Low-cost, Scalable and Practical Post Quantum Key Distribution Infrastructure for EDS

Rouzbeh Behnia, Attila A. Yavuz, Oregon State University {behniar,attila.yavuz}@oregonstate.edu)

GOALS

- **Authentication** and **integrity of control/measurement** data is **vital** for the **reliable operation of energy distribution systems**.
- Post-Quantum (PQ) computers will render existing cryptographic systems insecure

- **Develop efficient PQ secure key exchange systems**
  - Efficient: can be deployed in low-end PMUs
  - Cheap to deploy as compared with physically secure key distribution
  - No additional infrastructure needed

FUNDAMENTAL QUESTIONS/CHALLENGES

- **Critical vulnerabilities for smart-grids:**
  - False data injection attacks
  - Tampering commands
  - Cascade failures

- **PQ secure key exchange is vital**
  - Twenty nations are competing to win the quantum future
  - Conventional Crypto (e.g., RSA) will be broken!

- **Existing post-quantum secure methods are NOT enough**
  - **Extremely Expensive:** $\geq \$70k$ per device
  - **Require Fiber Optic Infrastructure:** Very expensive to deploy/maintain nationwide

+ Security is based on fundamental laws in physics
+ Unconditionally secure against eavesdroppers
- Expensive devices on each end | - Range < 100 KM
- Need of costly infrastructure | - Maintenance cost
- Not deployable on peripheral devices

RESEARCH PLAN

- **Design and Implement an efficient Computationally secure post-quantum key distribution**

- Security is based on computational problems
- Need to store a few Kb of keys on end machines
+ No need for additional hardware
+ No additional infrastructure is needed
+ Minimal maintenance cost
+ Deployable on low-end embedded devices
+ Can be bootstrapped with minimal usage of QKDs

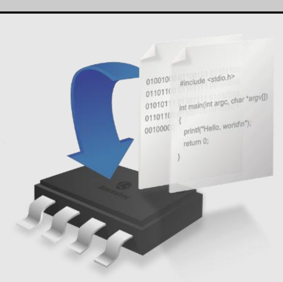
Thrust I – Phase 1:
Goal:
Identify Efficient CQKD Schemes

Thrust I – Phase 2:
Goal:
Develop the selected CQKDs
Evaluate parameters & Security

Thrust II – Phase 1:
Goal:
Optimize the realization of CQKDs
Harness efficient libraries
Employ commodity hardware (e.g., GPU)

Thrust II – Phase 2:
Goal:
Bootstrap CQKD with minimal usage of QKD

Thrust III
Goal:
Implement on embedded systems

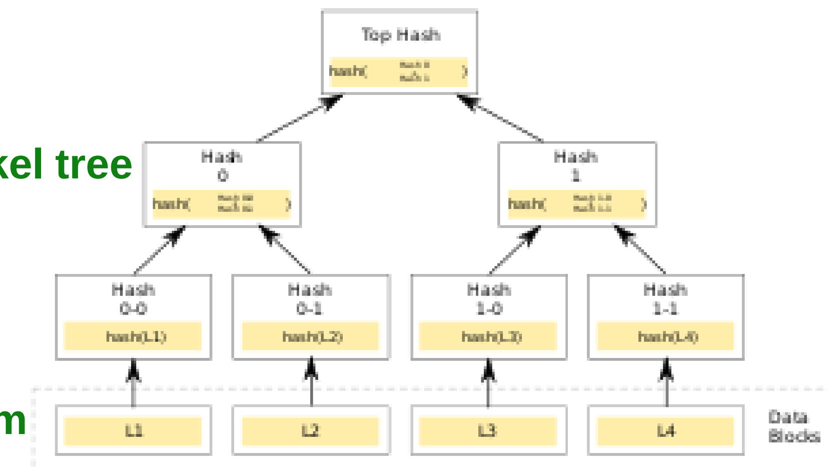


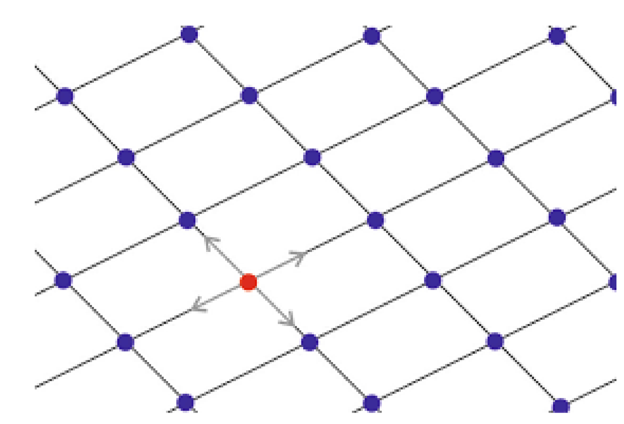
RESEARCH RESULTS

Observation I: Lattice-Based Schemes for the Most Efficient Solution

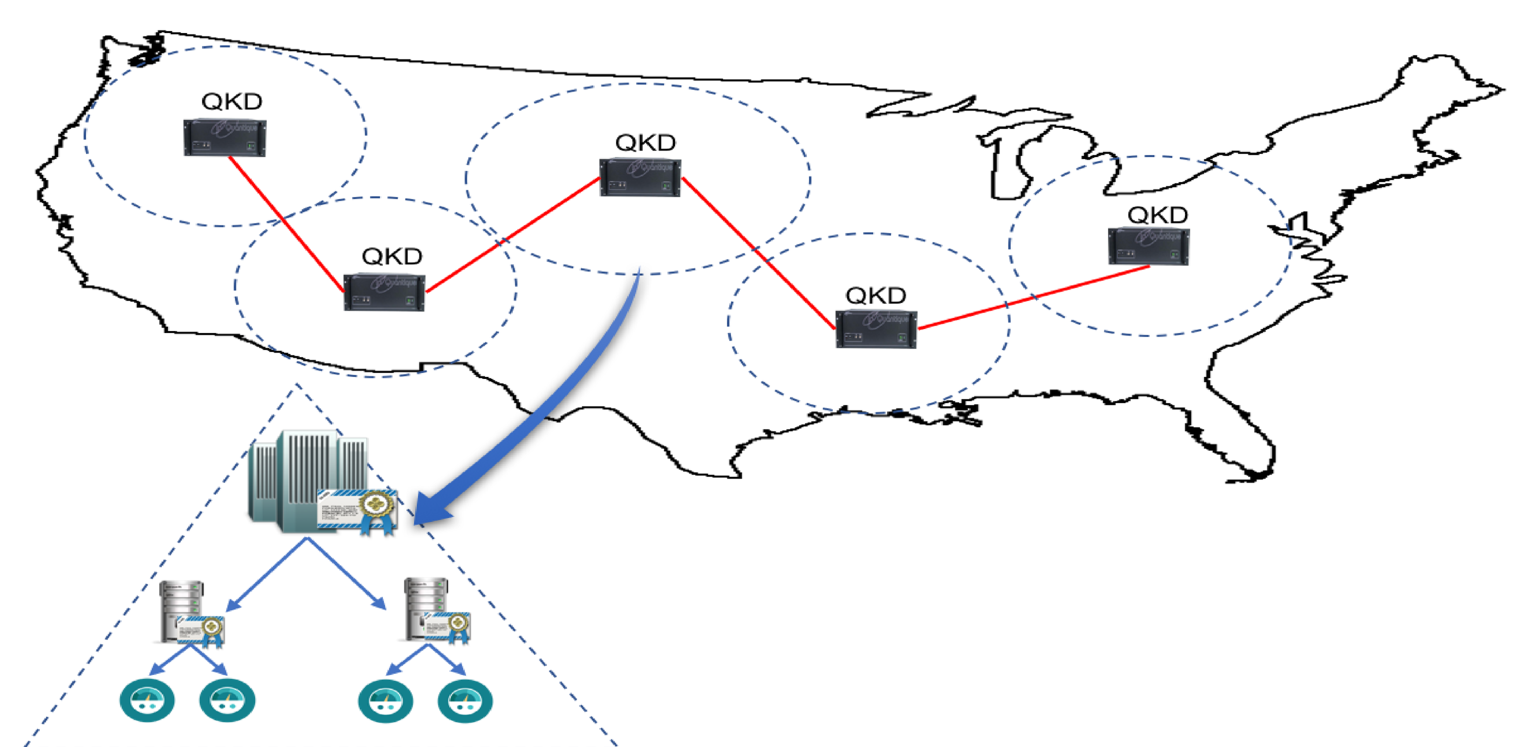
- **Kyber**, a lattice-based KEM scheme that performs both encapsulation and decapsulation of keys in only $38\mu s$
- For authentication, we considered schemes based on three primitives.

  - **Hash-based signatures:**
    - **Highly Secure**
    - **Based on hash functions and Merkel tree**
    - **Very large parameter sizes**
    - **Slow signing**
  - **Code-based signatures:**
    - **Based on the Fiat-Shamir transform**
    - **Very large key sizes**
    - **Slow signing**
  - **Lattice-based scheme:**
    - **Smaller key sizes**
    - **Efficient sign and verification**
    - **Worst case to average case reduction**





Observation II: Bootstrapping with highly secure key distribution devices (QKD) at the main command centers is possible to boost the security



CQKD Infrastructure

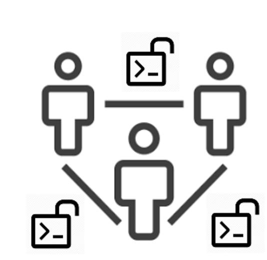
IMPACT ON STATE OF GRID SECURITY

- **Security against quantum computing capable adversaries**
  - The proposed system will offer confidentiality and authentication services for energy delivery systems against quantum computers.
- **Efficient and low cost key distribution**
  - The proposed system can be accommodated on low-end devices and sensors along with power stations.
- **Achieve high security with minimum infrastructure cost**
  - The new system can be deployed widely without requiring extensive use of physical post-quantum key distribution hardware, and can be bootstrapped by such hardware.

BROADER IMPACT

Post-quantum public key infrastructure

Open-source cryptographic framework



Broad applicability to other domains with time-critical needs

IoT Devices

COLLABORATION OPPORTUNITIES

- Collaboration and support from the industry can have the following impacts on this research:
  - The test and benchmark the system on simulated grids and testbeds to achieve **full-fledge practicality assessment and deployment**
  - Encourage the **broader adoption** of the system on IoT devices and systems that require long-term security

Contact: attila.yavuz@oregonstate.edu

- Activity webpage: https://cred-c.org/researchactivity/low-cost-scalable-and-practical-post-quantum-key-distribution

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG
FUNDING SUPPORTPROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY