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

Time-Sensitive Quantum Key Distribution (TSQKD)

GE Global Research

Improves the integrity and availability of grid communications without introducing complexity

This project develops an easy-to-adopt, quantum-protected, time-sensitive network (TSN) solution to secure operational technology communications against quantum computing attacks. This increases the availability and integrity of cybersecurity for industrial control systems in the power industry. TSN protects scheduled flows against denial-of-service attacks and can configure redundant paths. Quantum key distribution (QKD) protects data using a hash-based message authentication code that mitigates modification attacks. TSN and QKD are synergistic: TSN simplifies timing correlations in QKD systems and QKD eliminates security vulnerabilities in TSN. A measurement device-independent (MDI) QKD photonic integrated circuit has been designed for enabling QKD to be integrated directly into intelligent electronic devices for decreased cost and improved security and performance.

KEY TAKEAWAYS

- Implements a time-sensitive networking solution protected by quantum key distribution to detect man-in-the-middle attacks in real time
- Enhances availability of operations technology communications by using synchronized traffic flows to mitigate denial-of-service attacks while providing deterministic network control
- Enables remote management, diagnostic, and repair features for grid network and edge devices
- Develops a measurement device-independent quantum key distribution photonic integrated circuit that integrates quantum key distribution with network and edge devices reducing cost and increasing security and performance

OUTCOME

TSQKD is more secure, efficient, and scalable than either TSN or QKD used independently. Industrial control messages are scheduled with extreme precision and are protected against any attack, including a quantum computing attack. TSQKD ensures the integrity and availability of communications to the electric grid, even in the event of compromised devices. Expanding the reliability of QKD also eliminates key maintenance and reliance on third-party certificate authorities.

PARTICIPANTS	ROLE
GE Global Research	Time-sensitive networking for secure deterministic control of power grid using quantum key distribution; designs quantum key distribution photonic integrated chip.
Qubitekk	Provides bulk optic quantum key distribution
MITRE	Red team for the project
epb	Provides field test and demonstration

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Stephen Bush
Principal Investigator
GE Global Research
518-387-6827
bushsf@research.ge.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 2018 – December 2021

Total Award Value: $3,932,157
DOE Share: $2,864,189
Cost Share: $1,067,968

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