Quantum Computing Course

Sugata Gangopadhyay, Abhishek Chakraborty, C. A. Jothishwaran

Department of Computer Science and Engineering

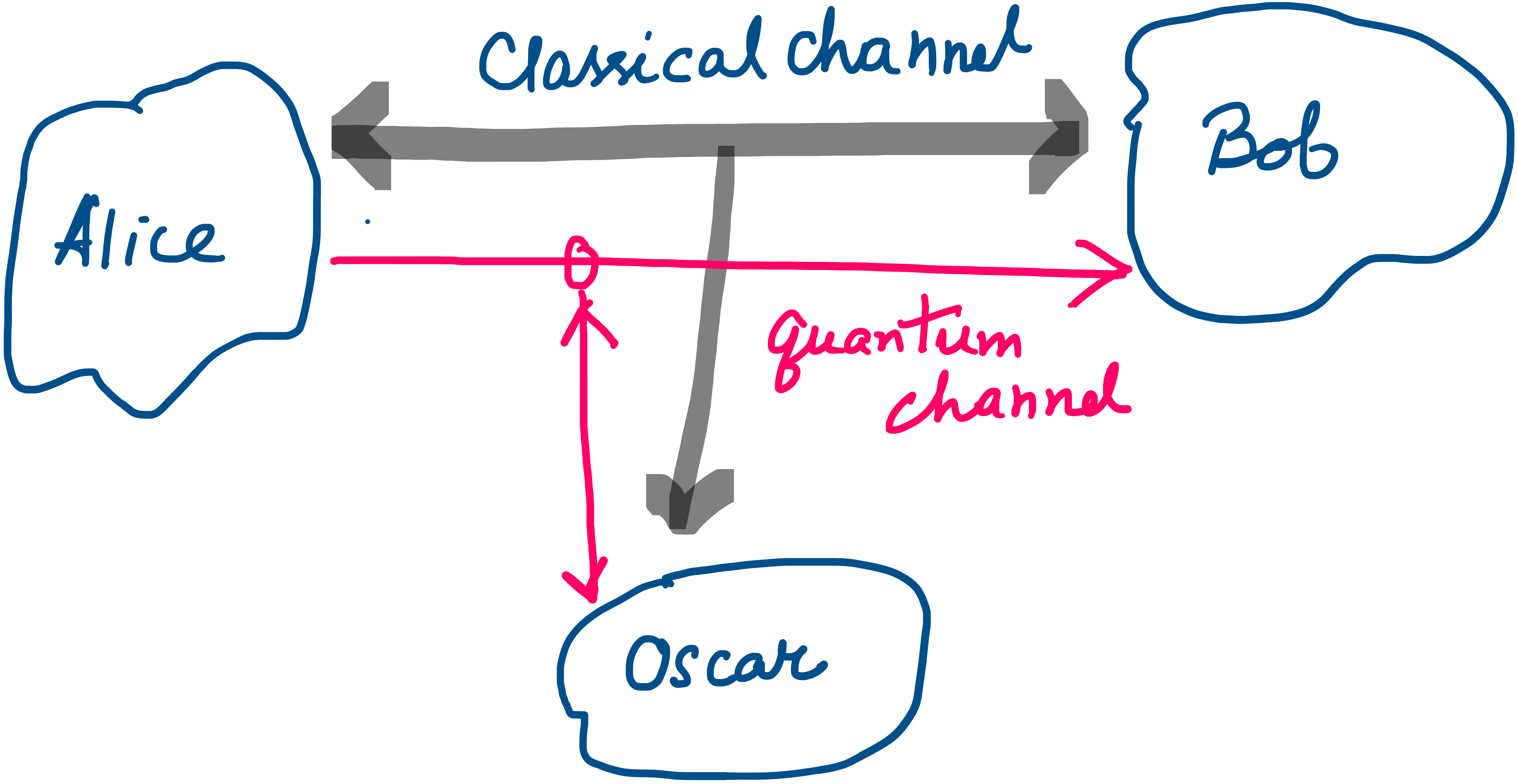
Indian Institute of Technology Roorkee

Module 4

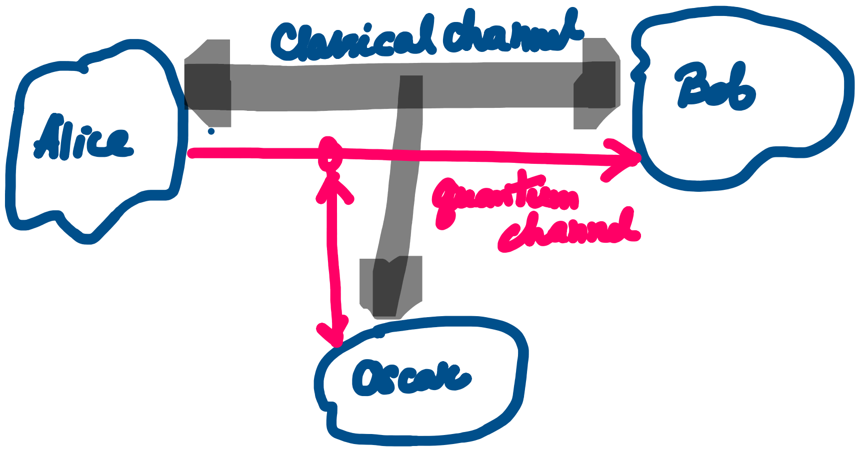
Lecture 2: Quantum Key Distribution

- BB84 in the presence of an eavesdropper
- Key distillation

A quantum key distribution protocol: BB84



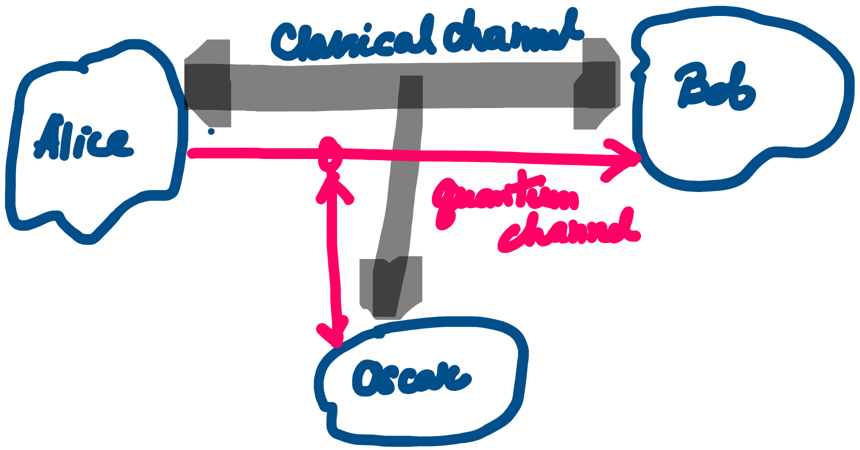
BB84



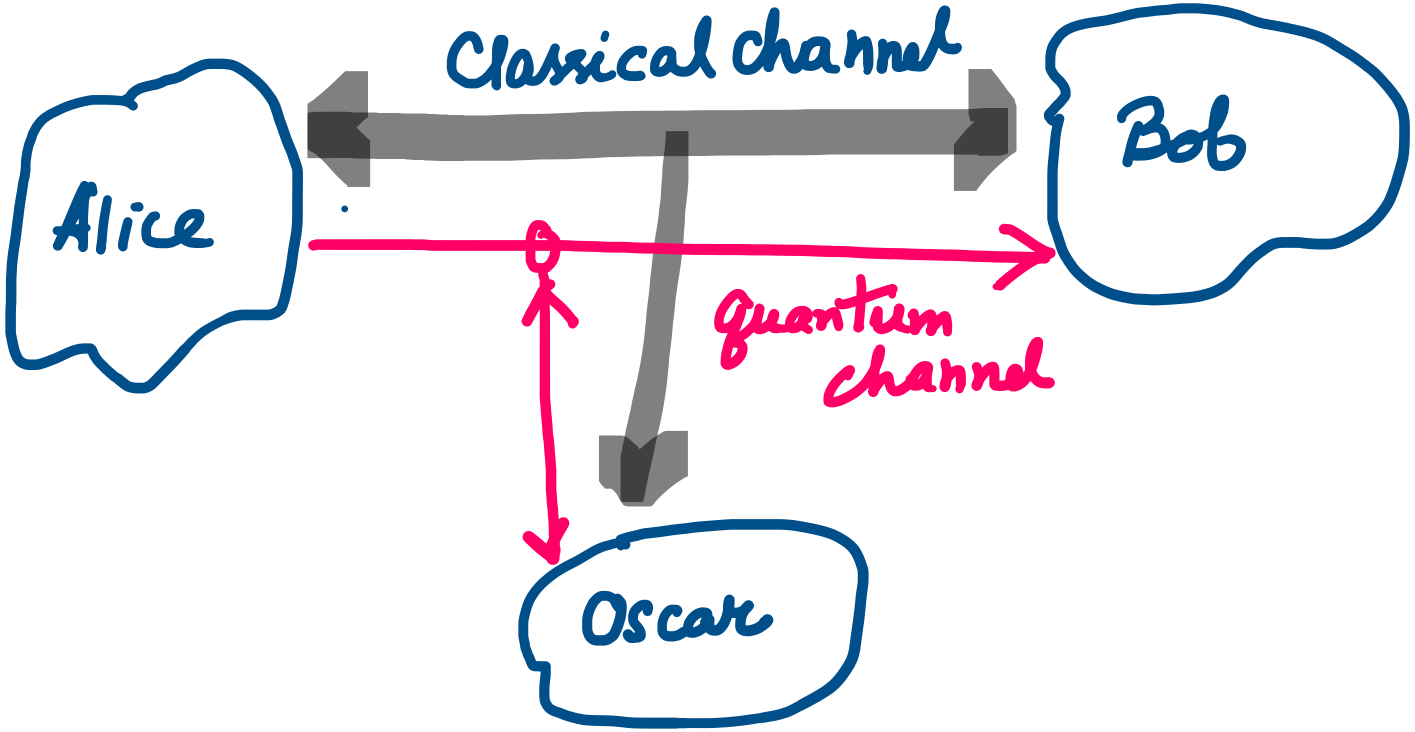
- Encoding using the standard basis
  - $0 \rightarrow |0\rangle$
  - $1 \rightarrow |1\rangle$
- Encoding using the Hadamard basis
  - $0 \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$
  - $1 \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

BB84

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



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

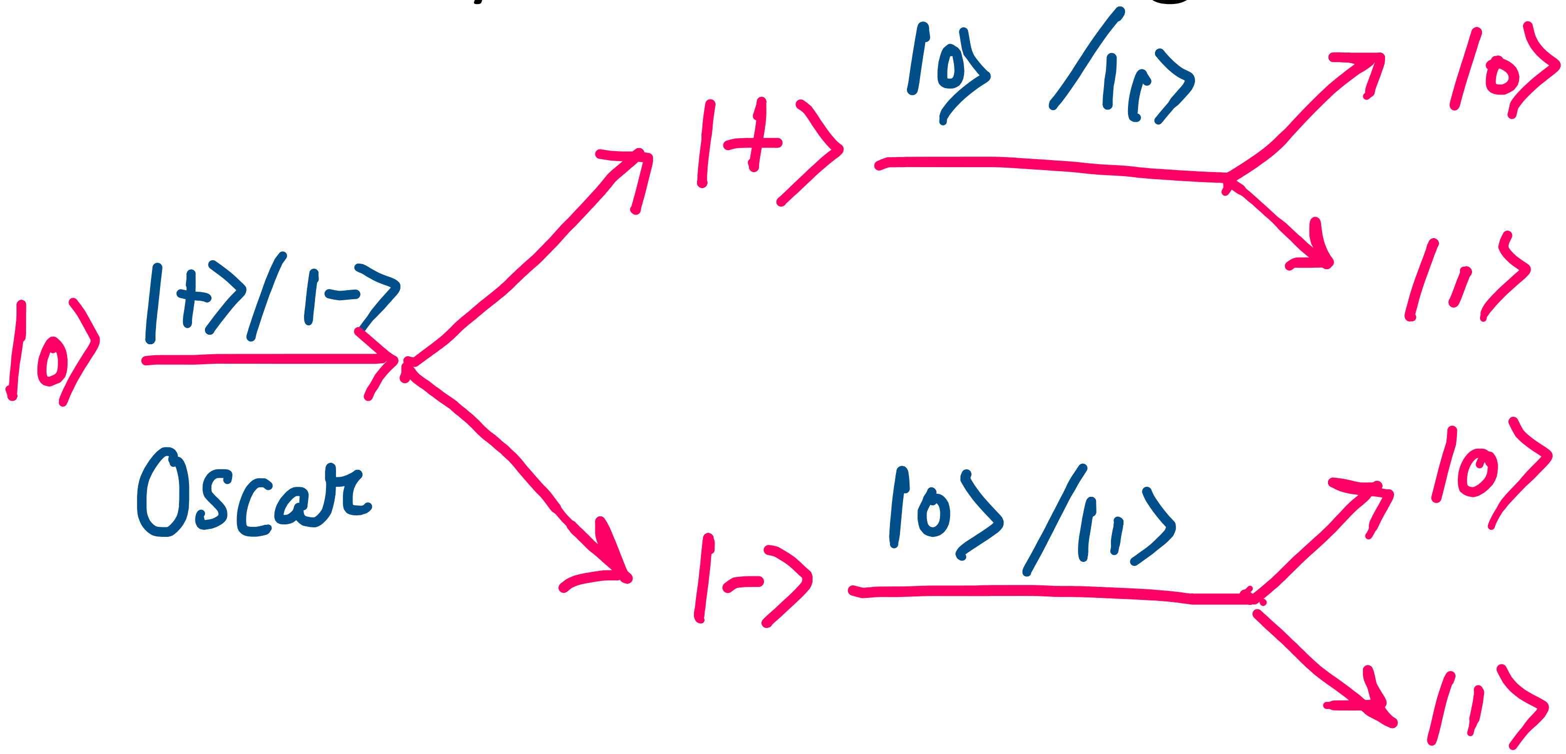
Key sifting

- After sending a long stream of key elements, Alice tells Bob which encoding rule she chose for each key element, and Bob is able to discard all the wrong elements.
- This part of the protocol is said to be sifting.
- It is assumed that all communications required to do the sifting are made over the classical authenticated channel. So the sifting process is not influenced by Oscar.

Detecting eavesdropping

- Suppose, by the way of attack, Oscar intercept a photon, measures it, and sends the photon resulting from the measurement to Bob.
    - Oscar has probability of $\frac{1}{2}$ of measuring with the correct basis.
    - When he does, he does not disturb the state and goes unnoticed.
    - When he measure in the wrong basis, he sends the wrong state to Bob.
    - With the wrong state, Bob will basically measure a random bit, which has a probability $\frac{1}{2}$ of matching Alice's bit an probability $\frac{1}{2}$ of being wrong.

Probability of introducing error



- So Oscar has a probability $\frac{1}{4}$ of introducing an error between Alice and Bob's bits.

Detecting eavesdropping

- Alice and Bob discloses a part of the sifted key.
  - A given protocol might specify that after a transmission of $\ell + n$ key elements numbered from 0 to $\ell + n - 1$, Alice randomly chooses n indices and communicates to Bob.
  - Alice and Bob then reveal the corresponding n key elements to count the number of errors.
  - Any error means that there was some eavesdropping.

- The absence of error gives some statistical confidence on the fact that there was no eavesdropping.

Distilling a secret key

- Alice and Bob count the number of errors in the disclosed key elements to obtain and estimate of the expected error factor e.

- From this they statistically estimate that Oscar knows no more than I_E bits on the ℓ key elements.

- Using the public classical authenticated channel Alice and Bob can still try to make a fully secret key. This is called key distillation.

Distilling a secret key

- Reconciliation
  - Alice and Bob discloses $|M|$ number of parity check bits.
  - Therefore Oscar has information on $I_E + |M|$ bits.
- Privacy amplification
  - Oscar has no information on $\ell - I_E - |M|$ bits.
  - This is done by a function $f: \{0,1\}^\ell \to \{0,1\}^m$ that spreads the ignorance of Oscar over the entire output.