Special Notice 13-SN-0004

Special Program Announcement for 2013 Office of Naval Research

Research Opportunity: Free Space Optical Quantum Key Distribution

I. INTRODUCTION:

This announcement describes an applied research program, entitled "Free Space Optical Quantum Key Distribution," to be launched under the ONRBAA13-001, Long Range Broad Agency Announcement for Navy and Marine Corps Science and Technology which can be found at http://www.onr.navy.mil/Contracts-Grants/Funding-Opportunities/Broad-Agency-Announcements.aspx. The research opportunity described in this announcement specifically falls under numbered paragraph 2 of the "Command, Control, Communications, Computers; Mathematics, Computers and Information Research (Code 31)" sub-section. The submission of proposals, their evaluation and the placement of basic research contracts and grants will be carried out as described in that Broad Agency Announcement.

The purpose of this announcement is to focus attention of the scientific community on (1) the area to be studied, and (2) the planned timetable for the submission of proposals.

II. TOPIC DESCRIPTION: Free Space Optical Quantum Key Distribution

The purpose of this topic will explore and exploit Free Space Optical Quantum Key Distribution. The program will pursue research that identifies, understands, and develops new knowledge, of issues controlling the performance of a system of a free space optical quantum key distribution system, operating in a naval environment. The algorithms, methods, techniques, and strategies must eventually support applied research and system engineering that would culminate in a demonstration and potentially fielded system for distribution of provably secure one time cryptographic pads.

Background:

Quantum Information Sciences have become a rapidly developing field with considerable research effort expended in the development of quantum bits (QBITs) and strategies to support quantum computation (QC). In parallel with efforts devoted to computation, it has long been recognized that the mathematical framework associated with quantum mechanics can enable secure communications without the need for additional cryptographic systems. Bennett and Brassard (BB84) proposed a method for secure communications based upon the use of non-orthogonal bases in 1984 that has been experimentally demonstrated in a number of settings. Since the publication of the BB84 protocol additional protocols, such as the Ekert 91 protocol (E91), have been proposed that also exploit quantum entanglement to insure secure communications. Regardless of the protocol, practical implementations of the protocol introduce errors arising from the inability to precisely implement the underlying mathematical structure that is called for in physical hardware. Since it is currently impossible to distinguish between the effects of these errors, and the presence of an

eavesdropper within the QCs channel additional tools such as privacy amplification and information reconciliation have been developed and implemented.

Much of the experimental research effort devoted to quantum communications has involved the use of non-dispersive fiber optics with low loss. However, there are a number of circumstances in which communications over a point-to-point optical link are desirable and a fiber implementation is impractical. To date experimental demonstrations of quantum communication protocols have occurred in relatively benign atmospheric conditions, such as between mountaintops, or mountaintops and satellites. While these experiments have demonstrated communication ranges that exceed 100 km, they have also demonstrated relatively low effective bit rates in comparison to fiber optic implementations. One goal of this announcement is to increase fundamental knowledge and understanding of the issues that currently prevent physical implementations of high effective bandwidth (on the order of 100 MB/sec), long range (> 30 km) provably secure QCs in challenging environments. These environments are characterized by dispersive, time varying atmospheres with significant scattering, and transmitters and receivers that are in motion.

Specifically the type of environment that we are concerned with exists between naval platforms operating on the surface of the sea, with communications ranges limited by the line of sight between platforms. The optical channel is both dispersive and non-stationary. As a result, there is significant scattering of the propagating photons due to the presence of aerosols, as well as losses due to absorption. Furthermore, because the platforms are in motion and not fully stabilized it will be difficult in the environment to maintain precise timing control and spatial alignment that supports resolving polarization states.

Objective: The Office of Naval Research (ONR) is interested in receiving proposals that develop the mathematical framework and associated analysis that eventually supports practical secure physical implementations of QCs schemes with high bandwidth, long range, provable secure communications.

The proposed research efforts must focus on the free space optical communications environment that has been described earlier. The primary emphasis should be on the mathematical framework with limited resources being devoted to experimental verification.

Research Concentration Areas:

Suggested research areas include but are not limited to the following thrusts:

- Understand the implications of imperfect physical implementations and environmental effects upon the security of Quantum Key Distribution (QKD) protocols. The extant security proofs and appeals to the no-cloning theorem strictly apply to faithful implementations of the protocol which have yet to be achieved in practice. Within this thrust we desire to understand the impacts of imperfect implementations, through

mathematical analysis techniques, upon the security and weaknesses of QKD protocols operating in realistic environments focusing upon the amount of information that can be extracted by an eavesdropper, the time required to obtain this information, and the resources required to obtain the information.

- The development of practical methods that would enable an eavesdropper to exploit flaws in the implementation of a QKD system to obtain information. As an example, due to the presence of aerosols with particles whose radius is on the order of the wavelength of light there will be significant scattering and information is potentially available to an attacker through the scattered light. ONR desires both a rigorous mathematical analysis and potential demonstration of methods that obtain information from the quantum communications channel without altering the transmitter or the receiver that the eavesdropper is present.

- The development of new protocols that offer enhanced security relative to extant protocols when implemented that take into account dispersion, absorption, and scattering of photons, timing uncertainty due to the optical path, and spatial jitter of the detectors arising from the failure to stabilize the detectors in space and time. Work proposed under this thrust should provide a rationale for the strategy that leads to a new protocol.

- The development of implementable methods that maximize the information that can be encoded on a single particle. Typically polarization, angular momentum, as well as time of arrival within a specified window have been employed to encode information. ONR is interested in receiving proposals that offer additional states and mechanisms to encode information. Work proposed under this thrust should provide a rationale for the selected encoding scheme and state.

- The development of schemes that produce random numbers that do not require additional whitening through software.

III. FULL PROPOSAL SUBMISSION AND AWARD INFORMATION

Full proposals should be submitted under **ONRBAA13-001** by **22 JAN 2013.** Full Proposals received after that date will be considered as time and availability of funding permit.

ONR anticipates that both grants and contracts will be issued for this effort. Full proposals for contracts should be submitted in accordance with the instructions at Section IV, Application and Submission Information, item 2.b, Full Proposals and item 6, Submission of Full Proposals for Contracts, Cooperative Agreements, and Other Transactions. Full proposals for grants should be submitted in accordance with the instructions at Section IV, Application and Submission Information, item 5, Submission of Grant Proposals through Grants.gov. All full proposals for grants must be submitted through www.grants.gov. The following information must be completed as

follows in the SF 424 to ensure that the application is directed to the correct individual for review: Block 4a, Federal Identifier: Enter N00014; Block 4b, Agency Routing Number, Enter the three (3) digit Program Office Code (311) and the Program Officer's name, last name first, in brackets (Schwartz, Carey). All attachments to the application should also include this identifier to ensure the proposal and its attachments are received by the appropriate Program Office.

ONR plans to fund six to eight individual awards with a value of $200K per year, using Basic Research funds. However, lower and higher cost proposals will be considered. The period of performance for projects may be from one to three years.

Although ONR expects the above described program plan to be executed, ONR reserve the right to make changes.

Funding decisions should be made by 22 FEB 2013. Selected projects will have an estimated grant award date of 13 MAY 2013 and an estimated contract award date of 12 AUG 2013.

VI. SIGNIFICANT DATES

Event	**Date**
Recommended Full Proposal Submission	22 JAN 2013
Notification of Selection: Full Proposals*	22 FEB 2013
Awards*	13 MAY 2013 (Grants) 12 AUG 2013 (Contracts)

Note: * These are approximate dates**.**

V. POINTS OF CONTACT

In addition to the points of contact listed in ONRBAA13-001, the specific points of contact for this announcement are listed below:

Technical Points of Contact:

Carey Schwartz, Program Officer, carey.schwartz@navy.mil

Business Point of Contact:

Jennifer Brown, Contract Specialist, Jennifer.brown4@navy.mil

VIII. SUBMISSION OF QUESTIONS

Any questions regarding this announcement must be provided to the Technical Points of Contact and/or the Business Point of Contact listed above. All questions shall be submitted in writing by electronic mail.

Answers to questions submitted in response to this Special Notice will be addressed in the form of an Amendment and will be posted to the following web pages:

- Federal Business Opportunities (FEDBIZOPPS) Webpage – https://www.fbo.gov/
- Grants.gov Webpage – http://www.grants.gov/
- ONR Special Notice Webpage - http://www.onr.navy.mil/Contracts-Grants/Funding-Opportunities/Special-Notices.aspx

Questions regarding Full Proposals should be submitted NLT two weeks before the dates recommended for receipt of Full Proposals. Questions after this date may not be answered.