Department of Information Engineering
MSc in Computer Engineering (a.y. 2024/2025)
University of Pisa

Quantum Computing and Quantum Internet

Luciano Lenzini
Full Professor
Department of Information Engineering
School of Engineering
University of Pisa, Italy
e-mail: lenzini44@gmail.com
http://www.iet.unipi.it/~lenzini/
http://www.originiinternetitalia.it/it/

Teleportation Using Werner States

Teleportation Using Werner States

- The procedure described in an earlier lecture allows for perfect teleportation of a state if one assumes that
  1. *perfect EPR pairs* are available
  2. *gates are perfect* and the
  3. *measurements are perfect*

  which is obviously **not** the case in practice

Teleportation Using Werner States

- To make the analysis more realistic, in what follows we assume that the EPR pairs *will not be maximally entangled*
- However, we continue to assume that *gates* and *measurements are perfect*
- We show that teleportation is still possible but *will not be perfect*

Teleportation Using Werner States

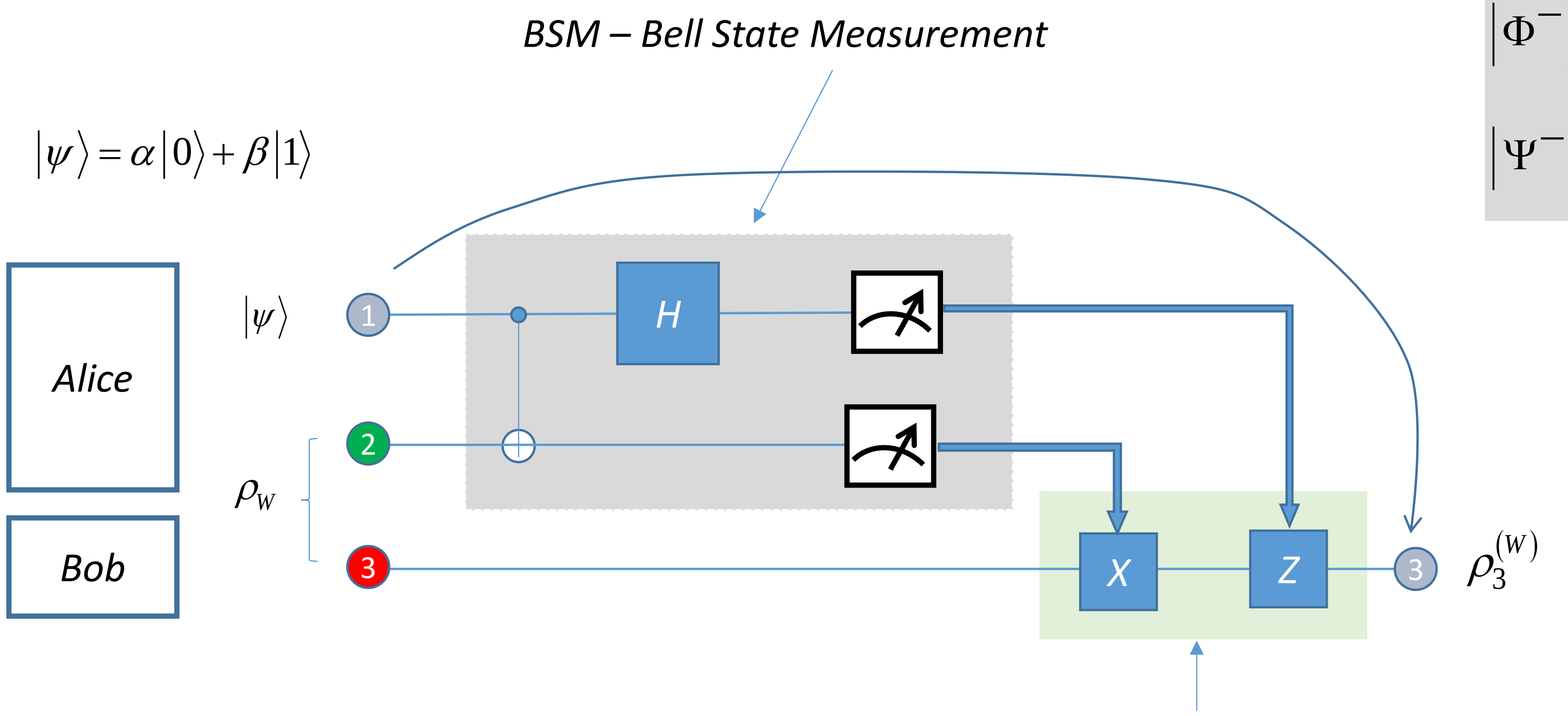
$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

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



Correction Operations

$$\rho_W = F|\Phi^+\rangle\langle\Phi^+| + \frac{1-F}{3}\left(|\Psi^-\rangle\langle\Psi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|\right)$$

Teleportation Using Werner States

- Instead of a perfect EPR pair, e.g. $|\Phi^+\rangle$, let us use a pair in a Werner state

$$\rho_W = A|\Phi^+\rangle\langle\Phi^+| + \frac{1-A}{3}\left(|\Psi^-\rangle\langle\Psi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|\right)$$

- The fidelity of this state with respect to $|\Phi^+\rangle$ is given by the quantity

$$F = \langle\Phi^+|\rho_W|\Phi^+\rangle = A$$

- As we discussed in an earlier lecture, *F* is the overlap of the *real state* ρ_W with the *ideal state* $|\Phi^+\rangle$, and thus *F* indicates how close the state ρ_W is to the ideal state $|\Phi^+\rangle$
- Since *F* = *A*, we use to write the Werner state as follows

$$\rho_W = F|\Phi^+\rangle\langle\Phi^+| + \frac{1-F}{3}\left(|\Psi^-\rangle\langle\Psi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|\right)$$

Teleportation Using Werner States

– Clearly, F = 1 defines a perfect EPR pair, and F = 1/4 corresponds to a completely depolarized state:

$$\rho_W = \frac{1}{4}\left(\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Phi^-\right\rangle\left\langle\Phi^-\right|\right) = \frac{1}{4} I$$

Teleportation Using Werner States

- Since we did not use a *perfect EPR pair,* the resulting state $\rho_3^{(W)}$ of *qubit 3* is no longer pure, but has the form:

$$\rho_3^{(W)} = |0\rangle\langle 0|\left(\frac{2F+1}{3}|\alpha|^2 + \frac{2(1-F)}{3}|\beta|^2\right)$$
$$+|0\rangle\langle 1|\left(\frac{4F-1}{3}\alpha\beta^*\right)$$
$$+|1\rangle\langle 0|\left(\frac{4F-1}{3}\alpha^*\beta\right)$$
$$+|1\rangle\langle 1|\left(\frac{2F+1}{3}|\beta|^2 + \frac{2(1-F)}{3}|\alpha|^2\right)$$

$$\rho_3^{(\Phi^+)} = |0\rangle\langle 0|\left(|\alpha|^2\right)$$
$$+|0\rangle\langle 1|\alpha\beta^*$$
$$+|1\rangle\langle 0|\alpha^*\beta$$
$$+|1\rangle\langle 1|\left(|\beta|^2\right)$$

Resulting state with *EPR* (*F* = 1)

Teleportation Using Werner States

– To see how close this state is to the initial state

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

one simply calculates the overlap between the ideal output state and the noisy state after teleportation

– One finds

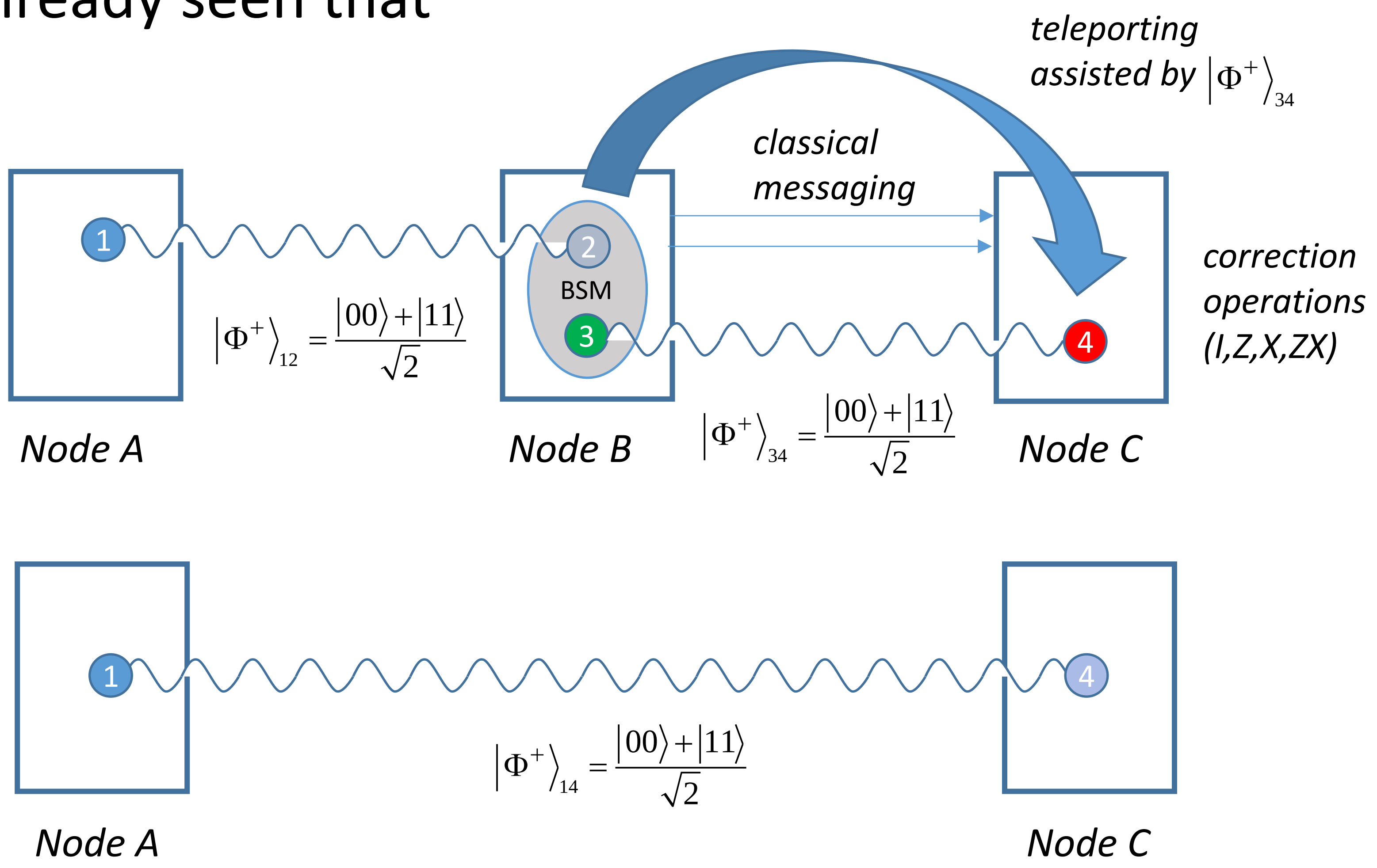
$$\hat{F} = \langle\psi|\rho_3^{(W)}|\psi\rangle = \frac{2F+1}{3} < 1$$

which is *independent* of the coefficients α and β

– Every state is thus teleported *with the same fidelity* $\hat{F} = (2F+1)/3$

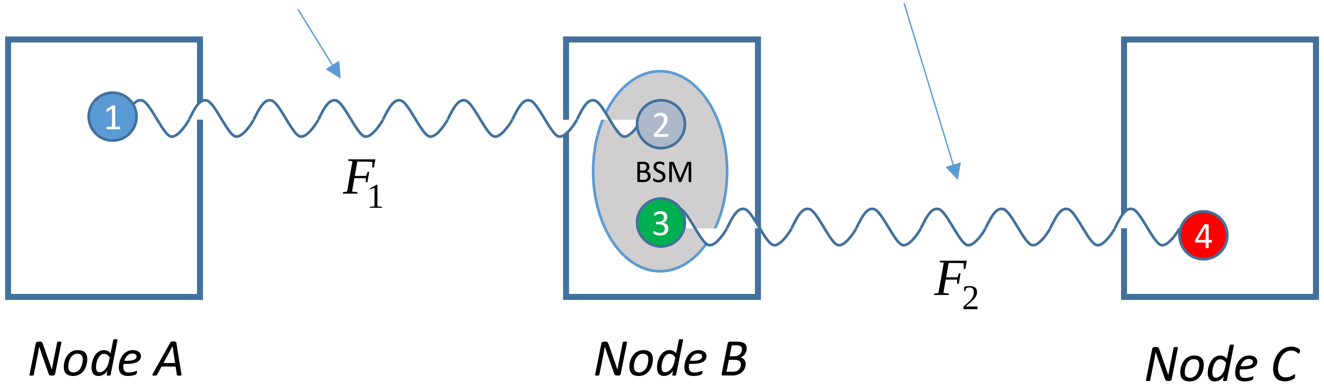
Entanglement Swapping of two EPR States

We have already seen that

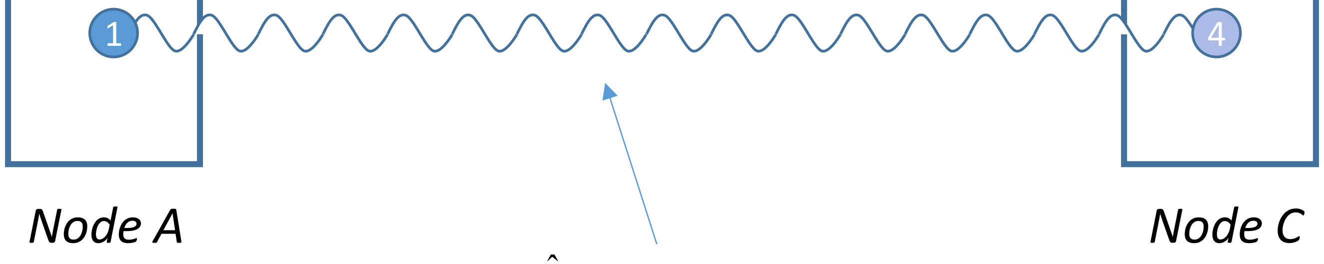


Entanglement Swapping of Two Werner States

$$\rho_{12} = F_1 |\Phi^+\rangle\langle\Phi^+| + \frac{1-F_1}{3}\left(|\Psi^-\rangle\langle\Psi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|\right) \qquad \rho_{34} = F_2 |\Phi^+\rangle\langle\Phi^+| + \frac{1-F_2}{3}\left(|\Psi^-\rangle\langle\Psi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|\right)$$



$$\hat{F} = F_1 F_2 + \frac{1}{3}(1-F_1)(1-F_2)$$



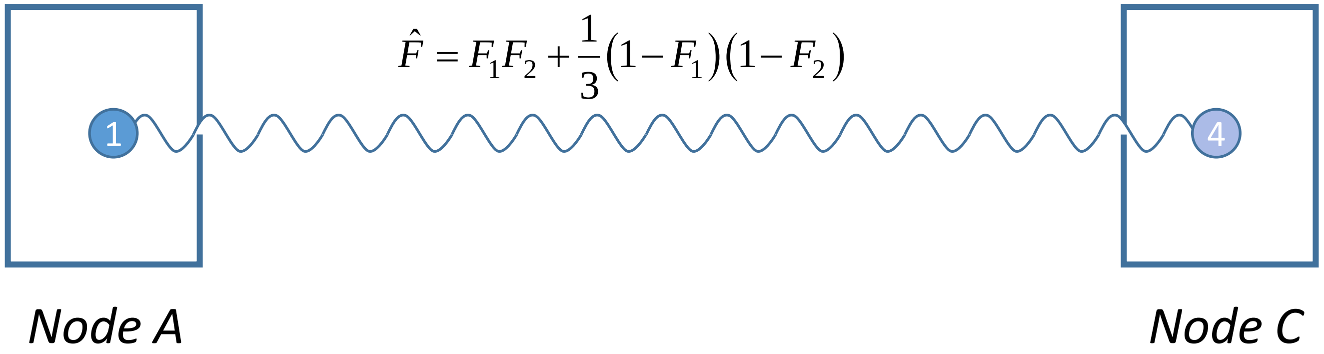
$$\rho_{14} = \hat{F} |\Phi^+\rangle\langle\Phi^+| + \frac{1-\hat{F}}{3}\left(|\Psi^-\rangle\langle\Psi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Phi^-\rangle\langle\Phi^-|\right)$$

Entanglement Swapping of two Werner States

- Let's comment on the fidelity

$$\hat{F} = F_1F_2 + \frac{1}{3}(1-F_1)(1-F_2) \Leftrightarrow \left(\frac{4\hat{F}-1}{3}\right) = \left(\frac{4F_1-1}{3}\right)\left(\frac{4F_2-1}{3}\right)$$

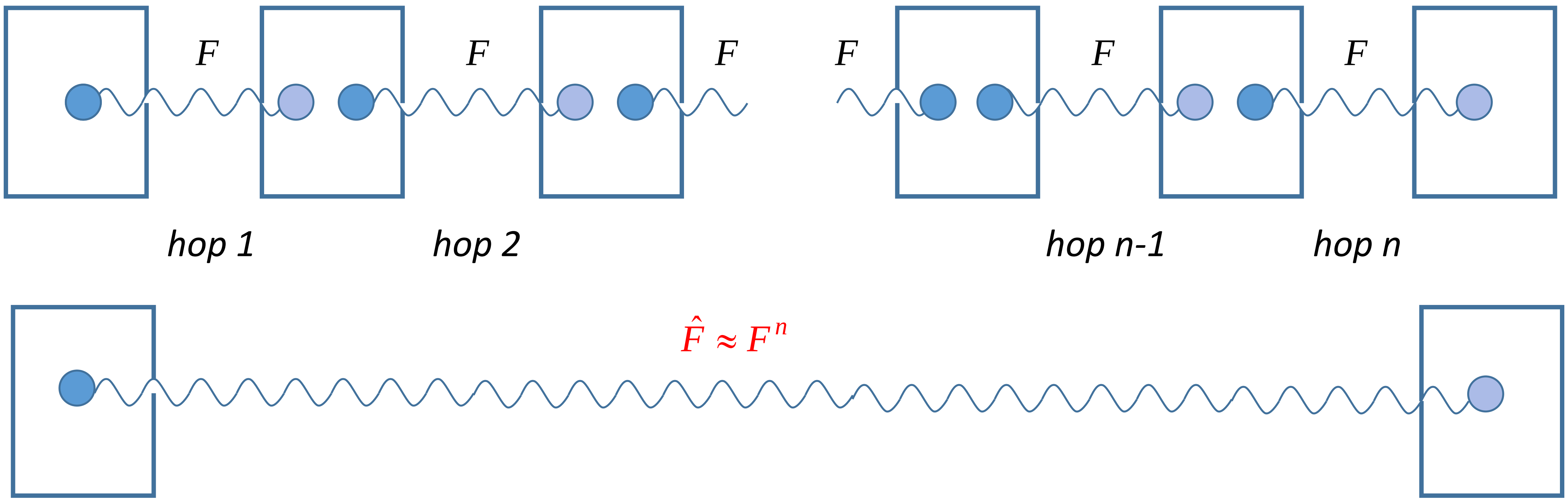
of the state ρ_{14}



- If $F_1 \approx 1$ and $F_2 \approx 1$ then $\hat{F} \approx F_1F_2$
- If $F_1 = F_2 = F \rightarrow \hat{F} = F^2$

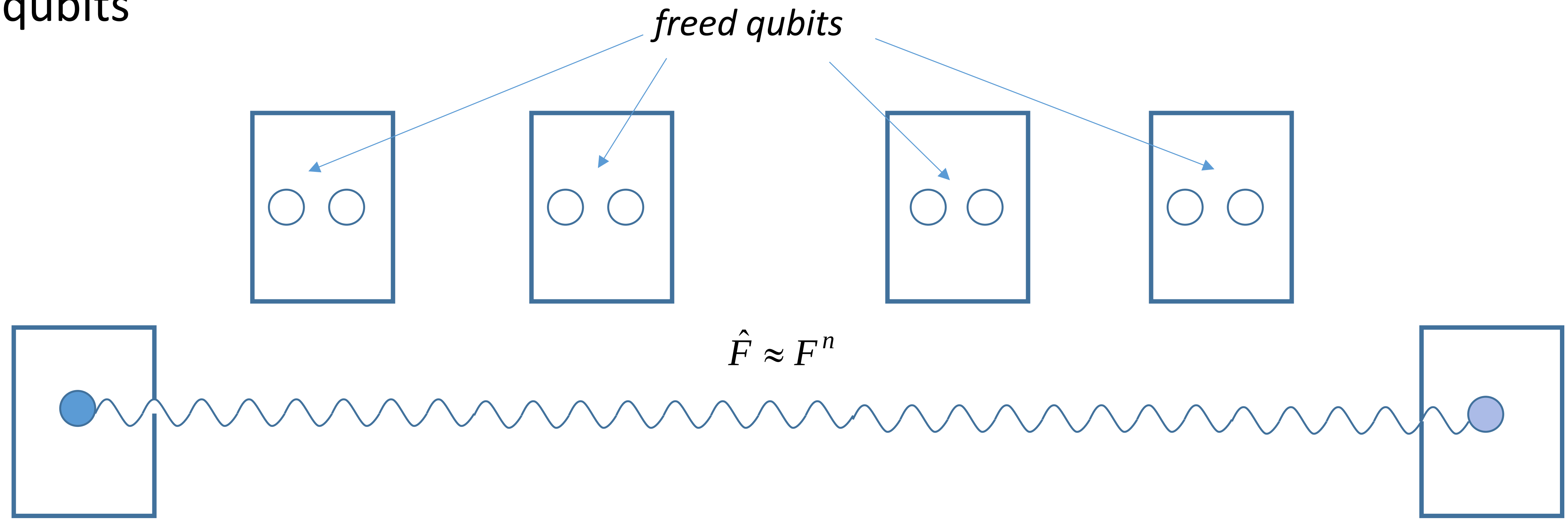
Entanglement Swapping of two Werner States

- Over n hops each with fidelity F, the resulting fidelity is $\hat{F} \approx F^n$
- Since $F < 1$, we are unable to sustain a high fidelity over more than a few hops when using entanglement swapping



Entanglement Swapping of two Werner States

- Note that this is independent of the order in which we do entanglement swapping
- After entanglement swapping, each intermediate repeater releases its qubits



Performance Evaluation Metrics

- So far, the focus has mainly been on the *Fidelity* of the teleported qubit along the end-to-end entangled connection
- However, other performance metrics are very relevant for assessing the performance of a quantum Internet, such as:

  a) *the end-to-end delay*, i.e., the time it takes to set up an end-to-end entangled connection between Alice and Bob, and

  b) *the maximum number of entangled connections that can be set up in a time unit (rate)* between Alice and Bob

Purification

Purification Protocol (BBPSSW)

- In this part, we will address what happens when we also include errors in our considerations
- We will learn how to handle these errors and create a state between Repeater *A* and Repeater *B* of acceptable fidelity
- Our desired state that we want to share between Repeater *A* and *B* is given by the **maximally entangled state** $|\Phi^+\rangle$
- In the density matrix form, we write it as the outer product,

$$\rho_{AB} = |\Phi^+\rangle\langle\Phi^+|$$

Purification Protocol (BBPSSW)

- In reality, there will always be some noise affecting the system
- The state ρ_{AB} will be a mixture of the desired pure state $|\Phi^+\rangle$, and some other unwanted noisy term ρ_{noise}
- With probability given by the fidelity *F*, we will have the desired state $|\Phi^+\rangle$, and with probability 1 − *F*, we will have some noisy state ρ_{noise}

$$\rho_{AB} = F\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left(1 - F\right)\rho_{noise}$$

Purification Protocol (BBPSSW)

- Rather than considering the general case of how noise affects our **maximally entangled state**, we will consider the specific example of a **bit-flip channel**, which we saw earlier
- This channel leaves the state unaffected with prob ability *F*, otherwise it applies the Pauli *X* operator to one of the qubits

$$\begin{aligned}\rho_{AB} &= F\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left(1-F\right)X_A\left|\Phi^+\right\rangle\left\langle\Phi^+\right|X_A \\ &= F\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left(1-F\right)\left|\Psi^+\right\rangle\left\langle\Psi^+\right|\end{aligned}$$

- We have applied the bit-flip channel to qubit *A*, but it does not matter whether we apply it to qubit *A* or *B*

Purification Protocol (BBPSSW)

- Keep in mind that this is just **one possible source of error** out of many
- One way of dealing with errors is to use *Quantum Error Correction* (*QEC*)
- QEC can detect and correct errors, but usually comes with a large overhead
- Here, we will look at a **less ambitious procedure** of simply **detecting errors**, known as **purification**

Purification Protocol (BBPSSW)

- The concept of *purification* was introduced in 1996 by Bennett, Brassard, Popescu, Schumacher, Smolin and Wootters [1,2]
- For simplicity, the scheme proposed by them will be called *BBPSSW protocol*
- The concept of purification involves extracting from a pool of imperfect EPR pairs, each with a low fidelity, at least one pair possessing higher fidelity, or ideally, one that is perfect ($F = 1$)
- To be precise, we need to distinguish between *purification protocol* and *distillation process*

[1] C. H. Bennett et al., Phys. Rev. Lett. 76, 722 (1996)

[2] C. H. Bennett et al., Phys. Rev. A 54, 3824 (1996)

Purification Protocol (BBPSSW)

- *Purification* is a test for the state ρ_{AB} that checks whether the state is affected by an error
- The test is not perfect and sometimes succeeds even when the state has undergone an error
- If the probability of this **“false positive”** is low enough, then the overall fidelity of the state increases
- It is this sense that we say that the state has been purified

Purification Protocol (BBPSSW)

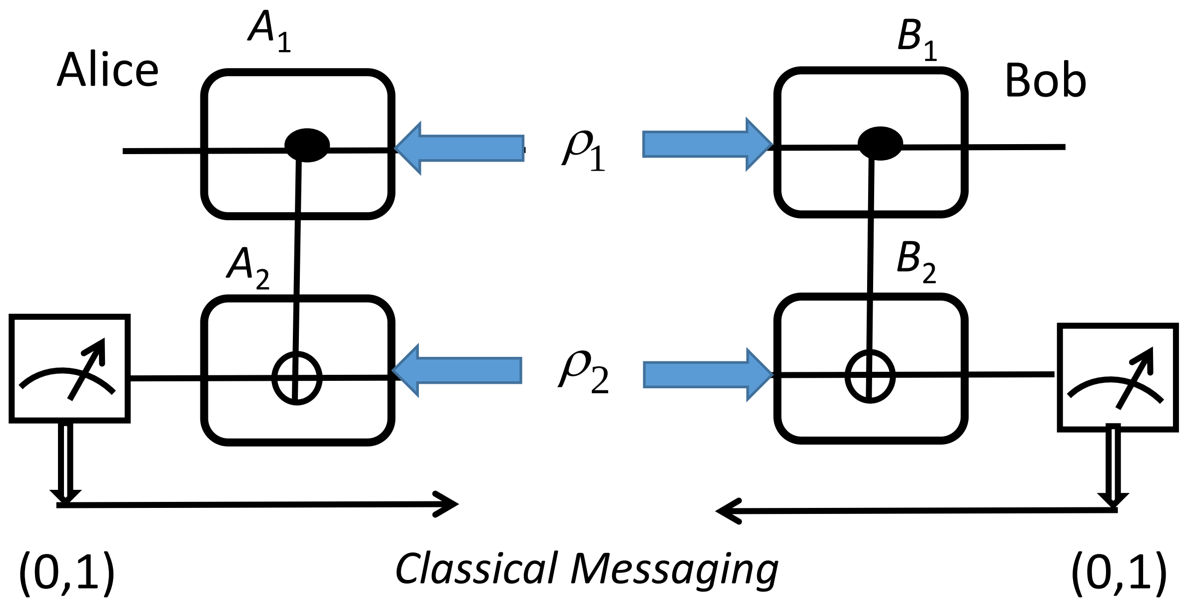
- There are two important things that we need to keep in mind when designing the purification procedure
- **First**, measurements can be used to reveal information about the state, but they are also very intrusive and destroy the entanglement that we are trying to preserve
- **Second**, the two qubits of the entangled state are spatially separated and held in separated repeaters
- This distance can be of the order of tens of kilometers for a link, or much longer over a network

Purification Protocol (BBPSSW)

- We can get around the first issue of destructive measurement by using another Bell pair to test whether the original pair has undergone the unwanted Pauli X flip
- This is done by entangling the second pair with the original one, and then measuring the second pair in order to extract useful information about the first pair without destroying it
- The second issue of the qubits being at distant locations can be overcome by simple **classical communication**

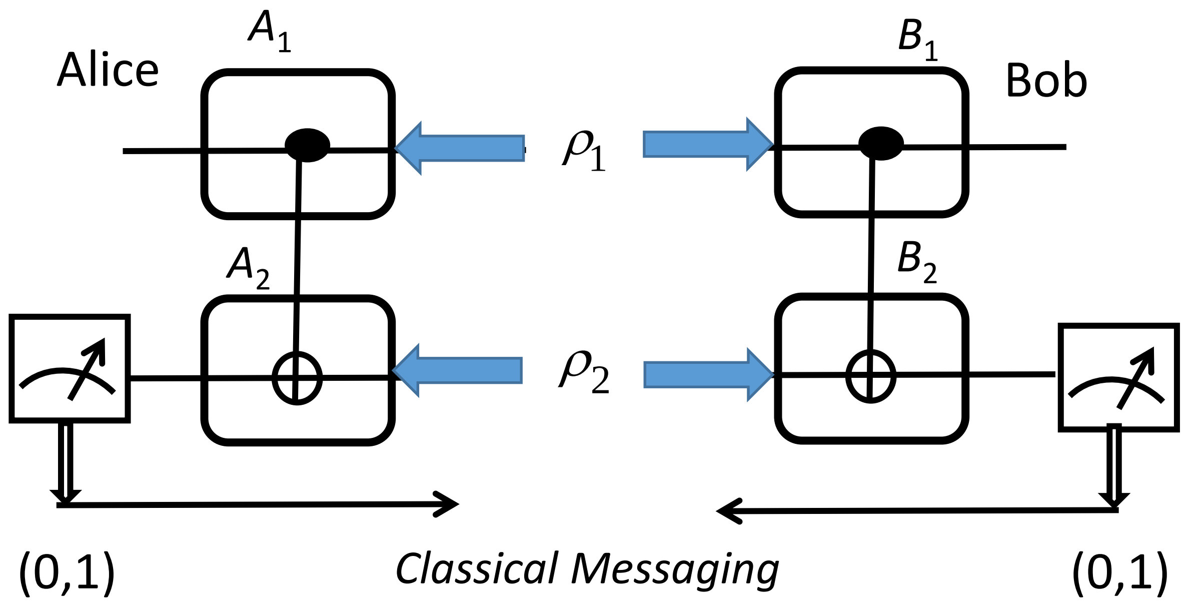
Purification Protocol (BBPSSW)

- Let's introduce the detailed protocol for entanglement purification for the Pauli *X* error
- The horizontal wires represent Bell pairs shared between Alice and Bob



- Ideally, these states are $|\Phi^+\rangle_1$ and $|\Phi^+\rangle_2$, but due to noise they will be mixed states ρ_1 and ρ_2
- Alice applies a CNOT gate on the qubits in her possession. Her qubit from the first pair acts as the **control** and her qubit from the second pair is the **target**

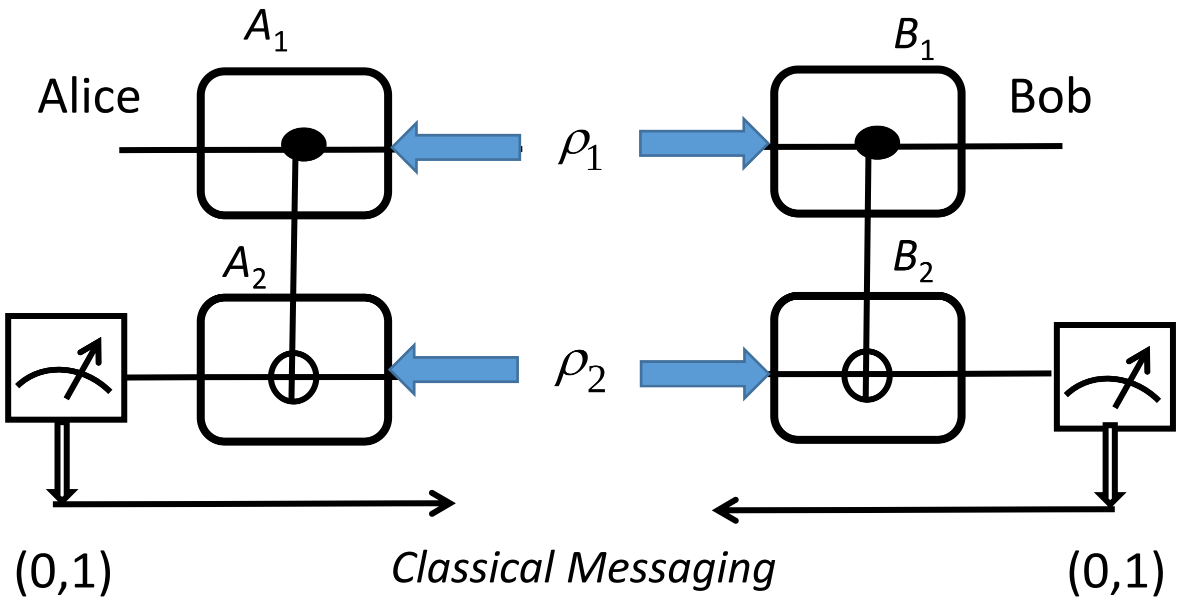
Purification Protocol (BBPSSW)



- Bob also performs a CNOT gate on his two qubits with the same control/target choice
- Alice and Bob then **measure the qubits of the second pair in the Pauli Z basis** and send the measurement outcomes to each other using classical messages
- They keep the first pair if the measurement outcomes are the same, meaning they both measured the state $|0\rangle$ or they both measured the state $|1\rangle$. We say that the **measurement outcomes are correlated**

Purification Protocol (BBPSSW)

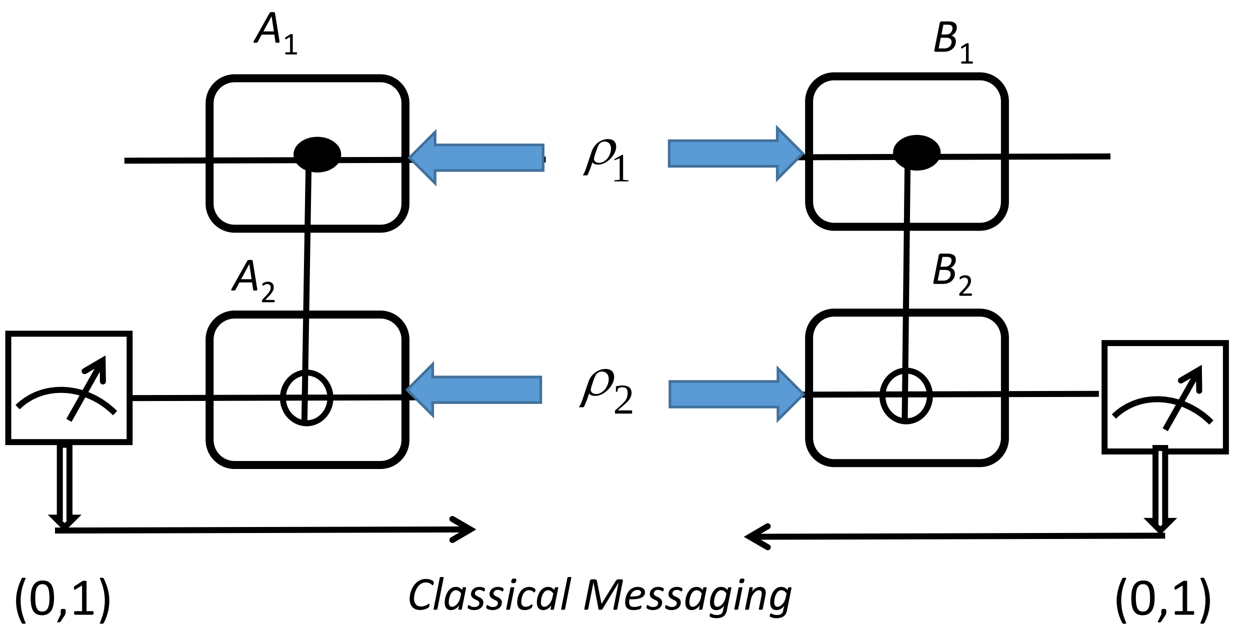
- Otherwise, they discard the first pair, as different measurement outcomes signal that an error has been detected
- *Pair 2*, having been measured and therefore no longer entangled, *is always discarded*
- We call pair 2 the *sacrificial pair*

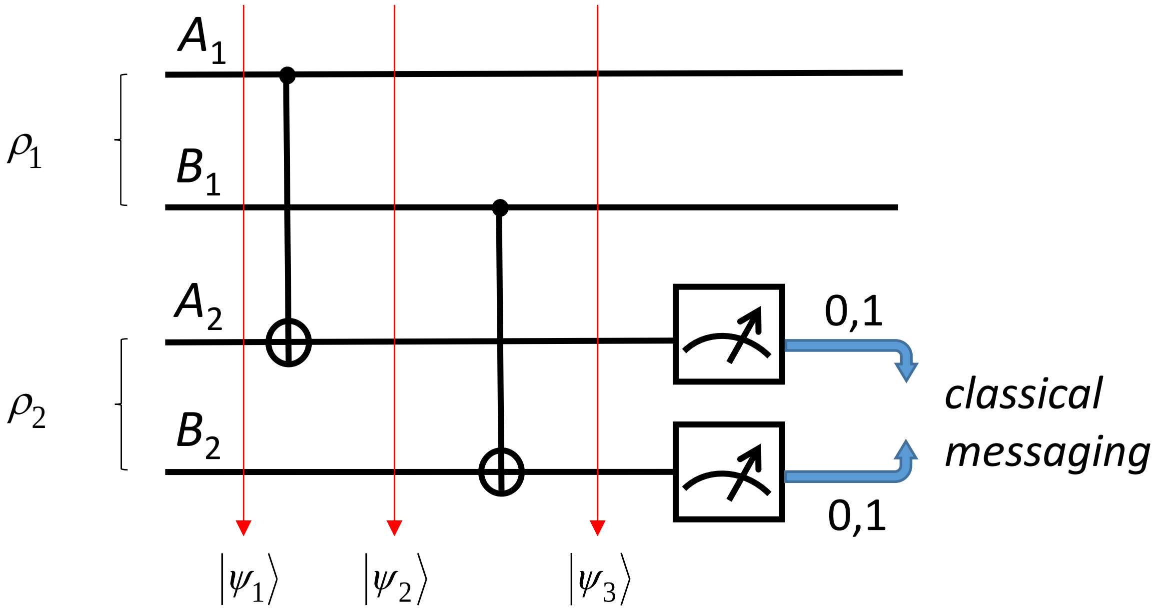


- Depending on the outcomes, one obtains *eventually a pair with higher fidelity*

BBPSSW

- The reason why this particular sequence of steps works will become clearer as we write it out step-by-step
- To do this we make reference to the quantum circuit reported on the right side





Purification Protocol With Imperfect Bell Pair

– As previously stated, we assume that the Bell pairs **are not perfect**

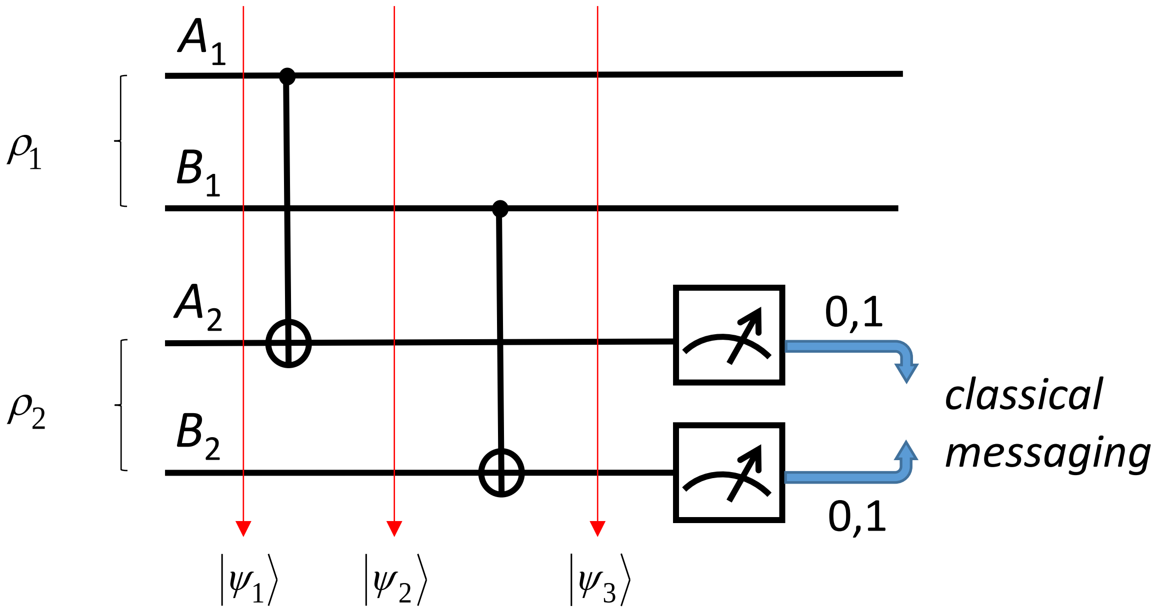
– More specifically, we consider the case where both Bell pairs may have suffered a *bit flip* error,

$$\rho_1 = F\left|\Phi^+\right\rangle_1\left\langle\Phi^+\right| + (1-F)\left|\Psi^+\right\rangle_1\left\langle\Psi^+\right|$$

$$\rho_2 = F\left|\Phi^+\right\rangle_2\left\langle\Phi^+\right| + (1-F)\left|\Psi^+\right\rangle_2\left\langle\Psi^+\right|$$

where

$$\left|\Phi^+\right\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad \left|\Psi^+\right\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$



Purification Protocol With Imperfect Bell Pair

– Since, $\rho_1 = F\left|\Phi^+\right\rangle_1\left\langle\Phi^+\right| + (1-F)\left|\Psi^+\right\rangle_1\left\langle\Psi^+\right|$ and $\rho_2 = F\left|\Phi^+\right\rangle_2\left\langle\Phi^+\right| + (1-F)\left|\Psi^+\right\rangle_2\left\langle\Psi^+\right|$

$$\rightarrow \quad \rho = \rho_1 \otimes \rho_2 = \left(F\left|\Phi^+\right\rangle_1\left\langle\Phi^+\right| + (1-F)\left|\Psi^+\right\rangle_1\left\langle\Psi^+\right|\right) \otimes \left(F\left|\Phi^+\right\rangle_2\left\langle\Phi^+\right| + (1-F)\left|\Psi^+\right\rangle_2\left\langle\Psi^+\right|\right)$$

$$= F^2\left(\left|\Phi^+\right\rangle_1\left\langle\Phi^+\right|\right)\otimes\left(\left|\Phi^+\right\rangle_2\left\langle\Phi^+\right|\right) + F(1-F)\left(\left|\Phi^+\right\rangle_1\left\langle\Phi^+\right|\right)\otimes\left(\left|\Psi^+\right\rangle_2\left\langle\Psi^+\right|\right)$$

$$+F(1-F)\left(\left|\Psi^+\right\rangle_1\left\langle\Psi^+\right|\right)\otimes\left(\left|\Phi^+\right\rangle_2\left\langle\Phi^+\right|\right) + (1-F)^2\left(\left|\Psi^+\right\rangle_1\left\langle\Psi^+\right|\right)\otimes\left(\left|\Psi^+\right\rangle_2\left\langle\Psi^+\right|\right)$$

$$= F^2\left(\left|\Phi^+\right\rangle_1\left|\Phi^+\right\rangle_{2\,1}\left\langle\Phi^+\right|_2\left\langle\Phi^+\right|\right) + F(1-F)\left|\Phi^+\right\rangle_1\left|\Psi^+\right\rangle_{2\,1}\left\langle\Phi^+\right|_2\left\langle\Psi^+\right|$$

$$+F(1-F)\left(\left|\Psi^+\right\rangle_1\left|\Phi^+\right\rangle_{2\,1}\left\langle\Psi^+\right|_2\left\langle\Phi^+\right|\right) + (1-F)^2\left|\Psi^+\right\rangle_1\left|\Psi^+\right\rangle_{2\,1}\left\langle\Psi^+\right|_2\left\langle\Psi^+\right|$$

Purification Protocol With Imperfect Bell Pair

– The **input** density matrix is then

$$\rho = \rho_1 \otimes \rho_2 = F^2 \left|\Phi^+\right\rangle_1 \left|\Phi^+\right\rangle_2 {}_1\left\langle\Phi^+\right|_2\left\langle\Phi^+\right|$$

$$+F\left(1-F\right)\left|\Phi^+\right\rangle_1 \left|\Psi^+\right\rangle_2 {}_1\left\langle\Phi^+\right|_2\left\langle\Psi^+\right|$$

$$+F\left(1-F\right)\left|\Psi^+\right\rangle_1 \left|\Phi^+\right\rangle_2 {}_1\left\langle\Psi^+\right|_2\left\langle\Phi^+\right|$$

$$+\left(1-F\right)^2\left|\Psi^+\right\rangle_1 \left|\Psi^+\right\rangle_2 {}_1\left\langle\Psi^+\right|_2\left\langle\Psi^+\right|$$

Purification Protocol With Imperfect Bell Pair

– To determine the evolution of the input density matrix, we need to look at the evolution of the following *bipartite pure states* when applied as an input to the purification circuit

$$|\Phi^+\rangle_1 |\Phi^+\rangle_2$$

$$|\Phi^+\rangle_1 |\Psi^+\rangle_2$$

$$|\Psi^+\rangle_1 |\Phi^+\rangle_2$$

$$|\Psi^+\rangle_1 |\Psi^+\rangle_2$$

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j| \xrightarrow{U} \rho' = \sum_j p_j U |\psi_j\rangle\langle\psi_j| U^\dagger$$

Result from the previous lecture

Purification Protocol $\left(\left|\Phi^+\right\rangle_1\left|\Phi^+\right\rangle_2\right)$

To start, we analyze the $\left|\Phi^+\right\rangle_1\left|\Phi^+\right\rangle_2$'s evolution when applied as an input to the purification circuit, where

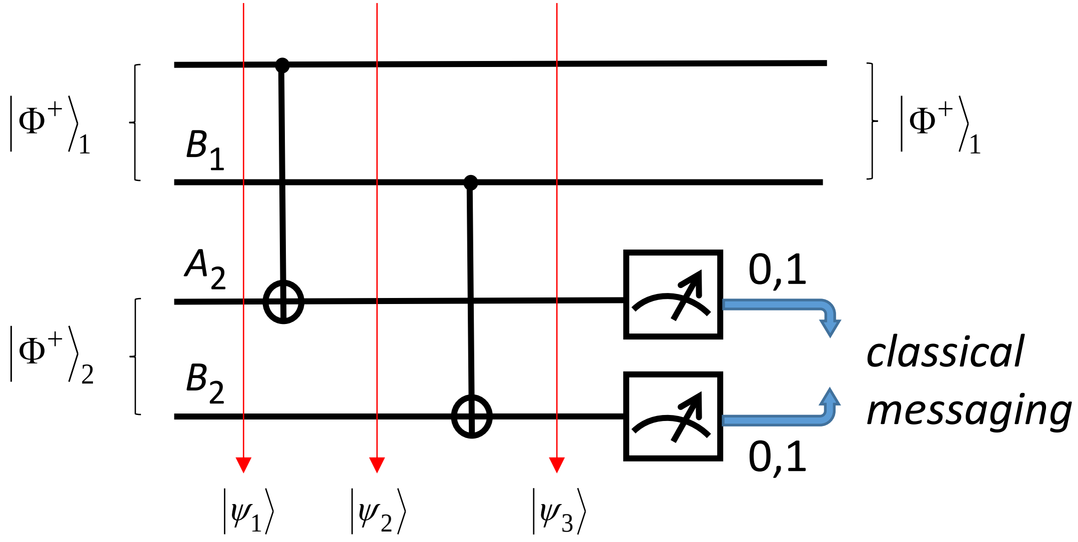
$$\left|\Phi^+\right\rangle = \frac{\left|00\right\rangle + \left|11\right\rangle}{\sqrt{2}}$$

Purification Protocol $\left(|\Phi^+\rangle_1|\Phi^+\rangle_2\right)$

The input state $|\psi_1\rangle$ to the circuit is

$$|\psi_1\rangle = |\Phi^+\rangle_1|\Phi^+\rangle_2 = \left(\frac{|00\rangle_1 + |11\rangle_1}{\sqrt{2}}\right) \otimes \left(\frac{|00\rangle_2 + |11\rangle_2}{\sqrt{2}}\right)$$

$$= \frac{1}{2}\left(|00\rangle_1|00\rangle_2 + |00\rangle_1|11\rangle_2 + |11\rangle_1|00\rangle_2 + |11\rangle_1|11\rangle_2\right)$$



Purification Protocol $\left(|\Phi^+\rangle_1 |\Phi^+\rangle_2\right)$

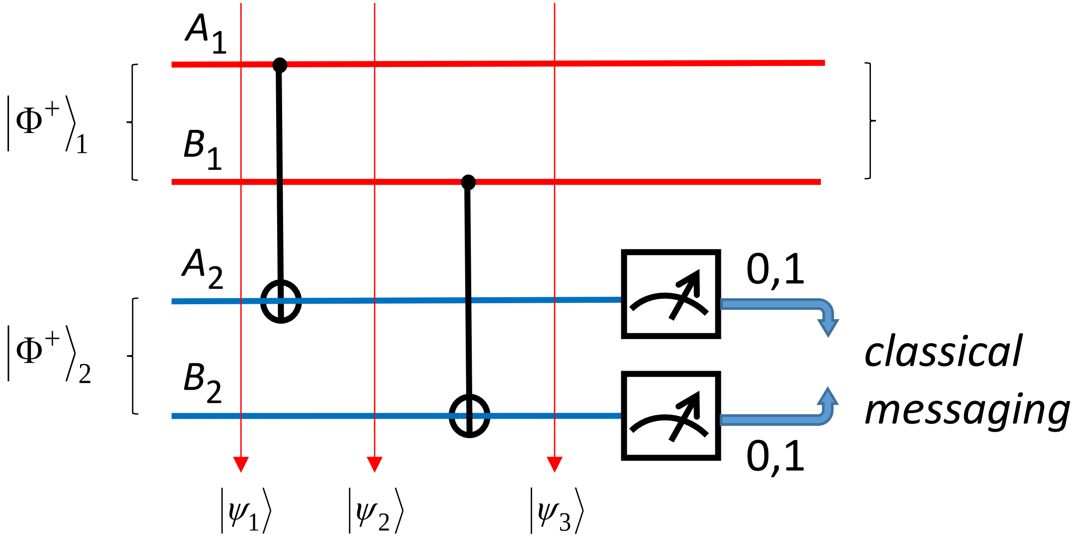
– Now, Alice and Bob each perform a CNOT gate using their half of pair 1 (A_1, B_1) as the control and their half of pair 2 (A_2, B_2) as the target

$$|\psi_1\rangle = 1/2\left(|00\rangle_1|00\rangle_2 + |00\rangle_1|11\rangle_2 + |11\rangle_1|00\rangle_2 + |11\rangle_1|11\rangle_2\right)$$

$$\xrightarrow{CNOT_1} |\psi_2\rangle = 1/2\left(|00\rangle_1|00\rangle_2 + |00\rangle_1|11\rangle_2 + |11\rangle_1|10\rangle_2 + |11\rangle_1|01\rangle_2\right)$$

control qubit

target qubit



Purification Protocol $\left(|\Phi^+\rangle_1|\Phi^+\rangle_2\right)$

– Now, Alice and Bob each perform a CNOT gate using their half of pair 1 (A_1, B_1) as the control and their half of pair 2 (A_2, B_2) as the target

$$|\psi_2\rangle = 1/2\left(|00\rangle_1|00\rangle_2 + |00\rangle_1|11\rangle_2 + |11\rangle_1|10\rangle_2 + |11\rangle_1|01\rangle_2\right)$$

control qubit

target qubit

$$\xrightarrow{CNOT_2} |\psi_3\rangle = 1/2\left(|00\rangle_1|00\rangle_2 + |00\rangle_1|11\rangle_2 + |11\rangle_1|11\rangle_2 + |11\rangle_1|00\rangle_2\right)$$

$$= 1/2\left[|00\rangle_1\left(|00\rangle_2 + |11\rangle_2\right) + |11\rangle_1\left(|11\rangle_2 + |00\rangle_2\right)\right]$$

$$= 1/2\left(|00\rangle_1 + |11\rangle_1\right)\left(|00\rangle_2 + |11\rangle_2\right) = |\Phi^+\rangle_1|\Phi^+\rangle_2$$

– Under our assumptions that everything is perfect, the two CNOT gates cancel

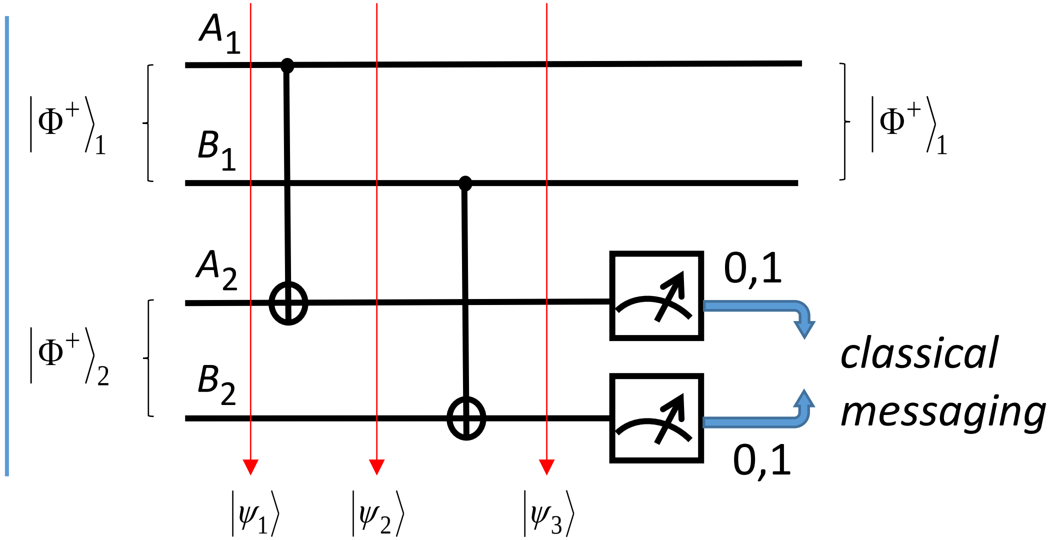
$$|\Phi^+\rangle_1|\Phi^+\rangle_2 \quad \rightarrow \quad |\Phi^+\rangle_1|\Phi^+\rangle_2$$

Purification Protocol $\left(|\Phi^+\rangle_1 |\Phi^+\rangle_2\right)$

- Next, Alice and Bob each measure their member of Bell pair 2 (A_2, B_2) in the computational basis $\{|0\rangle, |1\rangle\}$ and exchange the measurement results

$$|\psi_3\rangle = 1/2\left(|00\rangle_1 + |11\rangle_1\right) \otimes \left(|00\rangle_2 + |11\rangle_2\right)$$

$$= 1/2\left(|00\rangle_1 + |11\rangle_1\right)|00\rangle_2 + 1/2\left(|00\rangle_1 + |11\rangle_1\right)|11\rangle_2$$



- Dispensing with normalization, $|\psi_3\rangle$ collapses to

$$\left(|00\rangle_1 + |11\rangle_1\right)|00\rangle_2 = |\Phi^+\rangle_1 |00\rangle_2 \quad \text{or} \quad \left(|00\rangle_1 + |11\rangle_1\right)|11\rangle_2 = |\Phi^+\rangle_1 |11\rangle_2$$

Purification Protocol $\left(\left|\Phi^{+}\right\rangle_{1}\left|\Phi^{+}\right\rangle_{2}\right)$

- Since the measuring results *match* (i.e., (0.0) or (1.1)), the Bell pair 1 is *kept*
- Pair 2, having been measured and therefore no longer entangled, *is discarded*
- That's why we refer to pair 2 as the *sacrificial pair*

Purification Protocol $\left(\left|\Phi^+\right\rangle_1\left|\Psi^+\right\rangle_2\right)$

- Examining the circuit again, it is easy to see that if either of the Bell pairs has a bit flip error, Alice and Bob will find **different** values when they measure their qubits
- We prove this when $\left|\psi_1\right\rangle = \left|\Phi^+\right\rangle_1\left|\Psi^+\right\rangle_2$

$$\left|\psi_1\right\rangle = \left|\Phi^+\right\rangle_1\left|\Psi^+\right\rangle_2 = \left(\frac{\left|00\right\rangle_1 + \left|11\right\rangle_1}{\sqrt{2}}\right)\otimes\left(\frac{\left|01\right\rangle_2 + \left|10\right\rangle_2}{\sqrt{2}}\right)$$

$$= \frac{1}{2}\left(\left|00\right\rangle_1\left|01\right\rangle_2 + \left|00\right\rangle_1\left|10\right\rangle_2 + \left|11\right\rangle_1\left|01\right\rangle_2 + \left|11\right\rangle_1\left|10\right\rangle_2\right)$$

Purification Protocol $\left(|\Phi^+\rangle_1|\Psi^+\rangle_2\right)$

$$|\psi_1\rangle=\frac{1}{2}\left(|00\rangle_1|01\rangle_2+|00\rangle_1|10\rangle_2+|11\rangle_1|01\rangle_2+|11\rangle_1|10\rangle_2\right)$$

$$\xrightarrow{CNOT_1}\quad|\psi_2\rangle=\frac{1}{2}\left(|00\rangle_1|01\rangle_2+|00\rangle_1|10\rangle_2+|11\rangle_1|11\rangle_2+|11\rangle_1|00\rangle_2\right)$$

$$\xrightarrow{CNOT_3}\quad|\psi_3\rangle=\frac{1}{2}\left(|00\rangle_1|01\rangle_2+|00\rangle_1|10\rangle_2+|11\rangle_1|10\rangle_2+|11\rangle_1|01\rangle_2\right)$$

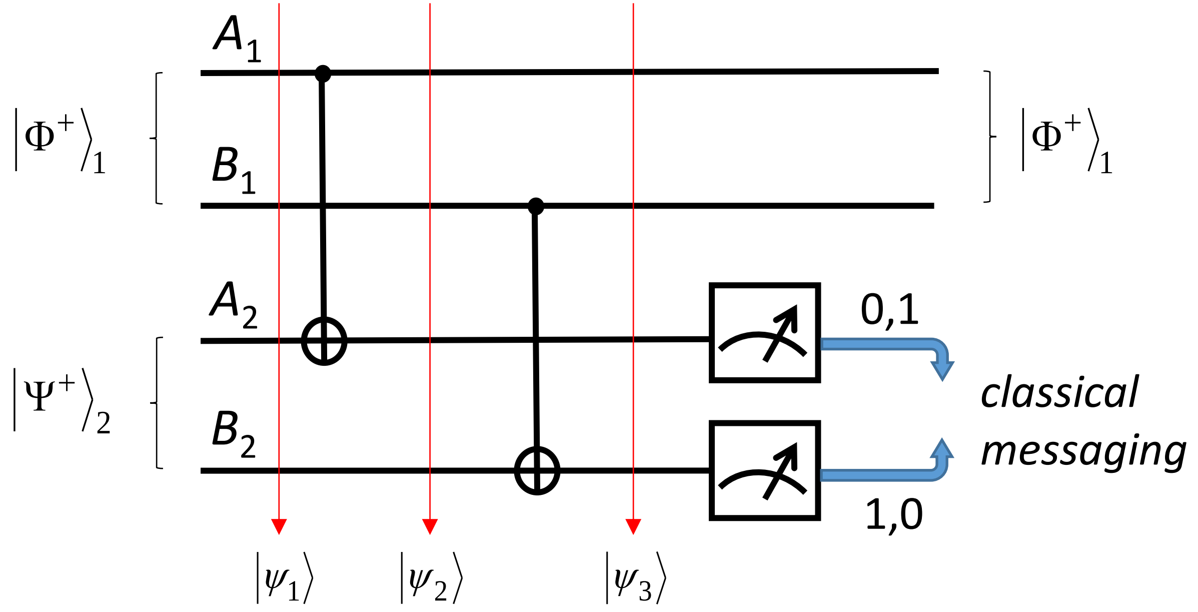
$$=\frac{1}{2}\left[\left(|00\rangle_1+|11\rangle_1\right)|01\rangle_2+\left(|00\rangle_1+|11\rangle_1\right)|10\rangle_2\right]$$

$$=\frac{1}{\sqrt{2}}\left[|\Phi^+\rangle_1|01\rangle_2+|\Phi^+\rangle_1|10\rangle_2\right]$$

control qubit

target qubit

Purification Protocol $\left(\left|\Phi^+\right\rangle_1\left|\Psi^+\right\rangle_2\right)$

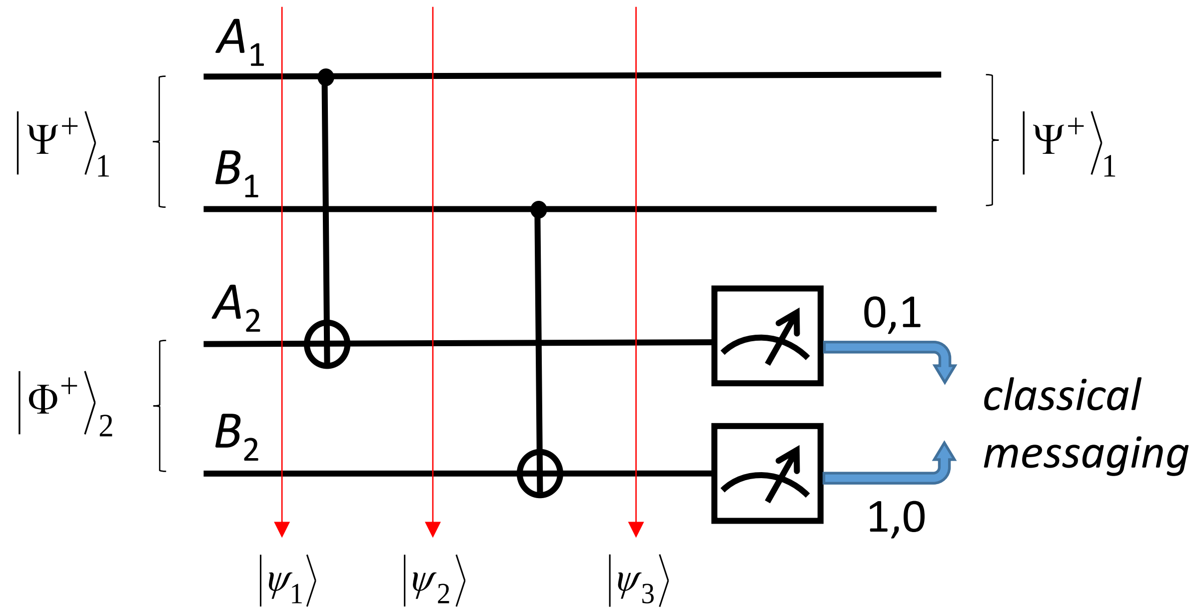


$$\left|\psi_3\right\rangle = \frac{1}{\sqrt{2}}\left[\left|\Phi^+\right\rangle_1 \left|01\right\rangle_2 + \left|\Phi^+\right\rangle_1 \left|10\right\rangle_2\right]$$

Purification Protocol $\left(|\Psi^+\rangle_1 |\Phi^+\rangle_2\right)$

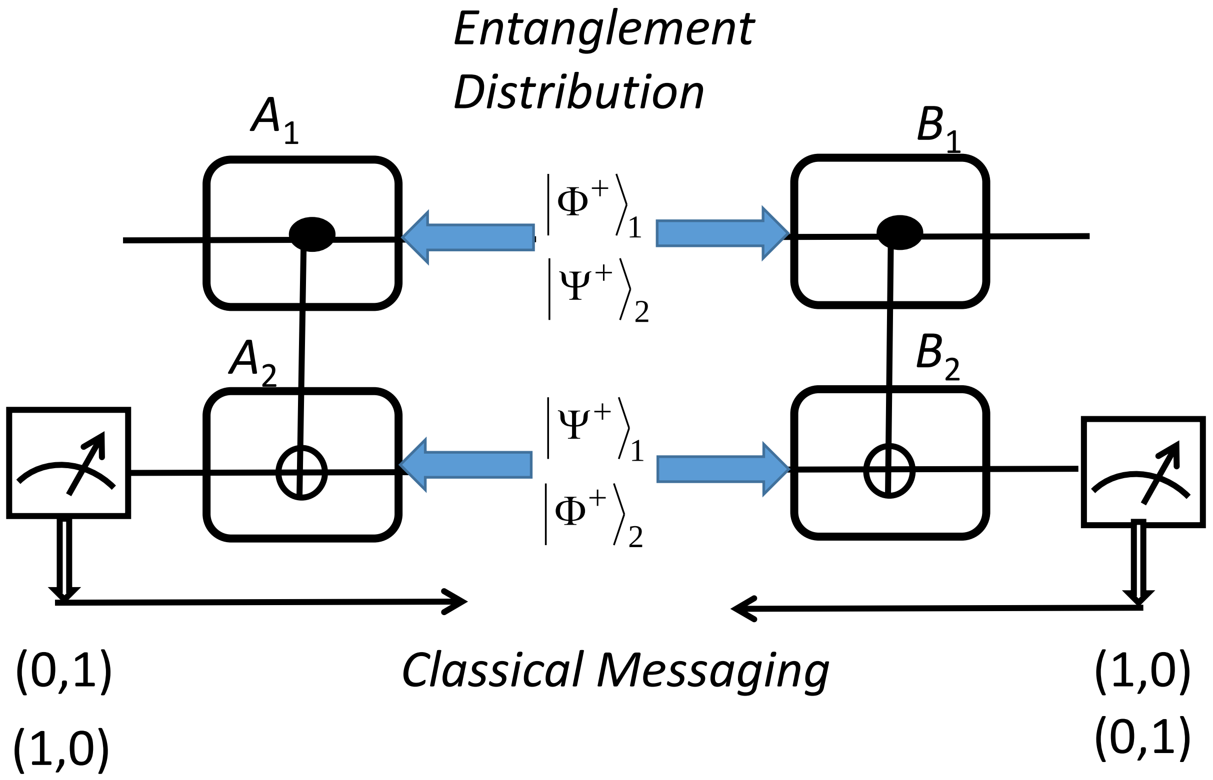
By following the same approach, it can be easily proved that for $|\Psi^+\rangle_1 |\Phi^+\rangle_2$ the following relation holds for $|\psi_3\rangle$

$$|\psi_3\rangle = \frac{1}{\sqrt{2}}\left[|\Psi^+\rangle_1 |01\rangle_2 + |\Psi^+\rangle_1 |10\rangle_2\right]$$



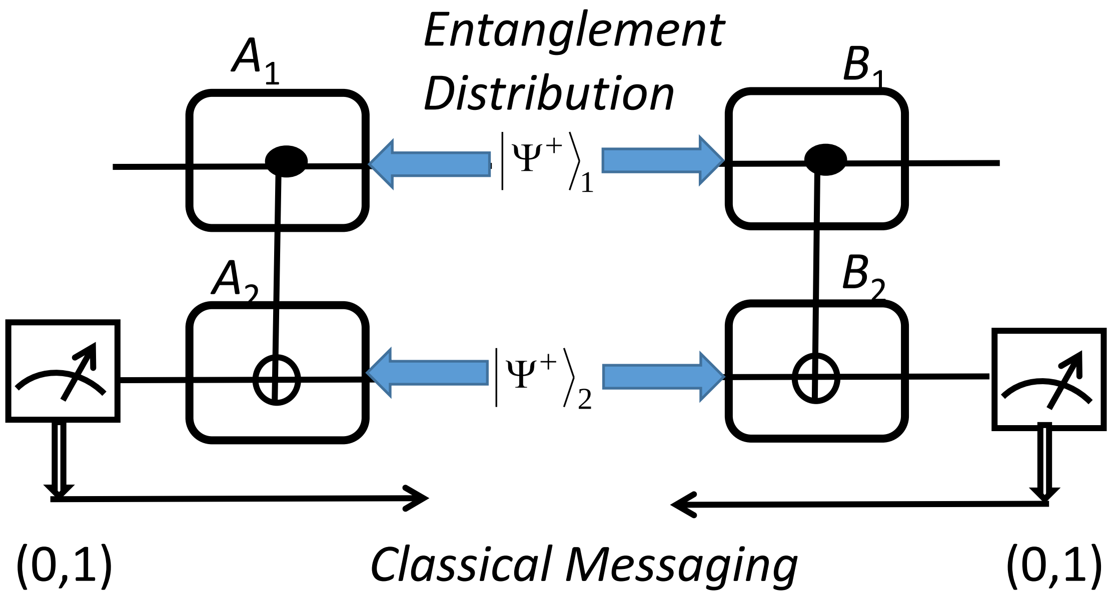
Purification Protocol $\left(|\Psi^+\rangle_1|\Phi^+\rangle_2\right)$

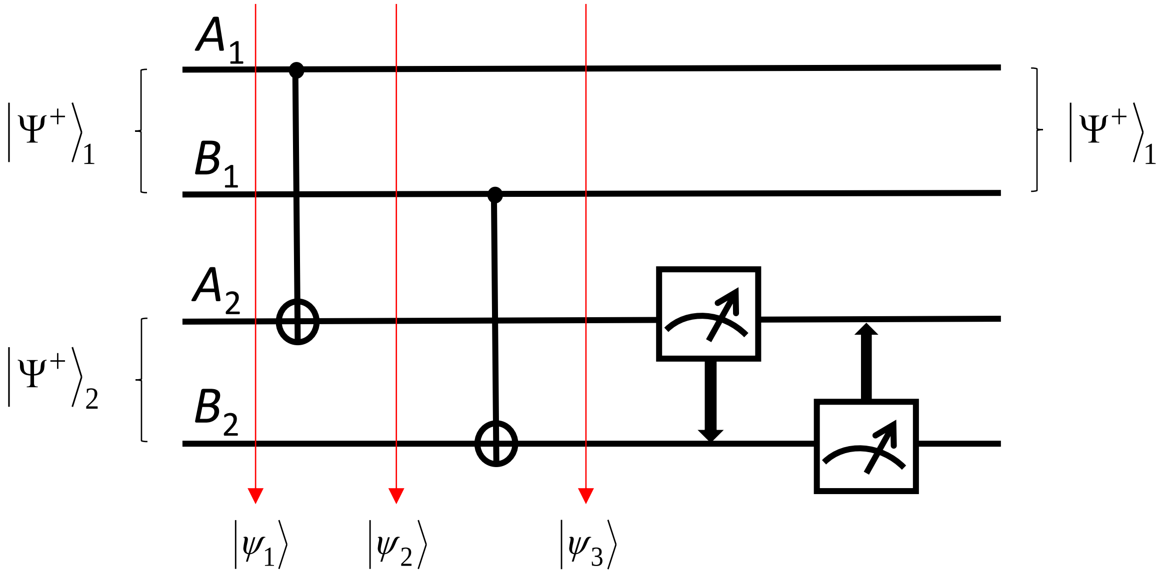
Thus, we have proved that if either of the Bell pairs has a bit flip error, Alice and Bob will find different values when they measure their qubits



Because we cannot tell if the error was in pair 1 or pair 2, we have no choice but to discard pair 1, even though it might be good

Purification Protocol $\left(|\Psi^+\rangle_1 |\Psi^+\rangle_2\right)$





Purification Protocol $\left(|\Psi^+\rangle_1|\Psi^+\rangle_2\right)$

- If both Bell pairs have an error, Alice and Bob will find the same value
- With probability $(1-F)^2$, the error in pair 1 goes undetected due to the error in pair 2
- Let’s prove it

$$|\psi_1\rangle = |\Psi^+\rangle_1|\Psi^+\rangle_2 = \left(\frac{|01\rangle_1 + |10\rangle_1}{\sqrt{2}}\right) \otimes \left(\frac{|01\rangle_2 + |10\rangle_2}{\sqrt{2}}\right)$$

$$= \frac{1}{2}\left(|01\rangle_1|01\rangle_2 + |01\rangle_1|10\rangle_2 + |10\rangle_1|01\rangle_2 + |10\rangle_1|10\rangle_2\right)$$

Purification Protocol $\left(|\Psi^+\rangle_1|\Psi^+\rangle_2\right)$

$$|\psi_1\rangle = \frac{1}{2}\left(|01\rangle_1|01\rangle_2 + |01\rangle_1|10\rangle_2 + |10\rangle_1|01\rangle_2 + |10\rangle_1|10\rangle_2\right)$$

$$\xrightarrow{CNOT_1} |\psi_2\rangle = \frac{1}{2}\left(|01\rangle_1|01\rangle_2 + |01\rangle_1|10\rangle_2 + |10\rangle_1|11\rangle_2 + |10\rangle_1|00\rangle_2\right)$$

$$\xrightarrow{CNOT_3} |\psi_3\rangle = \frac{1}{2}\left(|01\rangle_1|00\rangle_2 + |01\rangle_1|11\rangle_2 + |10\rangle_1|11\rangle_2 + |10\rangle_1|00\rangle_2\right)$$

$$= \frac{1}{2}\left[\left(|01\rangle_1 + |10\rangle_1\right)|00\rangle_2 + \left(|01\rangle_1 + |10\rangle_1\right)|11\rangle_2\right]$$

$$= \frac{1}{\sqrt{2}}\left[|\Psi^+\rangle_1|00\rangle_2 + |\Psi^+\rangle_1|11\rangle_2\right]$$

control qubit

target qubit

Purification Protocol With Imperfect Bell Pair

- As a conclusion, Alice and Bob each hold one half of each Bell pair

$$
\begin{aligned}
\rho = \rho_1 \otimes \rho_1 = F^2 & \left|\Phi^+\right\rangle_1 \left|\Phi^+\right\rangle_{2\,1}\left\langle\Phi^+\right|_2\left\langle\Phi^+\right| \\
& +F(1-F)\left|\Phi^+\right\rangle_1 \left|\Psi^+\right\rangle_{2\,1}\left\langle\Phi^+\right|_2\left\langle\Psi^+\right| \\
& +F(1-F)\left|\Psi^+\right\rangle_1 \left|\Phi^+\right\rangle_{2\,1}\left\langle\Psi^+\right|_2\left\langle\Phi^+\right| \\
& +(1-F)^2\left|\Psi^+\right\rangle_1 \left|\Psi^+\right\rangle_{2\,1}\left\langle\Psi^+\right|_2\left\langle\Psi^+\right|
\end{aligned}
$$

- Next, Alice and Bob each perform a CNOT gate using their half of pair 1 (A_1, B_1) as the control and their half of pair 2 (A_2, B_2) as the target
- Then, Alice and Bob each measure their member of Bell pair 2 (A_2, B_2) in the computational basis and exchange the measurement results

Purification Protocol With Imperfect Bell Pair

- If both pairs are in $|\Phi^+\rangle$, both pairs are perfect and, at the output of the circuit we still have two $|\Phi^+\rangle$ pairs

- This happens with probability F^2

- When the second pair is measured, Alice and Bob each have a 50% chance of finding 0 and 50% chance of finding 1, but when they exchange their measurement results, they will always find the same value (i.e., (0,0) or (1,1)) and *pair 1 is kept*

Purification Protocol With Imperfect Bell Pair

– If either of the Bell pairs has a bit flip error (i.e. $\left|\Phi^+\right\rangle_1 \left|\Psi^+\right\rangle_2$ or $\left|\Psi^+\right\rangle_1 \left|\Phi^+\right\rangle_2$), Alice and Bob will find different values when they measure their qubits

– For each case (i.e. $\left|\Phi^+\right\rangle_1 \left|\Psi^+\right\rangle_2$ or $\left|\Psi^+\right\rangle_1 \left|\Phi^+\right\rangle_2$), this happens with probability $F(1\text{-}F)$

– Because we cannot tell if the error was in pair 1 or pair 2, we have no choice but to *discard pair* 1, even though it might be good

Purification Protocol With Imperfect Bell Pair

- If both Bell pairs have an error, i.e. $|\Psi^+\rangle_1|\Psi^+\rangle_2$, Alice and Bob will find the same value, i.e. (0,0) or (1,1) and therefore *pair 1 is kept*
- With probability $(1-F)^2$, the error in pair 1 goes undetected due to the error in pair 2

Purification Protocol With Imperfect Bell Pair

– The table below shows the possible combinations of our two Bell pairs in purification, when the *only errors* are *bit flip errors*

Pair 1	Pair 2	Probability	Measurement Result	Action	Result	Comment
$\lvert\Phi^+\rangle$	$\lvert\Phi^+\rangle$	F^2	00 or 11	Keep	$\lvert\Phi^+\rangle$	**True Positive**
$\lvert\Phi^+\rangle$	$\lvert\Psi^+\rangle$	$F(1-F)$	01 or 10	Discard	N/A	False Negative
$\lvert\Psi^+\rangle$	$\lvert\Phi^+\rangle$	$(1-F)F$	01 or 10	Discard	N/A	True Negative
$\lvert\Psi^+\rangle$	$\lvert\Psi^+\rangle$	$(1-F)^2$	00 or 11	Keep	$\lvert\Psi^+\rangle$	**False Positive**

Purification Protocol With Imperfect Bell Pair

The essence of purification boils down to this:

– The operation "succeeds" (including the false positive case engendered by two errors) with probability $p_S = F^2 + (1-F)^2$ failing with probability $p_{Fail} = 2F(1-F)$

– When it succeeds, the resulting fidelity is $F' = \dfrac{F^2}{F^2 + (1-F)^2}$ and our final state is $\rho' = F' |\Phi^+\rangle\langle\Phi^+| + (1-F')|\Psi^+\rangle\langle\Psi^+|$

Pair 1	Pair 2	Probability	Measurement Result	Action	Result	Comment
$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	F^2	00 or 11	Keep	$\|\Phi^+\rangle$	True Positive
$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	$F(1-F)$	01 or 10	Discard	N/A	False Negative
$\|\Psi^+\rangle$	$\|\Phi^+\rangle$	$(1-F)F$	01 or 10	Discard	N/A	True Negative
$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$(1-F)^2$	00 or 11	Keep	$\|\Psi^+\rangle$	False Positive

Purification Protocol With Imperfect Bell Pair

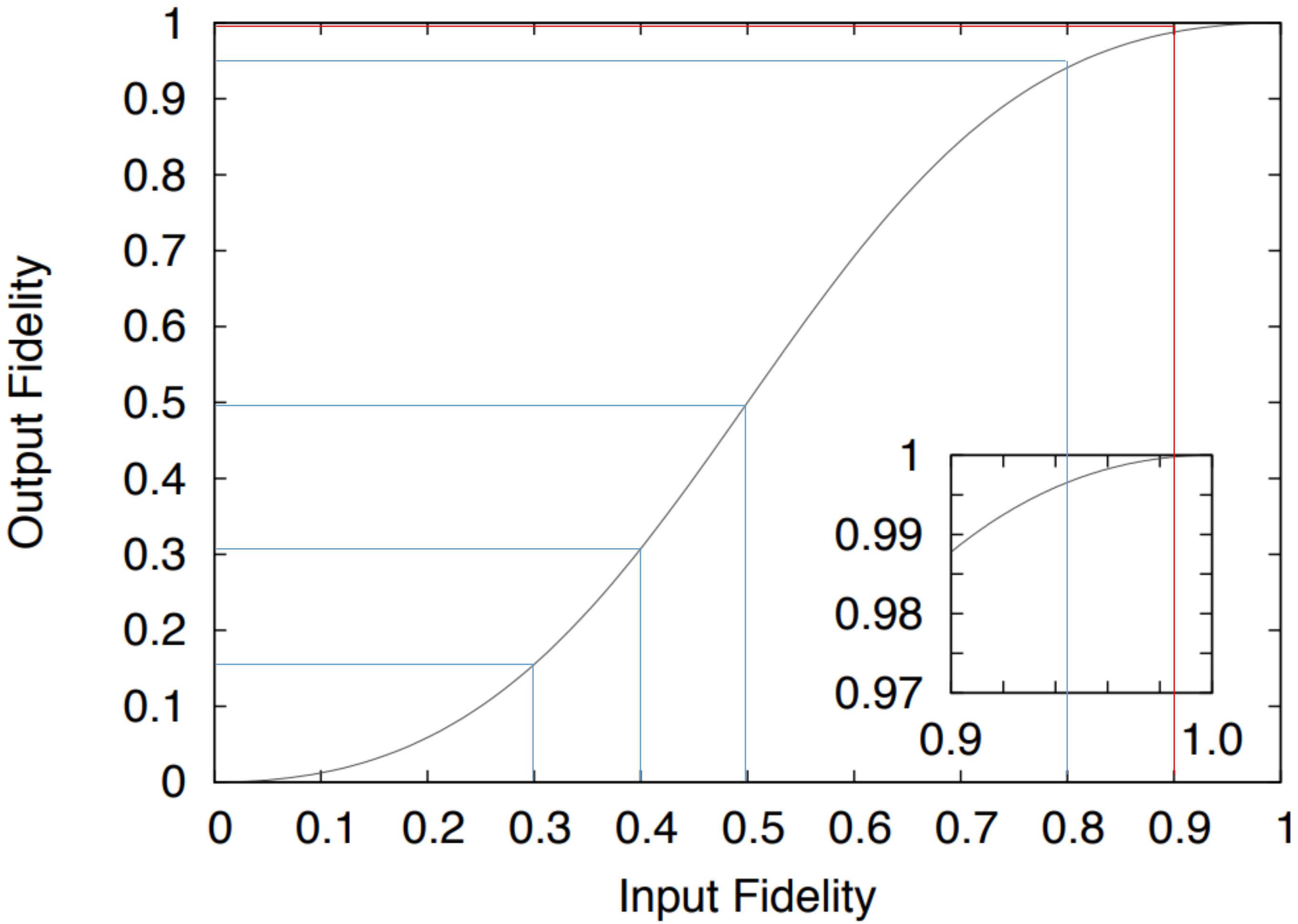
– It remains to check whether $F' > F$, i.e.

$$F' = \frac{F^2}{F^2 + (1-F)^2} > F \quad \rightarrow \quad \frac{F}{F^2 + (1-F)^2} > 1 \quad \rightarrow \quad F > F^2 + (1-F)^2 \quad \rightarrow$$

$$F(1-F) > (1-F)^2 \quad \rightarrow \quad F > 1-F \quad \rightarrow \quad F > 0.5$$

– Thus, if $F > 0.5$ then $F' > F$

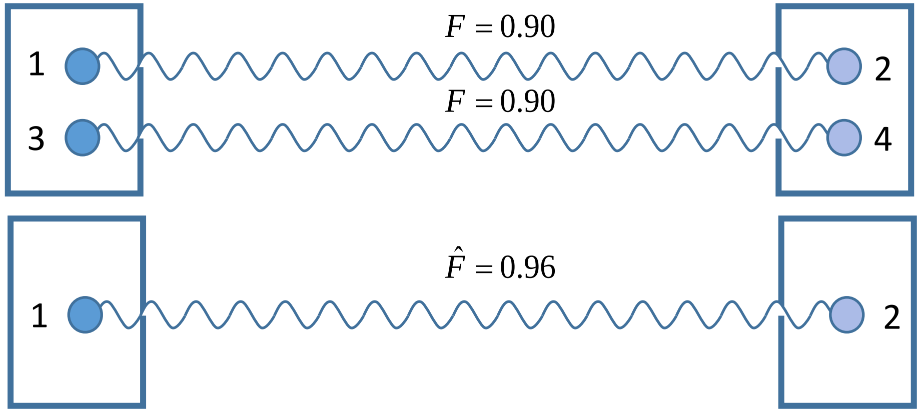
Purification Protocol With Imperfect Bell Pair



- The next figure shows the output fidelity as a function of input fidelity for basic purification of *two identical Bell pairs with bit flip errors only* and *perfect purification operations*
- Above the 0.5 threshold, the purification process will gain fidelity of desired state

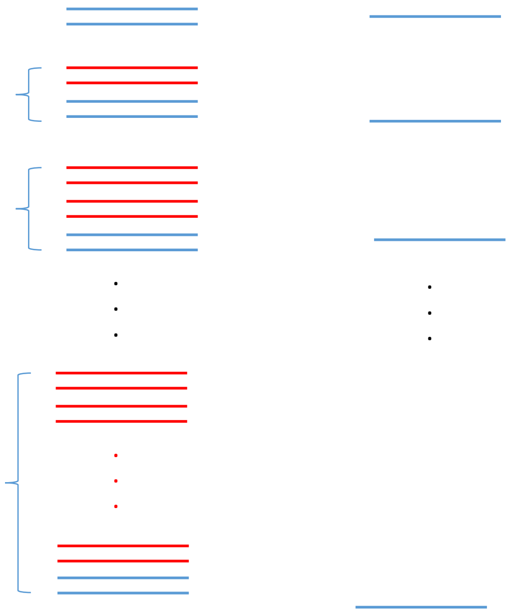
Purification Protocol Resources

- The *purification protocol* is a *probabilistic* protocol i.e., it creates probabilistically a higher fidelity pair $(\hat{F} = 0.96)$ out of two pairs with weaker fidelities $(F = 0.90)$
- We denote by p_s the probability to succeed, that is the probability that the measurement result is 00 or 11 when measuring particles (qubits) 3 and 4
- As previously mentioned, conventionally, these pairs are identified as the **source** and **target** pairs



In the following slide we calculate the average number of entangled pairs needed to obtain a purified pair

Purification Protocol Resources

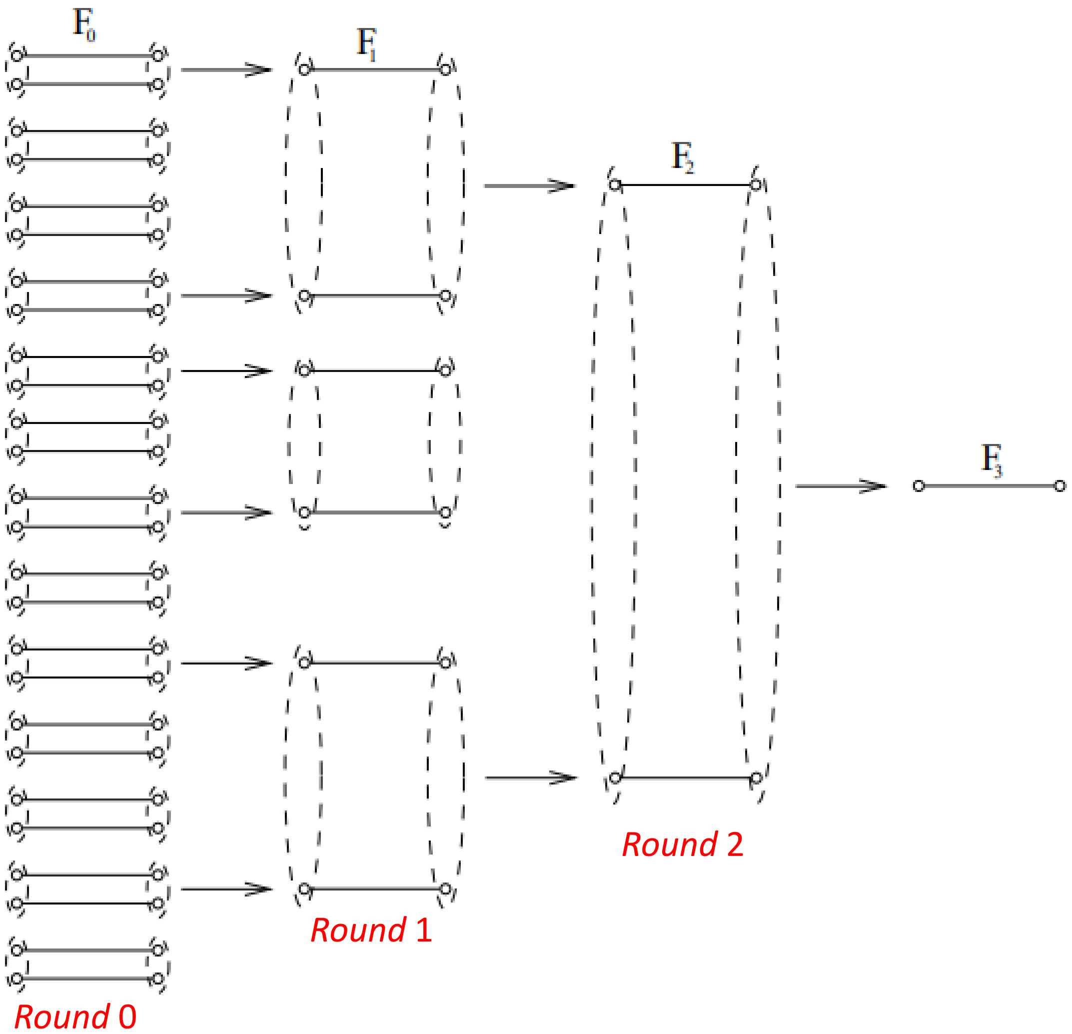


Probability	*Number of entangled connections consumed*	*Number of attempts made to achieve purification success*
p_S	2	1
$(1-p_S)\,p_S$	4	2
$(1-p_S)^2\,p_S$	6	3
$\vdots$	$\vdots$	$\vdots$
$(1-p_S)^{n-1}\,p_S$	$2n$	n

Average number of entangled connections needed to obtain a purified connection

$$=\sum_{n=1}^{\infty}(2n)(1-p_S)^{n-1}\,p_S=2p_S\sum_{n=1}^{\infty}n(1-p_S)^{n-1}=\frac{2p_S}{\left[1-(1-p_S)\right]^2}=\frac{2}{p_S}$$

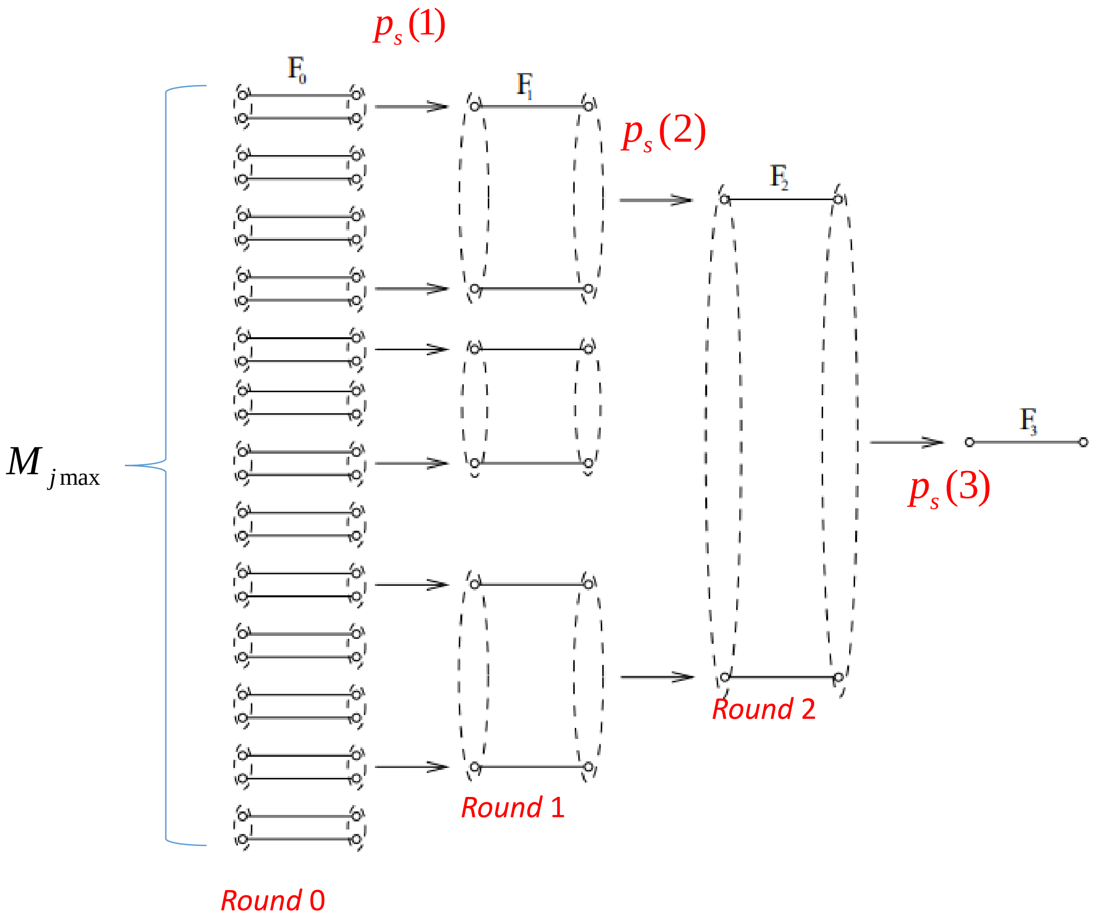
Distillation Process



- The *distillation process* consists of several rounds
- In each round, the pairs are combined into groups of two at a time, and the *purification protocol* is applied to them
- From round to round, the entanglement of the remaining pairs is increased
- The process can be iterated to produce even larger fidelities until (in theory after an infinite number of iteration) a maximally entangled Bell state is obtained

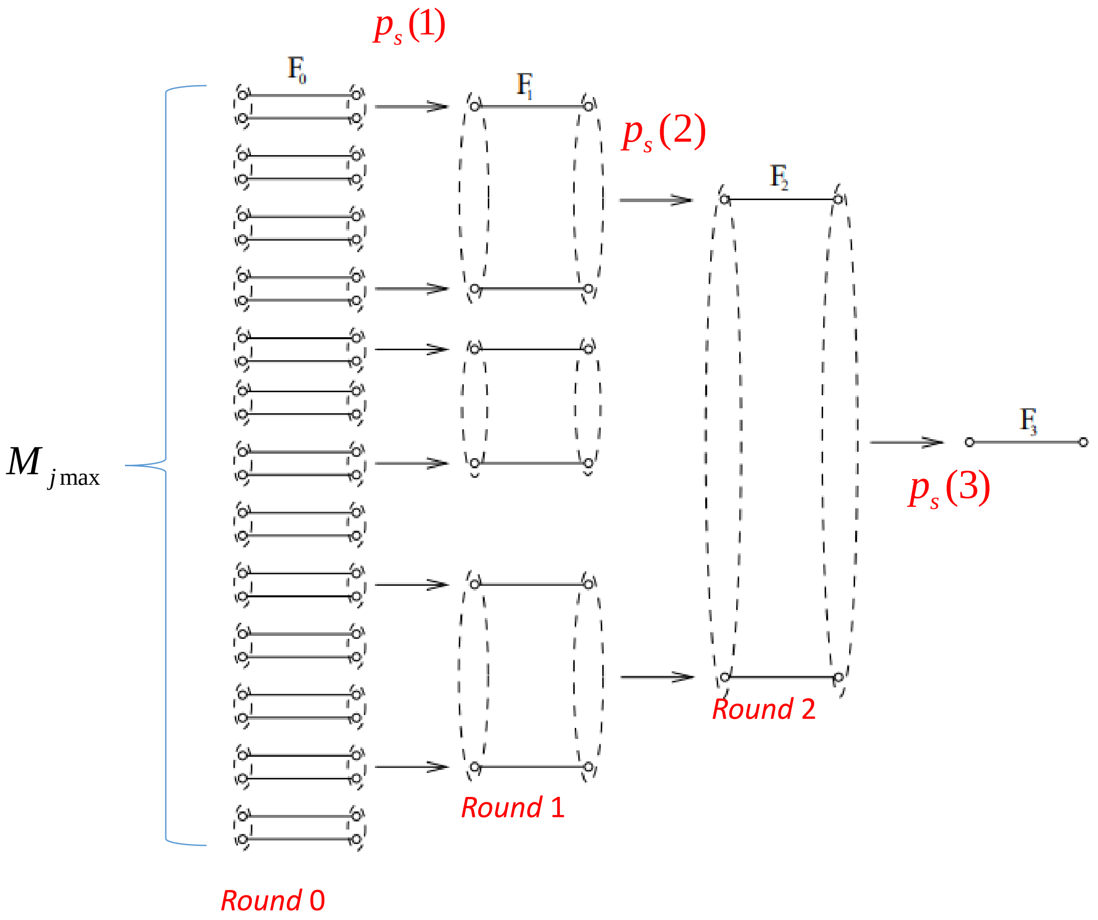
NOTE: There are alternative distillation processes: pumping, greedy, banded

Resources



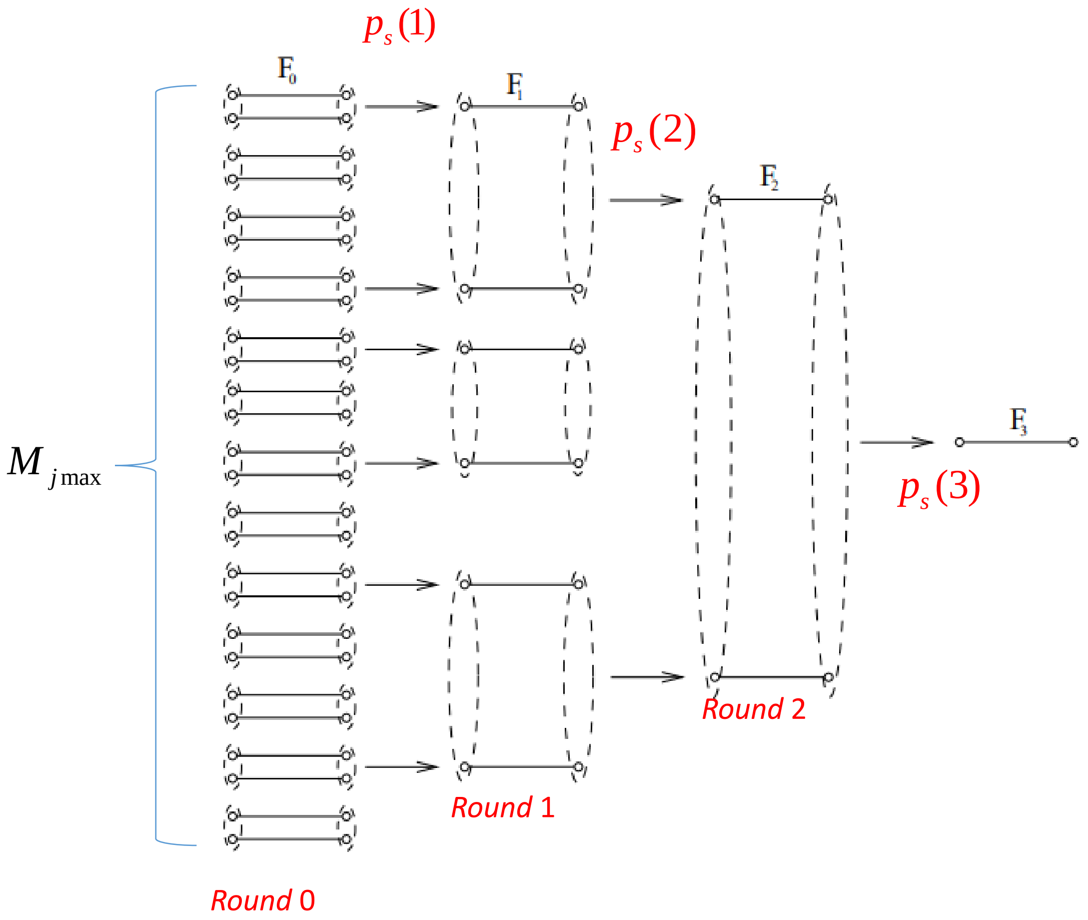
- One can give an expression for the total resources, that are the number of entangled connections needed to perform a given number of *rounds*.
- Let us assume that one always uses identical entangled connections for each round, and denote the initial fidelity, that is the fidelity of the entangled connections before any purification is performed by F_0.

Resources



- Let's call the fidelity after the first successful purification round F_1 and the fidelity after the j^{th} purification round F_j .
- The values of F_j can be obtained by iterated application of an expression (see later) using F_{j-1} as initial value.

Resources

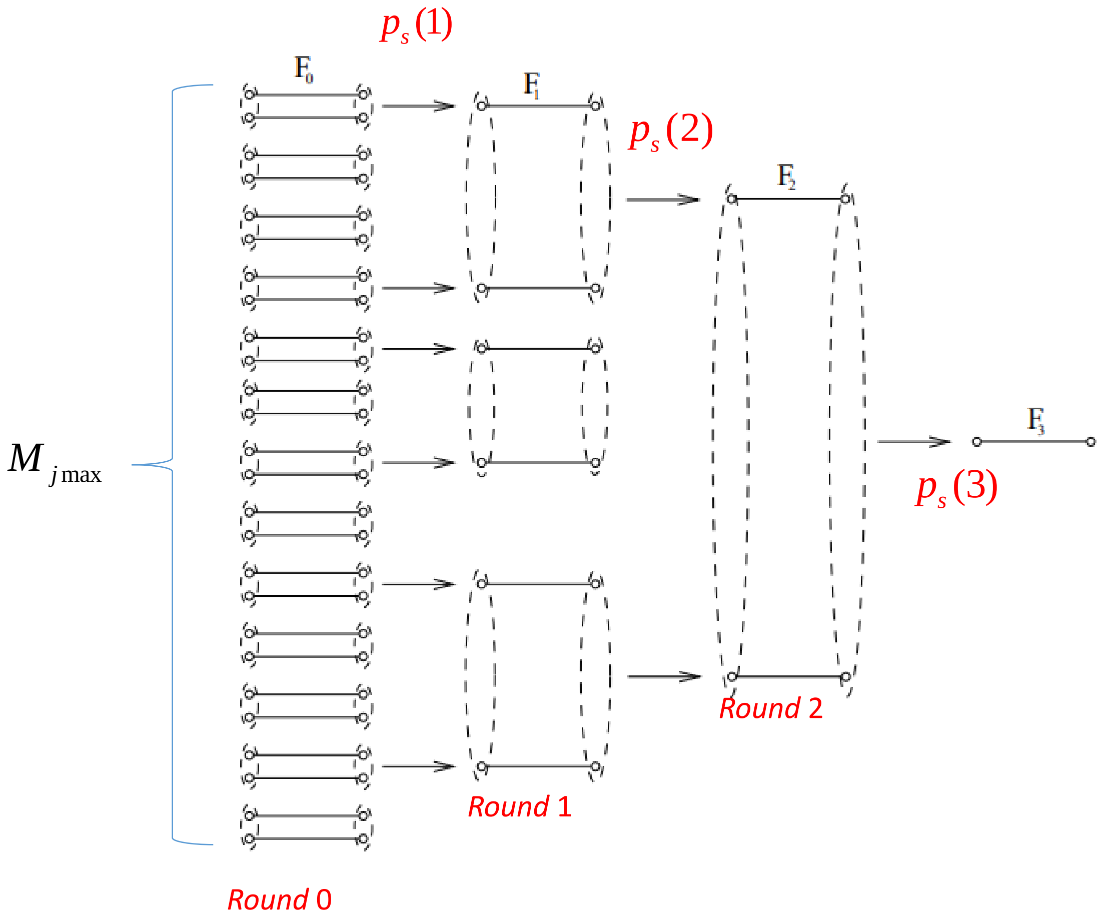


- After j_{max} successful purification rounds, the total number of entangled connections needed to obtain on average one entangled connections with fidelity $F_{j_{\max}}$ is given by

$$M_{j_{\max}} = \prod_{j=1}^{j_{\max}} \left[\frac{2}{p_s(j)} \right]$$

- where $p_s(j)$ is the probability that the purification protocol succeeds at the (j-1)th round.

Resources



If we begin with $M_{j_{\max}}$ entangled connections, at the end of the first round we will have on average

$$M_1 = \frac{M_{j_{\max}}}{2} p_s(1)$$

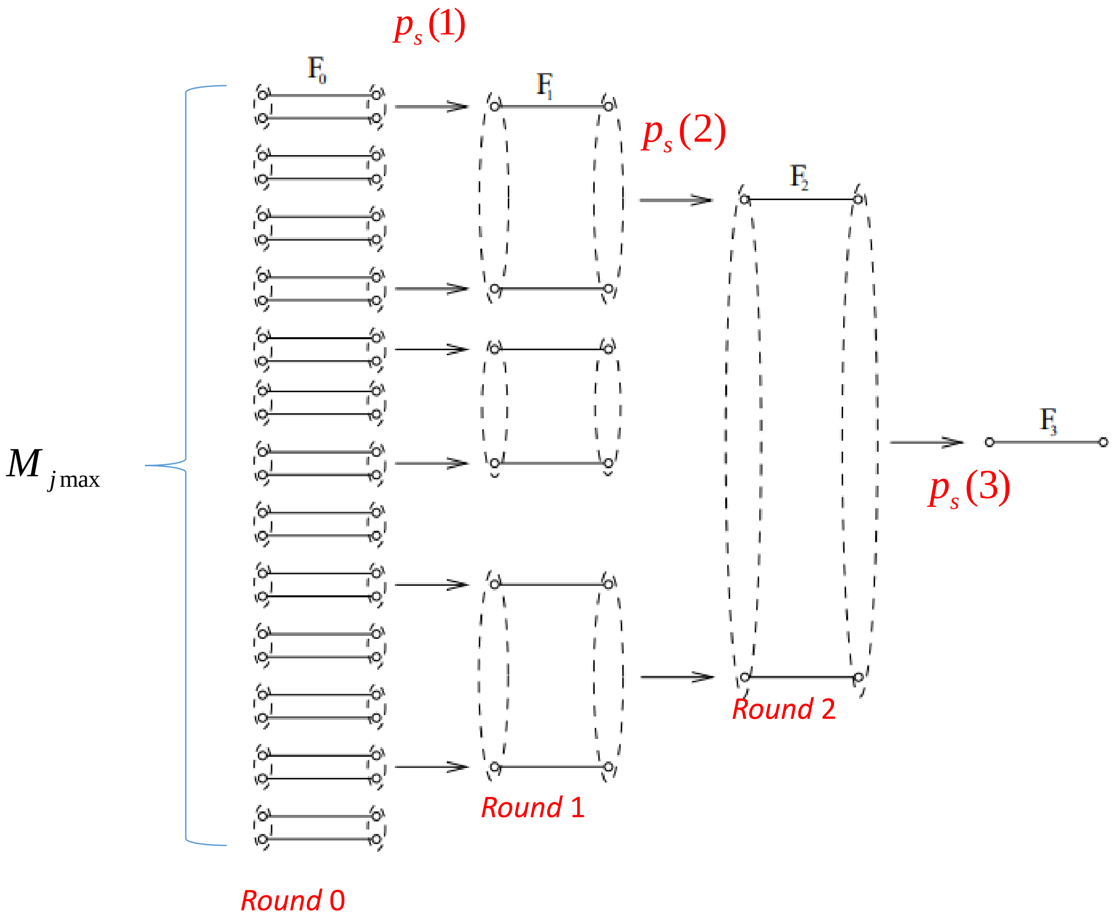
successfully entangled connections with fidelity $F_1 > F_0$

At the end of the second round, we have on average

$$M_2 = \frac{M_1}{2} p_s(2) = \frac{1}{2}\left(\frac{M_{j_{\max}}}{2} p_s(1)\right) p_s(2) = M_{j_{\max}} \left(\frac{p_s(1)}{2}\right)\left(\frac{p_s(2)}{2}\right)$$

successfully elementary pairs with fidelity $F_2 > F_1$

Resources



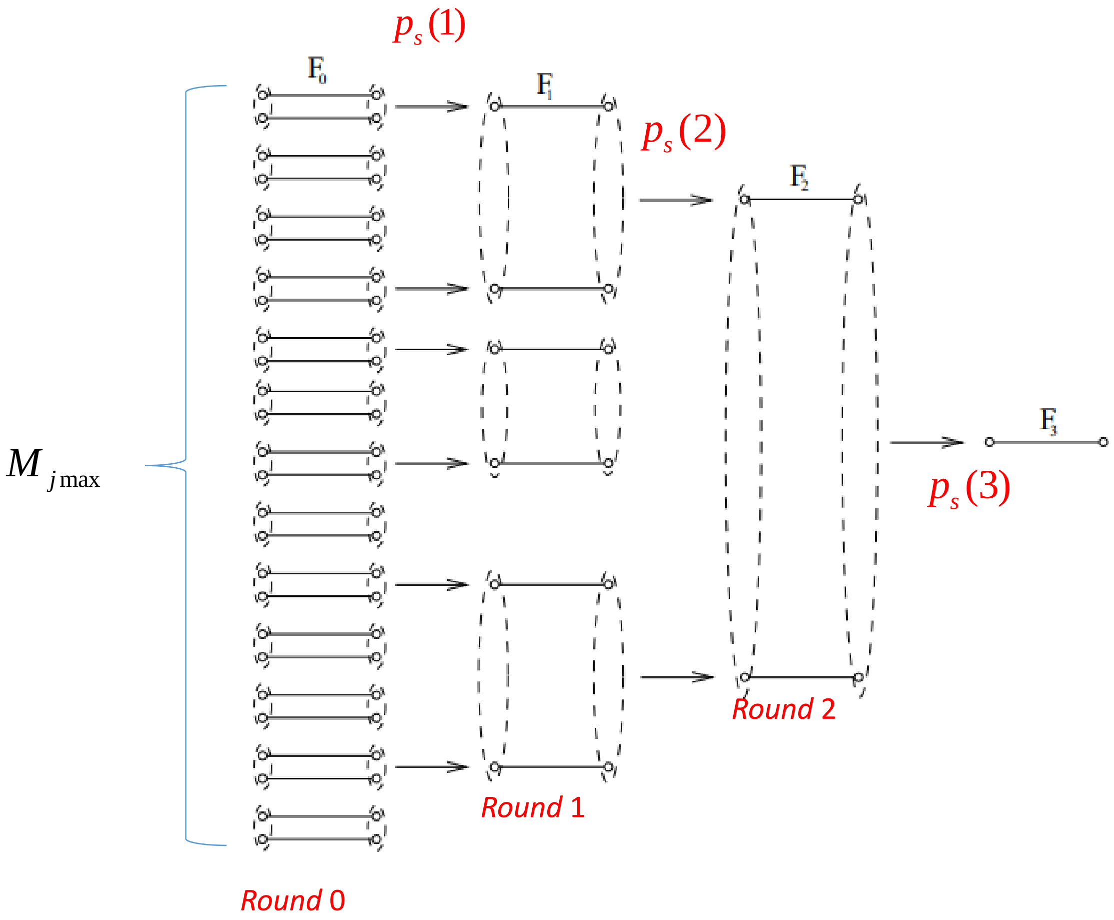
- If, after $j_{\max}$ successful purification rounds we should obtain, on the average, one elementary pair then we should impose the condition

$$M_{j_{\max}}\left[\frac{p_s(1)}{2}\right]\left[\frac{p_s(2)}{2}\right]\left[\frac{p_s(3)}{2}\right]\cdots\left[\frac{p_s(j_{\max})}{2}\right]$$

$$=\prod_{j=1}^{j_{\max}}\left[\frac{p_s(j)}{2}\right]=1$$

$$\rightarrow M_{j_{\max}}=\prod_{j=1}^{j_{\max}}\left[\frac{2}{p_s(j)}\right]$$

Resources



By using the notations in the figure, we can rewrite the fidelity expression

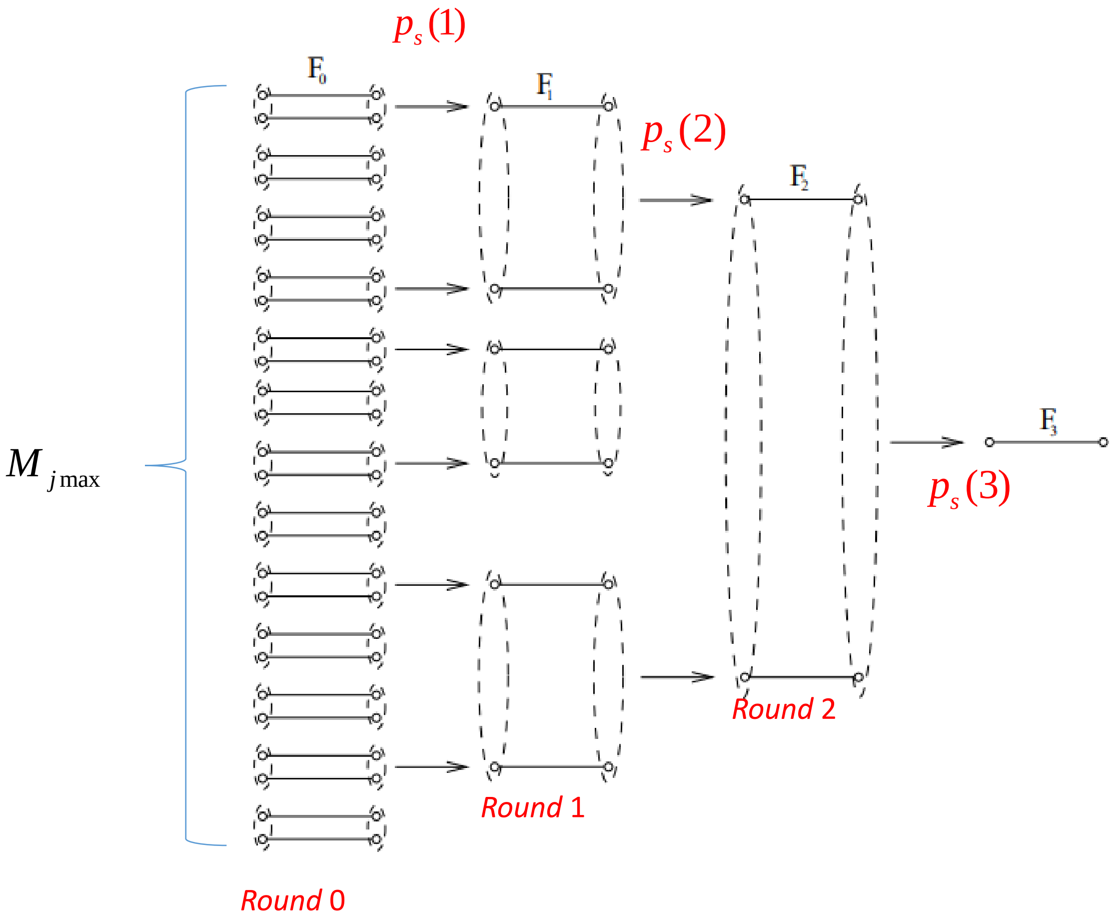
$$F' = \frac{F^2}{F^2 + (1-F)^2} \qquad [1]$$

calculated before, as following

$$F_1 = \frac{F_0^2}{F_0^2 + (1-F_0)^2}$$

In general, the value of F_j can be obtained by iterated application of [1] using F_{j-1} as initial value

Resources



Furthermore

$$p_s(1) = F_0^2 + (1 - F_0)^2$$

Typically, calculating $p_s(j)$ involves calculating fidelity F_{j-1} iteratively, as previously mentioned in the previous slide.

Deutsch’s Protocol (DEJMPS)

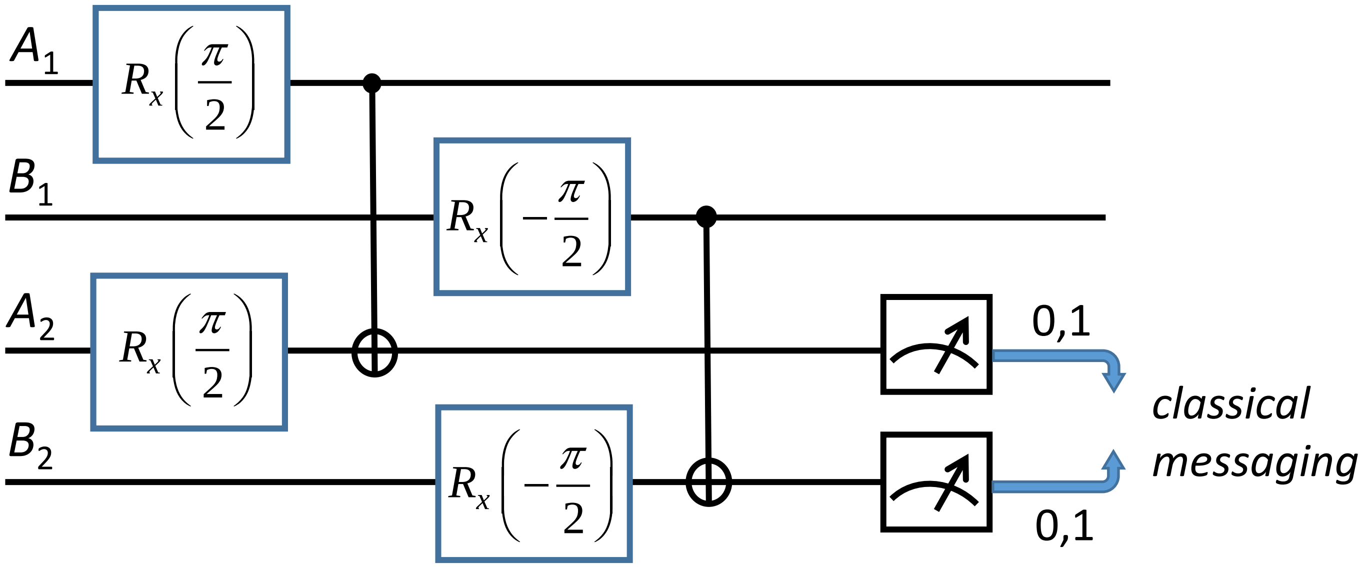
- Bennett’s protocol suffers from 2 major drawbacks
- For it to work, the initial state must be of the Werner form
- Secondly, it takes many rounds of purification to obtain a Werner state with fidelity above 99% when one starts with low fidelity pairs (e.g., $F = 85\%$)
- Deutsch et al. [1] addressed these issues by modifying Bennett’s protocol

[1] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, “Quantum privacy amplification and the security of quantum cryptography over noisy channels,” Phys. Rev. Lett., vol. 77, pp. 2818–2821, Sep 1996. [Online]. Available: https: //link.aps.org/doi/10.1103/PhysRevLett.77.2818

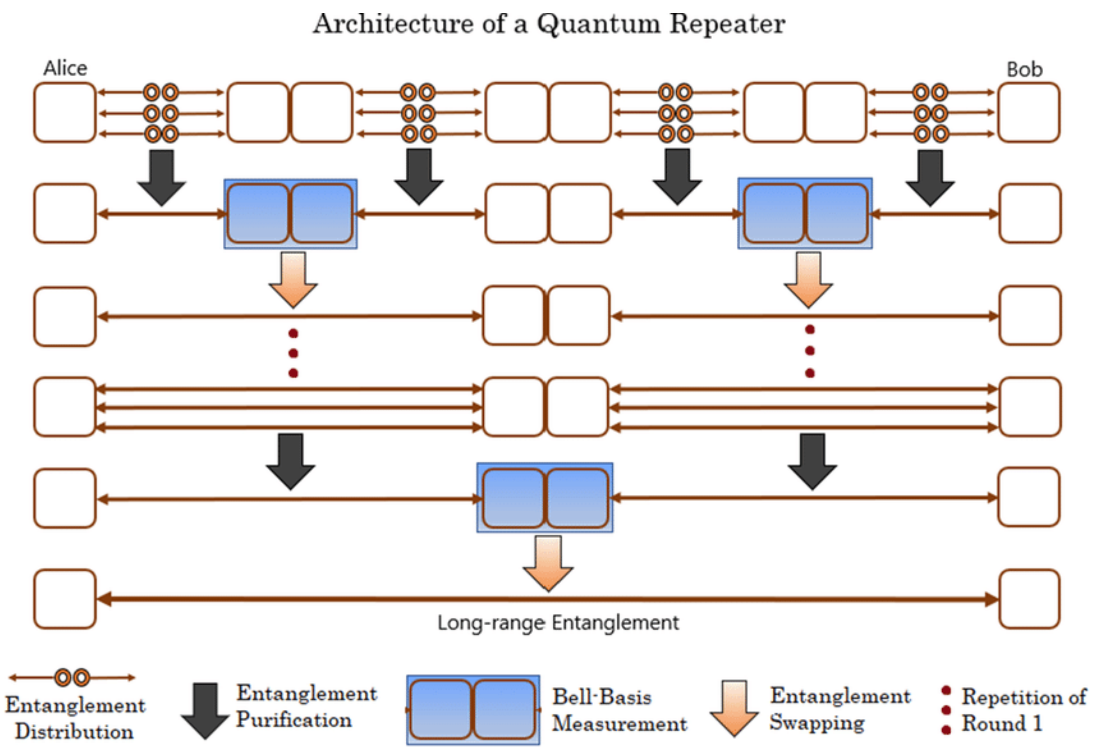
Deutsch’s Purification Protocol

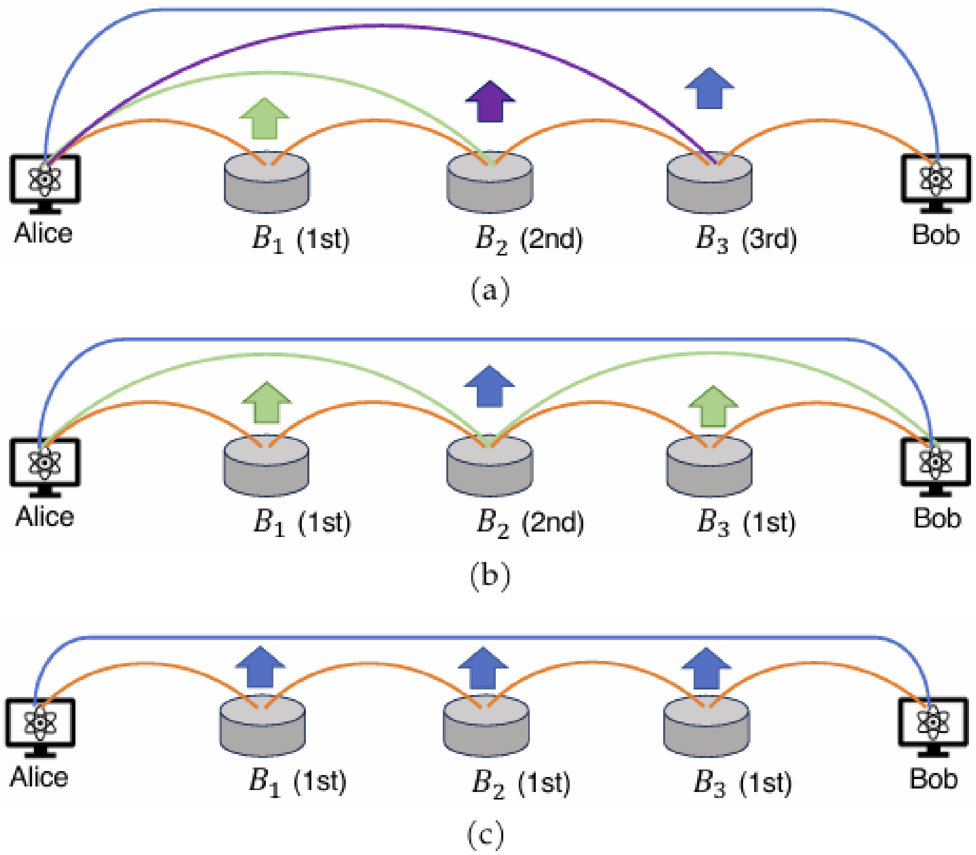
- Deutsch et al. proposed that, before applying the CNOT Gate, Alice should perform a rotation $Rx(\pi/2)$ on her qubits, and Bob should perform the inverse rotation $Rx(-\pi/2)$
- All the other operations may be performed as in Benett’s Algorithm
- This procedure results in a theoretical increase in fidelity of about **100 times** more than that of Bennett’s
- Moreover, the initial states of the Bell-Pairs need not be of the Werner form

Deutsch’s Purification Protocol



Distillation Process & Entanglement Swapping Working Jointly

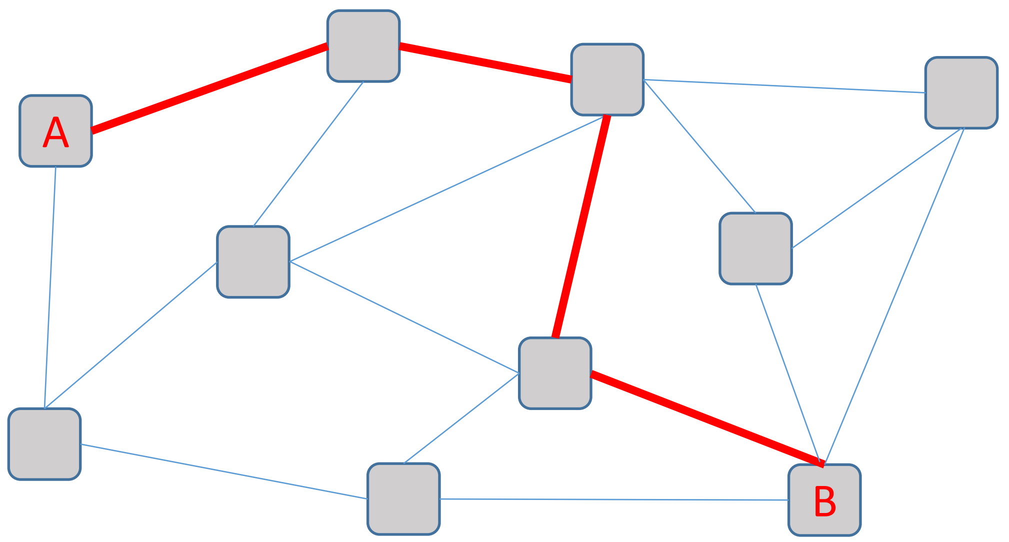




Linear vs Mesh Quantum Repeater Networks

– So far, we have considered linear quantum network repeater setups

– This choice might seem a limit because the quantum internet will undoubtedly be a mesh network



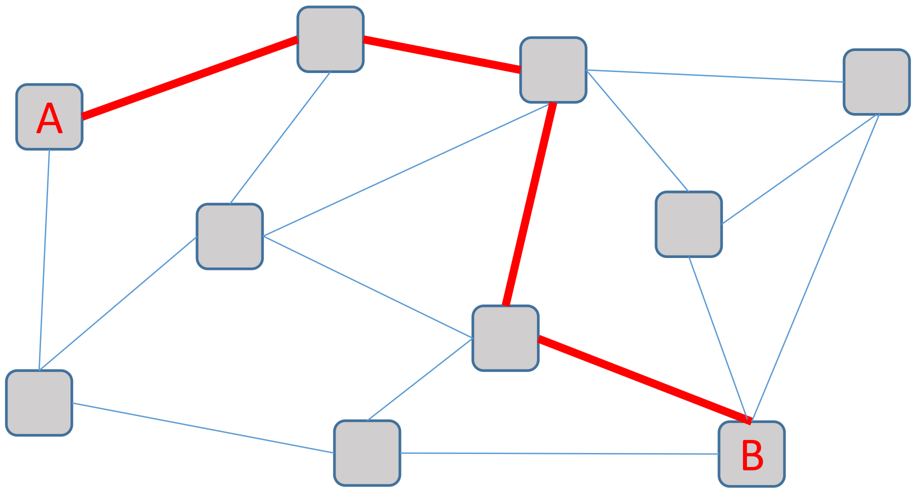
- However, we are actually studying the quantum Internet after the routing protocol has selected a path for developing the entangled connection
- This path is indeed a linear sequence of quantum repeaters

Making a Network

- We have considered two important ingredients that are needed to make a network
- We looked at how to create link-level entanglement between neighboring nodes, and how to extend it to end-to-end entanglement with entanglement swapping
- There are a few missing parts, however
- The main two are **routing**, and **multiplexing**

Making a Network

- We learnt from previous lectures that the job of a quantum network is to establish end-to-end entanglement between distant nodes, which is then consumed by applications
- The network needs a way of picking a suitable path (red path) along which to execute entanglement swapping that leads to this end-to-end connection

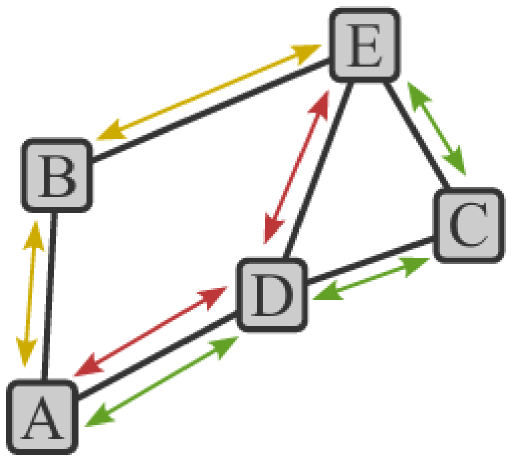


Making a Network

- The second issue is that the figure shows only one connection request being considered
- Of course, a network will most likely be used by more than one application at a time
- Therefore, the network should be able to satisfy multiple simultaneous connection requests between distinct end nodes
- How the network picks an appropriate path where it performs entanglement swapping is determined by the **routing algorithm** using information about the topology and condition of the network

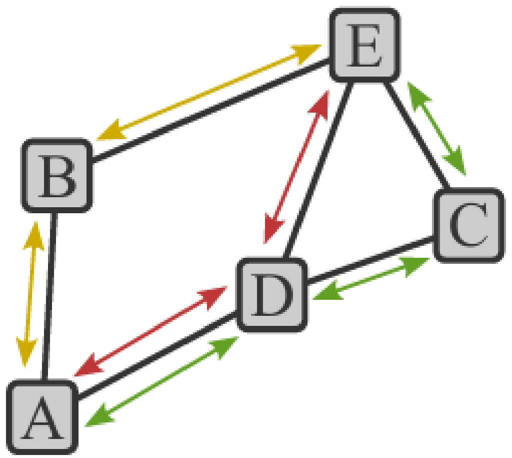
Making a Network

- The following figure shows a simple case of a quantum network with five nodes
- Let's say that nodes *A* and *E* would like to establish an entangled connection
- There are three possible paths that the network can choose
- It can swap entanglement at node *B* (option 1), or at node *D* (option 2), or at nodes *C* and *D* (option 3)
- Each option requires the establishment of different patterns of link-level entanglement



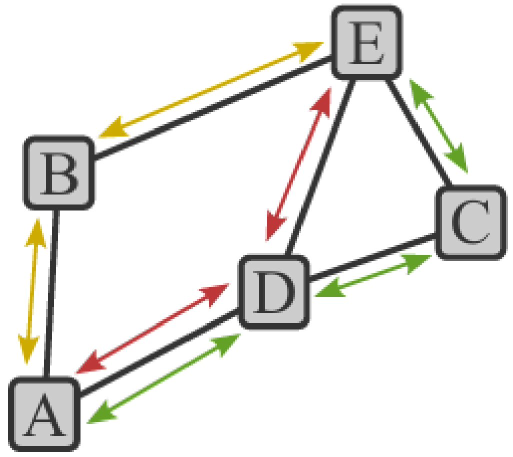
Making a Network

- **Option 1** requires link-level entanglement between *A-B* and *B-E* before the entanglement swapping can be executed
- Similarly, **option 3** requires link-level entanglement on the *A-D*, *D-C*, and *C-E* links
- In order to evaluate which path is best, we need to look at the cost for establishing the corresponding link-level entanglement, and then how to combine these costs in order to establish the cost for the entire path



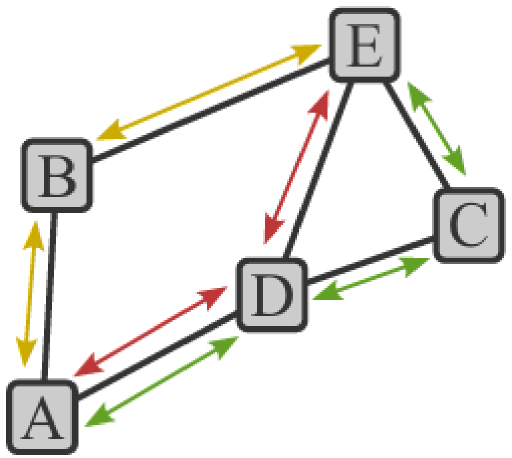
Making a Network

- One possible way to evaluate the link-level entanglement is **seconds per Bell pair at a threshold fidelity**
- We discussed how establishing a link-level entanglement involves photon emission from quantum memories, and subsequent measurement of these photons in the Bell basis
- These processes are all probabilistic, and so is loss of the photons in fiber
- Depending on the properties of the fiber as well as the quantum hardware at each node, the average time required to successfully establish link-level Bell pair will vary



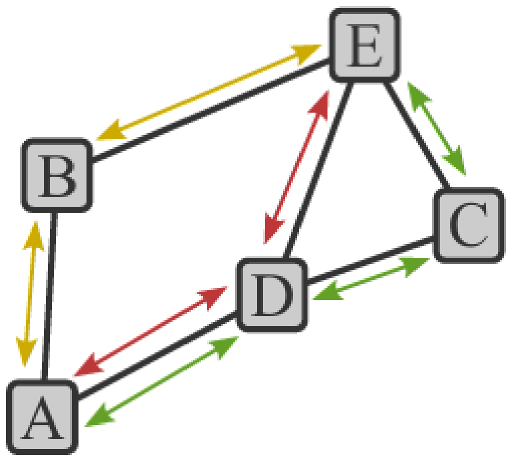
Making a Network

- How do we combine these costs for each individual link in order to know the full cost of establishing end-to-end entanglement over a path?
- One possibility is to use **Dijkstra's shortest path first algorithm**
- We can sum the link-level costs for an individual path in order to estimate the total cost
- We have seen that sometimes we need to purify Bell pairs, which reduces our effective throughput by at least a factor of two



Making a Network

- In order to balance the trade off between the rate of making raw Bell pairs and fidelity and make the comparison between two links fair, we demand that the link-level Bell pairs be of certain threshold fidelity, achieved using purification if necessary
- The exact value of this threshold is dictated by the needs of the application that is requesting the Bell pairs

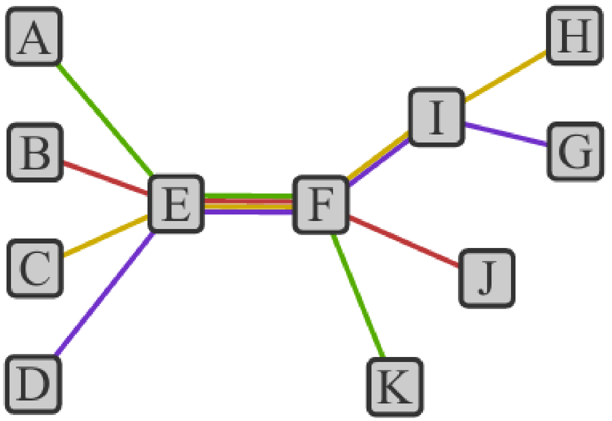


Making a Network

- The next issue that networks have to deal with is **multiplexing**
- The network will have to satisfy multiple simultaneous connection requests for end-to-end entanglement
- A good multiplexing scheme helps the network decide how to allocate its resources to satisfy these requests in a timely, reliable and fair manner

Making a Network

- The right figure shows four simultaneous requests for entanglement between nodes *A-K*, *B-J*, *C-H*, and *D-G*
- All of these requests need to use link-level entanglement between *E-F*, creating contention on this link
- Another link with contention is *F-I*, although only two connections need to use that link
- The network must know how to handle such requests, where a single link needs to be shared between multiple users or connections



Making a Network

- In this part, we have seen the four requirements for building a quantum network
- We started with the basic building block of establishing link-level entanglement between neighboring nodes of a network and how to handle pho ton losses
- Next, we discussed how to use entanglement swapping to splice the link-level entanglement into long-distance end-to-end connections between non-neighboring nodes
- Finally, we briefly discussed routing and multiplexing in quantum networks

Quantum Internet Protocol Stack

- Stemming from the knowledge gained through the previous lectures, we now show **one** of **three** available contributions for the Quantum Internet protocol stack
- In the upcoming slides, my focus will be on the layered model for quantum networks, which relies on bipartite entanglement, proposed by Wehner et al. in [1, 2, 3]

[1] A. Dahlberg, M. Skrzypczyk, T. Coopmans, et al., A link layer protocol for quantum networks, in: Proc. of ACM SIGCOMM ’19, 2019, p. 159–173.

[2] W. Kozlowski, S. Wehner, Towards large-scale quantum networks, in: Proc. of ACM NANOCOM ’19, 2019, pp. 1–7.

[3] W. Kozlowski, A. Dahlberg, S. Wehner, Designing a quantum network protocol, in: Proc. of the 16th International Conference on emerging Networking EXperiments and Technologies, 2020, pp. 1– 16.

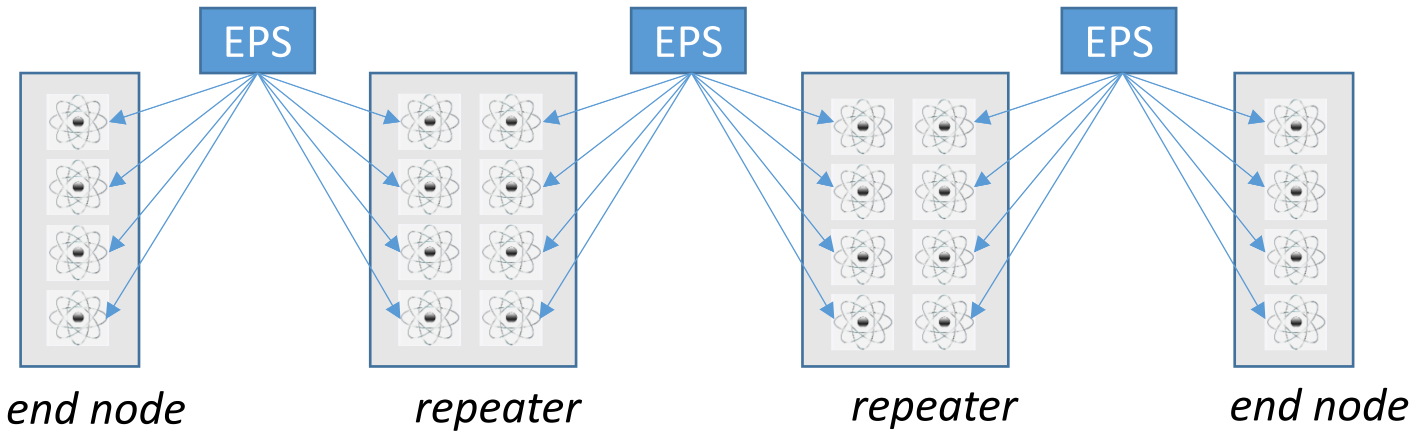
Quantum Internet Protocol Stack

Layers	Main Functionality
Application	Application
Transport	Qubit Transmission
Network	End to End Entanglement
Link	Robust Entanglement Generation
Physical	Entanglement Generation Attempt

The protocol stack by Wehner et al. is organized into five layers

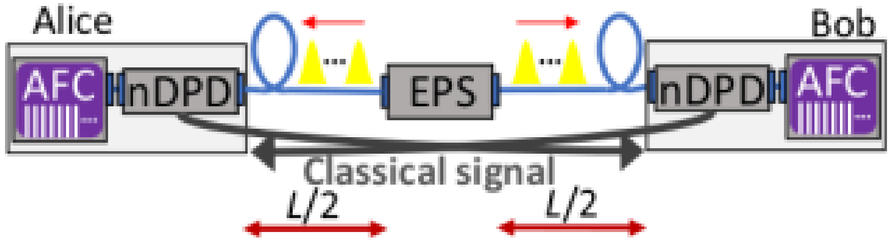
Physical Layer

- The first layer, i.e., the *Physical Layer,* attempts to generate entanglement between two nodes in well-defined time slots
- The physical layer protocol is a result of a deep understanding of the actual hardware implementations
- Specifically, the physical layer is mainly reduced to the physical generation of EPR pairs through laser pulses, with multiple EPR pairs generated for each couple of adjacent nodes



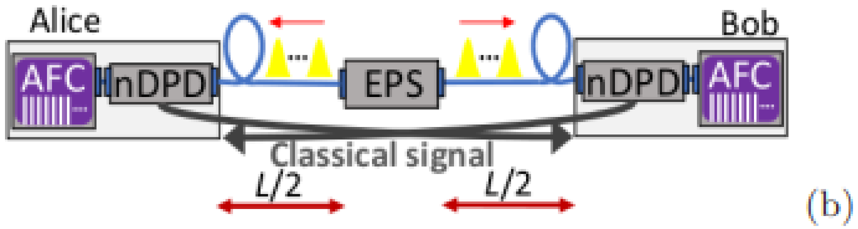
Link Layer

- Then, the *Link Layer* is in charge of enhancing the physical layer functionality by transforming *entanglement attempts* into a *robust entanglement generation service*
- The above two layers operate only on single-hop links

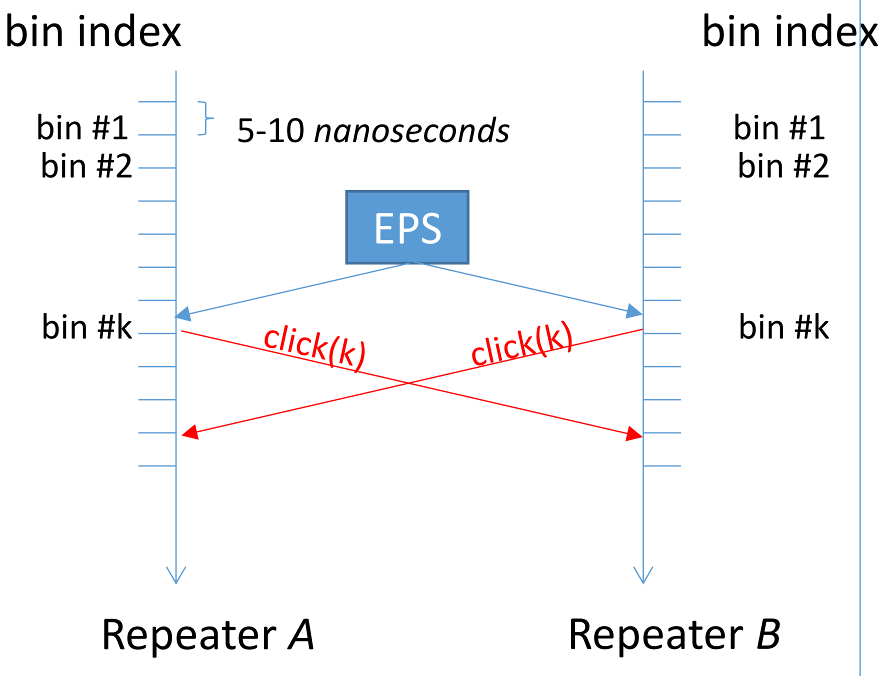


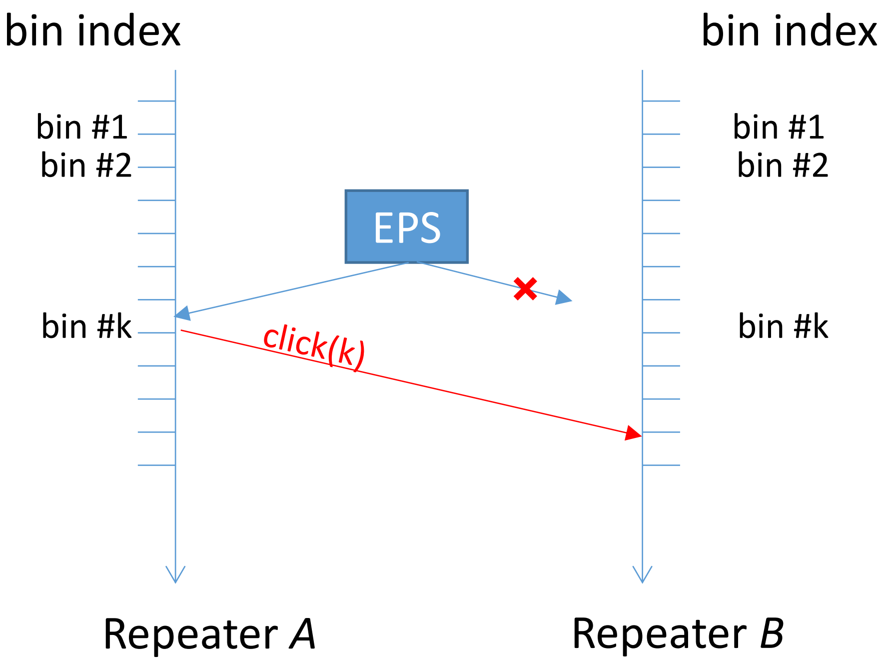
(b)

Link Layer



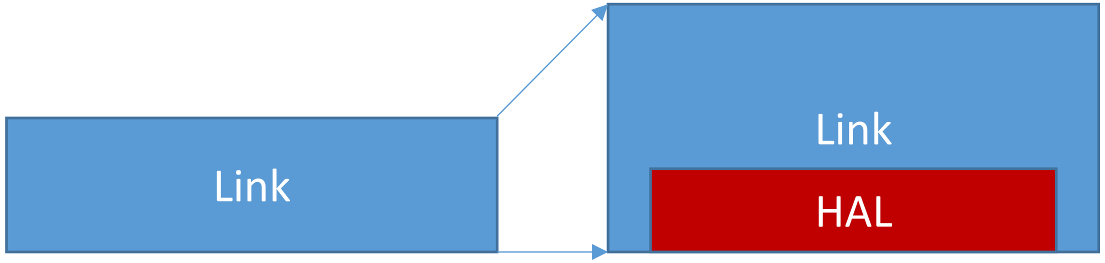
Click(k) is a form of heralded signal





Link Layer

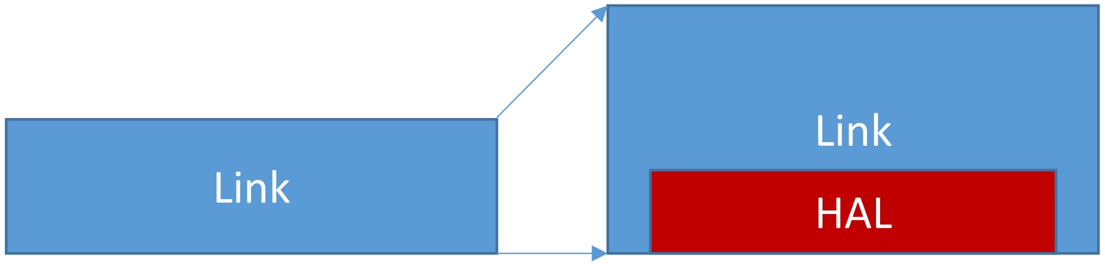
- Since there are several hardware technologies, the authors enriched the protocols with key parameters in order to make the model hardware independent
- However, such a feature led to the introduction of an additional sub-layer, referred to as Hardware Abstraction Sub-Layer



HAL - Hardware Abstraction Sub-Layer

Link Layer

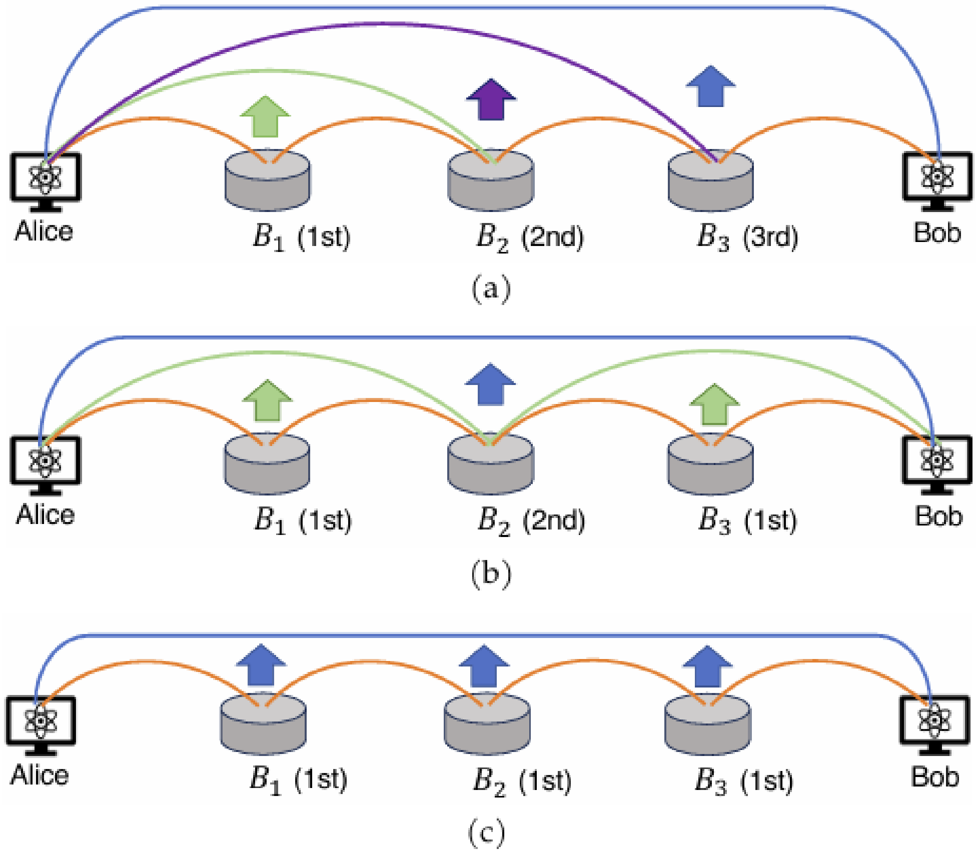
- As represented in the Figure, the HAL is a sub-layer of the link layer, and it is responsible for translating commands and outcomes between the physical layer and the rest of the protocol stack
- Hence, it constitutes a first proposal for abstracting the network protocols from the particulars of the specific physical hardware implementations



HAS - Hardware Abstraction Sub-Layer

Network Layer

- The third layer is the *Network Layer*, responsible for producing long-distance entanglement by means of entanglement swapping and purification, using the link layer services
- Three entanglement swapping policies on a five-nodes chain (two end nodes and three repeaters): (a) Sequential, (b) Nested, (c) As Soon As Possible (ASAP).
- The arcs represent entanglement between the two connected nodes, whereas the arrows and the legend specify the entanglement swapping order

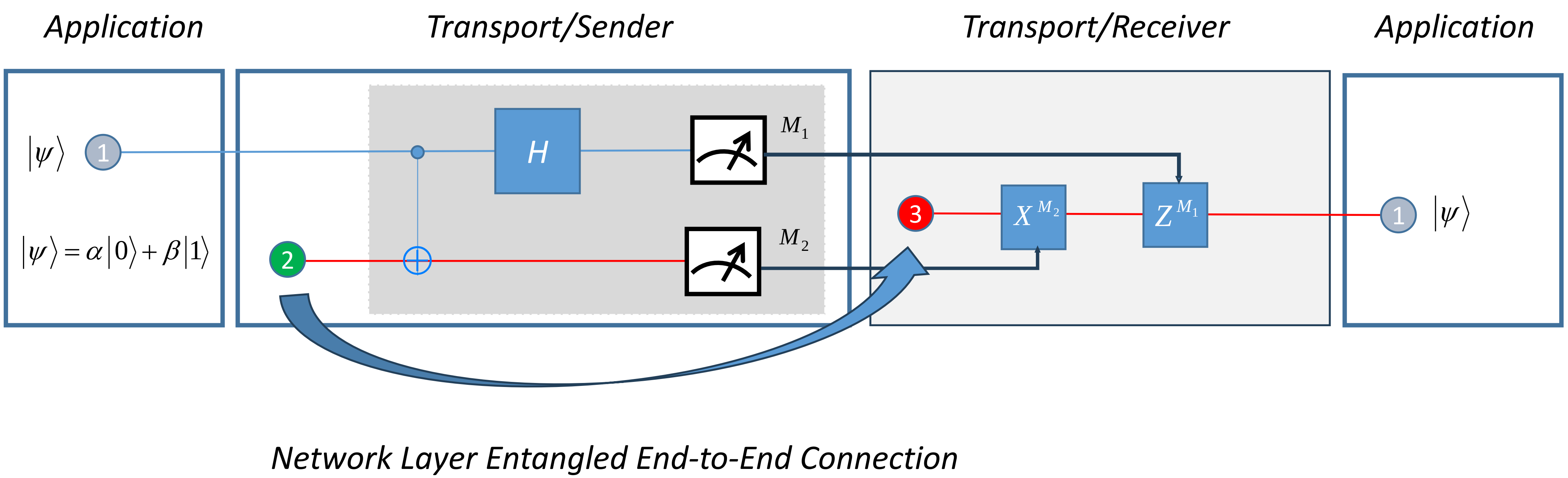


Transport Layer

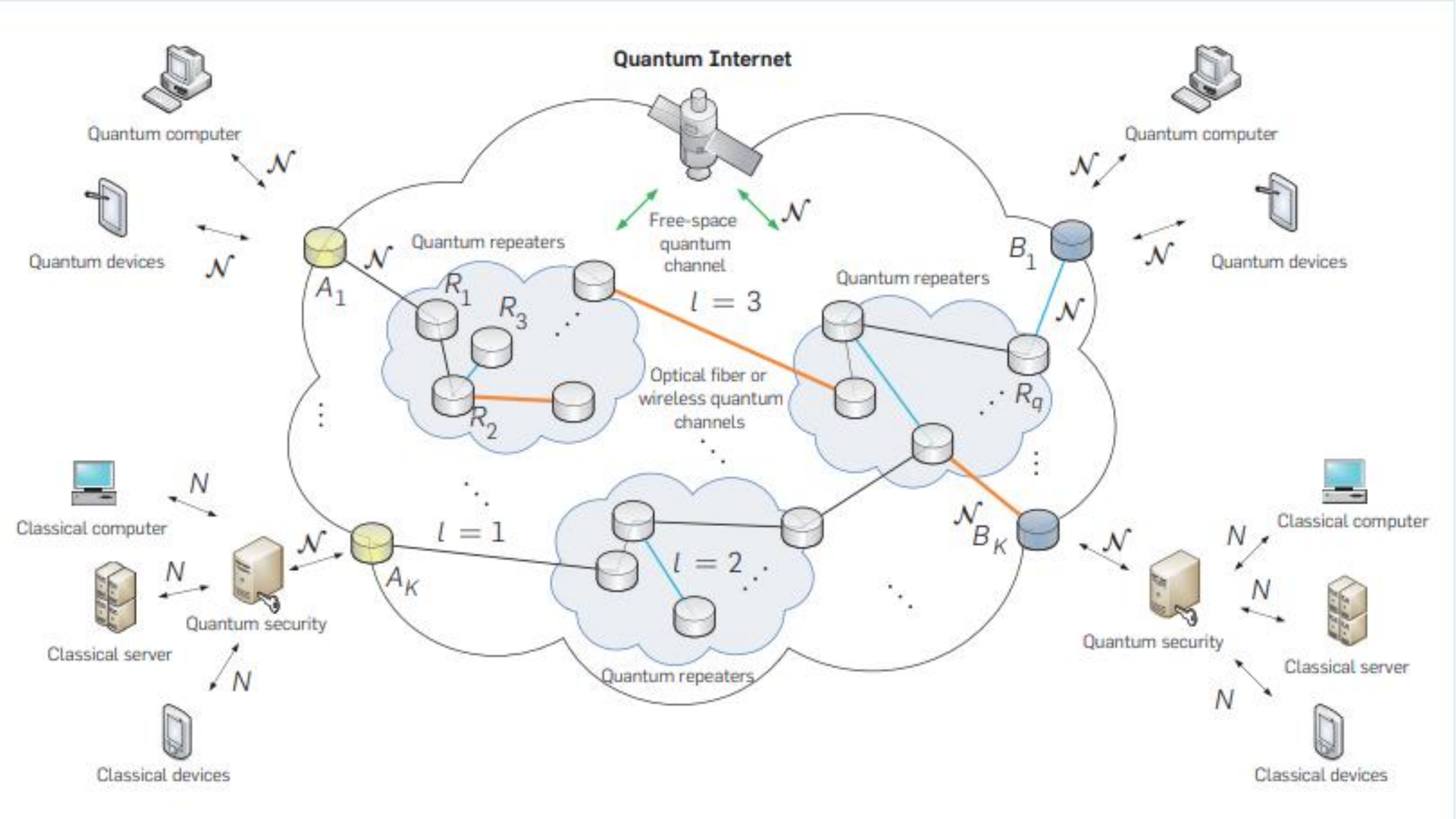
– The *Transport Layer* transfer qubit states – by using, for example, the teleportation process – according to the application layer request

Application Layer

– The *Application Layer* determines when an end-to-end entangled connection is required and which quantum state to teleport



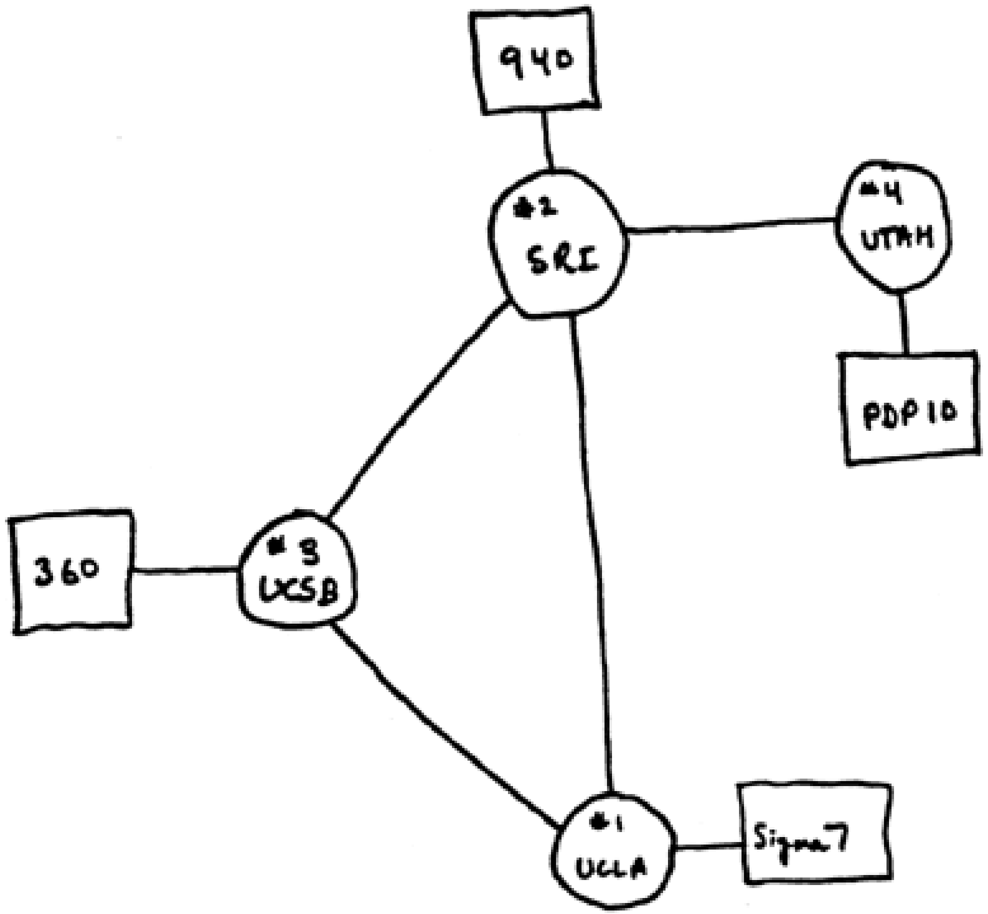
Conclusion



The implementation of the quantum Internet in the version illustrated in the figure is not possible with the current repeater technology

But the research is progressing very rapidly

Conclusion



That's pretty much what happened in 1969 with the Arpanet/Internet

From an initial setup of 4 nodes

……

Separable States Versus Entangled States

- Formally, the distinction between whether a state is entangled or not entangled rests upon whether its quantum state is separable or not
- Therefore, let us examine this question in more mathematical terms
- **Separable State** If a pure (mixed) state, $\left|\psi^{AB}\right\rangle$ ρ^{AB} , of a composite quantum system defined on a Hilbert space $H_A \otimes H_B$ can be written as

$$\left|\psi^{AB}\right\rangle = \left|\psi^{A}\right\rangle \otimes \left|\psi^{B}\right\rangle \quad \rho^{AB} = \sum_i p_i \rho_i^A \otimes \rho_i^B \quad ,$$

then $\left|\psi^{AB}\right\rangle$ ρ^{AB} , is said to be a *separable state*

Separable States Versus Entangled States

- **Entangled State** If a state, $\left|\psi^{AB}\right\rangle$ ρ^{AB} , of a composite quantum system defined on a Hilbert space $H_A \otimes H_B$ is not a separable state it is an entangled state
- Note that a state can be **entangled and pure**, or **entangled and mixed**, simultaneously

Peres-Horodecki Criterion

- Given a purported entangled state, ρ, how can we verify that ρ is, in fact, entangled?
- One approach to decide if a state is entangled, is to use the **Peres-Horodecki criterion**
- This criterion uses an operation on a density matrix known as the **partial transpose**

The Partial Transpose

- Let ρ be a bi-partite density operator expressed in the form:

$$\rho = \sum_{i,j,k,l} \rho_{ij;kl} \left| e_i^A \otimes e_j^B \right\rangle \left\langle e_k^A \otimes e_l^B \right|$$

where $\left| e_i^A \right\rangle$ is an eigenbasis for sub-space *A* and $\left| e_j^B \right\rangle$ is an eigenbasis for sub-space *B*

- Then the partial transpose ρ^{T_B} of the density operator ρ is:

$$\rho^{T_B} = \sum_{i,j,k,l} \rho_{il;kj} \left| e_i^A \otimes e_j^B \right\rangle \left\langle e_k^A \otimes e_l^B \right|$$

Peres-Horodecki Criterion

- **Peres-Horodecki Criterion**: A Necessary and Sufficient Test for Entanglement
- If a bi-partite state is **entangled**, its partial transpose always has **one or more negative eigenvalues**, but if it is **separable** its partial transpose has **no negative eigenvalues**.
- Thus, given a density operator ρ we can decide whether or not it is entangled by examining the signs of the eigenvalues of its partial transpose
- Note that we can define an analogous partial transpose over the "*A*" space as follows:

$$\rho^{T_A} = \sum_{i,j,k,l} \rho_{kj;il} \left| e_i^A \otimes e_j^B \right\rangle \left\langle e_k^A \otimes e_l^B \right|$$

Peres-Horodecki Criterion

- Even though the partial transpose ρ^{T_A} will usually be a different matrix from the partial transpose ρ^{T_B} **their eigenvalues will be the same**
- In applications of the partial transpose it is usually the eigenvalues of the partial transpose that we need rather than the partial transpose itself
- If this is the case, whether we use ρ^{T_A} or ρ^{T_B} is immaterial as their eigenvalues are the same

Peres-Horodecki Criterion

- Let's use the Peres-Horodecki Criterion to analyze a state which is diagonal in the Bell basis, i.e.,

$$\rho = p_1 \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + p_2 \left|\Phi^-\right\rangle\left\langle\Phi^-\right| + p_3 \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + p_4 \left|\Psi^-\right\rangle\left\langle\Psi^-\right|$$

- This state is described by 3 real parameters, since tr(ρ)=1
- The Werner state, which was introduced previously, is a special case given by

$$\rho_W = F\left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left(\frac{1-F}{3}\right)\left|\Phi^-\right\rangle\left\langle\Phi^-\right| + \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right|$$

- Let’s begin our analysis by calculating the outer products of the Bell states

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\phi^+\rangle\langle\phi^+| = \frac{1}{2}\left(|00\rangle + |11\rangle\right)\left(\langle 00| + \langle 11|\right)$$

$$= \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right)$$

$$|\phi^+\rangle\langle\phi^+| = \begin{array}{c c} & \begin{array}{cccc} 00 & 01 & 10 & 11 \end{array} \\ \begin{array}{c} 00 \\ 01 \\ 10 \\ 11 \end{array} & \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\phi^-\rangle\langle\phi^-| = \frac{1}{2}\left(|00\rangle - |11\rangle\right)\left(\langle 00| - \langle 11|\right) = \frac{1}{2}\left(|00\rangle\langle 00| - |00\rangle\langle 11| - |11\rangle\langle 00| + |11\rangle\langle 11|\right)$$

$$|\phi^-\rangle\langle\phi^-| = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}$$

L2

$$|\psi^+\rangle \doteq \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\psi^+\rangle\langle\psi^+| = \frac{1}{2}\left(|01\rangle + |10\rangle\right)\left(\langle 01| + \langle 10|\right) = \frac{1}{2}\left(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|\right)$$

$$|\psi^+\rangle\langle\psi^+| = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

$$|\psi^-\rangle\langle\psi^-| = \frac{1}{2}\left(|01\rangle - |10\rangle\right)\left(\langle 01| - \langle 10|\right) = \frac{1}{2}\left(|01\rangle\langle 01| - |01\rangle\langle 10| - |10\rangle\langle 01| + |10\rangle\langle 10|\right)$$

$$|\psi^-\rangle\langle\psi^-| = \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

3

$$= P_1 |\phi^+\rangle\langle\phi^+| + P_2 |\phi^-\rangle\langle\phi^-| + P_3 |\psi^+\rangle\langle\psi^+| + P_4 |\psi^-\rangle\langle\psi^-|$$

$$= \frac{1}{2}\begin{bmatrix} P_1 & 0 & 0 & P_1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ P_1 & 0 & 0 & P_1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} P_2 & 0 & 0 & -P_2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -P_2 & 0 & 0 & P_2 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & P_3 & P_3 & 0 \\ 0 & P_3 & P_3 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$+ \frac{1}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & P_4 & -P_4 & 0 \\ 0 & -P_4 & P_4 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} P_1+P_2 & 0 & 0 & P_1-P_2 \\ 0 & P_3+P_4 & P_3-P_4 & 0 \\ 0 & P_3-P_4 & P_3+P_4 & 0 \\ P_1-P_2 & 0 & 0 & P_1+P_2 \end{bmatrix}$$

$$\rho_W = \frac{1}{2}\Big[(P_1+P_2)|00\rangle\langle 00| + (P_1-P_2)|00\rangle\langle 11|$$
$$+ (P_3+P_4)|01\rangle\langle 01| + (P_3-P_4)|01\rangle\langle 10|$$
$$+ (P_3-P_4)|10\rangle\langle 01| + (P_3+P_4)|10\rangle\langle 10|$$
$$+ (P_1-P_2)|11\rangle\langle 00| + (P_1+P_2)|11\rangle\langle 11| \Big]$$

$$\rho_W^{T_B} = \frac{1}{2}\Big[(P_1+P_2)|00\rangle\langle 00| + (P_1-P_2)|01\rangle\langle 10|$$
$$+ (P_3+P_4)|01\rangle\langle 01| + (P_3-P_4)|00\rangle\langle 11|$$
$$+ (P_3-P_4)|11\rangle\langle 00| + (P_3+P_4)|10\rangle\langle 10|$$
$$+ (P_1-P_2)|10\rangle\langle 01| + (P_1+P_2)|11\rangle\langle 11| \Big]$$

$$\rho_W^{T_B} = \frac{1}{2}\begin{bmatrix} P_1+P_2 & 0 & 0 & P_3-P_4 \\ 0 & P_3+P_4 & P_1-P_2 & 0 \\ 0 & P_1-P_2 & P_3+P_4 & 0 \\ P_3-P_4 & 0 & 0 & P_1+P_2 \end{bmatrix}$$

Let's instantiate ρ_W^T into the Werner state

$$P_1 = F \qquad P_2 = P_3 = P_4 = \frac{1-F}{3}$$

$$P_1 + P_2 = F + \frac{1-F}{3} = \frac{3F + 1 - F}{3} = \frac{2F+1}{3}$$

$$P_1 - P_2 = F - \frac{1-F}{3} = \frac{3F - 1 + F}{3} = \frac{4F-1}{3}$$

$$P_3 + P_4 = 2\,\frac{1-F}{3}$$

$$P_3 - P_4 = 0$$

$$\rho_W^{T_B} = \frac{1}{2}\begin{bmatrix} \frac{2F+1}{3} & 0 & 0 & 0 \\ 0 & 2\,\frac{1-F}{3} & \frac{4F-1}{3} & 0 \\ 0 & \frac{4F-1}{3} & 2\,\frac{1-F}{3} & 0 \\ 0 & 0 & 0 & \frac{2F+1}{3} \end{bmatrix}$$

$$\rho_W^{T_B} = \begin{bmatrix} \frac{2F+1}{6} & 0 & 0 & 0 \\ 0 & \frac{1-F}{3} & \frac{4F-1}{6} & 0 \\ 0 & \frac{4F-1}{6} & \frac{1-F}{3} & 0 \\ 0 & 0 & 0 & \frac{2F+1}{6} \end{bmatrix}$$

$$\det\left(\rho_W^{T} - \lambda I\right) = \begin{bmatrix} \frac{2F+1}{6} - \lambda & 0 & 0 & 0 \\ 0 & \frac{1-F}{3} - \lambda & \frac{4F-1}{6} & 0 \\ 0 & \frac{4F-1}{6} & \frac{1-F}{3} - \lambda & 0 \\ 0 & 0 & 0 & \frac{2F+1}{6} - \lambda \end{bmatrix} = 0$$

$$= \left(\frac{2F+1}{6} - \lambda\right) \begin{vmatrix} \frac{1-F}{3} - \lambda & \frac{4F-1}{6} & 0 \\ \frac{4F-1}{6} & \frac{1-F}{3} - \lambda & 0 \\ 0 & 0 & \frac{2F+1}{6} - \lambda \end{vmatrix}$$

$$= \left(\frac{2F+1}{6} - \lambda\right)^2 \begin{vmatrix} \frac{1-F}{3} - \lambda & \frac{4F-1}{6} \\ \frac{4F-1}{6} & \frac{1-F}{3} - \lambda \end{vmatrix}$$

$$= \left(\frac{2F+1}{6} - \lambda\right)^2 \left[\left(\frac{1-F}{3} - \lambda\right)^2 - \left(\frac{4F-1}{6}\right)^2\right] = 0$$

$$\frac{2F+1}{6} - \lambda = 0$$

$$\left[\left(\frac{1-F}{3} - \lambda\right) - \left(\frac{4F-1}{6}\right)\right]\left[\left(\frac{1-F}{3} - \lambda\right) + \left(\frac{4F-1}{6}\right)\right] = 0$$

$$\begin{cases} \lambda = \dfrac{2F+1}{6} \\[2ex] \dfrac{1-F}{3} - \lambda = \dfrac{4F-1}{6} \\[2ex] \dfrac{1-F}{3} - \lambda = -\dfrac{4F-1}{6} \end{cases} \qquad \begin{cases} \lambda_{1,2} = \dfrac{2F+1}{6} \\[2ex] \lambda_3 = \dfrac{1-2F}{2} \\[2ex] \lambda_4 = \dfrac{1+2F}{6} \end{cases}$$

Il minimo autovalore è $\lambda_3 = \dfrac{1-2F}{2}$

Perciò ρ_w è separabile se $\lambda_3 \geq 0 \Rightarrow \dfrac{1-2F}{3} \geq 0 \Rightarrow \boxed{F \leq \frac{1}{2}}$

Per $\frac{1}{2} < F \leq 1$, ρ_w è entangled

Example

Consider this 2-qubit family of Werner states:

$$\rho = p|\Psi^-\rangle\langle\Psi^-| + (1-p)\frac{I}{4}$$

It can be regarded as the convex combination of $|\Psi^-\rangle$, a maximally entangled state, and the identity element, a maximally mixed state.

Its density matrix is

$$\rho = \frac{1}{4}\begin{pmatrix} 1-p & 0 & 0 & 0 \\ 0 & p+1 & -2p & 0 \\ 0 & -2p & p+1 & 0 \\ 0 & 0 & 0 & 1-p \end{pmatrix}$$

and the partial transpose

$$\rho^{T_B} = \frac{1}{4}\begin{pmatrix} 1-p & 0 & 0 & -2p \\ 0 & p+1 & 0 & 0 \\ 0 & 0 & p+1 & 0 \\ -2p & 0 & 0 & 1-p \end{pmatrix}$$

Its least eigenvalue is $(1-3p)/4$. Therefore, the state is entangled for $1 \geq p > 1/3$.