Raymond Newell

Los Alamos National Laboratory

Quantum Hardware Security Modules

LA-UR 16-29066

Cybersecurity for Energy Delivery Systems Peer Review

December 7-9, 2016

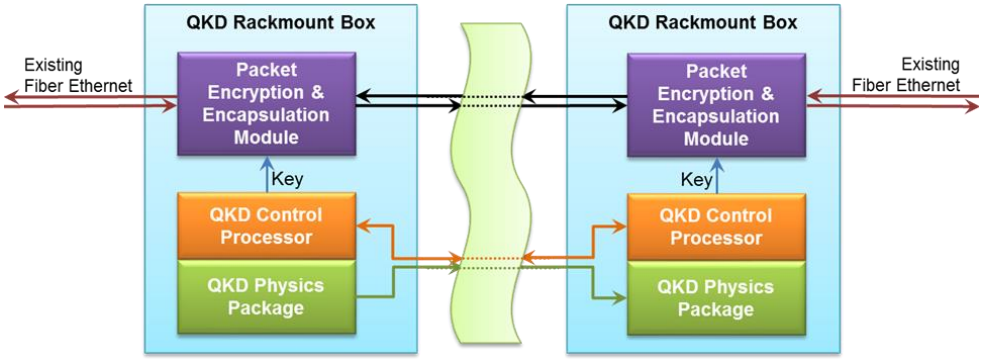
Summary: Quantum Hardware Security Modules

Objective

- Develop plug-and-play quantum encryption devices for smart grid applications

Schedule

- Oct 2014 – Sept 2017
- First field trials Feb 2015
- Validate new designs July 2016
- Engineered unit fielded Sept 2017



Performer:	**Los Alamos National Laboratory**
Federal Cost:	**$ 2,759,771**
Total Value of Award:	**$ 2,759,771**
Funds Expended to Date:	**19 %**

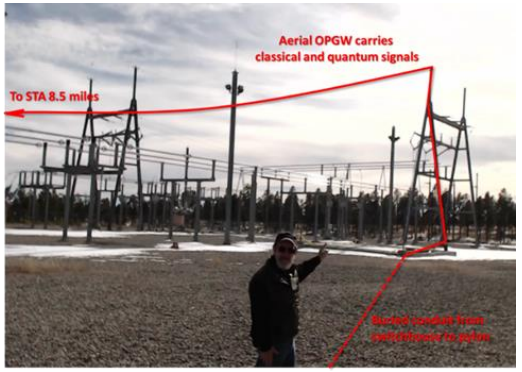
Advancing the State of the Art (SOA)

- Existing cryptography solutions for the grid are based on computational complexity
  - Strength against an adversary's abilities only weakens with time
  - Must routinely update, upgrade, or replace to maintain security
  - This is okay for phones and laptops (3-year replacement cycle), less desirable for critical infrastructure (3-decade replacement cycle, or more)
- Quantum Cryptography is based on physical laws
  - Strength against an adversary does not degrade over time
  - Requires fewer computational resources
- QC systems can be used as a bump-in-the-wire retrofit on existing control systems and networks
  - Invisible to end-user, but with much stronger security now and in the future
- Previously, we demonstrated streaming quantum encryption for synchrophasor data (C37.118), now focus is on moving beyond demonstration systems

Challenges to Success

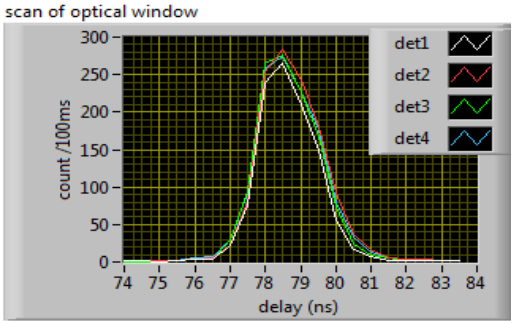
Transmitting quantum data over aerial fiber

- As optical fibers sway in the wind, they distort the quantum signals carried within. We have developed a polarization-tracking system which measures these distortions and compensates for them, effectively stabilizing the fiber.



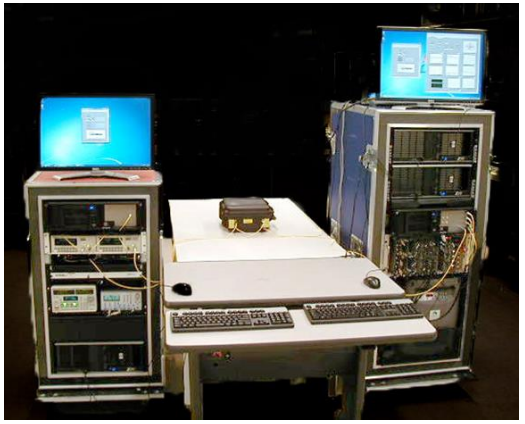
Distributing synchronization between terminals

- Quantum Comms require sub-nanosecond synchronization; we've developed a new clock-and-data-recovery architecture which maintains lock without interrupting the quantum transmission



Cost and facility footprint

- Our previous demonstration system filled two instrument racks and was over $140k in parts cost. Current system is below 1/2 the unit cost and 1/5 the size– we project significant reductions yet to come.



Progress to Date

Reduction in facility footprint and unit cost:

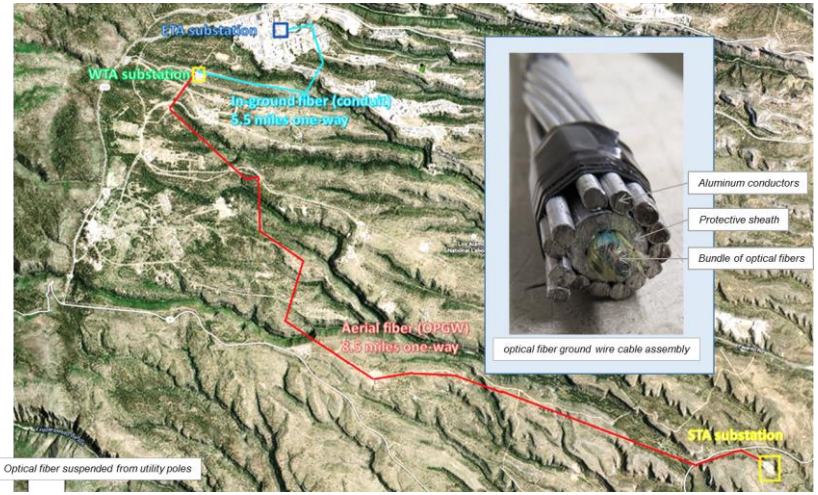
Lasers
Rubidium oscillator
Two variable optical attenuators
Laser driver and temperature controller
Pulse generator
Computer

Computer
Lasers
Laser driver
Temperature controller
Variable attenuators
Timing circuitry

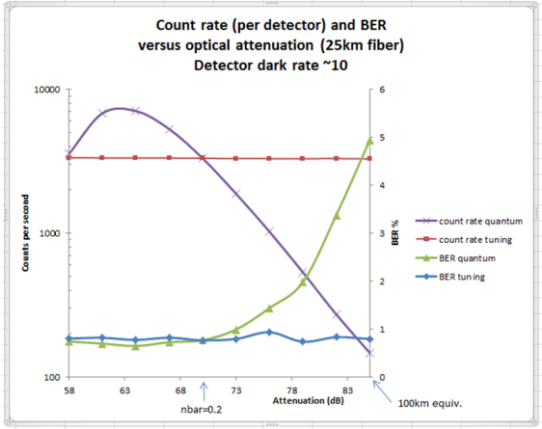
Computer
Computer
Polarization control, Lasers
Timing, digitization, power supplies
Pulse generator
Refrigerator and single photon detectors

Computer
Laser
Single photon detectors
Temperature controllers
Timing circuitry
Polarization Control
Power supplies

Operation over installed fiber



4x increase in range

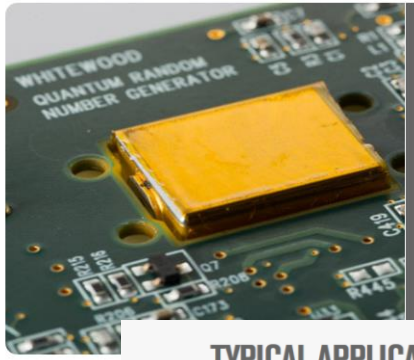


For the upgraded system, this operating range spans 20dB of attenuation, indicating that the system is capable of secure communication up to 100 km of fiber.

Collaboration/Technology Transfer

Dedicated History of Transition to Practice

The QC team at Los Alamos has a licensing agreement in place with WhiteWood Encryption Systems, Inc. Whitewood is a venture-backed startup created for the express purpose of developing Los Alamos IP portfolio and bringing products to market.



The Whitewood Entropy Engine has the following core capabilities:

- High performance random number generation of 200Mbps
- Designed to comply with NIST SP800-90B (draft)
- Access to raw entropy stream enables independent security testing and validation
- Real-time self-test processes ensure random data can be used with confidence
- Convenient PCIe plug-in card form factor
- Simple API to enable easy integration

2016 R&D 100 WINNER

TYPICAL APPLICATIONS FOR TRUE RANDOM NUMBER GENERATORS

Applications

- Cryptography
- Key management
- Crypto-currency
- Tokenization
- Authentication
- Payments
- PIN generation
- Statistical research and simulations
- Gaming and lotteries

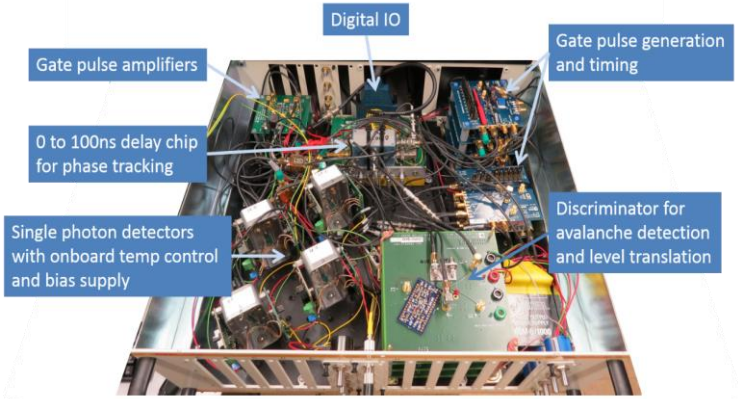
Product specification

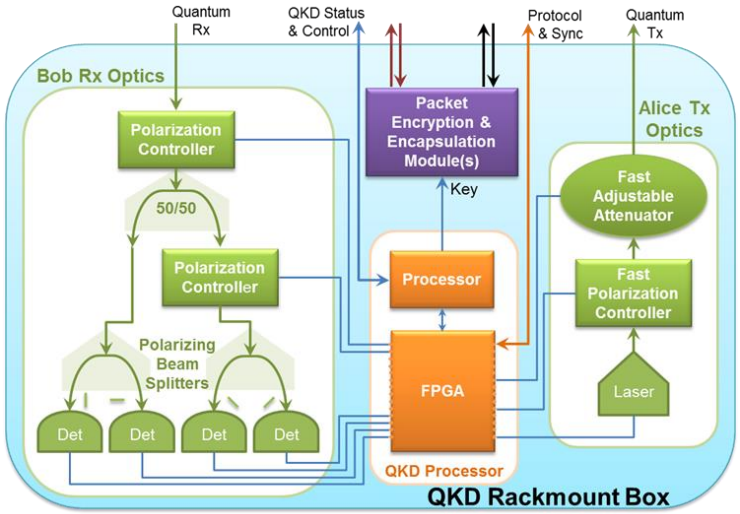
- Health Checks
  - Repetition count test (continuous)
  - Adaptive proportion test (continuous)
  - Conditioning block functional validation (startup)
- Physical and Electrical
  - Form factor: PCIe card (3/4 length)
- Entropy Production
  - Entropy conditioning: SHA-2 (512)
  - Output data rate: 200 Mbps
  - Entropy quality: >99.9% quantum sourced

Technical development funded by Los Alamos LDRD, DARPA
Technology transfer funded by DHS TTP program
Commercialization funded by Whitewood Encryption Systems

Next Steps for this Project

Reduce size, cost, and power by moving from module-level integration to custom circuit board





Replace windows-based control computer with embedded processor on FPGA

Additional slides

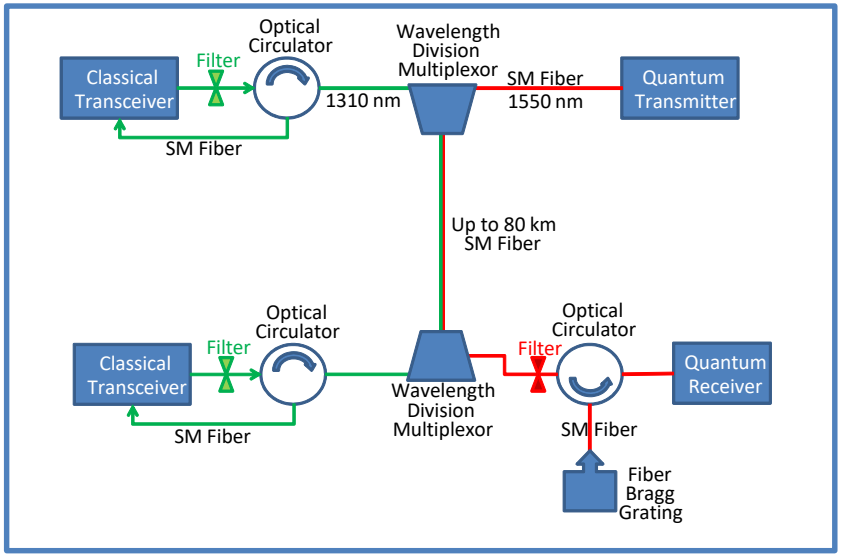
Transmitter upgrade: thermal stability by moving to two-fiber system

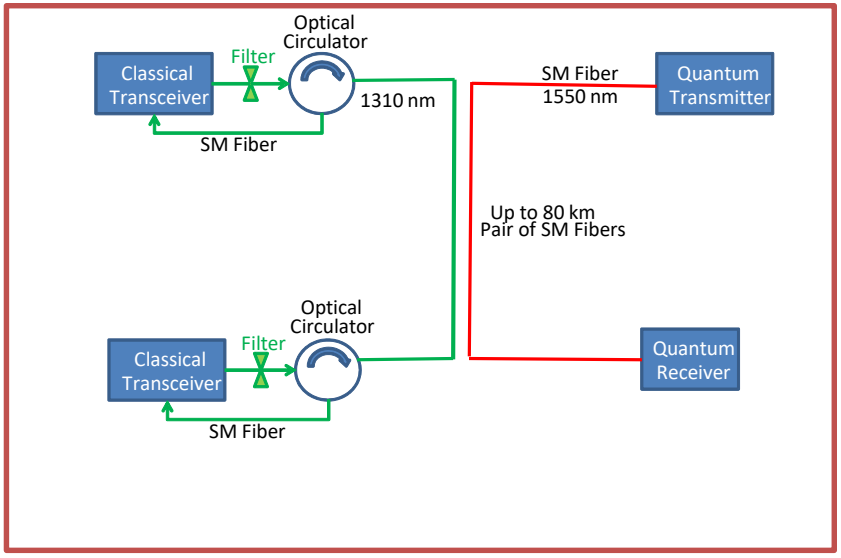
Our QC for the SmartGrid system was originally designed to operate over only one optical fiber: this came at a cost

- Narrowband optical filters to separate the quantum signals from the classical signals (10,000,000 x more powerful)
- These filters are very temperature sensitive; caused issues during our field testing

Lesson learned: optical fibers are almost always provisioned in pairs. In any real-world application, if one optical fiber is available to us then a second one is too.

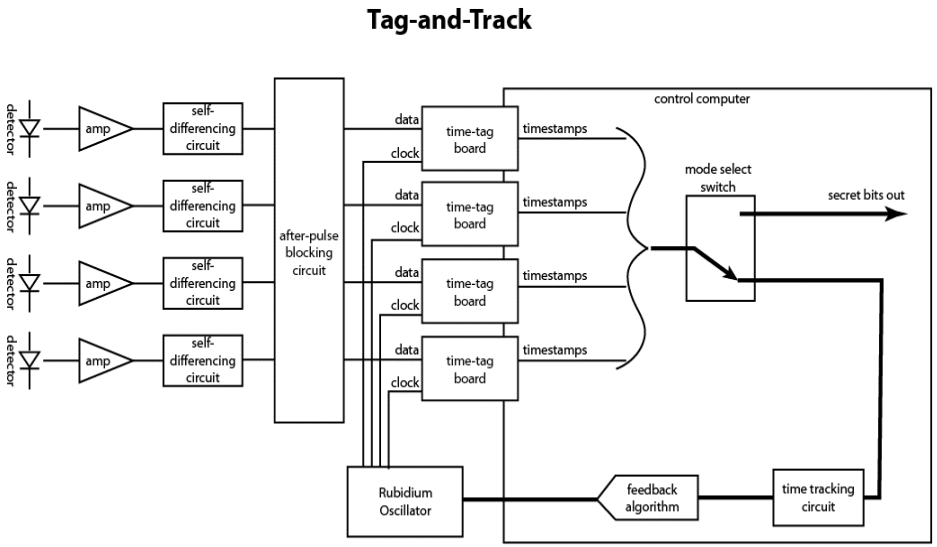
New strategy- use the second fiber for the classical channel





Additional benefit: laser stability requirement relaxed from ±0.05° stability to ±1°

Receiver upgrade: direct digitization replaces tag-and-track



It is necessary to synchronize the transmitter and receiver to sub-nanosecond precision.

In the past we have done so with a “tag-and-track” system.

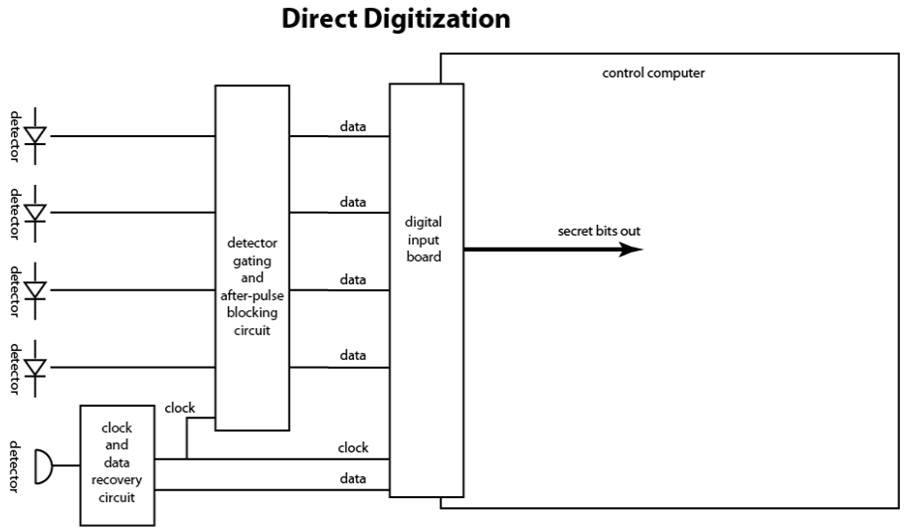
- Periodically interrupt key generation
- Switch to a time tracking algorithm
- Slew receiver clock while holding the transmitter clock fixed
- Assemble a histogram of detections to find the delay that puts them both in phase.
- Apply that delay, switch back to key generation

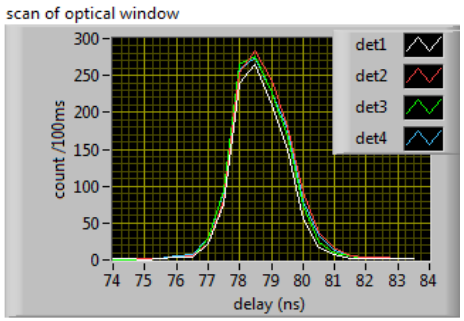
This worked well enough in the laboratory, where temperature is stable and nothing is moving. During field testing its shortcomings became apparent.

As much as 60% of the operating time in the field was given over to synchronization, with only brief periods of key exchange possible. Movement of the aerial fiber and temperature changes in the stations forced the system to trigger the synchronization mode again and again.

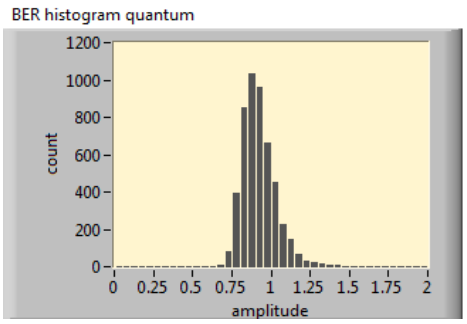
Additionally, the cost and complexity of the system are high, and Rubidium oscillators have a finite lifetime.

Receiver upgrade: direct digitization replaces tag-and-track





Four detectors synchronized
to within 100 picoseconds



Histogram of Bit Error Rate,
Two weeks unattended operation

To overcome these limitations we invented and implemented the direct digitization scheme. The classical communication channel is transmitted along with the single photons but on an adjacent fiber. This is a binary signal encoded with on-off-keying.

This signal is detected with a conventional photodiode at the receiver, and the on-off-keying code is recovered by a dedicated clock-and-data-recovery circuit.

This clock signal is synchronized to the signal photon signal because it has travelled down an adjacent fiber and accumulated the same delay.

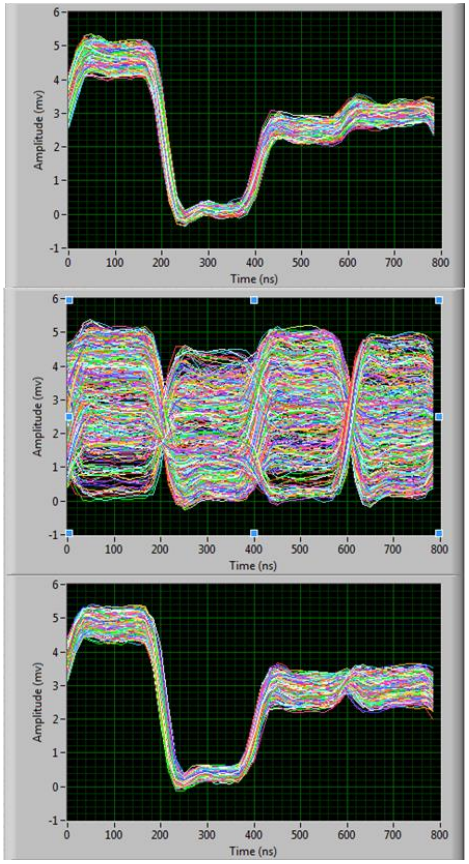
- It is used to gate the single-photon detectors directly; no tagging and tracking are required.
- The clock signal is synchronous with the output of the gating circuitry, so it can be used to trigger a standard digital input board. This vastly simplifies the interface to the computer.

Thermal effects and movement of the aerial fiber are common to both the classical and quantum channels, so they are automatically subtracted out by the clock recovery circuit.

Because key generation is now continuous, instead of interrupted, the polarization tracking system is far more robust. Previously it had to recover from every interruption; now it is able to maintain lock.

Polarization tracking over aerial fibers

The fibers used for grid control communications are often deployed on the same poles as transmission lines. As these fibers move in the wind the polarization state of photons travelling through the fiber is altered. Because we encode our quantum information on these polarization states, these alterations are a problem.



Received signals:
No polarization scrambling

Received signals:
With polarization scrambling

Received signals:
With polarization scrambling
And tracking system active

Los Alamos has invented and implemented a polarization-locking scheme which detects and corrects for these changes. It operates on the single-photon signals and stabilizes the signal even in strong winds.