SeaQuaKE: Sea-optimized Quantum Key Exchange

Technical Progress Report No. 3

Prepared for: Office of Naval Research
Contract #: N00014-14-C-0003
November 2014

Prepared by:
Paul Toliver, Principal Investigator
732-898-8146
ptoliver@appcomsci.com

Applied Communication Sciences

Drawing on its Telcordia, Bellcore and Bell Labs heritage, Applied Communication Sciences excels at creating innovative technologies and services to solve the most difficult and complex information and communications problems across commercial, carrier and government sectors. Applied Communication Sciences is legally registered as TT Government Solutions, doing business as Applied Communication Sciences. ACS operates as a standalone company under the corporate umbrella of its owner, The SI Organization, Inc.

REPORT DOCUMENTATION PAGE

FORM APPROVED
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED *(From - To)*
November 2014	Quarterly Technical Progress Report	September 2014 – November 2014

4. TITLE AND SUBTITLE

SeaQuaKE: Sea-optimized Quantum Key Exchange

Technical Progress Report No. 1

5a. CONTRACT NUMBER
N00014-14-C-0003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Paul Toliver

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

TT Government Solutions (dba Applied Communication Sciences)
150 Mount Airy Road
Basking Ridge, NJ 07920-2021

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
875 North Randolph Street, Arlington VA 22203

DCMA Springfield
Bldg. 93, Picatinny Arsenal, NJ 07806-5000

10. SPONSOR/MONITOR'S ACRONYM(S)
ONR, DCMA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A. Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

ONR-funded research: Special Notice 13-SN-0004 under ONRBAA13-001

14. ABSTRACT

This is the 3rd quarterly Technical Progress Report summarizing progress on the Sea-optimized Quantum Key Exchange (SeaQuaKE) project, which is led by Applied Communications Sciences under the ONR Free Space Optical Quantum Key Distribution Special Notice (13-SN-0004 under ONRBAA13-001).

In this technical report, we describe modeling results of an entangled photon-pair source based on spontaneous four-wave mixing for proposed application in a maritime quantum communications system. In particular, we consider wavelength-dependent performance of such a source taking into account critical material parameters. Furthermore, we extend this to full system modeling that includes not only the wavelength dependencies of the source within the transmitter element but also wavelength-dependent losses based on our previous channel simulations as well as a wavelength-dependent superconducting detector model.

15. SUBJECT TERMS

Quantum communications, free-space optical communications

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	17. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Same as report (SAR)	12	Paul Toliver
Unclassified	Unclassified	Unclassified			20. TELEPHONE NUMBER (732) 898-8146

Table of Contents

1 Summary

This is the 3rd quarterly Technical Progress Report summarizing progress on the Sea-optimized Quantum Key Exchange (SeaQuaKE) project, which is led by Applied Communications Sciences under the ONR Free Space Optical Quantum Key Distribution Special Notice (13-SN-0004 under ONRBAA13-001).

In this technical report, we describe modeling results of an entangled photon-pair source based on spontaneous four-wave mixing for proposed application in a maritime quantum communications system. In particular, we consider wavelength-dependent performance of such a source taking into account critical material parameters. Furthermore, we extend this to full system modeling that includes not only the wavelength dependencies of the source within the transmitter element but also wavelength-dependent losses based on our previous channel simulations as well as a wavelength-dependent superconducting detector model.

2 Introduction

The objective of the ONR SeaQuaKE project is to optimize the performance of free-space optical (FSO) quantum key distribution (QKD) operating under challenging maritime atmospheric conditions. In particular, a modeling framework will be developed to guide optimization of the *system operating wavelength* in order to maximize throughput and/or transmission distance over a wide range of atmospheric conditions. The framework will consider the major components of the quantum communication system including the transmitter, quantum channel, and receiver elements. Applied Communication Sciences (ACS) will focus its efforts on the transmitter and receiver elements, while Stevens Institute of Technology (SIT) will focus their effort on the free-space channel.

The focus areas over the last quarter include (i) development of a wavelength-dependent, entangled photon-pair source model and (ii) end-to-end system modeling that incorporates transmitter, channel, and receiver wavelength dependencies. The modeling approach we employed and the results of the analysis are described below.

3 Methods, Assumptions and Procedures

3.1 Source Architecture and Modeling

The QKD transmitter in our system is hyper-entanglement based in order to improve system throughput. Polarization and time-bin entanglement are the two degrees of freedom that will be utilized. The heart of the entanglement generator is the high-power pump and the passive fiber medium which generates correlated photon pairs through the process of spontaneous four-wave mixing (SFWM). We have already established in a previous report that viable technologies exist for pump lasers at all the wavelength bands of interest: 0.8, 1.3, 1.55, 3.5, and 9 μm. These wavelengths correspond to low-loss transmission windows in the atmosphere. Due to the apparent flexibility of many source technologies, and an additional low-loss window near 5 micron, we also consider this as a wavelength of interest in this report.

We consider in this report available material technologies for the correlated photon pair generation. We have chosen state-of-the-art materials which are currently being focused on for nonlinear optics in the near-infrared (NIR) and mid-wavelength infrared (MWIR) bands. We assume that the pump technology for each wavelength will be able to generate sufficient peak powers to optimally utilize the chosen material. Using standard SFWM equations, we are then able to calculate the correlated signal pair rates, and the spontaneous Raman generation rate. From these signal and noise photons, we calculate a coincidence-to-accidental ratio (CAR), which is a standard quantum system metric and is analogous to signal-to-noise ratio. As the CAR increases, the QKD system can more efficiently generate good key material. These source calculations are then plugged into the system model to predict actual QKD system performance over a free-space channel.

A simplified source model is considered for our analysis, which is shown in Figure 1 below. The passive components for producing hyperentanglement have been removed so that the impact of the varying critical materials properties can be properly evaluated.

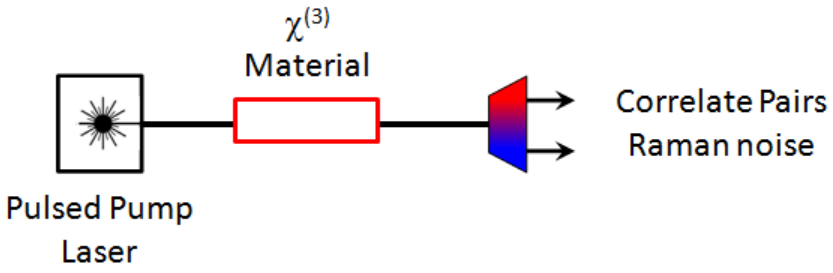

Figure 1. Source model for evaluating materials properties on correlated photon pair and Raman photon generation.

The materials chosen for SFWM in each wavelength band are summarized in Table 1 below. The relevant materials properties, e.g. the nonlinear refractive index (n_2) and Raman gain (g_R), have been taken from available literature. Where the wavelength dispersion of these parameters could not be found explicitly, established scaling rules were used to provide workable estimates. These materials can all be fabricated into optical fibers in order to maximize the nonlinear interaction lengths. We assume that through proper waveguide design, the zero-dispersion wavelength can be engineered for optimal correlated photon pair generation. For example, photonic crystal fiber

(PhC) is considered for pair generation at 0.8 μm in silica. Also, to simplify comparison, we assume the correlated photon pair filters are equally spaced from the pump (in frequency) for each wavelength band. In general, this tends to minimize the Raman noise and improve the coincidence-to-accidental ratio (CAR).

Table 1. Nonlinear SFWM Materials

Wavelength (μm)	Materials
0.8	Silica PhC
1.3	Silica
1.5	Silica
3.5	Tellurite
5	As_2S_3
9	As_2Se_3

Table 2 Acronyms: SFWM = spontaneous four wave mixing; PhC = photonic crystal fiber

3.2 Channel Model and Validation

Equipment for validating the channel model has been investigated in the past quarter. In particular, instruments for setting up a known particle distribution have been explored along with tunable source technologies for scanning transmission loss. There are no additional updates regarding channel modeling and validation in this quarter.

3.3 System Modeling

Using the source model described in Section 3.1 along with MODTRAN simulations of the atmospheric channel that were described in our previous quarterly report, the end-to-end performance of entanglement-based QKD system was projected. The previous results of the MODTRAN simulation for standard set of conditions (U.S. standard atmosphere, Navy Maritime aerosol model) assuming a 30 km free-space link distance at an altitude of 10 m are shown again for convenience in Figure 2. The channel transmittance was extracted at wavelengths corresponding to each of the possible source wavelengths (0.8, 1.3, 1.5, 3.5, 5, and 9 μm) for both the 10 km and 23 km modeled atmospheric visibility conditions. Note that since 0.8 μm was not included in the original MODTRAN simulation, the transmission was extrapolated from the general trend in loss observed close to 1 μm.

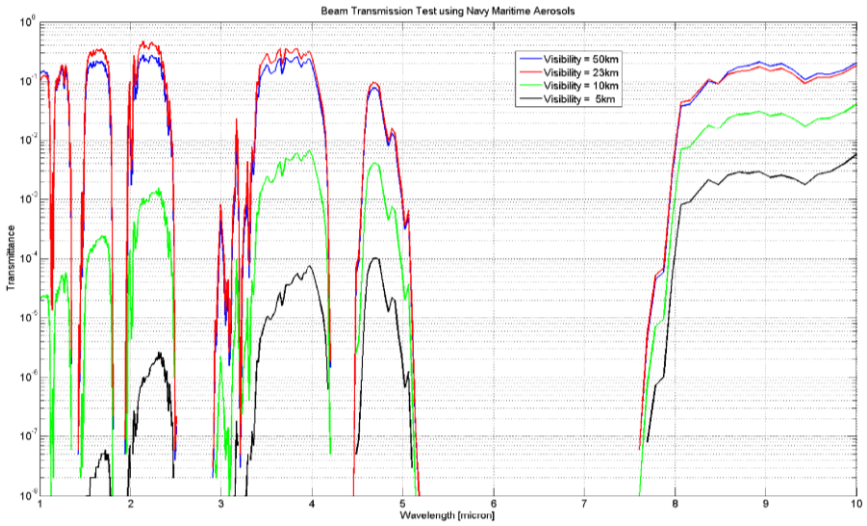

Figure 2. MODTRAN atmospheric simulation of 30 km free-space link with different atmospheric visibility levels. (Navy Maritime aerosol model, U.S. standard atmosphere, additional parameters defined in 2nd-quarterly report)

To estimate wavelength dependencies of the receiver over the SWIR to MWIR regions, the superconducting nanowire single-photon detector (SNSPD) model we originally used in our proposal was adopted. It is based on the following scaling law [1]:

$$\eta_{\text{det}}(\lambda) = \frac{\eta_0}{1+\left(\frac{\lambda}{\lambda_c}\right)^n}$$

that is fit to experimental measurements [2]. The parameters η_0 and λ_c correspond to the efficiency limit at small wavelengths and the cut-off wavelength, respectively. The cut-off wavelength and the exponent, *n*, are used as fitting parameters to the experimental data as shown in Figure 3 below.

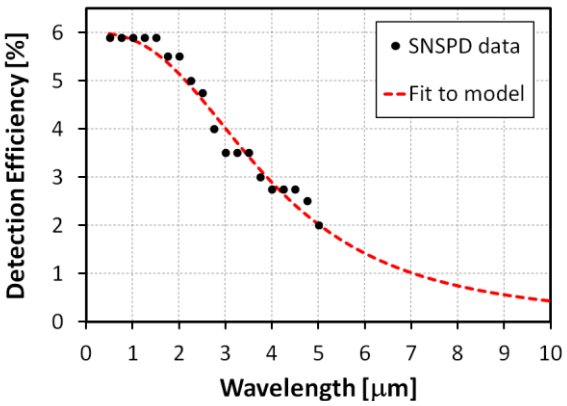

Figure 3. SNSPD efficiency vs. λ based on scaling model from [1] with fit to data from [2].

In addition to the Raman noise generated in the source, another important source of noise for SNSPDs is the presence of blackbody radiation, where the single-mode photon probability is given by

$$\mu_{BB} = \frac{\Delta\nu_{\text{det}}\Delta\tau_{\text{det}}}{\exp\left(h\nu_0/kT\right)-1}$$

where $\Delta\nu_{\text{det}}$ is the bandwidth of detection, $\Delta\tau_{\text{det}}$ is the detector gating window, h is the Planck constant, ν_0 is the center frequency, k is the Boltzmann constant, and T is the temperature in Kelvin. Similar to the source, a coincidence-to-accidentals ratio (CAR) can be calculated for the entire system by considering valid coincidences after relevant system losses are considered (i.e. channel transmittance and detector efficiency) compared to invalid coincidences that are primarily due to noise. In our system model, we assume spontaneous Raman scattering from the source and blackbody radiation as seen by detectors to be the dominant contributors to noise. From the system CAR, the system two-photon visibility (V) is calculated using $V = (CAR-1)/(CAR+1)$ and the quantum bit error rate ($QBER$) is calculated using $QBER = (1-V)/2$. Finally, using a entanglement-based system analysis modified from [3], the final key rate per detected pair is estimated by

$$R = q\left[1 - H_2(QBER+\xi) - f(QBER)H_2(QBER)\right]$$

where q is the basis reconciliation factor of ½, H_2 is the binary entropy function, ξ is a security parameter, and f is an error correction efficiency parameter. Lastly, the rate, R, is scaled by the average detected coincidence per source pump pulse to estimate the final average key rate per pulse.

4 Results and Discussion

4.1 Source Architecture and Modeling

Using the source model described in Section 3.1, the CAR was calculated for each material as a function of the pump power times the length (Power * Length = *PL*) as this product controls both the correlated photon pair and Raman noise generation rates. In our formulae, the former scales with the square of this product, and the latter is simply linearly proportional to the product.

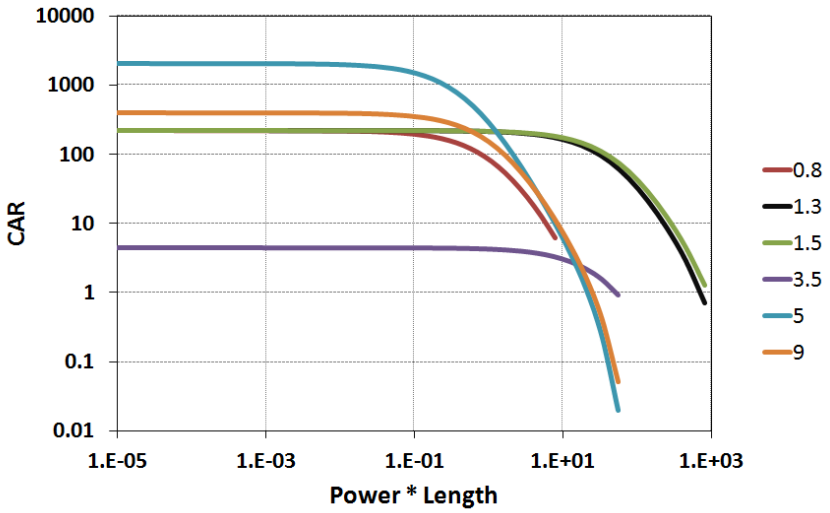

Figure 4. Calculated coincidence-to-accidental ratio (CAR) as a function of power*length for all wavelength bands

The results of the CAR calculation are summarized above in Figure 4. We observe that at low *PL* the CAR approaches a large static value for each material. In this regime, the relative quantity of the correlated pairs to noise photons is high, but the pair generation rate is quite low. Silica fiber is very common for photon pair generation in the NIR, and we observe that both of the chalcogenide fibers (As_2S_3 and As_2Se_3) in the MIR significantly out-perform silica in terms of CAR at low *PL*. As *PL* increases, the CAR tends to deteriorate though each material exhibits the beginning of its rapid decrease at different values for *PL*.

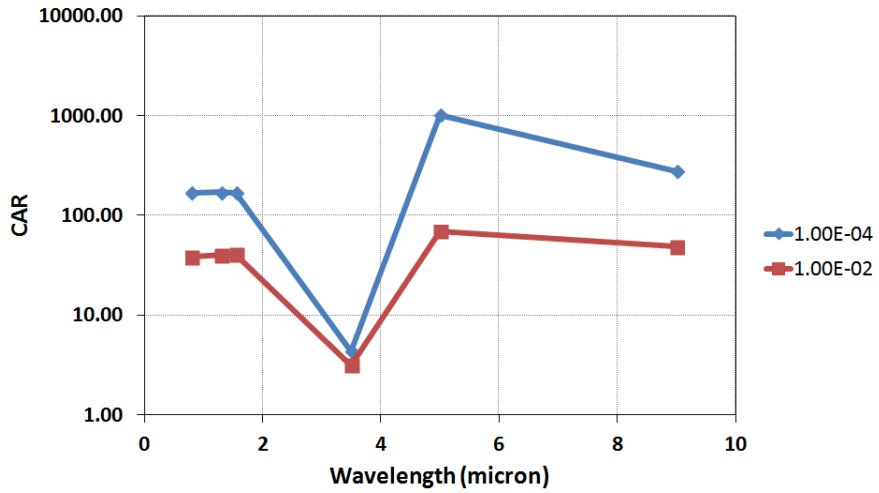

Figure 5. Calculated CAR in each wavelength band for two mean photon numbers

In Figure 5, we have computed the CAR in each wavelength band, assuming constant correlated photon pair generation rates (1e-4 (blue) and 1e-2 (red)). In this case, *PL* will be varied for each material to generate the desired pair rate. We note immediately that the larger pair rate, due to larger *PL*, corresponds to a lower CAR, which is consistent with Figure 4. Generally, higher pair generation rates will correspond to higher raw key rates for the QKD system, but lower CAR leads to lower two-photon visibilities and smaller net key rates. Figure 5 indicates that the source quality is highest at the longer MIR wavelengths, but the entire system model is required to determine which wavelength band will produce the highest net key rates. An updated system model incorporating this described source model is presented in Section 4.3 of this report.

4.2 Channel Model and Validation

There are no results to report related to the channel model or validation in this quarter of the project.

4.3 System Modeling

Using the system model described in Section 3.3 of the report, the system two-photon visibility and estimated key rate per coincidence detection were computed at the potential source wavelengths 0.8, 1.3, 1.5, 3.5, 5, and 9 μm. The modeling results for relatively good atmospheric visibility (23 km) and somewhat lower atmospheric visibility (10 km) based on MODTRAN results in Figure 2 are shown in Figure 6. As can be seen in this figure, the projected key rates are highest near 1.5 μm during good atmospheric visibility conditions, but quickly moves towards a longer wavelength of 3.5 μm as the atmospheric visibility drops. It is interesting that despite the fact that the modeled detection efficiency is reduced at these longer wavelengths as well as the fact that the source CAR is the lowest here, the improvements in channel loss more than compensate, resulting in a shift towards longer wavelength. With improvements in long-wavelength detection efficiency, the shift in optimal wavelength can be even greater, as illustrated in Figure 7 where a constant detection efficiency of 93% (previously demonstrated at 1.5 μm [4]) across all wavelengths was assumed. As can be seen, under reduced atmospheric visibility (i.e. 10 km), the optimal wavelength is pushed all the way out to 9 μm.

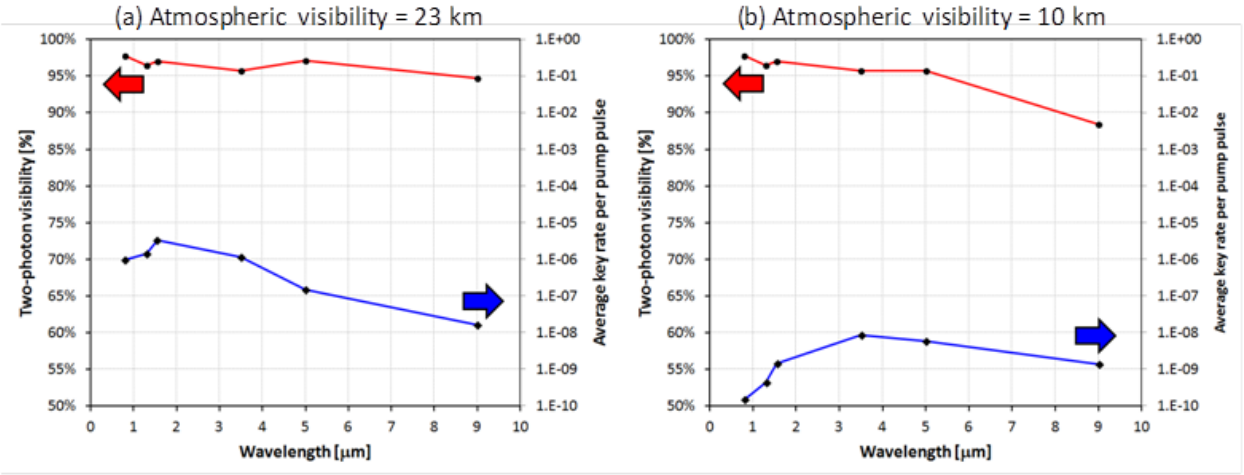

Figure 6. Modeling results of system two-photon visibility (*V*, left axis) and average key rate per pump pulse as a function of wavelength at atmospheric visibilities of (a) 23 km and (b) 10 km (assuming SNSPD detector model),'

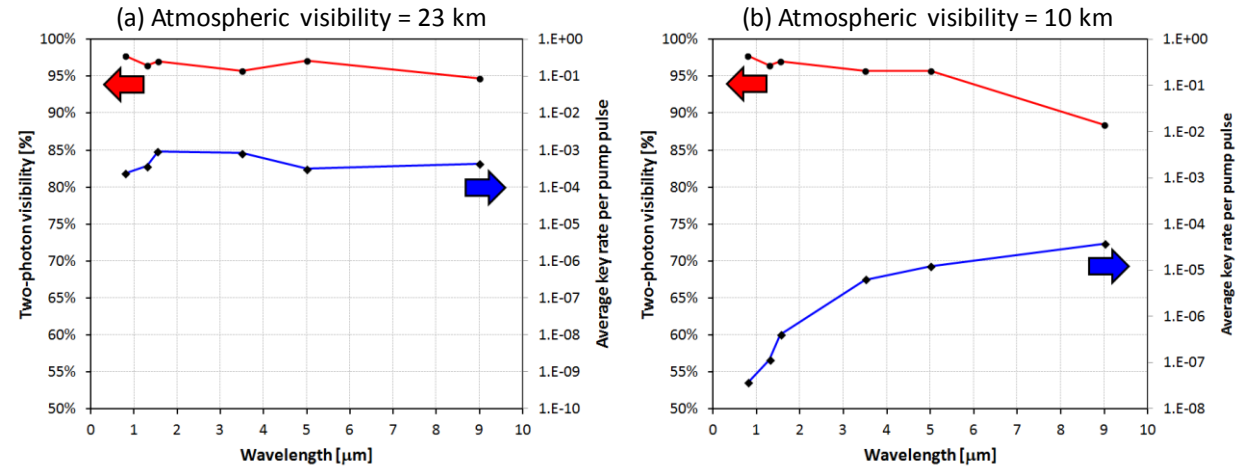

Figure 7. Modeling results of system two-photon visibility (*V*) and average key rate per pump pulse as a function of wavelength at an atmospheric visibility of (a) 23 km and (b) 10 km (assuming constant 93% detection efficiency).

4.4 Deliverables/Milestones

Date	Deliverable/Milestone	Status
June 2014	Progress Report No. 1: Year 1, 1st Quarter	✓
August 2014	Progress Report No. 2: Year 1, 2nd Quarter	✓
November 2014	Progress Report No. 3: Year 1, 3rd Quarter	✓
February 2015	Progress Report No. 4: Year 1, 4th Quarter	
May 2015	Progress Report No. 5: Year 2, 1st Quarter	
August 2015	Progress Report No. 6: Year 2, 2nd Quarter	
November 2015	Progress Report No. 7: Year 2, 3rd Quarter	
February 2016	Progress Report No. 8: Year 2, 4th Quarter	

May 2016	Progress Report No. 9: Year 3, 1st Quarter	
August 2016	Progress Report No. 10: Year 3, 2nd Quarter	
November 2016	Progress Report No. 11: Year 3, 3rd Quarter	
February 2017	Final Report	

5 Conclusions

In the last quarter of the SeaQuaKE project, ACS has developed a model for an entangled photon-pair source based upon the source architecture described in the previous report. The model is used to project source performance at the potential free-space transmission bands of 0.8, 1.3, 1.5, 3.5, 5, and 9 μm. In addition, a preliminary full system model incorporating transmitter, channel, and receiver wavelength dependencies was developed to project end-to-end key rate of a maritime quantum communications systems. Our results suggest that with current detector technologies and using maritime atmospheric models, the optimal wavelength may be near 1.5 μm under good atmospheric visibility (e.g. 23 km), but may quickly shift to a longer wavelength of 3.5 μm as the atmospheric visibility drops to 10 km. With possible future improvements in detector efficiency at longer wavelengths, our modeling suggest that the optimal wavelength may actually shift further out to 9 μm under reduced atmospheric visibility.

6 References

[1] Engel et al., "Temperature-dependence of detection efficiency in NbN and TaN SNSPD" arXiv:1210.5395v1 [cond-mat.supr-con] (2012).
[2] Marsili et al., "Efficient single photon detection from 500 nanometer to 5 micron wavelength," Nano Letters, 12, pg. 4799 (2012).
[3] J.-P. Bourgoin et al., A comprehensive design and performance analysis of low Earth orbit satellite quantum communication. New J. Phys. 15, 023006 (2013).
[4] F. Marsili et al., "Detecting single infrared photons with 93% system efficiency," Nat. Photonics 7(3), 210–214 (2013).