U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability

Scalable Quantum Cryptography Network for Protected Automation Communication

Making quantum key distribution (QKD) available to critical energy infrastructure

Background

The power grid is increasingly more reliant on a distributed network of automation components such as phasor measurement units (PMUs) and supervisory control and data acquisition (SCADA) systems, to manage the generation, transmission and distribution of electricity. As the number of deployed components has grown rapidly, so too has the need for accompanying cybersecurity measures that enable the grid to sustain critical functions even during a cyber-attack. To protect against cyber-attacks, many aspects of cybersecurity must be addressed in parallel. However, authentication and encryption of data communication between distributed automation components is of particular importance to ensure resilient energy delivery systems.

Advantages of Quantum Key Distribution

This research is making quantum key distribution (QKD), a key exchange technology grounded in the principles of quantum-physics, available to the energy sector, helping prevent unauthorized access to critical energy infrastructure data. The use of QKD to exchange secret cryptographic keys for use in traditional encryption algorithms, allows for the real-time detection of an adversary's attempt to intercept the key exchange, because any attempt to steal the key as it is communicated between trusted parties, changes the key in an immediate and measurable way, reducing the risk that information thought to be securely encrypted has actually been compromised.

Objectives

In the past, QKD solutions have been limited to point-to-point communications only. To network many devices required dedicated QKD systems to be established between every client on the network. This resulted in an expensive and complex network of multiple QKD links. To achieve multi-client communications over a single quantum channel, Oak Ridge National Laboratory (ORNL) developed a cost-effective solution that combined commercial point-to-point QKD systems with a new, innovative add-on technology called Accessible QKD for Cost-Effective Secret Sharing (AQCESS) nodes. AQCESS nodes are low-cost modules that modulate the quantum signal being propagated in a commercial QKD channel. Multiple AQCESS nodes can utilize the same common QKD channel, allowing any one node to communicate with any other node on the channel. Because the nodes are relatively simple—having no quantum source or detection devices—they have the potential to be low-cost and can be integrated into existing products. This research aims to make QKD a near-term solution to help secure critical energy infrastructure data from unauthorized access.

Benefits

- QKD lets the operator know, in real-time, if a secret key has been stolen
- Reduces the risk that a "man-in-the-middle" cyber-attack might allow unauthorized access to energy sector data

Partners

- Qubitekk, Inc. (lead)
- Oak Ridge National Laboratory (ORNL)
- Schweitzer Engineering Laboratories
- EPB
- University of Tennessee

Period of Performance

October 2016 – September 2019

Total Project Cost

Total: $4,612,000

Federal: $3,112,000

Cost Share: $1,137,319

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) research and development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber-attacks.

Contact Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Duncan Earl
Principal Investigator
Qubitekk, Inc.
(865) 599-5233
dearl@qubitekk.com

For More Information:

- http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity
- www.controlsystemsroadmap.net

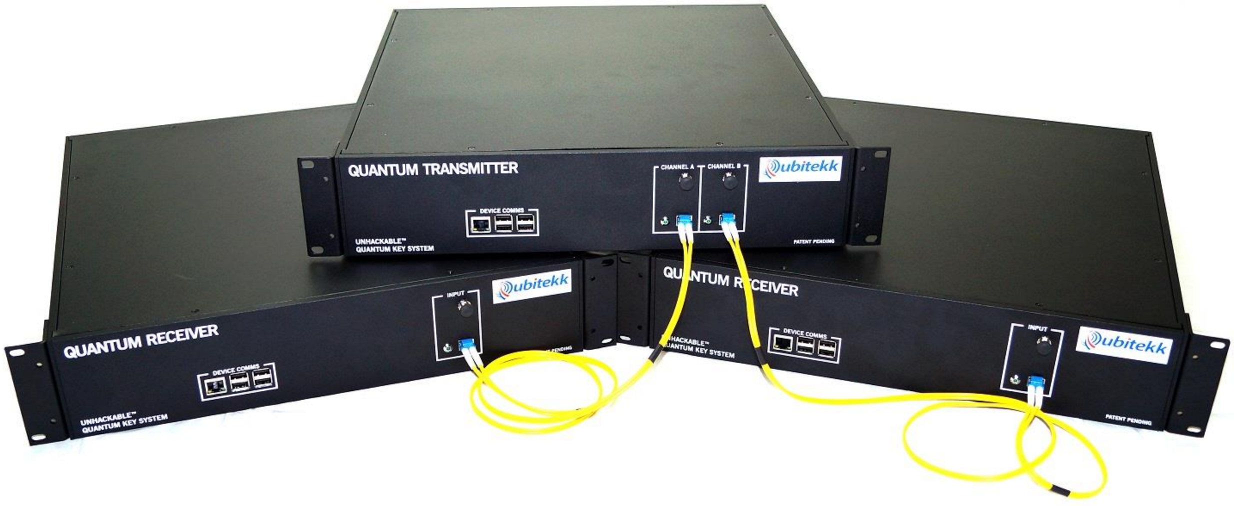

Figure 1: Commercial Quantum Key Distribution System - 1 Quantum Transmitter (middle), 2 Quantum Receivers (Left/Right)

Project Description

The proposed technology will help secure communications between deployed automation equipment critical to the operation of the electrical grid.

The industry-led team will utilize capabilities from quantum product developers, automation equipment vendors, utilities, national laboratories, and academia to develop the proposed technology, which will be integrated with commercial automation equipment. The team will deploy the technology on an operational grid where its interoperability, security features, and commercial viability will be demonstrated in a working controlled grid environment.

Tasks

The project team will develop and demonstrate a quantum encrypted network. By integrating newly developed entanglement-based QKD products, 2xN fiber optic switches, and automation devices equipped with enhanced AQCESS nodes, the developed network will provide a scalable method of authentication and data protection that is more secure against eavesdropping attacks.

Phase 1: R&D of a commercially-viable, prototype quantum network

The team will review the design of the proof-of-principle AQCESS nodes, and develop firmware to fully integrate the QKD system, the AQCESS nodes, and third-party automation equipment.

Phase 2: System deployment and field testing

Twenty automation devices—equipped with integrated pre-commercial AQCESS nodes—will be deployed with a compatible pre-commercial QKD system. Testing will include the measurement of system performance metrics.

Anticipated Results

Project results will include the following:

- Commercially-viable quantum key distribution network for the electrical grid that provides long-term security and meets minimum performance requirements necessary for grid automation.
- Affordable, long-term security to a large number of distributed power system devices.
- Real-time detection of adversarial attempts to steal the cryptographic keys needed to prevent unauthorized access to critical energy infrastructure data