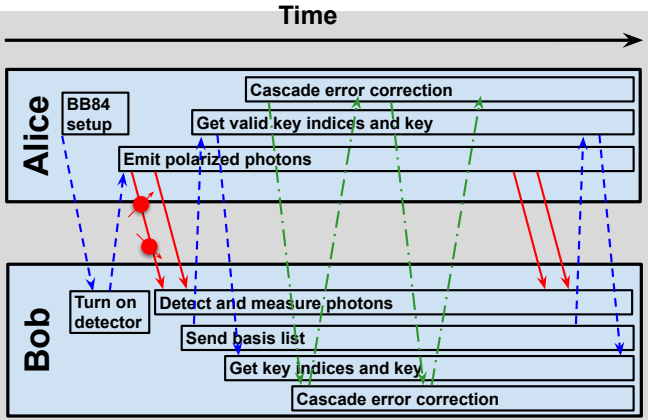
Securing Network Infrastructure with Quantum Protocols



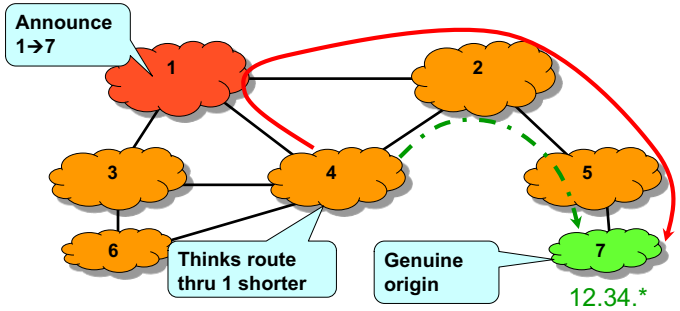
MARTIN SUCHARA

Argonne National Laboratory
msuchara@anl.gov

January 15, 2021
QuTCISS

ADDRESSING SECURITY SHORTCOMINGS OF THE TCP/IP NETWORK CONTROL PLANE

- TCP/IP networks suffer from many security vulnerabilities



- Development of the new quantum network control plane allows redesign
  - Secure protocols at all layers of the stack
  - Allow easy protocol “upgradability”

Scenario 1: use post-quantum cryptography

- Does not require significant changes in the data plane
- Key sizes too large for practical use, may lead to degraded performance
- No security guarantees, some schemes were broken

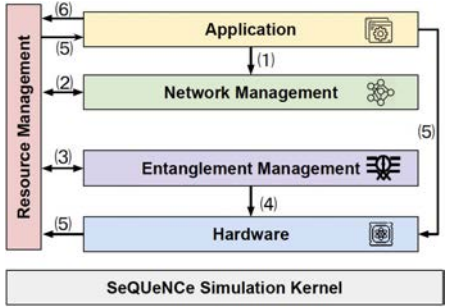
Scenario 2: use QKD and QDS protocols

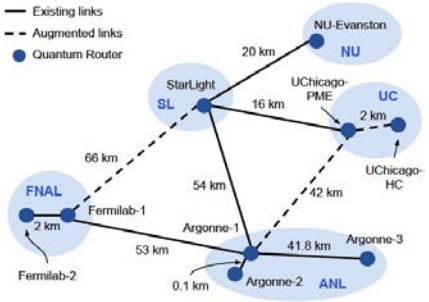
- Physical security guarantees
- Only solves confidentiality and integrity; vulnerable to availability threats
- Quantum digital signatures do not easily generalize to multiparty scenarios

SIMULATOR TO STUDY NETWORK ARCHITECTURE, PERFORMANCE, AND SECURITY

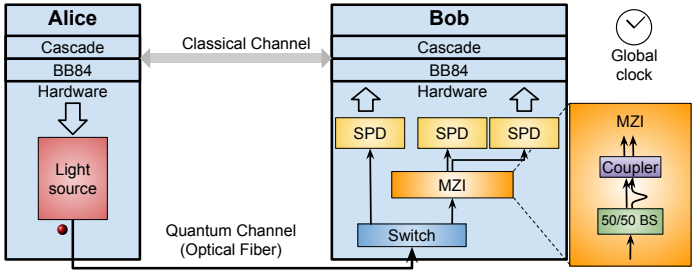
Argonne built Simulator of Quantum Network Communication (SeQUeNCe)

- Modularized design corresponds to the layers of the emerging quantum network protocol stack
- Implements protocols at all layers





Implemented BB84 and CASCADE with time-bin encoded qubits:



Future directions:

- Building secure protocols
  - E.g. secure routing with quantum position verification
- Standardization of quantum network protocols and architectures