Quantum Computing Course

Sugata Gangopadhyay, Abhishek Chakraborty, C. A. Jothishwaran

Department of Computer Science and Engineering

Indian Institute of Technology Roorkee

Module 4

Lecture 1: Quantum Key Distribution

- BB84

Key Distribution

- Keys
    - binary strings of numbers chosen randomly from a sufficiently large set
    - Provide the security for most cryptographic protocols, from encryption to authentication to secret sharing.
- The establishment of keys between the parties who wish to communicate is of fundamental importance in cryptography.

Classes of keys

x Sender | x Receiver

- Symmetric keys
  - A symmetric-key cryptosystem consist of a single key that is known to all legitimate users and no one else.

- Asymmetric keys
  - An asymmetric-key cryptosystem consists of keys that have two parts, public and private. The public key can be shared openly whereas the private key or the secret key need to be kept secret.

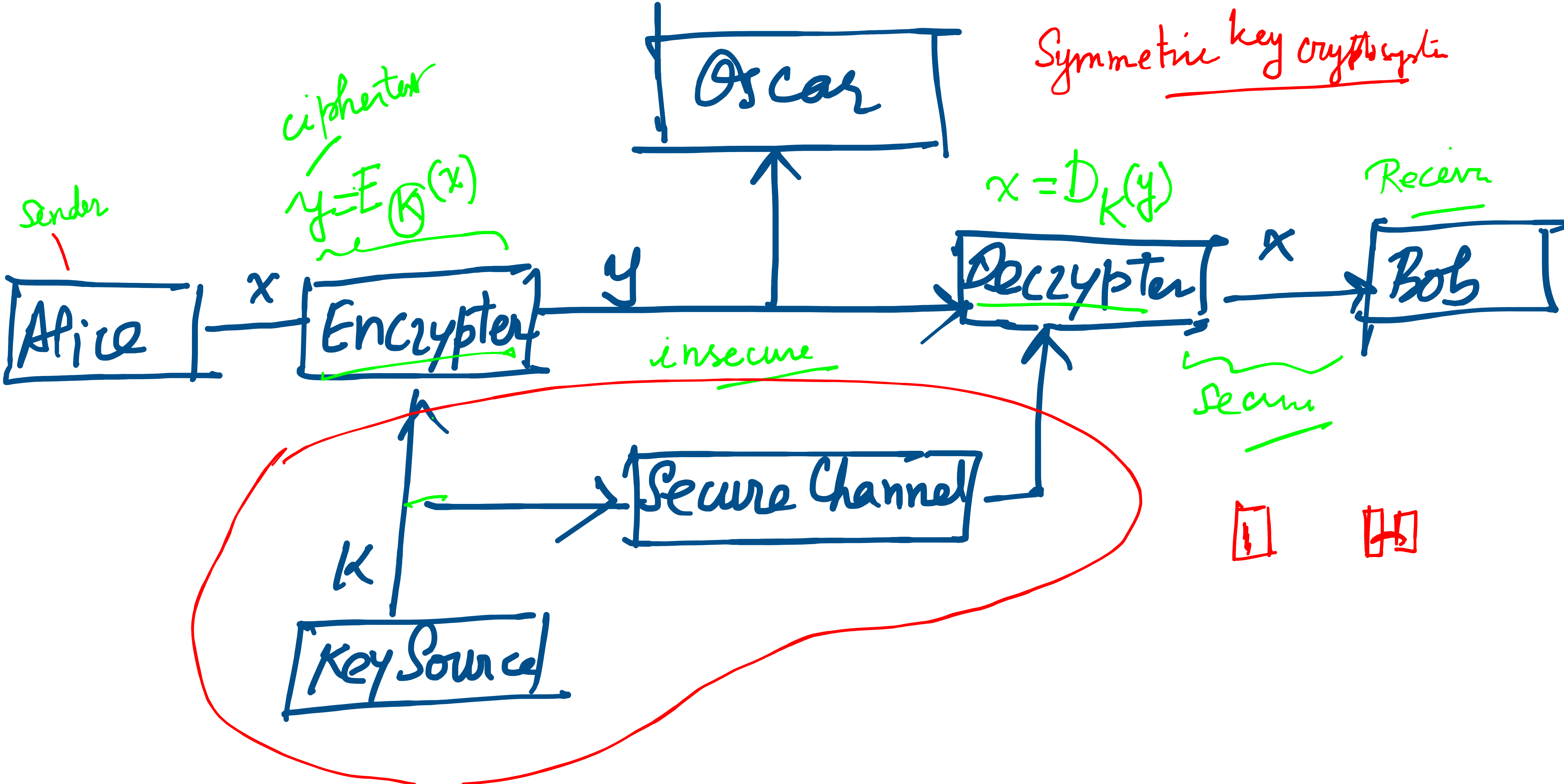
Public key

$E_K \rightarrow$ knowledge

$D_K \rightarrow$ does not give an idea of D_K.

sends $E_K(x)$ → Receiver

The communication Channel



QKD

Quantum key distribution protocol

- Quantum key distribution protocols establish symmetric key between two parties.

- As a convention we call the sender Alice and the receiver Bob.

Both the channels are public, insecure.

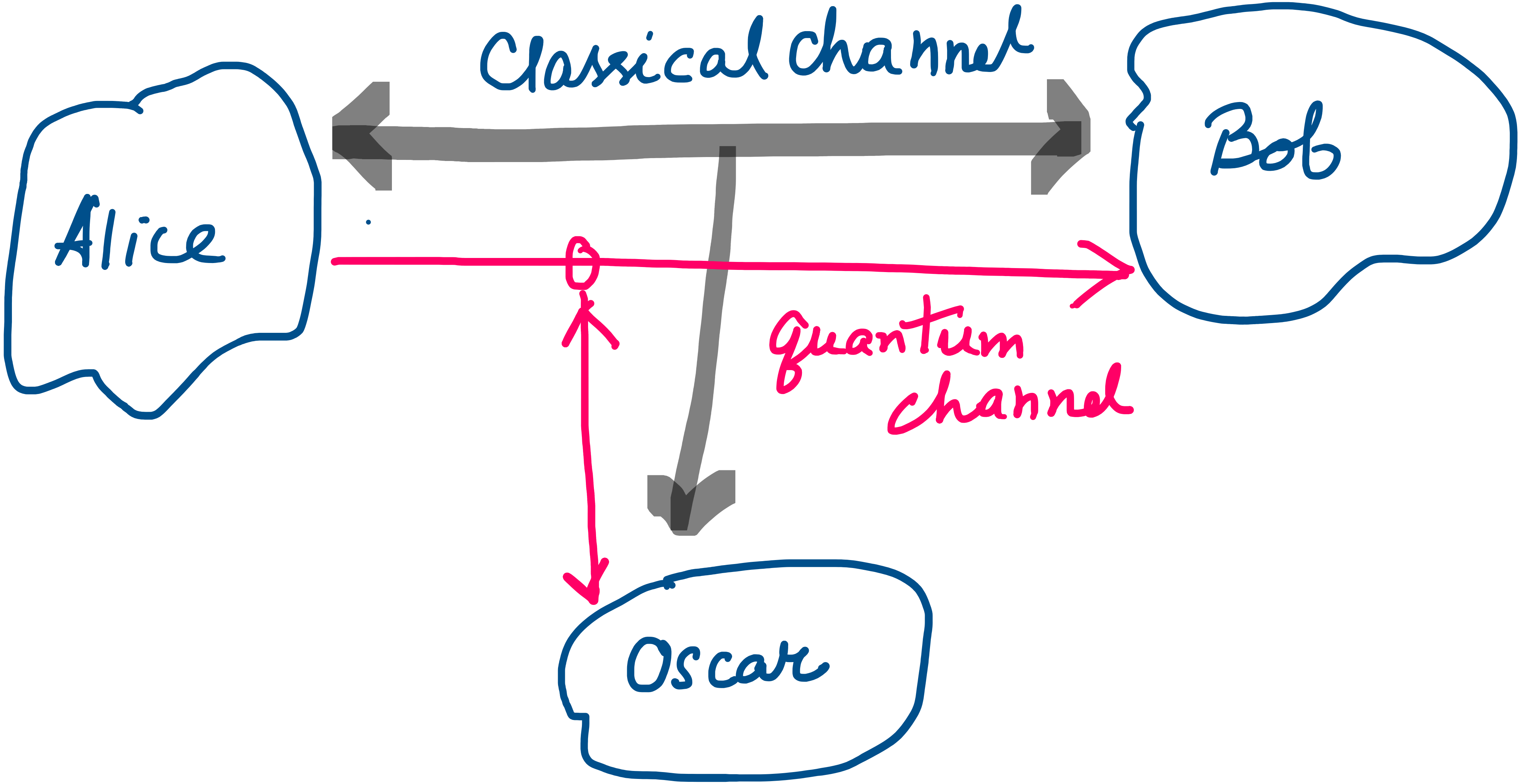
- The attacker or the adversary is call Oscar.

quantum channel

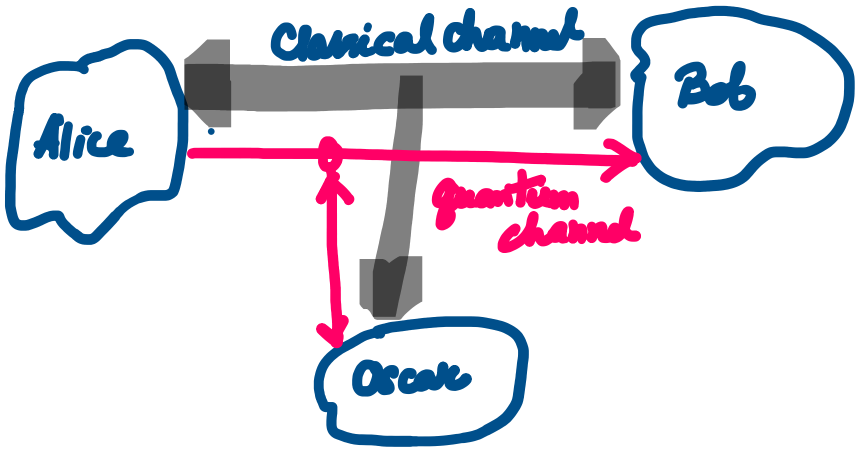
Alice → Bob

channel

A quantum key distribution protocol: BB84



BB84



- Encoding using the standard basis

$$\boxed{\begin{array}{l} \bullet\ 0 \to |0\rangle \\ \bullet\ 1 \to |1\rangle \end{array}}$$

$$\left.\begin{array}{l} 0 \mapsto |0\rangle \\ 1 \mapsto |1\rangle \end{array}\right\}$$

- Encoding using the Hadamard basis

  - $0 \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $1 \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$\begin{array}{l} 0 \mapsto |+\rangle \\ 1 \mapsto |-\rangle \end{array}$$

After this they do whatever they mean.

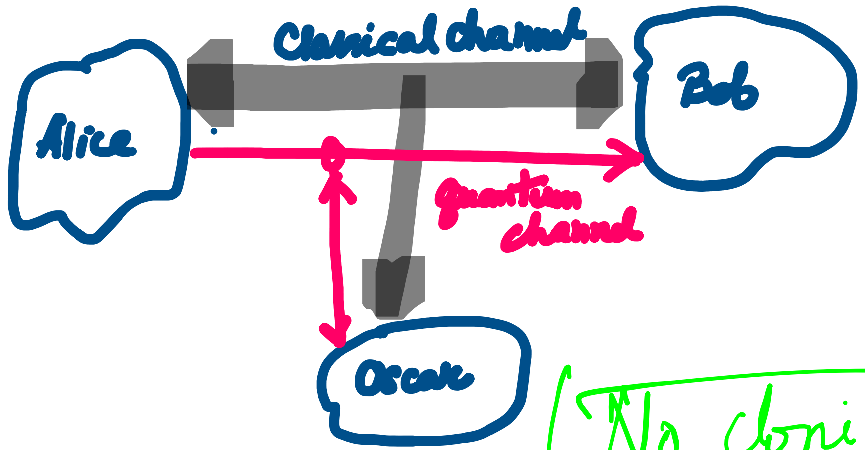
BB84

0 1 1 1 0 0

- Encoding using the standard basis
  - $0 \rightarrow |0\rangle$
  - $1 \rightarrow |1\rangle$

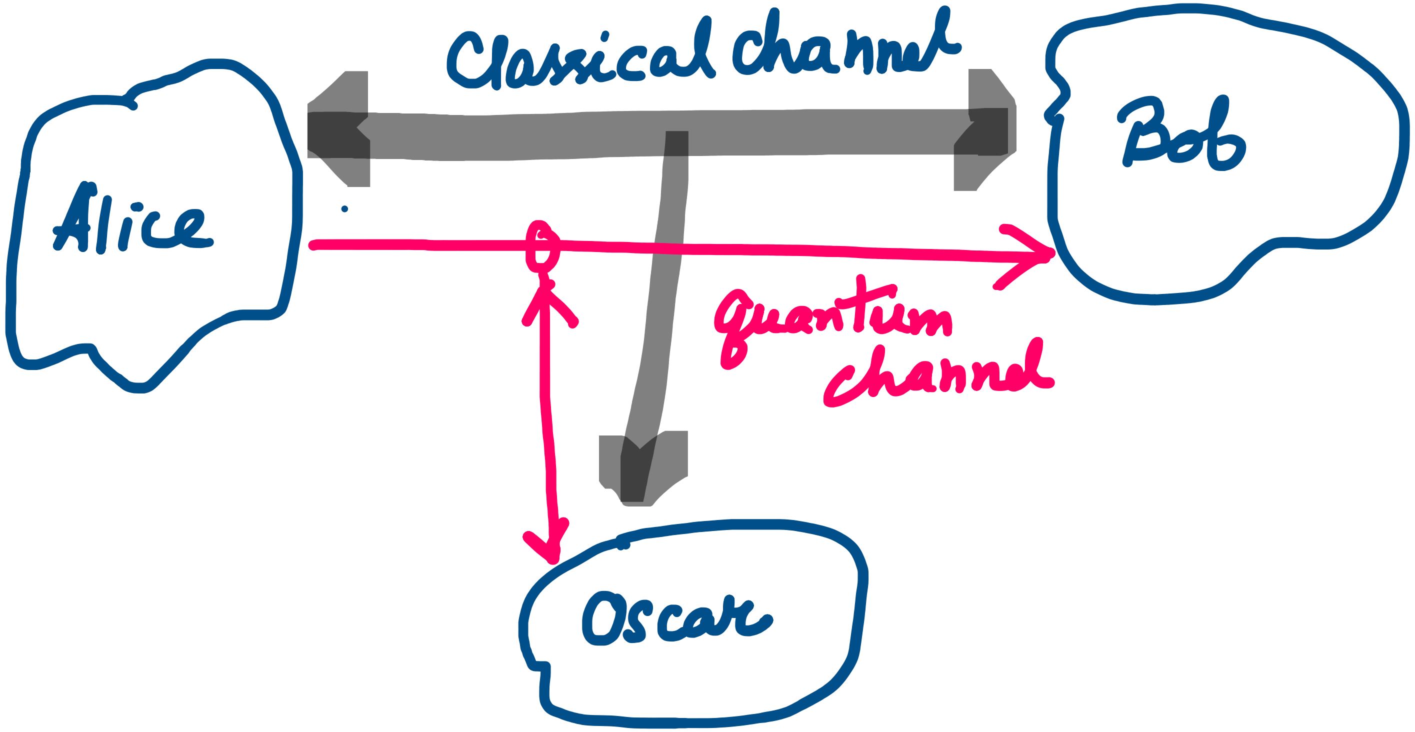
  } B_1
- Encoding using the Hadamard basis
  - $0 \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $1 \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

  } B_2



No cloning theorem

- Alice uses quantum or classical means to generate a random sequence of classical bit values
- Alice then randomly encodes each bit of this sequence in the polarization state of a photon by randomly choosing for each bit one of the following two agreed-upon bases in which to encode it.
- Bob measures the state of each photon he receives by randomly picking either basis.
- Over the classical channel Alice and Bob check that Bob has received a photon for every one Alice has sent.
- Then Alice and Bob tell each other the bases they used for encoding and decoding each bit.



- Encoding using the standard basis
  - $0 \rightarrow |0\rangle$
  - $1 \rightarrow |1\rangle$
- Encoding using the Hadamard basis
  - $0 \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $1 \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$