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

Quantum Physics Secured Communications for the Energy Sector

Oak Ridge National Laboratory (ORNL)

Nicholas A. Peters

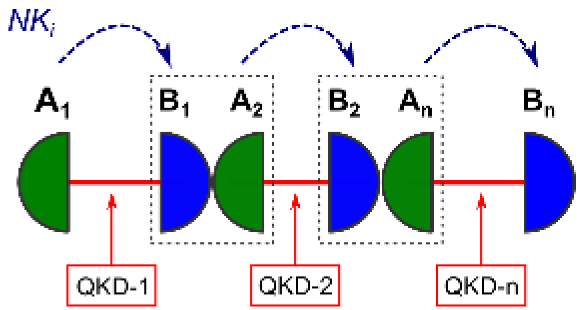
Cybersecurity for Energy Delivery Systems Peer Review

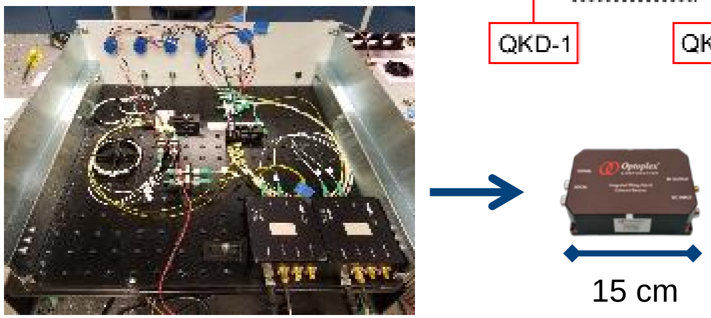
November 6-8, 2018

Summary: Quantum Physics Secured Communications for the Energy Sector

Objective

- Decrease cost (Bing Qi), and increase distance (Phil Evans), of Quantum Key Distribution systems that enable real-time detection of adversarial intrusion on control system networks.





Schedule

- **12/05/17-09/30/2020**
- Engage utility and supplier industry partners
- Utility site selected for Y1 demo
- Demonstration at a utility of a trusted node relay between two different types of QKD

Total Value of Award:	**$2,098,640**
Funds Expended to Date:	**23%**
Performer:	**ORNL**
Partners:	**LANL, Electric Power Board of Chattanooga (EPB), Optoplex**

Advancing the State of the Art (SOA)

- **QKD is distance-limited: optical channel loss exponentially reduces secret key rate.**
  - Quantum repeaters are proposed fix but are far away.
- **SOA: Trusted-node QKD extends the distance**
  - Implemented in various research demonstrations
  - Never implemented on an energy grid
- **QKD backbone network (e.g., power transmission)**
  - Delivers keys for authentication and other security tasks
  - Can build more complex local area networks (e.g., power distribution [EPB]).

Advancing the State of the Art (SOA) II—CV-QKD

- **CV-QKD implemented with "classical devices" (lasers and homodyne detectors)**
  - Potentially cost-effective: CV-QKD is resilient against background noise
  - SOA CV-QKD uses specially designed, "home-made" devices → not suitable for large-scale applications
- **Our approach: leverage commercial optical coherent communications system for CV-QKD**
  - If successful, commercial coherent communications system could operate in either a classical or quantum communications mode
- **Feasibility: quantum and classical coherent communication systems are similar but optimized differently**
  - The classical detectors approach the quantum noise limit
  - Classical system has less stringent requirements than quantum system
- **Output: a cost-effective building block for constructing semi-trusted QKD network, which can provide long-term security for energy delivery systems.**

Challenges to Success

Challenge 1: Dark fiber is a start, but there are other requirements

- Collaborate with network engineers to realize quantum link layer

Challenge 2: Disparate QKD systems: operating conditions, key rate, wavelength, etc.,

- Develop QKD-agnostic software layer to handle all key transactions

Challenge 3*: Existing commercial coherent receiver needs improvements to become "quantum grade"*

- We are working with a commercial vendor (Optoplex) to develop a compact, low-noise conjugate homodyne detector based on their existing product

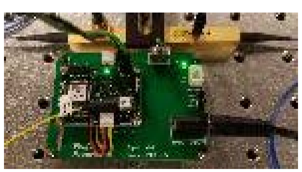
Challenge 4*:* Existing commercial coherent transmitter does not support CV-QKD modulation format

- We are developing a passive CV-QKD scheme with no active modulation.

Progress to Date

Major Accomplishments

- TN software demo using hop-by-hop technique
  - Implemented on laptops, moving to Raspberry-pi and MOXA hardware
- Partnership with EPB (subcontract in process)
- Joint ORNL & LANL demo plan for late 2018-early 2019 at EPB



- Collaboration with Optoplex resulted in a compact receiver for CV-QKD.
  - Purchase order issued.
- High-speed FPGA ADC/DAC devices acquired for system control and measurement.
  - Associated software developed
- Automatic bias control for intensity modulator demonstrated.

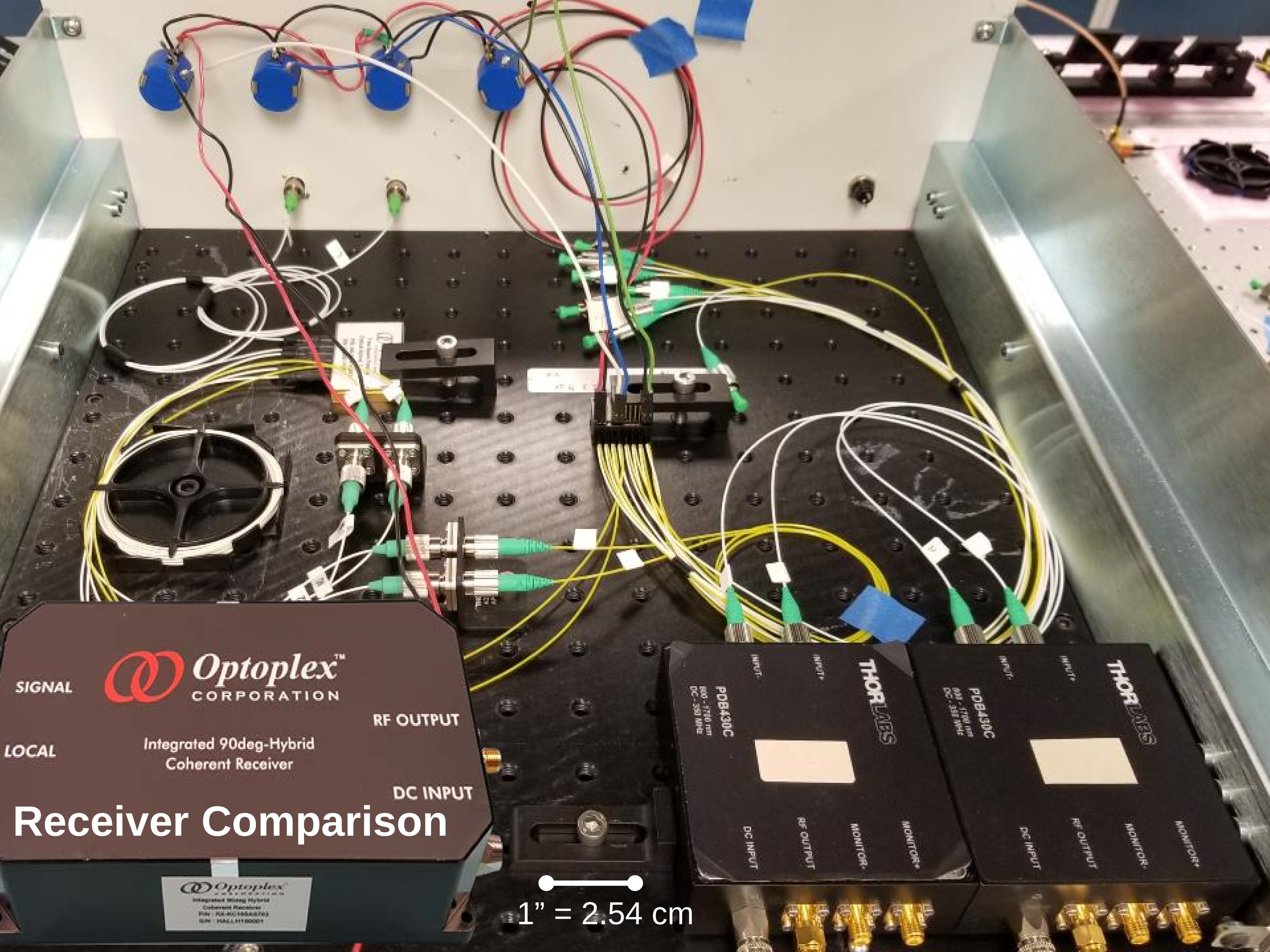
Collaboration/Technology Transfer

- Transferred CV-QKD receiver knowledge to Optoplex (Vendor)
- Transferred quantum-link layer requirements to EPB (electric utility and fiber optic network operator)
- Test plans to gain industry acceptance:
  - 12 months: Trusted node relay demonstration at a utility between two different types of QKD (interoperability)
  - 22 months: Demonstration of end-to-end key generation across two trusted nodes (three QKD systems)
  - 24 months: Trusted node relay demonstration at a utility yielding a higher secret bit rate than a single QKD system over the same distance
  - 36 months: Demonstration of end-to-end key generation across four trusted nodes (five QKD systems) at a partner utility site
  - 36 months: Demonstrations of CV-QKD and raw-key based authentication scheme at a partner utility site

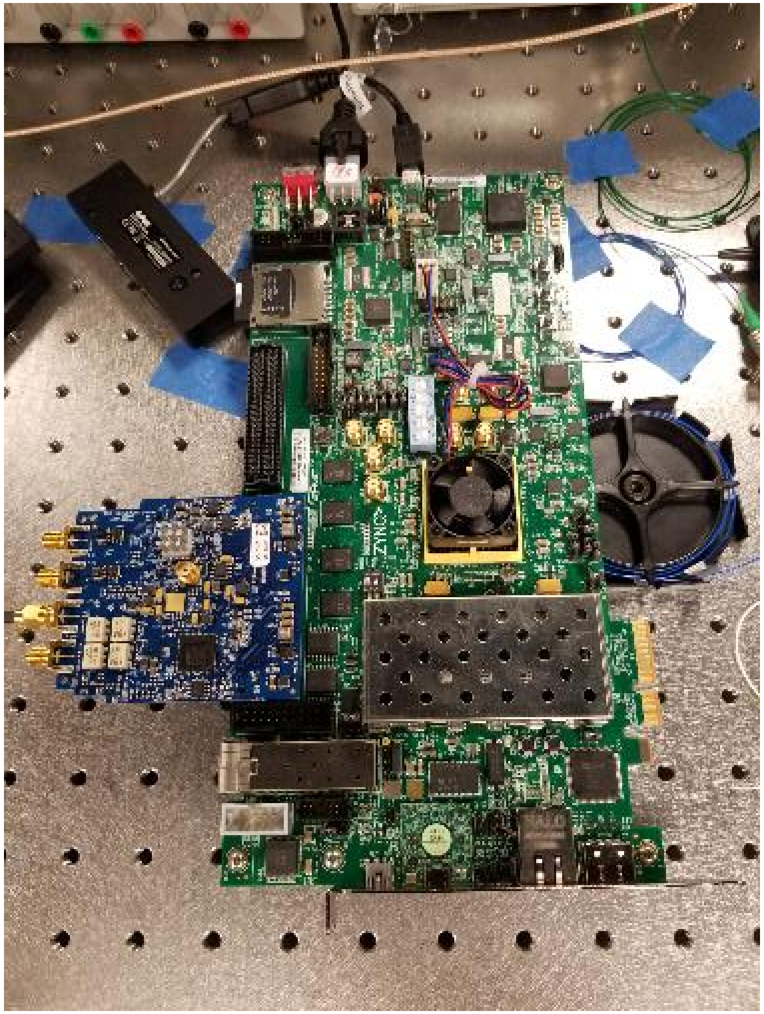
Next Steps for this Project

Approach for the next year

- Demonstrate trusted relays at increasing levels of complexity
- Experimental confirmation of Optoplex “quantum grade” receiver performance leading to construction of cost-effective coherent communication system to demonstrate classical communication and CV-QKD on same hardware
- Feasibility study of chip-size integration of CV-QKD
- Explore authentication protocols using shared imperfect randomness (rather than secure key)


Receiver Comparison
1” = 2.54 cm
Optoplex
CORPORATION
SIGNAL
LOCAL
RF OUTPUT
DC INPUT
Integrated 90deg-Hybrid
Coherent Receiver
THORLABS
PDB430C
INPUT-
INPUT+
DC INPUT
RF OUTPUT
MONITOR-
MONITOR+

Alice (Transmit) and Bob (Receive) Electronics



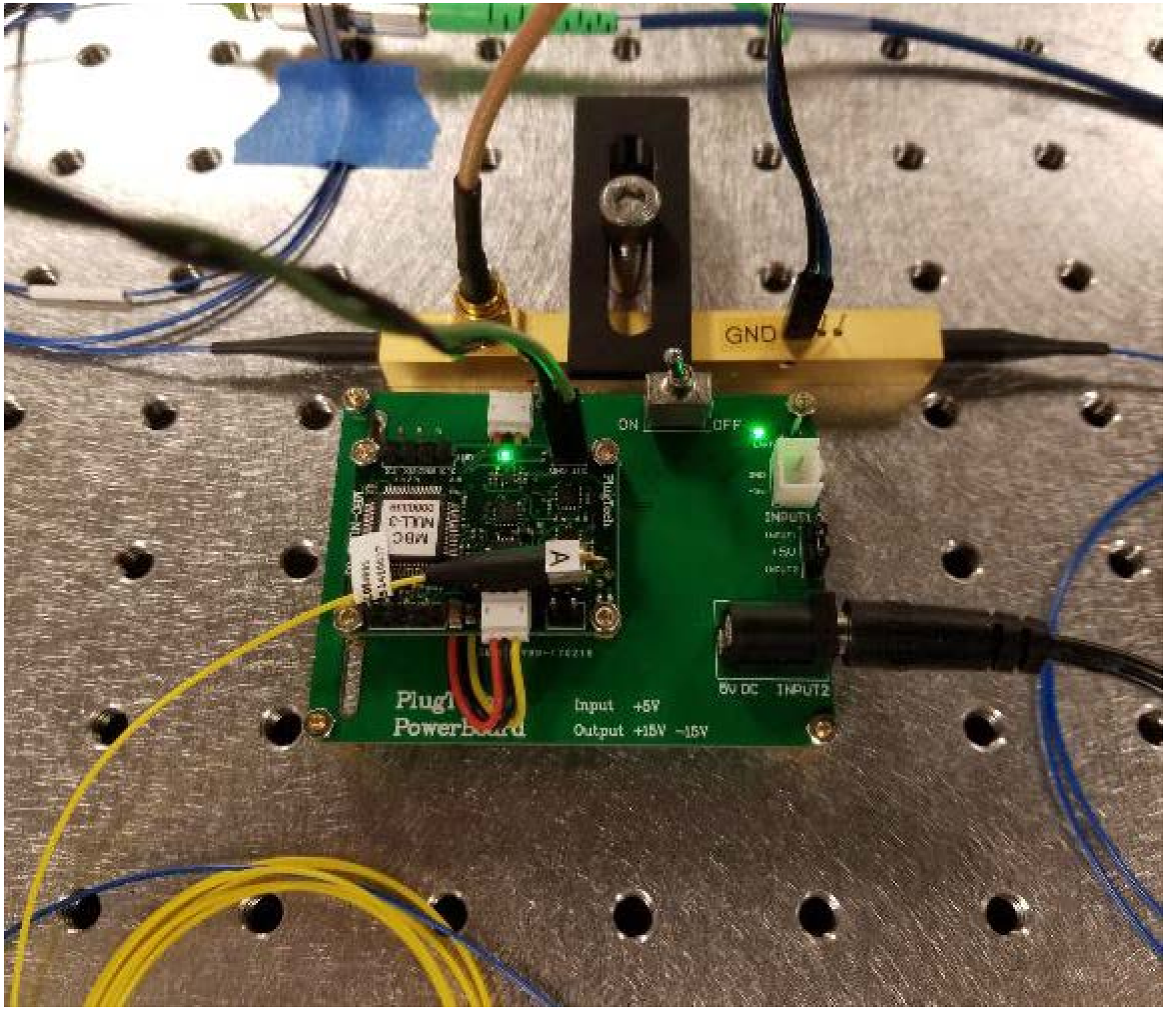
Alice's electronics:

- Sample the random noise from a quantum random number generator
- Transform the random noise into Gaussian random numbers
- Calculate amplitude and phase modulation voltages corresponding to random numbers
- Output the modulator drive signals

Bob's electronics:

- Sample the conjugate homodyne detector
- Perform data processing including synchronization and quadrature value calculation
- Implement polarization feedback control

Modulator Bias Controller



Provides a control voltage to compensate modulator bias-point drifts.

Two are needed at Alice's side to maximize the extinction ratio in pulse generation and amplitude modulation.