Quantum Communication Topics

Principle of Entanglement

Superdense Coding

Quantum Teleportation

BB84 Secure Key Distribution Protocol

1

Qubit Entanglement Summary

Qubit Interaction through the Entanglement Principle

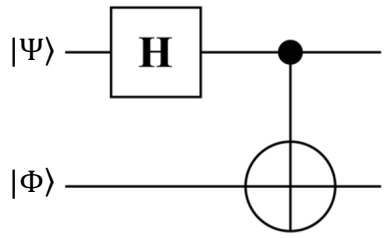
2

Bell States

- Bell States* are four canonical examples of 2-qubit bipartite entanglement
- A Bell State Generator circuit evolves two fiduciary states qubits into 4 different quantum states of entanglement
  - typically: one Hadamard and one Controlled-$\mathbf{X}$
- Many other circuits can generate entangled pairs
- Other types of canonical entanglement states exist
  - Greenberger-Horne-Zeilinger (*GHZ*) states – *M*-qubit bipartite entanglement
  - *W* states – *M*-qubit *M*-partite entanglement
  - Higher-dimensioned (qudit) Extensions

3

Bell State Generator



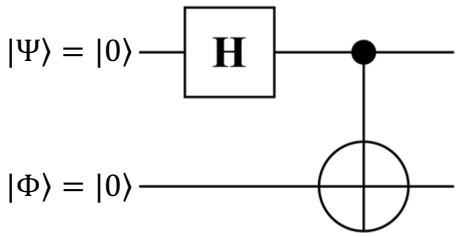
$$\mathbf{T} = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I})$$

$$\mathbf{T} = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \left(\frac{1}{\sqrt{2}}\right) \left(\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) = \left(\frac{1}{\sqrt{2}}\right) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

$$\mathbf{T} = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I}) = \left(\frac{1}{\sqrt{2}}\right) \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right) \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix}$$

4

Bell State, $|\Phi^+\rangle$



- Initialize 2 Qubits to Fiduciary State
  - "ground" states of computational basis

$$|\Psi\Phi\rangle = |00\rangle \rightarrow |\Phi^+\rangle$$

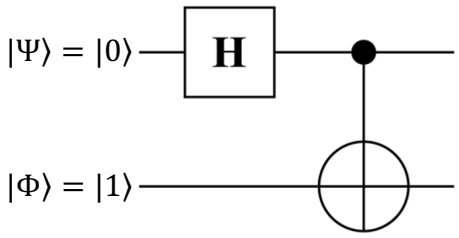
$$\mathbf{T} = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I}) = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}$$

$$|\Phi^+\rangle = \mathbf{T}|00\rangle = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I})|00\rangle = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

5

Bell State, $|\Psi^+\rangle$



- Initialize 2 Qubits to Fiduciary State
  - "ground/excited" states of computational basis

$$|\Psi\Phi\rangle = |01\rangle \rightarrow |\Psi^+\rangle$$

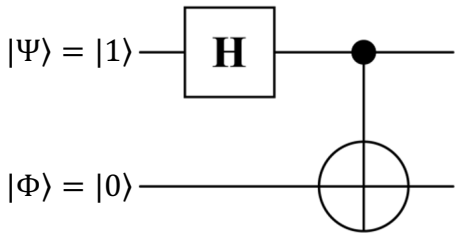
$$\mathbf{T} = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I}) = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}$$

$$|\Psi^+\rangle = \mathbf{T}|01\rangle = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I})|01\rangle = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}\begin{bmatrix}0\\1\\0\\0\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}0\\1\\1\\0\end{bmatrix} = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

6

Bell State, $|\mathbf{\Phi^-}\rangle$



- Initialize 2 Qubits to Fiduciary State
  - "excited/ground" states of computational basis

$$|\Psi\Phi\rangle = |10\rangle \rightarrow |\mathbf{\Phi^-}\rangle$$

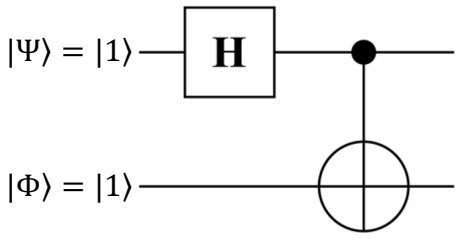
$$\mathbf{T} = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I}) = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}$$

$$|\mathbf{\Phi^-}\rangle = \mathbf{T}|10\rangle = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I})|10\rangle = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}\begin{bmatrix}0\\0\\1\\0\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1\\0\\0\\-1\end{bmatrix} = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\mathbf{\Phi^-}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

7

Bell State, $|\mathbf{\Psi^-}\rangle$



- Initialize 2 Qubits to Fiduciary State
  - "excited" states of computational basis

$$|\Psi\Phi\rangle = |11\rangle \rightarrow |\mathbf{\Psi^-}\rangle$$

$$\mathbf{T} = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I}) = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}$$

$$|\mathbf{\Psi^-}\rangle = \mathbf{T}|11\rangle = \mathbf{C_X}(\mathbf{H} \otimes \mathbf{I})|11\rangle = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}\begin{bmatrix}0\\0\\0\\1\end{bmatrix} = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}0\\1\\-1\\0\end{bmatrix} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

$$|\mathbf{\Psi^-}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

8

Four Canonical Bell States*

$$|\mathbf{\Phi}^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\Psi\Phi\rangle = |00\rangle \rightarrow |\mathbf{\Phi}^+\rangle$$

$$|\mathbf{\Psi}^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\Psi\Phi\rangle = |01\rangle \rightarrow |\mathbf{\Psi}^+\rangle$$

$$|\mathbf{\Phi}^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \qquad |\Psi\Phi\rangle = |10\rangle \rightarrow |\mathbf{\Phi}^-\rangle$$

$$|\mathbf{\Psi}^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} \qquad |\Psi\Phi\rangle = |11\rangle \rightarrow |\mathbf{\Psi}^-\rangle$$

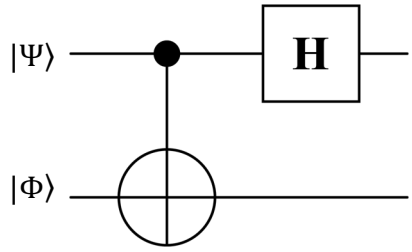
These are special cases of "EPR Pairs" – two entangled qubits - in reference to the 1935 paper† by Einstein, Podolsky and Rosen

†Einstein A, Podolsky B, Rosen N. Can quantum-mechanical description of physical reality be considered complete?. Physical review. 1935 May 15;47(10):777

*Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. Physical review letters. 1993 Mar 29;70(13):1895.

9

Detangling Bell States



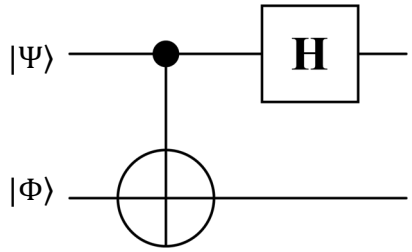
$$\mathbf{T}_{det} = (\mathbf{H} \otimes \mathbf{I})\mathbf{C}_\mathbf{X}$$

$$\mathbf{T}_{det} = (\mathbf{H} \otimes \mathbf{I})\mathbf{C}_\mathbf{X} = \left(\tfrac{1}{\sqrt{2}}\right)\left(\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} = \begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{bmatrix}\left(\tfrac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

$$\mathbf{T}_{det} = (\mathbf{H} \otimes \mathbf{I})\mathbf{C}_\mathbf{X} = \left(\tfrac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} = \left(\tfrac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\\ 1 & 0 & 0 & -1\\ 0 & 1 & -1 & 0\end{bmatrix}$$

10

Detangling the $|\Phi^+\rangle$ Bell State - Example



$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\mathbf{T}_{det}|\Phi^+\rangle = (\mathbf{H} \otimes \mathbf{I})\mathbf{C_X}|\Phi^+\rangle$$

$$\mathbf{T}_{det}|\Phi^+\rangle = (\mathbf{H} \otimes \mathbf{I})\mathbf{C_X}|\Phi^+\rangle = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\\ 1 & 0 & 0 & -1\\ 0 & 1 & -1 & 0\end{bmatrix}\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\\ 1 & 0 & 0 & -1\\ 0 & 1 & -1 & 0\end{bmatrix}\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix}1\\0\\0\\1\end{bmatrix}$$

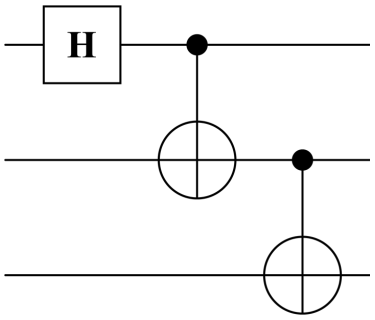
$$\mathbf{T}_{det}|\Phi^+\rangle = (\mathbf{H} \otimes \mathbf{I})\mathbf{C_X}|\Phi^+\rangle = \left(\frac{1}{2}\right)\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\\ 1 & 0 & 0 & -1\\ 0 & 1 & -1 & 0\end{bmatrix}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \left(\frac{1}{2}\right)\begin{bmatrix}2\\0\\0\\0\end{bmatrix} = \frac{2|00\rangle}{2} = |00\rangle$$

11

Greenberger-Horne-Zeilinger (*GHZ*) States

- *GHZ* states are Bipartite
- Example of a 3-qubit *GHZ* state and generator
- Generalized Bell State generator

$$|GHZ_3\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$



- General form for $M \geq 3$ qubits:

$$|GHZ_M\rangle = \frac{|0\rangle^{\otimes M} + |1\rangle^{\otimes M}}{\sqrt{2}}$$

GHZ Generator Circuit adds more qubits at bottom of circuit with an additional Controlled-**X** (*CNOT* or $\mathbf{C_X}$) gate for each additional qubit

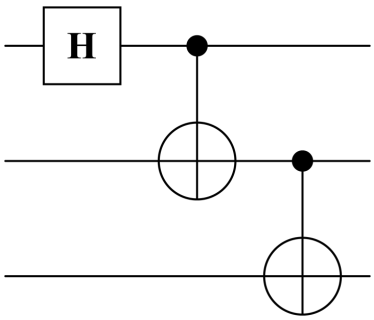
* D. Greenberger, M. Horne and A. Zeilenger, "Going Beyond Bell's Theorem," in **Bell's Theorem, Quantum Theory and Conceptions of the Universe**, Springer Publishers, Dordrecht, Netherlands, October 31, 1989, pp. 69-72.

12

Greenberger-Horne-Zeilinger (GHZ) States

- GHZ states are Bipartite, General Form:

$$|GHZ\rangle = \frac{|0\rangle^{\otimes M} + |1\rangle^{\otimes M}}{\sqrt{2}}$$



- Example of a 2-qubit GHZ state

$$|GHZ_2\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\mathbf{\Psi}^+\rangle \text{ (Bell State)}$$

- Example of a 1-qubit GHZ state

$$|GHZ_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \mathbf{H}|0\rangle$$

Setting M=2 yields the Bell state $|\mathbf{\Phi}^+\rangle$.

Note that if we let M=1, we get a single qubit in superposition, $\mathbf{H}|0\rangle$. This would appear to *suggest that a qubit in superposition is the same thing as a qubit that is entangled with itself*!

13

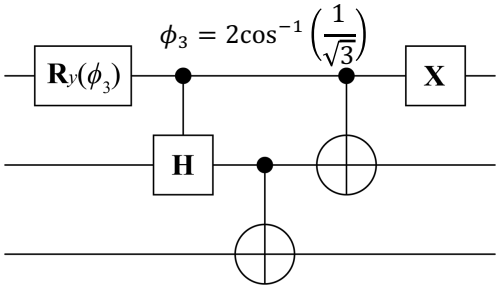
W States

- W states are M-partite, named after **W**olfgang Dür, Guifré Vidal and Ignacio Cirac (2002)
- Example of a 3-qubit W state and generator

$$|W_3\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}$$

$$|W_2\rangle = |\mathbf{\Psi}^+\rangle, \text{ (Bell State)}$$

$$|W_M\rangle = \frac{|0\rangle^{\otimes(M-1)}|1\rangle + \sqrt{M-1}|W_{M-1}\rangle|0\rangle}{\sqrt{M}}$$



Measurement of single qubit *Likely* results in entangled W_{M-1}-state since measurement outcome is probably $|0\rangle$.
Probability entangled state results is $\frac{M-1}{M}$.
Probability that basis state results (measured $|1\rangle$) is $\frac{1}{M}$.

* W. Dür, G. Vidal and I. Cirac, "Three Qubits can be Entangled in Two Inequivalent Ways," *Physical Review A*, vol. 62, no. 2, Nov. 14, 2000, p. 062314.

14

Forms of Entanglement

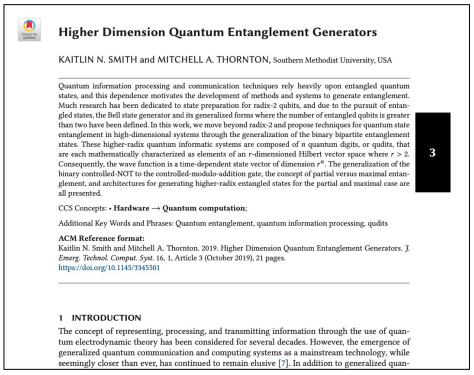
- "*Bipartite*" means two terms in the symbolic expression, "tripartite" means three terms in the symbolic expression
- "*Perfect*" entanglement means the magnitudes of squared probability coefficients are all equal
- "*Full*" entanglement means all qubits in a quantum state are entangled with one another
- "*Partial*" entanglement means that some, but not all, qubits forming the quantum state are entangled
- "*Entangling gate*" refers to the two- (or more) qubit gate in a circuit that causes entanglement to occur
- Entanglement cannot be achieved (purposely) without the inclusion of a multi-qubit gate – the "entangling gate"
- The presence of a multi-qubit gate does not guarantee that entanglement will occur

15

Entanglement in Higher-Dimensional Systems

- Higher-dimensional Systems use Radices/Bases greater than two (2)
  - The Quantum State is based upon a Basis Set comprising more than two basis vectors
- Survey of Higher-Dimensional Entanglement and Generators:

  K.N. Smith and M.A. Thornton, "Higher Dimension Quantum Entanglement Generators," ACM Journal on Emerging Technologies in Computing Systems, vol. 16, no. 1, 21 pp., Oct. 2019.



Higher Dimension Quantum Entanglement Generators

KAITLIN N. SMITH and MITCHELL A. THORNTON, Southern Methodist University, USA

Quantum information processing and communication techniques rely heavily upon entangled quantum states, and this dependence motivates the development of methods and systems to generate entanglement. Much research has been dedicated to state preparation for radix-2 qubits, and due to the pursuit of entangled states, the Bell state generator and its generalized forms where the number of entangled qubits is greater than two have been defined. In this work, we move beyond radix-2 and propose techniques for quantum state entanglement in high-dimensional systems through the generalization of the binary bipartite entanglement states. These higher-radix quantum informatic systems are composed of n quantum digits, or qudits, that are each mathematically characterized as elements of an r-dimensioned Hilbert vector space where $r > 2$. Consequently, the wave function is a time-dependent state vector of dimension r^n. The generalization of the binary controlled-NOT to the controlled-modulo-addition gate, the concept of partial versus maximal entanglement, and architectures for generating higher-radix entangled states for the partial and maximal case are all presented.

CCS Concepts: • **Hardware → Quantum computation**;

Additional Key Words and Phrases: Quantum entanglement, quantum information processing, qudits

ACM Reference format:
Kaitlin N. Smith and Mitchell A. Thornton. 2019. Higher Dimension Quantum Entanglement Generators. *J. Emerg. Technol. Comput. Syst.* 16, 1, Article 3 (October 2019), 21 pages.
https://doi.org/10.1145/3345501

3

1 INTRODUCTION

The concept of representing, processing, and transmitting information through the use of quantum electrodynamic theory has been considered for several decades. However, the emergence of generalized quantum communication and computing systems as a mainstream technology, while seemingly closer than ever, has continued to remain elusive [7]. In addition to generalized quan-

16

Superdense Coding

Communicate Classical Information by Transmitting a Smaller Number of Qubits

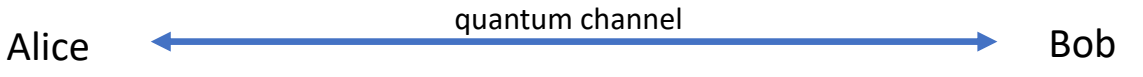
17

Superdense Coding for Secure Information Exchange

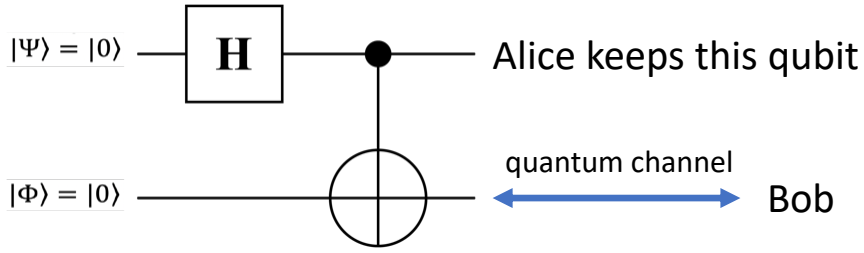
- An Application of Quantum Entanglement
- Allows a sender (Alice) to send two (2) classical bits to receiver (Bob) by transmitting only a single qubit
  - assuming that Alice and Bob already share qubits from an entangled pair
- Basis is the Sharing of Entangled (EPR) Pairs
- Assumes Presence of a Quantum Communication Channel
  - Typically, a Quantum channel is photonic (fiber-based)
- Can be considered as the Opposite of Quantum Teleportation (1 qubit is sent/received by transmitting 2 classical bits)
- This is Secure since an eavesdropper (Eve) will only have a single entangled qubit and she will be unable to extract Bob's two bits from it

18

Superdense Coding Channel



- Alice Prepares an Entangled Pair $|\Psi\Phi\rangle = |\mathbf{\Phi}^+\rangle$ by Initializing the Pair to a Ground State, $|\Psi\Phi\rangle = |00\rangle$, and Evolving them with a Bell State Generator:



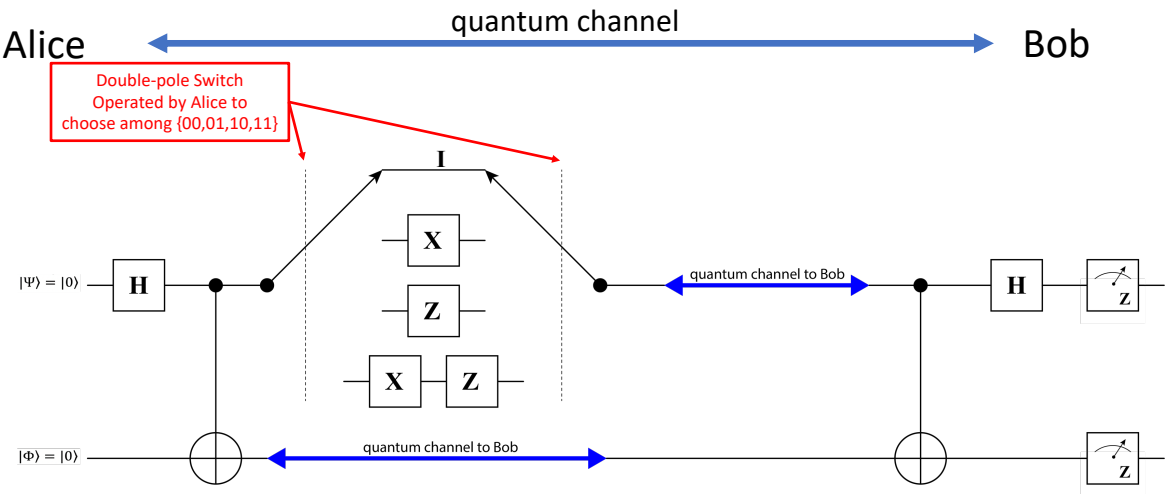
19

Superdense Coding Channel

- After preparing the Entangled Pair and transmitting one qubit to Bob over a quantum Channel, she chooses to evolve her qubit through:
  - no single qubit gate, transfer matrix is $\mathbf{I}$
  - a Pauli-$\mathbf{X}$, transfer matrix is $\mathbf{X}$
  - a Pauli-$\mathbf{Z}$, transfer matrix is $\mathbf{Z}$
  - a Pauli-$\mathbf{Y}$, transfer matrix is $\mathbf{Y}$ (or, typically, Pauli gates of $\mathbf{X}$ followed by $\mathbf{Z}$, since $\mathbf{XZ}$=-$i\mathbf{Y}$)
- Alice then transmits her processed qubit to Bob
- Bob now has a pair of qubits and he detangles them
- The result is that Bob has one of the basis pairs $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$
  - If Alice chose $\mathbf{I}$, Bob has $|00\rangle$, the detangled version of Bell state $|\mathbf{\Phi}^+\rangle$
  - If Alice chose $\mathbf{X}$, Bob has $|01\rangle$, the detangled version of Bell state $|\mathbf{\Psi}^+\rangle$
  - If Alice chose $\mathbf{Z}$, Bob has $|10\rangle$, the detangled version of Bell state $|\mathbf{\Phi}^-\rangle$
  - If Alice chose $\mathbf{XZ}$, Bob has $|11\rangle$, the detangled version of Bell state $|\mathbf{\Psi}^-\rangle$

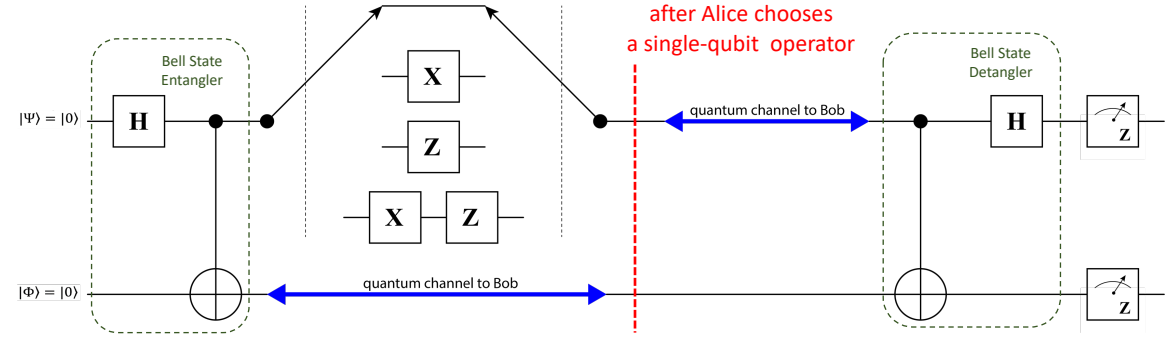
20

Complete Superdense Coding Circuit



21

Superdense Coding States

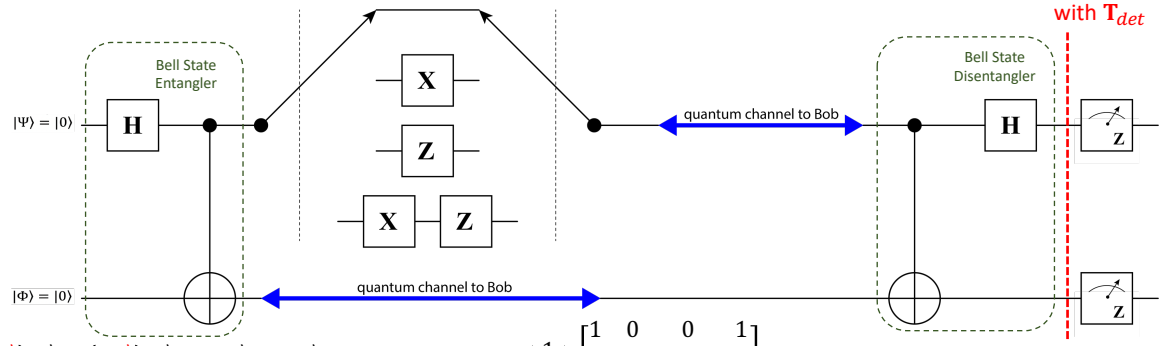


$$\frac{(\mathbf{I}|0\rangle)|0\rangle + (\mathbf{I}|1\rangle)|1\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad \frac{(\mathbf{Z}|0\rangle)|0\rangle + (\mathbf{Z}|1\rangle)|1\rangle}{\sqrt{2}} = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$\frac{(\mathbf{X}|0\rangle)|0\rangle + (\mathbf{X}|1\rangle)|1\rangle}{\sqrt{2}} = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \qquad \frac{(\mathbf{XZ}|0\rangle)|0\rangle + (\mathbf{XZ}|1\rangle)|1\rangle}{\sqrt{2}} = \frac{|10\rangle - |01\rangle}{\sqrt{2}}$$

22

Superdense Disentagled States



Consider the State after disentangling with $\mathbf{T}_{det}$

$$\frac{(\mathbf{I}|0\rangle)|0\rangle + (\mathbf{I}|1\rangle)|1\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle$$

$$\frac{(\mathbf{X}|0\rangle)|0\rangle + (\mathbf{X}|1\rangle)|1\rangle}{\sqrt{2}} = \frac{|10\rangle + |01\rangle}{\sqrt{2}} = |\Psi^+\rangle$$

$$\frac{(\mathbf{Z}|0\rangle)|0\rangle + (\mathbf{Z}|1\rangle)|1\rangle}{\sqrt{2}} = \frac{|00\rangle - |11\rangle}{\sqrt{2}} = |\Phi^-\rangle$$

$$\frac{(\mathbf{XZ}|0\rangle)|0\rangle + (\mathbf{XZ}|1\rangle)|1\rangle}{\sqrt{2}} = \frac{|10\rangle - |01\rangle}{\sqrt{2}} = |\Psi^-\rangle$$

$$\mathbf{T}_{det} = \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{bmatrix}$$

$$\mathbf{T}_{det}|\Phi^+\rangle = |00\rangle$$

$$\mathbf{T}_{det}|\Psi^+\rangle = |01\rangle$$

$$\mathbf{T}_{det}|\Phi^-\rangle = |10\rangle$$

$$\mathbf{T}_{det}|\Psi^-\rangle = |11\rangle$$

23

Quantum Teleportation

An Application of Quantum Entanglement

24

Quantum Teleportation

- An Application of Quantum Entanglement
- "Teleports" or Transfers Quantum Information from one location to another
- Basis is the Sharing of Entangled (EPR) Pairs
- Assumes Presence of two Communication Channels
  - Classical
  - Quantum
- Can be considered as the Opposite of Superdense Coding since Transmitting 2 Classical Bits enable 1 qubit to be exchanged
- Secure Communication since eavesdropper Eve can only observe the classical bits that are used to detangle a shared EPR pair

25

Quantum Teleportation: The Scenario

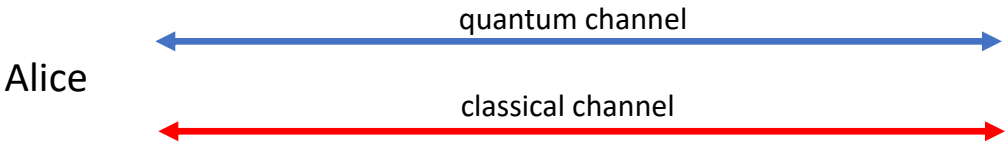
- Alice wants to send Bob Quantum Information in the Form of a Qubit

$$|\Omega\rangle = \alpha|0\rangle + \beta|1\rangle$$

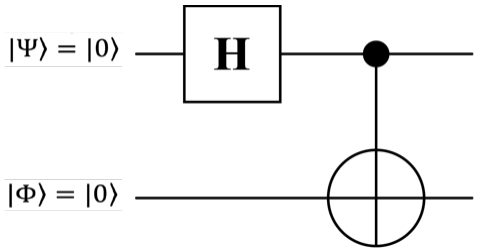
- Alice does not want to Send Bob $|\Omega\rangle$ over a Quantum Channel for Security Reasons
- Impossible to use Classical Channel since it would Require an Infinite Number (∞) of Classical Bits to Accurately Send the Probability Amplitudes, (α, β)
- Alice cannot Measure her Qubit to Observe the Probability Amplitudes since it would Collapse into a Measurement Eigenbasis vector
- Alice cannot Copy her Qubit into Another Qubit due to the "No Cloning" Theorem
- Assume that there Exists a Classical Communication Channel and a Quantum Communication Channel that Connect Alice and Bob

26

Quantum Teleportation Channels

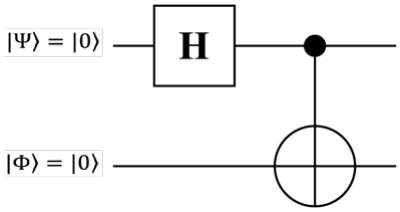


- Alice Prepares an Entangled Pair $|\Psi\Phi\rangle$ by Initializing the Pair to a Ground State, $|\Psi\Phi\rangle = |00\rangle$, and Evolving them with a Bell State Generator:



27

Alice's Entangled Pair



$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \qquad \mathbf{C_X} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

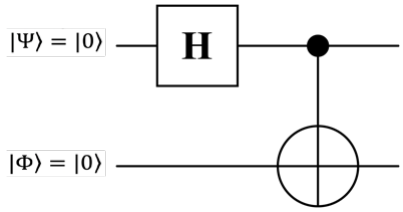
- The overall Transfer Matrix is:

$$\mathbf{T} = \mathbf{C_X}(\mathbf{H}\otimes\mathbf{I}) = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\left(\frac{1}{\sqrt{2}}\right)\left(\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\otimes\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}$$

28

Alice's Entangled Pair



$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \qquad \mathbf{C_X} = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

- The Entangled Pair $|\Psi\Phi\rangle$ state becomes:

$$\mathbf{T}|\Psi\Phi\rangle = \mathbf{T}|00\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 0 & 1 & 0 & -1\\ 1 & 0 & -1 & 0\end{bmatrix}\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

29

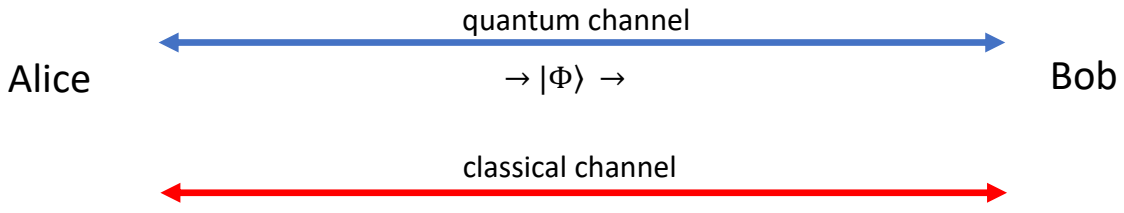
Alice's Combined State

- Alice's Combined 3-qubit State is:

qubit to be "sent" to Bob

$$|\Omega\Psi\Phi\rangle = (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

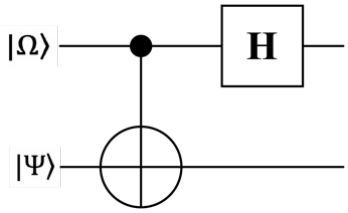
- Alice Retains $|\Psi\rangle$ and Sends Bob $|\Phi\rangle$ Over the Quantum Channel
- Alice has $|\Omega\Psi\rangle$ and Bob has $|\Phi\rangle$



30

Alice's Next Step

- Alice Evolves her Qubit Pair, $|\Omega\Psi\rangle$, with the Detangling Circuit:



- The Transfer Matrix for this Circuit is:

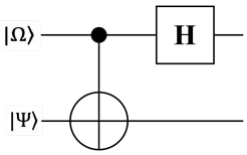
$$\mathbf{T}_r = (\mathbf{H} \otimes \mathbf{I})\mathbf{C_X} = \left(\frac{1}{\sqrt{2}}\right)\left(\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \otimes \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right)\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$$

$$= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{bmatrix}\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\\ 1 & 0 & 0 & -1\\ 0 & 1 & -1 & 0\end{bmatrix}$$

31

Alice's Next Step (cont.)

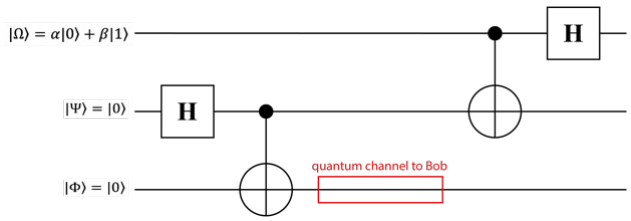
- Alice Evolves her Qubit Pair, $|\Omega\Psi\rangle$, with the Following Circuit:



- The Transfer Matrix for this Circuit is:

$$\mathbf{T}_r = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\\ 1 & 0 & 0 & -1\\ 0 & 1 & -1 & 0\end{bmatrix}$$

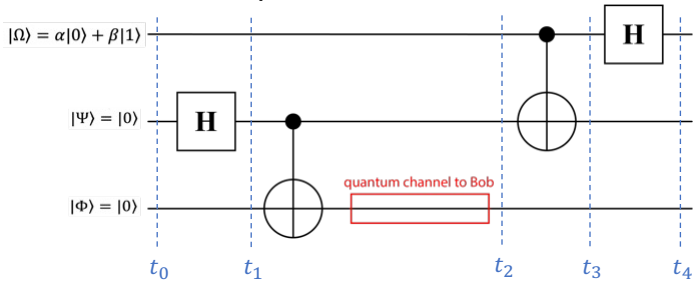
- Although Alice Possesses $|\Omega\Psi\rangle$ and Bob Possesses $|\Phi\rangle$, when Alice Evolves her Pair, it Affects the State of Bob's Qubit, $|\Phi\rangle$, since $|\Psi\Phi\rangle$ are Entangled.
- We Must Consider all Three Qubits, $|\Omega\Psi\Phi\rangle$, the Joint State is given by this overall circuit:



32

The 3-Qubit Joint State

- We compute the joint state of $|\Omega\Psi\Phi\rangle$ as:



- At time t_0:

$$|\Omega\Psi\Phi(t_0)\rangle = (\alpha|0\rangle + \beta|1\rangle)|00\rangle$$

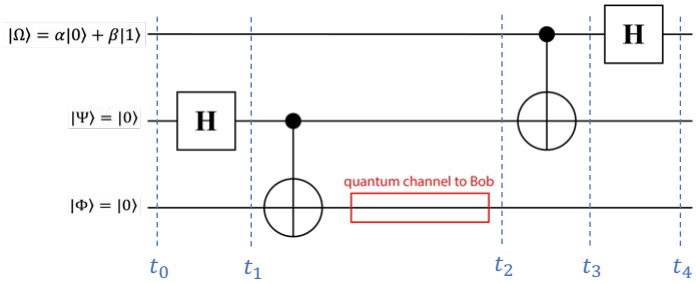
- At time t_1:

$$|\Omega\Psi\Phi(t_1)\rangle = (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle$$

33

The 3-Qubit Joint State (cont.)

- We compute the joint state of $|\Omega\Psi\Phi\rangle$ as:



- At time t_2:

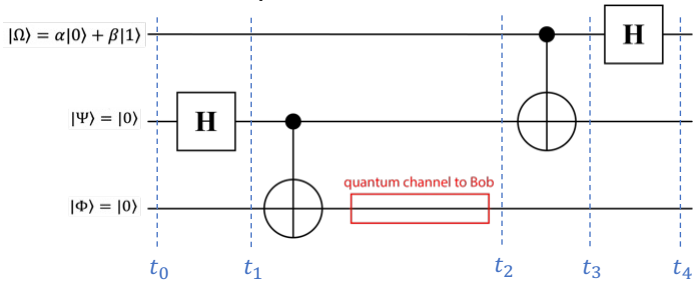
$$|\Omega\Psi\Phi(t_2)\rangle = (\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

Entangled state

34

The 3-Qubit Joint State (cont.)

- We compute the joint state of $|\Omega\Psi\Phi\rangle$ as:



- At time t_3:

$$|\Omega\Psi\Phi(t_3)\rangle = (\mathbf{C_X} \otimes \mathbf{I}_2)(\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

$$\mathbf{C_X} \otimes \mathbf{I}_2 = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)\big(|0\rangle\langle 0| + |1\rangle\langle 1|\big)$$

35

The 3-Qubit Joint State (cont.)

- At time t_3:

$$|\Omega\Psi\Phi(t_3)\rangle = (\mathbf{C_X} \otimes \mathbf{I}_2)(\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

$$\mathbf{C_X} \otimes \mathbf{I}_2 = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)\big(|0\rangle\langle 0| + |1\rangle\langle 1|\big)$$

Using Explicit Notation:

$$\mathbf{C_X} \otimes \mathbf{I}_2 = \left(\begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&1&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&1\\0&0&0&0\end{bmatrix} + \begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&1&0\\0&0&0&0\end{bmatrix}\right)$$

$$\otimes \left(\begin{bmatrix}1&0\\0&0\end{bmatrix} + \begin{bmatrix}0&0\\0&1\end{bmatrix}\right)$$

$$\mathbf{C_X} \otimes \mathbf{I}_2 = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} \otimes \begin{bmatrix}1&0\\0&1\end{bmatrix} = \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\end{bmatrix}$$

36

The 3-Qubit Joint State (cont.)

- At time t_3:

$$|\Omega\Psi\Phi(t_3)\rangle = (\mathbf{C_X} \otimes \mathbf{I}_2)(\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

Using Dirac's Notation:

$$\mathbf{C_X} \otimes \mathbf{I}_2 = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)(|0\rangle\langle 0| + |1\rangle\langle 1|)$$

$$\begin{aligned}&\mathbf{C_X} \otimes \mathbf{I}_2 \\ &= |000\rangle\langle 000| + |010\rangle\langle 010| + |100\rangle\langle 110| + |110\rangle\langle 100| \\ &+ |001\rangle\langle 001| + |011\rangle\langle 011| + |101\rangle\langle 111| + |111\rangle\langle 101|\end{aligned}$$

- Notice how the matrices, in terms of BraKet outer products, combine in the above Equation
- The Kets combine as rightmost term and the Bras combine as rightmost term

37

The 3-Qubit Joint State (cont.)

- At time t_3:

$$|\Omega\Psi\Phi(t_3)\rangle = (\mathbf{C_X} \otimes \mathbf{I}_2)(\alpha|0\rangle + \beta|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

$$|\Omega\Psi\Phi(t_3)\rangle = \left(\frac{1}{\sqrt{2}}\right)(\mathbf{C_X} \otimes \mathbf{I}_2)(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$$

$$\begin{aligned}&|\Omega\Psi\Phi(t_3)\rangle \\ &= \left(\frac{1}{\sqrt{2}}\right)(|000\rangle\langle 000| + |010\rangle\langle 010| + |100\rangle\langle 110| + |110\rangle\langle 100| \\ &+ |001\rangle\langle 001| + |011\rangle\langle 011| + |101\rangle\langle 111| + |111\rangle\langle 101|)(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)\end{aligned}$$

$$|\Omega\Psi\Phi(t_3)\rangle = \left(\frac{1}{\sqrt{2}}\right)(\alpha|000\rangle\langle 000|000\rangle + \beta|110\rangle\langle 100|100\rangle + \alpha|011\rangle\langle 011|011\rangle + \beta|101\rangle\langle 111|111\rangle)$$

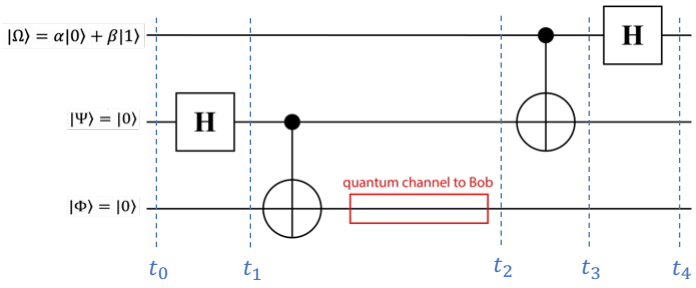
$$|\Omega\Psi\Phi(t_3)\rangle = \left(\frac{1}{\sqrt{2}}\right)(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$$

38

The 3-Qubit Joint State (cont.)

- At time t_3:

$$|\Omega\Psi\Phi(t_3)\rangle = \left(\frac{1}{\sqrt{2}}\right)(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$$



- At time t_4:

$$|\Omega\Psi\Phi(t_4)\rangle = (\mathbf{H} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2)\left(\frac{1}{\sqrt{2}}\right)(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$$

39

The 3-Qubit Joint State (cont.)

- At time t_4:

$$|\Omega\Psi\Phi(t_4)\rangle = (\mathbf{H} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2)\left(\frac{1}{\sqrt{2}}\right)(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$$

$$\mathbf{H} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2 = \mathbf{H} \otimes \mathbf{I}_4$$
$$= \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)$$

$$\mathbf{H} \otimes \mathbf{I}_4$$
$$= \frac{1}{\sqrt{2}}(|000\rangle\langle 000| + |000\rangle\langle 100| + |100\rangle\langle 000| - |100\rangle\langle 100| + |001\rangle\langle 001| + |001\rangle\langle 101| + |101\rangle\langle 001|$$
$$- |101\rangle\langle 101| + |010\rangle\langle 010| + |010\rangle\langle 110| + |110\rangle\langle 010| - |110\rangle\langle 110| + |011\rangle\langle 011| + |011\rangle\langle 111|$$
$$+ |111\rangle\langle 011| - |111\rangle\langle 111|)$$

$$|\Omega\Psi\Phi(t_4)\rangle$$
$$= \frac{1}{2}(|000\rangle\langle 000| + |000\rangle\langle 100| + |100\rangle\langle 000| - |100\rangle\langle 100| + |001\rangle\langle 001| + |001\rangle\langle 101| + |101\rangle\langle 001|$$
$$- |101\rangle\langle 101| + |010\rangle\langle 010| + |010\rangle\langle 110| + |110\rangle\langle 010| - |110\rangle\langle 110| + |011\rangle\langle 011| + |011\rangle\langle 111|$$
$$+ |111\rangle\langle 011| - |111\rangle\langle 111|)(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$$

40

The 3-Qubit Joint State (cont.)

- At time t_4:

$$|\Omega\Psi\Phi(t_4)\rangle$$
$$= \frac{1}{2}(|000\rangle\langle 000| + |000\rangle\langle 100| + |100\rangle\langle 000| - |100\rangle\langle 100| + |001\rangle\langle 001| + |001\rangle\langle 101| + |101\rangle\langle 001|$$
$$- |101\rangle\langle 101| + |010\rangle\langle 010| + |010\rangle\langle 110| + |110\rangle\langle 010| - |110\rangle\langle 110| + |011\rangle\langle 011| + |011\rangle\langle 111|$$
$$+ |111\rangle\langle 011| - |111\rangle\langle 111|)(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle)$$

$$|\Omega\Psi\Phi(t_4)\rangle$$
$$= \frac{1}{2}(|000\rangle\langle 000|\alpha|000\rangle + |100\rangle\langle 000|\alpha|000\rangle + |001\rangle\langle 101|\beta|101\rangle - |101\rangle\langle 101|\beta|101\rangle$$
$$+ |010\rangle\langle 110|\beta|110\rangle - |110\rangle\langle 110|\beta|110\rangle + |011\rangle\langle 011|\alpha|011\rangle + |111\rangle\langle 011|\alpha|011\rangle)$$

$$|\Omega\Psi\Phi(t_4)\rangle = \frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \beta|001\rangle - \beta|101\rangle + \beta|010\rangle - \beta|110\rangle + \alpha|011\rangle + \alpha|111\rangle)$$

41

The 3-Qubit Joint State (cont.)

- At time t_4:

$$|\Omega\Psi\Phi(t_4)\rangle = \frac{1}{2}(\alpha|000\rangle + \alpha|100\rangle + \beta|001\rangle - \beta|101\rangle + \beta|010\rangle - \beta|110\rangle + \alpha|011\rangle + \alpha|111\rangle)$$

$$|\Omega\Psi\Phi(t_4)\rangle =$$
$$\frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle)$$
$$+\frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle)$$
$$+\frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle)$$
$$+\frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

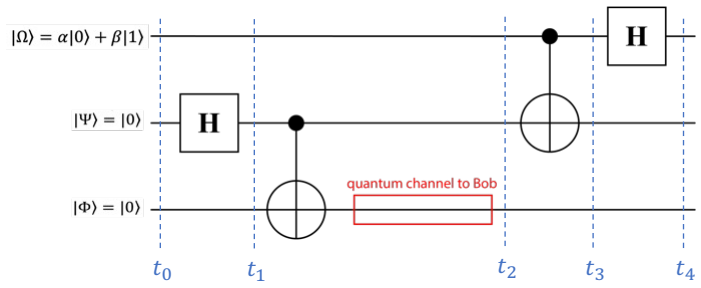
42

The 3-Qubit Joint State (cont.)

- At time t_4:

$$|\Omega\Psi\Phi(t_4)\rangle =$$
$$\frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle)$$
$$+\frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle)$$
$$+\frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle)$$
$$+\frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

Alice's qubits — Bob's qubit



- At time t_4, Alice caused her qubits to evolve into a (computational) basis state
- Since Alice retained qubit $|\Psi\rangle$, which was entangled with Bob's qubit, $|\Phi\rangle$, the rightmost $\mathbf{C_X}$ gate served to entangle Alice's qubit $|\Omega\rangle$ with Bob's qubit $|\Phi\rangle$
- This entangling operation "teleported" the probability amplitudes of Alice's $|\Omega\rangle$ to Bob's $|\Phi\rangle$

43

Eliminating the Superposition in the Joint State

- At time t_4, the three qubits are in (perfect) Superposition since the Four possible states each have probability amplitudes of one-fourth.

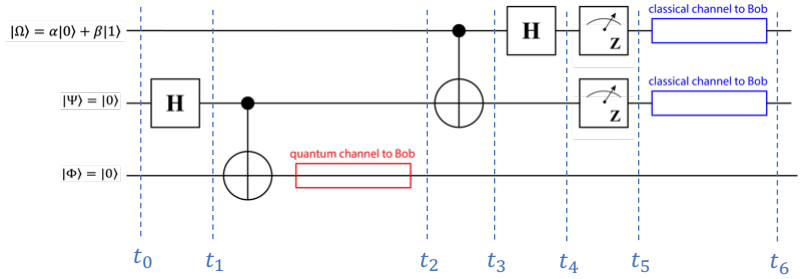
$$|\Omega\Psi\Phi(t_4)\rangle = \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle) + \frac{1}{2}|01\rangle(\alpha|1\rangle + \beta|0\rangle) + \frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle) + \frac{1}{2}|11\rangle(\alpha|1\rangle - \beta|0\rangle)$$

- Alice can Measure her two qubits $|\Omega\Psi\rangle$ with respect to the computational basis by using the Pauli-$\mathbf{Z}$ observable
- This measurement will force Alice's two qubits to collapse into one of the four basis states, $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$ with equal probability
- When Alice performs her measurement, this causes Bob's qubit to collapse into one of the following four states:

$$|\Phi_{00}\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\Phi_{01}\rangle = \alpha|1\rangle + \beta|0\rangle, \quad |\Phi_{10}\rangle = \alpha|0\rangle - \beta|1\rangle, \quad |\Phi_{11}\rangle = \alpha|1\rangle - \beta|0\rangle$$

44

Alice Measures her Two Qubits and Tells Bob the Outcome



- At time t_5, Alice has measured her two qubits causing them to collapse into one of the four (4-dimensional) basis states: $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$
- Alice's measurement "collapses" the 3-qubit joint superposition and causes Bob's qubit to likewise "collapse" into one of these four states (that is still in superposition)

$|\Phi_{00}\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\Phi_{01}\rangle = \alpha|1\rangle + \beta|0\rangle, \quad |\Phi_{10}\rangle = \alpha|0\rangle - \beta|1\rangle, \quad |\Phi_{11}\rangle = \alpha|1\rangle - \beta|0\rangle$

- At time t_6, Alice has has told Bob which of the four outcomes, 00, 01, 10 or 11, that resulted

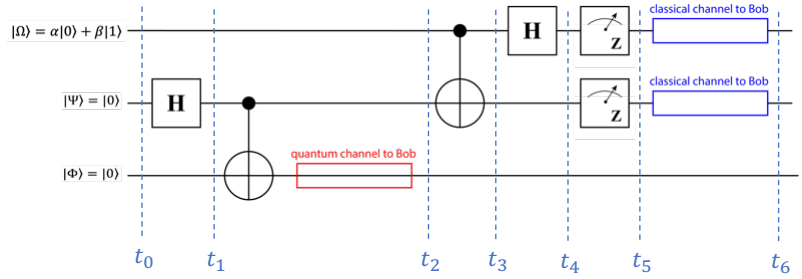
45

Alice Measures her Two Qubits and Tells Bob the Outcome

- At time t_6, Alice has told Bob, using the classical channel, which of the four outcomes, 00, 01, 10 or 11, resulted from her measurements
- When Bob receives Alice's measurement results, (00, 01, 10 or 11), he knows that his qubit $|\Phi\rangle$ has <u>one</u> of these forms:

$|\Phi_{00}\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\Phi_{01}\rangle = \alpha|1\rangle + \beta|0\rangle, \quad |\Phi_{10}\rangle = \alpha|0\rangle - \beta|1\rangle, \quad |\Phi_{11}\rangle = \alpha|1\rangle - \beta|0\rangle$

- The desired result is for Bob to evolve his qubit $|\Phi\rangle$ such that it assumes the form of $|\Omega(t_0)\rangle = \alpha|0\rangle + \beta|1\rangle$, the original state that Alice is "teleporting" to Bob



46

How can Bob Evolve his Teleported Qubit ?

- At time t_6, Bob possesses $|\Phi(t_6)\rangle$ that is one of these states:

  $|\Phi_{00}\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\Phi_{01}\rangle = \alpha|1\rangle + \beta|0\rangle, \quad |\Phi_{10}\rangle = \alpha|0\rangle - \beta|1\rangle, \quad |\Phi_{11}\rangle = \alpha|1\rangle - \beta|0\rangle$

- At time t_6, Bob knows which state he has since Alice sent him a classical 2-bit value indicating which one he has:

Alice sent Bob:	Bob knows his qubit state:	Bob wants to have:	What operator(s) does Bob need?
00	$\|\Phi_{00}\rangle = \alpha\|0\rangle + \beta\|1\rangle$	$\|\Phi(t_7)\rangle = \|\Omega(t_0)\rangle = \alpha\|0\rangle + \beta\|1\rangle$	
01	$\|\Phi_{01}\rangle = \alpha\|1\rangle + \beta\|0\rangle$	$\|\Phi(t_7)\rangle = \|\Omega(t_0)\rangle = \alpha\|0\rangle + \beta\|1\rangle$	
10	$\|\Phi_{10}\rangle = \alpha\|0\rangle - \beta\|1\rangle$	$\|\Phi(t_7)\rangle = \|\Omega(t_0)\rangle = \alpha\|0\rangle + \beta\|1\rangle$	
11	$\|\Phi_{11}\rangle = \alpha\|1\rangle - \beta\|0\rangle$	$\|\Phi(t_7)\rangle = \|\Omega(t_0)\rangle = \alpha\|0\rangle + \beta\|1\rangle$	

47

How can Bob Evolve his Teleported Qubit ?

- At time t_6, Bob possesses $|\Phi(t_6)\rangle$ that is one of these states:

  $|\Phi_{00}\rangle = \alpha|0\rangle + \beta|1\rangle, \quad |\Phi_{01}\rangle = \alpha|1\rangle + \beta|0\rangle, \quad |\Phi_{10}\rangle = \alpha|0\rangle - \beta|1\rangle, \quad |\Phi_{11}\rangle = \alpha|1\rangle - \beta|0\rangle$

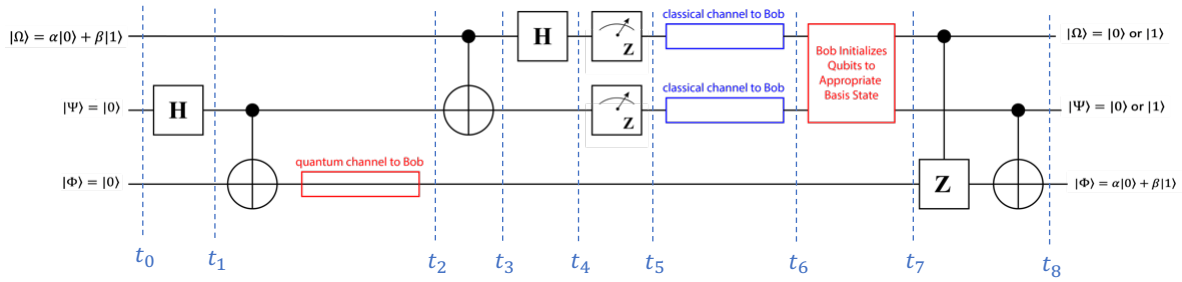
- At time t_6, Bob knows which state he has since Alice sent him a classical 2-bit value indicating which one he has:

Alice sent Bob:	Bob knows his qubit state:	Bob wants to have:	What operator(s) does Bob need?
00	$\|\Phi_{00}\rangle = \alpha\|0\rangle + \beta\|1\rangle$	$\|\Phi(t_7)\rangle = \|\Omega(t_0)\rangle = \alpha\|0\rangle + \beta\|1\rangle$	$\mathbf{I}_2$, (no operator)
01	$\|\Phi_{01}\rangle = \alpha\|1\rangle + \beta\|0\rangle$	$\|\Phi(t_7)\rangle = \|\Omega(t_0)\rangle = \alpha\|0\rangle + \beta\|1\rangle$	$\mathbf{X}$, (bit-flip)
10	$\|\Phi_{10}\rangle = \alpha\|0\rangle - \beta\|1\rangle$	$\|\Phi(t_7)\rangle = \|\Omega(t_0)\rangle = \alpha\|0\rangle + \beta\|1\rangle$	$\mathbf{Z}$, (phase-flip)
11	$\|\Phi_{11}\rangle = \alpha\|1\rangle - \beta\|0\rangle$	$\|\Phi(t_7)\rangle = \|\Omega(t_0)\rangle = \alpha\|0\rangle + \beta\|1\rangle$	$\mathbf{Z}$ & $\mathbf{X}$, (phase- & bit-flip)

48

Bob Evolves his Qubit to the Teleported State

- At time t_6, Bob Initializes his own version of Qubits $|\Omega\rangle$ and $|\Psi\rangle$ into the Basis States indicated by Alice's Classical Communication to Him:
- At time t_7, Bob has Evolved his Qubit, $|\Phi(t_7)\rangle$, with the Controlled-$\mathbf{Z}$ and Controlled-$\mathbf{X}$ gates, $\mathbf{C_Z}$ and $\mathbf{C_X}$:

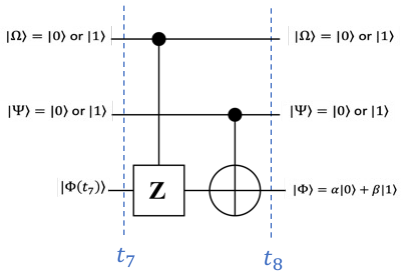


- At time t_8, Bob possesses the qubit $|\Phi(t_8)\rangle = |\Phi(t_0)\rangle = \alpha|0\rangle + \beta|1\rangle$, and the Only Information Alice sent Bob was an Entangled Qubit, $|\Phi(t_2)\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, and Two Bits of Classical Information, 00, 01, 10, or 11.

49

Bob's Circuit

- What is the transfer function of Bob's circuit?



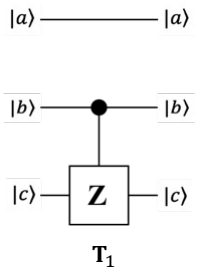
$$\mathbf{C_Z} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\mathbf{C_X} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

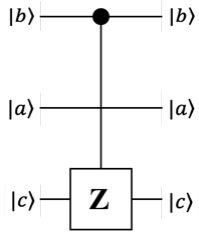
50

Bob's Circuit

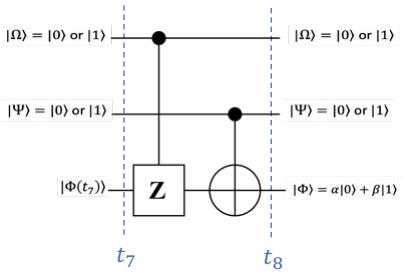
- What is the transfer function of Bob's circuit?
- Must Account for the "middle" qubit in the $\mathbf{C_Z}$ gate
- One way to determine the 3-qubit transfer function is to use a permutation matrix, $\mathbf{P}$
- Compare these two circuits where the leftmost is represented by transfer matrix, $\mathbf{T}_1$, and the rightmost (*i.e.*, part of Bob's circuit) by $\mathbf{T}_2$



$\mathbf{T}_1$



$\mathbf{T}_2$



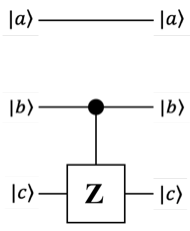
$$\mathbf{C_Z} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\mathbf{C_X} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

51

Bob's Circuit – Controlled-$\mathbf{Z}$ Operator

- Transfer function of $\mathbf{C_Z}$ with no "middle" qubit is:

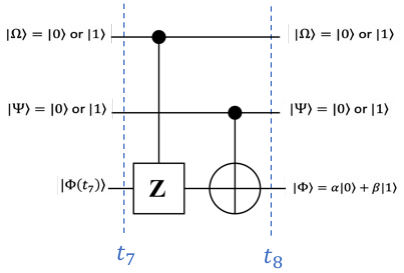


$$\mathbf{T}_1 = \mathbf{I}_2 \otimes \mathbf{C_Z}$$

$$= (|0\rangle\langle 0| + |1\rangle\langle 1|)\,(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11|)$$

$$= |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| - |011\rangle\langle 011|$$
$$+|100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 110| - |111\rangle\langle 111|$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$



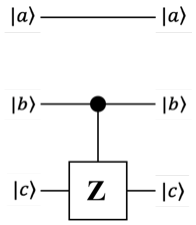
$$\mathbf{C_Z} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\mathbf{C_X} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

52

Bob's Circuit – Controlled-**Z** Operator

- Transfer function of $\mathbf{C_Z}$ with no "middle" qubit is:



$$\mathbf{T}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

output state Kets

input state Bras

	|000⟩	|001⟩	|010⟩	|011⟩	|100⟩	|101⟩	|110⟩	|111⟩
|000⟩	1	0	0	0	0	0	0	0
|001⟩	0	1	0	0	0	0	0	0
|010⟩	0	0	1	0	0	0	0	0
|011⟩	0	0	0	−1	0	0	0	0
|100⟩	0	0	0	0	1	0	0	0
|101⟩	0	0	0	0	0	1	0	0
|110⟩	0	0	0	0	0	0	1	0
|111⟩	0	0	0	0	0	0	0	−1

- Consider the input/output relationship where the evolved matrix "Ket" (column vectors) are possible output states for a given "Bra" (row vector) is the un-evolved input state, when the input state is also a basis vector.
- We can label the Ket and Bra vectors of the transfer matrix
- Each term in the Dirac form of the Transfer matrix is of the form:

$$|abc\rangle\langle abc|$$

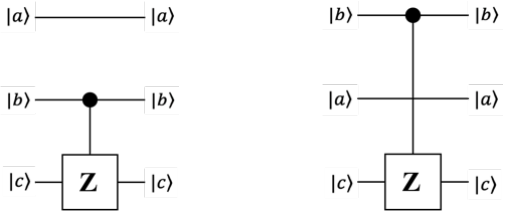
- We Permute above matrix with:

$$|bac\rangle\langle bac|$$

53

Permuting the matrix

- We Permute above matrix with $|bac\rangle\langle bac|$



	|000⟩	|001⟩	|010⟩	|011⟩	|100⟩	|101⟩	|110⟩	|111⟩
|000⟩	1	0	0	0	0	0	0	0
|001⟩	0	1	0	0	0	0	0	0
|010⟩	0	0	1	0	0	0	0	0
|011⟩	0	0	0	−1	0	0	0	0
|100⟩	0	0	0	0	1	0	0	0
|101⟩	0	0	0	0	0	1	0	0
|110⟩	0	0	0	0	0	0	1	0
|111⟩	0	0	0	0	0	0	0	−1

- Interchanging the ab values with ba in the Ket labels: |000⟩ |001⟩ |100⟩ |101⟩ |010⟩ |011⟩ |110⟩ |111⟩
- Indicates matrix Kets 010 switched with 100, and 011 is switched with 101
- Switching the Kets (column vectors) results in the lower right matrix

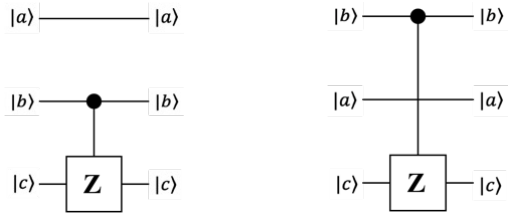
"switched" output state Kets

	|000⟩	|001⟩	|100⟩	|101⟩	|010⟩	|011⟩	|110⟩	|111⟩
|000⟩	1	0	0	0	0	0	0	0
|001⟩	0	1	0	0	0	0	0	0
|010⟩	0	0	0	0	1	0	0	0
|011⟩	0	0	0	0	0	−1	0	0
|100⟩	0	0	1	0	0	0	0	0
|101⟩	0	0	0	1	0	0	0	0
|110⟩	0	0	0	0	0	0	1	0
|111⟩	0	0	0	0	0	0	0	−1

54

Permuting the matrix (cont.)

- We Permute above matrix with $|bac\rangle\langle bac|$



"switched" output state Kets

	|000⟩	|001⟩	|100⟩	|101⟩	|010⟩	|011⟩	|110⟩	|111⟩
|000⟩	1	0	0	0	0	0	0	0
|001⟩	0	1	0	0	0	0	0	0
|010⟩	0	0	0	0	1	0	0	0
|011⟩	0	0	0	0	0	−1	0	0
|100⟩	0	0	1	0	0	0	0	0
|101⟩	0	0	0	1	0	0	0	0
|110⟩	0	0	0	0	0	0	1	0
|111⟩	0	0	0	0	0	0	0	−1

- We must likewise interchange the appropriate row vectors
- Finally, we relabel the Ket and Bra vectors to be in sequential order as shown on following slide

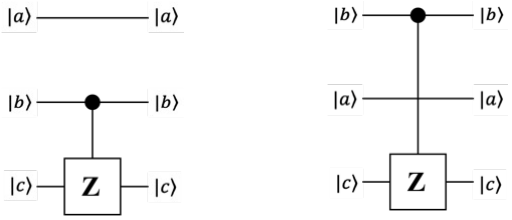
"switched" output state Kets

"switched" input state Bras	|000⟩	|001⟩	|100⟩	|101⟩	|010⟩	|011⟩	|110⟩	|111⟩
|000⟩	1	0	0	0	0	0	0	0
|001⟩	0	1	0	0	0	0	0	0
|100⟩	0	0	1	0	0	0	0	0
|101⟩	0	0	0	1	0	0	0	0
|010⟩	0	0	0	0	1	0	0	0
|011⟩	0	0	0	0	0	−1	0	0
|110⟩	0	0	0	0	0	0	1	0
|111⟩	0	0	0	0	0	0	0	−1

55

Permuting the matrix (cont.)

- We Permute above matrix with $|bac\rangle\langle bac|$



"switched" output state Kets

"switched" input state Bras	|000⟩	|001⟩	|100⟩	|101⟩	|010⟩	|011⟩	|110⟩	|111⟩
|000⟩	1	0	0	0	0	0	0	0
|001⟩	0	1	0	0	0	0	0	0
|100⟩	0	0	1	0	0	0	0	0
|101⟩	0	0	0	1	0	0	0	0
|010⟩	0	0	0	0	1	0	0	0
|011⟩	0	0	0	0	0	−1	0	0
|110⟩	0	0	0	0	0	0	1	0
|111⟩	0	0	0	0	0	0	0	−1

"relabeled" output state Kets

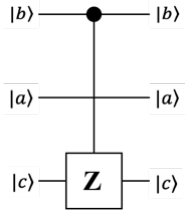
"relabeled" input state Bras	|000⟩	|001⟩	|010⟩	|011⟩	|100⟩	|101⟩	|110⟩	|111⟩
|000⟩	1	0	0	0	0	0	0	0
|001⟩	0	1	0	0	0	0	0	0
|010⟩	0	0	1	0	0	0	0	0
|011⟩	0	0	0	1	0	0	0	0
|100⟩	0	0	0	0	1	0	0	0
|101⟩	0	0	0	0	0	−1	0	0
|110⟩	0	0	0	0	0	0	1	0
|111⟩	0	0	0	0	0	0	0	−1

- We must likewise interchange the appropriate row vectors
- Finally, we relabel the Ket and Bra vectors to be in sequential order as shown on following slide
- This is the Transfer matrix for the $\mathbf{C_Z}$ gate with the "middle qubit"

56

Bob's Circuit – Controlled-$\mathbf{Z}$ Operator

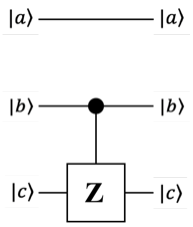
- Transfer function of $\mathbf{C_Z}$ with no "middle" qubit is:



$$\mathbf{T}_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

- This is the same thing as multiplying $\mathbf{T}_1$ with a permutation matrix, $\mathbf{P}$, that interchanges the appropriate Kets and Bras and with $\mathbf{P}^{\mathrm{T}}$ that interchanges appropriate Bras with Kets

$$\mathbf{P} = |000\rangle\langle 000| + |001\rangle\langle 001| + |100\rangle\langle 010| + |101\rangle\langle 011| + |010\rangle\langle 100| + |011\rangle\langle 101| + |110\rangle\langle 110| + |111\rangle\langle 111|$$



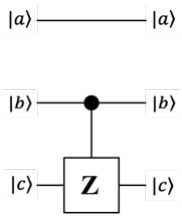
$$\mathbf{T}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\mathbf{P} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

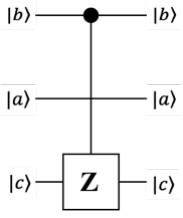
57

Verify Permutation: $\mathbf{T}_2 = \mathbf{P}\mathbf{T}_1\mathbf{P}^{\mathrm{T}}$

- Transfer function of $\mathbf{C_Z}$ with no "middle" qubit is:



$$\mathbf{T}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$



$$\mathbf{T}_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix}$$

$$\mathbf{T}_2 = \mathbf{P}\mathbf{T}_1\mathbf{P}^{\mathrm{T}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

58

Verify Permutation: $\mathbf{T}_2 = \mathbf{P}\mathbf{T}_1\mathbf{P}^{\mathrm{T}}$ (cont.)

$$\mathbf{T}_2 = \mathbf{P}\mathbf{T}_1\mathbf{P}^{\mathrm{T}} = \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&-1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&-1\end{bmatrix}\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{bmatrix}$$

$$= \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&1\end{bmatrix}\begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&-1&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&-1\end{bmatrix} = \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&-1&0&0\\0&0&0&0&0&0&1&0\\0&0&0&0&0&0&0&-1\end{bmatrix} = \mathbf{T}_2$$

59

Bob's Circuit

- What is the transfer function of Bob's circuit?
- Now we know that the $\mathbf{C_Z}$ with the "middle" qubit is represented with:

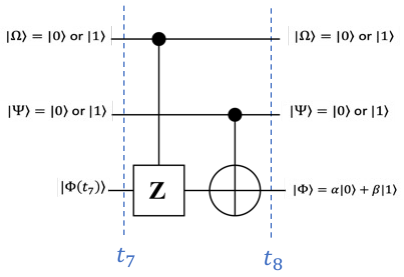
$$\mathbf{T}_2 = \mathbf{P}\mathbf{T}_1\mathbf{P}^{\mathrm{T}} = \mathbf{P}(\mathbf{I}_2 \otimes \mathbf{C_Z})\mathbf{P}^{\mathrm{T}}$$

- The transfer function for Bob's circuit, shown in upper left, denoted by $\mathbf{T}_3$, is:

$$\mathbf{T}_3 = (\mathbf{I}_2 \otimes \mathbf{C_X})\mathbf{T}_2 = (\mathbf{I}_2 \otimes \mathbf{C_X})\mathbf{P}(\mathbf{I}_2 \otimes \mathbf{C_Z})\mathbf{P}^{\mathrm{T}}$$

- The explicit form of $(\mathbf{I}_2 \otimes \mathbf{C_X})$ is:

$$\mathbf{I}_2 \otimes \mathbf{C_X} = \begin{bmatrix}1&0\\0&1\end{bmatrix} \otimes \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix} = \begin{bmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{bmatrix}$$



$$\mathbf{C_Z} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$$

$$\mathbf{C_X} = \begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

60

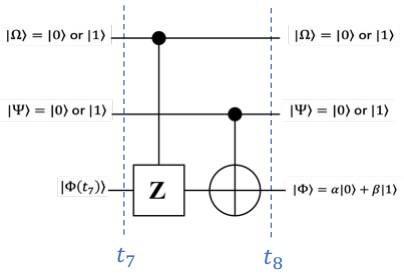
Bob's Circuit (cont.)

- What is the transfer function of Bob's circuit?
- The explicit form of Bob's circuit is:

$$\mathbf{T}_3 = (\mathbf{I}_2 \otimes \mathbf{C_X})\mathbf{P}(\mathbf{I}_2 \otimes \mathbf{C_Z})\mathbf{P}^{\mathrm{T}}$$

$$= \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix} \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&0&0&-1 \end{bmatrix}$$

$$= \begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&-1&0&0\\ 0&0&0&0&0&0&0&-1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

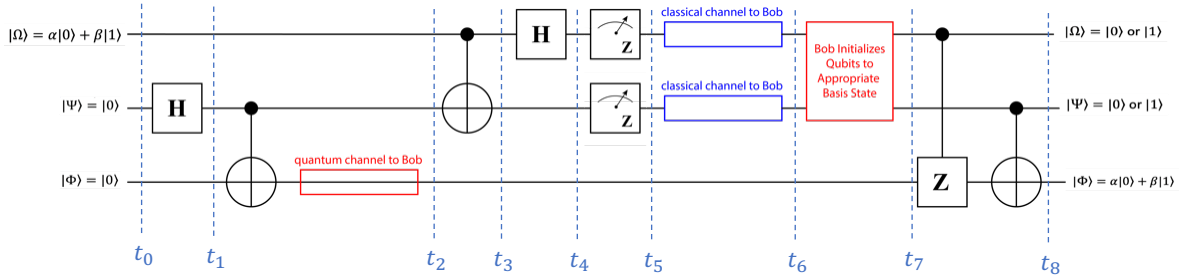


$$\mathbf{C_Z} = \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&1&0\\ 0&0&0&-1 \end{bmatrix}$$

$$\mathbf{C_X} = \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{bmatrix}$$

61

Transfer Matrix of Entire Teleportation Circuit



- Alice's circuit from time t_0 to t_4 is represented by transfer matrix $\mathbf{T}_0$:

$$\mathbf{T}_0 = (\mathbf{H} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2)(\mathbf{C_X} \otimes \mathbf{I}_2)(\mathbf{I}_2 \otimes \mathbf{C_X})(\mathbf{I}_2 \otimes \mathbf{H} \otimes \mathbf{I}_2)$$

$$= \left(\frac{1}{\sqrt{2}}\begin{bmatrix} 1&1\\ 1&-1 \end{bmatrix} \otimes \begin{bmatrix} 1&0\\ 0&1 \end{bmatrix} \otimes \begin{bmatrix} 1&0\\ 0&1 \end{bmatrix}\right)\left(\begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{bmatrix} \otimes \begin{bmatrix} 1&0\\ 0&1 \end{bmatrix}\right)$$

$$\left(\begin{bmatrix} 1&0\\ 0&1 \end{bmatrix} \otimes \begin{bmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{bmatrix}\right)\left(\begin{bmatrix} 1&0\\ 0&1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}}\begin{bmatrix} 1&1\\ 1&-1 \end{bmatrix} \otimes \begin{bmatrix} 1&0\\ 0&1 \end{bmatrix}\right)$$

62

Transfer Matrix of Entire Teleportation Circuit (cont.)

- Alice's circuit from time t_0 to t_4 is represented by transfer matrix $\mathbf{T}_0$:

$$\mathbf{T}_0 = (\mathbf{H} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2)(\mathbf{C_X} \otimes \mathbf{I}_2)(\mathbf{I}_2 \otimes \mathbf{C_X})(\mathbf{I}_2 \otimes \mathbf{H} \otimes \mathbf{I}_2)$$

$$= \frac{1}{2}\left(\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} \otimes \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}\right) \begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\end{bmatrix} \begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix} \left(\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \otimes \begin{bmatrix}1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\\ 1 & 0 & -1 & 0\\ 0 & 1 & 0 & -1\end{bmatrix}\right)$$

63

Transfer Matrix of Entire Teleportation Circuit (cont.)

- Alice's circuit from time t_0 to t_4 is represented by transfer matrix $\mathbf{T}_0$:

$$\mathbf{T}_0 = (\mathbf{H} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2)(\mathbf{C_X} \otimes \mathbf{I}_2)(\mathbf{I}_2 \otimes \mathbf{C_X})(\mathbf{I}_2 \otimes \mathbf{H} \otimes \mathbf{I}_2)$$

$$= \frac{1}{2}\begin{bmatrix}1 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1\\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1\end{bmatrix} \begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\end{bmatrix} \begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$$

$$\begin{bmatrix}1 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0\\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1\\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1\end{bmatrix}$$

64

Transfer Matrix of Entire Teleportation Circuit (cont.)

- Alice's circuit from time t_0 to t_4 is represented by transfer matrix $\mathbf{T}_0$:

$$\mathbf{T}_0 = (\mathbf{H} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2)(\mathbf{C_X} \otimes \mathbf{I}_2)(\mathbf{I}_2 \otimes \mathbf{C_X})(\mathbf{I}_2 \otimes \mathbf{H} \otimes \mathbf{I}_2)$$

$$= \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 & 0 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & -1 \end{bmatrix}$$

65

Transfer Matrix of Entire Teleportation Circuit (cont.)

- Alice's circuit from time t_0 to t_4 is represented by transfer matrix $\mathbf{T}_0$:

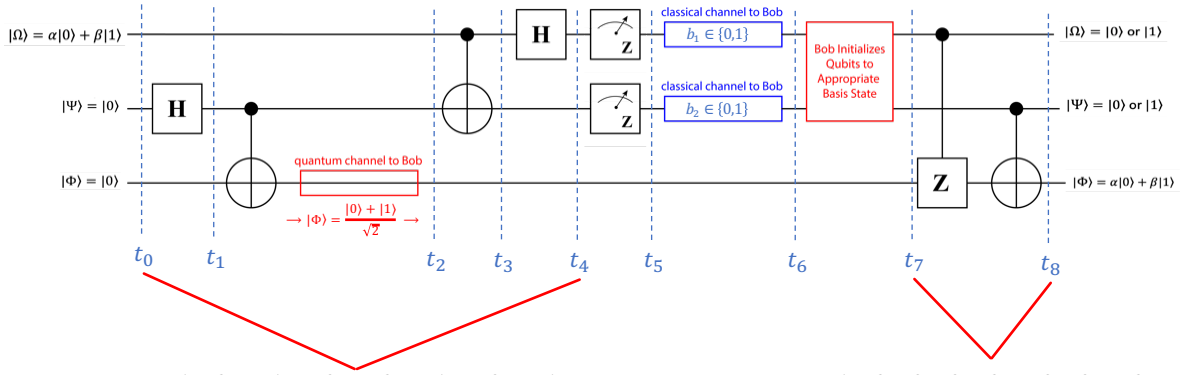
$$\mathbf{T}_0 = \frac{1}{2}\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & -1 \end{bmatrix}$$

- Bob's circuit from time t_7 to t_8 is represented by transfer matrix $\mathbf{T}_3$:

$$\mathbf{T}_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

66

Transfer Matrix of Entire Teleportation Circuit



$$\mathbf{T}_0 = \frac{1}{2}\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 1 & 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 & 1 & 0 & 1 & 0 \\ 1 & 0 & -1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & -1 & 0 & 1 \\ 0 & 1 & 0 & 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 & -1 & 0 & -1 & 0 \\ 1 & 0 & -1 & 0 & 0 & -1 & 0 & -1 \end{bmatrix}$$

$$\mathbf{T}_3 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

67

Quantum Teleportation: Summary

- Quantum Teleportation Exploits Entanglement to (theoretically) Instantly Transfer Information
  - information is NOT transmitted over a channel either wirelessly or over a wireline
- It does NOT instantly transfer matter or energy
- It does instantly transfer an energy state
- Requires Transmission of Matter/energy over a channel
- Successfully Demonstrated Experimentally
- Applications in Cyber Security
  - EXAMPLE: Secure Encryption Key Distribution
- Does NOT violate Speed-of-Light Transmission Limits (special relativity) since Information is NOT transmitted, but a quantum state host and 2 Classical bits are transmitted

68

BB84 Encryption Protocol

69

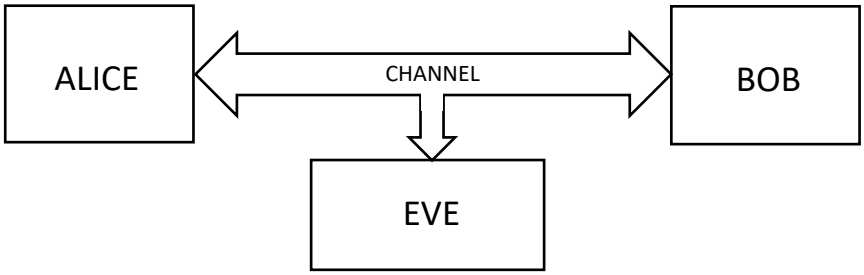
Symmetric Encryption

- *Symmetric Encryption* requires each party (Alice and Bob) to Share a Secret *Encryption Key*
- Once each Party is in possession of the *Secret Key*, they can send Encrypted messages to one another
- The sender, Alice, uses her Secret key to Encrypt the *Plaintext* into *Ciphertext*
  - "good" ciphertext has the statistical properties of appearing to resemble an equally-likely, random bit stream
- The receiver, Bob, uses the secret key to Decrypt the Ciphertext to obtain the Plaintext.
- The vulnerable portion of this encryption scheme is the Distribution of the Secret Keys (*i.e.*, "key distribution")

70

Eavesdropping MITM

- A BIG Problem in Key Distribution is a "Man-in-the-middle Eavesdropping" Attack



- In a Classical Wired or Wireless Communication Channel, Eavesdropping can occur during Key Exchange and defeats the entire process, special key exchange protocols established such as Diffie-Hellman for classical encryption
  - this is how the **`https`** protocol works, for example
  - based on very difficult-to-solve math problems (for Turing/classical computers)
- It is believed that Quantum Computers can defeat these methods since they are based on hard-to-solve Math Problems that can be much easier to solve for QC

71

Bennett & Brassard, 1984

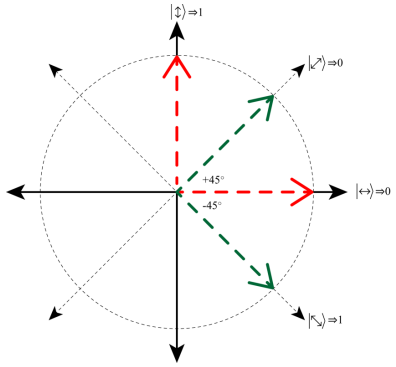
- A (more) Secure Cryptographic Key Exchange protocol for Classical Encryption was Devised in 1984 by Bennett and Brassard known as "BB84"
- Requires a Redundant Quantum Symbol, a Quantum Channel, as well as the Classical Channel
- Typically Implemented with Photons as "Flying Qubits" over a Channel comprised of Fiber Optic Cables (wired) or Free Space (wireless)
- Consider Photon Polarization as the Quantum Observable for a Symbol Set
  - symbols are 2 Orthogonal qubits, $|\leftrightarrow\rangle$, and $|\updownarrow\rangle$ and 2 Orthogonal qubits, $|\nearrow\rangle$, and $|\nwarrow\rangle$, known as the Rectilinear and Diagonal sets
  - redundant because two (2) representations of bit zero (0) and two representations of bit one (1)
  - $\{|\leftrightarrow\rangle, |\nearrow\rangle\}$ represent bit (0) and $\{|\updownarrow\rangle, |\nwarrow\rangle\}$ represent bit (1); note that these are Non-orthogonal for each Bit

72

Quantum Symbol Set

- Often referred to as:
  - Rectilinear Set: $R=\{|\leftrightarrow\rangle, |\updownarrow\rangle\}$ Represents Classical Bits: $\{0, 1\}$
  - Diagonal Set: $D=\{|\nearrow\rangle, |\nwarrow\rangle\}$ Represents Classical Bits: $\{0, 1\}$
- In total, this is a (complete) Non-Orthogonal Basis Set over $\mathbb{H}_2$, (*aka*, a Complete, Redundant, Non-orthogonal Basis)

Polarization Diagram

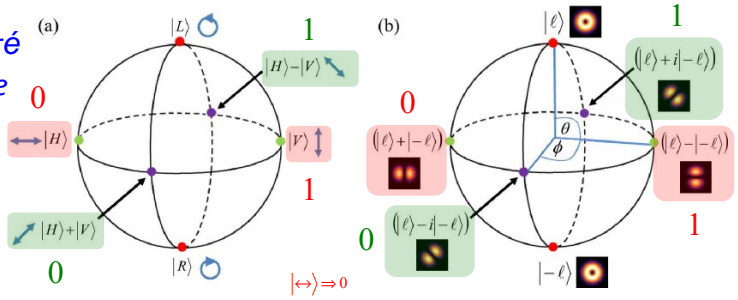


73

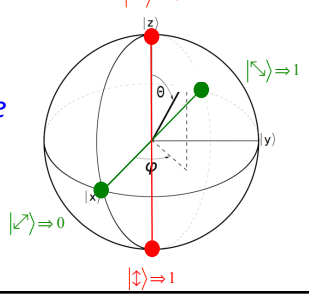
Poincaré and Bloch Sphere

- Non-orthogonal and Redundant Symbol Set

Poincaré Sphere



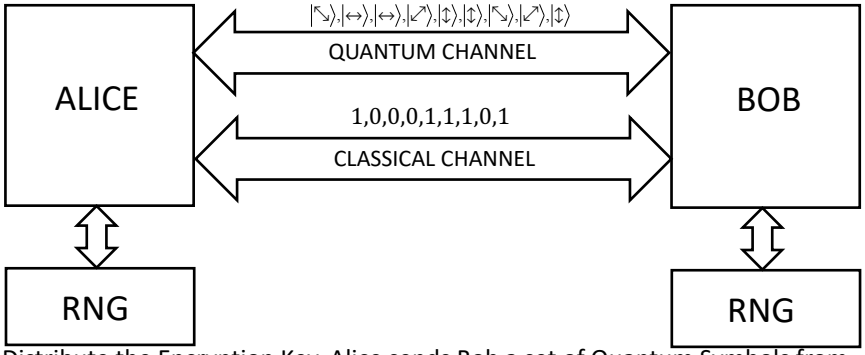
Bloch Sphere



74

Key Distribution Scheme

- The Encryption Key Distribution Scheme

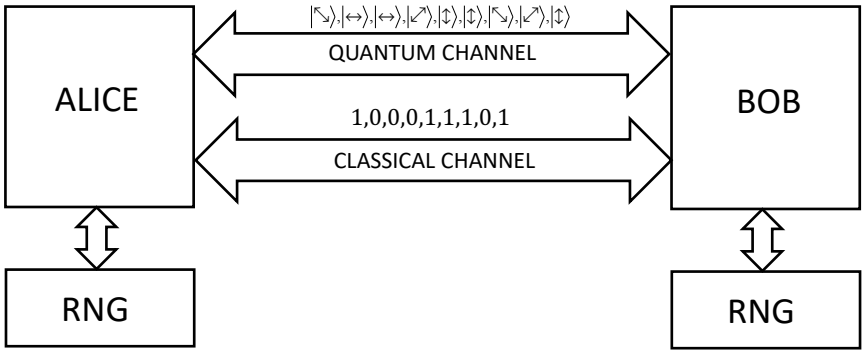


- To Distribute the Encryption Key, Alice sends Bob a set of Quantum Symbols from the Non-orthogonal Quantum Alphabet, $\{|\leftrightarrow\rangle, |\updownarrow\rangle, |\swarrow\rangle, |\nwarrow\rangle\}$
- Alice uses a Random Number Generator (RNG) to generate a Random String of Classical Bits to send to Bob
- Alice also uses the RNG again to choose whether to encode each Bit using one of the two Orthogonal Basis sets, $\mathbb{H}_{2,R}=\{0\Rightarrow|\leftrightarrow\rangle, 1\Rightarrow|\updownarrow\rangle\}$, or $\mathbb{H}_{2,D}=\{0\Rightarrow|\swarrow\rangle, 1\Rightarrow|\nwarrow\rangle\}$.

75

Key Distribution (cont.)

- The Encryption Key Distribution Scheme

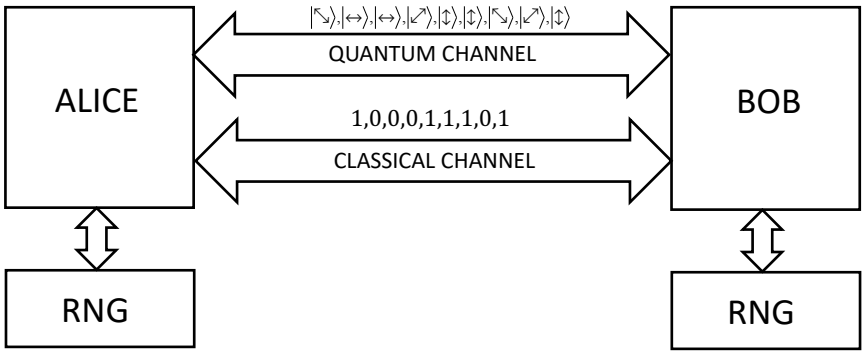


- Bob doesn't know whether Alice chose basis set $\mathbb{H}_{2,R}$ or basis set $\mathbb{H}_{2,D}$
- Bob uses his RNG to choose one of the two Measurement Bases, $\mathbb{H}_{2,R}$ or $\mathbb{H}_{2,D}$, to Measure each received Quantum Symbol
- If Bob chooses the Correct Observable, he Perfectly Measures Alice's Qubit, otherwise he collapses Alice's Qubit randomly into either a 0 or a 1 and, on average, he "guesses" the Correct Observable half of the time

76

Key Distribution (cont.)

- The Encryption Key Distribution Scheme



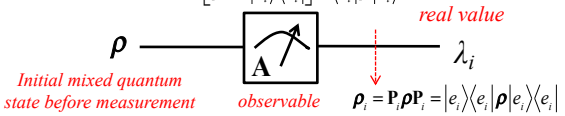
- After Alice has sent a suitably long string of qubits, Bob uses the Classical Channel to tell Alice which Observable he used, $\mathbf{A}_Z$ or $\mathbf{A}_X$, to measure each qubit, but he DOES NOT tell Alice the measurement outcome
- Alice uses the classical channel to tell Bob which time he used the "correct" Observable
- Alice and Bob discard the Bits corresponding to Bob's "incorrect" Measurements and they now share a set of bits that Bob correctly measured; this can serve as their secret key and they can use it for Encrypted Communication over the Classical Channel

77

Alice's Quantum Symbol Alphabet

- Recall Projective Measurements:

$$\text{Prob}\left[\boldsymbol{\rho} \Rightarrow |a_i\rangle\langle a_i|\right] = \langle a_i|\boldsymbol{\rho}|a_i\rangle$$



- Assume Alice is using $\mathbb{H}_{2,R}$, if she has a perfect RNG, then p_k=1/2 and the alphabet is:

$$\rho_R = \sum_{k=0}^{n-1} p_k |\Psi_k\rangle\langle\Psi_k| == p_0|\leftrightarrow\rangle\langle\leftrightarrow| + p_1|\updownarrow\rangle\langle\updownarrow| = \frac{1}{2}\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1&0\end{bmatrix} + \frac{1}{2}\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0&1\end{bmatrix}$$

$$= \frac{1}{2}\begin{bmatrix}1&0\\0&0\end{bmatrix} + \frac{1}{2}\begin{bmatrix}0&0\\0&1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1&0\\0&1\end{bmatrix}$$

- Likewise, when Alice uses $\mathbb{H}_{2,D}$ with a perfect RNG:

$$\rho_D = \sum_{k=0}^{n-1} p_k |\Psi_k\rangle\langle\Psi_k| = p_0|\swarrow\rangle\langle\swarrow| + p_1|\nwarrow\rangle\langle\nwarrow| = \frac{1}{2}\left(\frac{1}{\sqrt{2}}\right)^2\begin{bmatrix}1\\1\end{bmatrix}\begin{bmatrix}1&1\end{bmatrix} + \frac{1}{2}\left(\frac{1}{\sqrt{2}}\right)^2\begin{bmatrix}1\\-1\end{bmatrix}\begin{bmatrix}1&-1\end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix}1&1\\1&1\end{bmatrix} + \frac{1}{4}\begin{bmatrix}1&-1\\-1&1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1&0\\0&1\end{bmatrix}$$

- Thus, we see that:

$$\rho_A = \rho_R = \rho_D$$

78

Recall the Observables

- Projective measurements use an Observable constructed from the Measure Basis:

$$\mathbf{A} = \sum_{i=1}^{n} \lambda_i \mathbf{P}_i = \sum_{i=1}^{n} \lambda_i \left|e_i\right\rangle\left\langle e_i\right|$$

- Rectilinear Basis, $\mathbb{H}_{2,R}$, uses Observable $\mathbf{A_Z}$ with measurement outcomes $\{\lambda_{\leftrightarrow}, \lambda_{\updownarrow}\}=\{-1,+1\}$:

$$\mathbf{A_Z} = \lambda_{\leftrightarrow}\left|\leftrightarrow\right\rangle\left\langle\leftrightarrow\right| + \lambda_{\updownarrow}\left|\updownarrow\right\rangle\left\langle\updownarrow\right| = (1)\begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} + (-1)\begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Diagonal Basis, $\mathbb{H}_{2,D}$, uses Observable $\mathbf{A_X}$ with measurement outcomes $\{\lambda_{\swarrow\nearrow}, \lambda_{\nwarrow\searrow}\}=\{+1,-1\}$:

$$\mathbf{A_X} = \lambda_{\swarrow\nearrow}\left|\swarrow\nearrow\right\rangle\left\langle\swarrow\nearrow\right| + \lambda_{\nwarrow\searrow}\left|\nwarrow\searrow\right\rangle\left\langle\nwarrow\searrow\right| = \lambda_{\swarrow\nearrow}\left(\frac{1}{\sqrt{2}}\right)^2\begin{bmatrix} 1 \\ 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \end{bmatrix} + \lambda_{\nwarrow\searrow}\left(\frac{1}{\sqrt{2}}\right)^2\begin{bmatrix} 1 \\ -1 \end{bmatrix}\begin{bmatrix} 1 & -1 \end{bmatrix}$$

$$= \lambda_{\swarrow\nearrow}\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \lambda_{\nwarrow\searrow}\frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = (1)\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + (-1)\frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- Alice chooses the Encoding Basis, $\mathbb{H}_{2,R}$ or $\mathbb{H}_{2,D}$, randomly and Bob chooses the Measurement Observable, $\mathbf{A_Z}$ or $\mathbf{A_X}$, randomly based on their own RNG outputs.
- The total event space is comprised of four (4) different events:
  1) E1: Alice chooses $\mathbb{H}_{2,R}$ and Bob chooses $\mathbf{A_Z}$; Bob correctly measures Alice's qubit
  2) E2: Alice chooses $\mathbb{H}_{2,R}$ and Bob chooses $\mathbf{A_X}$; Bob incorrectly measures Alice's qubit, random result
  3) E3: Alice chooses $\mathbb{H}_{2,D}$ and Bob chooses $\mathbf{A_Z}$; Bob incorrectly measures Alice's qubit, random result
  4) E4: Alice chooses $\mathbb{H}_{2,D}$ and Bob chooses $\mathbf{A_X}$; Bob correctly measures Alice's qubit

79

Expected Value of Measurements

- Projective measurements use an Observable constructed from the Measure Basis:

$$\mathbf{A} = \sum_{i=1}^{n} \lambda_i \mathbf{P}_i = \sum_{i=1}^{n} \lambda_i \left|e_i\right\rangle\left\langle e_i\right|$$

- Rectilinear Basis, $\mathbb{H}_{2,R}$, uses Observable $\mathbf{A_Z}$ with measurement outcomes $\{\lambda_{\leftrightarrow}, \lambda_{\updownarrow}\}=\{-1,+1\}$:

$$\mathbf{A_Z} = \lambda_{\leftrightarrow}\left|\leftrightarrow\right\rangle\left\langle\leftrightarrow\right| + \lambda_{\updownarrow}\left|\updownarrow\right\rangle\left\langle\updownarrow\right| = (1)\begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} + (-1)\begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Diagonal Basis, $\mathbb{H}_{2,D}$, uses Observable $\mathbf{A_X}$ with measurement outcomes $\{\lambda_{\swarrow\nearrow}, \lambda_{\nwarrow\searrow}\}=\{+1,-1\}$:

$$\mathbf{A_X} = \lambda_{\swarrow\nearrow}\left|\swarrow\nearrow\right\rangle\left\langle\swarrow\nearrow\right| + \lambda_{\nwarrow\searrow}\left|\nwarrow\searrow\right\rangle\left\langle\nwarrow\searrow\right| = \lambda_{\swarrow\nearrow}\left(\frac{1}{\sqrt{2}}\right)^2\begin{bmatrix} 1 \\ 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \end{bmatrix} + \lambda_{\nwarrow\searrow}\left(\frac{1}{\sqrt{2}}\right)^2\begin{bmatrix} 1 \\ -1 \end{bmatrix}\begin{bmatrix} 1 & -1 \end{bmatrix}$$

$$= \lambda_{\swarrow\nearrow}\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \lambda_{\nwarrow\searrow}\frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = (1)\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + (-1)\frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

- We can compute the Expected Value of Bob's measurements for the Four different Events
- Recall that the Expected Value of a Measurement is given by:

$$\left\langle \mathbf{A} \right\rangle_{\rho} = \sum_{j=1}^{m} p_j \left\langle \mathbf{\Psi}_j \middle| \mathbf{A} \middle| \mathbf{\Psi}_j \right\rangle = \mathrm{Trace}\left(\boldsymbol{\rho}\mathbf{A}\right)$$

80

Expected Value of Measurements (cont.)

- When Bob chooses to use observable $\mathbf{A}_Z$:

$$\langle \mathbf{A}_Z \rangle_\rho = \text{Trace}(\rho \mathbf{A}_X) = \text{Trace}\left(\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) = \text{Trace}\left(\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) = 0$$

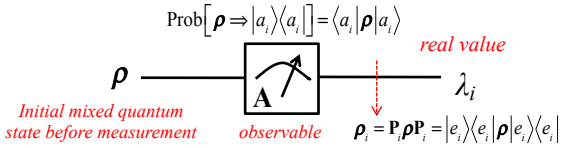
- Since Bob's measurement outcomes are $\{\lambda_{\leftrightarrow}, \lambda_{\updownarrow}\}=\{-1,+1\}$, this means that it is expected that he will measure $\lambda_{\leftrightarrow}=-1$ half of the time and $\lambda_{\updownarrow}=+1$ half of the time
- Likewise, when Bob chooses to use observable $\mathbf{A}_X$:

$$\langle \mathbf{A}_X \rangle_\rho = \text{Trace}(\rho \mathbf{A}_X) = \text{Trace}\left(\frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = \text{Trace}\left(\frac{1}{2}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = 0$$

- Since Bob's measurement outcomes are $\{\lambda_{\swarrow}, \lambda_{\nwarrow}\}=\{+1,-1\}$, this means that it is expected that he will measure $\lambda_{\swarrow} = +1$ half of the time and $\lambda_{\nwarrow} = -1$ half of the time
- We can now compute the probabilities for each of the four events:
  1) E1: Alice chooses $\mathbb{H}_{2,R}$ and Bob chooses $\mathbf{A}_Z$; Bob correctly measures Alice's qubit
  2) E2: Alice chooses $\mathbb{H}_{2,R}$ and Bob chooses $\mathbf{A}_X$; Bob incorrectly measures Alice's qubit, random result
  3) E3: Alice chooses $\mathbb{H}_{2,D}$ and Bob chooses $\mathbf{A}_Z$; Bob incorrectly measures Alice's qubit, random result
  4) E4: Alice chooses $\mathbb{H}_{2,D}$ and Bob chooses $\mathbf{A}_X$; Bob correctly measures Alice's qubit

81

Probabilities of Each Event



- **E1**: Alice chooses $\mathbb{H}_{2,R}$ and Bob chooses $\mathbf{A}_Z$; Bob correctly measures Alice's qubit. 2 cases:

1) Alice sends $|\leftrightarrow\rangle$ representing the classic bit "0":

$$\rho_{\text{Sent}} = \sum_{k=0}^{0} p_k |\leftrightarrow\rangle\langle\leftrightarrow| = p_0 |\leftrightarrow\rangle\langle\leftrightarrow| = (1)\begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\text{Prob}[\text{Bob correctly measures } |\leftrightarrow\rangle \Rightarrow 0] = \text{Prob}[\rho_{\text{Bob}} \Rightarrow |\leftrightarrow\rangle\langle\leftrightarrow|] = \langle\leftrightarrow|\rho_{\text{Sent}}|\leftrightarrow\rangle$$

$$= \begin{bmatrix} 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1$$

$$\text{Prob}[\text{Bob incorrectly measures } |\updownarrow\rangle \Rightarrow 1] = \text{Prob}[\rho_{\text{Bob}} \Rightarrow |\updownarrow\rangle\langle\updownarrow|] = \langle\updownarrow|\rho_{\text{Sent}}|\updownarrow\rangle$$

$$= \begin{bmatrix} 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 0$$

1) Alice sends $|\updownarrow\rangle$ representing the classic bit "1": (cont. on next slide)

82

Probabilities of Each Event (cont.)

- **E1**: Alice chooses $\mathbb{H}_{2,R}$ and Bob chooses $\mathbf{A_Z}$; Bob correctly measures Alice's qubit. 2 cases:

  2) Alice sends $|\updownarrow\rangle$ representing the classic bit "1":

$$\rho_{\text{Sent}} = \sum_{k=0}^{0} p_k |\updownarrow\rangle\langle\updownarrow| = p_1 |\updownarrow\rangle\langle\updownarrow| = (1)\begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\leftrightarrow\rangle \Rightarrow 0\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\leftrightarrow\rangle\langle\leftrightarrow|\right] = \langle\leftrightarrow|\rho_{\text{Sent}}|\leftrightarrow\rangle$$

$$= \begin{bmatrix} 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 & 0 \end{bmatrix}\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 0$$

$$\text{Prob}\left[\text{Bob correctly measures } |\updownarrow\rangle \Rightarrow 1\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\updownarrow\rangle\langle\updownarrow|\right] = \langle\updownarrow|\rho_{\text{Sent}}|\updownarrow\rangle$$

$$= \begin{bmatrix} 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = 1$$

83

Probabilities of Each Event (cont.)

- **E2**: Alice chooses $\mathbb{H}_{2,R}$ and Bob chooses $\mathbf{A_X}$; Bob incorrectly measures Alice's qubit. 2 cases:

  1) Alice sends $|\leftrightarrow\rangle$ representing the classic bit "0":

$$\rho_{\text{Sent}} = \sum_{k=0}^{0} p_k |\leftrightarrow\rangle\langle\leftrightarrow| = p_0 |\leftrightarrow\rangle\langle\leftrightarrow| = (1)\begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\nearrow\rangle \Rightarrow 0\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\nearrow\rangle\langle\nearrow|\right] = \langle\nearrow|\rho_{\text{Sent}}|\nearrow\rangle$$

$$= \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{2}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\nwarrow\rangle \Rightarrow 1\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\nwarrow\rangle\langle\nwarrow|\right] = \langle\nwarrow|\rho_{\text{Sent}}|\nwarrow\rangle$$

$$= \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix} 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{2}$$

  1) Alice sends $|\updownarrow\rangle$ representing the classic bit "1": (cont. on next slide)

84

Probabilities of Each Event (cont.)

- **E2**: Alice chooses $\mathbb{H}_{2,R}$ and Bob chooses $\mathbf{A_X}$; Bob incorrectly measures Alice's qubit. 2 cases:
  2) Alice sends $|\updownarrow\rangle$ representing the classic bit "1":

$$\rho_{\text{Sent}} = \sum_{k=0}^{0} p_k |\updownarrow\rangle\langle\updownarrow| = p_1 |\updownarrow\rangle\langle\updownarrow| = (1)\begin{bmatrix} 0 \\ 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\nearrow\rangle \Rightarrow 0\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\nearrow\rangle\langle\nearrow|\right] = \langle\nearrow|\rho_{\text{Sent}}|\nearrow\rangle$$
$$= \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{2}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\nwarrow\rangle \Rightarrow 1\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\nwarrow\rangle\langle\nwarrow|\right] = \langle\nwarrow|\rho_{\text{Sent}}|\nwarrow\rangle$$
$$= \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix} 1 & -1 \end{bmatrix}\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ -1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ -1 \end{bmatrix} = \frac{1}{2}$$

85

Probabilities of Each Event (cont.)

- **E3**: Alice chooses $\mathbb{H}_{2,D}$ and Bob chooses $\mathbf{A_Z}$; Bob incorrectly measures Alice's qubit. 2 cases:
  1) Alice sends $|\nearrow\rangle$ representing the classic bit "0":

$$\rho_{\text{Sent}} = \sum_{k=0}^{0} p_k |\nearrow\rangle\langle\nearrow| = p_0 |\nearrow\rangle\langle\nearrow| = (1)\left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix} 1 \\ 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\leftrightarrow\rangle \Rightarrow 0\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\leftrightarrow\rangle\langle\leftrightarrow|\right] = \langle\leftrightarrow|\rho_{\text{Sent}}|\leftrightarrow\rangle$$
$$= \begin{bmatrix} 1 & 0 \end{bmatrix}\left(\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\right)\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \end{bmatrix}\frac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\updownarrow\rangle \Rightarrow 1\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\updownarrow\rangle\langle\updownarrow|\right] = \langle\updownarrow|\rho_{\text{Sent}}|\updownarrow\rangle$$
$$= \begin{bmatrix} 0 & 1 \end{bmatrix}\left(\frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\right)\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \end{bmatrix}\frac{1}{2}\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2}$$

  1) Alice sends $|\nwarrow\rangle$ representing the classic bit "1": (cont. on next slide)

86

Probabilities of Each Event (cont.)

- **E3**: Alice chooses $\mathbb{H}_{2,D}$ and Bob chooses $\mathbf{A}_Z$; Bob incorrectly measures Alice's qubit. 2 cases:
  2) Alice sends $|\nwarrow\rangle$ representing the classic bit "1":

$$\rho_{\text{Sent}} = \sum_{k=0}^{0} p_k |\nwarrow\rangle\langle\nwarrow| = p_1 |\nwarrow\rangle\langle\nwarrow| = (1)\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 \\ -1 \end{bmatrix}\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\leftrightarrow\rangle \Rightarrow 0\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\leftrightarrow\rangle\langle\leftrightarrow|\right] = \langle\leftrightarrow|\rho_{\text{Sent}}|\leftrightarrow\rangle$$
$$= \begin{bmatrix} 1 & 0 \end{bmatrix}\left(\frac{1}{2}\right)\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & 0 \end{bmatrix}\frac{1}{2}\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{2}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\updownarrow\rangle \Rightarrow 1\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\updownarrow\rangle\langle\updownarrow|\right] = \langle\updownarrow|\rho_{\text{Sent}}|\updownarrow\rangle$$
$$= \begin{bmatrix} 0 & 1 \end{bmatrix}\left(\frac{1}{2}\right)\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 0 & 1 \end{bmatrix}\begin{bmatrix} -1 \\ 1 \end{bmatrix} = \frac{1}{2}$$

87

Probabilities of Each Event (cont.)

- **E4**: Alice chooses $\mathbb{H}_{2,D}$ and Bob chooses $\mathbf{A}_X$; Bob correctly measures Alice's qubit. 2 cases:
  1) Alice sends $|\nearrow\rangle$ representing the classic bit "0":

$$\rho_{\text{Sent}} = \sum_{k=0}^{0} p_k |\swarrow\rangle\langle\swarrow| = p_0 |\swarrow\rangle\langle\swarrow| = (1)\left(\frac{1}{\sqrt{2}}\right)^2\begin{bmatrix} 1 \\ 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

$$\text{Prob}\left[\text{Bob correctly measures } |\swarrow\rangle \Rightarrow 0\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\swarrow\rangle\langle\swarrow|\right] = \langle\swarrow|\rho_{\text{Sent}}|\swarrow\rangle$$
$$= \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 & 1 \end{bmatrix}\left(\frac{1}{2}\right)\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 2 \\ 2 \end{bmatrix} = 1$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\nwarrow\rangle \Rightarrow 1\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\nwarrow\rangle\langle\nwarrow|\right] = \langle\nwarrow|\rho_{\text{Sent}}|\nwarrow\rangle$$
$$= \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 & -1 \end{bmatrix}\left(\frac{1}{2}\right)\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 1 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 0$$

  2) Alice sends $|\nwarrow\rangle$ representing the classic bit "1": (cont. on next slide)

88

Probabilities of Each Event (cont.)

- **E4**: Alice chooses $\mathbb{H}_{2,D}$ and Bob chooses $\mathbf{A_X}$; Bob correctly measures Alice's qubit. 2 cases:

  2) Alice sends $|\nwarrow\rangle$ representing the classic bit "1":

$$\rho_{\text{Sent}} = \sum_{k=0}^{0} p_k |\nwarrow\rangle\langle\nwarrow| = p_1 |\nwarrow\rangle\langle\nwarrow| = (1)\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 \\ -1 \end{bmatrix}\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

$$\text{Prob}\left[\text{Bob incorrectly measures } |\nearrow\rangle \Rightarrow 0\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\nearrow\rangle\langle\nearrow|\right] = \langle\nearrow|\rho_{\text{Sent}}|\nearrow\rangle$$

$$= \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 & 1 \end{bmatrix}\left(\frac{1}{2}\right)\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 1 & 1 \end{bmatrix}\begin{bmatrix} 0 \\ 0 \end{bmatrix} = 0$$

$$\text{Prob}\left[\text{Bob correctly measures } |\nwarrow\rangle \Rightarrow 1\right] = \text{Prob}\left[\rho_{\text{Bob}} \Rightarrow |\nwarrow\rangle\langle\nwarrow|\right] = \langle\nwarrow|\rho_{\text{Sent}}|\nwarrow\rangle$$

$$= \left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 & -1 \end{bmatrix}\left(\frac{1}{2}\right)\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}\left(\frac{1}{\sqrt{2}}\right)\begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 1 & -1 \end{bmatrix}\begin{bmatrix} 2 \\ -2 \end{bmatrix} = 1$$

89

Summary of Different Events

- Summary of Events:

	Alice Sends:	Bob Measures with Observable:	Probability that Bob Receives the Correct "Bit"	Sending/Measurement Bases Match ?
E1	$\|\leftrightarrow\rangle \Rightarrow 0$	$\mathbf{A_Z}$	1	YES
	$\|\leftrightarrow\rangle \Rightarrow 0$	$\mathbf{A_X}$	½	NO
E2	$\|\updownarrow\rangle \Rightarrow 1$	$\mathbf{A_Z}$	1	YES
	$\|\updownarrow\rangle \Rightarrow 1$	$\mathbf{A_X}$	½	NO
E3	$\|\nearrow\rangle \Rightarrow 0$	$\mathbf{A_Z}$	½	NO
	$\|\nearrow\rangle \Rightarrow 0$	$\mathbf{A_X}$	1	YES
E4	$\|\nwarrow\rangle \Rightarrow 1$	$\mathbf{A_Z}$	½	NO
	$\|\nwarrow\rangle \Rightarrow 1$	$\mathbf{A_X}$	1	YES

- We can compute the the overall probability that Bob obtains the classical bit (after randomly choosing one of the two Measurement bases) that Alice intended to send

90

Probability Bob Receives "Correct" Bit

- Assume that Alice and Bob Possess Independent and Very High Quality RNGs
  - this means that each RNG bit is equally likely to be 0 or 1
- Probability Bob obtains the "correct" bit:

$$\Pr[\text{Bob obtains correct bit}] = \Pr[\text{Alice sends 0}]\Pr[\text{Bob obtains 0}] + \Pr[\text{Alice sends 1}]\Pr[\text{Bob obtains 1}]$$

- Probability Bob obtains 0-valued Bit:

$$\Pr[\text{Bob obtains 0}] = \Pr[\text{Bob uses "correct" observable}]$$
$$+ \Pr[\text{Bob uses "incorrect" observable}]\Pr[\text{Bob measures "correct" bit with wrong observable}]$$

- Probability Bob obtains 1-valued Bit:

$$\Pr[\text{Bob obtains 1}] = \Pr[\text{Bob uses "correct" observable}]$$
$$+ \Pr[\text{Bob uses "incorrect" observable}]\Pr[\text{Bob measures "correct" bit with wrong observable}]$$

- Born's Rule (subjective probability):

$$\Pr[\text{Bob measures "correct" bit with wrong observable}] = \frac{1}{2}$$

91

Probability Bob Receives "Correct" Bit (cont.)

- From Bob's RNG:

$$\Pr[\text{Bob uses "correct" observable}] = \frac{1}{2} \qquad \Pr[\text{Bob uses "incorrect" observable}] = \frac{1}{2}$$

- Probability Bob obtains 0-valued Bit:

$$\Pr[\text{Bob obtains 0}] = \Pr[\text{Bob uses "correct" observable}]$$
$$+ \Pr[\text{Bob uses "incorrect" observable}]\Pr[\text{Bob measures "correct" bit with wrong observable}]$$
$$= \frac{1}{2} + \left(\frac{1}{2}\right)\left(\frac{1}{2}\right) = \frac{3}{4}$$

- Probability Bob obtains 1-valued Bit:

$$\Pr[\text{Bob obtains 1}] = \Pr[\text{Bob uses "correct" observable}]$$
$$+ \Pr[\text{Bob uses "incorrect" observable}]\Pr[\text{Bob measures "correct" bit with wrong observable}]$$
$$= \frac{1}{2} + \left(\frac{1}{2}\right)\left(\frac{1}{2}\right) = \frac{3}{4}$$

- From Alice's RNG:

$$\Pr[\text{Alice sends 0}] = \frac{1}{2} \qquad \Pr[\text{Alice sends 1}] = \frac{1}{2}$$

92

Probability Bob Receives "Correct" Bit (cont.)

- Overall probability Bob obtains the correct bit is:

$$\Pr[\text{Bob obtains correct bit}] = \Pr[\text{Alice sends } 0]\Pr[\text{Bob obtains } 0] + \Pr[\text{Alice sends } 1]\Pr[\text{Bob obtains } 1]$$

$$\Pr[\text{Bob obtains } 0] = \frac{3}{4} \qquad \Pr[\text{Bob obtains } 1] = \frac{3}{4}$$

$$\Pr[\text{Alice sends } 0] = \frac{1}{2} \qquad \Pr[\text{Alice sends } 1] = \frac{1}{2}$$

$$\Pr[\text{Bob obtains correct bit}] = \Pr[\text{Alice sends } 0]\Pr[\text{Bob obtains } 0] + \Pr[\text{Alice sends } 1]\Pr[\text{Bob obtains } 1]$$
$$= \left(\frac{1}{2}\right)\left(\frac{3}{4}\right) + \left(\frac{1}{2}\right)\left(\frac{3}{4}\right) = \frac{3}{8} + \frac{3}{8} = \frac{3}{4}$$

- Thus, Bob will possess 75% of the True-valued Bits that Alice intended to Send
- Alice will then send Bob a Bit-string over the Classical Channel that Indicates if she used the $\mathbb{H}_{2,R}$ or $\mathbb{H}_{2,D}$ Basis
- Bob can discard those Bits he Measured with the Incorrect Measurement Basis

93

Bob's Bits

- On Average, Bob will have Chosen the Correct Measurement Basis 50% of the time
- He Discards the Following Events:

	Alice Sends:	Bob Measures with Observable:	Probability that Bob Receives the Correct "Bit"	Sending/Measurement Bases Match ?
E1	$\|\leftrightarrow\rangle \Rightarrow 0$	$\mathbf{A}_z$	1	YES
	~~$\|\updownarrow\rangle \Rightarrow 0$~~	~~$\mathbf{A}_x$~~	~~½~~	~~NO~~
E2	$\|\updownarrow\rangle \Rightarrow 1$	$\mathbf{A}_z$	1	YES
	~~$\|\leftrightarrow\rangle \Rightarrow 1$~~	~~$\mathbf{A}_x$~~	~~½~~	~~NO~~
E3	~~$\|\nearrow\rangle \Rightarrow 0$~~	~~$\mathbf{A}_z$~~	~~½~~	~~NO~~
	$\|\swarrow\rangle \Rightarrow 0$	$\mathbf{A}_x$	1	YES
E4	~~$\|\searrow\rangle \Rightarrow 1$~~	~~$\mathbf{A}_z$~~	~~½~~	~~NO~~
	$\|\nwarrow\rangle \Rightarrow 1$	$\mathbf{A}_x$	1	YES

- Bob now possesses half (on average) of the bits Alice sent, but they are all 100% accurate

94

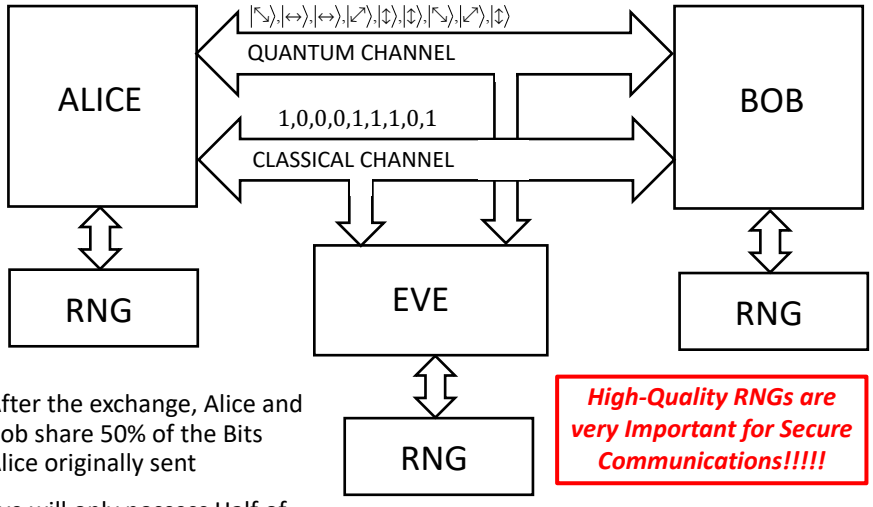
Alice's Bits

- Next, Bob sends Alice a bit-string over the classical channel indicating which bits he Incorrectly Measured
- Alice discards the Bits that Bob Measured Incorrectly
- Alice and Bob now both possess about 50% of the bits that Alice Randomly Generated (with her RNG)
- They can now use their bitstrings as a Secret Encryption Key and can send Ciphertext traffic over the Classical Channel
- Key Distribution has thus been Accomplished
- An Eavesdropper, Eve, on the Quantum Channel is Forced to make Random Choices of Measurement Bases and thus would make Measurement choices Independent of Bob's measurement basis choices
- Even when Eve can also "snoop" the Classical channel, she could only determine which bits were correctly exchanged between Bob and Alice, but she could NOT determine what the bit-values are

95

MITM Eavesdropper

- Consider this Scenario



- After the exchange, Alice and Bob share 50% of the Bits Alice originally sent

High-Quality RNGs are very Important for Secure Communications!!!!!

- Eve will only possess Half of those or 25% AND she will NOT KNOW which half are correct !!!!!

96

BB84 Illustrated

https://youtu.be/LaLzshIosDk (1:56)

97

BB84 Explained

https://www.youtube.com/watch?v=uiiaAJ3c6dM (5:57)

98