U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

A Prototype for Ultimate Secure Transmission and Analysis of Smart Grid Data on the Wire BNL

E. Figueroa, D. Katramatos

Cybersecurity for Energy Delivery Systems (CEDS) Peer Review

October 6-7, 2020

Project Overview

Objective:

- Long term vision:
  Provide hack-proof encryption to data flowing between different sources and destinations in the smart grid network with quantum-protected keys, while allowing in-network analysis nodes to access the encrypted data and analyze them while in transit in real/near-real time.
- 2-year objective:
  Develop a classical/quantum hybrid network prototype towards a highly secure system in the context of energy delivery.

Schedule:

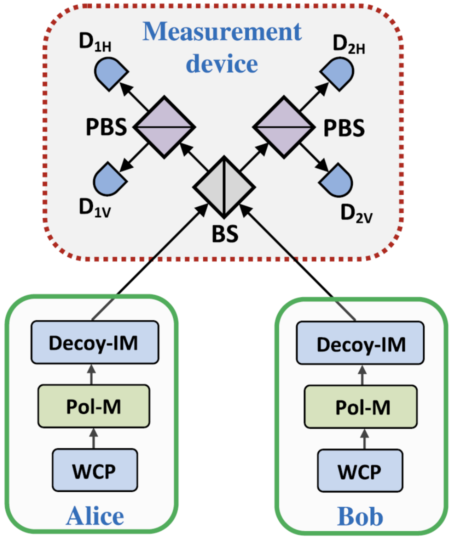
- 1/24/2020 – 1/31/2022
- Proof-of-concept prototype by early 2022

Total Value of Award:	**$2,000,000**
Funds Expended to Date:	**11.5%**
Performer:	**BNL**
Partners:	**SBU, ORNL, LANL**

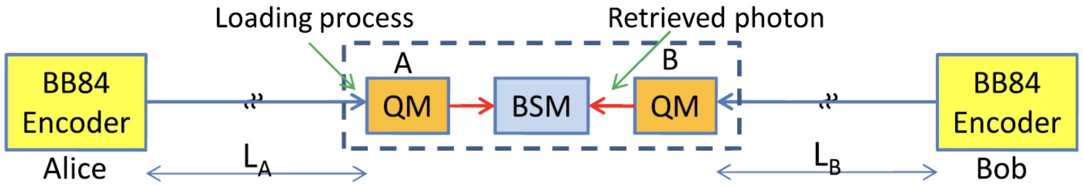
State of the Art in QKD

MDI QKD / Twin-field QKD PRL 108, 130503 (2012)

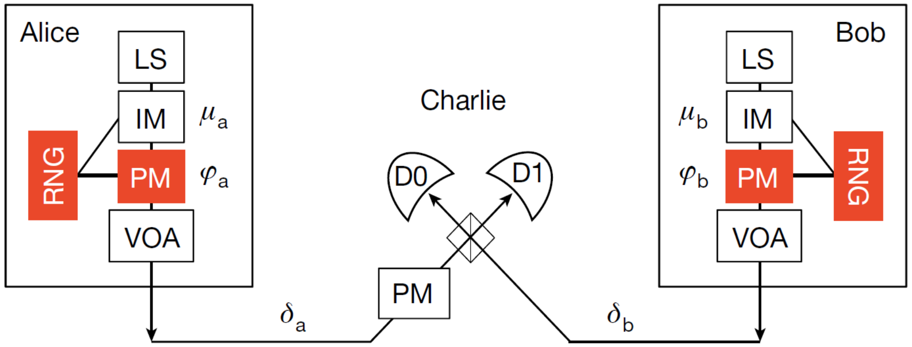
- **Quantum Communication**
  - State preparation, Distribution, Measurement
- **Quantum Cryptography**
  - Sifting, Parameter estimation, Error correction, Privacy amplification



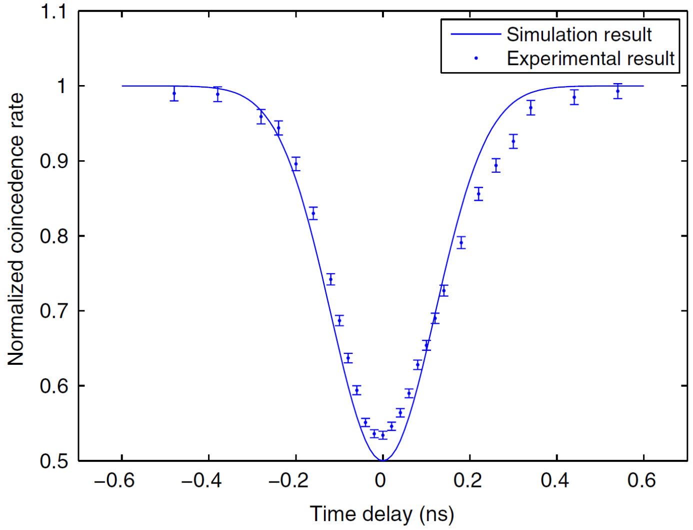
Memory-Assisted MDI QKD NJP 16, 043005 (2014)



Twin-Field QKD Nature 557, 400 (2018)



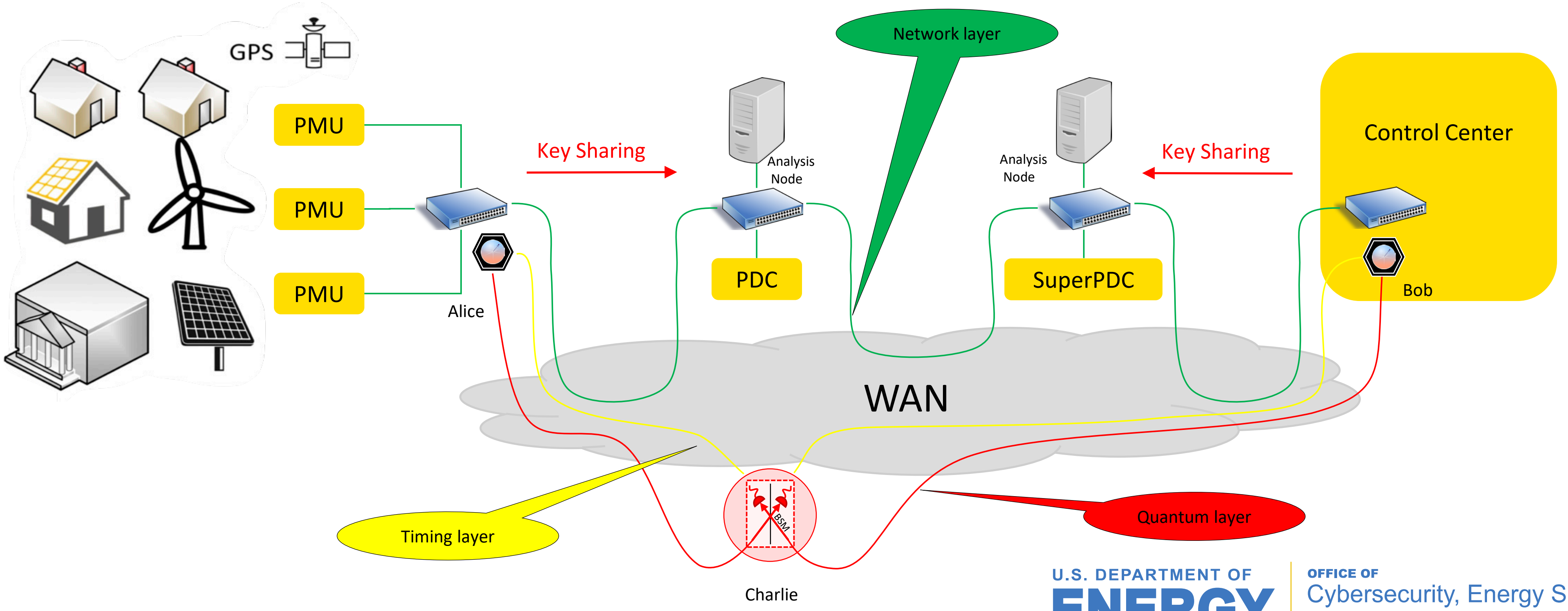
Key Measurement: Photon Indistinguishability (HOM Interference)



Advancing the SOA (Application)

Platform to perform in-network computations on data in transit encrypted with quantum-protected keys.

- Three technology layers:
  - Phase 1: Quantum layer for qubit transmission.
  - Phase 2: Classical timing network layer for sub-nanosecond synchronization of quantum devices.
  - Phase 3: Classical data network layer for communication between data sources (e.g., PMUs, PDCs) and destinations (in-network analysis nodes, super PDCs, control centers).

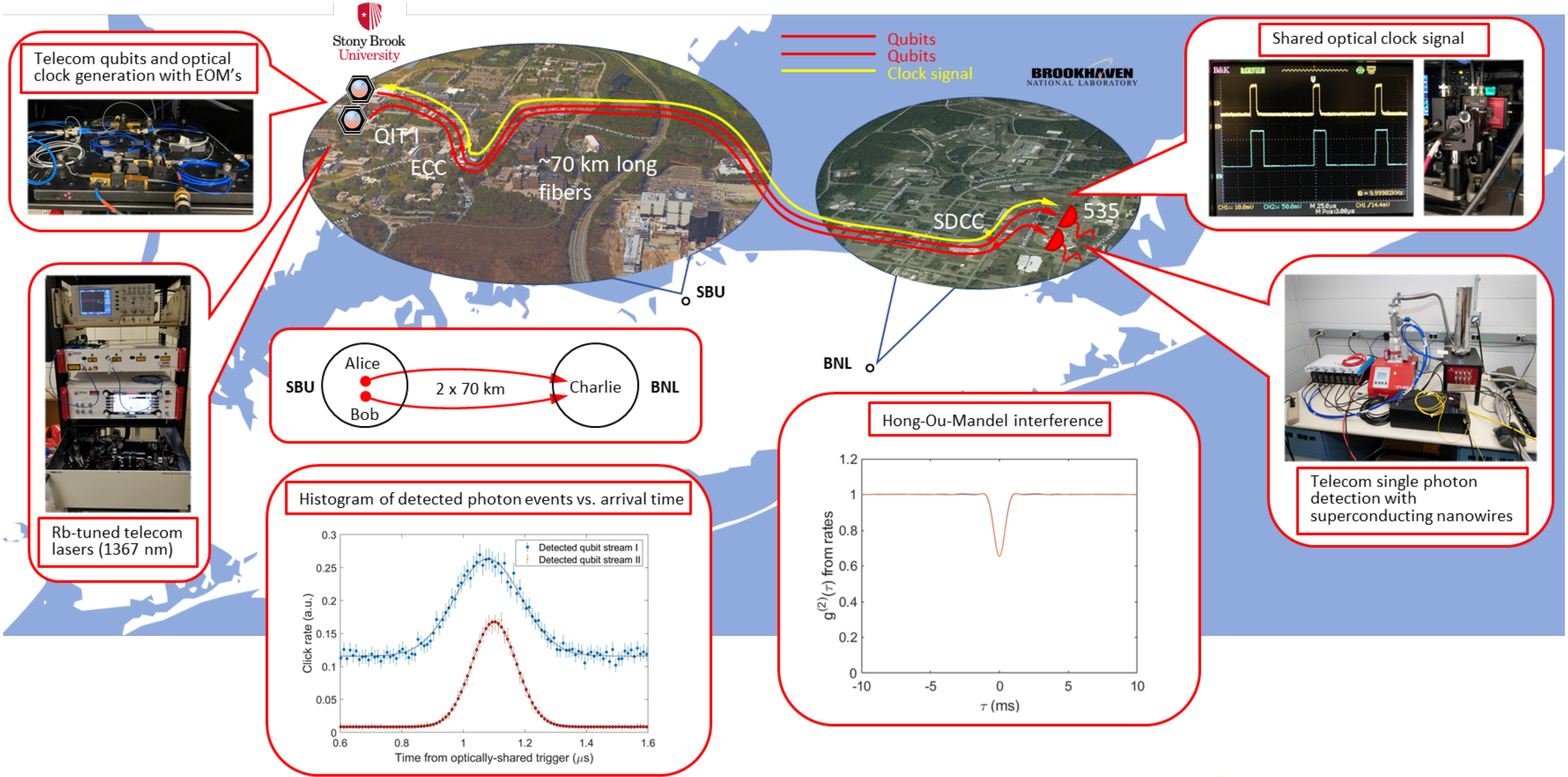


Measurement Device Independent QKD

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

Highlight: longest US qubit transmission

- Successful qubit transmission over ~140km in twin-beam configuration.
- HOM interference of communicated qubits after long distance transmission.



Telecom qubits and optical clock generation with EOM's

Rb-tuned telecom lasers (1367 nm)

Shared optical clock signal

Telecom single photon detection with superconducting nanowires

Histogram of detected photon events vs. arrival time

Hong-Ou-Mandel interference

Challenges to Success

1) Field a real-life quantum network that can deliver keys over long-distances:

- MDI QKD works for longer distances, quantum coherence must be preserved.
- Might need to be quantum-memory assisted.

2) Achieve timing and control of the network over optical fibers:

- Sub-nanosecond synchronization of quantum devices over optical fibers.
- Fast optically-shared classical control signal distribution.

3) Multiplexing timing and control signals with data traffic:

- Timing/control should be multiplexed with data traffic.
- Coexistence for quantum/classical signals.

4) A hybrid classical/quantum crypto-system requires key sharing:

- Putting together a fully secure system, including key-sharing impervious to quantum computer attacks, is a hard problem surpassing the scope of the current project.

5) Unforeseen delays (pandemic)

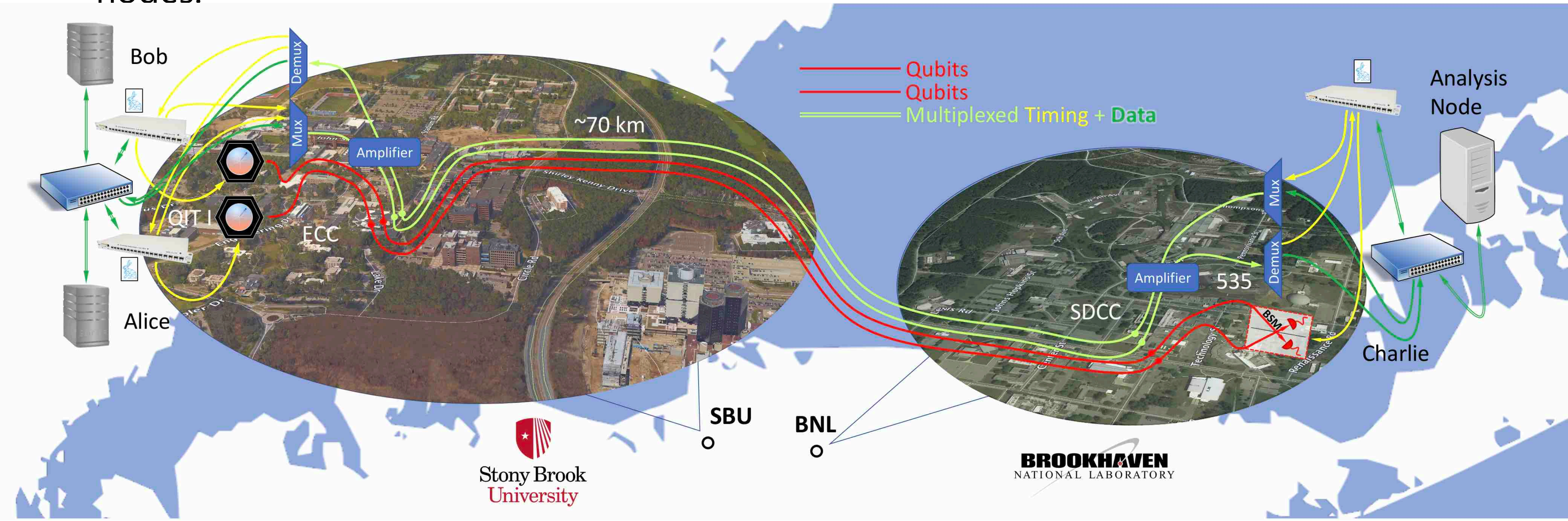
Collaboration/Sector Adoption

Plans to transfer technology/knowledge to end user:

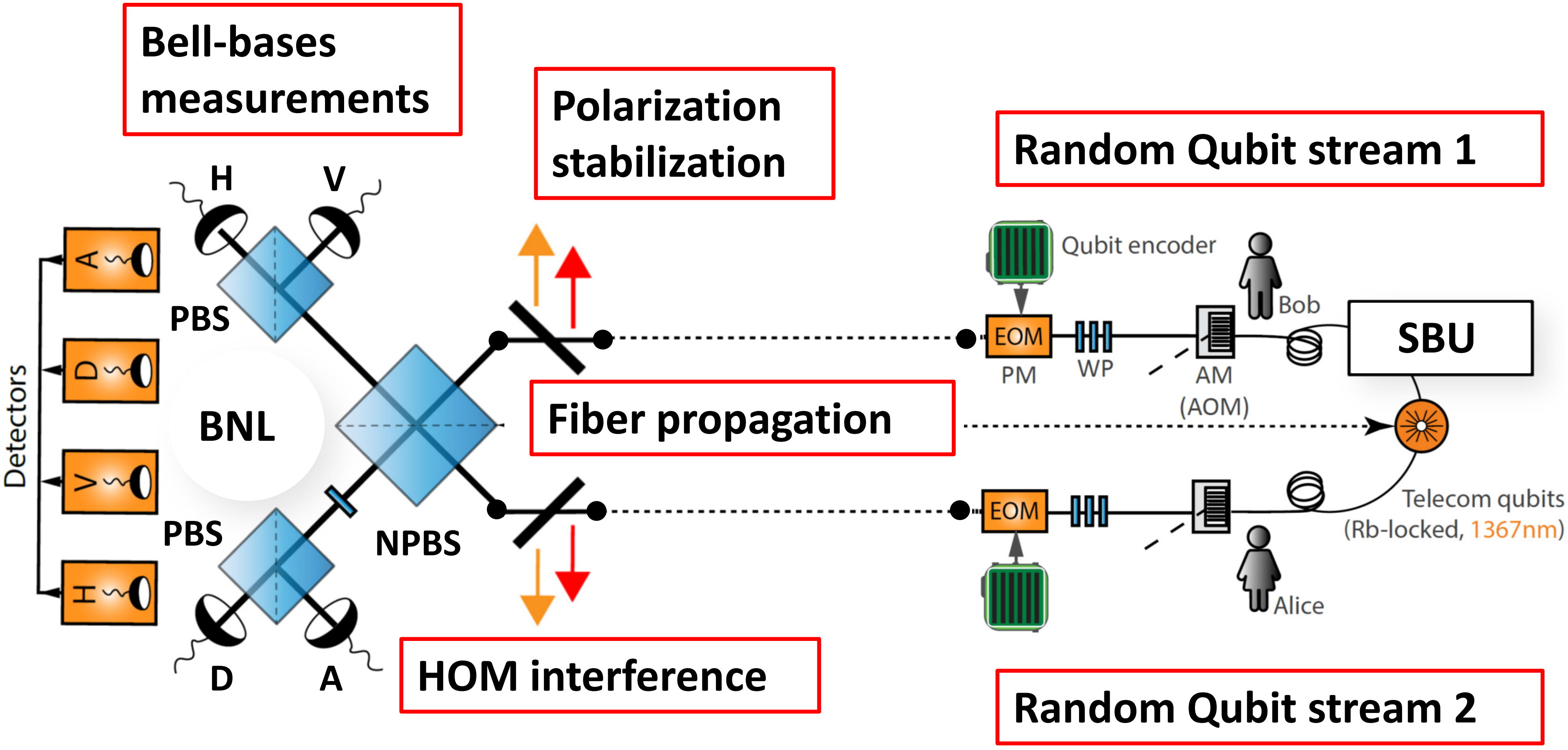
- With independent federal grants, SBU has developed patents regarding quantum communication technology (Provisional patent: PCT/US19/24601 (2019) and Provisional filling 62/909515 (2020)).
- As and example of further IP development, SBU has created a licensing agreement with Qunnect Inc, a startup company.
- A similar cooperative research and development agreement (CRADA) between SBU, BNL and other partners is in the works.
- In the context of Quantum Center creation, we have developed a consortium of industry partners interested in the applications of Quantum Communication.
  - NYS Technology Enterprise Corp, Qunnect, Quibtekk, TOPTICA Photonics, Quantonation, SeeQC, ID Quantique, Corning, ARCH Venture Partners, CenturyLink, NYSERNet, Internet2, ConEdison.
- As hybrid classical/quantum networks evolve, we will pursue an IP development strategy in the systems and algorithms parts.

Next Steps: Hybrid Quantum/Classical Net

- The quantum labs at BNL and SBU share four ~70km long fiber strands.
- Quantum signals: Alice and Bob (qubit generators) are located at SBU and Charlie (detectors) at BNL and utilizing one pair of fibers.
- Classical traffic: The data and timing/control network traffic will be multiplexed in the 2nd fiber pair using COTS DWDM networking technology.
- Currently implementing classical communication infrastructure and data analysis nodes.



Technical Aspects: Bell State Measurement



Bell-bases measurements

Polarization stabilization

Random Qubit stream 1

Fiber propagation

HOM interference

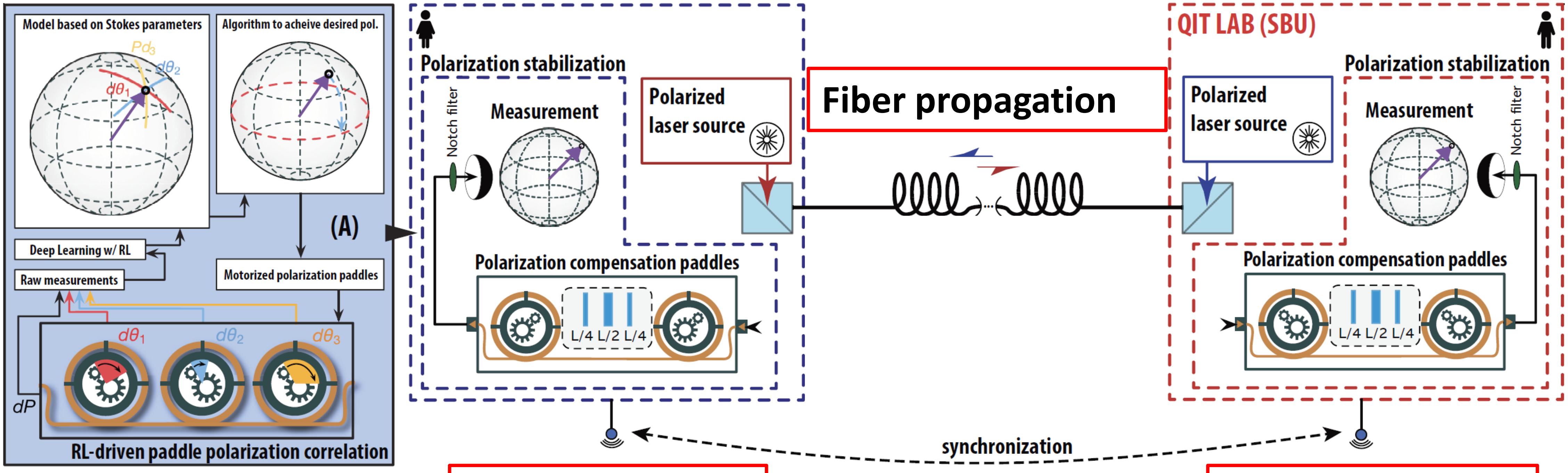
Random Qubit stream 2

- Random qubit electronics ready.
- Polarization stabilization in progress.
- BSM setup under construction.

Technical Aspects: Polarization Stabilization

ML polarization compensation

Bell measurement references


Model based on Stokes parameters
Pd_3
$d\theta_2$
$d\theta_1$
Algorithm to acheive desired pol.
(A)
Deep Learning w/ RL
Raw measurements
Motorized polarization paddles
$d\theta_1$
$d\theta_2$
$d\theta_3$
dP
RL-driven paddle polarization correlation
Polarization stabilization
Notch filter
Measurement
Polarized laser source
Polarization compensation paddles
L/4 L/2 L/4
QIT LAB (SBU)
Polarization stabilization
Polarized laser source
Measurement
Notch filter
Polarization compensation paddles
L/4 L/2 L/4
synchronization

Fiber propagation

In/out real-time polarization measurement

Switched H, V, A, D inputs

- ML algorithms ready.
- Proof of principle demonstrated, long-distance stabilization in progress (joint work with LANL, Raymond Newell).
- Optically-triggered network control under development.

Technical Aspects: MDI-QKD Data Analysis

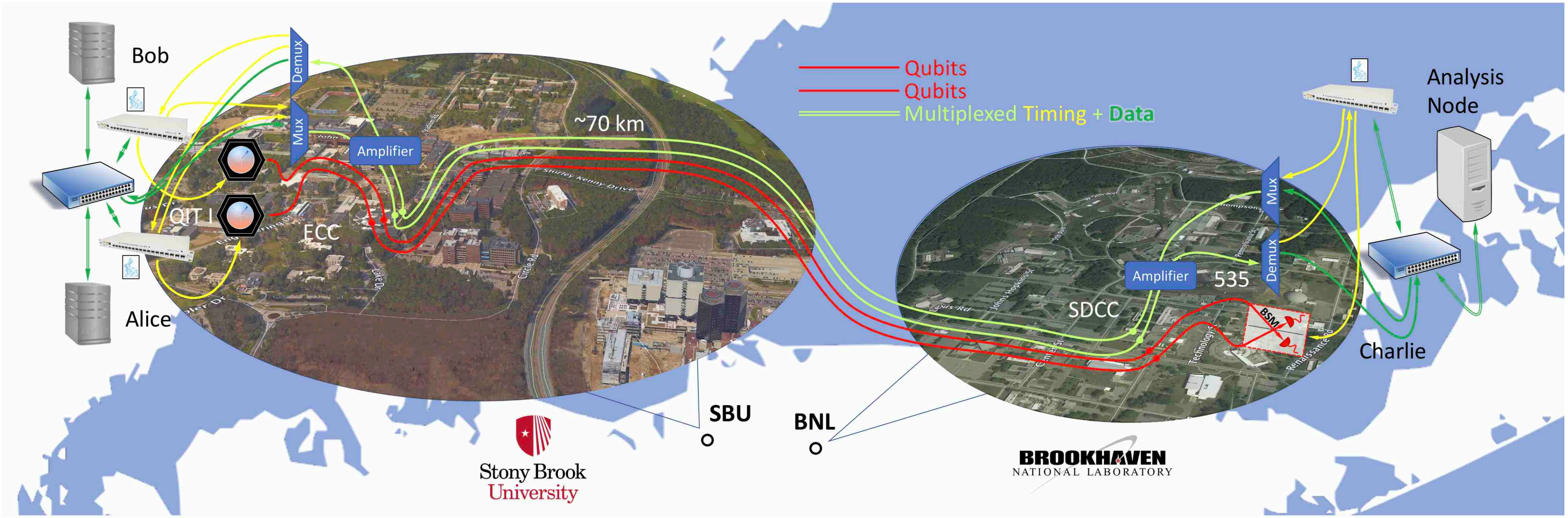
MDI QKD / Twin-field QKD

- **Quantum Communication (quantum-only part):**
  - State Preparation, Distribution, Measurement
- **Quantum Cryptography (quantum/classical part, joint work w/ORNL, Bing Qi):**
  1. **Sifting:** If Charlie reports a successful BSM result, Alice and Bob broadcast their intensity and basis settings.
  2. **Parameter estimation:** Compute the quantum bit error rate (QBER).
  3. **Error correction:** For those sets that passed the parameter estimation, we use information reconciliation schemes.
  4. **Privacy amplification:** Alice and Bob apply a random universal hash function to obtain secret key.
  5. **Key sharing:** Development of key-exchange algorithms to communicate quantum keys to data analysis nodes.

Goal: Proof of concept MDI QKD in the testbed by end of year 2.

Technical Aspects: Timing/Control + Data

- Timing nodes at all 3 stations will synchronize all devices to sub-nanosecond level using the White Rabbit protocol.
- A switch at SBU will be connected through the long fiber pair to a switch at BNL in a long-distance private network configuration for key-sharing and in-network analysis experiments.
- Timing, control, and data signals will be on different DWDM channels and will be multiplexed before entering and demultiplexed after exiting the long fibers.
- Two servers connected to the SBU switch will stream encrypted data (e.g., from Alice to Bob); the SBU switch will mirror the data streams to the analysis server at BNL, where the data will be analyzed in near-real time.
- Goal: establish setup resembling the targeted topology (slide #4) by end of year 2.



Technical Aspects: Utilizing Quantum Keys

Utilizing the quantum-generated keys in a classical context.

- The Analysis on the Wire project @ BNL has demonstrated in-network analysis of streaming unencrypted smart meter data (*"Electricity Load Forecasting with Collective Echo State Networks,"* SmartGridComm 2020).
- An in-network computation platform can accommodate execution of a wide range of algorithms for analysis and cybersecurity.
- What happens with encrypted data streams?
  - Analysis nodes must first decrypt and then process data – possible if encryption key can be shared.
- Encryption key sharing is possible.
  - Depending on application, key is accessible or can be extracted at Alice and/or Bob.
  - Classical encryption can be used for secure sharing (but can be broken by a quantum computer).
  - Assuming successful MDI QKD, initial iteration will use classical encryption for key sharing.
  - Further research for fully secure sharing is required (e.g., post-quantum encryption). Not in current project scope.
- Vision: develop combined quantum/hybrid system with secure key sharing capabilities in (possible) years 3 and 4.