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

Multi-Hop Quantum Networking for Electric Grid Security

Los Alamos NATIONAL LABORATORY EST. 1943

Leveraging advances in quantum technology to optimize security and cyberattack recovery across electric grid infrastructure

This project develops hardware and software solutions to secure quantum communication nodes and implements quantum systems on the links between these nodes. Recent advances in quantum communication systems make use of hardware-based quantum relay nodes across communication infrastructures that extend the distance across which quantum information can be shared. However, installing and maintaining expensive quantum repeaters may be impractical in many instances. This project operationalizes hardware trust anchors at each network node and implements quantum-safe key switching protocols to manage the distribution of quantum-generated secret keys to utility sites, such as control centers and substations. In addition, the project enhances grid resiliency by joining an existing power-flow optimization toolkit with physics-augmented machine learning techniques to enhance recovery following a cyberattack, should one occur outside the quantum-secured portion of the network.

KEY TAKEAWAYS

- Secures quantum communication infrastructures across the electric grid
- Operationalizes efficient and quantum-safe key switching protocols to minimize costs and maximize distances
- Optimizes recovery time after a cyberattack with physics-augmented machine learning

OUTCOME

This project delivers secure, efficient, and scalable quantum networking to the electric grid by improving the security of QKD links and network architecture. This work enhances the architectural security of relay nodes within the QKD network and allows for more efficient cyberattack mitigation and recovery.

PARTICIPANTS	ROLE
Los Alamos NATIONAL LABORATORY EST. 1943	Leads the effort to develop hardware and software solutions for quantum-enhanced grid security. Los Alamos National Laboratory is also its own electric utility; laboratory-owned substations and distribution network are used as a testing and demonstration site.

CONTACT INFORMATION

Initial Leads:

Raymond Newell
Principal Investigator
Los Alamos National Laboratory
505-695-4370
raymond@lanl.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