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 Report: 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, Seth Lloyd, 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
1210 Amsterdam Avenue, Mail Code 2205
Room 254 Engineering Terrace
New York, NY 10027 -7003

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.1

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution 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 establish a fundamental information-theoretic understand of quantum secure communication and to devise a practical, implementations of quantum key distribution protocols in an integrated photonic architecture. We report our progress on experimental and theoretical aspects.

15. SUBJECT TERMS
quantum information; quantum key distribution; secure communication; photonics; photonic networks; photonic interconnects

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 Report: Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

ABSTRACT

The goal of this program is to establish a fundamental information-theoretic understand of quantum secure communication and to devise a practical, implementations of quantum key distribution protocols in an integrated photonic architecture. We report our progress on experimental and theoretical aspects.

Progress on Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

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

(Dated: January 29, 2011)

The goal of this program is to establish a fundamental information-theoretic understand of quantum secure communication and to devise a practical, implementations of quantum key distribution protocols in an integrated photonic architecture. We report our progress on experimental and theoretical aspects.

I. OVERVIEW

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 theoritcal 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.

The team has begun an effort to start from classical privacy-capacity for the MIMOME (multiple-input, multiple-output, multiple-eavesdropper) wireless channel [1] and convert it to a corresponding privacy-capacity result for classical information transmission over a MIMOME bosonic channel. Beginning from an analysis of the effect of atmospheric turbulence on the sift and error probabilities of a BB84 QKD link operating in the far field power-transfer regime [2], we are also beginning to study how to adapt the formalism to treat the entangled photon protocol in the near and far-field limits. In particular, we are incorporating the parameters for the Columbia photonic network discussed in Section III.

III. PHOTONIC INTEGRATED CHIP

The aim of the experimental component of the present project is to develop an integrated photonic architecture for high-speed, photon-efficient quantum key distribution.

In the construction of the photonic integrated chip (PIC), we are currently developing multiple low-loss waveguide couplers, a high-speed on-chip switches, and unbalanced Franson interferometers. Two chip designs have been completed: one employs a single wavelength channel, and the other includes two wavelength channels which are multiplexed and de-multiplexed from the transmission line using chip-integrated add/drop filters. The first test chips are now being fabricated using electron beam lithography. Figure 1 shows the electron beam lithography mask for the photonic networks that will be employed by Alice and Bob.

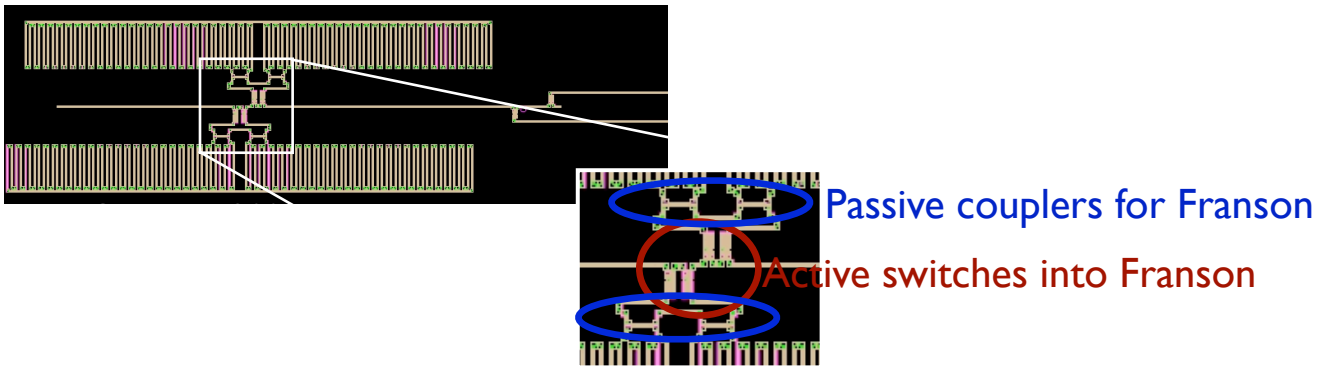

FIG. 1: The mask design shows two wavelength channels (top and bottom arms), each of which includes one half of a Franson interferometer with a 200-ps delay (meander pattern) and two active switches routing light either directly to the detector or first to the interferometer, then the detector.

The chips are designed to implement a quantum key distribution protocol based on reference [3]. Currently, the network is developed with 200-ps long delays, which are visible in the meander patterns, and which enable Alice and Bob to detect an eavesdropper's POVM with up to 400-ps time duration. The chip also includes sets of two ring-based photonic switches that direct photons to the detector for the generation of the private key, or send them to the Franson interferometer to carry out a security analysis based on the Franson interferometer visibility. The switches combine the outgoing photons onto a common channel, which is then directed to the detectors. In this way, we are able to reduce the number of detectors by factor two compared to the implementation in Reference [3].

Coupling into and out of the chip is accomplished using inverse-taper waveguide couplers. To scale these couplers to multiple wavelength channels that are anticipated for achieving the targeted bit-rate of 1 Gbit/s, we are currently implementing optical fiber arrays coupled to spatially matched inverse-taper waveguide couplers. Using photonic chips supplied by collaborators at IBM, we have tested the coupling efficiency into and out of a 1-mm silicon-on-insulator waveguide. Initial experiments indicate total transmission losses below 11 dB. This test required a new setup, which was completed in Dec. 2011 and is shown in Fig. 2. The system is connected to a new Ti:Sapph laser for the generation of entangled photon pairs by spontaneous parametric down conversion (SPDC). The laser is also used to control the switches using photogenerated carrier injection. Using new high-speed photonic test equipment capable of measuring up to 2 GHz modulation speed, we are currently evaluating the modulation rate. This is expected to be well above 100 MHz.

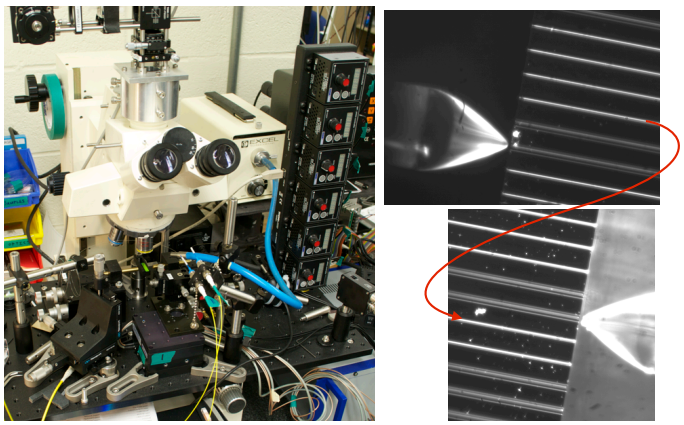

FIG. 2: Optical setup for the characterization of the photonic integrated chip. The setup contains two 3-axis piezo controlled stages for input/output coupling through inverse tapered silicon waveguides and lensed fiberes, as shown on the right. The setup also includes a converted high-resolution microscope to control multiple photonic switches by photogenerated carriers.

The chip will furthermore be integrated with the superconducting nanowire single photon detectors (SNSPDs). To this end, we are developing a new technology that we term 'micro flip-chip bonding' in which SNSPD detectors, located on a thin sapphire substrate about 20-50 micrometers on the side, are positioned onto matched photonic waveguides on the silicon chip. This technique promises to greatly simplify the integration of superconducting chips with the complex silicon photonic chip architecture. See Section V for more details.

Using passive silicon waveguide chips, we are furthermore testing interference fringes of photon pairs in a Hong-Ou-Mandel setup. However, the experiment is severely limited by low efficiency and repetition rate of the InGaAs detector; this will be improved by switching to SNSPDs at MIT.

The security in the time-bin entangled photon QKD protocol [3] is checked by measuring the visibility of interference fringes in a fourth-order coherence measurement in the Franson interferometer shared between Alice and Bob. In Figure 3, we plot the expected fringe visibility as a function of the time delay in the Franson interferometer arms and as a function of Eve's POVM timing resolution. The data is plotted for a waveguide loss of 3 dB/cm. To detect Eve's measurement, the repetition time of the protocol should be below ~ 400 ps. With a detector jitter of 50 ps, this may allow up to eight temporal basis states, though four states is more practical to reduce timing errors. To achieve a larger set of temporal bins, lower waveguide loss will be required. We estimate that most losses are due to surface roughness. We are currently addressing this problem in a two-pronged approach, optimizing the fabrication conditions of the present silicon ridge waveguides, and developing a new waveguide design in which the mode is confined far from the Si surface.

IV. ULTRAHIGH FLUX ENTANGLED PHOTON SOURCE & TIME-ENERGY ENTANGLEMENT D-DIMENSIONAL QKD

The SPDC sources will be implemented using PPKTP crystal samples with 46.2 μm grating periods, one from Raicol and one from AdvR, to determine their phase matching curves. We have conducted tests that indicate that nonlinear coefficients and bandwidths are as expected, with Raicol crystal slightly more efficient than AdvR crystal. The phase matching wavelengths for degenerate operation are shifted to the blue of 1560 nm. We have also received the PPKTP waveguide crystal and are in the process of testing its efficiency and phase matching characteristics. Initial experiments indicate that it is possible to couple pump light at 780 nm into the waveguide with coupling efficiency of 70-75%. If the waveguide crystal meets specifications, it will be AR coated before integration into the QKD setup as the SPDC source.

V. WAVEGUIDE-INTEGRATED SNSPD

We are presently designing and and fabricating a waveguide (WG)-integrated superconducting nanowire single-photon detector (SNSPD) that will be scalable to eight or more independent detectors. As mentioned above, the integration, which is jointly undertaken by MIT and Columbia, employs a new chip bonding technique that enables optimal absorption of light from a photonic waveguide in Si into the SNSPD. The bonding process requires a thin sapphire substrate under the SNSPD detector, as illustrated in Fig. 4. Toward this end, we are exploring mechanical polishing and chemical etching techniques

[1] A. Khisti, S. Diggavi, and G. W. Wornell. Secret key agreement using asymmetry in channel state knowledge. *Digest of IEEE International Symposium on Information Theory*, 2009.

[2] Jeffrey H. Shapiro. Near-field turbulence effects on quantum-key distribution. *Phys. Rev. A*, 67(2):022309, Feb 2003.

[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.

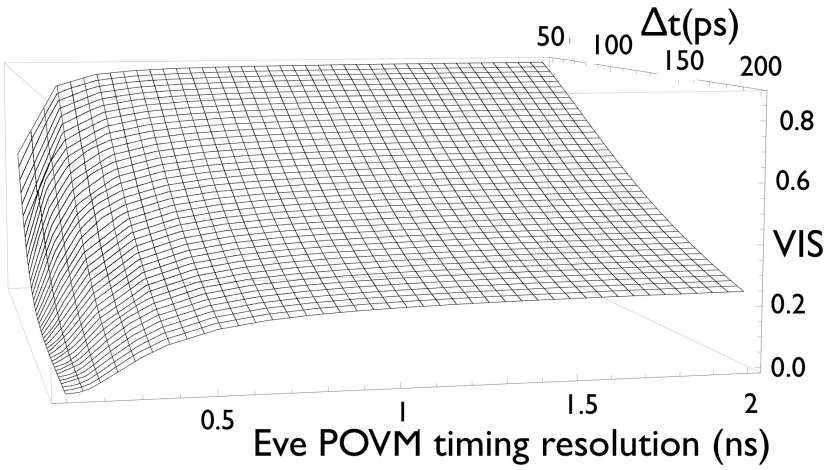

FIG. 3: Visibility as a function of Franson interferometer delay and Eve's POVM timing resolution, assuming 3dB/cm loss in the Si waveguide. Under these conditions, ~ 4 bits (16 bins of 40 ps) appears feasible. For a larger temporal dimension, a lower waveguide loss is being developed.

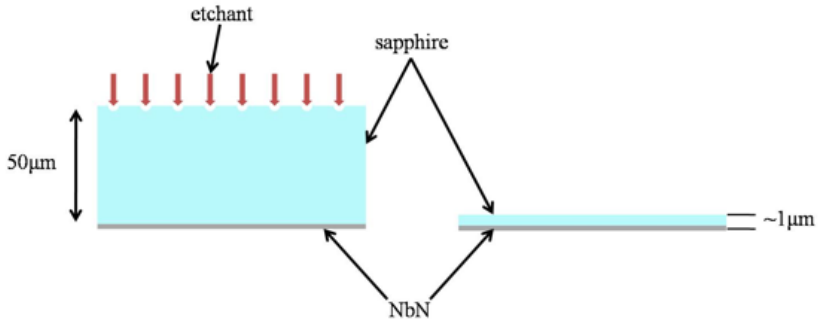

FIG. 4: Preparation of SNSPD detector for micro flip-chip bonding.