Department of

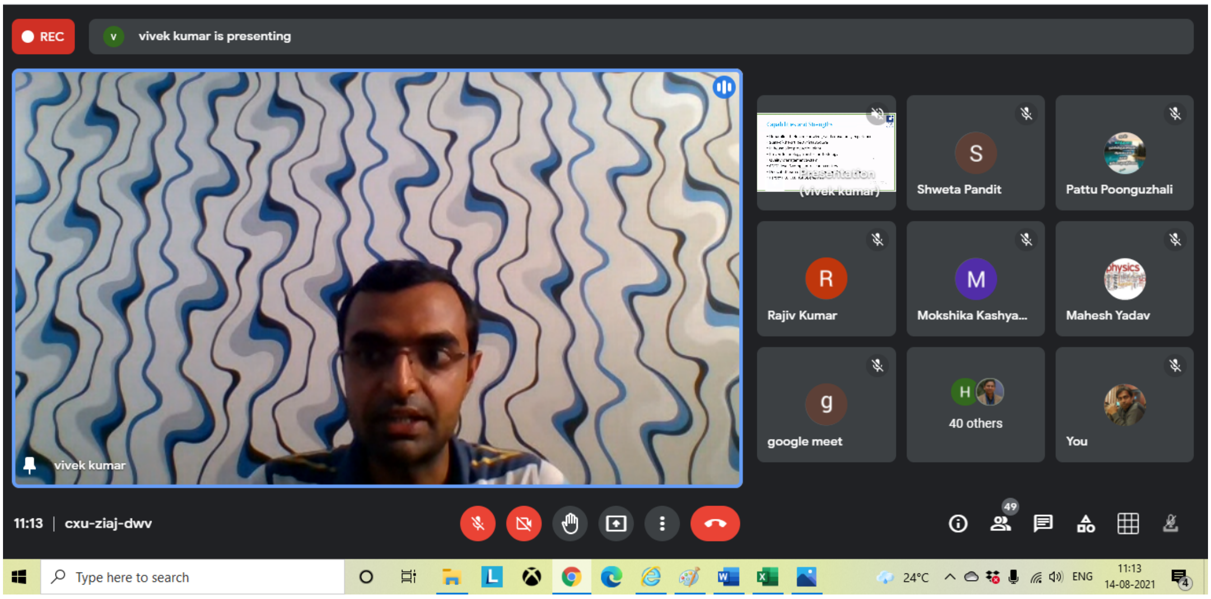
Electronics and Communication Engineering

Jaypee University of Information Technology Waknaghat

Event Report: Session-7

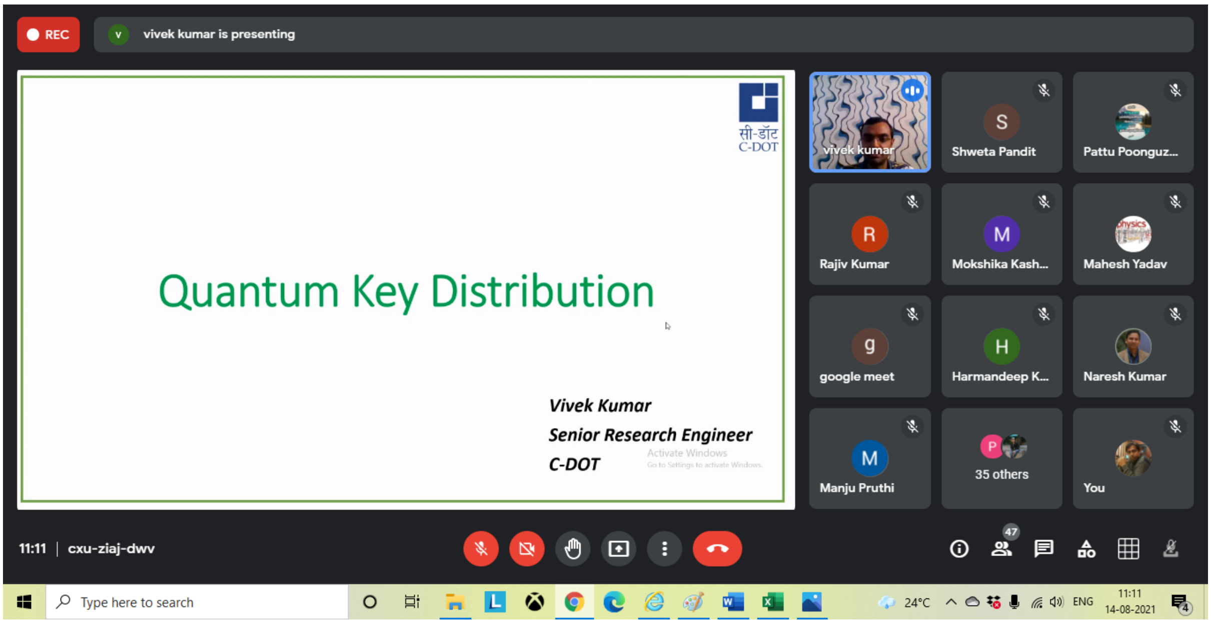
14th Aug, 2021

Department of Electronics and Communication Engineering of Jaypee University of Information Technology, Solan organized the sixth session of "Workshop on Industrial Revolution 4.0" on 14th Aug 2021. The topic of the seventh session was **Quantum key Distribution** and **Mr. Vivek Kumar, Senior Research Engineer, Centre for Development of Telematics (C-DOT)** was the honourable speaker.



Dr. Shweta Pandit, Assistant Professor in Department of Electronics and Communication Engineering welcomed and introduced the speaker. Our eminent speaker, Mr. Vivek Kumar has done his bachelors in Electronics and Telecommunication in 2009 and in the same year he cleared the GATE examination and opted for MTech in Optoelectronics and optical communication in IIT Delhi. After completing the MTech in 2011 he got selected as Research Engineer in C-DOT. He has spent the past ten years working in different optical technologies in C-DOT. His work was mainly related to PCB designing and network architecture conceptualization. Some of the major Projects he did in C-DOT are:

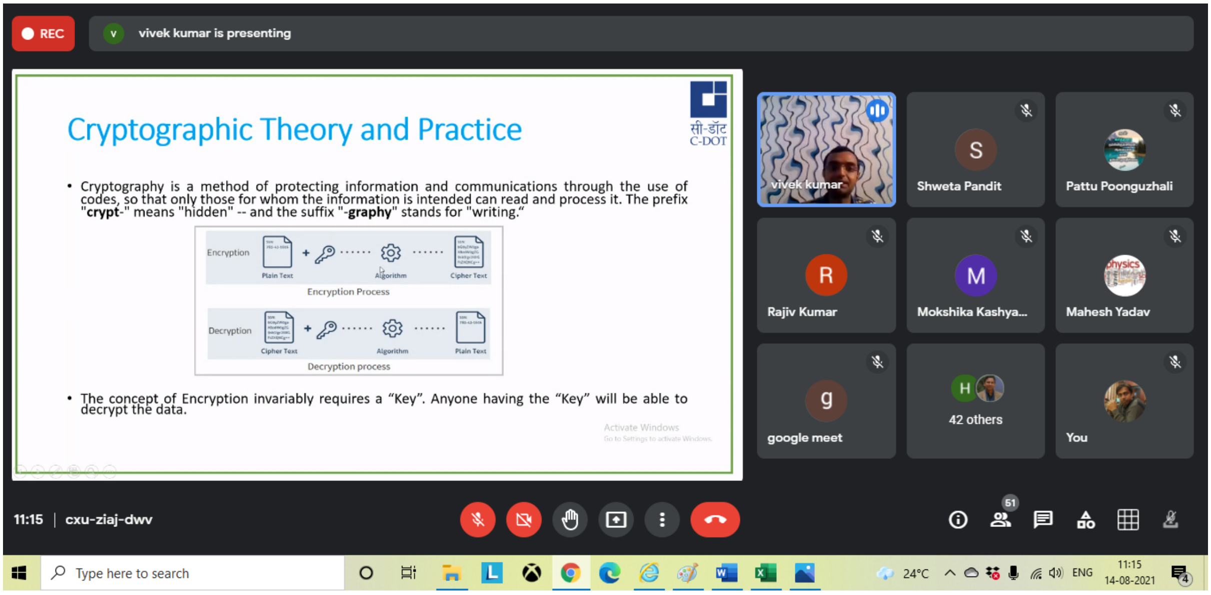
- GPON System: Gigabit Passive Optical Network
- FFLS System: Fibre Fault Localization system
- DWDM System: Dense wavelength division Multiplexing
- QKD System: Quantum Key Distribution



Quantum Key Distribution

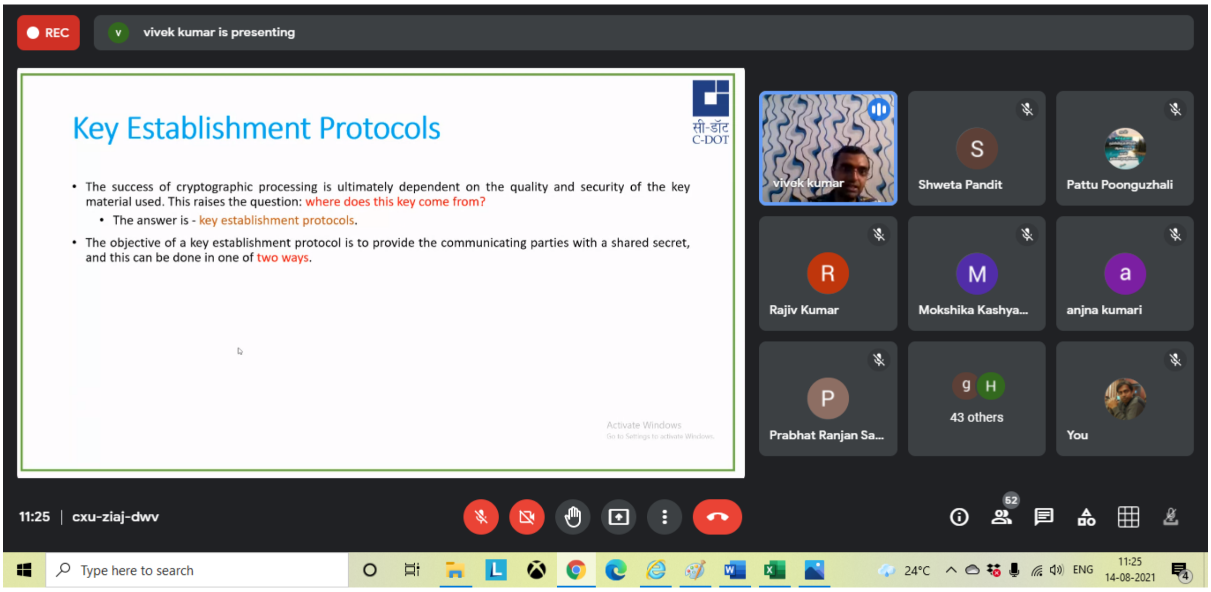
Vivek Kumar
Senior Research Engineer
C-DOT

Mr. Vivek started his lecture by introducing the C-DOT and the type of technologies on which C-DOT works. Coming to the main topic of the session, he first briefly described the requirement of security while designing any IoT system. He described the different security algorithms available and also gave an idea about the limitations of these security algorithms.



Cryptographic Theory and Practice

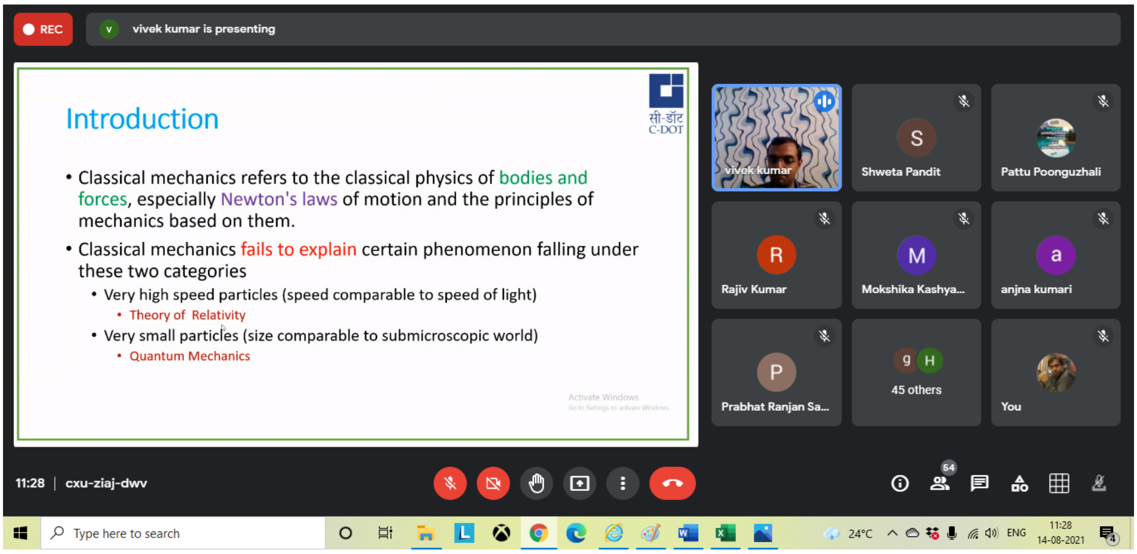
- Cryptography is a method of protecting information and communications through the use of codes, so that only those for whom the information is intended can read and process it. The prefix "**crypt**-" means "hidden" -- and the suffix "**-graphy**" stands for "writing.“
- The concept of Encryption invariably requires a “Key”. Anyone having the “Key” will be able to decrypt the data.



Key Establishment Protocols

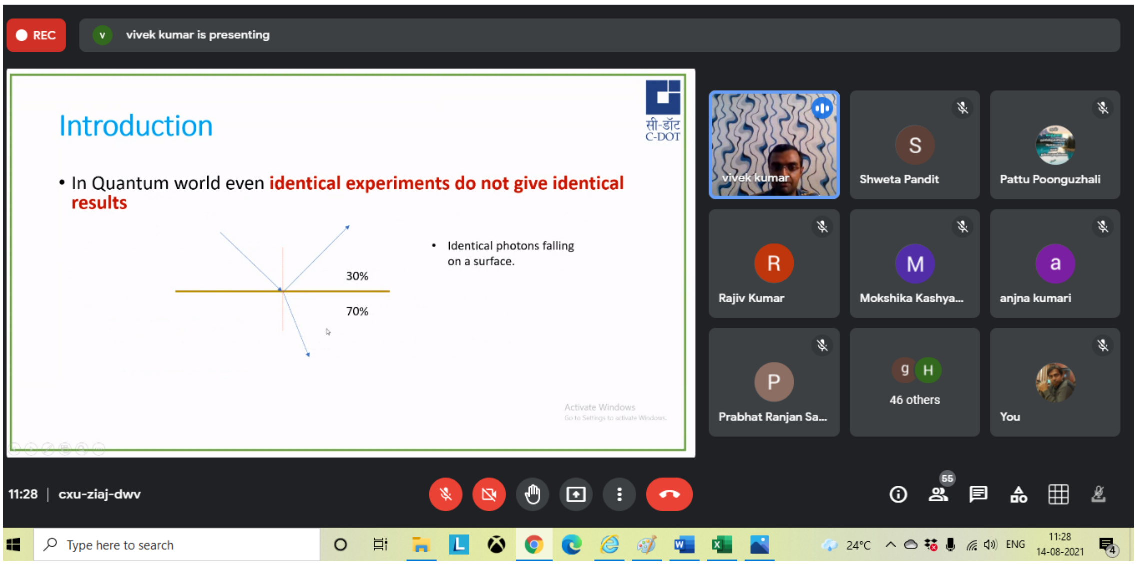
- The success of cryptographic processing is ultimately dependent on the quality and security of the key material used. This raises the question: where does this key come from?
  - The answer is - key establishment protocols.
- The objective of a key establishment protocol is to provide the communicating parties with a shared secret, and this can be done in one of two ways.

To start with the concept of Quantum key generation, he started with the basic difference between classical physics and Quantum theory. He then discussed basics and protocols of Quantum key Distribution (QKD).



Introduction

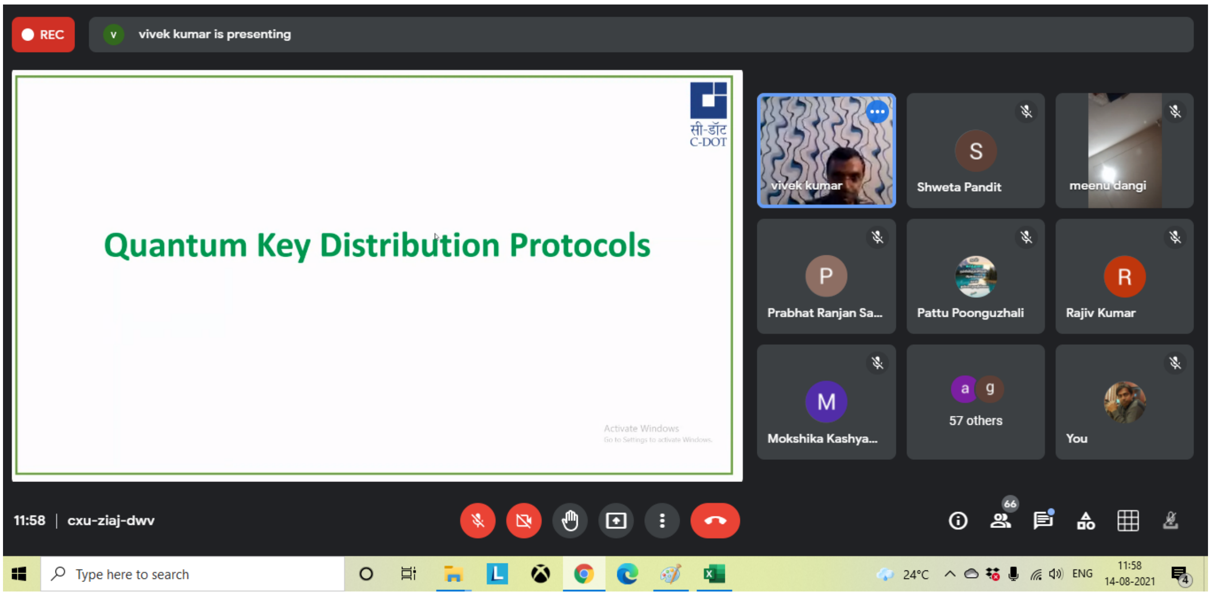
- Classical mechanics refers to the classical physics of bodies and forces, especially Newton's laws of motion and the principles of mechanics based on them.
- Classical mechanics fails to explain certain phenomenon falling under these two categories
  - Very high speed particles (speed comparable to speed of light)
    - Theory of Relativity
  - Very small particles (size comparable to submicroscopic world)
    - Quantum Mechanics



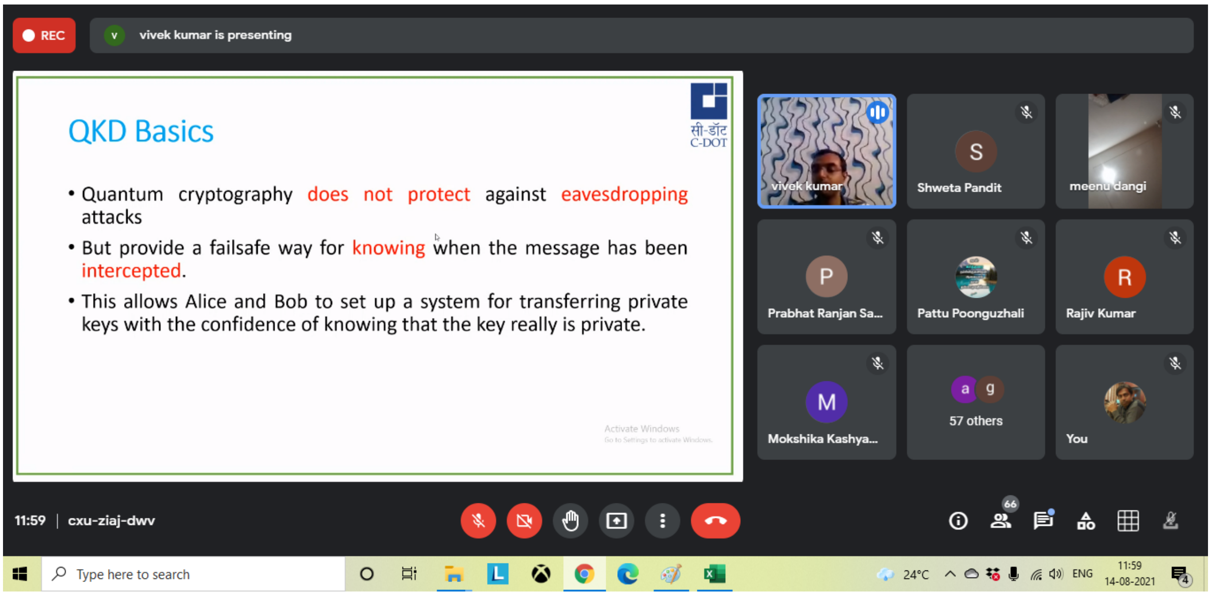
Introduction

- In Quantum world even **identical experiments do not give identical results**

- Identical photons falling on a surface.

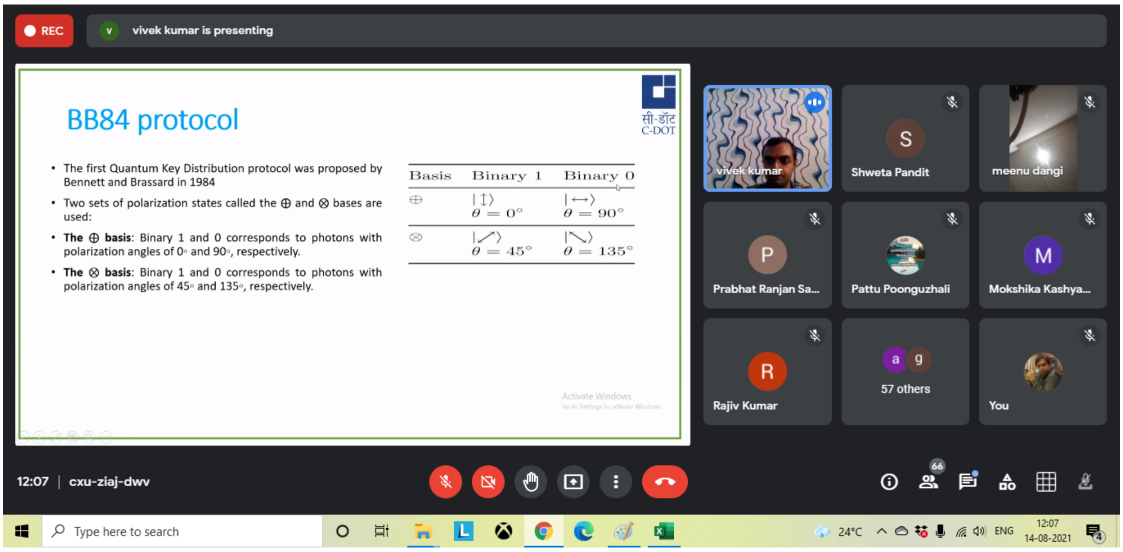


Quantum Key Distribution Protocols



QKD Basics

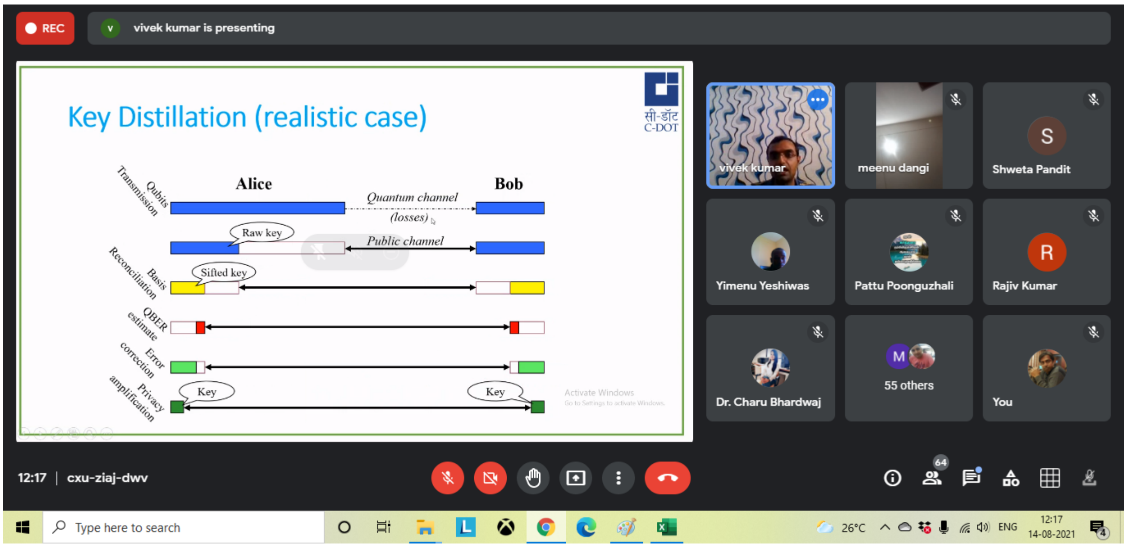
- Quantum cryptography does not protect against eavesdropping attacks
- But provide a failsafe way for knowing when the message has been intercepted.
- This allows Alice and Bob to set up a system for transferring private keys with the confidence of knowing that the key really is private.



BB84 protocol

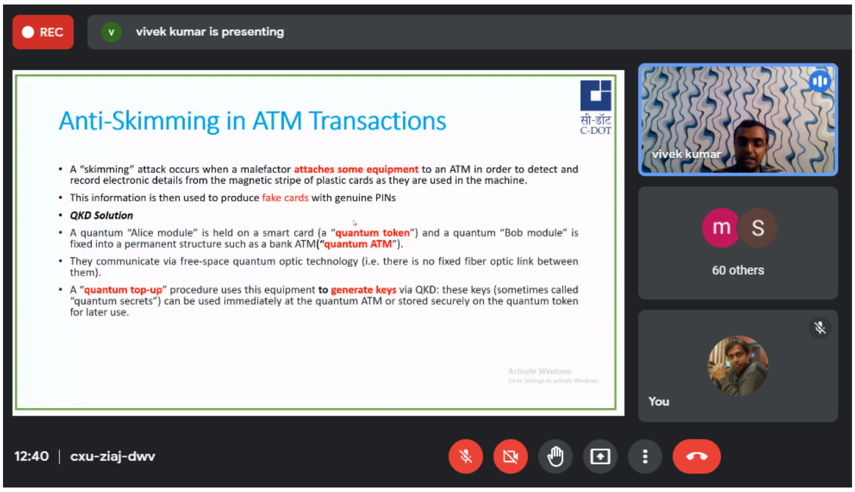
- The first Quantum Key Distribution protocol was proposed by Bennett and Brassard in 1984
- Two sets of polarization states called the ⊕ and ⊗ bases are used:
- **The ⊕ basis**: Binary 1 and 0 corresponds to photons with polarization angles of 0◦ and 90◦, respectively.
- **The ⊗ basis**: Binary 1 and 0 corresponds to photons with polarization angles of 45◦ and 135◦, respectively.

Basis	Binary 1	Binary 0
$\oplus$	$\lvert\updownarrow\rangle$ $\theta = 0^\circ$	$\lvert\leftrightarrow\rangle$ $\theta = 90^\circ$
$\otimes$	$\lvert\nearrow\rangle$ $\theta = 45^\circ$	$\lvert\searrow\rangle$ $\theta = 135^\circ$



Key Distillation (realistic case)

At the end of the presentation, he discussed various applications where QKD is used for providing security.



Anti-Skimming in ATM Transactions

- A "skimming" attack occurs when a malefactor **attaches some equipment** to an ATM in order to detect and record electronic details from the magnetic stripe of plastic cards as they are used in the machine.
- This information is then used to produce fake cards with genuine PINs
- ***QKD Solution***
- A quantum "Alice module" is held on a smart card (a "**quantum token**") and a quantum "Bob module" is fixed into a permanent structure such as a bank ATM(**"quantum ATM**").
- They communicate via free-space quantum optic technology (i.e. there is no fixed fiber optic link between them).
- A "**quantum top-up**" procedure uses this equipment **to generate keys** via QKD: these keys (sometimes called "quantum secrets") can be used immediately at the quantum ATM or stored securely on the quantum token for later use.

The session ends with the answers to the questions from the participants. Overall, the session gave an idea about the security algorithms with respect to Quantum keys.