Quantum-based Secure Communications for Remote Operations
NEUP Project 21-24354

2023 ARSS Fall Program Review

Stylianos Chatzidakis
Assistant Professor
School of Nuclear Engineering
Purdue University

October 2023
West Lafayette, IN
Team Info

- **Purdue**
  - Stylianos Chatzidakis (Assistant Professor and Associate Reactor Director, SRO)
  - True Miller (Reactor supervisor, SRO)
  - Brian Jowers (Electronics/I&C reactor staff, RO)
  - V. Theos, Z. Dahm, K. Vasily, K. Gkouliaras, W. Richards, R. Ughade (Grad students)

- **Collaborators**
  - Robert Ammon (Curtiss-Wright)
  - Phil Evans (ORNL)
  - Terry Cronin (Toshiba)

- **TPOC:** Katya Le Blanc (INL) and Ben Cipiti (Sandia)
New technologies...new challenges

- Secure communications
- Process flow (electricity, heat)

Operations -> Service Provider -> Markets

New reactor concepts => Significantly different requirements than existing fuel cycle facilities

Digitalization => New architectures and new vulnerabilities

New technologies => Quantum computing
Adversaries now have access to new tools with unprecedented capabilities
What about Cybersecurity?

“I don’t care what you do, just keep the plant running!”
- CEO of a large chemical processing plant on security
Energy sector high on target list

**Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity**

The hack underscored how vulnerable government and industry are to even basic assaults on computer networks.

**DIVE BRIEF**

**FBI: US energy sector faces ‘reconnaissance, scanning’ by Russian hackers; 5 companies targeted**

Published March 23, 2022

**COMPUTING**

**How a quantum computer could break 2048-bit RSA encryption in 8 hours**

A new study shows that quantum technology will catch up with today’s encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 20 years or so.
Goals & Objectives

Goal: Experimentally and numerically investigate quantum-based secure communications and demonstrate under prototypic conditions in PUR-1.

Objectives:
1. Develop a robust quantum communication modeling and simulation framework to support the analysis of QKD systems
2. Develop a cyber physical testbed with remote monitoring and communications in PUR-1
3. Perform testing with prototypic QKD equipment and evaluate performance with and without cyber events
One Time Pad Scheme Guarantees Confidentiality

**Encryption**

- **Message bit** $x_i$
- **Key bit** $k_i$

**Transmission**

- $x_i + k_i \mod 2$
- Encrypted bit $y_i$

**Decryption**

- $y_i \mod 2$
- Message bit $x_i$

**Key distribution method**

True Random Number Generator
Quantum Key Distribution Provides Detection of Adversary

Quantum channel

Public channel/Network connection

Alice:
$N$ random bits

Shared key

Parameter estimation,
Privacy amplification

Sifting:
Bases shared in public channel

Bob:
$N$ random bases, decodes

Alice:
$N$ random bases, encoding
How it works

Send photons $\rightarrow$ Measure QBER $\rightarrow$ Higher QBER $\rightarrow$ Lower Security

$SKR = \frac{\text{final secret key length}}{\text{sifted key length}}$

$QBER = q_e (1 - q_{ch}) + (1 - q_e)q_{ch} = \frac{\varepsilon}{4} + \frac{2q}{3} (2 - \varepsilon)$
Our work so far…

Development of NuQKD a novel simulation tool for engineering applications.

Formulation of a nuclear reactor communications reference scenario

Analysis of reactor signals and required bandwidth

Modelling of channel imperfections and attacker scenarios

Evaluation of QKD performance for nuclear reactor communications
NuQKD simulation algorithm

**Inputs (Universal):**
- Number of iterations (n)
- Number of photons (raw key size)
- Intercepted rate (ε)
- Depolarization parameter (p)
- Sharing bits fraction (f)
- IP address & socket port

**Outputs (Universal):**
- Sifted key length
- QBER
- Elapsed time (Classical Channel)

**Inputs (Optional):**
- Repetition frequency (ν furnish)
- Channel attenuation (a)
- Transmission distance
- Detector efficiency (η)
- Dead time (τ)
- Random attack rate

**Outputs (Optional):**
- Elapsed time (Quantum Channel)
- Sifted key rate
- QBER of remaining bits
- ROC Curve

**BB84 simulation (optical fiber and free space)**

**Equipment imperfections (source, channel, detector)**

**Bit strings from True Random Number Generator (TRNG)**

**Two-terminal /Single terminal execution**

**Modular design approach**

**Advanced customization of multiple input parameters**

**Evaluation and export of various performance metrics**
NuQKD is now benchmarked and fully operational
Reactor reference scenario

1. Reactor to Remote Workstation (RTU)
2. Reactor to Data Storage Station
3. Reactor to Energy Grid / Consumer Network
Reactor data & Bandwidth

- PUR-1 data used as case study
- 67 core signals
  - 1 Hz sampling
  - 6-digit accuracy
- Min and max values recorded:
  - Over 24 hours of operation
  - Including transients and outliers

533 bps required to transmit all 67 signals
Introducing PUR-1

Fully Digital I&C

Operator Console

Reactor Pool
Before and after...

1960 - 2017

2019 - present
Towards a Real-Time Cyber-Physical Digital Twin
Towards a Real-Time Cyber-Physical Digital Twin

PUR-1
Towards a Real-Time Cyber-Physical Digital Twin

OT/IT Comms

PUR-1

RMSS
Towards a Real-Time Cyber-Physical Digital Twin

**PUR-1 Facility**
- Testbed
- PUR-1 I&C System
- Reactor Instrumentation
- Reactor Facility
- Neutron Detector
- PLC
- Remote location

**RMSS**
- Digital Twin
- Data & Information Analysis
- Simulation Software
- Recommended Actions
- Diagnostics/Consequences Analysis

**Control rack**
- OT/IT Comms
- OT & IT System
- Sensor Data
- HMI

**PUR-1**
- Control rack

**RMSS**
- Radiation Imaging and Nuclear Sensing Laboratory
Installing and Testing AMDR

- Actuator
- AMDR
- Guide tubes
- Support structure

Completed May 2023
Digital/Cyber Remote Station

- RTP 3000 TAS N+
- Nuclear grade PLC
- 16 CH AI/IAO
- 32 CH DI/DO
- Field Programmable Gate Array
- Power distribution unit
- Actuator control

- IT Monitoring
- R-TIME GUI
- Real-time diagnostics
- Siemens S7 PLC
- UPS APC/1500

Stats:
- 2000 parameters
- 1kHz sampling

To GPU
Remote Monitoring System Operational

Remote Monitoring and Simulation Station
- Network Switch
- Simulated Noise
- OTP Encryption
- Remote Control Setup

PUR-1 Facility
- QKD Sender/Receiver
- AMDR
- Reactor PLC
- Reactor Instrumentation
- Reactor Core
- Testbed Instrumentation

Physical System
- Digital Controller
- Ethernet Switch
- "Intruder"
- Historian

RMSS / Virtual System
- Real-Time Data from Reactor Instrumentation
Instrumentation & Control

**Instrumentation**
- 4 neutron detectors (FC, UIC, CIC) => cps, % power, change rate
- 3 radiation area monitors (mR/hr)
- 1 air monitor (Ci/m3)
- Water chemistry (°C, μS/cm), confinement pressure (kPa)

**Control**
- RTP 3000, Ethernet-TCP/IP communications
- R-Time (sampling rate up to 1 kHz)

**Archived data (process, network, and host)**
- All instruments, operator actions, alarms, shim and reg rod positions, source position, HVAC, magnet, pump current/voltage, etc.
- PLC, UPS (battery status, freq, V, A), and system diagnostics
- Network traffic (bandwidth, packet analysis, etc.)
- Engineering workstation host system processes
Normal and Abnormal States

• Normal operation/state
  • Startup procedure
  • Any power level up to 100% (up to 2% change rate per supervisor guidance)
  • Irradiations
  • Shutdown by gang lower or SCRAM
  • Multiple operators

• Simulated abnormal states (tentative)
  • Power excursion (ramp up > 2%, alarm @6%), modify critical rod positions, etc.
  • Oscillations (e.g., equipment degradation), unusual power levels
  • Equipment on/off (pump, HVAC, temperature increase)
  • Cyber
    • Eavesdropping (e.g., process and operation data)
    • Data exfiltration (e.g., Monju type attack, steal host system data)
    • DoS (e.g., Davis-Besse, Browns-Ferry)
    • False data injection (e.g., Stuxnet type replay attack, data tampering)
  • Multiple scenarios (e.g., DoS for distraction+replay attack+oscillations)
Datasets for Benchmarking

Dataset #1
- SS
  - Low power
  - High power

Dataset #2
- Raw
  - Curated

Dataset #3
- Normal
  - Gang lower
- Abnormal
  - SCRAM

Transient
- Start-up
- Power change
- Full cycle
- Shutdown
  - 1_Shutdown.csv
  - 2_Shutdown.txt
  - 3_Shutdown.xlsx

File data format

File header

<table>
<thead>
<tr>
<th>Point #</th>
<th>Point Name</th>
<th>Database</th>
<th>Point Type</th>
<th>Point Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RHR-Pool-LVL</td>
<td>PUR1</td>
<td>Analog Input</td>
<td>POOL TOP RAN LEVEL</td>
</tr>
<tr>
<td>2</td>
<td>NFD-1-CPS</td>
<td>PUR1</td>
<td>Analog Input</td>
<td>CH 1 LOG WIDE RANGE</td>
</tr>
<tr>
<td>3</td>
<td>NFD-1-CN</td>
<td>PUR1</td>
<td>Analog Input</td>
<td>CH 1 LOG CHANGE RATE</td>
</tr>
<tr>
<td>4</td>
<td>NFD-2-LOG</td>
<td>PUR1</td>
<td>Analog Input</td>
<td>CH 2 LOG POWER</td>
</tr>
</tbody>
</table>
DoS and FDI
Conclusions

- Explored potential of addressing nuclear I&C confidentiality requirements with QKD
- Developed novel simulation tool (NuQKD) offering unique features
- Constructed reference reactor scenario inspired from modern designs
- Cyber-physical testbed installed and operational
- More than 2000 OT and IT signals including real-time cyber events
- Preliminary results are promising, justify further real-world experimentation
Publications (1/2)

**Journal papers**


**Theses**


Publications (2/2)

**Conference papers**


Acknowledgements

This research is being performed using funding received from the DOE Office of Nuclear Energy’s Nuclear Energy University Programs under contract DE-NE00009174.

We also thank Lon Dawson and Ben Cipiti at Sandia and Katya Le Blanc at INL for fruitful discussions and expert input.
Questions?