Project Overview

Objective

• Provide industrial & utility networks with fast, deterministic, simple, and secure communication.

• Leverage synergy between time-sensitive networking (TSN) and quantum key distribution (QKD) to time-sensitive quantum key distribution (TSQKD)

Schedule: Oct 1, 2018 – Sep 31, 2021

<table>
<thead>
<tr>
<th>Report</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report on target demonstration scenario</td>
<td>3/31/2019</td>
</tr>
<tr>
<td>Report on design alternatives for integration of QKD with TSN</td>
<td>9/30/2019</td>
</tr>
<tr>
<td>Report on commercialization plan</td>
<td>9/30/2019</td>
</tr>
<tr>
<td>Standards-based YANG network management model</td>
<td>9/30/2019</td>
</tr>
<tr>
<td>Report on optical chip integration requirements and benefits</td>
<td>12/31/2019</td>
</tr>
<tr>
<td>Report on Time-Sensitive QKD-integrated architecture and technology gaps</td>
<td>9/30/2019</td>
</tr>
<tr>
<td>Time-Sensitive QKD scheduling software report</td>
<td>9/30/2020</td>
</tr>
<tr>
<td>Report on technologies for implementing integrated QKD chip architectures and filling identified gaps</td>
<td>3/31/2020</td>
</tr>
<tr>
<td>Report on Time-Sensitive QKD test suite</td>
<td>9/30/2020</td>
</tr>
</tbody>
</table>

Total Value of Award: $3,932,157

Funds Expended to Date: 74.44%

Performer: GE Research

Partners: Qubitekk MITRE EPB
Advancing the State of the Art (SOA) I

- *Describe current “state of the art”*
  - Classical RSA cryptography (RSA), Diffie-Hellmann (DH), Public Key Infrastructure (PKI), Post-Quantum Cryptography (PQC).
  - Alice & Bob Quantum Key Distribution (QKD) equipment: $10K+ each, box-sized, requires utilities (power, cooling water) and routine maintenance.
  - Quality-of-Service (QoS) and traffic isolation achieved through virtual Local-Area Networks (LAN) and basic prioritization.

- *Describe the feasibility of your approach*
  - Fiber connections used to implement QKD.
  - Time-Sensitive Network (TSN) provides deterministic communication with per stream QoS and flow control (Ethernet).

- *Describe how your approach is better than the SOA*
  - Simpler and more difficult to compromise; eavesdropper detected.
  - New Photonic Integrated Chip (PIC) design enables low-cost, low-form factor QKD for all edge devices on power grid.
Advancing the State of the Art (SOA) II

- **Describe how the end user of your approach will benefit**
  - Simpler, lower-cost, more secure.
  - Enables a converged, fully-characterized network.

- **Describe how your approach will advance the cybersecurity of energy delivery systems**
  - TSN enforces flow patterns at nanosecond resolution that resist cybersecurity attacks by restricting traffic injection.
  - QKD physical layer key generation and distribution improvement over classical cybersecurity and TSN enables low-cost control of Measurement-Device-Independent (MDI) QKD.
    - Eavesdropper (Eve) detection, high key entropy, simpler.

- **Describe the potential for sector adoption**
  - QKD standardization
    - Institute of Electrical and Electronics Engineers (IEEE) P1913 Software-Define Quantum Communication.
    - European Telecommunications Standards Institute (ETSI).
    - International Telecommunication Union (ITU).
Progress to Date

Major Accomplishments

- Patents (~8 filed):
  - Combining measurement device independent-quantum key distribution (MDI-QKD) and time-sensitive networks (TSN).
  - Time-sensitive network (TSN) scheduling with QKD.
  - QKD protection of TSN flows.
  - QKD-protected TSN time synchronization.

- Pathways for Sector Adoption:
  - Good communication/collaboration with GE businesses who supply utilities with communication and control equipment.

- Key Discoveries:
  - Photonic integrated circuit (PIC) chip design for edge devices & TSN compatible mode of operation analyzed.
Progress to Date

Milestones

• Designed grid solution with QKD-protected TSN
  • Including QKD authentication and encryption of TSN configuration.

• Developed qkd-linuxptp to integrate QKD-enabled Linux generalized Precision Time Protocol (gPTP) with the qkd-distributor.

• Eavesdropper designed and remote programming operation partially implemented.

• Designed simplified key mapping that assigns the keys based on actual data flows.

• Designed Time-Sensitive QKD (TSQKD) technology using grid standards and integrated into legacy equipment:
  • Distributed Network Protocol (DNP3) integrated with Secure SCADA Protocol for the 21st century (SSP21) over TSN.
  • Quantum symmetric keys used with IEC 61850 Routable-Generic Object-Oriented Substation Event (R-GOOSE) authenticity and encryption.
Challenges to Success

Challenge 1: Competition from PQC (post quantum cryptography), which tries to overcome quantum computing with increased complexity

- Steps taken to overcome challenge: keep informed of PQC progress, mostly funded by NIST, and discuss classical methods with GE experts.

Challenge 2: First attempt to secure time synchronization (gPTP) for TSN

- Designed and implemented QKD authentication for all time synchronization messages.

Challenge 3: Reducing operational complexity

- Leveraged TSN constructs for protected data streams and centralized network configuration to distribute keys.

Challenge 4: Expensive, large, high-maintenance equipment required for QKD implementation

- QKD approach that can be implemented entirely within PIC chips at edge devices without expensive equipment.

- Amortize QKD technologies across Intelligent Electronic Devices (IED) in a substation (@ 20 IEDs/substation, a $50k QKD device = Δ$2.5k/IED...closer to manageable).
Collaboration/Sector Adoption

- **Plans to transfer technology/knowledge to end user**
  - What category is the targeted end user for the technology or knowledge? (e.g., Asset Owner, Vendor, OEM)
    - QKD for utility asset protection could be used both by a utility (asset owner) and their OEMs, such as GE’s Grid Automation business.
  - What are your plans to gain industry acceptance?
    - Wavelength division multiplex all classical traffic (QKD and duplex data) to eliminate the need for additional fiber when introducing QKD to a link.
    - Insert into GE Grid Automation’s Mutli-Generational Product Plan (MGPP) and look for (1) customer funded pilot installations that will (2) lead to outward year insertion.
    - Zero extra configuration by OT staff will be key to lowest total installed cost.

- **Funding for a follow-on project will be required to reduce MDI-QKD PIC to practice**

- Describe testing and demonstrations planned:
  - Demonstration of R-GOOSE quantum encrypted communications on commercial product, GE Grid Solutions Universal Relay (to be setup with GE Grid Solutions).

- What is the timeline for demonstration and sector adoption?
  - Demonstration at EPB is in 2021. Sector adoption depends on further developments, costs, and competition (e.g., PQC).
IEEE P1913 Quantum Communication NETCONF/YANG Standard

Quantum Key Types
key-rate, entropy, etc.

QKD Types
sifting error-estimation, error-reconciliation, qber, alarms, entropy, key-generation, ...

Quantum Source Types
discrete-source, entangled-pair-source, continuous-source, ...

Passive Quantum Optics Types
beamsplitter, grating, lens, etc.

Networked Quantum Detector Types
augment /if:interfaces/if:interface:

Quantum Network View
2 Modules enabling independent quantum network subcomponents

Quantum Technology Types
continuous-variable, discrete-variable, integrated-quantum-optics, ...

Photon Encoding Types
stokes-vector, poincare-sphere, jones-matrices, bloch-sphere, ...

Coincidence Counter Types
external-internal-clock, coincidence-results, counter-operating-parameters, ...

Quantum Receiver Types
discrete-source, entangled-pair-source, continuous-source, ...

Multidetector Unit Types
detector* [id]

Quantum Optics View

Quantum Information Science View

1 QKD is only one of many possible applications

2 Modules enabling independent quantum network subcomponents
Next Steps for this Project

Approach for the next year or to the end of project

• Key Milestones to accomplish
  • Integration of all the networking and QKD components for Phase II
  • Field Test Automation
  • During demo of project, test ability of equipment to detect eavesdropper using variable fiber optic splitter (remotely operated)

• Upcoming significant events
  • Successful demonstration of our TSQKD equipment and approach at EPB utility in Chattanooga with Qubitekk
QKD-Protected Time Synchronization for TSN

Standards integration

QKD system

QKD (optical) channel

1. Key id

2. Traceable time source

3. Exchange PTP frames

4. All types of PTP frames are authenticated

5. Ethernet payload

Key + Lifetime id. is used to generate signature over

ICV

Key id.

RJ45 (Ethernet) link

gPTP master

gPTP slave

gPTP slave
|t₁–t'₁| = peak-to-peak PDV error of TSN network under the presence of uncontrolled traffic.

In a typical TSN network:
|t₁–t'₁| < 100 ns

**TSN delivers keys on isolated ethernet links to a pair of communicating nodes (Alice and Bob) at the exact same time. Basically synchronous delivery of keys with an error < 100 nsec**
QKD network with PIC chips for MDI-QKD

TSN-controlled
PIC chip design for Alice / Bob

Small, low-cost, ubiquitous QKD on a chip

Funding for a follow-on project will be required to reduce MDI-QKD PIC to practice
TSN-Synchronized Quantum Internet LAN

Coincidence control example...

**INDUSTRIAL QUANTUM NETWORK**

- **Quantum Source(s)**
  - Periodically trigger source
  - Periodically route to same det. at same time
  - Network Interface

- **Benes switch**
  - Fiber
  - $p_d_1$, $p_d_2$

- **Passive Optics (beamsplitter)**
  - $t_c$

- **Quantum Receiver(s)**
  - Network Interface
  - Set detector parameters, gating, etc.
  - Set windows, etc., periodically collect results

- **Coincidence Counter(s)**
  - Network Interface

**IEEE P1913**

- Offset $t_1$, $t_2$, $t_3$, $t_4$, $t_5$
- Ethernet (TSN)

**DETERMINISTIC CONTROL**

- Quantum Controller

**U.S. DEPARTMENT OF ENERGY**

- Office of Cybersecurity, Energy Security, and Emergency Response