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

Quantum Integrated Chip Scale Security (QuICSS)

OAK RIDGE National Laboratory

Reducing costs and increasing applicability of quantum key distribution architecture

Many aspects of modern communications require shared keys as a root of cybersecurity. This project researches, develops, and demonstrates continuous variable quantum key distribution (CV-QKD) technology tailored to the energy grid. CV-QKD is a novel secure communications technology with security based in the laws of quantum physics. As a result, the security of keys distributed by CV-QKD remains intact regardless of advances in technology, giving a long-term security guarantee that exceeds the service life of energy delivery infrastructure. CV-QKD uses attenuated light pulses and homodyne detectors that allows CV-QKD to be deployed alongside classical traffic with little to no penalty, preserving the bulk of a fiber's bandwidth and improving operating costs. The team is expanding on its previous work to develop, implement, and demonstrate new CV-QKD protocols that can be transitioned to an on-chip system. This makes possible the economical manufacturing and widespread adoption of quantum communications cybersecurity solutions.

KEY TAKEAWAYS

- Builds upon previous work in continuous variable quantum key distribution
- Demonstrates on-chip quantum solutions to enable real world implementations of quantum secure communications
- Reduces costs and demonstrates manufacturability of quantum devices

OUTCOME

This project delivers a new CV-QKD protocol that has major implementation advantages for bulk optical fiber infrastructures. This research develops a quantum solution that can be manufactured on photonic chips at large-scale and at low-cost, enabling the seamless integration of quantum-secured communications across the energy sector.

PARTICIPANTS	ROLE
OAK RIDGE National Laboratory	Leads project system design concepts, chip fabrication procurement, testing, and validation.
BYU BRIGHAM YOUNG UNIVERSITY	Leads detailed chip-scale device designs and simulation; participates in chip testing.

CONTACT INFORMATION

Initial Leads:

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

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: October 2020 – September 2023

Total Award Value: $2,000,000
DOE Share: $2,000,000
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