# Classification of Quantum Repeater Attacks

Shigeya Suzuki, Rodney Van Meter

at SENT ’15, 8th February 2015, San Diego CA, USA

# Presentation Outline

- Quantum Repeater and its elements
- Model of Quantum Repeater
- Classification of Quantum Repeater Attacks

# Quantum Repeater and its elements

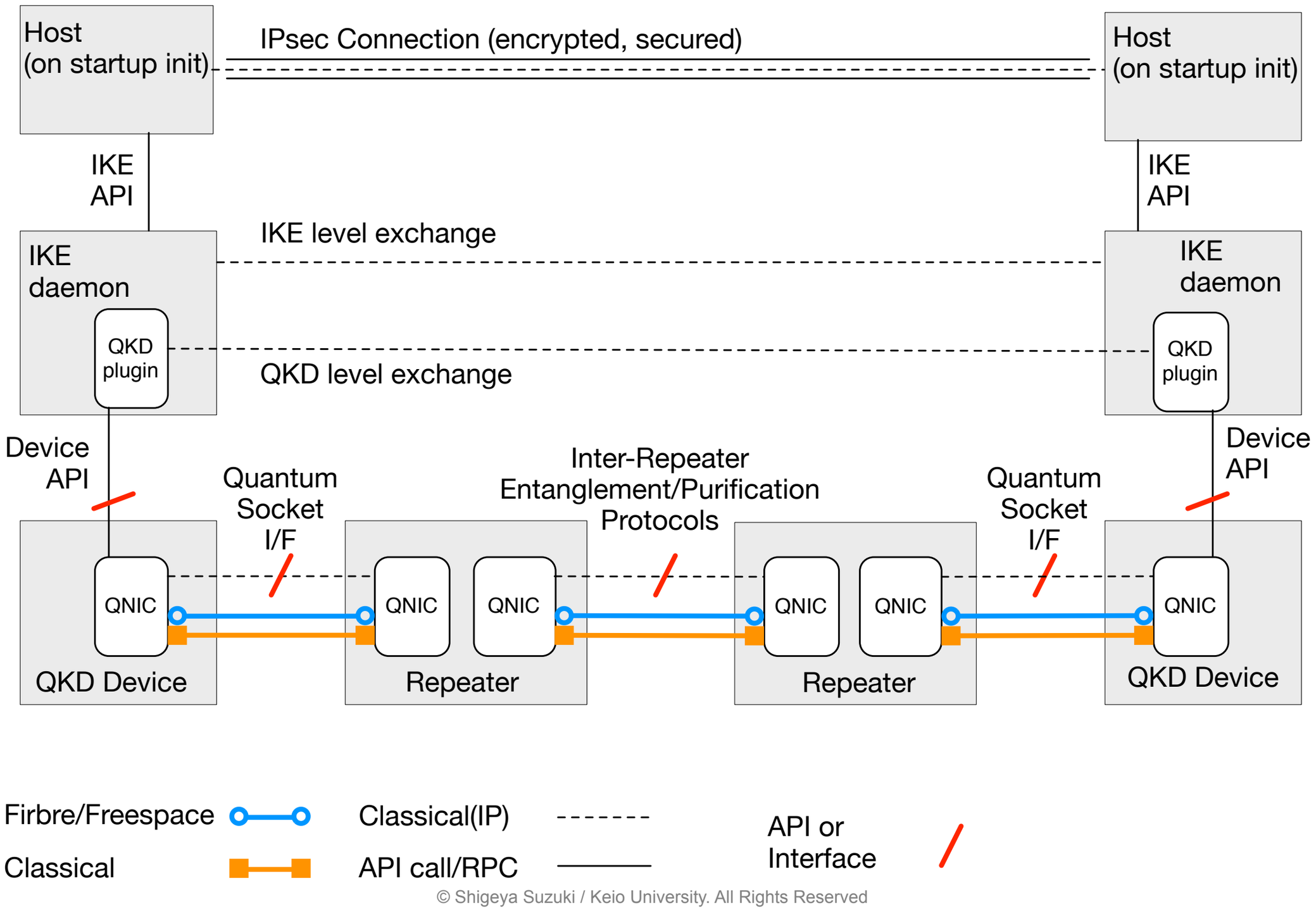
# Quantum Application and Repeater

- A quantum application, or its server will use quantum state teleported from client to do something interesting

- To create Quantum Internet, we need to have a way to application client to send a quantum state to a quantum application server

- Quantum repeater, which take the roles of a router in classical internet, is a key to create Quantum Internet

# Example

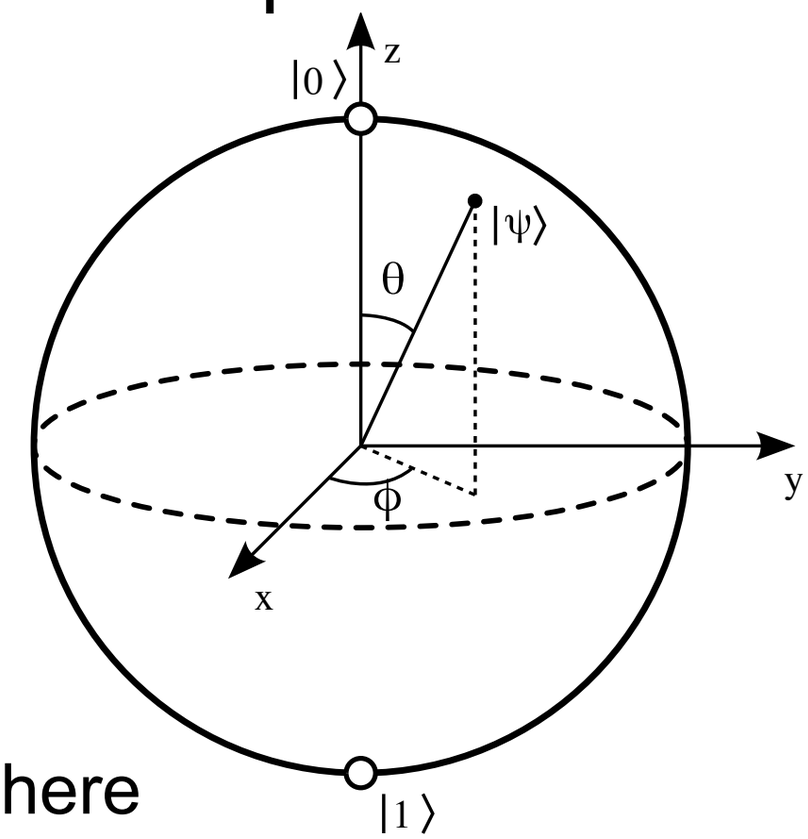


# Quantum Repeater Elements

- Qubits
- Fidelity of a Qubit
- Entanglement
- Bell Pair and Teleportation
- Fidelity and Purification
- Entanglement Swapping
- Multi-hop entanglement by Purification and Entanglement swap
- Quantum Repeater

# Qubits

- Each qubits represents single quantum state
- May hold either simple state or complex states like superposition
- Measuring the state of a qubit cause state collapse

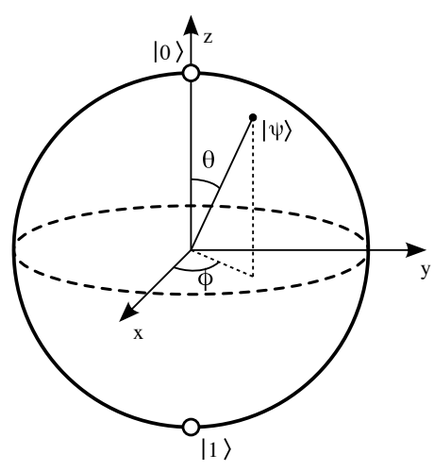



Bloch Sphere

By Glosser.ca, CC BY-SA 3.0, via Wikimedia Commons

# Fidelity of a Qubit

- How well the qubit hardware correctly represents the state we want to set is important
- Described by the *fidelity* of the qubit
  - e.g., you want set direction of the spin of an electron, and how close the spin actually points to your desired direction is the fidelity
- Essentially, it's the probability that the state does what you want  when you use/measure it

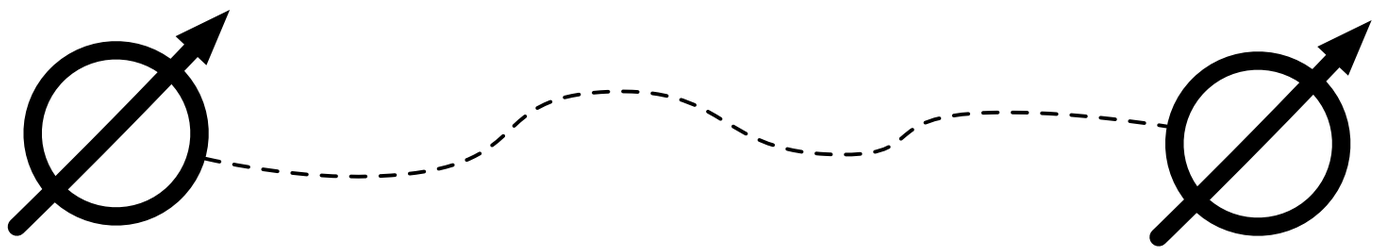


# Entanglement

- By using some known procedure, it is possible to create entangled pairs of qubits
- Some operations on one entangled qubit affects the other

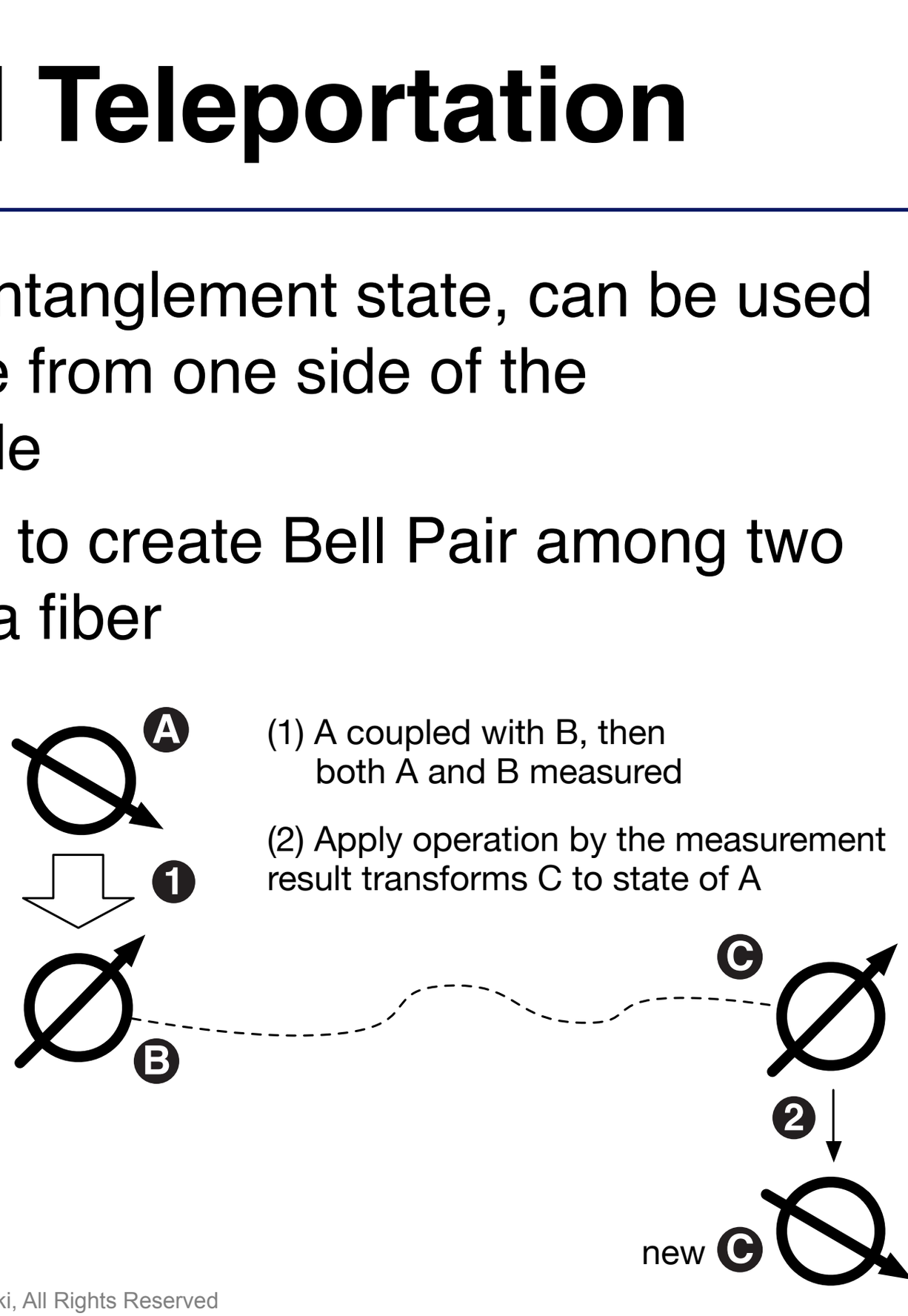
  ➡ does not mean we can remotely flip a qubit!
- Happens over any distance

  ➡ cannot be used to send data faster than light



# Bell Pair and Teleportation

- Bell Pair, which is a kind of entanglement state, can be used to teleport one quantum state from one side of the entanglement to the other side
- Current known scheme allow to create Bell Pair among two distant qubits connected via a fiber
- Requires supporting classical communication
- Destroys entanglement
  - ➡ so making more entanglement is the work of the network!



# Fidelity and Purification

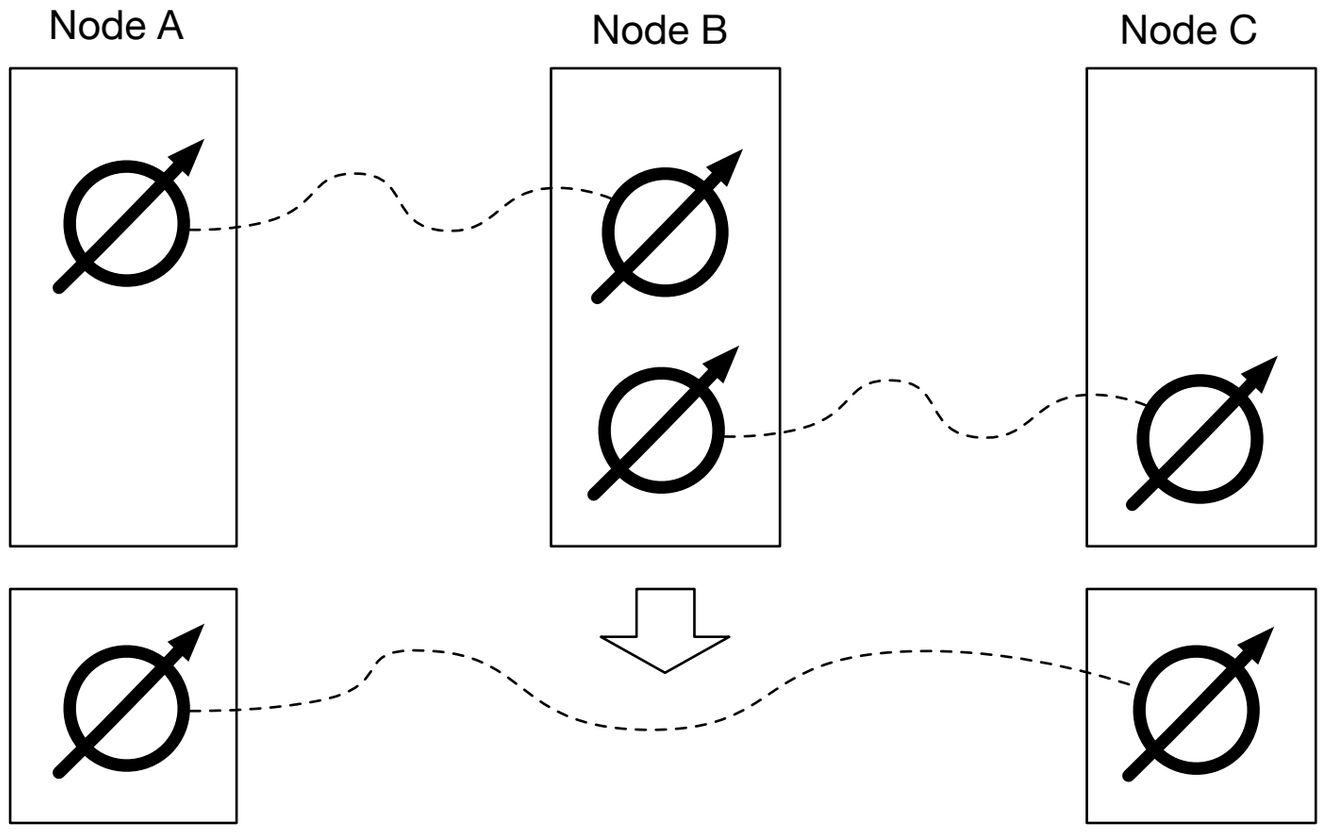
- Just created entanglement between two nodes may not have desired fidelity
- Various qubit operations may diminish fidelity, too

- To use for communication, either improve fidelity of the qubit or apply error correction scheme using multiple qubits

- Purification protocol creates single better fidelity entangled pair from two entangled pairs

# Entanglement Swapping

- Entanglement swapping operation extends distance of entangled qubits by splicing two pairs of entanglements into one




- After entanglement swapping, qubits in the middle node does not provide any role, can be reused

# Multi-hop entanglement by Purification and Entanglement swap

- By using purification and entanglement swap repeatedly in coordinated manner among nodes, we can create entangled qubits between any two user specified nodes

# Qubits - security point of view

- When Alice and Bob want to communicate, we want
  - Detect existence of any eavesdropper
  - To be sure Alice and Bob are actually communicating

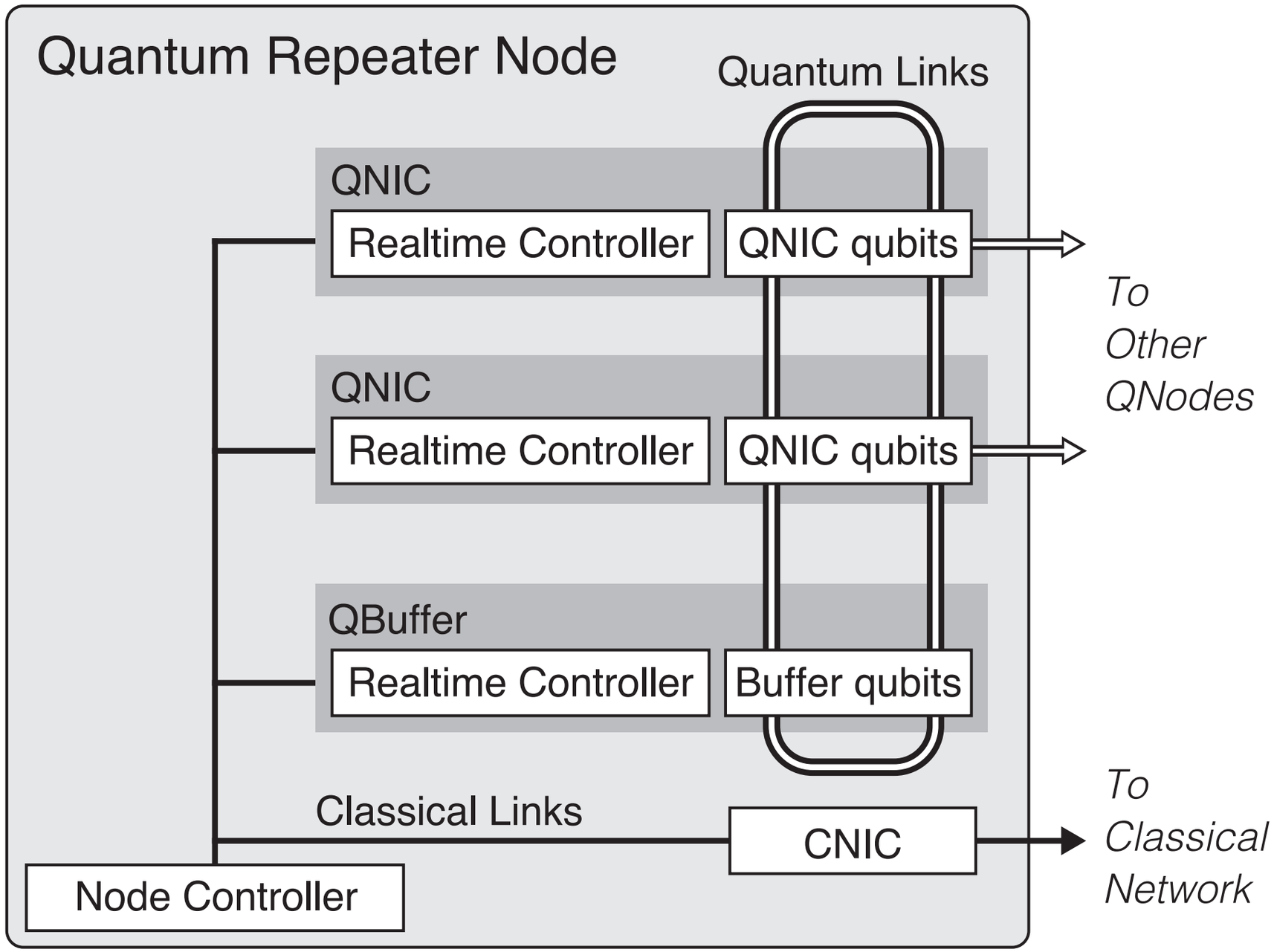
# Detection of eavesdroppers

- By applying quantum tomography on randomly select entangled qubits to detect eavesdropper

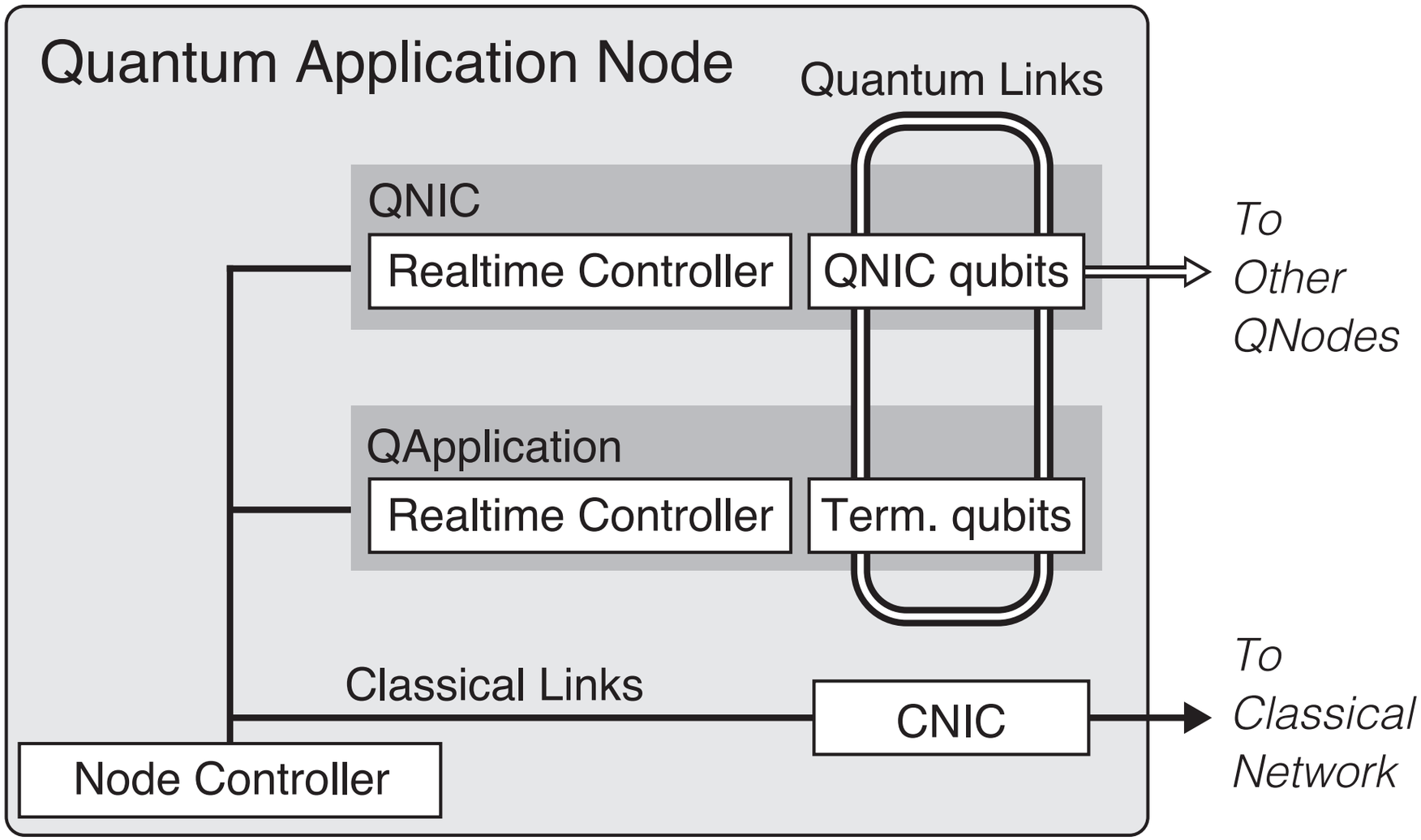
- But If an eavesdropper can predict the selection of qubits for quantum tomography, he/she can remain undetectable by not touching the selected qubit

# Model of Quantum Repeater System

# Quantum Repeater Node



# Quantum Application Node



# Peculiarities of Quantum Repeaters

- Quantum operation require classical communications
- Requires realtime operation
- Hop by hop decision on each router is not feasible

# Quantum operation require classical communications

- Many of the operation on entangled pair, or teleportation require communication using classical information system

# Requires Realtime operation

- Operation should be done in realtime, synchronized manner
  - All of the operation onto qubits must be controlled by realtime manner
  - Some of the operation among nodes should be done in accurately synchronized clocks

# Hop by hop decision is not feasible

- (Extending entanglement one hop at a time is not feasible)

- Creation of end-to-end entanglement require repeated and coordinated creation of entanglements among participating nodes in between two end nodes
  - Creation of an entangled pair require physical connection
  - Qubit's fidelity decays as time passes
    - Purification require two entangled pairs on same nodes

# Classification of Attacks

# Elements Grouping wrt attack vector characteristics

- Qubits
  - Terminal qubits
  - Interface qubits
  - Buffer qubits

- Channels
  - In-node quantum channels
  - Inter-node quantum channels
  - Inter-node classical channels

- Classical node resources

# Qubits

- Terminal qubits
  - Qubits used as interface to application. Has direct interface to application, but no direct interface to outside of the node
- Interface qubits
  - Qubits which has direct interface to outside of the node
- Buffer qubits
  - Qubits which works in between terminal qubits and interface qubits to work as buffers. No direct interface to application or outside of the node

# Channels

- In-node quantum channels
- Inter-node quantum channels

- Inter-node classical channels

# Classical node resources

- Node has usual classical components such as:
  - Power supply and external power
  - Clocks
  - Buses
  - etc, etc…

# Relationship with RFID system

- Quantum repeater systems and RFID systems has similar properties
- Both systems are tightly coupled hybrid systems of sensing and software elements, and also expect to make use of the effects of interaction with the outside world

- Due to this, We have referenced some of discussion on attack to RFID systems

# Attack to Qubits

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Terminal qubits | Eavesdropper detectable | Possibility of out-of-system attacks | Vulnerable to direct attacks and its variants, like classical system |
| Interface qubits | Eavesdropper detectable but direct attack to Quantum interface demonstrated | (same as above) | (same as above) |
| Buffer qubits | Eavesdropper detectable | (same as above) | (same as above) |

# Attack to Quantum Channels

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| In-node quantum channels | Safe | N/A | Vulnerable to direct attacks and its variants,<br>like classical system |
| Inter-node quantum channels | Eavesdropper detectable but direct attack to Quantum interface demonstrated | N/A | Vulnerable to direct attacks and its variants,<br>like classical system |

# Attack to Classical Channels and Classical node resources

| | Confidentiality | Integrity | Availability |
|---|---|---|---|
| Inter-node classical channels | Vulnerable to Classical Confidentiality attack possible | N/A | Vulnerable to Classical Availability attack possible |
| Classical node resources | Vulnerable to Classical Confidentiality attack possible | Vulnerable to Classical Integrity attack possible | Vulnerable to Classical Availability attack possible |

# Summary

- In this paper, we provided an model of a quantum repeater network and grouped elements of them, then, provided an analysis on a quantum repeater architecture based on our current knowledge
  - On confidentiality, quantum repeater systems have great advantage by applying quantum tomography to detect third party eavesdropper
  - On integrity and availability, a quantum repeater system seems to be not so different from a classical network system
- Since quantum repeater system heavily depends on classical information system, classical part is a key to make quantum repeater system secure

**Acknowledgements**

This research has been supported by
Asian Office of Aerospace Research and Development,
Air Force Office of Scientific Research under grant 144051