Integrating Quantum Concepts into Cyber Security

Session 2: Classical and Quantum Networks

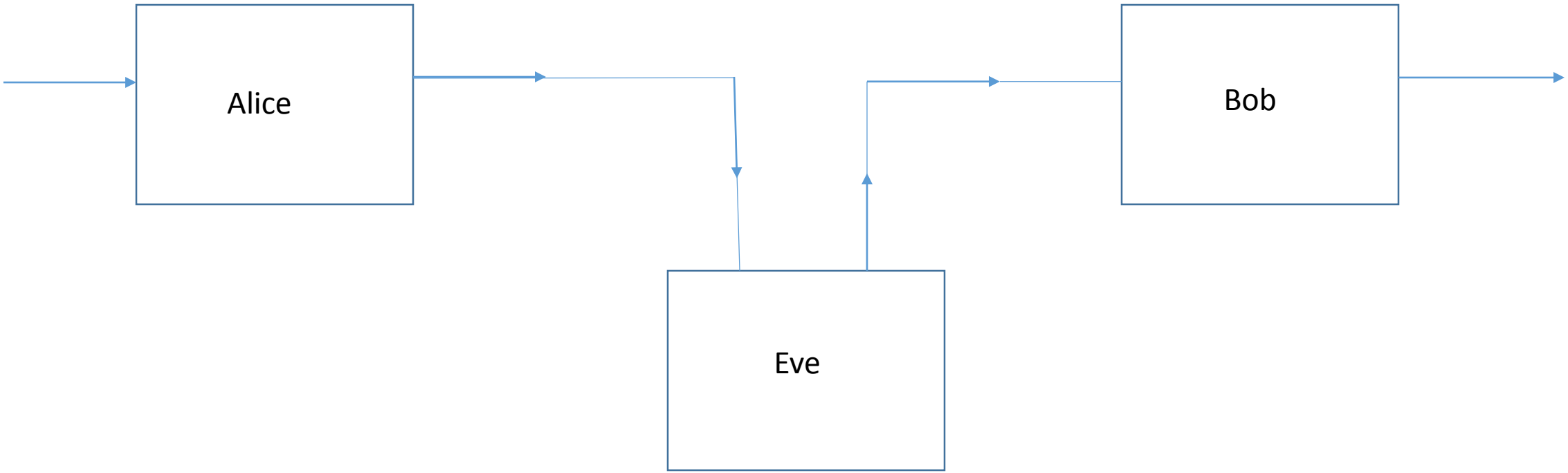
Dr William Joseph Spring

ACSAC 35, Condado Plaza Hilton, San Juan, Puerto Rico, USA

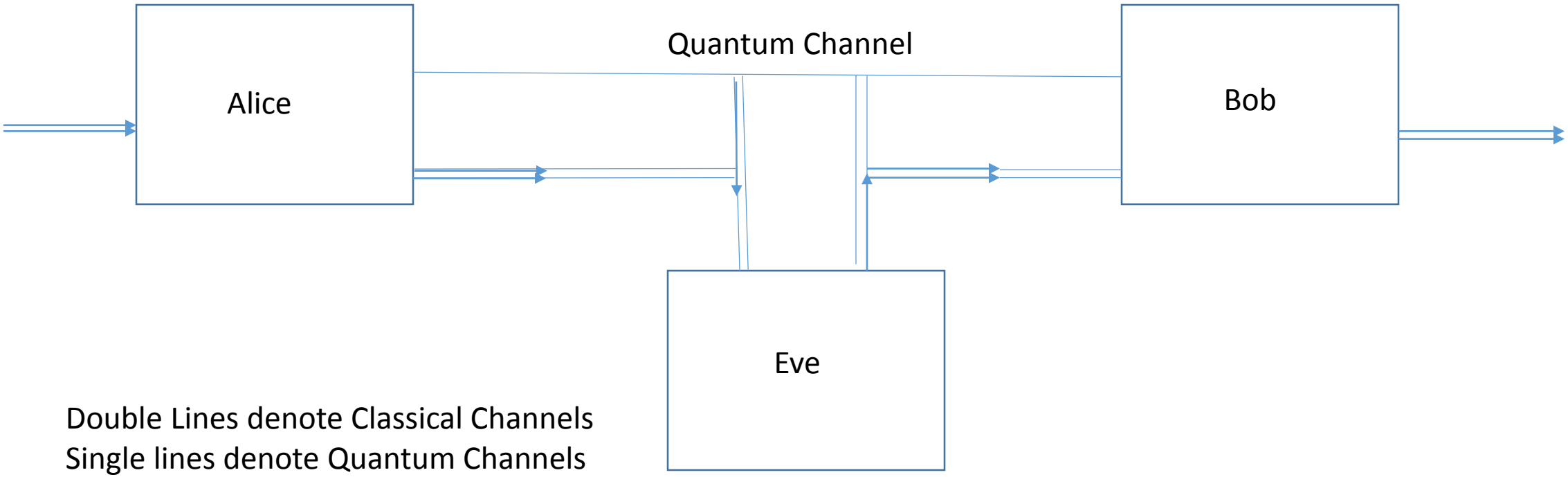
9th – 13th December 2019

Communication Channels

Standard Classical Communication Channel



Standard Quantum Communication Channel



Double Lines denote Classical Channels
Single lines denote Quantum Channels

Communication

Classical

- States represented by bits
  - Scalars
- Gates
  - Logical
  - AND, OR, NAND, NOR, …]
- Multipartite States
  - Nibbles, words, bytes, …
- Properties
  - Cloning
  - No Entanglement

Quantum

- States represented by qubits
  - Vectors
- Gates
  - Matrices
  - Hadamard, Pauli, CNOT, …
- Multipartite States
  - Tensor products of states
- Properties
  - No Cloning
  - Entanglement

Quantum Tools

The tools employed include and are not limited to

- States
  - Superposition, Entanglement, No cloning
- Gates
  - Hadamard, CNOT, Pauli, … , Unitary (Reversible)
- Measurement
  - Via self adjoint operators, (not Reversible, in general)
  - Outcomes real valued eigenvectors of measurement operators
- Multipartite States
  - Represented using tensor products

- Applications
  - Networks, Teleportation, Quantum Key Agreement, Authentication, Integrity, …
- Resources
  - Entanglement and Entanglement Swapping, No Cloning

Activity 2a - Threat Models

Activity 2a

1. Draw the quantum communication model from the slides.
2. Explain what is meant by entanglement.
3. Draw the circuit for generating EPR (Einstein, Podolsky, Rosen) pairs and derive the four Bell states that can be produced.
4. Alice the sender encodes bits using the Z basis and sends these as photons to Bob the receiver. Describe a possible threat to the quantum channel. What steps would you advise to block the threat described? Hence describe an improved model for the communication protocol. Could entanglement help?
5. What threats do you feel the above protocol could be susceptible to if entanglement was employed?

Networks and Distributed Systems

Introduction

- Recent developments in technology for quantum based repeaters have extended the range available for communicating information enabling the potential for realising quantum networks, distributed systems and a quantum based internet.
- Quantum repeaters employing entanglement swapping are currently reported as achieving distances in excess of 100km together with reports of direct peer to peer quantum key distribution also in excess of 100km.
- Quantum based networks are under development with a range of 2000km, with private commercial quantum communication networks already reported as completed.

Azuma. K, et al (2015) All Photonic Quantum Repeaters, Nature Communications

Ren, Ji-Gang, et al (2017) Ground to satellite Quantum Teleportation, arXiv:1707.00934

Introduction

- Quantum processing promises the possibility for obtaining solutions to a range of ‘difficult’ problems.
- From a security perspective this involves the possibility of
  - Breaking Asymmetric Key Algorithms via Shor’s Algorithm
    - The RSA algorithm based on the IFP (Integer Factorisation Problem)
    - The El Gamal algorithms based on the DLP (Discrete Logarithm Problem)
  - Working in secure communication channels for ‘free’
  - Detecting eavesdroppers on a communication channel
  - Developing quantum based cryptographic schemes
  - Detecting intruders within a system
  - Developing new insights for a range of different fields

What is a Quantum Distributed System?

- Harry Buhrman and Hein Röhrig:
  - Under the heading of *Applications in Distributed Computing three models of quantum communication are presented:*
    - *Communication via qubits*
      - *BB84, B92*
    - *Parties share EPR pairs but communication is via a classical bit channel*
      - *Teleportation*
    - *Parties share EPR pairs and communicate via qubits*
      - *Entanglement Swapping*

What is a Quantum Distributed System?

- Rodney van Meter:
  - Quantum Communication is ‘the exchange of quantum states over a distance, generally requiring the support of substantial classical communication’
  - *Quantum networks may be described as operating in at least three modes*
    - *The teleportation of (quantum) states*
    - *The teleportation of (quantum) gates*
    - *The creation of distributed quantum states*

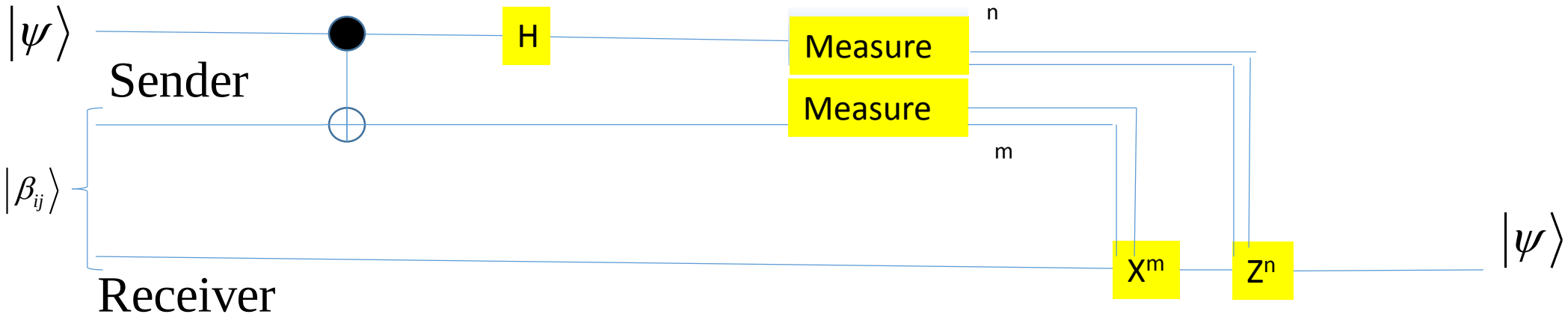
What is a Quantum Distributed System?

- Rodney van Meter:
  - To make use of proposed h/w platforms (ion traps, quantum dots, NV diamond) which offer ‘good optical connections … monolithic computation’ needs to be split into ‘pieces for distributed computation’
  - Three categories of distributed quantum application:
    - Distributed numeric computation (in which knowledge of input data, algorithms used and output data are unknown by server)
    - Cryptographic functions (include secret key generation, Byzantine agreement and secret sharing)
    - Sensor or cybernetic services (high precision interferometry, clock synchronisation)

Communication via Qubits

Parties share EPR pairs but communication is via a classical bit channel

Teleportation



A gate based circuit for teleporting a state from sender to receiver

Multipartite States

For multipartite states we have vectors of the form

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \otimes \ldots \otimes |\psi_n\rangle = |\psi_1\rangle|\psi_2\rangle|\psi_3\rangle \ldots |\psi_n\rangle = |\psi_1 \ \psi_2 \ \psi_3 \ \ldots \ \psi_n\rangle$$

With corresponding density operators

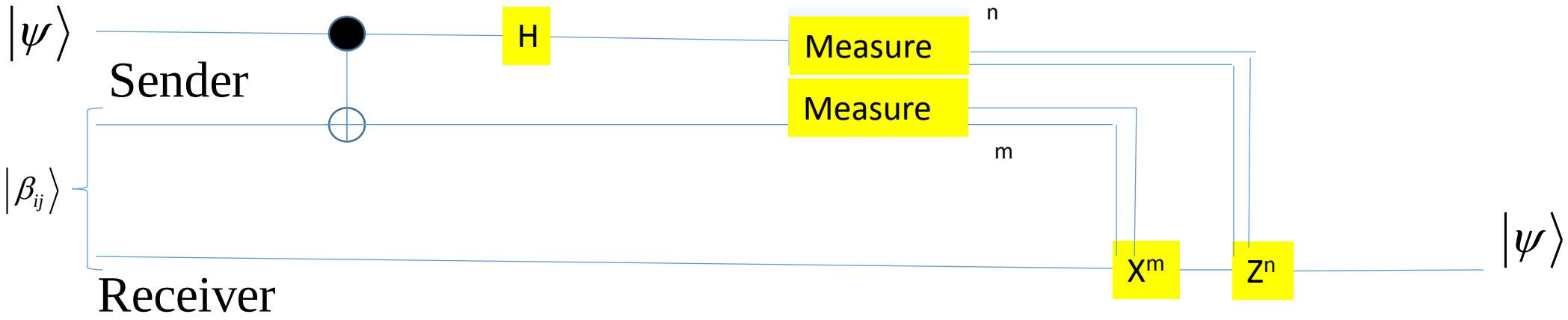
$$\rho = \rho_1 \otimes \rho_2 \otimes \rho_3 \otimes \ldots \otimes \rho_n = \rho_1 \ \rho_2 \ \rho_3 \ \ldots \rho_n$$

In which

$$|\psi_i\rangle \text{ denotes a qubit and } \rho_i = |\psi_i\rangle\langle\psi_i|$$

This leads us to the concept of entanglement, a major resource in QIP (Quantum Information Processing)

Teleportation



A gate based circuit for teleporting a state from sender to receiver

Entangled States – Major Resource

Two fundamental views

- Algebraically no common vector factors, irreducible, prime states
- Correlation View – Entangled photons are seen to be correlated or anti-correlated (both spin up or both spin down as opposed to one spin up and the other spin down)
- Examples:
  - Bell states, GHZ states, W states

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

- Partial entanglement for subsystems of a general system also used

Gate Based

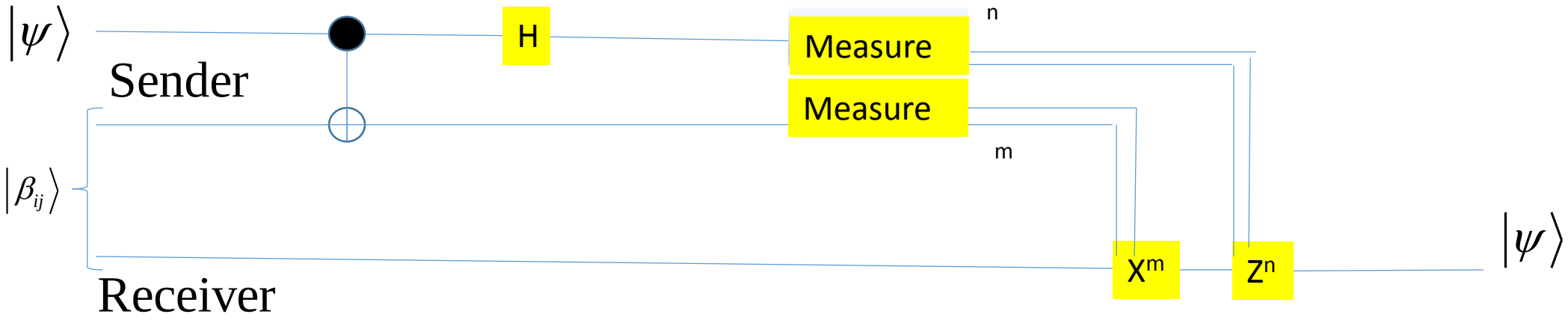
- A gate based quantum circuit is one in which a series of unitary (self inverse) operators (matrices) are applied and possibly followed by a final measurement to obtain a classical outcome
- The unitary operators can, for example, involve the Pauli gates, the Hadamard, CNOT, Phase gates, …
- Examples
  - generating Bell states
  - Teleportation

A gate based circuit for generating a Bell state

Teleportation

- Sender has unknown quantum state that they wish to send to a receiver
- Cannot measure (generally changes the state) or take copies (No Cloning Theorem)
- Resource: Sender and Receiver share
  - an EPR channel (Bell state)
  - and a classical channel

Teleportation



A gate based circuit for teleporting a state from sender to receiver

Teleportation Protocol

$$\text{Let } |\psi\rangle|\beta_{ij}\rangle$$

$$= (\alpha|0\rangle + \beta|1\rangle)(\frac{|0\,j\rangle + (-1)^i|1\bar{j}\rangle}{\sqrt{2}})$$

$$= \frac{1}{\sqrt{2}}(\alpha|00\,j\rangle + (-1)^i\alpha|01\bar{j}\rangle + \beta|10\,j\rangle + (-1)^i\beta|11\bar{j}\rangle)$$

$$\text{Applying } CNOT \otimes I$$

$$\mapsto \frac{1}{\sqrt{2}}(\alpha|00\,j\rangle + (-1)^i\alpha|01\bar{j}\rangle + \beta|11\,j\rangle + (-1)^i\beta|10\bar{j}\rangle)$$

$$\text{Now applying } H \otimes I \otimes I$$

$$\mapsto \frac{1}{\sqrt{2}}(\alpha|+0\,j\rangle + (-1)^i\alpha|+1\bar{j}\rangle + \beta|-1\,j\rangle + (-1)^i\beta|10\bar{j}\rangle)$$

$$= \frac{1}{2}(|00\rangle(\alpha|\,j\rangle + (-1)^i\beta|\,\bar{j}\rangle) + |01\rangle(\beta|\,j\rangle + (-1)^i\alpha|\,\bar{j}\rangle)$$

$$+|10\rangle(\alpha|\,j\rangle - (-1)^i\beta|\,\bar{j}\rangle) - |11\rangle(\beta|\,j\rangle - (-1)^i\alpha|\,\bar{j}\rangle))$$

Teleportation

Measuring w.r.t. the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ *generates either* $|\psi\rangle, X|\psi\rangle, Z|\psi\rangle$ or $ZX|\psi\rangle$ each of which produce $|\psi\rangle$

Activity 2b - Threat Models

Teleportation Model

Activity 2b - Teleportation

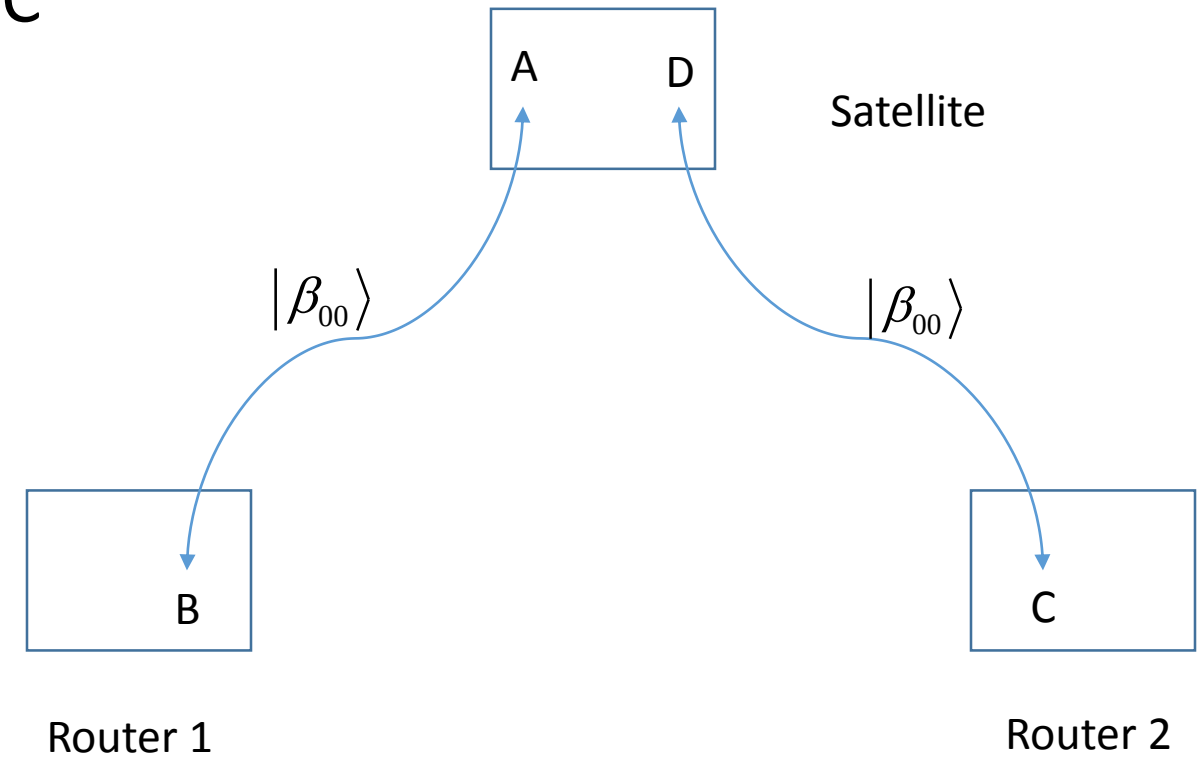
1. In the teleportation protocol above derive the last line for the Bell state with i = j = 0.
2. What are the possible outcomes for Bobs photon after measurement by the sender Alice?
3. Hence what would Bob have to do to the photon at the receivers side of the protocol in order to reconstruct the unknown quantum state that the sender had?
4. Does the teleportation protocol give us communication at the speed of light?
5. Does Alice still have the unknown quantum state and Bob now have a copy?

Communication via Qubits

Parties share EPR pairs and communicate via qubits

Entanglement Swapping

- Satellite generates two entangled Bell states, one at A and one at D
- One of the two photons at A is sent to B; and likewise one is sent from D to C



Entanglement Swapping

Let $|\beta_i\rangle_{AB}$ and $|\beta_j\rangle_{CD}$ denote two Bell states with $i, j \in \{0 = 00, 1 = 01, 2 = 10, 3 = 11\}$ such that $|\beta_i\rangle_{AB}$ denotes entanglement between A and B and $|\beta_j\rangle_{CD}$ denotes entanglement between C and D.

Then $|\beta_i\rangle_{AB}|\beta_j\rangle_{CD} = \sum_{k=0}^{3} |\beta_{(i+k) \bmod 4}\rangle_{AD} |\beta_{j+(-1)^{(i+j)}k \bmod 4}\rangle_{BC}$

We consider the case for $|\beta_0\rangle_{AB}|\beta_0\rangle_{CD} = |\beta_{00}\rangle_{AB}|\beta_{00}\rangle_{CD}$ with $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Entanglement Swapping

Let $|\psi\rangle$ denote the state vector for the system. Then $|\psi\rangle$

$$= |\beta_{00}\rangle_{AB} |\beta_{00}\rangle_{CD}$$

$$= \frac{1}{2}(|00\rangle_{AB} |00\rangle_{CD} + |00\rangle_{AB} |11\rangle_{CD} + |11\rangle_{AB} |00\rangle_{CD} + |11\rangle_{AB} |11\rangle_{CD})$$

$$= \frac{1}{2}(|00\rangle_{AD} |00\rangle_{BC} + |11\rangle_{AD} |11\rangle_{BC} + |01\rangle_{AD} |01\rangle_{BC} + |10\rangle_{AD} |10\rangle_{BC})$$

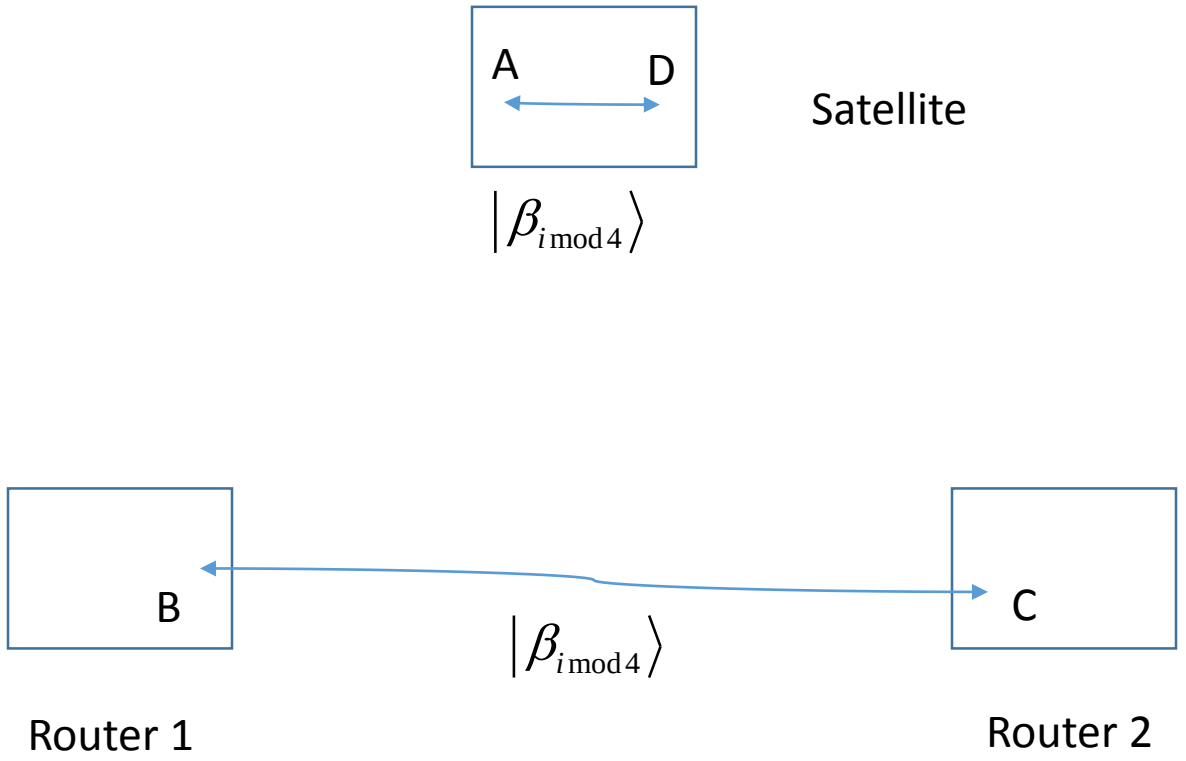
$$= \frac{1}{2\sqrt{2}}(|00\rangle_{AD} (|\beta_{00}\rangle + |\beta_{10}\rangle)_{BC} + |11\rangle_{AD} (|\beta_{00}\rangle - |\beta_{10}\rangle)_{BC} + |01\rangle_{AD} (|\beta_{01}\rangle + |\beta_{11}\rangle)_{BC} + |00\rangle_{AD} (|\beta_{01}\rangle - |\beta_{11}\rangle)_{BC})$$

$$= \frac{1}{2}(|\beta_{00}\rangle_{AD} |\beta_{00}\rangle_{BC} + |\beta_{01}\rangle_{AD} |\beta_{01}\rangle_{BC} + |\beta_{10}\rangle_{AD} |\beta_{10}\rangle_{BC} + |\beta_{11}\rangle_{AD} |\beta_{11}\rangle_{BC})$$

Taking a Bell measurement w.r.t AD (local) we obtain a particular (global) Bell state w.r.t BC

Entanglement Swapping

- Taking a local measurement of the two satellite photons at A and D results in establishing a global EPR channel between B and C



Quantum Heterogeneity

- Quantum Networks
  - Fibre Optic Networks, Free Space Networks, Cavity – QED Networks
  - DARPA QKD Network (2001),
  - SECOQC QKD Network (Vienna) Secure Communication based on Quantum Cryptography, (2003)
  - Tokyo QKD Network, (2009)
  - Hierarchical Network, Wuho, China, (2009)
  - Geneva Area Network (SwissQuantum)
  - Shanghai – Beijing 2000km Network (2016)
- Quantum Hardware
  - Phase 2: Engineering improvements in repeaters, quantum CPU's: The Sycamore Processor and quantum supremacy (
- Quantum Operating Systems
  - Cambridge Quantum Computing (CQCL) new o/s t|ket>
- Quantum Programming Languages
  - Quantum Imperative Paradigm
    - Quantum Pseudocode, QCL - Quantum Computing Language, Q Language, qGCL, LanQ, Qiskit
  - Quantum Functional Paradigm
    - QFC, QPL, QML, Quipper

Activity 2b - Threat Models

Entanglement Swapping

Activity 2b – Teleportation and Entanglement Swapping

1. In theory could you set up entanglement between the North and South pole?
2. If entanglement swapping is employed in a point to point manner from router to router between sender and receiver, with storage at the router prior to sending on the next stage what security implications do you perceive with respect to the teleportation protocol?