. H. Shapiro, and R. Garcia-Patron "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. Garcia-Patron, 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.

Theses

B. I. Erkmen, "Phase-Sensitive Light: Coherence Theory and Applications to Optical Imaging," Ph.D. thesis, Department of Electrical Engineering and Computer Science, MIT 2008; also Res. Lab. Electron. Technical Rep. 722.

S. Guha, "Multiple-User Quantum Information Theory for Optical Communication Channels," Ph.D. thesis, Department of Electrical Engineering and Computer Science, MIT 2008; also Res. Lab. Electron. Technical Rep. 723.

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.