REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
12-10-2015	Final report	09/12/12 - 09/13/15

4. TITLE AND SUBTITLE

Quantum Communication Using Macroscopic Phase Entangled States

5a. CONTRACT NUMBER

5b. GRANT NUMBER

W31P4Q-12-1-0015

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

J.D. Franson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

University of Maryland at Baltimore County
1000 Hilltop Circle
Baltimore, MD 21250

8. PERFORMING ORGANIZATION REPORT NUMBER

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

U.S. Army AMCOM Contracting Center, CCAM-RD-A, Redstone Arsenal, AL 35898
U.S. Army RDECOM-AMRDEC, RDMR-WSD, Redstone Arsenal, AL 35898
DARPA-DSO, 3701 North Fairfax Drive, Arlington, VA 22203-1714

10. SPONSOR/MONITOR'S ACRONYM(S)

AMCOM,AMRDEC, DARPA

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution unlimited. Fundamental research exempt from prepublication controls.

13. SUPPLEMENTARY NOTES

DARPA-funded research; BAA 12-42, Defense Sciences Office-Wide Broad Agency Announcement

14. ABSTRACT

This final report describes the accomplishments of the program after 36 months of funding. A new long-range QKD protocol was proposed and its security was investigated. A pulsed Sagnac interferometer for single-shot phase shift measurements was investigated but not completed due to technical difficulties. Other methods for producing single-photon nonlinear phase shifts were investigated. Randomly-chosen unitary transformations were used to decrease the mutual information available to an eavesdropper. Several nonlinear effects were demonstrated using metastable xenon in a high-finesse cavity, including a nonlinear cross-phase shift. The nonlinear phase shifts were enhanced. Other techniques for long-range secure quantum communications were investigated based on the use of a small amount of shared prior key.

15. SUBJECT TERMS

entangled, photons, DARPA, quantum, secure,communications

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			J.D. Franson
Unclassified	Unclassified	Unclassified	UU	10	19b. TELEPHONE NUMBER *(Include area code)* 410-455-8115

i.

Quantum Communication Using Macroscopic Phase Entangled States

Final Report
Reporting Period: Sept. 12 2012 – Sept. 13 2015

Sponsored by
Defense Advanced Research Projects Agency (DOD)
Defense Sciences Office
DARPA BAA 12-42

Issued by:
U.S. Army Contracting Command, Aviation & Missile Command Contracting Center under

Grant No.: W31P4Q-12-1-0015

Technical Agent:
U.S. Army RDECOM, Aviation & Missile Research, Development & Engineering Center

Name of Contractor: University of Maryland at Baltimore County
Principal Investigator: Dr. James Franson
Business Address: 1000 Hilltop Circle, Baltimore, MD 21250
Phone number: 410-455-8115
Effective date of grant: 12 September, 2012
Grant expiration date: 13 September, 2015

ii. Description of the Effort

Most of the current methods for secure communications are based on public-key cryptography. Although this approach is very convenient to implement, it would become totally insecure if quantum computers are eventually developed. Quantum key distribution (QKD) provides an alternative form of secure communications whose security is based on the laws of physics (the Heisenberg uncertainty principle.) As a result, QKD systems are immune to an attack by quantum computers.

Quantum communications applications, including quantum key distribution (QKD), are currently limited by the fact that the useful bit rate decreases exponentially as a function of increasing range due to the effects of photon loss. The overall goal of the DARPA Quiness program was to investigate the feasibility of extending the range of QKD systems up to distances of 10,000 km at high data rates. For defense purposes, it is important to know whether or not that is feasible and the Quiness program can be viewed as a success regardless of the outcome of that question.

We proposed to develop an entirely new approach to quantum communications that is based on nonlocal interference between entangled macroscopic coherent states of light. Coherent states are produced by a laser, for example, and they are the closest approximation to classical states of light. One of their unique features is that their coherence properties remain intact as they travel over large distances in optical fibers, while only their amplitude decreases. This suggests that coherent states may be a good candidate for long-distance QKD.

A key feature of our approach is that the values of the bits themselves are carried by macroscopic coherent states, which are nearly as robust to loss and amplification as are the classical pulses of light used in commercial optical fiber communications systems. The security of a QKD system can be ensured by performing nonlocal quantum interference measurements on a fraction of the transmitted pulses. This approach decouples the loss from the secure bit rate, which is one of the main goals of the Quiness program.

Over the three-year duration of the Quiness program, we investigated the properties of a new form of quantum interference that is illustrated in Fig. 1. The system starts with two laser pulses that are relatively weak but still contain a large number (~1000) photons in a coherent state. The two laser beams pass through two Kerr atomic media that can produce a shift in the phase of a laser pulse provided that a single photon from another source and at a different frequency is also present in the medium. Since the single photon can travel along two separate paths as shown in the figure, this creates a state in which there is a quantum superposition of one or the other beam having been shifted in phase (a so-called Schrodinger cat state). The two laser beams then travel in opposite directions to the two ends of a QKD system where they interact with two more single photons and two Kerr media. As described in more detail in the attached list of publications, the results of this process violate Bell's inequality, which proves that no eavesdropper can obtain the information transmitted in this way. Thus such a system would be secure, even in the presence of an attack by a quantum computer.

One of the main goals of our program was to investigate several different ways in which to implement the Kerr medium that allows a single photon to change the phase of a laser beam passing through it. This is a challenging task, given that the interactions between single photons are very small. As a result, all three collaboratoring groups (UMBC, U. Rochester, and Boston U.) investigated different approaches towards achieving this goal. In general, these approaches consist of confining the single photon and the laser beam to a small region, such as a resonant cavity, that contains a large number of atoms in their ground state. Confining the photon increases its electric field strength, since a photon has a fixed energy, and this increases the interaction between the laser beam and the photon, as mediated by the atoms. As described in more detail, we investigated high-finesse cavities containing xenon atoms, lower-finesse cavities and traps with rubidium atoms, and solid-state waveguides with small mode areas for this purpose.

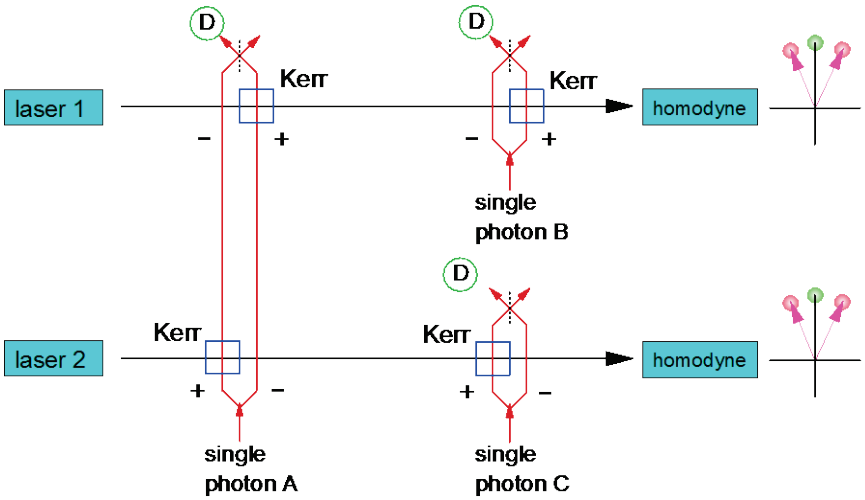


Fig. 1. The nonlocal interferometer investigated as a potential method for quantum key distribution.

Another goal was to perform a theoretical analysis of the degree of security that could be achieved in a QKD system based on this approach. Any information lost to the environment is typically assumed (conservatively) to be available to an eavesdropper, and this must be taken into account in designing a secure QKD system. The achievable operating range and corresponding secure data rate was calculated using several different approaches. It was found that our original approach should be expected to achieve an operational range of 400 km, while a modified approach may be able to extend the range beyond that.

Roughly speaking, it is the fact that the information in a single photon cannot be copied to produce two equivalent photons that is responsible for the security of a QKD system. As a result, QKD systems cannot use amplifiers, as can be shown using the no-cloning theorem of quantum information theory. It is possible, however, to implement quantum repeaters that essentially compensate for the effects of loss without copying the information in a single photon.

The technique described in Fig. 1 can be adapted to implement quantum repeaters, and a secondary goal of the program was to investigate this possibility. Another part of this task involved experimental demonstrations of a QKD system based on this approach in collaboration with a testbed to be developed at the Laboratory for Telecommunications Sciences (LTS).

A final goal was to investigate alternative forms of QKD that are based on different security assumptions and might therefore extend the operating range. For example, if it is assumed that the sender and recipient of the secure information share a small amount of private key initially, then there are more general approaches that appear to be capable of extending the useful range of the system.

iii. Significant accomplishments

A summary of the most significant accomplishments is as follows:

- Development of improved techniques to extend the expected range.
  - The expected range was extended to 400 km by using quantum state discrimination techniques.

- Demonstration of nonlinear phase shifts as required for the nonlocal interferometer of Fig. 1.
  - Experiments were performed using high-finesse resonators with xenon atoms, low-finesse resonators with rubidium atoms, and nonlinear waveguides.
  - All three demonstrated nonlinear phase shifts ~1 μ rad.
  - Although these experiments were successful, larger nonlinear phase shifts would be required to implement a QKD system as discussed below.

- Security analysis of QKD systems.
  - The approach shown in Fig. 1 was shown to be secure at ranges of at least 400 km.

- Development of hardware required for implementing a QKD system.
  - The hardware necessary for a demonstration of QKD was assembled, but the nonlinear phase shifts were too small for this purpose as described above.

- Investigation of alternative methods for QKD
  - Two approaches based on the use of a small amount of prior shared key was shown to be potentially useful at much larger ranges.
  - A preliminary experimental demonstration of a simple form of such a system was achieved.

A more detail list of accomplishments on a month-to-month basis can be found in our most recent monthly report but is not included here due to space limitations.

iv. Task-by task account of progress

Task 1. Development of basic interferometers and nonlinear phase shifts.

Task 1a. Theoretical analysis of nonlinear phase mechanisms. Theoretical calculations were performed to determine the optimal method for producing nonlinear phase shifts. The results were in good agreement with the experimental data for high-finesse cavities, but the results for low-finesse cavities were unexpectedly low.

Task 1b. Experimental investigations of nonlinear phase mechanisms. Experimental investigations of the theoretically-predicted nonlinear phase shifts were performed by all three collaborating groups. All observed nonlinear phase shifts but they were smaller than expected. Ways to increase the phase shifts to useful levels are discussed below. Two photographs of the high-finesse cavity experiment are shown in Fig. 2.

Task 1c. Demonstration of a nonlocal interferometer. The nonlinear interferometer of Fig. 1 could not be demonstrated because the nonlinear Kerr phase shifts were too small. The hardware necessary to support this task was developed, however, including the capability to convert photons at 823 nm to and from 1550 nm for low-loss propagation in optical fibers as illustrated in Fig. 3.

Task 1d. Demonstration of basic QKD capability. A QKD system could not be implemented based on Fig. 1 because of the small nonlinear phase shifts. An alternative QKD system was demonstrated using the data locking technique illustrated in Fig. 4, however.

Task 1e. Incorporation of the interferometers into a QKD testbed. Our work did not progress to the point that we could incorporate it into the QKD testbed at LTS.

Task 2. Increased range and improved capabilities .

Task 2a. *Theoretical investigations of methods to increase the nonlinear phase shift.* The expected range was increased to 400 km using state vector discrimination techniques.

Task 2b. Theoretical investigations of the effects of decoherence and ways to further reduce it. The effects of photon loss and decoherence in optical fibers were analyzed, including the effects of phase-insensitive amplifiers. Although an amplifier eliminates the violation of Bell's inequality, it was found that it may still be possible to implement secure quantum communications if the use of preshared secret key is allowed.

Task 2c. Experimental demonstration of enhanced nonlinear phase shifts. This subtask was not accomplished due to unexpected technical difficulties. Limited phase shifts were achieved in several different ways, however.

Task 3. Quantum repeaters and high-speed testbed.

Task 3a. Further experimental and theoretical work on enhanced phase shifts. Other approaches for increasing the phase shift were considered but not yet been implemented, such as reducing the volume of the high-finesse cavity. There was insufficient time to implement this approach during the Quiness program, but we hope to achieve that goal in a follow-on NSF project.

Task 3b. Demonstration of entanglement swapping and distillation. These effects could not be demonstrated due to the small phase shifts achieved.

Task 3e. Final report. A final report is being submitted herewith.

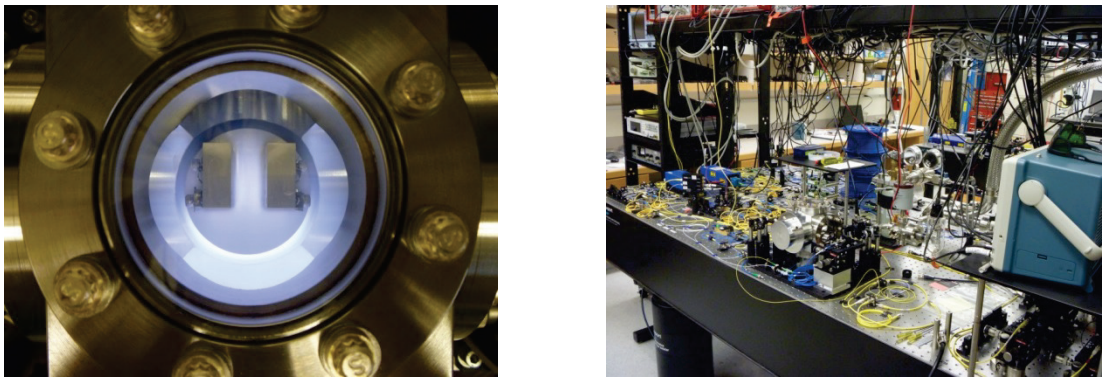


Fig. 2. Photographs of the high-finesse cavity experiment using metastable xenon (left image).

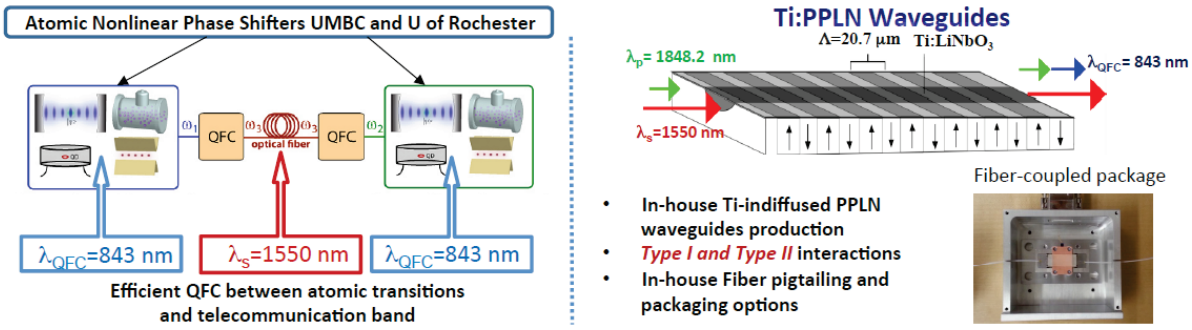


Fig. 3. Frequency conversion of photons from 843 nm to 1550 nm and back again. This allows the photons to interact with the atoms in a high-finesse atom and then propagate with low loss in an optical fiber.

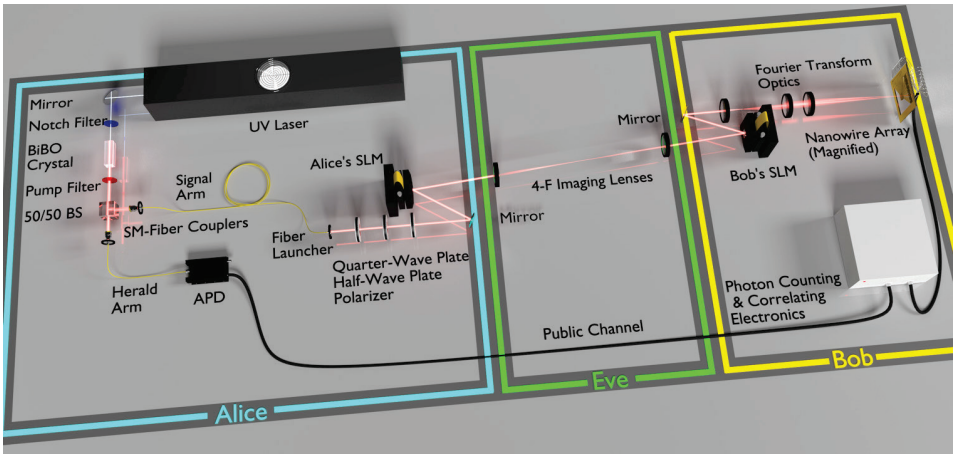


Fig. 4. Experimental demonstration of the data locking technique used for secure communications.

v. Summary

This program consisted of a collaboration between UMBC, Boston U., and U. Rochester. The primary goal was to investigate the feasibility of an approach for extending the range of QKD systems based on the use of nonlocal interference of macroscopic coherent states. The biggest technical challenge was producing a sufficiently large nonlinear phase shift (Kerr effect) to allow the final states from the interferometer to be distinguished. For a number of technical reasons, sufficiently large nonlinear phase shifts were not achieved in order to experimentally demonstrate QKD using this approach.

The nonlinear phase shift could be increased by several orders of magnitude by reducing the volume of the high-finesse cavity, which would allow QKD systems of this kind to be implemented. We are continuing to pursue this goal under a follow-on NSF grant. It should be noted that other groups did succeed in producing sufficiently large phase shifts during this time using other techniques, so that the basic approach is still promising.

Alternative methods for secure communications over large distances were also investigated based on the use of small amounts of shared secret key. In that case, secure quantum communications may be possible over large distances but at the expense of reduced levels of security. In practice, the goal of any secure communications system is to bound the amount of information available to an eavesdropper below some acceptable level, and absolute security may not be a realistic requirement.

vi. List of patents

- Patent application # 14/508,741, “Quantum key distribution over large distances using amplifiers and unitary transformations”, James Franson, Todd Pittman, Brian Kirby, and Garrett Hickman

vii. List of publications

- G. Jaeger, D. S. Simon, and A. V. Sergienko, "Coherent state quantum key distribution based on entanglement sudden death," on-line, *Quantum Information Processing*, 16 July (2015). DOI 10.1007/s11128-015-1063-4
- D. S. Simon, C. A. Fitzpatrick and A. V. Sergienko, "Discrimination and synthesis of recursive quantum states in high-dimensional Hilbert spaces," *Physical Review A*, v. 91, 043806 (2015).
- Gregg Jaeger, "Measurement and fundamental processes in quantum mechanics," *Foundations of Physics* ,v. 45, pp. 806-819 (2015).
- D.S. Simon, G. Jaeger, and A. V. Sergienko, "Coherent state quantum key distribution with entanglement witnessing", *Physical Review A*, v. 89, 012315 (2014).
- David Simon, Gregg Jaeger, and Alexander Sergienko "Quantum information in communication and imaging, " *International Journal of Quantum Information*, v.12, 143004 (2014).
- Gregg S. Jaeger "On the identification of the parts of compound quantum objects." *Foundations of Physics*, v.44, 709-724 (2014).
- Gregg S. Jaeger and Alexander V. Sergienko "Entanglement sudden death: a threat to advanced quantum key distribution?", *Natural Computing,* .v. 13, pp. 459-467 (2014).
- David Simon and Alexander Sergienko", High-capacity quantum key distribution via hyperentangled degrees of freedom" *New Journal of Physics*, v.16, 063052 (2014).
- Gregg Jaeger, "What in the (quantum) world is macroscopic?", *Am. J. Phys*. 82, 896 (2014)
- Gregg Jaeger, David Simon, and Alexander V. Sergienko", Implications of disentanglement and locality induction for quantum information processing and cryptography, *Quantum Matter* v. 2, 427-435 (2013).
- P. Ben Dixon, Gregory A. Howland, Curtis J. Broadbent, John C. Howell, and James Schneeloch, "Violation of Continuous-Variable Einstein-Podolsky-Rosen Steering with Discrete Measurements" Phys. Rev. Lett. **110**, 130407 (2013).
- James Schneeloch, Curtis J. Broadbent, John C. Howell, "Uncertainty relation for mutual information", Phys. Rev. A **90** 062119 (2014).
- James Schneeloch, Curtis J. Broadbent, and John C. Howell, "Improving Einstein-Podolsky-Rosen steering inequalities with state information", Phys. Lett. A **378** 766-769 (2014).
- B.T. Kirby and J.D. Franson, "Nonlocal Interferometry using Macroscopic Coherent States and Weak Nonlinearities", Phys. Rev. A **87**, 053822 (2013).
- M. Lai, J.D. Franson, and T.B.Pittman, "Transmission Degradation and Preservation for Tapered Optical Fibers in Rubidium Vapor", Applied Optics **52**, 2595 (2013).
- T.B. Pittman, D.E. Jones, and J.D. Franson, "Ultralow-Power Nonlinear Optics Using Tapered Optical Fibers in Metastable Xenon", Phys. Rev A **88**, 053804 (2013).
- B.T. Kirby and J.D. Franson, "Entangled Coherent State Interferometry Over Long Distances Using State Discrimination", Phys. Rev. A. **89**, 033861 (2014).

- G.T. Hickman, T.B. Pittman, and J.D. Franson, "Nonlinear Optics at Ultra-Low Power Levels using Metastable Xenon in a High-Finesse Optical Cavity", Optics Express **22**, 1-6 (2014).
- B.T. Kirby, G.T. Hickman, T.B. Pittman, and J.D. Franson, "Feasibility of Single Photon Cross-Phase Modulation using metastable Xenon in a High Finesse Cavity", Optics Communications **337**, 57 (2015).
- D.E. Jones, J.D. Franson, and T.B. Pittman, "Saturation of atomic transitions using subwavelength diameter tapered optical fibers in rubidium vapor", JOSA B **31**, 1997 (2014).
- D.E. Jones, J.D. Franson, and T.B. Pittman, "Ladder-Type Electromagnetically Induced Transparency using Nonofiber-Guided Light in a Warm Atomic Vapor", Phys. Rev. A **92**, 043806 (2015).
- J.D. Franson and B.T. Kirby, "Origin of Quantum Noise and Decoherence in Distributed Amplifiers", accepted for publication in Physical Review A (2015).
- G.T. Hickman, T.B. Pittman, and J. D. Franson, "Low-Power Cross-Phase Modulation in a Metastable Xenon-Filled Cavity", accepted for publication in Physical Review A (2015).

viii. List of public presentations

- J.D. Franson, "Quantum Communication Using Entangled Photon Holes", Frontiers in Optics Conference, Rochester, NY, Oct. 14-18, 2012. (Invited)
- B. T. Kirby and J.D. Franson, "Nonlocal Interferometry Using Macroscopic Coherent States and Weak Nonlinearities", March Meeting of the American Physical Society, Baltimore, MD, Mar. 18-22, 2013.
- T.B. Pittman, M.M. Lai, and J.D. Franson, "Enhanced Transmission for Ultra-Low-Power Nonlinear Optics Experiments Using Tapered Optical Fibers in Rubidium Vapor", CLEO/QELS Conference, San Jose, CA, June 9-14, 2013.
- Gregg Jaeger, "Macroscopic Realism and Quantum Information." Quantum Theory: Advances and Problems, Vaxjo Sweden June 2013.
- J.D. Franson, "Schrodinger Cats and Nonlocal Interferometry", Tenth Coherence and Quantum Optics Conference, Rochester, NY, June 17-20, 2013 (Invited)
- J.D. Franson, "Schrodinger Cats and Nonlocal Interferometry", Wigner Conference, Budapest Hungary, Nov. 11-14 (Invited).
- B.T. Kirby and J.D. Franson, "Nonlocal Interferometry Using Macroscopic States and State Discrimination", CLEO/QELS conference, San Jose, CA, June 9-12, 2014.
- D.E. Jones, J.D. Franson, and T.B. Pittman, "Saturation of Atomic Transitions with a Tapered Optical Fiber in Rubidium Vapor", CLEO/QELS conference, San Jose, CA, June 9-12, 2014.
- J.D. Franson, "Quantum Communication Using Entangled Photon Holes", Frontiers in Optics Conference, Rochester, NY, Oct. 14-18, 2012. (Invited)
- B. T. Kirby and J.D. Franson, "Nonlocal Interferometry Using Macroscopic Coherent States and Weak Nonlinearities", March Meeting of the American Physical Society, Baltimore, MD, Mar. 18-22, 2013.

- T.B. Pittman, M.M. Lai, and J.D. Franson, “Enhanced Transmission for Ultra-Low-Power Nonlinear Optics Experiments Using Tapered Optical Fibers in Rubidium Vapor”, CLEO/QELS Conference, San Jose, CA, June 9-14, 2013.
- Gregg Jaeger, "Macroscopic Realism and Quantum Information.” Quantum Theory: Advances and Problems, Vaxjo Sweden June 2013.
- J.D. Franson, “Schrodinger Cats and Nonlocal Interferometry”, Tenth Coherence and Quantum Optics Conference, Rochester, NY, June 17-20, 2013 (Invited)
- J.D. Franson, “Schrodinger Cats and Nonlocal Interferometry”, Wigner Conference, Budapest Hungary, Nov. 11-14 (Invited).
- B.T. Kirby and J.D. Franson, “Nonlocal Interferometry Using Macroscopic States and State Discrimination”, CLEO/QELS conference, San Jose, CA, June 9-12, 2014.
- D.E. Jones, J.D. Franson, and T.B. Pittman, “Saturation of Atomic Transitions with a Tapered Optical Fiber in Rubidium Vapor”, CLEO/QELS conference, San Jose, CA, June 9-12, 2014.
- J.D. Franson, “Entanglement and Decoherence”, QTPA Conference, Vaxjo, Sweden, June 8-11, 2015 (Invited).
- G.T. Hickman, T.B. Pittman, and J.D. Franson, “Xenon-Based Nonlinear Fabry-Perot Interferometer for Quantum Information Applications”, CLEO/QELS Conference, San Jose, CA, May 10-15, 2015.
- J.D. Franson and B.T. Kirby, “Effects of Distributed Amplifiers on Quantum Coherence”, CLEO/QELS Conference, San Jose, CA, May 10-15, 2015.

ix. Poster presentations

None

Quantum Communication Using Macroscopic Phase Entangled States

Final Report
Reporting Period: Sept. 12 2012 – Sept. 13 2015

Sponsored by
Defense Advanced Research Projects Agency (DOD)
Defense Sciences Office
DARPA BAA 12-42
Issued by:
U.S. Army Contracting Command, Aviation & Missile Command Contracting Center under
Grant No.: W31P4Q-12-1-0015

Technical Agent:
U.S. Army RDECOM, Aviation & Missile Research, Development & Engineering Center

Name of Contractor: University of Maryland at Baltimore County
Principal Investigator: Dr. James Franson
Business Address: 1000 Hilltop Circle, Baltimore, MD 21250
Phone number: 410-455-8115
Effective date of grant: 12 September, 2012
Grant expiration date: 13 September, 2015

OVERVIEW

Public key cryptography is widely used but would be insecure against an attack by a quantum computer.

Quantum key distribution (QKD) is secure against any attack but its range is currently very limited.

The major goal of this project was to investigate a new approach to QKD that may increase the range.

Based on nonlocal quantum interference effects between weak coherent states (laser pulses).

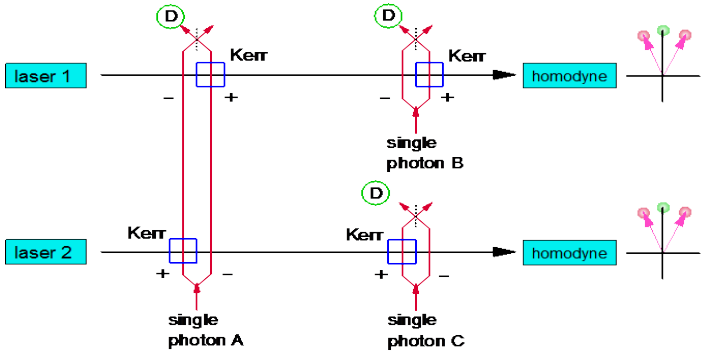
Another goal was to investigate the security of this approach.

A final goal was to investigate other potential long-range methods for secure quantum communications.

Based on the use of a small amount of shared secret key.

KEY CHALLENGES

The approach was based on a nonlocal interferometer in which a single photon can shift the phase of a laser pulse (Kerr effect):



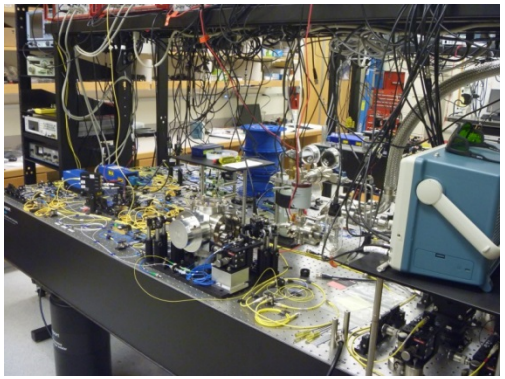
The biggest challenge was developing a technique for producing a sufficiently large nonlinear phase shift from a single photon.

All three collaborating groups investigated different approaches.

SINGLE-PHOTON PHASE SHIFTS

All three teams developed techniques to allow a single photon to produce a phase shift in a laser beam.

UMBC developed a high-finesse cavity filled with metastable xenon atoms as shown below:



U. Rochester demonstrated a nonlinear phase shift using a low-finesse cavity and rubidium atomic vapor.

Boston U. demonstrated a nonlinear phase shift using nonlinear waveguides.

The nonlinear phase shifts were smaller than expected.

ADDITIONAL CHALLENGES

The approach needed to be optimized to give the maximum operational range.

Theoretical analyses needed to be performed to demonstrate that the approach was secure against any eavesdropping attack.

Alternative approaches were also considered in an effort to increase the range.

- Such as the possibility of using a small amount of previously shared secret key.

Task 1 – DEVELOPMENT OF BASIC INTERFEROMETER AND NONLINEAR PHASE SHIFT

Task 1a. Theoretical analysis of nonlinear phase mechanisms. Theoretical calculations were performed to determine the optimal method for producing nonlinear phase shifts. The results were in good agreement with the experimental data for high-finesse cavities, but the results for low-finesse cavities were unexpectedly low.

Task 1b. Experimental investigations of nonlinear phase mechanisms. Experimental investigations of the theoretically-predicted nonlinear phase shifts were performed by all three collaborating groups. All observed nonlinear phase shifts but they were smaller than expected. Ways to increase the phase shifts to useful levels are discussed below.

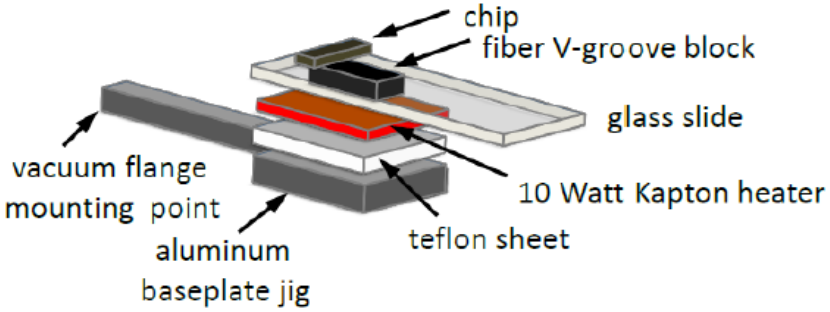
Task 1c. Demonstration of a nonlocal interferometer. The nonlinear interferometer of Fig. 1 could not be demonstrated because the nonlinear Kerr phase shifts were too small. The hardware necessary to support this task was developed, however, including the capability to convert photons at 823 nm to and from 1550 nm for low-loss propagation in optical 3.

Task 1d. Demonstration of basic QKD capability. A QKD system could not be implemented based on Fig. 1 because of the small nonlinear phase shifts. An alternative QKD system was demonstrated using the data locking technique.

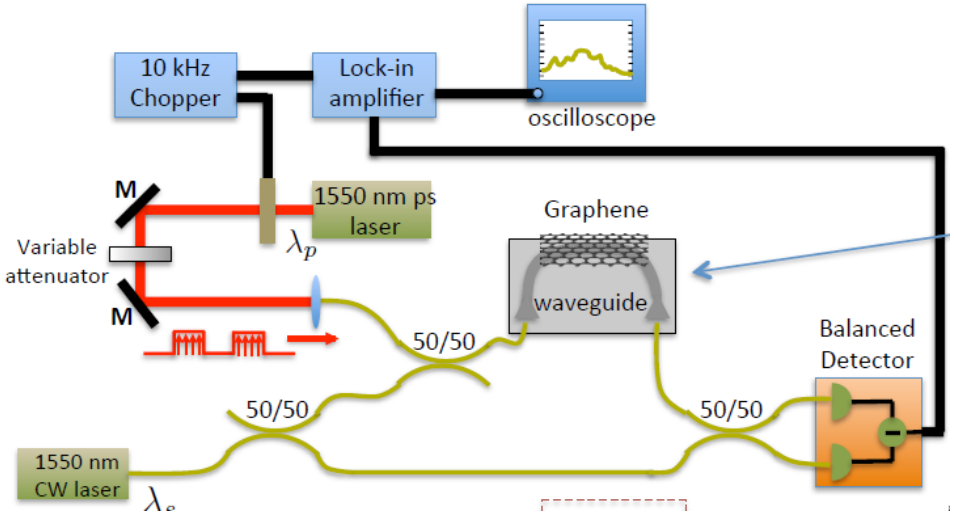
Task 1e. Incorporation of the interferometers into a QKD testbed. Our work did not progress to the point that we could incorporate it into the QKD testbed at LTS.

OTHER NONLINEAR PHASE SHIFT EXPERIMENTS

chip vacuum mount/heater unit



Sandia microresonator on a chip



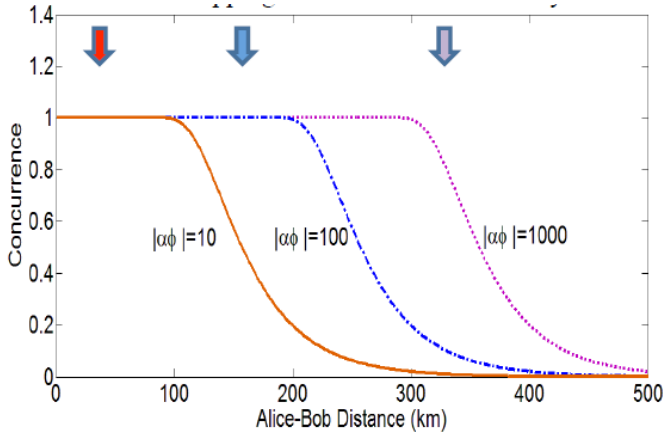
Graphene monolayer on a waveguide

Task 2 – INCREASED RANGE AND IMPROVED CAPABILITIES

Task 2a. *Theoretical investigations of methods to increase the nonlinear phase shift.* The expected range was increased to 400 km using state vector discrimination techniques.

Task 2b. Theoretical investigations of the effects of decoherence and ways to further reduce it. The effects of photon loss and decoherence in optical fibers were analyzed, including the effects of phase-insensitive amplifiers. Although an amplifier eliminates the violation of Bell's inequality, it was found that it may still be possible to implement secure quantum communications if the use of pre-shared secret key is allowed.

Task 2c. Experimental demonstration of enhanced nonlinear phase shifts. This subtask was not accomplished due to unexpected technical difficulties. Limited phase shifts were achieved in several different ways, however.



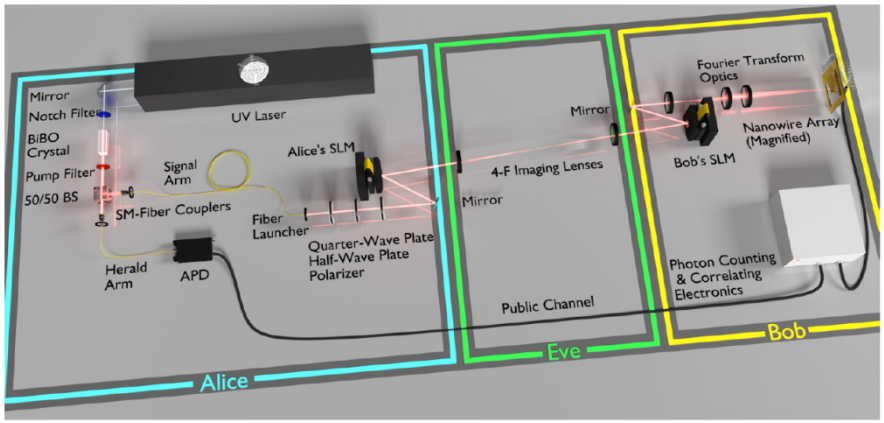
Theoretical calculations of increased range.

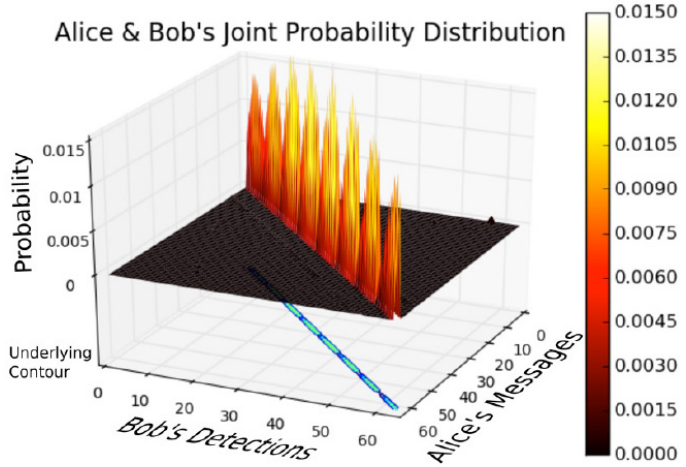
TASK 3 – QUANTUM REPEATERS AND HIGH SPEED TESTBED

Task 3a. Further experimental and theoretical work on enhanced phase shifts. Other approaches for increasing the phase shift were considered but not yet been implemented, such as reducing the volume of the high-finesse cavity. There was insufficient time to implement this approach during the Quiness program, but we hope to achieve that goal in a follow-on NSF project.

Task 3b. Demonstration of entanglement swapping and distillation. These effects could not be demonstrated due to the small phase shifts achieved.

Task 3e. Final report. In addition to these slides, a final report has been submitted.





Quantum enigma experiment

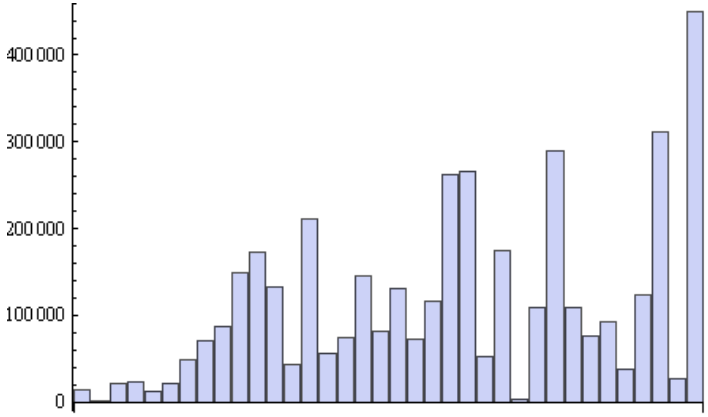
FINANCIAL SUMMARY

Funding increments:

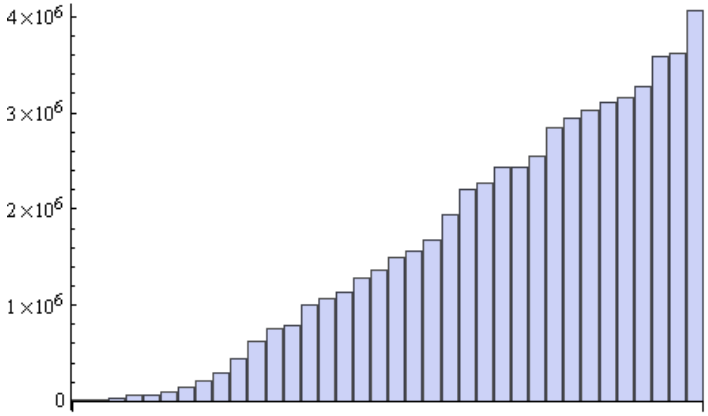
9/12/12	$259,608
2/12/13	$1,000,000
5/24/13	$594,444
1/14/14	$455,552
3/05/14	$911,115
6/17/11	$879,281

Total funding: $4,100,000

Total billed: $4,066,601



Monthly billed



Cumulative billed

The planed spending was approx. uniform except for a slight increase during the time of summer salaries.

The final billing period was larger than average due to summer salary and the usual delay in billing by subcontractors.

SUMMARY

The primary goal of this project was to investigate the possibility of increasing the range of QKD systems.

Based on nonlocal interferometry using coherent states.

Significant accomplishments:

Small nonlinear phase shifts were demonstrated in three different ways.

- Not sufficient to achieve the Quiness goals.

The potential range of the system was increased using state-vector discrimination.

The proposed system was shown to be secure at ranges up to 400 km.

Alternative methods of secure quantum communications were investigated.

Overall conclusion:

Long-range QKD may only be possible using quantum repeaters.

Long-range secure communications may be achievable using small amounts of prior shared key.