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

Low-Cost, Scalable and Practical Post Quantum Key Distribution

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Computationally secure resilience for America's critical infrastructure

Quantum computing promises game changing technological advances, but also threatens to break most existing encryption techniques. While quantum key distribution (QKD) can provide high security based on the laws of physics, scalability issues hinder its wide adoption. This project helps physical QKD scale, significantly reducing deployment and infrastructure costs. The research team is developing an efficient and authenticated computationally secure QKD (CQKD) network to distribute QKD-generated keys via traditional infrastructure. The team will operationalize a CQKD network for EDS security to distribute post-quantum keys via highly secure hash-based signatures that are resilient to quantum man-in-the-middle attacks. CQKD offers a post-quantum communication backbone that can cover a vast majority of critical EDS infrastructure without the need of expensive QKD hardware and costly dedicated fiber optic deployments. As a result, only a fraction of EDS infrastructure will need QKD, while the rest of the infrastructure will be protected with CQKD.

KEY TAKEAWAYS

- Develops a computationally secure encryption methodology to operationalize quantum-secure solutions across pre-existing critical infrastructure
- Overcomes significant barriers to scalable quantum key distribution
- Offers a cost effective and rapidly deployable solution for enhancing smart grid security

OUTCOME

This project advances network resiliency, offering low-cost, rapidly deployable CQKD to EDS networks. It will help overcome the financial and infrastructural hurdles associated with manual symmetric key distribution that have kept operators from deploying post-quantum security across critical infrastructure in the U.S.

PARTICIPANTS	ROLE
CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM	The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts.
Oregon State University	Leads research, development, and testing
OAK RIDGE National Laboratory	Engages in discussions as complementary CEDS performer in QKD
Los Alamos NATIONAL LABORATORY EST. 1943	Engages in discussions as complementary CEDS performer in QKD

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Attila Yavuz
Assistant Professor
University of South Florida
813-974-0419
attilaayavuz@usf.edu

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

This is a subproject sponsored by the CREDC academic consortium, led by the University of Illinois.

CREDC Period of Performance: October 2015 – May 2022

CREDC Total Award Value: $28,099,258
DOE Share: $22,476,290
Cost Share: $5,622,968

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