Practical Quantum Security for Grid Automation

Minimize cost and increase security by enabling a grid-compatible, long-term QKD solution for guaranteed secure communications

Background

The U.S. electric grid relies on energy delivery control systems to manage the generation, transmission and distribution of electricity. Encryption of data communicated within these systems is of particular importance, as adversaries employ increasingly sophisticated methods to infiltrate control systems by exploiting flaws in software and grid communication protocols.

Ideally, encryption solutions should remain effective for the life of the grid, even in the face of continuous improvements in attacker hardware and computational abilities. Quantum Key Distribution (QKD) uses principles of quantum physics to securely exchange cryptographic keys that can then be used by traditional cryptographic algorithms to secure communications between the sender and receiver of the keys. One significant benefit of QKD is that, unless known laws of physics are violated, attempted adversarial interception of the key exchange will always be evident.

Barriers

- Limited "shelf-life" of currently deployed encryption methods, which are vulnerable to near-term improvements in computational power.
- Computationally weak keys that represent a single point of failure can compromise grid security.
- Traditional QKD system limitation of only point-to-point or single-client communications.

Project Description

The grid requires multiple energy delivery system devices to communicate over a single encrypted channel. Oak Ridge National Laboratory has developed a solution based on an enhancement to traditional QKD systems. The upgrade allows for multiple clients to communicate over a single quantum channel using low-cost quantum modulators, called AQCESS (**A**ccessible **Q**KD for **C**ost-**E**ffective **S**ecret **S**haring) nodes.

Multiple AQCESS nodes can utilize a common QKD channel, allowing any one node to communicate with any other node on the channel. The nodes can also be made compatible with existing grid communication protocols for seamless integration with existing grid components.

This project will research, develop and demonstrate an innovative QKD solution with long-term security for grid components. In collaboration with partners, this new technology will be integrated into commercial grid components and will be deployed within an operational grid application where its security performance will be characterized.

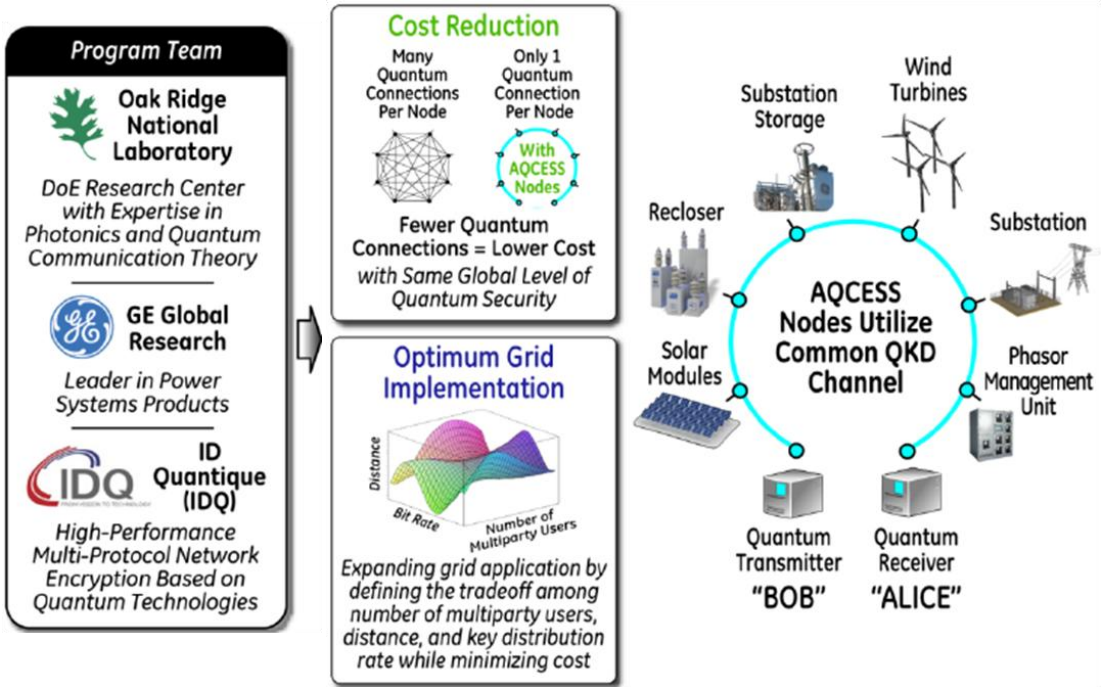
Benefits

- Unbreakable encryption for grid components
- Reduced cost and complexity to implement quantum key distribution
- Elimination of significant security threats for the life of grid
- Physical tamper detection of communication lines

Partners

- Oak Ridge National Laboratory
- GE Global Research
- ID Quantique

Project Overview



Technical Objectives

The project consists of research, development and demonstration efforts that will produce an economical, near-term realization of QKD for grid components.

Phase 1: Proof of Principle

- Design and develop proof-of-principle AQCESS node.
- Study tradeoffs between the number of AQCESS nodes, total fiber length, and maximum transmission length.
- Identify energy delivery system components and applications best suited to integrate with the technology.

Phase 2: Prototype

- Develop and integrate a prototype with the best-suited component or application.
- Validate performance of multi-client communication over a bench-top QKD system.
- Modify existing commercial QKD system to enable communication with the AQCESS node.

Phase 3: Demonstration

- Prepare equipment and a detailed test plan for measuring and validating system performance.
- Install and test the technology in a power grid application and test bed.

End Results

The project will produce:

- An economical QKD solution for the energy sector capable of multi-point communications along a common channel
- Technology that enables long-term security of communications for grid components

Content last updated: September 2013

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) 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 emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Warren Grice
Principal Investigator
Oak Ridge National Laboratory
865-241-2061
gricew@ornl.gov

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov