MPC
Topic 2

GROUP 2

Sudip Datta(2021CSB006)
Prashanjit Pradip Basu(2021CSB010)
Sayantan Datta(2021CSB048)
Arnab Nath(2021CSB054)
Puyush(2021CSB111)

Cellular Networks

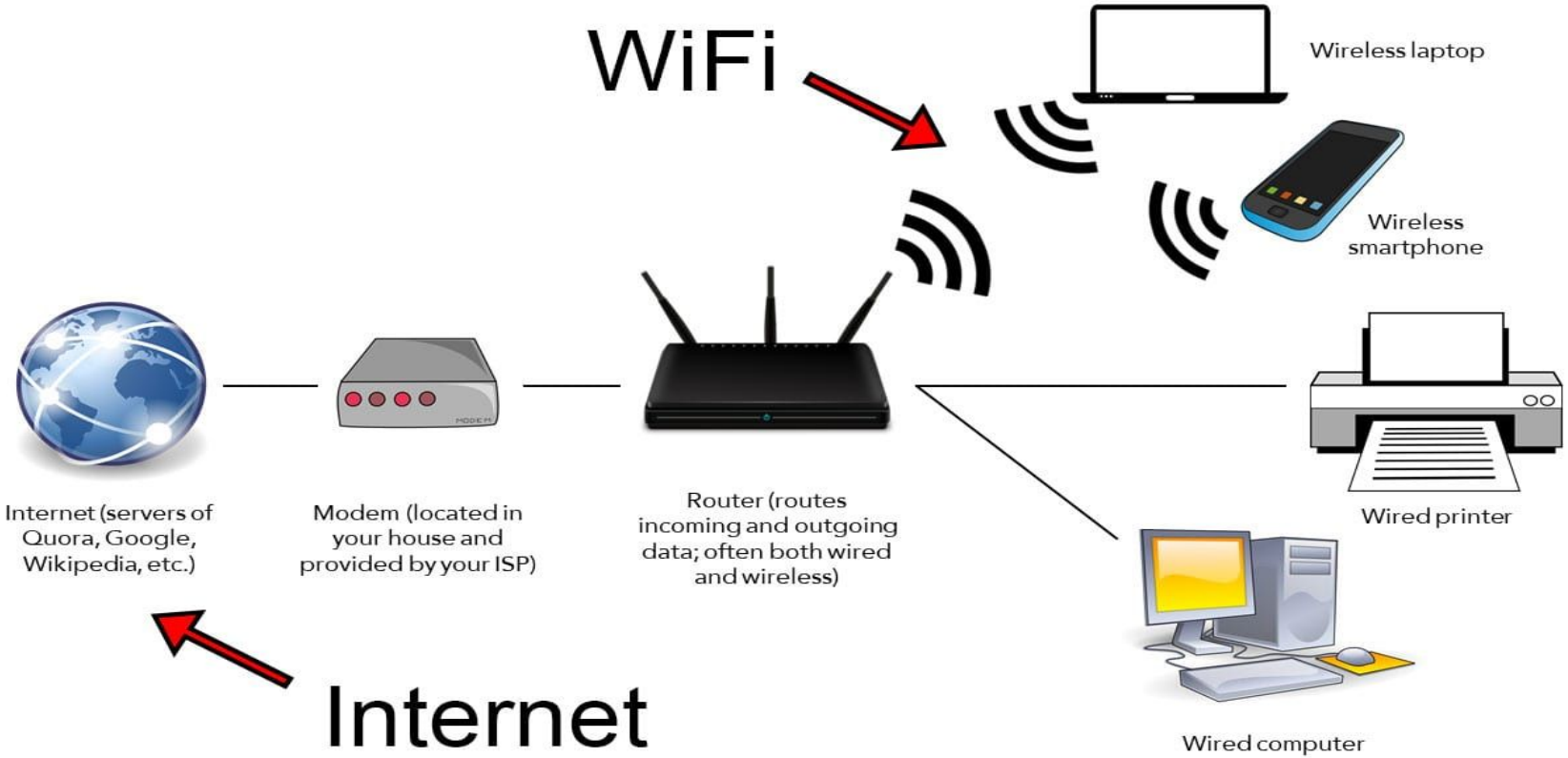
1. Mobile data creates a wireless connection by enabling devices to communicate through radio frequencies.
2. Data uploaded or downloaded via mobile network is broadcasted from or to a central cellular base station or microcell.
3. A single microcell can cover a broad geographical location and multiple cells can overlap to transmit data effectively.

Wifi Networks

1. Wifi is a signal that is used to connect to internet wirelessly.
2. Router is used to connect multiple users wirelessly through radio frequencies.
3. A computer's wireless adapter translate data into a radio signal and transmits it using an antenna.
4. Wireless router receives the signal and decodes it. It sends the information to the Internet using physical, wired connection.

Advantages : High speed data transfer with more reliability

Disadvantages : Limited range and extra hardware(router) needed


WiFi
Wireless laptop
Wireless smartphone
Internet (servers of Quora, Google, Wikipedia, etc.)
Modem (located in your house and provided by your ISP)
Router (routes incoming and outgoing data; often both wired and wireless)
Wired printer
Wired computer
Internet

Bluetooth

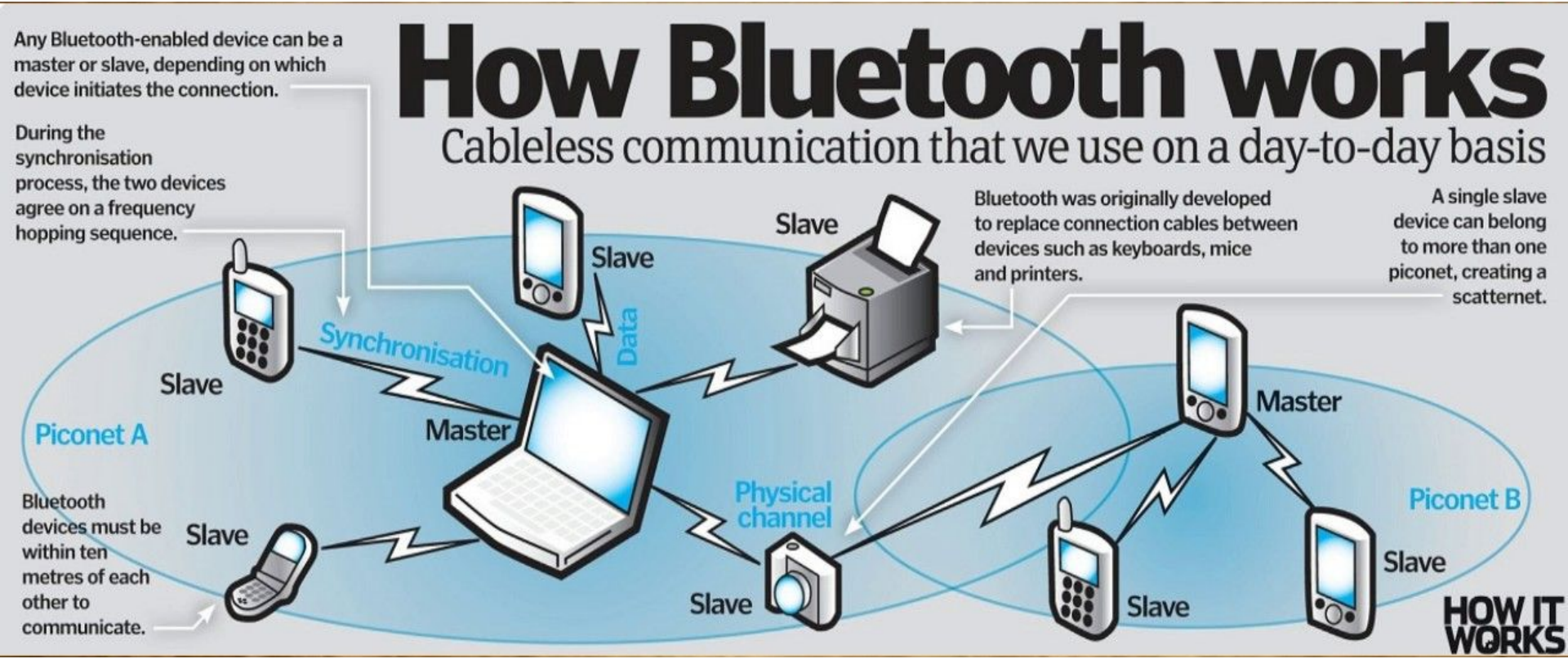
1. Bluetooth devices communicate directly with each other, rather than sending traffic through an in-between device such as a wireless router.
2. Bluetooth devices communicate using low-power radio waves on a frequency band between 2.4 MHz.
3. Two types: Bluetooth Low Energy (LE) and Bluetooth Classic
4. Bluetooth peripherals connected to the same device creates a personal area network or piconet.

How Bluetooth Operates

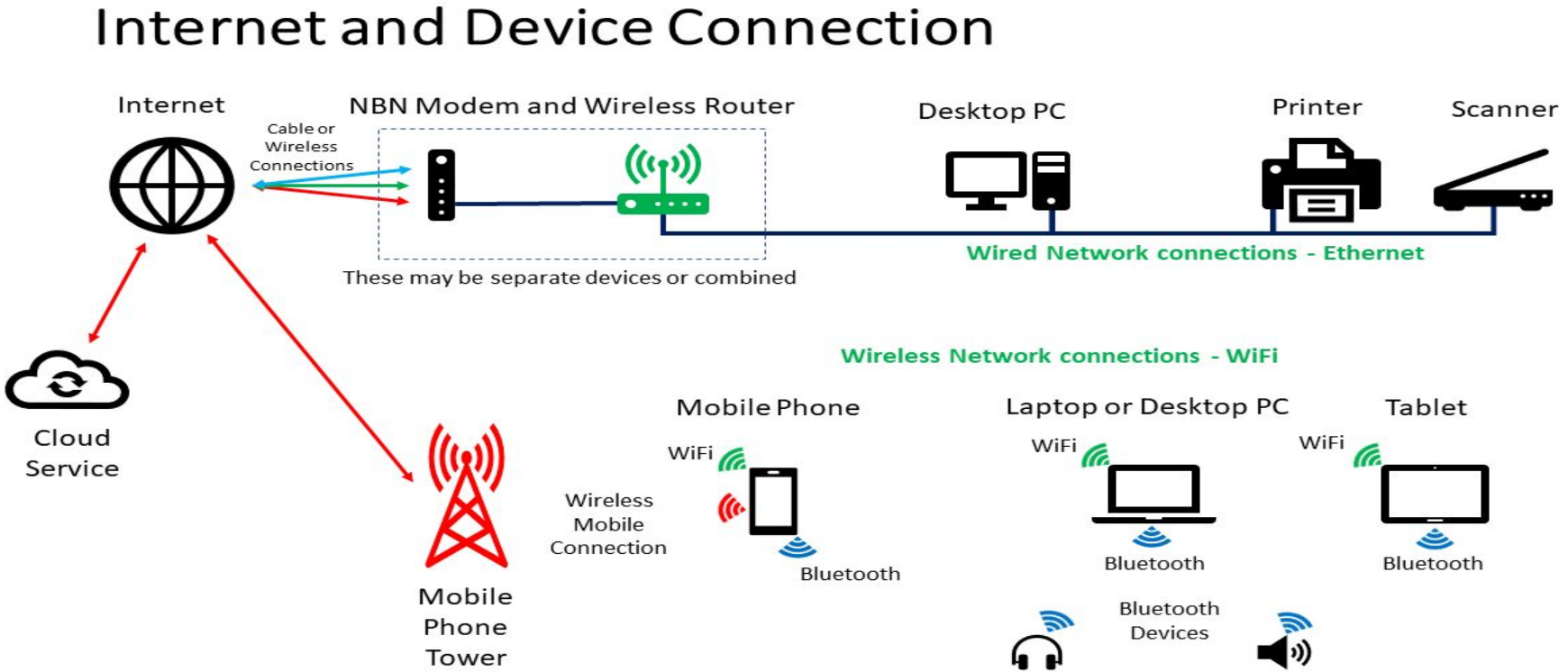
1. Devices must always be paired(For device trusting and send data encrypted).
2. When two bluetooth devices are in range a electronic conversation takes place to check if other device is trusted and if any data to send.
3. bluetooth devices creates piconets.
4. Once a piconet is established, its members hop radio frequencies in unison so they stay in touch with one another and avoid interfering with other Bluetooth piconets
5. Bluetooth technology can change frequency automatically if any frequency is busy, it is called adaptive frequency hopping.

Why Ip address is needed

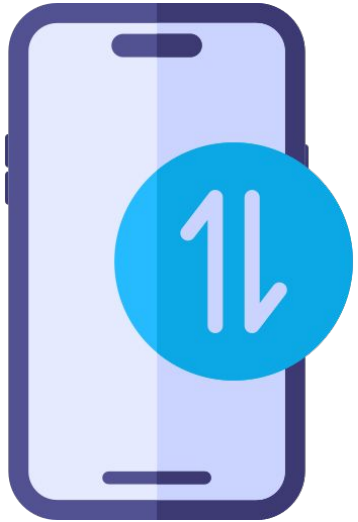
1. Both cellular networks and wifi uses the concept of Ip address.
2. In wifi only router has public ip. Devices connected to the router have private ip.
3. When device needs to send data it goes to router using the device's private ip as source, but when it leaves the router and connect to the Internet source changes to public ip address of router.
4. In Mobile networks, each cell tower acts as a router with wide range. Connection between cell tower and mobile happens through satellite. Each cell tower is connected to Internet through wire.
5. Bluetooth does not need IP address. Each bluetooth device has its own 6 byte bluetooth address(similar to mac address). This address is used to uniquely identify each device in piconet.


How Bluetooth works
Cableless communication that we use on a day-to-day basis
Any Bluetooth-enabled device can be a master or slave, depending on which device initiates the connection.
During the synchronisation process, the two devices agree on a frequency hopping sequence.
Bluetooth was originally developed to replace connection cables between devices such as keyboards, mice and printers.
A single slave device can belong to more than one piconet, creating a scatternet.
Slave
Slave
Slave
Synchronisation
Data
Master
Piconet A
Physical channel
Bluetooth devices must be within ten metres of each other to communicate.
Slave
Slave
Master
Slave
Slave
Piconet B
HOW IT WORKS

How Wifi, mobile network and bluetooth works



Comparison between data based connectivity and and temporary wifi at public places.



Security

Data-Based Connectivity: Generally more secure because it uses cellular networks with strong encryption and authentication methods. It’s harder for hackers to intercept data.

Temporary Public Wi-Fi: Often less secure, especially if it's open or doesn’t require a password. Hackers can set up fake hotspots or intercept unencrypted data, making it risky for sensitive activities like banking.

Reliability and Coverage

Data-Based Connectivity: Offers broad coverage depending on your cellular provider. It’s reliable as long as there’s a cell tower nearby, even in remote areas.

Temporary Public Wi-Fi: Limited to specific locations (cafes, airports, etc.) and can be spotty or overloaded during peak times. Connection drops are more common.

Speed and Performance

Data-Based Connectivity: Speeds can vary based on network type (4G, 5G) and location. In many cases, it provides consistent performance, though it may slow down during peak usage times or in crowded areas.

Temporary Public Wi-Fi: Speed depends on the number of users and the quality of the Wi-Fi setup. Often slower and less reliable due to congestion, throttling, or poor infrastructure.

Cost

Data-Based Connectivity: Costs are tied to our mobile plan, which can be expensive if we exceed data limits or when on roaming.

Temporary Public Wi-Fi: Often free or low-cost, especially in places like libraries, cafes, and airports. However, some premium networks may charge fees for better speeds or access.

Privacy

Data-Based Connectivity: It is more private as it doesn’t expose our device to a local network that others can access. Your data is handled directly by your cellular provider.

Temporary Public Wi-Fi: Public Wi-Fi networks can collect data on our browsing activity, and shared networks increase exposure to other connected devices.

Difference between cellular and Whatsapp calls

Cellular Calls: The whole geographical area covered by the network is partitioned into a number of hexagonal cells. Each cell is serviced by base station and a set of these are connected to mobile switching centre. The only wireless connection in cellular network is in between Mobile station and Base station. When a mobile station is turned on within the coverage of network, MS scans the group of Forward Control Channels(broadcast all traffic requests) in the search of strongest base station. A request containing MIN, ESN, etc is sent to serving Base Station which is then transferred to concerned Mobile Switching Centre. After validating the request, MSC instructs the BS to assign a pair of unused FVC and RVC for voice transmission and reception.

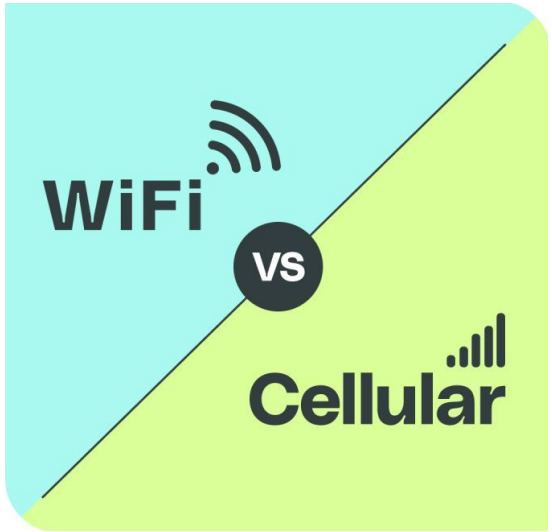
WhatsappCalls:

Unlike cellular calls, where a dedicated line/channel is used for the entire duration of the call, WhatsApp calls are based on **VoIP (Voice over Internet Protocol)**, i.e uses packet-switching which means voice data is transmitted over the internet in the form of data packets where it's reassembled at the other end. It require an internet connection, either via Wi-Fi or mobile data. It uses **Opus Codec** to compresses your voice and adjusts the quality based on your internet connection to maintain the call's quality.

WhatsApp uses **WebRTC (Web Real-Time Communication)** technology, which is an open-source protocol suite that enables peer-to-peer communication over the internet, bascially for signalling anad connection setup. WhatsApp uses **RTP(Real-Time Transport Protocol)**, a standard protocol for delivering real-time audio and video over IP networks. RTP packets also contain timestamps and sequence numbers to help maintain proper timing and order of audio playback.

WhatsApp encrypts the signaling messages and media using **Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)** to protect the communication channels. These protocols ensure that the communication between devices and WhatsApp servers remains secure. WhatsApp calls primarily use **UDP(User Datagram Protocol)** for data transfer as it does not require error-checking or retransmission like TCP and speed is more important than perfect data accuracy in voice calls.

Using Wi-fi when Cellular Network is deactivated



Cellular networks rely on a network of base stations (cell towers) that are managed by mobile network operators and provide wide-area coverage by connecting devices to a central core network.

Wi-Fi uses a different communication protocol, IEEE 802.11, as well as different frequency bands for networking. A device connects to a Wi-Fi access point (such as a router) that serves as a gateway to the internet.

Using Wi-fi when Cellular Network is deactivated

When we deactivate our cellular network, its essentially disabling the phone's ability to communicate with the base stations. However, this does not interfere with other communication layers that do not rely on cellular infrastructure. Even when cellular networks are deactivated, the device's Wi-Fi module can still function, thus wi-fi is still usable when cellular network is deactivated.

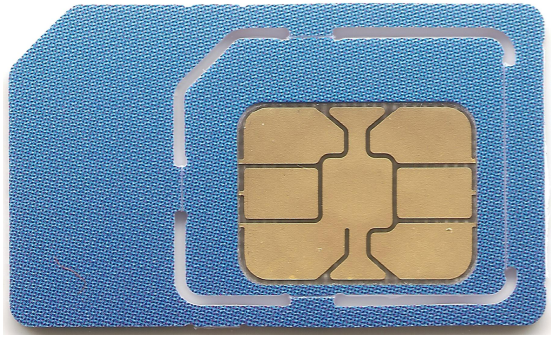
How it happens?

- Cellular networks use licensed spectrum (e.g., 700 MHz to 3.5 GHz) for communication, whereas Wi-Fi operates in the ISM (Industrial, Scientific, and Medical) band, which is unlicensed.
- While both operate at the network layer of the OSI model, in cellular networks, packets are routed through the carrier's infrastructure, while in Wi-Fi, packets are transmitted directly through a local network to an internet gateway.

The distinct frequencies and modulation techniques along with the separation in routing protocols ensure that disabling one network doesn't impact the other.

What Is Present Inside a SIM ?

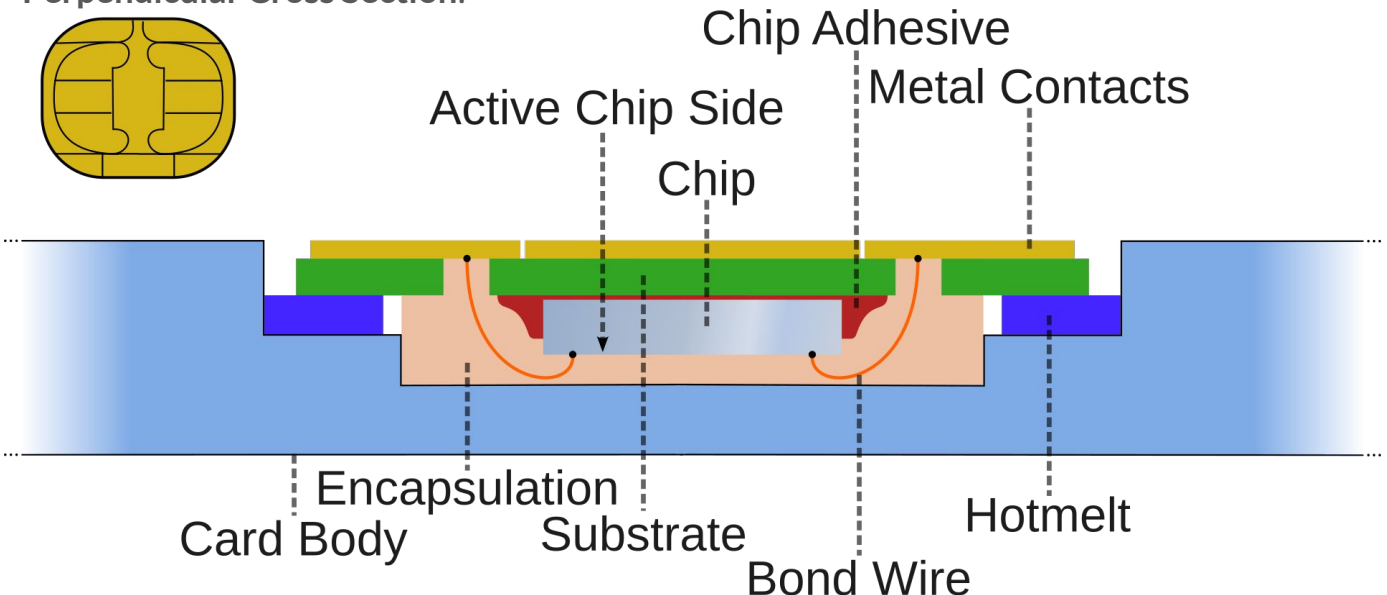
A **SIM** (**Subscriber Identity Module**) **card** is an integrated circuit (IC) intended to securely store an international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephone devices.



Technically the actual physical card is known as a universal integrated circuit card (UICC); this **smart card** is usually made of PVC with embedded metal contacts and semiconductors, with the SIM as its primary component. In practice the term "SIM card" is still used to refer to the entire unit and not simply the IC.

What Is Present Inside a SIM Card?

Perpendicular Cross Section:



IC Chip on a SIM Card

The IC chip on a SIM card is a key component responsible for secure communication and user authentication on mobile networks. It includes:

- **Microcontroller**: Manages data processing and runs the SIM's operating system (usually a variant of **Java Card**).
- **Memory Types**:
  - **EEPROM**: Stores user-specific data (e.g., IMSI, Ki).
  - **RAM**: Temporary storage for processing tasks.
  - **ROM**: Holds the SIM's permanent data and operating system.
- **Security Features**: Encrypts data, handles authentication, and stores secret keys (e.g., Ki).
- **Protocols**: Communicates with mobile devices via ISO/IEC 7816 and GSM/LTE protocols.
- **Contact Pads**: Facilitate physical connection with the device for power and data transfer.

Security Module

Security is an important aspect of a SIM card. The SIM card's chip includes various security features to ensure secure storage of information and protection against tampering:

- **Ki (Authentication Key)**: A 128-bit secret key stored securely on the SIM card and never transmitted over the network. It's used during the authentication process.
- **Encryption Algorithms**: SIM cards use algorithms like **A3**, **A5**, and **A8** for encryption and authentication in GSM networks. Modern SIMs may use more advanced algorithms for 3G/4G networks.
- **Cryptographic Co-Processor**: Some modern SIM cards have dedicated hardware to perform cryptographic operations like key generation, hashing, and digital signing, improving both security and performance.

Informations Preserved In a SIM Card

A SIM card preserves essential data for mobile network access and user identification, including:

- **IMSI (International Mobile Subscriber Identity)**: A unique identifier used for authenticating users on a mobile network.
- **ICCID (Integrated Circuit Card Identifier)**: A unique serial number that identifies the SIM card globally.
- **Ki (Authentication Key)**: A secret key used for secure network authentication.
- **Phone Number (MSISDN)**: The user's mobile number associated with the SIM.
- **Contacts and SMS**: Some SIM cards store a limited number of phone contacts and text messages.
- **Network Preferences**: Information like the preferred network list for roaming and connectivity settings.

References

1. https://en.wikipedia.org/wiki/SIM_card
2. https://en.wikipedia.org/wiki/Smart_card
3. https://www.youtube.com/watch?v=iJFnYBJJiuQ&t=94s
4. https://www.phindia.com/Books/BookDetail/9788120339521/mobile-computing-dasbit-sikdar
5. https://en.wikipedia.org/wiki/Cellular_network
6. https://en.wikipedia.org/wiki/WhatsApp

THANK YOU