REPORT DOCUMENTATION PAGE	Form Approved OMB NO. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggesstions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any oenalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

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

4. TITLE AND SUBTITLE 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, 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.9

12. DISTRIBUTION AVAILABILITY 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

We report on the theoretical and experimental progress on photon-efficient quantum key distribution. We have derived theoretical bounds on the upper bound on the private capacity and developed a novel large-alphabet quantum key distribution protocol employing security through measurements in mutually unbiased bases. In experimental efforts, we advanced the photonic integrated chip architecture, including linear optics for security checks and chip-integrated high-performance single photon detectors.

15. SUBJECT TERMS
Information theory, quantum information, optical communications, cryptography

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

Report Title

Ultra-Dense Quantum Communication Using Integrated Photonic Architecture

ABSTRACT

We report on the theoretical and experimental progress on photon-efficient quantum key distribution. We have derived theoretical bounds on the upper bound on the private capacity and developed a novel large-alphabet quantum key distribution protocol employing security through measurements in mutually unbiased bases. In experimental efforts, we advanced the photonic integrated chip architecture, including linear optics for security checks and chip-integrated high-performance single photon detectors.

Ultra-Dense Quantum Communication Using Integrated Photonic Architecture Phase II, Quarterly Report 1

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

Feb. 3, 2012

Abstract: We report on the theoretical and experimental progress on photon-efficient quantum key distribution. We have derived theoretical bounds on the upper bound on the private capacity and developed a novel large-alphabet quantum key distribution protocol employing security through measurements in mutually unbiased bases. In experimental efforts, we advanced the photonic integrated chip architecture, including linear optics for security checks and chip-integrated high-performance single photon detectors.

I. Information Capacity of a Photon and Transmission in Free Space (Wang, Chandrasekaran, Wornell, and Shapiro)

As detailed in Ref.[1], we have proved an upper bound on the private capacity of the single-mode noiseless bosonic wiretap channel. Combined with a previous lower bound, we obtained the low photon-number asymptotic expression for the private capacity. We then showed that the multiple-mode noiseless bosonic wiretap channel is equivalent to parallel single-mode channels, so that single- mode bounds can be applied.

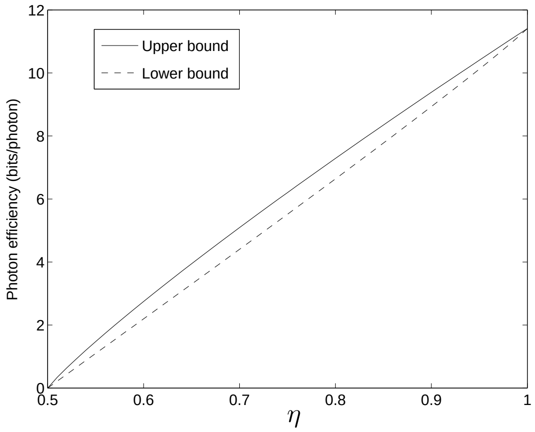

Figure 1 Comparison of the upper and lower bounds on the photon efficiency (in bits per photon) computed from (8) and (3), for mean(n) = 10^{-3}.

We are presently evaluating the ergodic capacity lower bound when focused-beam, Hermite-Gaussian, or Laguerre-Gaussian modes are employed by the transmitter. We are also beginning to analyze the architecture needed for the channel tracking (adaptive optics) that is presumed in this paper, as well as the photon budget needed for that tracking.

Secrecy capacity of the bosonic wiretap channel **(**Wornell Group**):** The Wornell group is investigating the fundamental limits of communication. The team has now developed the coding and modulation techniques that make it possible to approach the key distribution rate over optical channels, in the regime of simultaneously high photon and bandwidth efficiencies [2]. The team developed a simple and robust system design for free-space optical communication that incorporates pulse-position modulation (PPM) over multiple spatial degrees of freedom in order to achieve high photon and spectral efficiency. Further, in the context of key distribution, the team determined the optimal rate using a Poisson source of entangled photon pairs and photon detectors, and showed how to approach it using PPM parsing of the detected photon stream.

II. High-dimensional quantum key distribution protocol in photonic integrated chip

Large-alphabet quantum key distribution using dispersive optics

Our team has developed a simplified theoretical proposal for time-domain high-dimensional quantum key distribution [3]. This protocol, which we call *"Large-alphabet quantum key distribution using dispersive optics'*, stands out in several ways:

(i) Multiple bits of information are encoded in each photon.
(ii) Information is encoded in frequency and time (as opposed to degrees of freedom such as polarization or spatial modes), making its implementation ideal for fiber optics networks.
(iii) The protocol promises unprecedented communication speed exceeding 100 Mbps per frequency channel.

As in a high-dimensional analog of the BBM92 QKD protocol, security is provided by the use of two mutually unbiased bases for photon arrival time measurements. To this end, we introduce a high-dimensional unitary transformation, using simple dispersive optics exhibiting normal and anomalous group velocity dispersion (such devices are well developed in telecom). An eavesdropper Eve can only make measurements as long as she hides behind channel loss; this requirement leads us to our estimate of the minimum distillable information between Alice and Bob. Following careful theoretical models, we explore the performance of the protocol for realistic experimental conditions. The results are extremely encouraging and point to an entirely new way for high-performance quantum key distribution using modern fiber communications. We believe that this protocol could mark a major advance in the field of quantum key distribution, because (1) it enables high-dimensional QKD in standard single mode, single core telecom fibers; (2) engineered dispersion can potentially encode temporal information in up to d+1 measurement bases for a d-dimensional system while previous large-alphabet QKD protocols employing Fourier-conjugate bases are limited to two measurement bases; (3) unlike most other high-dimensional QKD protocols, the number of detectors in our protocol does not scale with the dimension because we always measure in the time domain.

Alice and Bob build up a secure key by measuring temporal correlations between entangled photons, as illustrated in Fig. 2b. These photons have some correlation time σ_{cor} and are measured over some time frame duration, T_α, where the alphabet size of order T_α/σ_{cor} can be very large. These correlations were employed for large dimensional QKD [4], but no security proof of this protocol exists to our knowledge.

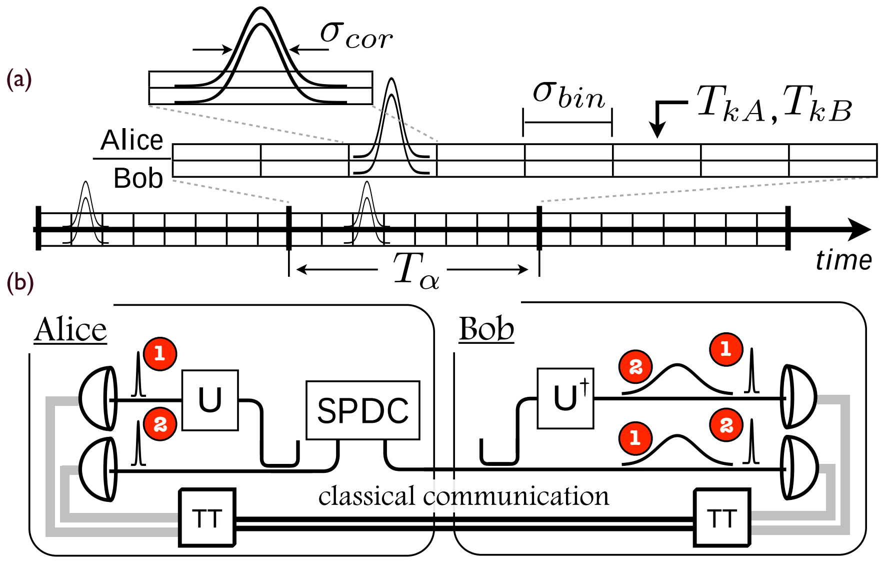

Figure 2. Alice's SPDC unit generates two entangled photons; Alice keeps one and sends the other to Bob. Before measuring the arrival time of the photon, Alice either applies (Case 1) or does not apply (Case 2) dispersion. In doing so, she projects Bob's photon onto this basis, so that Bob must apply dispersion (Case 1) or not apply dispersion (Case 2) to recover the temporal correlations of the two photons. (b) Alice and Bob measure coincidences against a periodic array of time bins T_{kA} and T_{kB}.

The protocol outlined in Figure 2 provides security through the use of two or more mutually unbiased bases that enable Alice and Bob to establish correlations, while observing measurements by Eve. Alice, who shares a clock with Bob, generates a biphoton state by spontaneous parametric down conversion (SPDC), which results in two-photon pairs in the weak-driving regime. Alice and Bob randomly measure with and without dispersion, as outlined in Fig. 2b. Measurements made in the same basis are correlated, as required to establish a secret key. Measurements in the wrong bases yield no correlations. As in other QKD schemes employing MUB, Eve introduces detectable errors because she will measure in the incorrect basis some of the time.

In Ref. [3], we show that the Alice and Bob can measure in the two mutually unbiased bases using bases transformations consisting of group velocity dispersion, as shown in Figure 3. Finally, we have also calculated the information advantage of Alice and Bob over Eve, assuming Eve intercepts the maximum number of photons allowable to remain undetected. The result is shown in Figure 4, as a function of channel loss, for a variety of experimental conditions concerning SPDC pump power and detector dark counts.

We have so far only considered this new protocol for a single wavelength channel, where we expect to be able to reach approximately 100 Mbps at 6 bits per photon. We are now expanding this theoretical protocol to exploit spectral correlations as well as temporal correlations. In particular, using 8 wavelength channels for an additional 3 bpp and two polarization states for one additional bpp, we expect to be able to reach 10 bpp at a rate approaching 200 Mbps. Currently, the ‘dispersive optics’ QKD protocol employs large temporal bins above 100 ps – much larger than the 35 ps assumed jitter time of the detectors, to reduce errors in the shared key between Alice and Bob. However, it appears that error correction codes can reduce this error, so that it becomes possible to choose tighter temporal bins. We are currently investigating this approach so that the key generation rate can be improved by another factor of 2-3. Finally, the key generation rate can be scaled up by the addition of spectral channels. We have included realistic values for implementation on photonic integrated chips, as recently explored in a related study on deterministic single photon generation using post-selection and feed-back [3].

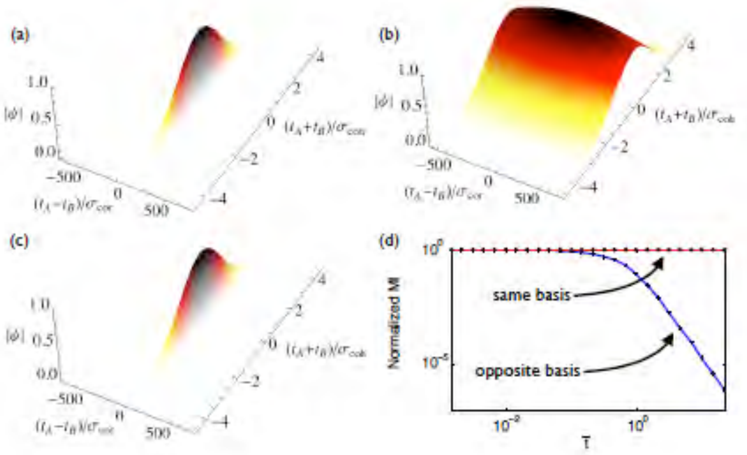

Figure 3 The bi-photon envelope function plotted when neither Alice nor Bob apply dispersion (a), either Alice or Bob applies dispersion (b), and Alice and Bob both apply dispersion (c). The extent of the spreading is quantified by the mutual information, which is plotted in (d) against t normalized to the alphabet length. The case where both Alice and Bob do or do not apply dispersion is shown in red, and the case where only one applies dispersion is shown in blue.

Photonic Integrated Chip (PIC) Development

1. PIC setups for Alice and Bob. (Englund group, Columbia)**.** We now have Alice’s and Bob’s PICs ready and undergoing testing of the Franson interferometer, which enables testing of entanglement in the temporal basis between Alice and Bob. The computer-controlled closed-loop fiber alignment system for Alice and Bob’s setups now enable less than 3% intensity fluctuations over more than 24 hours testing. We anticipate that in the next two to three months, we will have shown quantum entanglement in the Franson interferometer, to ‘certify’ the chip for the implementation of the QKD protocol employing the Franson interferometer security check. In the meantime, PIC chips will be delivered to MIT by March 2012.

Chip-scale temporal dispersive elements, cryogenic coupling and stabilization, preliminary quantum measurements, and hyperentanglement generation and detection (C.W. Wong, D. Englund and F. Wong)

1. Chip-scale temporal dispersive elements. Prompted by the new temporal architecture, we examined the pulse stretching of 2 ps to 1 ns pulse widths within highly dispersive chip-scale photonic crystal elements. The chip-scale group velocity dispersion – to – loss ratio achieved and measured by the Wong group is on the order of several times below the silica optical fibers. This enables tolerable (Rayleigh-induced) scattering losses of, for example, a few dB while affording compact millimeter-scale robust on-chip implementations. Fourier time-step simulations demonstrate the capability to stretch the pulses up to 104 ps and has been designed for both anomalous and normal dispersion. We believe the 1 ns pulse widths should be well within reach. (This work is complementary from our prior Nature Photonics 4, 862 (2010) work on 500 femtosecond temporal soliton compression.) On a sidenote, coherent swept wavelength interferometry was also developed to characterize the dispersive elements, along with determining the scattering losses in the ppKTP waveguide quantum sources. The first fabrication set is targeted for March 2012, with InPho chip received and characterization prior to July 2012.

2. Cryogenic coupling and stabilization. Over the past few months we have also achieved cryogenic fiber-chip coupling, with optical resonances have been observed just several days ago. With the cryogenic compact 5-axis piezoelectric stages, feedback locking and more quantification of the coupling will be examined. Concurrently room-temperature 6-axis feedback locking and fiber-chip coupling stabilization was achieved where the coupling fluctuations and drift was suppressed from ~ 1.15-dB over one hour to less than 0.068-dB over one hour.

3. Preliminary quantum measurements. Chip-scale single photon and Hong-Ou-Mandel detection and observation – in the near-infrared – is a primary focus and ongoing. About two weeks ago, we were able to improve the fiber-array (two-input two-output) coupling from 30-dB to 12-dB. (Four-inputs four-outputs, or more, is also feasible.) This enables the infrared chip-scale coincidence measurements to be within reach, and will be demonstrated for this program.

4. Hyperentanglement generation and detection. The chip-scale hyperentanglement module is near-completion in the design, and test fabrication is on-track for this month. The hyperentanglement detection module is prepared, followed by the generation module. The single-photon two-qubit chip is also characterized with attenuated photon sources and ready for quantum statistical characterization currently.

Milestones this quarter:

- Initiated chip-scale temporal dispersive element realization towards pulse stretching to 1-ns pulse widths, in both anomalous and normal dispersion regimes.
- Achieved coherent swept wavelength interferometry for characterization of the chip-scale dispersive element and ppKTP scattering losses.
- Improved fiber array coupling to 12-dB.
- Demonstrated cryogenic fiber-chip coupling with 5-axis piezoelectric control.
- Demonstrated fiber-chip feedback stabilization to less than 0.068-dB drift over one-hour.
- Hyperentanglement chip module design almost-ready; test fabrication underway.

- Third-generation InPho chips fabrication underway.

Experimental Quantum Key Distribution

1. Hydraharp coincidence counting electronics (F. Wong group)

The Hydraharp has an 80-ns dead time for each detection channel, which limits the maximum rate that coincidences can be measured. With the availability of more than 2 time-to-digital channels, we have decided to reduce the effect of the dead time limitation by using an electronic switch that switches between two or more channels periodically. The Hydraharp malfunctioned recently and had to be sent back to the manufacturer for repair. This has prevented us from making essential measurements such as the fiber-based Franson quantum interference.

2. Free-Space Franson interferometer (F. Wong group)

In the first Franson setup, as reported at the program Review in Oct. 2011, we obtained only 93% quantum interference visibility due mainly to loss imbalance of the short and long paths. This was confirmed by a 95% visibility for classical interference. We have made improvement to the loss balance by wrapping the long-path fiber around a small-diameter cylinder to induce adjustable bending losses. We have since measured a classical interference of 99.7% suggesting that we should be able to achieve Franson quantum interference visibility of 97% or better. The best reported Franson quantum interference visibility is 97%. We plan to perform the quantum interference measurement with our improved Franson interferometer as soon as the Hydraharp coincidence counting electronics is repaired.

Detector Development

1. PPKTP waveguides for high-brightness photon pair generation at 1550nm (Franco Wong, Englund)

We assembled the second set of a pair of self-differencing InGaAs APD single-photon counters, running at 625 MHz gating repetition rate. The detectors, like the first set, was measured to have a detection quantum efficiency of 20-25%, and dark count rates of 5-10 kHz at a duty cycle of 10%. We have also helped assemble a third set of detectors under a different program so that we can have access to these two additional detectors for use with our DWDM QKD system, in which each DWDM channel requires at least one detector. The Englund group finished performance testing of their 2 InGaAs APDs, finding a minimum timing resolution of 50 ps at -20 degrees C, and a repetition rate of 625 MHz.

2. Waveguide-integrated Superconducting Nanowire Single Photon Detectors (Berggren, Englund)

The main goal of this effort is to realize an on-chip waveguide-coupled Superconducting Nanowire Single-Photon Detector (SNSPD). The waveguides are fabricated separately on photonic integrated circuit (PIC) chips, while the SNSPDs are fabricated on membranes. These membranes are then flipped and the detector aligned to the waveguide. The advantage of this approach is that the detectors are fabricated and tested separately from the delicate PIC chip, which is then safe from damages due to further detector fabrication steps, which involve high temperatures, application of solvents, metal evaporation and lithography.

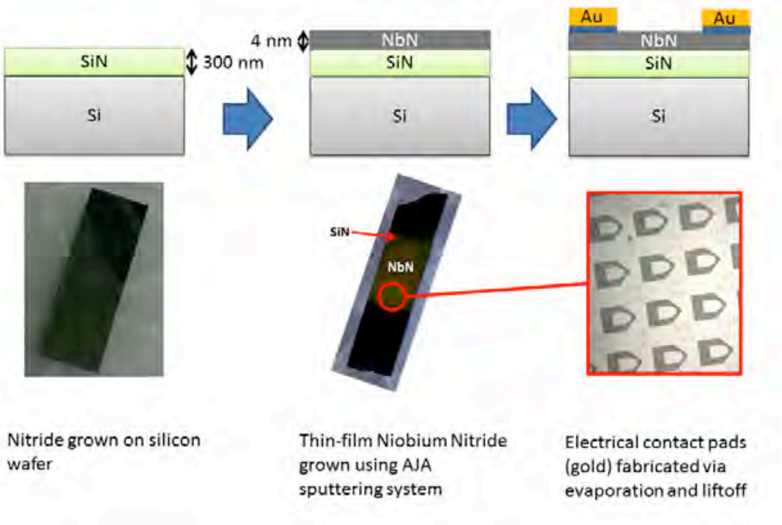
SiN
Si
4 nm
300 nm
NbN
SiN
Si
Au
Au
NbN
SiN
Si
SiN
NbN
Nitride grown on silicon wafer
Thin-film Niobium Nitride grown using AJA sputtering system
Electrical contact pads (gold) fabricated via evaporation and liftoff

Figure 4: NbN layer (detector material) and gold pads used for electrical contact.

The fabrication of membrane-SNSPDs comprises the following steps: Niobium Nitride (NbN) growth on Silicon Nitride (figure 4), SNSPD fabrication via electron beam lithography (figure 7), detector testing, membrane fabrication (figure 8) and alignment of the membrane to a waveguide (figure 11). Our progress so far on these steps is outlined below.

Niobium Nitride growth on Silicon Nitride

The past month included progress in re-vitalizing the sputtering system, increasing the stability of our resistance measurements, and gaining new data to characterize the deposition process. For the sputtering system, we have cleaned the cryo valve (which was jamming) and replaced the core of our cryo pump (which had an artificially high equilibrium temperature). On the measurement side, we have worked to re-design parts of the T_c measurement apparatus including using Indium foil for vibration free cont

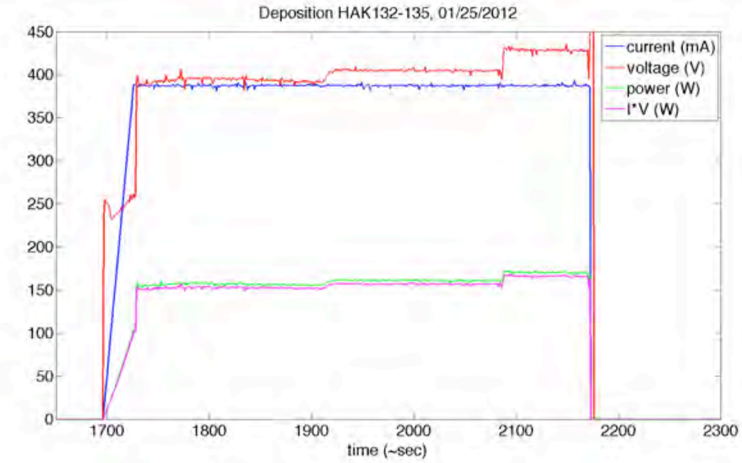

Figure 5. Current, voltage, and power readings from the power supply during a DC magnetron sputtering event. Voltage jumps correspond with Ar pre-sputtering, Ar+N2 pre-sputtering, and the opening of the shutter.

act and greater temperature and current control during the measurement. Lastly we have added the ability to read out the real-time current, voltage, and power of the sputtering system (figure 8) allowing us to do new characterization measurements of our plasma and target including the interdependence of voltage, current, and total gas pressure (figure 9).

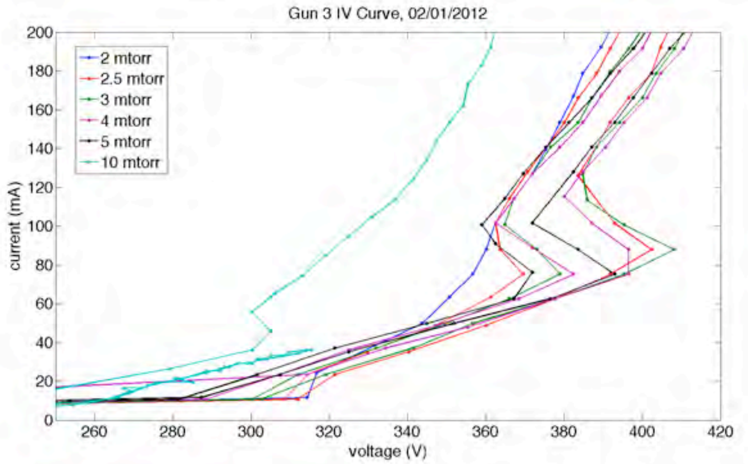

Figure 6: IV-curve for a gun as a function of pressure. The curves display an S-shape that is found in the research literature. The IV-curve is helpful to determining the operating point of the deposition.

SNSPD fabrication on Silicon Nitride

So far we have fabricated 2 working SNSPD-on-SiN chips with >200 detectors on each chip. The fabrication steps are outlined in figure 7. We have tested ~15 of these detectors for single-photon operation and timing jitter. The detectors that we had previously fabricated in our group based on NbN films that we had grown on MgO substrates had a timing jitter of ~30ps. However, the new detectors that we have fabricated on Silicon Nitride substrates have a timing jitter of ~100ps. Based on the low critical temperature of our current film (outlined in the previous report) compared to our previous films grown on MgO, we conclude that the film quality accounts for the increased jitter. In order to improve the performance of our films, we have intensified our NbN optimization efforts in the last month.

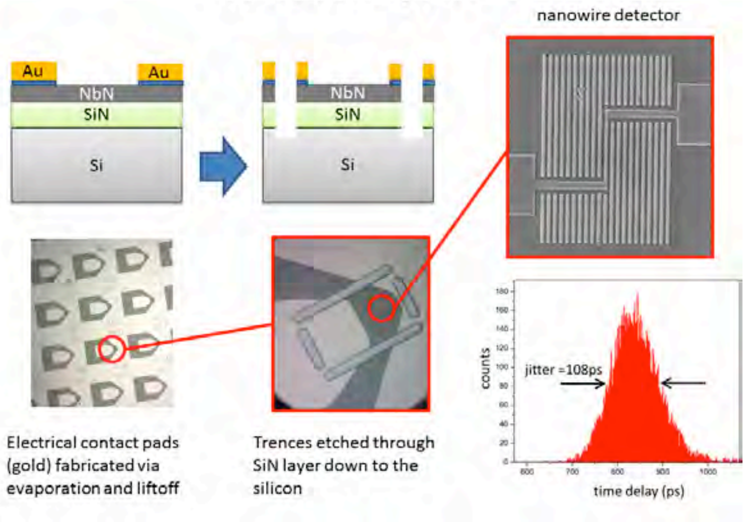
nanowire detector
Au
Au
NbN
SiN
Si
NbN
SiN
Si
Electrical contact pads (gold) fabricated via evaporation and liftoff
Trences etched through SiN layer down to the silicon
counts
jitter =108ps
180
160
140
120
100
80
60
40
20
0
600
700
800
900
1000
time delay (ps)

Figure 7: Nanowire fabrication.

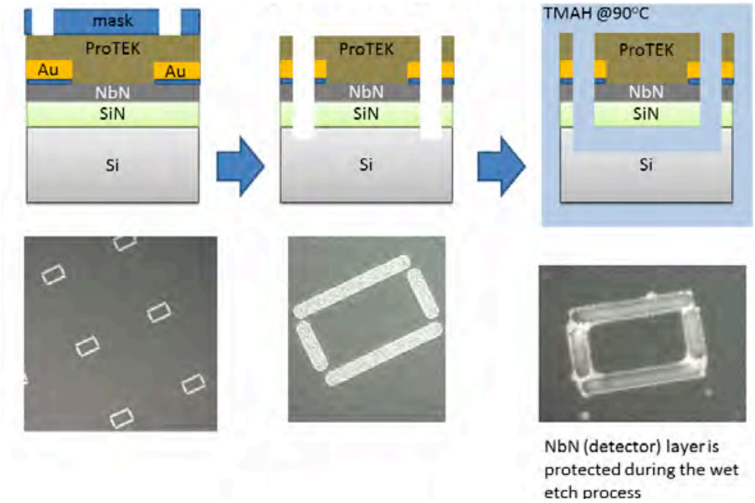
mask
ProTEK
Au
Au
NbN
SiN
Si
ProTEK
NbN
SiN
Si
TMAH @90°C
ProTEK
NbN
SiN
Si
NbN (detector) layer is protected during the wet etch process

Figure 8: Current membrane under-cut process.

Membrane fabrication

We intend to fabricate membrane-SNSPDs by employing a wet etch process (TMAH) that selectively etches the underlying Silicon without etching the Silicon Nitride layer (figure 8). However, we observed that the hot TMAH solution etches the NbN layer as well, and that the detector has to be protected during the etch. Our current approach is to apply a protective coating called ProTEK (often used to fabricate MEMS) on top of the NbN (detector) layer. The membrane under-cut process with ProTEK has so far shown <5% yield. The main issues we are currently experiencing are:

(1) Penetration of TMAH from the sides of the trenches through the NbN layer. Due to this penetration the TMAH can etch through large areas of the NbN layer, which can lead to the release of the protective layer during the solution. We are working on addressing

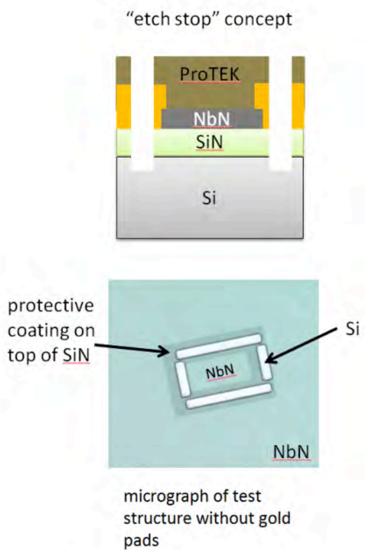
"etch stop" concept
ProTEK
NbN
SiN
Si
protective coating on top of SiN
Si
NbN
NbN
micrograph of test structure without gold pads

Figure 9: Etch stop features.

this issue by patterning NbN-free regions around the trenches (figure 9)

(2) Penetration of TMAH into the protective layer. This is mainly due to sputtering damages that result from a previous dry etch process that we use to transfer the trench pattern into the thick protective layer and the SiN substrate. The rough, non-transparent surface of the protective layer shown in figure 8 is likely due to this sputtering effect. We are going to address this issue by using a photosensitive protective layer and evaporation masks (figure 10).

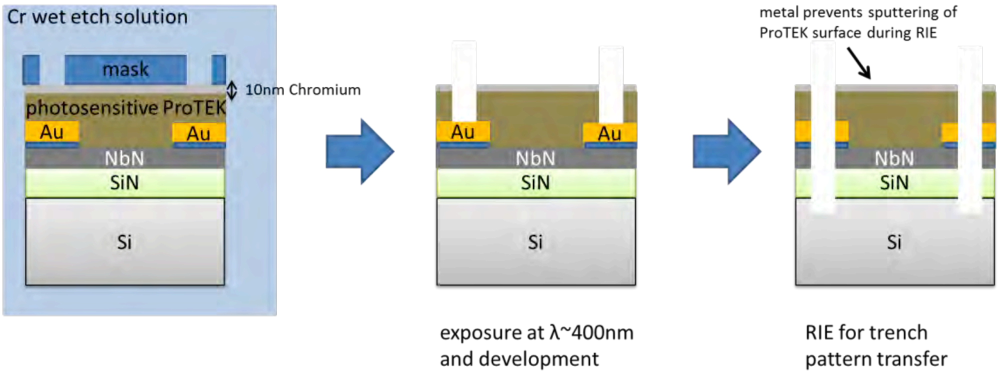

Figure 10: New ProTEK process.

Alignment of membrane-SNSPD to waveguide

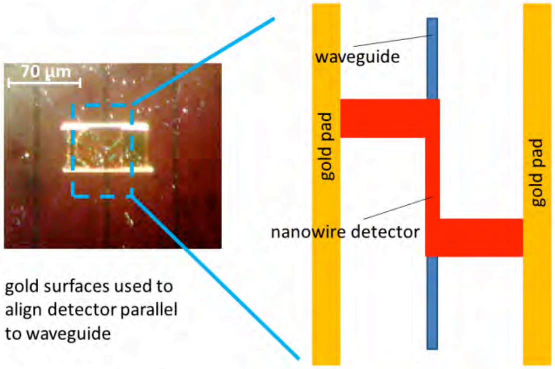

Figure 11: Current alignment scheme

New alignment approach

In order to achieve higher-precision alignment between the detector and the waveguide, we will implement a two-step approach. Rough alignment will be achieved by mechanically pressing the edge of the membrane to a parallel step structure on the waveguide chip (figure 12). After the rough alignment, matching alignment marks on both the membrane and the waveguide will be used to achieve fine alignment (figure 13).

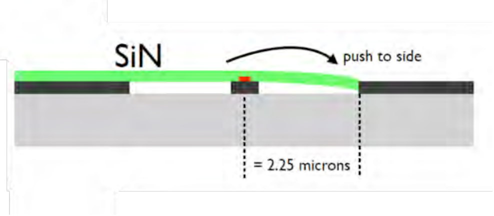

Figure 12: Mechanical alignment.

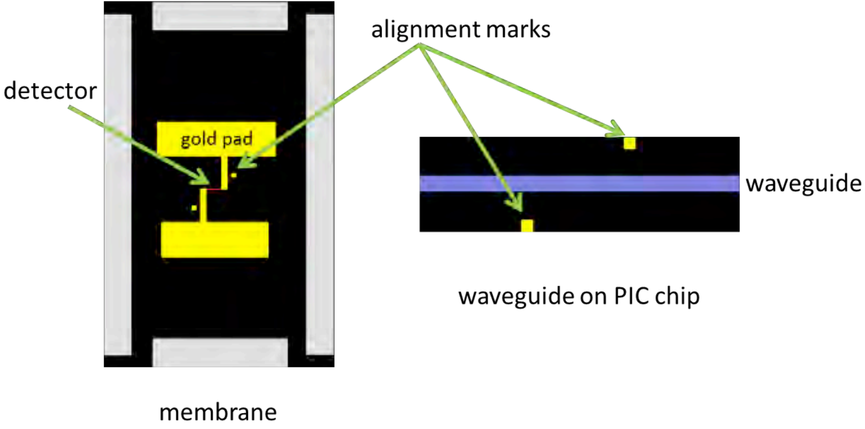

Figure 13: Fine alignment using gold marks.

Design of 8-channel testing setup

During the last quarter we also focused on the design of a set-up able to test and 8-channel Photonic Integrated Chip (PIC) with Superconducting Nanowire Single-Photon Detectors (SNSPDs). The requirements that the set-up has to meet are: (1) to have an input optical channel, (2) to have 8 bias and read-out channels for the SNSPDs (3) to reach a stable cryogenic temperature, (4) to be shielded from external radiations and (5) to reach high system efficiency. These goals can be achieved with a cryogen-free cryostat based set-up. However the design and the fabrication of this kind of set-up takes several months so this solution will be adopted for the final phase. In the meanwhile the tests can be done with a dip-probe set-up directly immersed in liquid-He, by sacrificing the high detection efficiency. We designed a dip-probe set-up, that can be built in two months, able to test an 8-channel PIC with SNSPDs at a temperature of 1.6 K. In Figure 14 we show the head of the dip-probe where the Chip is held.

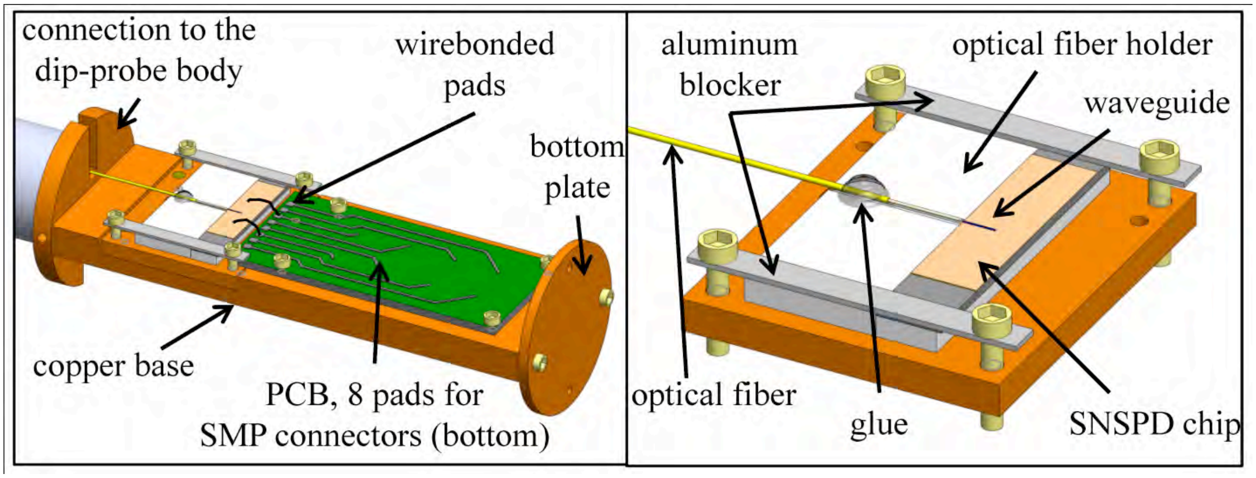

Figure 14: On the left, design of the dip-probe head. Normally the head is covered with a brass cylindrical cap but in this case the cap was removed for showing purposes. The black scribbles represent two of the eight wirebonds from the PIC to the PCB. On the right, particular of the chip holder with single-mode optical fiber aligned to the PIC waveguide.

III. Publications

1. Private-Capacity Bounds for Bosonic Wiretap Channels, Ligong Wang, Jeffrey H. Shapiro, Nivedita Chandrasekaran, and Gregory W. Wornell, submitted to IEEE International Symposium on Information Theory (2012)
2. On High-Efficiency Optical Communication and Key Distribution, Yuval Kochman and Gregory W. Wornell, under review (2012)
3. Efficient generation of single and entangled photons on a silicon photonic integrated chip, J. Mower and D. Englund, Phys. Rev. A, 84:052326, (2011).
4. I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. 98, 060503 (2007).
5. Directional free-space coupling from photonic crystal waveguides, Cheng-Chia Tsai, Jacob Mower, and Dirk Englund, Optics Express 19 (21), 20586-96 (2011)

6. Dense Wavelength Division Multiplexed Quantum Key Distribution Using Entangled Photons, J. Mower, F.N.C Wong, J. H. Shapiro, and D. Englund, arXiv:1110.4867 (2011)
7. Large-alphabet quantum key distribution using dispersive optics, Jacob Mower, Pierre Desjardins, and Dirk Englund