Warren Grice
Oak Ridge National Lab

Grid Security with Quantum Architectures and Resources (Grid SQuARe)

Cybersecurity for Energy Delivery Systems Peer Review
July 24-26, 2012
Objective

- Identify situations in which quantum information techniques provide enhanced grid security.

Technical Approach

- Develop a quantitative comparison of quantum capabilities and grid requirements. Identify gaps and/or existing overlaps.
- Tasks:
  - List capabilities and requirements
  - Develop design tools
  - Foster dialog between QKD vendors and power industry

Schedule

- Deliverables on schedule for FY12

Performers: Quantum Inf. Sci. Team, ORNL

Partners: Various informal
Quantum Key Distribution (QKD)

QKD Limitations
- Short distances (< 150 km)
- Low data rates
- Better for Symmetric Key Encryption
- Great security, but expensive
Technical Approach and Feasibility

Quantum Key Distribution (QKD)

QKD Limitations
- Short distances (< 150 km)
- Low data rates
- Better for Symmetric Key Encryption
- Great security, but expensive

Grid Communication
- Short distances (< 150 km)
- Low data rates
- Small number of devices means SKE is practical
- Affordability and accessibility addressed later
Technical Approach and Feasibility

Grid Analysis (Opportunities)
- Identify security vulnerabilities
- Characterize communication techniques
- Understand network architecture

Technology Assessment (Solutions)
- Study commercial QKD systems
- Evaluate compatibility
- Understand limitations

GRID REQUIREMENTS
QKD CAPABILITIES

Converge
- Identify overlap between requirements and capabilities
- Find the “best” problem to solve
- Develop tools for effective comparisons
Technical Approach and Feasibility

- **Challenges to Success**
  - Quantum Information SMEs generally not familiar with cyber challenges for energy delivery systems
    - Seeking input from grid experts
  - Commercial QKD systems not designed for grid
    - Working with QKD vendors
    - Developed modeling tool
  - QKD provides great security, but is limited to two clients
    - Developing low-cost technique for multi-client QKD (ORNL proprietary)
• **Major Accomplishments**
  – Developed tool to model various QKD options
  – Frequency-entangled photon source fabricated and characterized
  – Fast, low-cost single-photon detectors fabricated and tested
  – Method for practical access to QKD links

• **Actual Progress vs Planned Progress**
  – Project scope changed in March
  – Largely on time and on budget
• Plans to transfer technology/knowledge to end user
  – This project will identify gaps (or overlap) between QKD capabilities and security needs
  – Will continue to foster dialog between QKD industry and utilities/equipment providers
  – Seeking partners for development of AQCESS and other ORNL IP
Next Steps

• **Approach for the next year**
  – Develop list of QKD capabilities
  – Develop list of needs: Which security needs are the best candidates for quantum solutions?
  – Primary risk is lack of access to technical specs

• **Potential follow-on work:**
  – GE and ID Quantique are interested in collaboration to develop **AQCESS** technique
Quantum Cryptography Applied to Electric Grid Security

Cybersecurity for Energy Delivery Systems Peer Review
July 24-26, 2012
Quantum Cryptography Applied to Electric Grid Security

- **Objective**
  - Utilize quantum cryptography to strengthen the security of transmitted PMU/PDC data packets

- **Technical Approach**
  - Develop a portable polarization-based, fiber optic quantum communication (QC) system, and associated control software
  - Quantify system performance over dark fiber, and coexisting with classical optical com
  - Demonstrate system operation at the TCIPG test bed

- **Schedule**
  - Complete coexistence and protection switching measurements, and maximize transmission distance by Aug 15th

- **Performers**: Physics Division LANL
- **Partners**: UI TCIPG
Technical Approach and Feasibility

• **Approach**
  – Current encryption systems rely on computational difficulty in factoring a large number
  – Quantum encryption systems have security rooted in the laws of physics
  – Implement the QC protocol over fiber by:
    • Transmitting polarized photons in one of two mutually unbiased bases, and in one of two possible bit values
    • Detecting polarized photons in one of two randomly chosen bases, and in one of two possible bit values
  – Encrypted data is cryptographically secure against advances in computing and factorization algorithms
Technical Approach and Feasibility

- **Challenges to Success**
  - Detection of single photons
    - InGaAs detectors cooled to -62 deg C
    - Detectors are enabled with a ~1ns gate, which must be synchronous with the single-photon arrivals
    - Atomic clocks are phase-locked by the quantum signal, to sub-nanosecond levels
  - Coexistence of single photons and classical signal requires extreme filtering
    - Combination of thin film filters, fiber-Bragg gratings and optical circulators
• Major Accomplishments
  – Portable, reliable system developed
  – System performance quantified
  – Data packets encrypted in real-time using quantum keys, with low latency
Collaboration/Technology Transfer

- **Plans to transfer technology/knowledge to end user**
  - QC will be an added security layer to PMU/PDC data packets
  - Industry acceptance will be gained by demonstrating performance at the UI TCIPG test bed
  - Integration with existing infrastructure is achieved by ensuring interoperability with C37.118 PMU data format, and by maintaining low latency when encrypting/decrypting data packets
Next Steps

• **Approach for the next year**
  – Relocate QC system to the UI TCIPG test bed for performance testing
  – Minor risk of delicate equipment being damaged in shipment

• Demonstrating compatibility with installed control systems will advance industry acceptance of QC systems
System Block Diagram

PMU data in → encryptor → "classical" data link → decryptor → PMU data out

QC system transmitter:
- laser
- modulator

QC system receiver:
- polarimeter
- Single photon detectors

Quantum keys

Single photon data link
Latency and Bandwidth

Latency vs Packet Size

Latency in microseconds vs Packet size in bytes
Quantum Bit Error Rate Distribution

Baseline Bit Error Rate Histogram
48hr Continuous Operation, 25km fiber
System Timing Stability

Photon Arrival Time Histogram
48hr Continuous Operation
Secret and Sifted Bit Generation Rates vs. Distance

- Sifted rate (dark)
- Sifted rate (light)
- Secret rate (dark)
- Secret rate (light)