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

Scalable Quantum Cryptography Network for Protected Automation Communication

Providing quantum key distribution for critical energy infrastructure security

Qubitekk is developing a commercial quantum key distribution (QKD) system using quantum entanglement to detect attempted eavesdropping and safely exchange data and the cryptographic keys used to encrypt operational network communication. Growing networks of grid automation devices create a target for sophisticated attacks that attempt to manipulate or spoof device-to-device communications. QKD uses principles of quantum physics to safeguard cryptographic keys and data as they are exchanged on a fiber optic line, using signals that physically and measurably change if an adversary attempts to intercept the key thereby protecting the ensuing data. Qubitekk is developing low-cost nodes that can integrate into existing devices and communicate with any other nodes on a common QKD channel, unlike the dedicated point-to-point channels required by traditional QKD solutions. The commercial system offers a scalable, cost-effective QKD solution for energy critical infrastructure operational networks, specifically industrial control systems, and integrate with existing commercial hardware.

KEY TAKEAWAYS

- Uses quantum key distribution to exchange keys in traditional encryption algorithms, allowing real-time detection of attempts to intercept communications information
- Enables multi-client communications over a single quantum channel
- Operationalizes a cost-effective solution that combines commercially available point-to-point quantum key distribution systems

OUTCOME

This project operationalizes a commercially viable QKD network using quantum entanglement for the electric grid, providing real-time detection of adversarial attempts to intercept communications information by intercepting the cryptographic keys and is used to prevent unauthorized access to industrial control systems and critical energy infrastructure data.

PARTICIPANTS	ROLE
Qubitekk	Develops quantum entanglement system for quantum key distribution and systems Integration
OAK RIDGE National Laboratory	Science and Research partner providing quantum key distribution expertise
SEL SCHWEITZER ENGINEERING LABORATORIES	Provides ruggedized communications equipment
epb	Host utility; Fiber optics network provider
THE UNIVERSITY OF TENNESSEE KNOXVILLE	Provides quantum state control and manipulation

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Duncan Earl
Principal Investigator
Qubitekk
865-599-5233
dearl@qubitekk.com

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: October 2016 – September 2021

Total Award Value: $4,602,987
DOE Share: $3,102,487
Cost Share: $1,500,000

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: September 2021