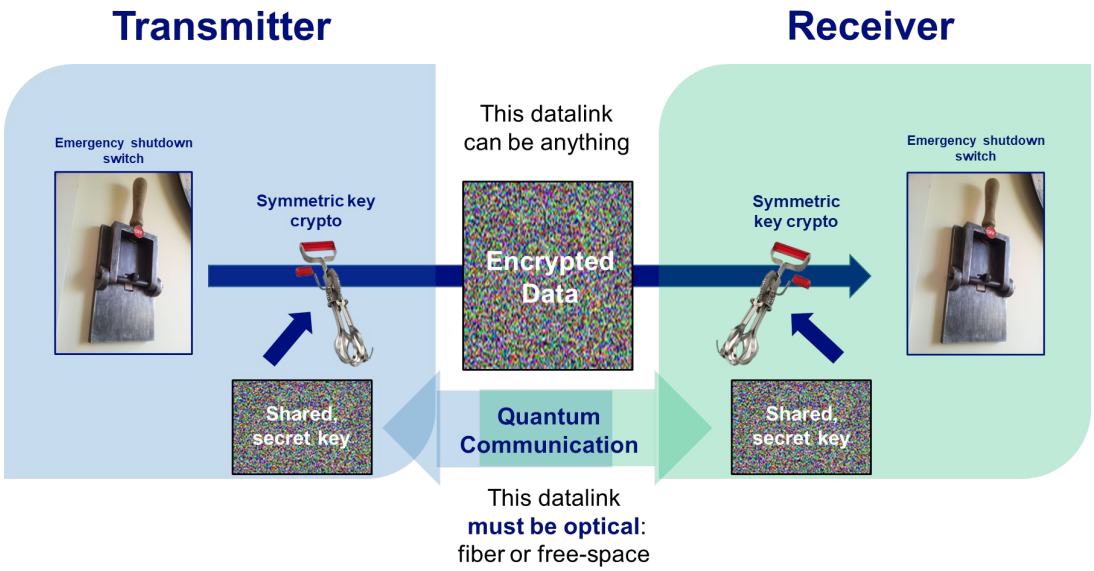


Los Alamos NATIONAL LABORATORY

Quantum Enhanced Communication Security

LA-UR-22-27660
8/1/2022

POTENTIAL AREAS FOR PARTNERSHIP

Quantum Enhanced Communication Security (QECS) leverages the unpredictable nature of quantum states to create shared secret random numbers which cannot be duplicated, hacked or cracked. These unpredictable random numbers are used as raw material in an array of data security purposes, such as cryptographic keys or authentication tokens. Quantum transmission can be performed through an optical fiber or via free space line-of-sight link.

The ideal partner will augment LANL expertise to expedite commercialization by bringing unique expertise in microelectronics and photonics design and manufacturing for communication systems application areas including fiber optic, free-space laser, satellite or airborne secure communications.

The Laboratory is looking for a partner to commercialize these technologies, with the expectation that substantial manufacturing will be done in the U.S.

SUMMARY

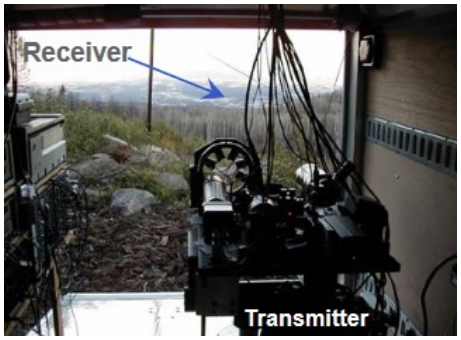
Privacy and authentication are essential features of virtually all communication systems. This is an area in which Quantum Networks particularly excel. By applying a user selected quantum operator to a system, information can be sent to the receiver without a chance of an eavesdropper being able to surreptitiously record the sent information. Without the proper quantum operator to decode the information, the eavesdropper will corrupt the sent information without being able to use it themselves.

BENEFITS

QECS systems have been developed for short distance fiber-based as well as long distance free space quantum communications systems.

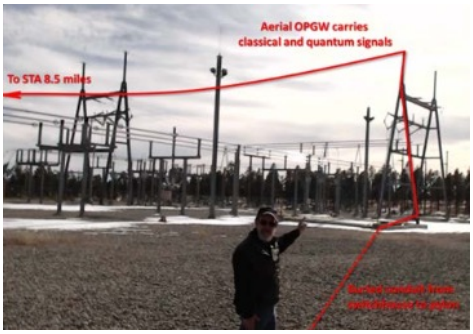
- Economical: Room temperature operation obviates cryogenics.
- Versatile: Microchip to board level scalability
- Highly secure: Elementary quantum optical processes ensure true random number generation, essential for multifactor authentication.
- Efficient: Embedded elementary components can be easily monitored for enhanced cyber security.
- Compact: Configurable as quantum network interconnect

FCI
Richard P. Feynman Center for Innovation
at Los Alamos National Laboratory



Through the air

Critical infrastructure protection



Electric grid security

WHAT IS UNIQUE ABOUT THE TECHNOLOGY

Although the quantum key distribution technique was not created at Los Alamos, laboratory researchers have taken the technology, quite literally, to new lengths in the interest of national security. Los Alamos pioneered free-space quantum communications to establish secure *ad hoc* networks, vital for satellite quantum communications (QC), which holds the potential to extend the reach of QC globally. In parallel, Los Alamos scientists have demonstrated QC over existing optical fiber links, including buried fiber and fiber suspended from utility poles.

WHAT'S BEHIND OUR TECHNOLOGY

In quantum secured networks, parties encode information on quantum states of single photons, transmit and receive those photons, and make measurements of the quantum states. Quantum states such as polarization and optical phase are commonly used. The series of measurements results in secret information which is shared between the communicating parties, which they may then use to secure their data. Because the transmitted photons cannot be intercepted or duplicated without being destroyed, any attempt at interception will be seen by trusted parties.

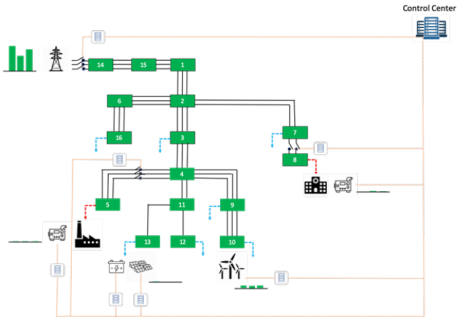
OUR COMPETITIVE ADVANTAGES

Los Alamos researchers pioneered key developments networks for quantum enhanced secure communications. Our early work focused on securing point-to-point links between two parties and we have recently extended these security assurances from pairwise links to a mesh network. Los Alamos has developed multi-party authentication and privacy solutions which are plug-and-play compatible with a wide variety of existing and developing communication infrastructure such as quantum SSL VPN, quantum-secure encryption routers, optical switching machines and wavelength division multiplexing terminals of quantum channels.

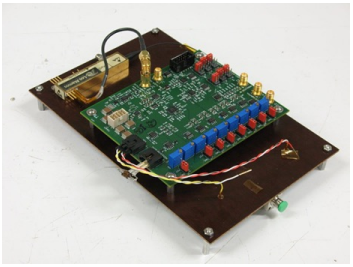
OUR TECHNOLOGY STATUS

Our research comprises a wide variety of quantum enhanced secure communication capabilities at various stages in research, development, demonstration and deployment for potential products. From forward-looking research into post-quantum cryptography to turn-key fully-engineered systems, we have a complete portfolio of science and technologies ready to be applied to commercial applications.

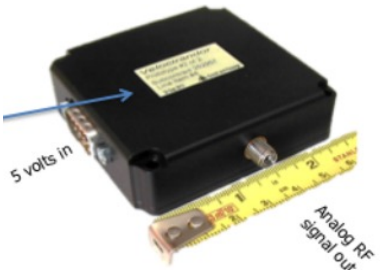
Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is managed by Triad National Security, LLC, for the National Nuclear Security Administration of the U.S. Department of Energy under contract 89233218CNA000001.



Network topography



Quantum state generator



Quantum random number generator

PREFERRED PARTNER ATTRIBUTES

Ample in-house technical expertise in microelectronics, optics, miniaturization, or other engineering disciplines (electrical, mechanical, systems, or aerospace).

Familiarity with communications commerce and US government policy.

Adequate financial and human resources to be dedicated to this commercialization effort.

One or more U.S. executives with whom Triad business personnel may interact.

CRITERIA OF SCORING?

Criteria	Scoring
Technical feasibility (30%)	Highest scoring applicants will provide a comprehensive proposal with a high probability of success, relying on evolvement or deployment of existing and working technologies. Proposals will provide excellent commercial opportunities.
Commercial sustainability (30%)	Highest scoring applicants will demonstrate strong understanding of the current market as well as how their approach will be both commercially sustainable and beneficial.
Benefit to the US (20%)	Highest scoring applicants will provide excellent, detailed evidence of the benefits that the collaboration would enable them to provide to the US economy.
Sound management (20%)	Highest scoring applicants demonstrate an approach to risk and program management that is aligned with industry best practice.

INTERESTED? HERE ARE YOUR NEXT STEPS

Please submit an email letter of interest outlining how your organization envisions using and deploying this innovative technology. Please include background about your organization, relevant information of your ability to commercialize innovative technologies and your access to working capital.

Please respond with "Quantum Enhanced Communications Security" – Commercial Interest – Company Name" in the subject line, to: rossm@lanl.gov

We will acknowledge receipt of each respondent and advise next steps once this commercial call is officially closed. Depending on the responses received additional requirements may be requested including: a commercialization plan, attending a web-based commercialization workshop, or an on-site technical briefing.

APPENDIX A: PUBLICATIONS AND IP

United States Patents & Patent Applications:

U.S. Pat. No. 9,002,009, entitled, “Quantum Key Distribution Using Card, Base Station and Trusted Authority”, issued April 7, 2015 (S118973.002).

U.S. Pat, No. 9,287,994, entitled “Great Circle Solution to Polarization-based Quantum Communication in Optical Fiber”, issued March 15, 2016 (S121591.001).

U.S. Pat. No. 9,509,506, entitled “Quantum Key Management”, issued November 29, 2016 (S121874.001).

U.S. Pat. No. 9,680,640, entitled “Secure Multi-Party Communication with Quantum Key Distribution Managed by Trusted Authority”, issued June 13, 2017 (S133310.000).

U.S. Pat. No. 9,866,379, entitled “Polarization Tracking System for Free-Space Optical Communication, Including Quantum Communication”, issued January 9, 2018 (S121971.001).

U.S. Pat. No. 9,887,976, entitled “Multi-Factor Authentication Using Quantum Communication”, issued February 6, 2018 (S121991.004).

U.S. Pat. No. 9,819,418, entitled “Quantum Communications System With Integrated Photonic Devices”, issued November 14, 2017 (S121997.003).

U.S. Pat. No. 10,044,504, entitled “Long-Haul High Rate Quantum Key Distribution”, issued August 7, 2018 (S133050.001).

U.S. Pat. No. 10,291,399, entitled “Quantum-Secured Communications Overlay for Optical Fiber Communications Networks”, issued May 14, 2019 (S133099.002).

U.S. Pat. No. 10,574,461, entitled “Streaming Authentication and Multi-Level Security for Communications Networks Using Quantum Cryptography”, issued February 25, 2020 (S133131.002).

U.S. Pat. No. 10,587,402, entitled “Long-Haul High Rate Quantum Key Distribution”, issued March 10, 2020 (S133050.003).

U.S. Pat. No. 10,972,189, entitled “Long-Haul High Rate Quantum Key Distribution”, issued April 6, 2021 (S133050.004).

U.S. Pat. Appl. No. 16/700,116, entitled “Streaming Authentication and Multi-Level Security for Communications Networks Using Quantum Cryptography”, filed February 24, 2020 (S133131.003).

APPENDIX A: PUBLICATIONS AND IP

Publication Example:

Evans, Phil, Peterson, Glen, Morgan, Tyler, Jones, Ken, Morrison, Steve, Newell, Raymond, and Peters, Nicholas. Demonstration of a Quantum Key Distribution Trusted Node on an Electric Utility Fiber Network. United States: N. p., 2019. Web. doi:10.1109/IPCon.2019.8908470

Video link：https://www.youtube.com/watch?v=FDNbkr-Nb-o