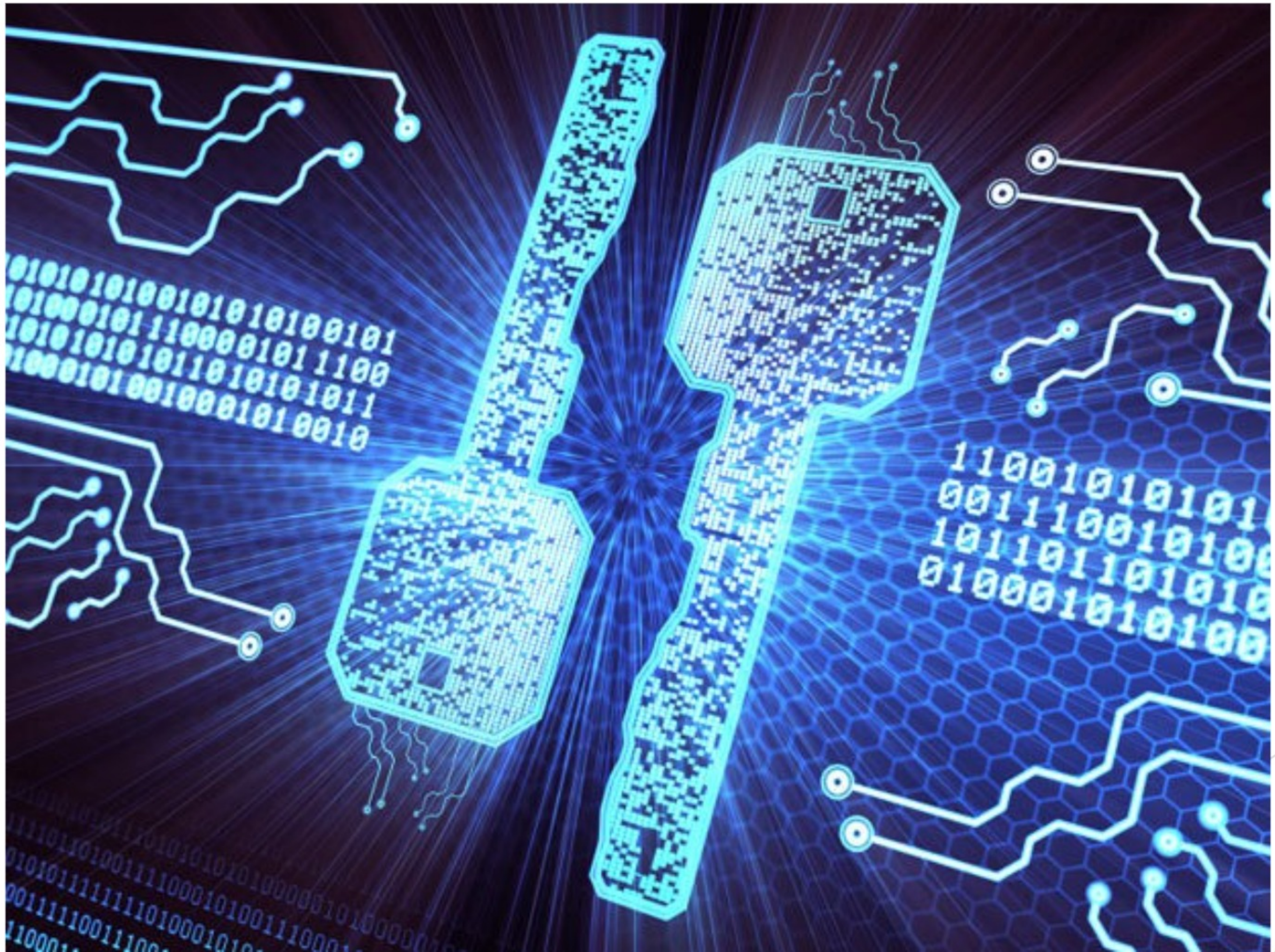
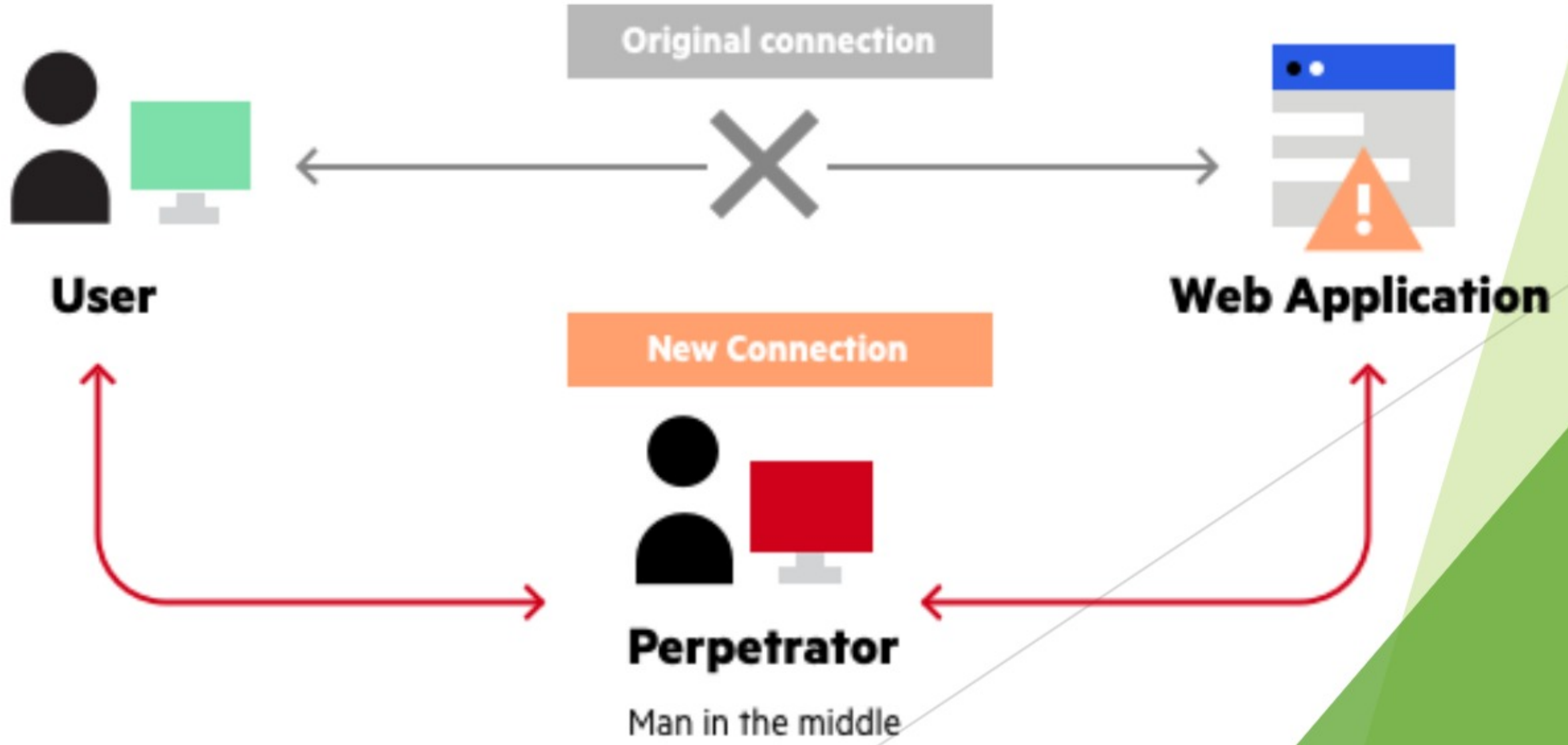
QUANTUM CRYPTOGRAPHY



WHY DO WE NEED QUANTUM INTERNET AND QUANTUM COMPUTING:

LIMITATIONS OF CLASSICAL COMPUTING:

- The Speed of Classical Computers is Limited :
  For Example a 32 bit processor can only process 32 bit per second
- Transmission of Information in Classical Computing is prone to Middle-Man-Attacks



HOW ARE MIDDLE MAN ATTACKS ACTUALLY PROPAGATED:

The Attacker makes free , malicious , password unprotected wi-fi -hotspots

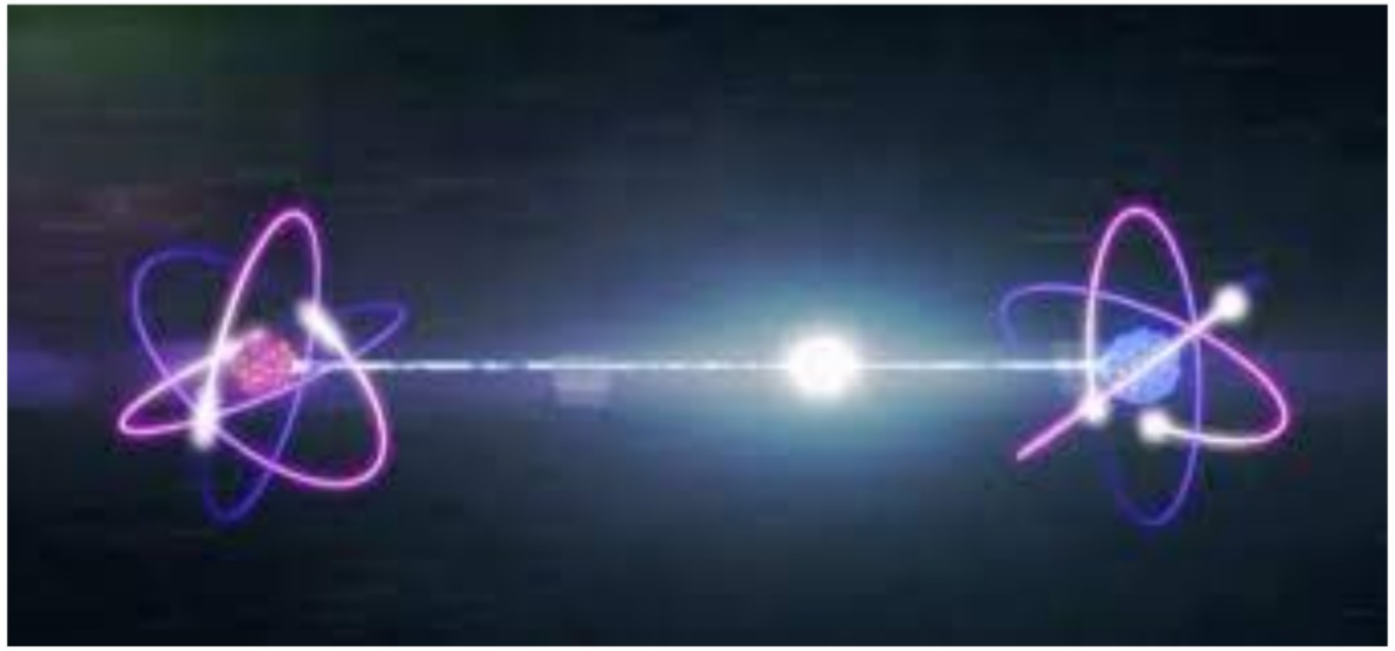
i)Victims are entrapped when they connect to this public hotspot
ii)Attacker gains full visibility about the data exchange
iii)Further ARS Spoofing can be done by attacker since both the user and attacker are in the same network
iv)In this process the attacker's MAC Address is linked to the IP Address of the internet Network by sending so the messages sent by the user are transmitted to the attacker rather than sending them to the web application

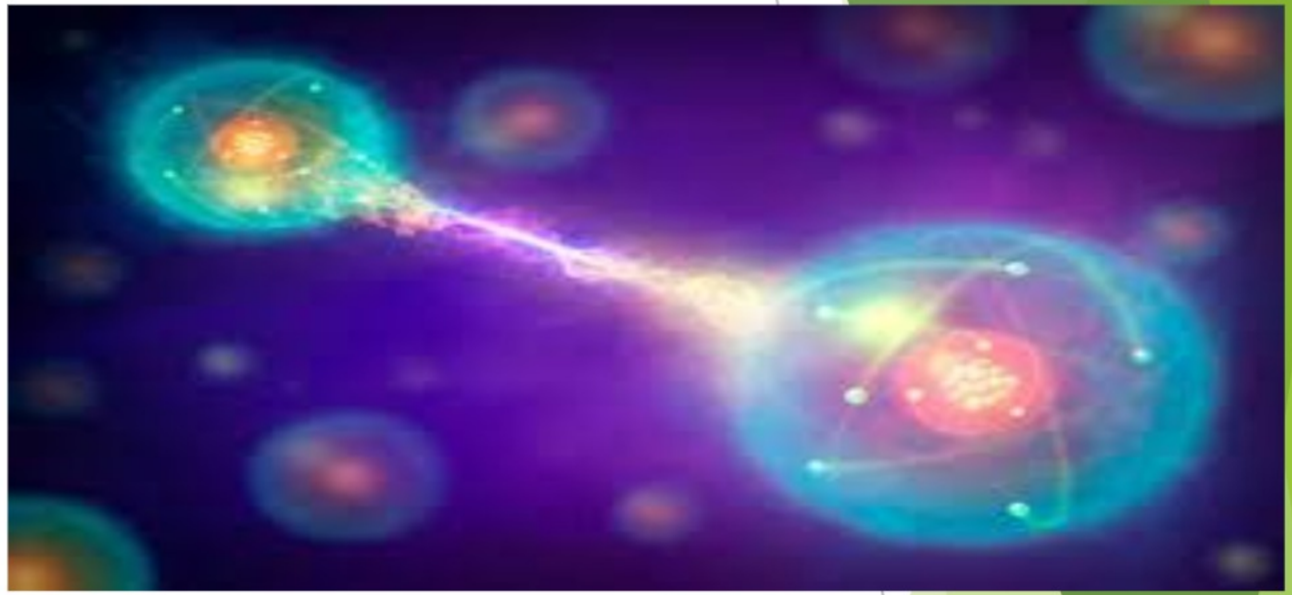
PREVENTION OF MAN IN THE MIDDLE ATTACKS

In spite of many great attempts to completely avoid Man-in-the-Middle attacks our classical computing and encrypting methods are not 100% fail-proof as attackers still intrude into our confidential data.

To Solve the Above problem few concepts in Quantum Physics like Quantum Entanglement and Quantum superposition have been suggested by great scientists and software developers

QUANTUM ENTANGLEMENT





“The Phenomenon where two generated particles correlate in such a manner that the quantum state of one of the particles cannot be independently determined without the other in the group even if the distance between them is Large”

IMPLEMENTATION OF QUANTUM ENTANGLEMENT:

In Quantum Computing we have few special bits called qubits which take two classical bits at a time.

So a n-qubit quantum processor can compute the results of 2^n bits per second

MODE OF TRANSFER OF INFORMATION:
In contrast to classical internet where ALL the bits are transferred in the form of voltage or light pulses , in Quantum Internet, only the quantum states of two entangled qubits is transferred from source to destination.
Do we have a solution to transfer quantum states from source to destination??

Brief project execution

- Inspired from quantum cryptography we planned to create a security system based on quantum entanglement and superposition which generates a private code to prevent eavesdropping by using simple quantum circuits
- In our code we generate 8 different quantum circuits
- 4 of them are for einstein and 4 of them are for bohr lets assume
- Einstein measures on a 4 sets of basis and bohr measures on another 4 sets of basis which may be same or different
- Finally they see if their basis match each other and from the matched ones a private code is generated by a simple logic
- If man in the middle attacks happen the entangled qubits get disentangled and private key is not generated , so its a safe way of encrypting a information into this security system and decrypting it later
- We tried our best in executing the code hope u check it out too!

- https://github.com/tankisank/quantum-cryptography/blob/main/x.ipynb