Raymond Newell

Los Alamos National Laboratory

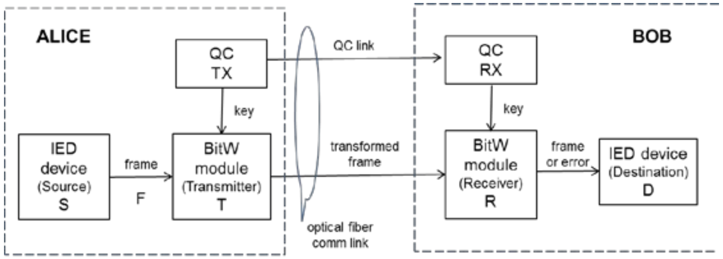
High-Security, Low-Latency, Stream-Wise Authentication and Encryption of Intelligent Electronic Device Links Enabled by Quantum Cryptography

Cybersecurity for Energy Delivery Systems Peer Review

August 5-6, 2014

Summary

- **Objective**
  - Low latency, high security encryption and authentication of grid control and data signals over installed optical fiber, including aerial fiber
- **Schedule**
  - 2013 – 2015
  - Measure dual-wavelength polarization wander in aerial fiber – done
  - Streaming message authentication codes in IED devices – done
  - Polarization tracking in aerial fiber – Aug/Sept 14
  - Demonstration on utility installed fiber- Sept/Oct 14



- **Total Value of Award:** $420k
- **% Funds expended to date:** 73.2%
- **Performer:** Los Alamos National Laboratory
- **NB:** Jane E. Norldholt, PI, will retire 7/2014 Raymond Newell has assumed PI role

Advancing the State of the Art (SOA): QC over Aerial fiber & Coexistence

- **The LANL Quantum Communications (QC) team has demonstrated streaming data encryption for smart grid control signals over optical fiber links. This demonstration at the TCIPG testbed at UI-Urbana Champaign transmitted encrypted synchrophasor data over static optical fibers.**
- **Optical fibers used by electric utilities are often installed on utility poles up in the air. These aerial fibers present unique challenges to the QC system; the transmitted light polarization states wander around as the fiber moves in the wind.**
- **We will invent, develop, and deploy a polarization tracking upgrade to our existing QC For The SmartGrid system to overcome this limitation and allow widespread adoption of quantum security technologies to the energy sector.**

Advancing the State of the Art (SOA): Message Authentication Codes

- **Encrypting grid control signals and data may not be enough- encrypted data is still subject to manipulation unless the data is also authenticated. Message authentication codes (MACs) provide security against substitution, impersonation, or replay of data. However, present-day MAC retrofits add unacceptable latency to grid control systems because a standard implementations (hashed message authentication codes) can only be calculated once a large block of data is available.**
- **Streamwise Message Authentication Codes do not suffer the latency penalty, but are rarely used because they require much larger quantities of secret key material**
- **By providing fresh cryptographic key material at high rates, our QC system can support new streaming MAC codes with new keys for each message, enabling high rate, high security transmission of grid control signals with encryption and authentication**

Challenges to Success

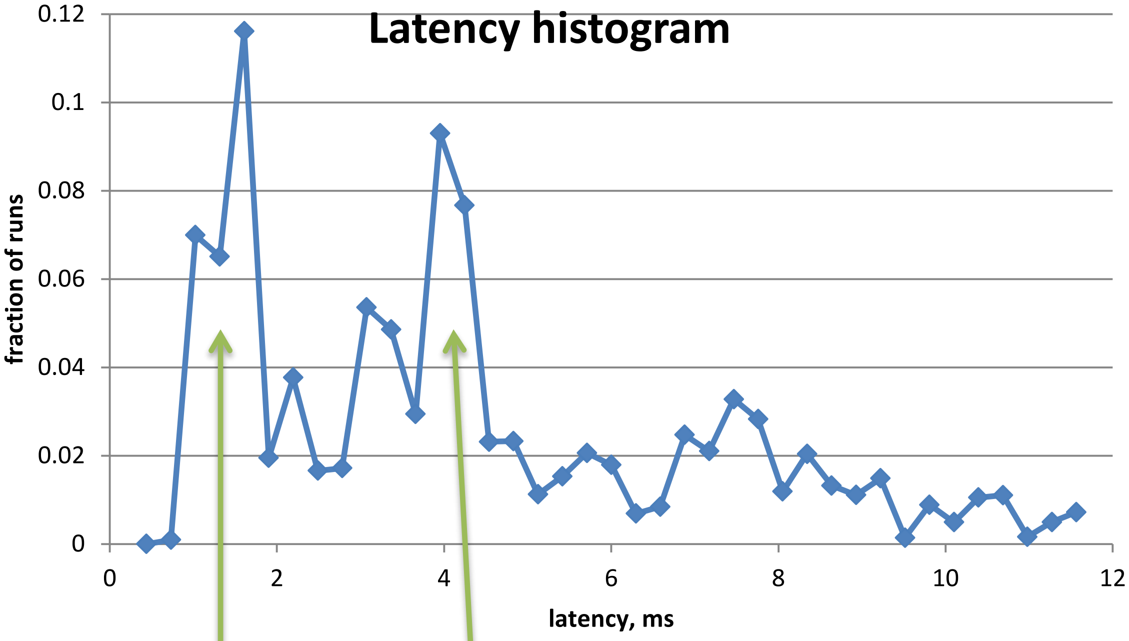
- **Polarization wander in aerial fiber**
  - Two polarization tracking strategies under development
    - One tracks a polarization fiducial signal at very different wavelength (e.g. 1310 nm vs. 1550 nm) and exploits properties of optical fiber to stabilize polarization
    - Other tracks a fiducial at nearby wavelength (eg 1550 nm vs 1552 nm) and uses strong filtering to separate the two
- **Wavelength cross-talk between adjacent channels**
  - Transmission of data payload (optical power $\approx$ 0.001 W) on the same fiber as the quantum signal (optical power $\approx$ 0.00000000001 W) requires strong isolation between the two. We use temporal and spectral filtering to minimize cross-talk.
- **Meeting latency requirements with installed hardware**
  - Timing jitter and built-in latency in our chosen demonstration hardware are comparable to our target latency. We mitigate this risk by driving down latency and jitter in our hardware.

MAC Latency below 5 ms

System used Quantum keys to authenticate all data packets exchanged between two SEL 311 protection relays.

End-to-end authentication time was recorded during two weeks unattended operation.

These tests were performed over static (not aerial) fiber.



< 2 ms
Desired operating point

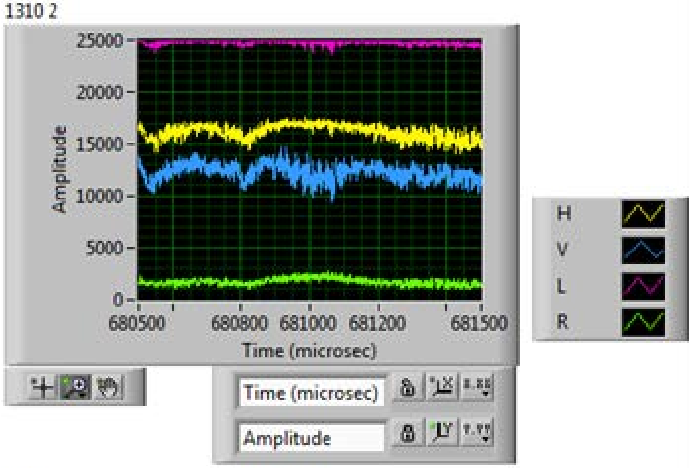
2 ms of jitter in packet timing detector circuitry:
Upgrade planned for third week of July

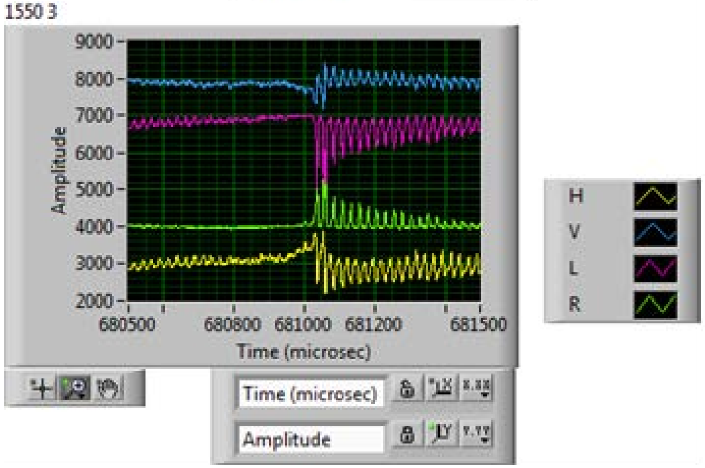
Measured polarization diversity in aerial fiber

We measured the polarization wander at 1310 nm and 1550 nm in 2.5km aerial fiber installed at LANL electric grid

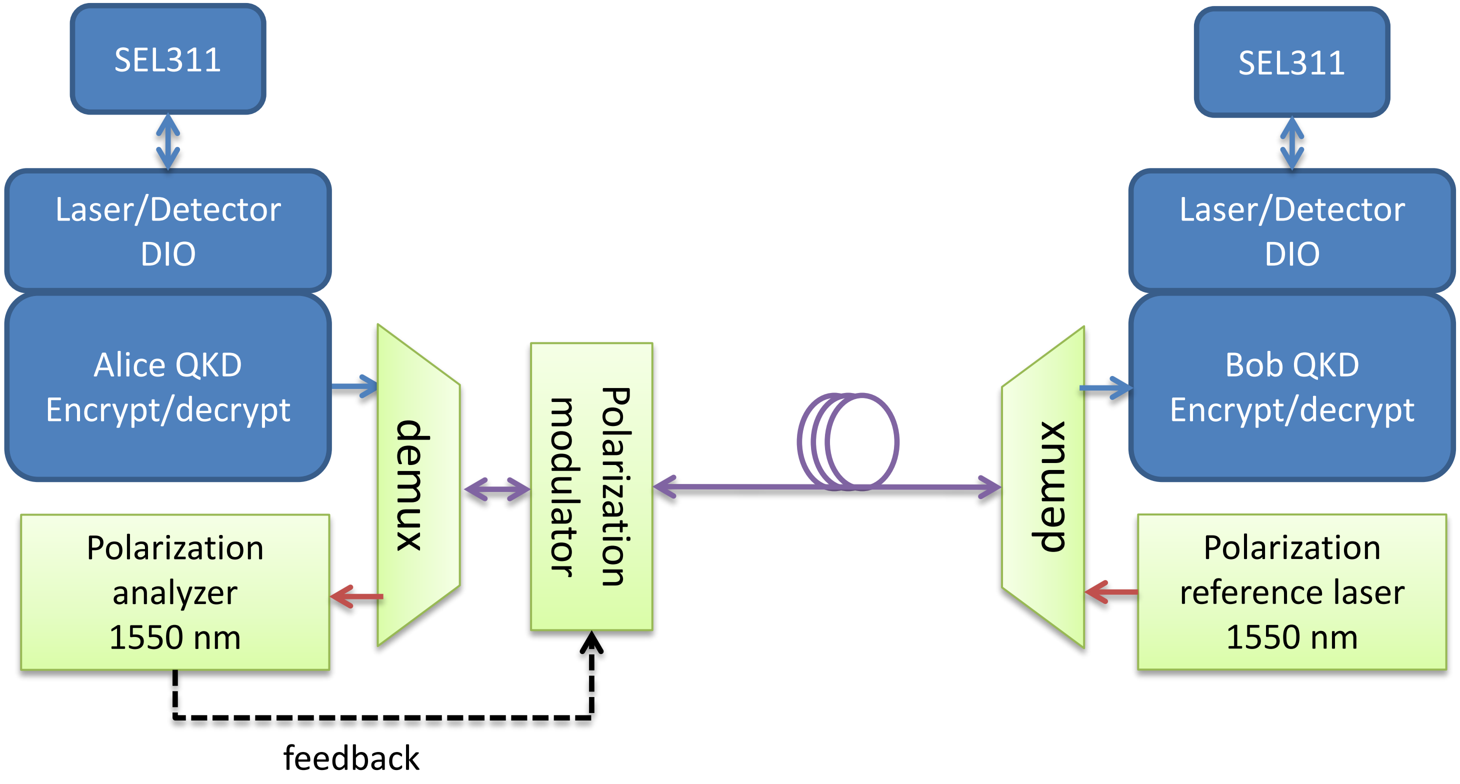
Our initial strategy was to stabilize polarization at 1310 nm, and thereby stabilize it at 1550 nm as well.

Measurements indicate lower-than-expected correlation between polarization changes at 1310 and 1550 nm; this is a significant obstacle to our initial strategy





Polarization tracking at nearby wavelengths



Collaboration/Technology Transfer

- **We are in the final stages of signing a license agreement to transfer all LANL quantum communications IP to a new commercial enterprise**
- **Significant venture capital investment**
- **This new company will develop commercial versions of LANL-invented QC hardware for applications including grid security**
- **Details likely available during Peer Review – ask me!**

Next Steps for this Project

- **Demonstrate successful polarization tracking over moving fiber in the laboratory**
  - Very close to accomplishing this goal already
- **Move existing hardware to 2.5 km Aerial fiber installed in LANL electric grid**
  - Terminals and support infrastructure have been identified and prepared for installation
- **Characterize system performance (authentication latency, QC bit error rates, system uptime) over a variety of weather conditions**
  - Late summer and fall in NM typically a very wide variety of conditions
- **Prepare final report**