U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Quantum Physics Secured Communications for the Energy Sector

OAK RIDGE National Laboratory

Overcoming distance limitations and expense of quantum key distribution

This project addresses the distance limitations and expense of quantum key distribution (QKD) and develops new quantum protocols for authentication and data integrity. Continuous variable (CV) QKD is a practical solution for its potential for low cost and its compatibility with existing fiber optic networks. The project team will research repurposing integrated commercial off-the-shelf technology developed in classical coherent optical communications systems and using the same communications system for both QKD and classical communication. The team will determine the cost scalability of an extended national scale link enabled by this project. The QKD distance limitation can be overcome with a trusted node relay approach, which relies on the combination of keys from two QKD links that terminate in a common trusted location. The project will also address the expense of QKD systems by leveraging advances in coherent optical transceivers for communication.

KEY TAKEAWAYS

- Demonstrates quantum approaches to security
- Offers grid cybersecurity rooted in the laws of physics, rather than in computational complexity
- Applies particularly to grid applications, where hardware is designed for decades of service

OUTCOME

This project produces a cost-effective CV-QKD system. It will demonstrate that quantum-grade hardware can operate in energy infrastructure environments while simultaneously relayed, removing the distance limitations of single systems. The result will be a key management server enabling multiplexing so that keys can be established between any two endpoints that have not met but have established trust with the key server.

PARTICIPANTS	ROLE
Oak Ridge National Laboratory	Leads the overall project including the entirety of the CV-QKD thrust; contributing a QKD system and overall control software for the trusted node demonstrations.
Los Alamos National Laboratory EST. 1943	Partners on the trusted node demonstration; contributing a quantum key distribution system and support for a demonstration.
Qubitekk	Partners on the trusted node demonstration; contributing a quantum key distribution system and support for a demonstration.
epb	Provides fiber and engineering support for the trusted node demonstrations.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Nicholas A. Peters
Principal Investigator
Oak Ridge National Laboratory
865-576-3386
petersna@ornl.gov

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: September 2017 – March 2021

Total Award Value: $2,499,844
DOE Share: $2,499,844
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021