Superdense Coding

Monday, April 5, 2021 8:37 AM

Recall: Entropy

Given 7-bit msg:

$S: \quad b_1 \; b_2 \; b_3 \; \cdots \; b_7 \quad , \; b_i \in \{0,1\}$

$$H_S = \sum_x Prob(x) \cdot \log_2\left(\frac{1}{Prob(x)}\right)$$

$$= \frac{1}{128} \cdot \log_2(128) + \frac{1}{128} \cdot \log_2(128) + \cdots + \frac{1}{128} \cdot \log_2(128)$$

$$= 128 \left| \frac{1}{128} \cdot \log_2(128) \right|$$

$$= \log_2(128) = 7 \text{ bits}$$

Recall: Diffie-Hellman key Exchange Protocol

① Based on D-Log problem

② Used to exchange a key (in public)

1] e.g. The Entropy of 2-bits is the amount of information in a 2-bit message.

① if Alice wants to send the outcome of a die to Bob. Can she code it using 2-bits?

Classically, No. Because we have 6 possible

Classically, No. Because we have 6 possible values, and the entropy is $H = \log_2(6) = 2.58$ bits

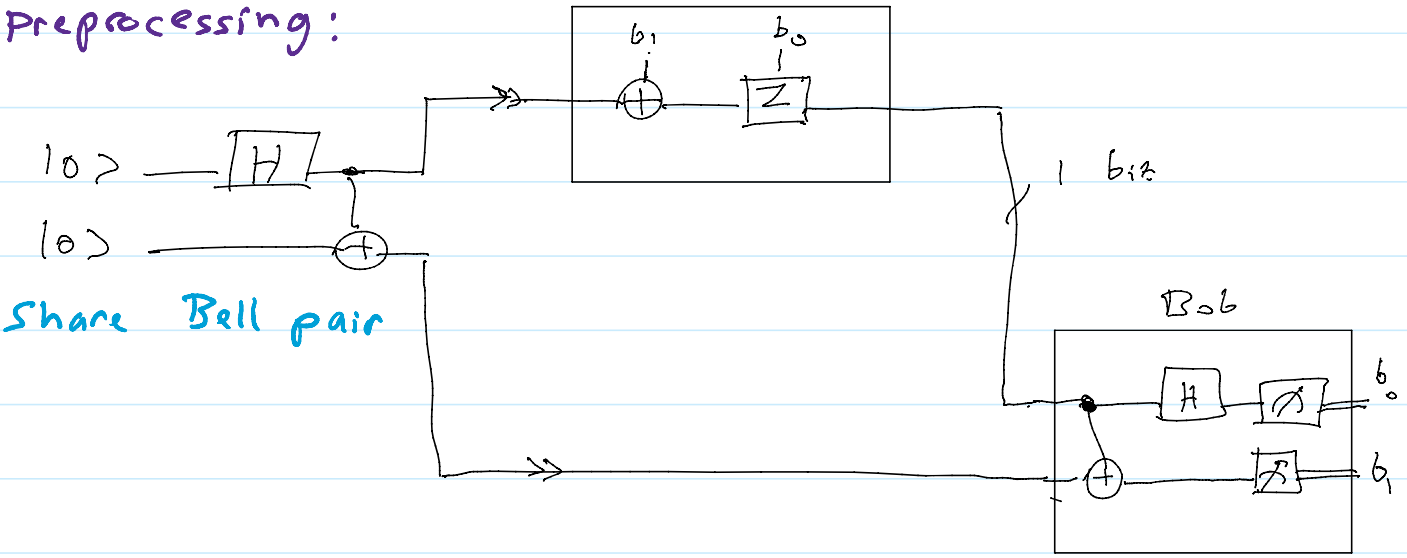
Using Quantum bits, Yes. By superdense coding.

2] Superdense Coding:

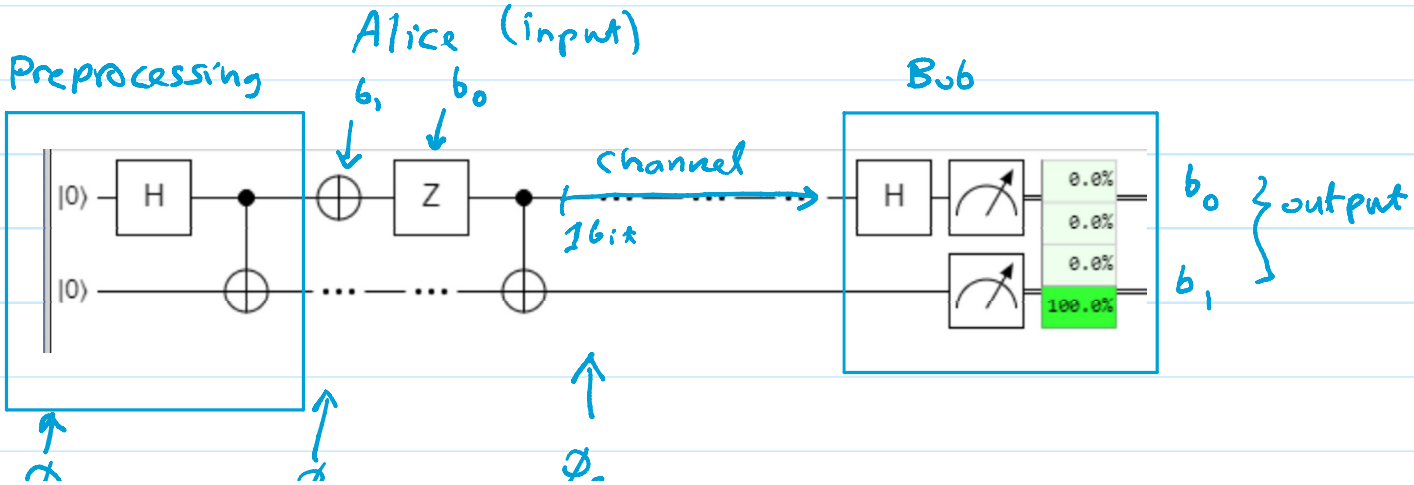
A protocol to send 2 classical bits of information from Alice to Bob using one qubit.

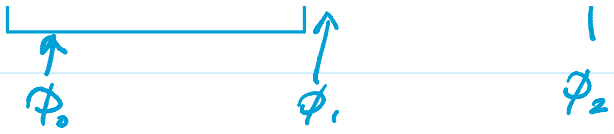
Alice $(b_1\ b_0)$ $\{00, 01, 10, 11\}$

Preprocessing:



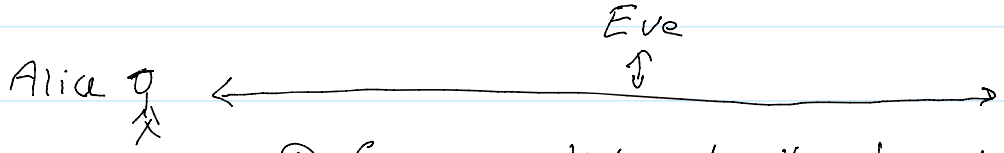
3] Implementation on Quick





4] Quantum Key Exchange:

① Classical Channel:

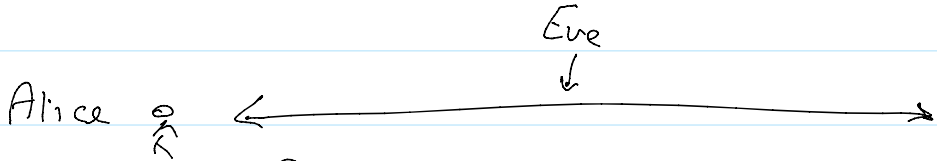


① Eve can listen to the channel "stealthy"

② She can copy all information (ciphertext, keys, plaintext)

Diffie-Hellman KE protocol uses D-Log problem to secure the key.

② Quantum Channel:



① Measuring the qubit-stream alters it.

② No-Cloning theorem: Eve cannot copy the qubit-stream.

Bennett-Brassard (in 1984): BB84 Protocol