REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
	Technical Report	-

4. TITLE AND SUBTITLE
Progress on Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

5a. CONTRACT NUMBER
W911NF-10-1-0416

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
0D10BH

6. AUTHORS
Dirk Englund, Karl Berggren, Jeffrey Shapiro, Chee Wei Wong, Franco Wong, and Gregory Wornell

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Columbia University
615 West 131st Street, Room 254, Mail Code 8725
Studebaker Building
New York, NY 10027 -7922

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
58496-PH-DRP.13

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
The goal of this program is to increase the private information capacity of optical channels. Here we report on the theoretical and experimental progress, including the development of a large-alphabet quantum key distribution protocol that uses measurements in mutually unbiased bases.

15. SUBJECT TERMS
quantum information, integrated optics, photonic integrated chip

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dirk Englund
UU	UU	UU	UU		19b. TELEPHONE NUMBER 212-851-5958

Report Title

Progress on Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

ABSTRACT

The goal of this program is to increase the private information capacity of optical channels. Here we report on the theoretical and experimental progress, including the development of a large-alphabet quantum key distribution protocol that uses measurements in mutually unbiased bases.

Progress on Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

Dirk Englund, Karl Berggren, Jeffrey Shapiro, Chee Wei Wong, Franco Wong, and Gregory Wornell

(Dated: May 9, 2012)

The goal of this program is to increase the private information capacity of optical channels. Here we report on the theoretical and experimental progress, including the development of a large-alphabet quantum key distribution protocol that uses measurements in mutually unbiased bases.

Contents

I. PROBLEM STATEMENT

To understand the limits of optical communications, it is necessary to consider light at the level of photons, described by quantum theory. This theory has profound consequences, including the possibility of transmitting information in unconditionally secure ways. However, many questions are still unclear, including the information capacity and transfer rate of optical channels. These questions are of fundamental importance in information science, but are also of increasing technological relevance in emerging communication systems that offer new possibilities in terms of speed, security, and power consumption.

The goal of this program is to experimentally and theoretically investigate the fundamental information capacity of optical communications and to develop revolutionary technology that will enable unprecedented information content, in excess of 10 bits per photon (bpp), while guaranteeing absolute security at high communication rates of 1 Gbps or more. The following sections detail the progress towards theoretical and experimental goals.

II. INFORMATION CAPACITY OF A PHOTON AND TRANSMISSION IN FREE SPACE

A fundamental question concerns the privacy capacity of optical optical communications, as set by the laws of physics. We are interested in answering this question for the situation in which all degrees of freedom of the photon may be employed, including spatial, temporal, and polarization modes. Over the past months, the Shapiro group

obtained low-photon-number asymptotic expression for private capacity of optical communication; combined with previous upper bound, this provides photon efficiency bounds. This work showed that the multiple-mode noiseless bosonic wiretap channel is equivalent to parallel single-mode channels, implying that single- mode bounds apply. The Wornell group developed coding and modulation techniques to approach the key distribution rate over optical channels, in the regime of simultaneously high photon and bandwidth efficiencies[1]. This led to an enhanced pulse-position modulation (PPM) technique. The Wornell group is currently working with the experimental team to determine how to approach the optimal rate using PPM parsing of the detected photon stream.

III. HIGH-DIMENSIONAL QUANTUM KEY DISTRIBUTION (QKD) PROTOCOL USING DISPERSIVE OPTICS

We are developing a high-dimensional quantum key distribution (QKD) protocol suitable for integration with telecommunication infrastructure. In this approach, the key is generated by the temporal correlations of photons measured in mutually unbiased bases using dispersive optics.

High-dimensional quantum key distribution protocols make use of correlations of photons within a high-dimensional (more than 2-dimensional) Hilbert space. This enables generating multiple bits per photon and potentially faster secure key generation. Temporal correlations [2] are particularly appealing because they are robust during propagation through single-mode fiber and free space.

We consider a protocol in which Alice and Bob build a secure key by measuring the arrival times of entangled photons, as illustrated in Fig. 1a. To start, Alice shares a clock with Bob and generates a biphoton state by spontaneous parametric down conversion (SPDC). In the weak pumping regime, the down-converted state can be approximated by $|\Psi_{AB}\rangle = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty}\psi(t_A,t_B)\,|t_A,t_B\rangle\,dt_A dt_B$, where $|t_A,t_B\rangle = \hat{a}_A^\dagger(t_A)\hat{a}_B^\dagger(t_B)\,|0\rangle$ and $\hat{a}_A^\dagger(t_j)$ ($\hat{a}_B^\dagger(t_j)$) denotes the creation operator at time t_j for Alice (Bob). We approximate $\psi(t_A,t_B) \propto \exp[-(t_A-t_B)^2/4\sigma_{cor}^2]\exp[-(t_A+t_B)^2/16\sigma_{coh}^2]\exp[i\omega_p/2\cdot(t_A+t_B)]$, where σ_{coh} is the coherence time of the pump field at ω_p and the correlation time, σ_{cor}, is given by the phase matching bandwidth of the SPDC crystal. $|\Psi_{AB}\rangle$ therefore describes the superposition of photon pair states with duration of order σ_{cor} over a period of order σ_{coh}.

Alice measures one photon of the pair and sends the other to Bob. Both group the photon arrival times into bins of duration $\sigma_{bin} > \sigma_{cor}$ within a repeating time frame of duration T_α to generate the characters in their shared message. The resulting dimensionality of this system is $d = T_\alpha/\sigma_{bin}$. Possible values are $T_\alpha = 10$ ns (limited by the pair generation rate), and $\sigma_{bin} = 100$ ps (limited by detector timing jitter and the finite correlation time), resulting in $d \sim 100$.

The security of our protocol relies on Alice and Bob measuring in two mutually unbiased bases (MUB), as shown in Fig. 1b. To switch between bases, Alice and Bob can apply standard second-order dispersive elements to impart a unitary transformation $\hat{U}$ in time. $\hat{U}$ in the frequency domain is $\Delta = \int e^{-\frac{1}{2}i\beta L\omega^2}\,|\omega\rangle\langle\omega|\,d\omega$, so that $\hat{U} = \mathcal{F}^\dagger\Delta\mathcal{F}$, where $\mathcal{F}$ is the Fourier transform.

In passing through the second-order dispersive medium, a short pulse is spread as its frequency components move out of phase. For large dispersion, the biphoton correlation time, σ_{cor} is extended to $\sigma'_{cor} = \frac{1}{\sqrt{2}}\beta_{tot}L/\sigma_{cor}$, where $\beta_{tot} = \beta_{2A} + \beta_{2B}$ and β_{2A} (β_{2B}) is the dispersion introduced by Alice (Bob) [3]. As β_{tot} increases, the temporal correlation between Alice's and Bob's photons decreases. However, the original correlation time can be preserved if $\beta_{2A} = -\beta_{2B}$, which implies that $\Delta_B = \Delta_A^\dagger$ and further that $\hat{U}_B = \hat{U}_A^\dagger$. Therefore if Alice applies $\hat{U}_A$, Bob can apply $\hat{U}_A^\dagger$ to recover the original temporal correlations between their photons.

To verify that these transformations enable measurements in two MUB, we calculate the mutual information between Alice and Bob, $I(A,B)$ and plot this in Fig. 1c as a function of the normalized time parameter $\bar{t} = (D_A, D_B)L\Lambda/T_\alpha$, where, $D_{A,B} = -2\pi c\beta_{2A,2B}/\lambda^2$, λ is the photon center wavelength, L is the length over which dispersion occurs, and Λ is the biphoton bandwidth in wavelength. $\bar{t}$ quantifies the fraction of T_α over which a narrow biphoton pulse is spread. If Alice and Bob apply $\hat{U}_A$ and $\hat{U}_A^\dagger$, respectively, $I(A,B)$ does not decrease, as shown in the red curve of Fig. 1c. On the other hand, if either Alice applies $\hat{U}_A$ or Bob applies $\hat{U}_A^\dagger$, then the mutual information sharply decreases when $\bar{t}$ exceeds one. Second-order dispersion therefore enables Alice and Bob to make measurements in two mutually

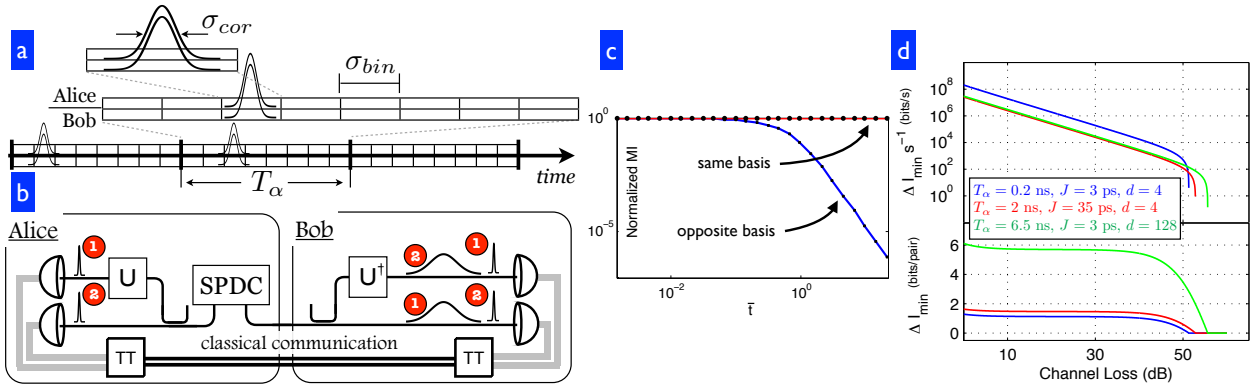

FIG. 1: (a) Alice and Bob group synchronized bins of duration σ_{bin} into alphabets of length $T_\alpha = d \cdot \sigma_{bin}$, for dimensionality d. (b) Alice and Bob can switch between measurement bases using unitary transformations. (c) Mutual information (MI) between Alice and Bob as a function of dispersion applied by Alice given that Bob also applies dispersion (red) and does not (blue), normalized to the MI given that no dispersion was applied. (d) Performance of our protocol for different values of detector timing jitter J, dimensionality d, and frame duration T_α.

unbiased, orthonormal bases.

A. Security and Communication Rates

In the protocol, Alice and Bob can thus establish some mutual information $I(A,B)$, while Eve can obtain some shared information with Alice, $I(A,E)$. We consider $\Delta I_{\min} = I_{\min}(A,B) - I_{\max}(A,E)$ to find the minimum information advantage Bob has over Eve.

We limit Eve to the intercept-resend attack and measurements in the same bases used by Alice and Bob to derive basic system requirements [recent theoretical work on high-dimensional QKD using MUB suggests that there are means to protect against more general attacks]. Alice and Bob attribute all errors to Eve's measurements and can therefore detect Eve 's intrusion by an increased error rate in their raw key as long as their time bin resolution, σ_{bin}^{fine}, is smaller than σ_{cor}.

When building the sifted key, Alice and Bob group these time bins into larger bins of duration σ_{bin} to decrease errors resulting from detector jitter and the finite correlation time. Fig. 1d plots $\Delta I_{\min}$ for a range of d, detector timing jitter J and T_α. Performance is maximized for small J and d.

Compared to protocols employing MUB in position-momentum and energy-time, our time-bin protocol requires fewer detectors — as few as one detector per party if the beam-splitters are replaced with active switches. The low number of detectors can increase resilience to intercept-resend attacks due to a lower dark count probability. We note that entangled photons are not fundamentally necessary for the protocol; for instance Alice can employ heralded single photons with random generation times in two MUB. Here, the heralding represents a convenient way to randomly generate the time coordinate of the signal photon; alternatively, a randomly-triggered deterministic single photon source could also be used.

B. Next three months

We are currently working on a full security proof of the dispersive optics QKD protocol. We are also expanding the QKD algorithm to reach end of program targets, using both spectral and temporal correlations. We will employ MUB in both degrees of freedom. We seek to reach a maximum alphabet size (Schmidt #) in time-energy basis with practical instrumentation, suitable for telecom networks, fiber and free-space.

IV. PHOTONIC INTEGRATED CHIP

The experimental component of this project focuses on the development of an integrated photonic architecture for high-speed, photon-efficient quantum key distribution. The chip will implement two kinds of QKD protocols using time-energy entangled photon pairs, which are generated using a spontaneous parametric downconversion (SPDC) source.

In the first protocol, Alice and Bob have identical chips which contain a photonic integrated circuit (PIC) for the key generation and the security check. An incident photon on Alices or Bobs setup is analyzed either (1) directly on a photon detector or (2) after a Mach Zehnder interferometers that makes up one half of a Franson interferometer, which enables a measurement of the degree of entanglement between the two photons [2]. These measurements corresponds to projections in two bases, (1) and (2). A measurement by Alice reduces the entanglement, which could be detected in the Franson fringe visibility [3]. The probabilities of performing measurements in the key generation or security check bases can be adjusted dynamically to rapidly adjust the network performance to potentially changing conditions. The second protocol implements the MUB QKD scheme described above.

In the past 3 months, the Englund group, in collaboration with Solomon Assefa at IBM, have fabricated a third generation of photonic integrated chips (PICs). These include networks for the Franson and MUB-based QKD protocols, as well as an array of test structures to study the performance of the major individual components of these circuits. In addition, for the first time, we have also implemented a metal layer that serves as contacts for integrated SNSPD detectors, as well as heating elements to fine-tune photonic chip components such as WDM filters, directional couplers, and interferometer phases. We are now completing the polymer couplers for inverse tapered waveguide couplers and will test the chip beginning May 21. Columbia has also completed 4 self-differencing InGaAs photodetectors and a PPKTP waveguide source, provided by the Chee Wei Wong group. Under room temperature conditions, we have measured 10% total detection efficiency within the gating period of the detectors; we are now testing the detectors at -40 C, where we expect a system efficiency closer to 20%. The source now provides more than 5M photon pairs per second at $\sim$ 5mW pumping with a newly installed diode laser. We have also completed Alice's and Bob's setups; they are now individually computer controlled, including closed-loop fiber coupling systems and locked temperatures using two thermo-electric cooling systems. We also completed a computer controlled free-space Hong-Ou-Mandel setup that shows 93% classical visibility; this visibility is still rather low and we are working to improve the visibility to beyond 98%. The HOM setup will be used to characterize the PPKTP sour at Columbia. With the completion of the PICs, source, detectors, and Alice and Bob's setups, we are ready to test quantum correlations between Alice and Bob's PICs.

A. Dispersive optics choices

To perform MUB transformations for 64 temporal bins (each assumed to be 32 ps long, as given by the detector jitter), we require on the order of 2 ns optical dispersion. This may be accomplished using (1) commercial WDM components or (2) on-chip devices.

(1) The best commercial component we identified is the ClearSpectrum DCMX-Dispersion Compensation Module Extended Reach from TeraXion. This device provides dispersion compensation for 200km SMA-28 fiber, which corresponds to 4000ps/nm. Taking 16 ps to correspond to 0.25 nm at 1500 nm, two units therefore spread 16-ps pulses to approximately 2 ns, as required for 64 time bins. The loss of this dispersion compensation unit is advertised as less than 3dB, resulting in 6dB for two units. The company also offers the opposite dispersion with less than 4 dB of loss (or, at the worst less than 8 dB of loss if higher bandwidth is needed) in the ClearSpectrum CDE-Chromatic Dispersion Emulator. In normal and anomalous dispersion, losses are tolerable. More units could be combined to provide higher dispersion to enable smaller bandwidth (32 ps biphoton correlation time instead of 16 ps) and longer bins (64 ps instead of 32 ps). We have purchased and are awaiting ClearSpectrum modules for normal and anomalous dispersion of 2 ns.

(2) Our on-chip solutions for pulse compression and dispersion in photonic crystal waveguides is one of the best

in the world and has a dispersion-to-loss ratio more than 50X better than nanowire channel waveguides and ∼ 25X worse than SMF28 silica fibers. Please also see our prior work [4] on the dispersion-to-loss ratio. Preliminary short pulse simulations and rigorous (completed) design of the photonic crystals indicate the needed dispersion can be achieved in ∼ 1 mm to 2 mm. The linear Rayleigh scattering loss is approximately 1 to 2.5-dB/mm (measured by the Wong group) and hence the scattering loss from the dispersive element can be kept within 1-dB to 5-dB. Pulse spreading factors of up to 105X have been designed and currently fine-tuned for the InPho program, for both positive and negative dispersion. Loss – on the silicon foundry semiconductor chip – is kept within 3-dB or less and will delivered by Wong group for integration with the full InPho chip. A target of 4-nm to 16-nm bandwidth is designed. The chip layout is near complete and will be integrated in the IBM fab in approximately 2 weeks. The experimental demonstrations will be completed prior to the Phase I review.

In the detailed comments below, we summarize the dispersive optics solutions for preliminary QKD demonstrations, as well as the above-mentioned 64 x 32-ps solution (shown in red), which we believe will be secure as it operates near the quantum measurement limit.

1. Requirements:

Preliminary QKD Demonstration: Option 1: 1ps → 2ns requires D·(1km) > 500 ps/nm Option 2: 1ps → 6.5ns requires D·(1km) > 1600 ps/nm

Heisenberg-Uncertainty Limited Option: Option 3: 16ps → 2ns requires D·(1km) >8000 ps/nm

2. Solutions:

Option 1: TDC-100 strain controllable-chirped Fiber Bragg Grating from Alnair Labs

- Wideband option, normal and anomalous dispersion offered
- Use four gratings for ∼500 ps/nm and 4·2 dB = 8 dB loss
- Units with smaller bandwidths but comparable dispersion offer ∼1dB given, so 4dB total loss for this Option.

Option 2: TDC-100 strain controllable-chirped Fiber Bragg Grating from Alnair Labs

- Use 12 gratings for ∼1500 ps/nm and 12·2 dB = 24 dB loss
- Assuming 1dB loss per unit, 12dB total for this Option

Option 3: ClearSpectrum DCMX-Dispersion Compensation Module Extended Reach from TeraXion, intended for WDM

- Insertion loss <3dB loss. (200km SMF-28 fiber is about 4000ps/nm = 200km·20ps/km/nm.)
- Opposite dispersion available (ClearSpectrum CDE-Chromatic Dispersion Emulator from TeraXion) w/ <8dB loss. <4dB option appears to be sufficient.

Option 4: On-chip deliverables:

- Arrayed waveguide grating (shown here): ∼8dB ∼400ps/nm simulated; ∼15dB ∼700ps/nm
- Coupled-Ring Optical Waveguide (shown here): in band insertion loss 4dB, <10 GHz bandwidth, O(100ps) offered, not purely GVD.
- Low-loss dispersive photonic crystal waveguides, with loss of 3-dB or less, for ∼ 100× pulse spreading to ∼ 2-ns pulsewidths. Experimental pulse compression already demonstrated with less than 3-dB of loss; currently experimental implementation the pulse spreading.

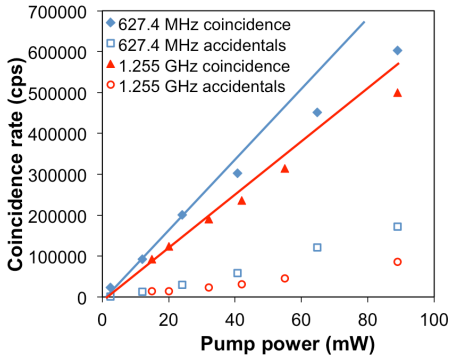

FIG. 2: Maximum pair generation rate: 8.9×10^8 pairs/s at 89 mW pump. Detector donditions: 627.4 MHz (1.255 GHz) sinusoidal gating with duty cycle of 0.25, measuring 773 kcps (586 kcps) raw coincidences.

V. ULTRAHIGH FLUX ENTANGLED PHOTON SOURCE & TIME-ENERGY ENTANGLEMENT d-DIMENSIONAL QKD

MIT has achieved a maximum pair generation rate of $8.9{\cdot}10^8$ pairs/s from a PPKTP waveguide at 89 mW pump power, as shown in Fig. 2. This section reports on progress at MIT on the fiber-optic and chip-based Franson interferometers and InGaAs detectors.

Fiber-optic Franson interferometer: MIT has overcome previous limitations in the Franson visibility to achieve record-high quantum interference visibility. We have now confirmed our suspicion that it is due to dispersion between the long and short paths of the fiber loop in each arm. We have compared three cases: (i) standard fiber loop, (ii) narrow bandpass filter for SPDC source to reduce the dispersion effect, and (iii) dispersion engineering with LEAF fiber to equalize the dispersion between the long and short paths (without the narrowband filter). We observed visibilities of 98.2%, 99.4%, and 99.6% for the uncompensated case (i), the bandpass filtered case (ii), and the compensated unfiltered case (iii), respectively, as shown in Fig. 3. All were measured without background subtraction. The results clearly indicate that dispersion was the main cause of visibility degradation in uncompensated Franson interferometric measurements, and that we are now able to recover the lost visibility with dispersion engineering of the fiber loop. Franson visibility of over 97% has never been reported, to our knowledge. The high visibility we have obtained bodes well for our privacy amplification requirement. The new postdoc Zheshen Zhang is working on security issues including privacy amplification and how it depends on Franson visibility.

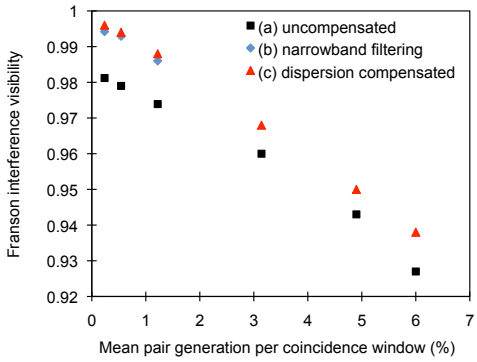

FIG. 3: PPKTP photon pair generation.

Chip-based Franson interferometer: We have received the first generation Franson chip from Columbia and Zheshen and Tian are setting up coupling optics to couple light from free space into the chip efficiently.

InGaAs detectors: We are putting together two more InGaAs detectors for single-photon counting so that multiple detectors can be used to increase the detection of raw key bits.

VI. WAVEGUIDE-INTEGRATED SNSPD

The Berggren and Englund groups are presently completing first prototypes of a waveguide (WG)-integrated superconducting nanowire single-photon detector (SNSPD) that will be scalable to eight or more independent detectors. The updates since the last quarterly report are as follows.

- **Detector fabrication on silicon nitride (SiN)**
- Revamped NbN SNSPD-on-SiN fab:
- Jitter$\sim$ 30ps FWHM at 1550nm (completed milestone for PhII)
- We have achieved a system detection efficiency above 10%.
- Detector yield of 90% on SiN chip
- Detector release yield $\sim$60-70%
- Improved SNSPD-SiN designs for flip-chip-bonding process
- **PIC upgrades for SNSPD integration:**
- Gold contacts
- Alignment precision to $<$ 200nm. Scalable approaches: stamping (in progress)

A. Next three months

We are completing a new cryostat for all-in-one integration of eight simultaneously running SNSPD detectors and the PIC. Alice and Bobs setups will be separate, but will be housed in same cryostat. We will push the system detection efficiency beyond 20%, and seek to demonstrate a coupling efficiency from the waveguide to the SNSPD in excess of 50%.

---

[1] Y. Kochman and G.W. Wornell. On high-efficiency optical communication and key distribution. In *Information Theory and Applications Workshop (ITA), 2012*, pages 172 –179, feb. 2012.

[2] J. D. Franson. Two-photon interferometry over large distances. *Phys. Rev. A*, 44:4552–4555, Oct 1991.

[3] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.*, 98(6):060503, Feb 2007.

[4] P. Colman, C. Husko, S. Combrie, I. Sagnes, C. W. Wong, and A. De Rossi. Temporal solitons and pulse compression in photonic crystal waveguides temporal solitons and pulse compression in photonic crystal waveguide. *Nature Photonics*, 4:862–868, 2010.