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

Trusted Relay Node Networking

Los Alamos National Laboratory (LANL)

Raymond Newell PhD

Cybersecurity for Energy Delivery Systems Peer Review

November 6-8, 2018

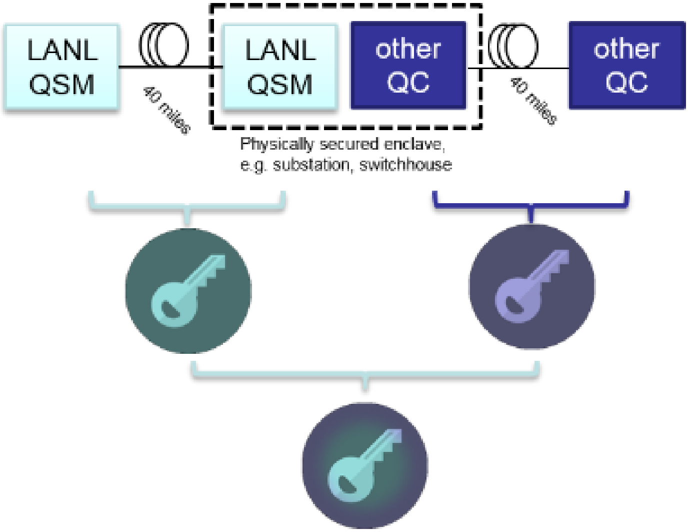
Summary: Trusted Relay Node Networking

Objective

- We will demonstrate that a succession of quantum-secured links, joined by relay nodes located in physically-secured locations, can overcome existing distance limitations.

Schedule

- Start Feb 2018, end Feb 2021
- Field tests:
  - Q1 2019 (TBD)
  - Q1 2020
  - Q4 2020
- Demonstrate interoperability of different Quantum Communication systems
- Bring security benefits of quantum communications to long-range links
- Show that quantum communication systems can exchange cryptographic key material over different physical-layer implementations



Total Value of Award:	$ 400,000
Funds Expended to Date:	19.7%
Performer:	Los Alamos National Laboratory
Partners:	Oak Ridge National Laboratory, EPB

Los Alamos NATIONAL LABORATORY EST.1943

OAK RIDGE National Laboratory

epb

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

Advancing the State of the Art (SOA)

- Existing quantum links are limited in range to ~100 miles, in practice much less. We will demonstrate that a succession of such links, joined by relay nodes located in physically-secured locations, can overcome this limitation.

- Nationwide deployment of quantum technologies will require interoperable systems from multiple vendors. An operator must be able to "plug-and-play" a quantum device without regard for the underlying physics. It is essential to deploy quantum technologies without the undue burden on operators that would result from disparate technologies

Advancing the State of the Art (SOA)

- The primary objective of this effort will be to develop and demonstrate a three-node network extending quantum communications by building and deploying trusted relay nodes. This work will address two existing impediments to widespread implementation of quantum communications technology: limitations on the maximum link range, and non-interoperable implementations. By developing and implementing a systems-level approach to interoperable trusted relay nodes, we will bring the security assurances of quantum communication systems to long-haul distances.

Challenges to Success

Lack of existing Quantum Communication standards

- There are several competing standards for classical key management and authentication, and very many homebrew solutions. But no standards are dedicated to quantum comms.
- The team has agreed on a standard keyfile format, with metadata in a header, 256-bit keys, and checksum

Sensitive equipment in a harsh environment

- Quantum signals are inherently weak, so detection equipment must be sensitive
- Reliable operation in a substation environment is challenging: thermal range, vibration, and EMF can be challenging
- The team includes seasoned engineers with decades experience in design for harsh environments

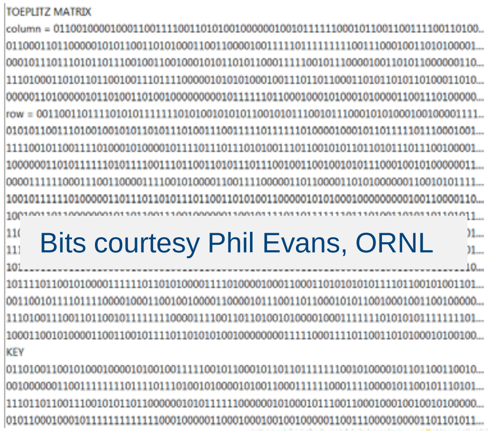
Progress to Date

Major Accomplishments

- Site visit and technical working meeting, July 2018

Photographs of optical fiber patch panel at EPB’s Riverside and Tennessee Tech power distribution substations. Duplex SMF28e+ single mode fiber with LC terminators.

- Agreement on keyfile data format



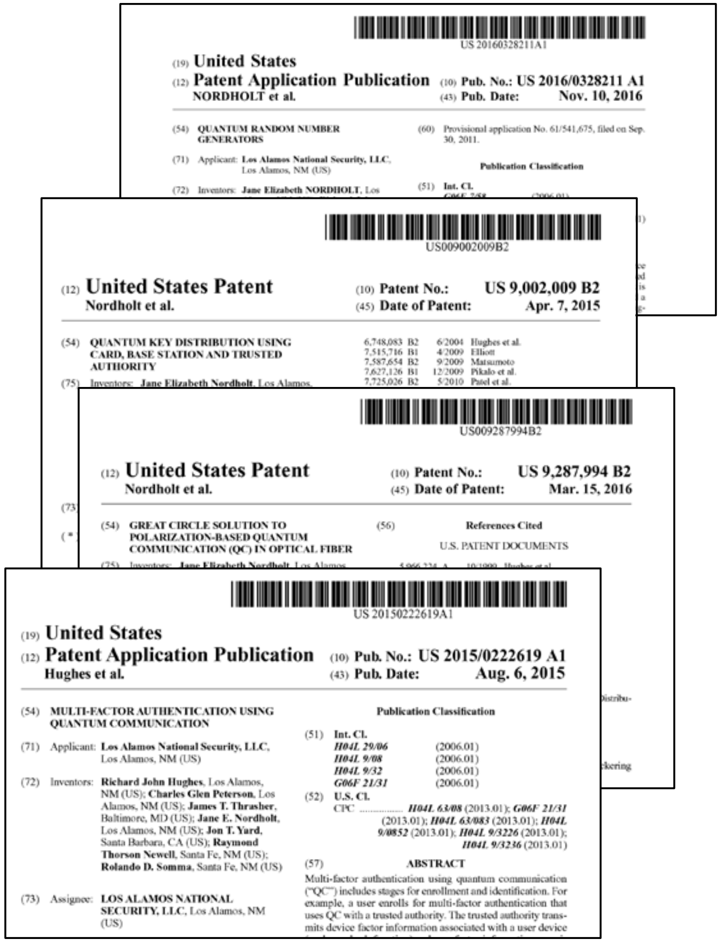
```
TOEPLITZ MATRIX
column = 011001000010001100111100110101001000000100101111110001011001100111100110100...
01100011011000001010110011010100011001100001001111101111111110011100010011010100001...
00010111011101011011100100110010001010110101100011111001011100001001101011000000110...
11101000110101101100100111011110000010101010001001110110110001101011010110100011010...
00000110100000101101001101001000000000101111110110001000101000101000011001110100000...
row = 001100110111101010111111101010010101011001010111001011100010101000100100001111...
01010110011101001001010110101110100111001111101111110100001000101101111101110001001...
11110010110011110100010100001011110111011101010011101100101011011010111011100100001...
10000001101011111101011110011101100110101110111001001100100101011100010010100000011...
00001111110001110011000011110010100001100111100000110110000110101000000110010101111...
10010111111010000011011101101011101100110101001100000101010001000000000100110000110...
100[illegible]11...
110[illegible]01...
111[illegible]01...
101[illegible]10...
10111101100101000011111101101010000111101000010001100011010101010111101100101001101...
00110010111101111000010001100100100001100001011100110110001010110010001001100100000...
11101001110011011001011111111000011110011011010010100001000111111101010101111111101...
10001100101000011001100101111011010101001000000000111110001110110011010100010100100...
KEY
01101001100101000100001010010011111001011000101101101111111001010000101101100110010...
00100000011001111111101111011101001010000101001100011111100011110000101100101110101...
11101101100111001010110110000000101011111110000000101000101110011000100010010010100000...
01011000100010111111111111100010000011000100010010010000011001110000100001101101011...
```

Bits courtesy Phil Evans, ORNL

Collaboration/Technology Transfer

Plans to transfer technology/knowledge to end user

- Industry acceptance will be pursued by
  1. Establishing strong IP portfolio (13 granted, 26 pending at last count)
  2. Licensing agreements with commercialization parts (negotiations ongoing)
  3. Cooperative Research and Development Agreements with partners to transition technology out of LANL
  4. Mature products available for sale to asset owners



US 20160328211A1

(19) United States
(12) Patent Application Publication (10) Pub. No.: US 2016/0328211 A1
NORDHOLT et al. (43) Pub. Date: Nov. 10, 2016

(54) QUANTUM RANDOM NUMBER GENERATORS

(60) Provisional application No. 61/541,675, filed on Sep. 30, 2011.

(71) Applicant: Los Alamos National Security, LLC, Los Alamos, NM (US)

Publication Classification

(72) Inventors: Jane Elizabeth NORDHOLT, Los

(51) Int. Cl.

US009002009B2

(12) United States Patent (10) Patent No.: US 9,002,009 B2
Nordholt et al. (45) Date of Patent: Apr. 7, 2015

(54) QUANTUM KEY DISTRIBUTION USING CARD, BASE STATION AND TRUSTED AUTHORITY

(75) Inventors: Jane Elizabeth Nordholt, Los Alamos,

6,748,083	B2	6/2004	Hughes et al.
7,515,716	B1	4/2009	Elliott
7,587,654	B2	9/2009	Matsumoto
7,627,126	B1	12/2009	Pikalo et al.
7,725,026	B2	5/2010	Patel et al.

US009287994B2

(12) United States Patent (10) Patent No.: US 9,287,994 B2
Nordholt et al. (45) Date of Patent: Mar. 15, 2016

(54) GREAT CIRCLE SOLUTION TO POLARIZATION-BASED QUANTUM COMMUNICATION (QC) IN OPTICAL FIBER

(56) References Cited

U.S. PATENT DOCUMENTS

US 20150222619A1

(19) United States
(12) Patent Application Publication (10) Pub. No.: US 2015/0222619 A1
Hughes et al. (43) Pub. Date: Aug. 6, 2015

(54) MULTI-FACTOR AUTHENTICATION USING QUANTUM COMMUNICATION

(71) Applicant: Los Alamos National Security, LLC, Los Alamos, NM (US)

(72) Inventors: Richard John Hughes, Los Alamos, NM (US); Charles Glen Peterson, Los Alamos, NM (US); James T. Thrasher, Baltimore, MD (US); Jane E. Nordholt, Los Alamos, NM (US); Jon T. Yard, Santa Barbara, CA (US); Raymond Thorson Newell, Santa Fe, NM (US); Rolando D. Somma, Santa Fe, NM (US)

(73) Assignee: LOS ALAMOS NATIONAL SECURITY, LLC, Los Alamos, NM (US)

Publication Classification

(51) Int. Cl.

H04L 29/06	(2006.01)
H04L 9/08	(2006.01)
H04L 9/32	(2006.01)
G06F 21/31	(2006.01)

(52) U.S. Cl.
CPC *H04L 63/08* (2013.01); *G06F 21/31* (2013.01); *H04L 63/083* (2013.01); *H04L 9/0852* (2013.01); *H04L 9/3226* (2013.01); *H04L 9/3236* (2013.01)

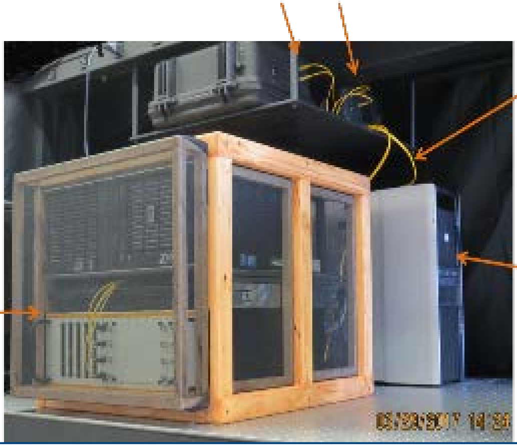
(57) ABSTRACT

Multi-factor authentication using quantum communication ("QC") includes stages for enrollment and identification. For example, a user enrolls for multi-factor authentication that uses QC with a trusted authority. The trusted authority transmits device factor information associated with a user device

Next Steps for this Project

In December 2018 or January 2019 (exact date TBD) we will transport our Quantum Hardware Security Module system to EBP for integration and testing with a comparable system delivered by ORNL.

25km optical fiber spools
for Communication and
Quantum Channels

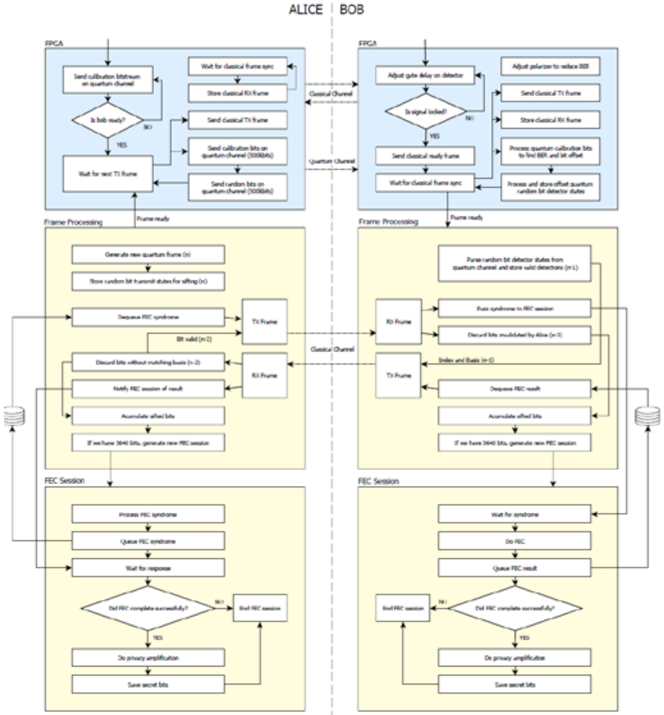


Standard SMF-28
Duplex fiber optic cables

Transmitter "Alice"
(all required electro-optics
housed in PC chassis)

Receiver "Bob"
PC, electronics and
electro-optics mounted
in transportable rack

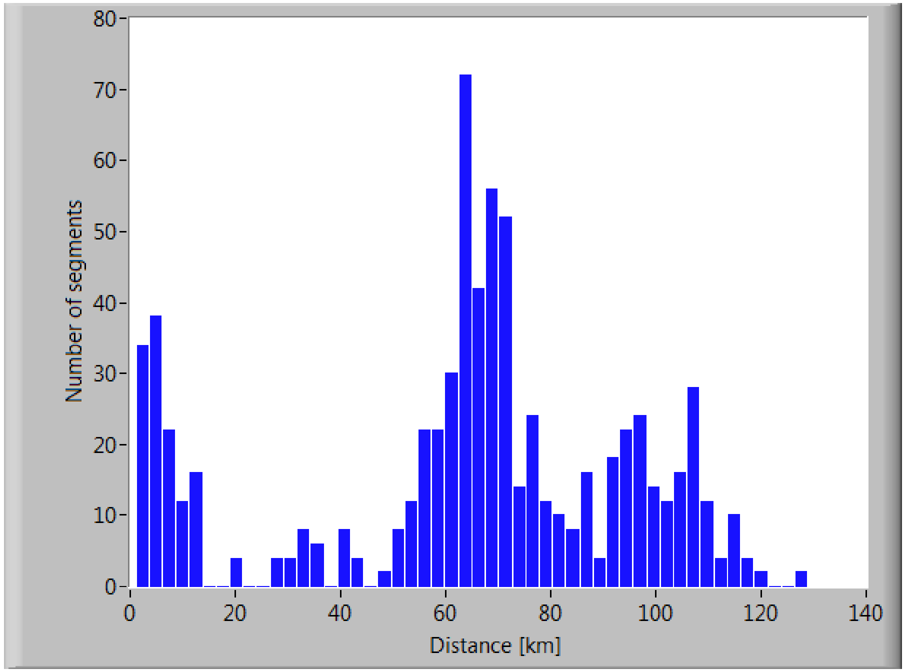
03/20/2017 14:24


ALICE
BOB
FPGA
Send calibration bitstream on quantum channel
Is bob ready?
NO
YES
Wait for next TX frame
Wait for classical frame sync
Store classical RX frame
Send classical TX frame
Send calibration bits on quantum channel (500kbits)
Send random bits on quantum channel (500kbits)
Classical Channel
Quantum Channel
FPGA
Adjust gate delay on detector
Is signal locked?
NO
YES
Send classical ready frame
Wait for classical frame sync
Adjust polarizer to reduce BER
Send classical TX frame
Store classical RX frame
Process quantum calibration bits to find BER and bit offset
Process and store offset quantum random bit detector states
Frame Processing
Frame ready
Generate new quantum frame (n)
Store random bit transmit states for sifting (n)
Dequeue FEC syndrome
TX Frame
Bit valid (n-2)
Discard bits without matching basis (n-2)
Notify FEC session of result
RX Frame
Accumulate sifted bits
If we have 3640 bits, generate new FEC session
Classical Channel
Frame Processing
Frame ready
Parse random bit detector states from quantum channel and store valid detections (n-1)
RX Frame
Pass syndrome to FEC session
Discard bits invalidated by Alice (n-3)
Index and Basis (n-1)
TX Frame
Dequeue FEC result
Accumulate sifted bits
If we have 3640 bits, generate new FEC session
FEC Session
Process FEC syndrome
Queue FEC syndrome
Wait for response
Did FEC complete successfully?
NO
End FEC session
YES
Do privacy amplification
Save secret bits
FEC Session
Wait for syndrome
Do FEC
Queue FEC result
Did FEC complete successfully?
NO
End FEC session
YES
Do privacy amplification
Save secret bits

80 km range would enable 70% of ESNet’s links

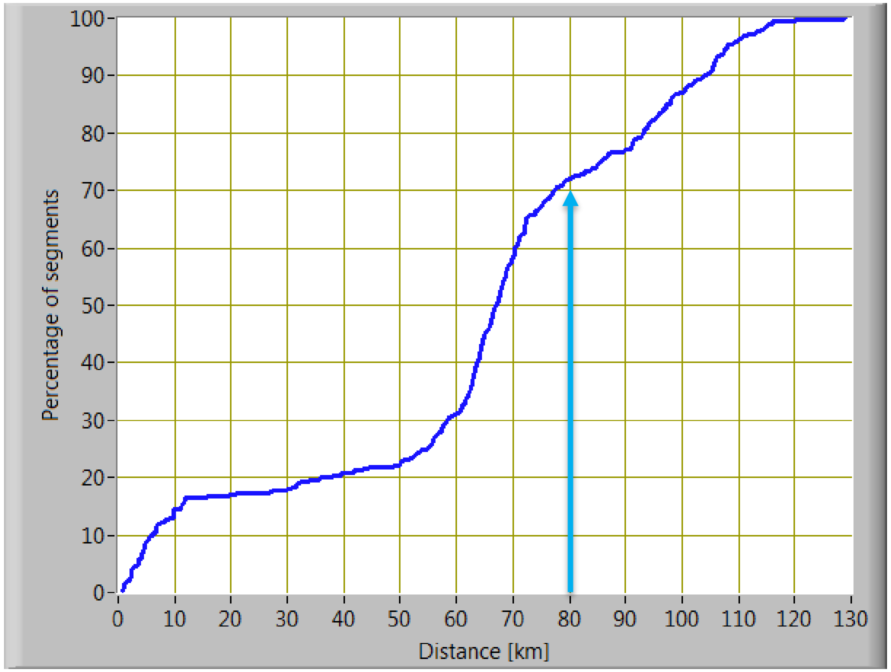
This is a histogram of all 734 fiber spans that comprise ESnet, sorted according to span length.

Histogram



A cumulative histogram of the same data set shows that 70% of all spans are 80km or less.

Cumulative Histogram



Data courtesy of Christopher Tracy, ESnet LBNL. Thanks to Sean Peisert.

A graded approach

This talk

Trusted Relay Nodes

Fully quantum links

Classical relay

Building is assumed to be secure

Next talk

Trust*worthy* Relay Nodes

Fully quantum links

Classical relay

Classical Crypto + Physically Unclonable Functions

No secure building needed

k

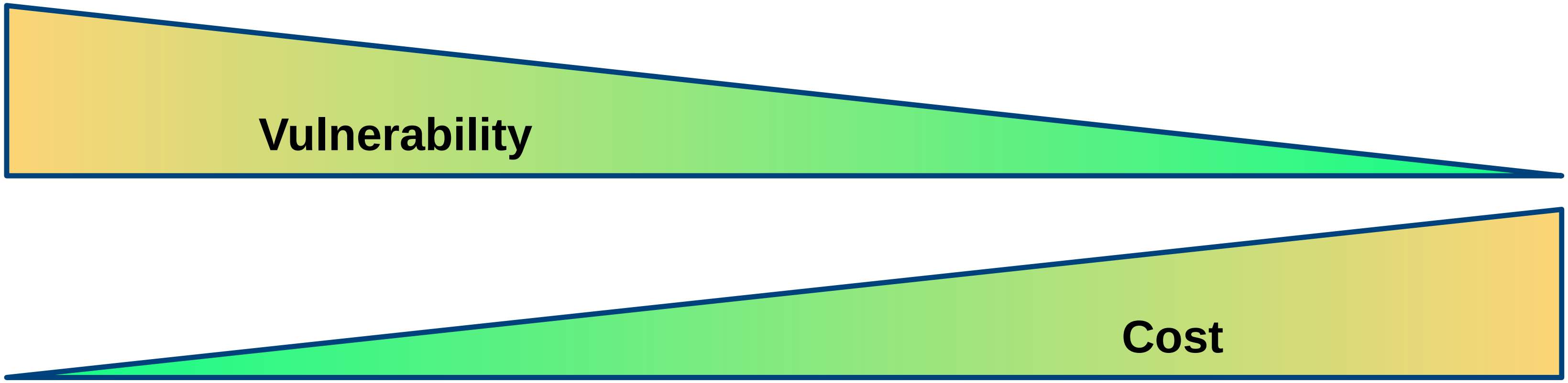
Quantum Repeaters

Fully quantum links

Fully quantum relay

Outside of scope for OE

(but very worthwhile!)


Vulnerability
Cost