U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Trustworthy Relay Node Networking
Los Alamos National Laboratory (LANL)

Alia Long

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

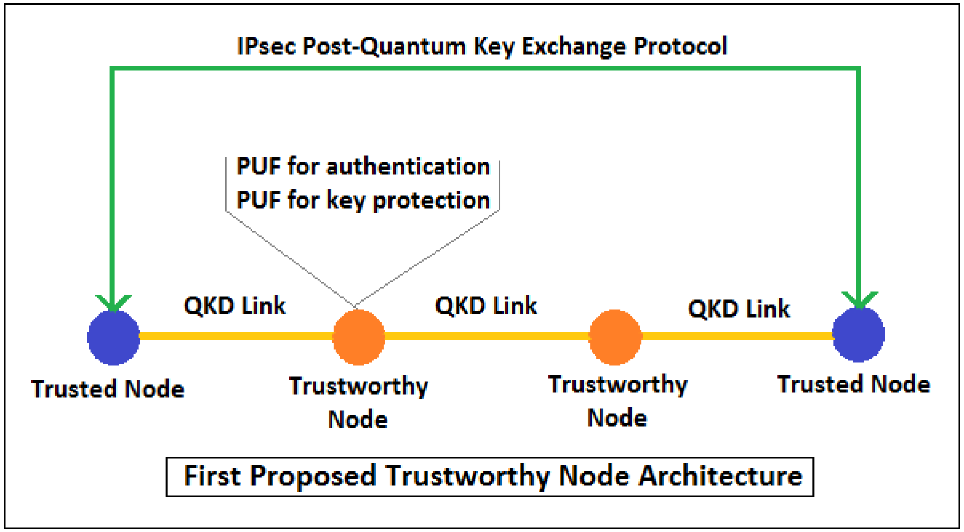
Summary: Trustworthy Relay Node

Objective

- Existing quantum links are limited in range to ~100 miles, extending the distance for Quantum Key Distribution (QKD) requires trusted nodes with physical security.
- Design a trustworthy relay node to securely extend distance and flexibility of QKD use without operator supervision.

Schedule

- January 2018/September 2020
- QC Requirements doc.-Delayed
- Framework Architecture-10/2018
- A trustworthy relay node for QKD creates the possibility for long-term, physically secure infrastructure communications.



Total Value of Award:	**$ 1,500,000**
Funds Expended to Date:	**20.9%**
Performer:	**Los Alamos National Laboratory**
Partners:	**Oak Ridge National Laboratory, EPB, Qubitekk Inc.**

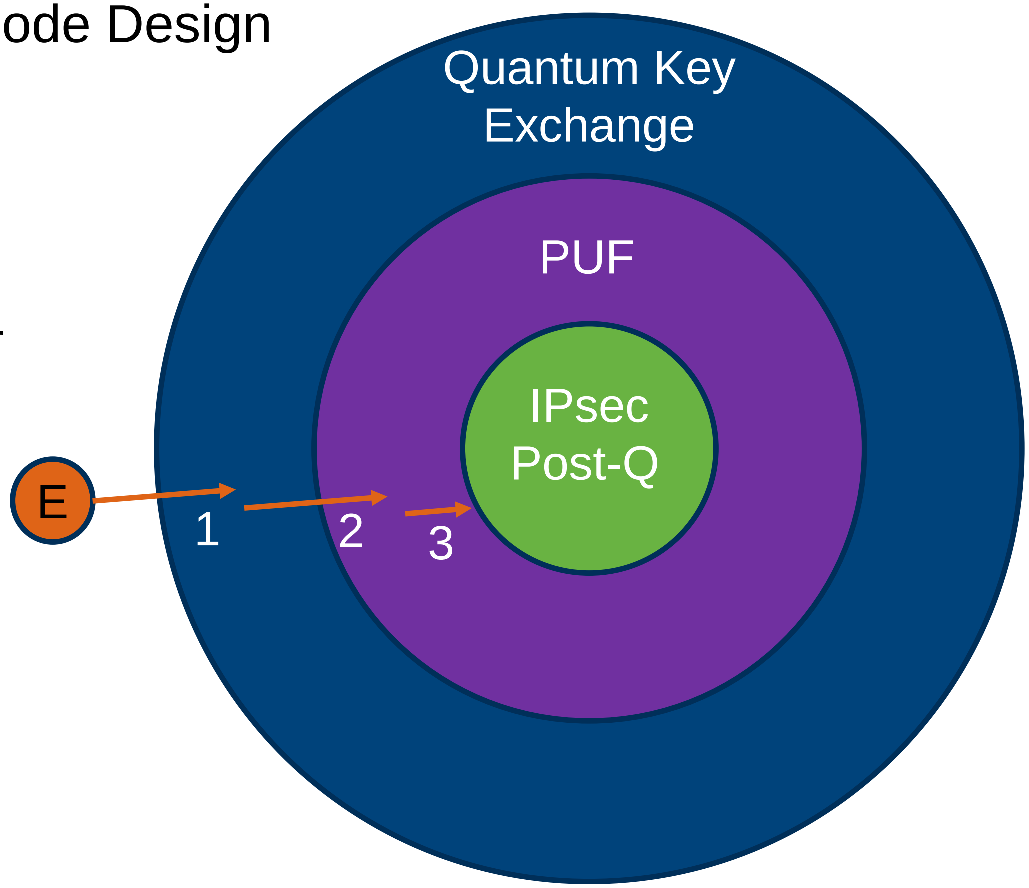
Advancing the State of the Art (SOA)

- Energy Grid communications are unencrypted or at best PKI. Forward development for secure communications must work toward the next level of secure architecture.
- In unencrypted communications, command and control of SCADA systems, distributed across regions and even countries, is openly available for a man-in-the-middle attack. Methods exist for breaking encrypted data and authentication is weak.
- QKD is resistant to a man-in-the-middle attack, except for the weak points at nodes when the message must be unencrypted and re-encrypted with a second key for the next leg.
- QKD technology is developed and tested enough to begin R&D for application. Fiber lines are used for communication in many grids, infrastructure which can also be used for QKD.

Advancing the State of the Art (SOA)

Defense in Depth Approach to Node Design

1) Eve must break through physical barrier at relay node to get link key.
2) Eve must break through physical unclonable function (PUF) barrier to access link key.
   - Prior Post-Q initiation, need (different) PUF authentication to complete link with stolen key.
   - Must also authenticate with a remote node to establish communication channel.
   - After IPsec Post-Q initiation, key is never available at relay node.
3) Post-Q theoretically not breakable with even a quantum computer.



U.S. DEPARTMENT OF ENERGY | OFFICE OF CYBERSECURITY, ENERGY SECURITY, AND EMERGENCY RESPONSE

Challenges to Success

Challenge 1) Determine parameter space that satisfies security needs and the computation & bandwidth requirements of the application.

- Risk Mitigation: If computation / bandwidth needs to be reduced we can switch to Ring LWE which is more complicated but allows for significantly smaller keys.

Challenge 2) Current approach requires all secret keys to be refreshed at the same time.

- Risk Mitigation - develop strategies for secrets to be generated continuously into protected buffers on nodes.

Challenge 3) Current approach requires secret keys to be present on relay nodes for short periods of time.

- Risk Mitigation: PUF protected computation space.

Challenge 4) Silicon PUF may not be reliable in severe environmental conditions

- Risk Mitigation: Have not found a reason that proper shielding and PUF design/implementations cannot overcome this. Preparing to test research findings. Also looking into PUF implementations which are not susceptible to environmental influence.

Progress to Date

- Survey of SOA for requirements document.
- Meeting with ORNL, Qubitekk, EPB to decide on test architecture.
- Research on PUF technology and applications
- PUF on FPGA implementation
- Research on Post-Quantum Cryptography
- Implementation of Learning with Errors Encryption and Homomorphic Computation, including Key Switching
- Calculations of computational complexity
- Research into side-channel attacks.

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Prototype demonstration in lab on 6/2020
- Prototype demonstration in Partner facility 9/2020
- Final report of findings 9/2020
- Conference and Journal papers for peer review as relevant.

Next Steps for this Project

- Test a multi-node implementation of key switching, LWE algorithm, determine if we will use existing software and modify to our needs or continue to develop our test software.
- Determine metrics needed for timing, bandwidth, computation, and security with LWE.
- Investigate LWE implementation on an FPGA
- Test FPGA PUF reliability in controlled and stressed environmental conditions. Observe the effect of proper shielding.

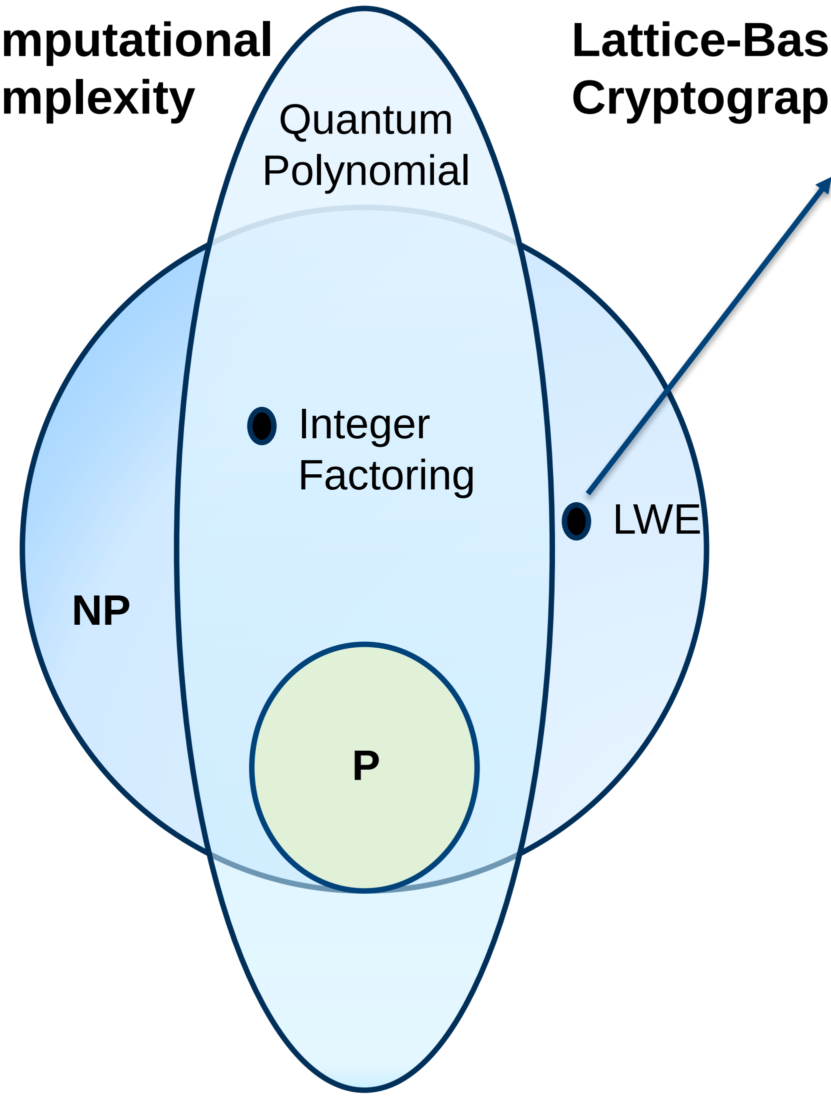
$$\mathbb{R} = \left(\frac{1}{x}\sum_{y-1}^{x}\frac{HD\ (Ri,R'i,y)}{n} \text{ X } 100\%\right) \approx 0\%$$

(A measure of Hamming distance between intra-chip PUF responses)

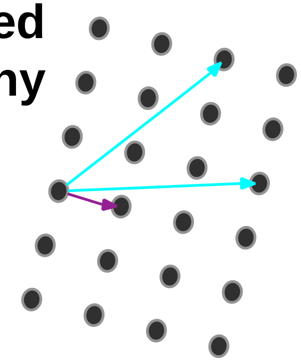
- Integrate PUF with LWE implementation.
- Research quantum technology for authentication.

Post-Quantum Cryptography

Computational Complexity



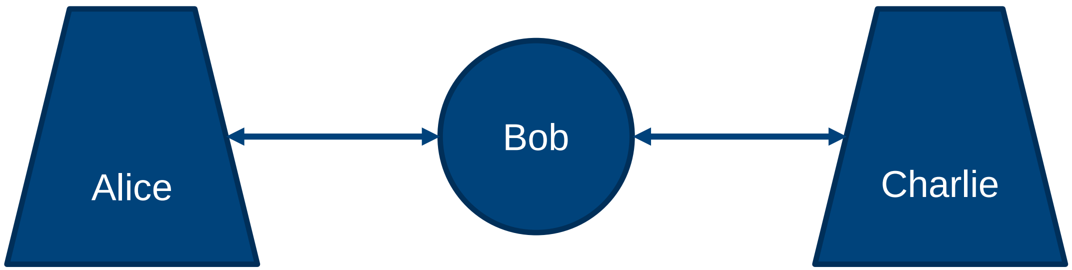
Lattice-Based Cryptography



Given the input vectors (turquoise), determine the shortest lattice vector (plum)

- Learning with Errors (LWE) a Lattice-Based Cryptographic Algorithm with which we have implemented a key switching algorithm.
- Introduced 13 years ago, this is the most used post-Q cryptographic primitive.
- A modification of this, Ring-LWE, uses a smaller key size and has OpenSource IPsec-based implementation, StrongSwan

Key Switching



<u>Setup: Key Generation</u>

- Alice and Bob generate secret key s_1
- Bob and Charlie generate secret key s_2
- Bob generates key switching transforms T and U and **deletes s_1 and s_2**

<u>Message Sending: Encryption and Decryption</u>

- Alice encrypts message m under key s resulting in c_1
- Alice sends Bob the cipher c_1
- Bob performs the transform **T** to c_1 achieving c_2
- Bob sends the new cipher c_2 to Charlie

The transforms T, U reveal no information about s_1 and s_2 and cannot be used for decryption.