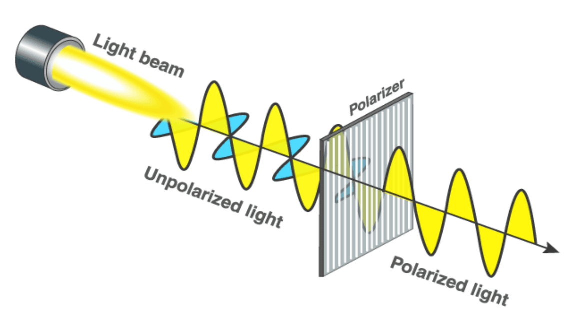
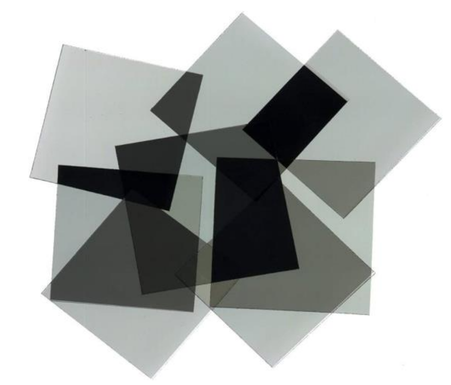
POLARIZATION IN QUANTUM KEY DISTRIBUTION

Miranda Wang, Anna Burns, Kashika Adhikari, Helen Beebe, Aylin Ozus, Ashley Park, Joy Xia

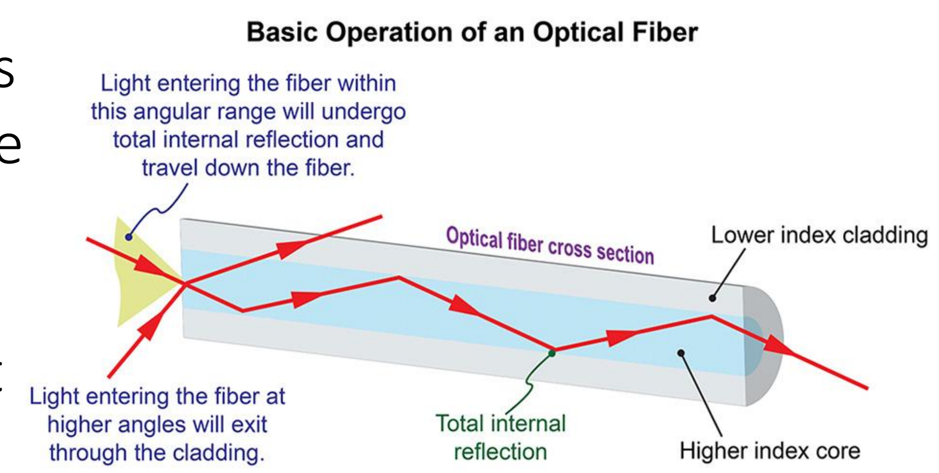
How Polarization and Optical Fibers Work

Polarization refers to the restriction of light to one basis (orientation). This is an example of light acting as a wave, rather than a particle.





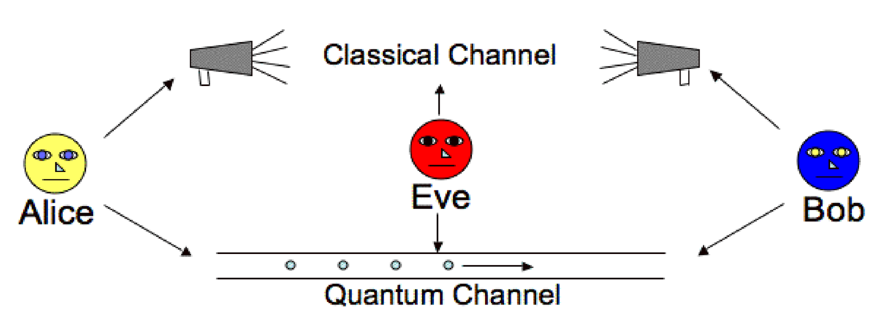
Optical fibers are used to transmit information over long distances at high speeds. Light travels through the denser glass core, which has a higher index of refraction than the less dense plastic cladding.
Due to **total internal reflection**, 100% of light is trapped inside the core and reflects off the sides at a critical angle, allowing it to travel through the optical fiber.



Explaining Quantum Key Distribution

Quantum Key Distribution (QKD) is a set of instructions detailing how to establish a secure communication channel.

For example, Alice (the sender) is trying to send Bob (the receiver) information through light using a sequence of classical bit values of 0 and 1. By polarizing the light, Alice encodes each bit into either the:



1) Standard Basis using the respective classical bits into corresponding quantum bits
$0 \rightarrow |\uparrow\rangle$ y-basis
$1 \rightarrow |\rightarrow\rangle$ x-basis
2) Hadamard Basis using equal superpositions of the standard basis states
$0 \rightarrow |\nearrow\rangle = 1/\sqrt{2}\,(|\uparrow\rangle + |\rightarrow\rangle)$
$1 \rightarrow |\nwarrow\rangle = 1/\sqrt{2}\,(|\uparrow\rangle - |\rightarrow\rangle)$

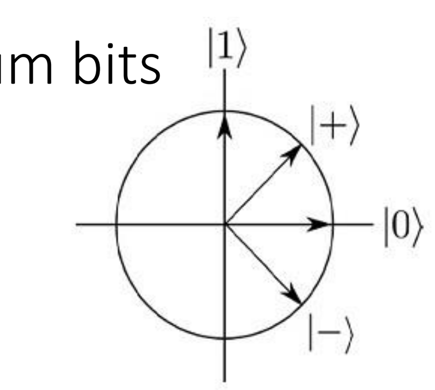
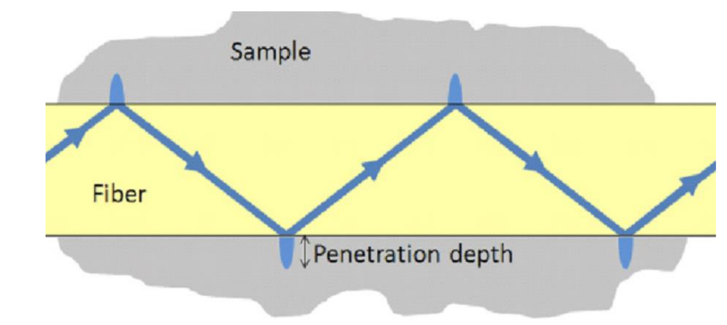


Figure 3.1: Standard and Hadamard basis states represented on the real plane.

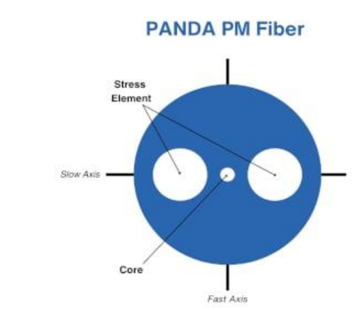
Eve, a 3rd-party eavesdropper, does not know which basis Alice is using and thus, measures incorrectly 50% of the time. This collapses the qubit, meaning there will be a 25% chance that Bob measures a different bit value than the one Alice sent. Afterwards, Alice and Bob compare the bases they used for each qubit through the classical channel and conclude that either they have a **secure private key** OR they have detected that an **eavesdropper is present**. Both situations allow Alice and Bob to run little risk of establishing a compromised key.

Benefits and Applications

In an optical fiber, light sometimes travels through the boundary as an **evanescent wave** into the cladding, attributed to its wave nature. As a result, **dispersion** occurs, which changes the speed that light travels, due to the differences in index of refraction in the materials.



Polarization can be used inside an optical fiber, known as **polarization-maintaining (PM) fibers** to prevent this disruption and improve signal integrity.



In classic **cryptography,** communicating parties share a secret sequence of numbers called a key which is used to encrypt/decrypt data. Current intrusion detection systems however, frequently alert for false positives. **QKD** protocols (establishing keys by encoding qubits into polarization states) prevent the decryption of data because intruders will always be detected.
Quantum Communications can be used in:

- Banking to protecting details about clients' accounts
- Government & Defense to ensure protection of classified data from espionage
- Finances/Credit Cards to safeguard business data and credit card information

Limitations

There are several communication and security requirements in **QKD** as it is highly implementation dependent rather than assured through the laws of physics:

1. Only a partial solution: **QKD** ensures a secure secret code but does not guarantee that the message came from the right person or hasn't been tampered with.
2. Cannot be easily implemented: **QKD** cannot be implemented as a network service or in a software and lacks flexibility for upgrades.
3. Extra infrastructure: Long distances require the use of relays or special stations that are costly.

References/Acknowledgements

This work was completed as part of the Quantum Engineering Research and You (QuERY) program at Bellaire High School, supported by the Harvard Quantum Initiative and MIT CQE-iQuISE (Center for Quantum Engineering, Interdisciplinary Quantum Information Science and Engineering program). We would like to thank our mentor, **Katie Barajas**, and **Dr. Jimmy Newland** for their leadership and guidance!

1. National Security Agency/Central Security Service > Cybersecurity > Quantum Key Distribution (QKD) and Quantum Cryptography QC, National Security Agency/Central Security Service, https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/