Quantum Cryptography

Amir H. Karamlou

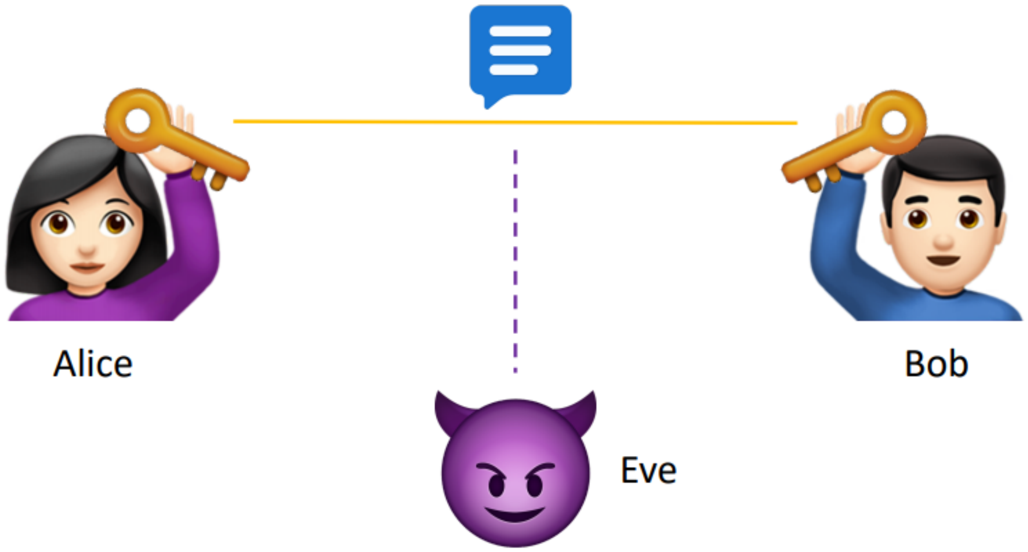
Quantum Summer Camp

16 July 2020

ENGINEERING QUANTUM SYSTEMS
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
NSF

What is an Cryptography?

Cryptography: To ensure Secure communication between two parties



Binary One-Time-Pad

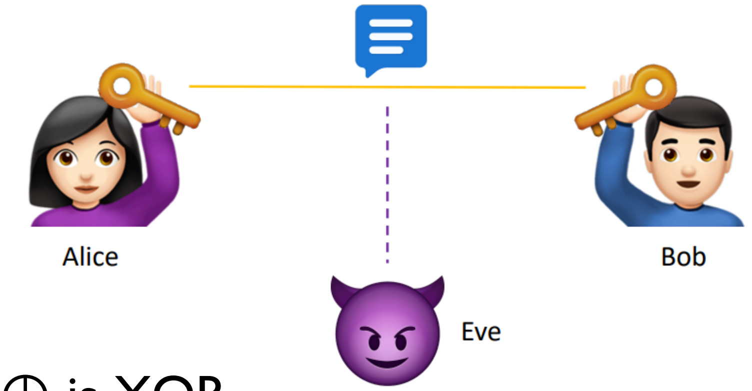
Let's assume that Alice and Bob share a randomly generated binary key k

$$k = 01011001$$

And Alice wants to send the message m to Bob

$$m = 10001001$$

Alice encrypts her message by sending Bob $m \oplus k$



$\oplus$ is XOR

Bob can decrypt the message by XORing the encrypted message with his key

$$(m \oplus k) \oplus k = m \oplus (k \oplus k) = m$$

$$\begin{array}{rl} & m = 10001001 \\ \oplus & k = 01011001 \\ \hline & 11010000 \end{array}$$

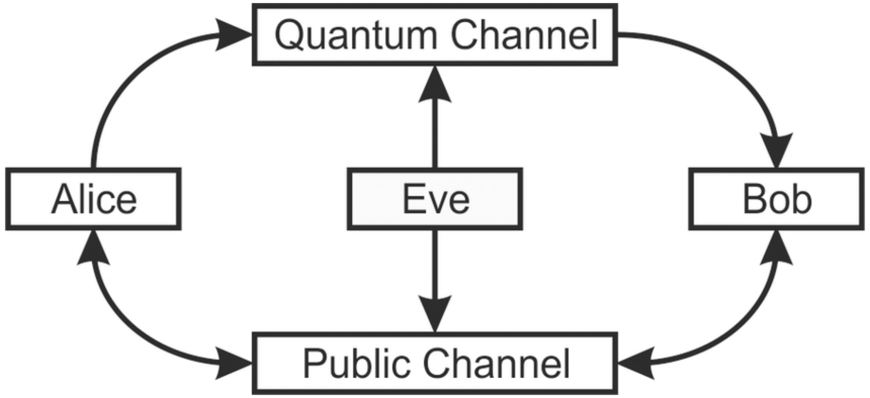
$$\begin{array}{rl} & (m \oplus k) = 11010000 \\ \oplus & k = 01011001 \\ \hline & 10001001 \end{array}$$

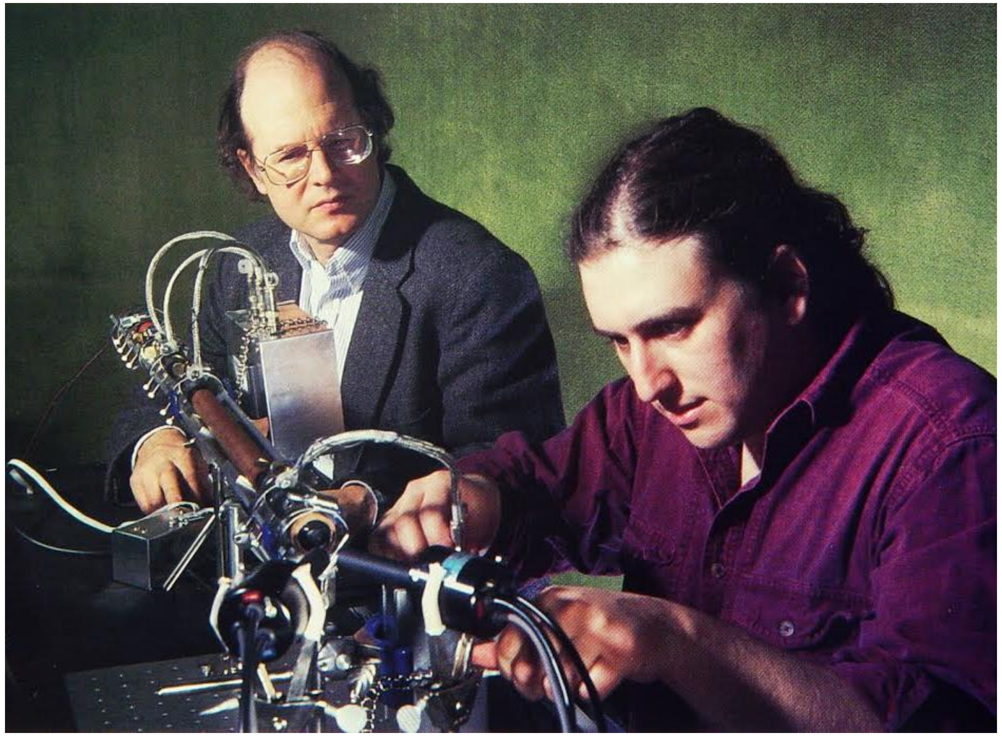
Binary One-Time-Pad

- Binary one-time-pads are fully secure based on the laws of probability
- Each pad is only fully secure for a single use
  – We need a new key for every message sent
- Challenge: How can we distribute the shared key between Alice and Bob securely?
  – Also referred to as Key Distribution
- Using quantum mechanics!
  – Security guaranteed by the laws of physics!!

Quantum Key Distribution (QKD)

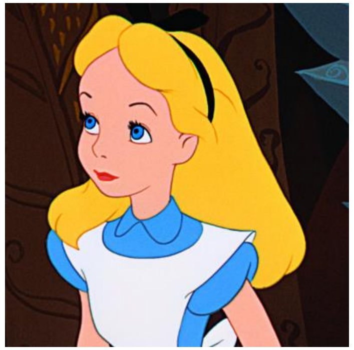
- First QKD protocol: BB84
  - Developed by Charles Bennett and Gilles Brassard in 1984
- Relatively easy to implement
- Takes advantage of quantum no-cloning theorem
- Safety guaranteed based on the laws of physics





Quantum Key Distribution (QKD)

How Does it work?



	$\|0,1\rangle$	$\|+,-\rangle$
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

Choses a bit-string at random: 10101001

Choses a random set of basis with the same length

Basis options: $|0,1\rangle$ or $|+,-\rangle$

Reminder: $|+\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|-\rangle = H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

What if we measure in the wrong basis?

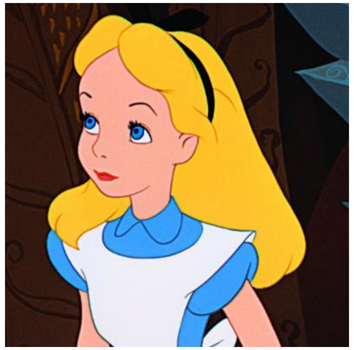
- You get a random bit instead of the message

$|+\rangle$ or $|-\rangle \begin{cases} 50\%\ |0\rangle \\ 50\%\ |1\rangle \end{cases}$

$|0\rangle$ or $|1\rangle \begin{cases} 50\%\ |+\rangle \\ 50\%\ |-\rangle \end{cases}$

Quantum Key Distribution (QKD)

How Does it work?



Alice sends her qubits to Bob

Bob and Alice compare their basis for each qubit

Choses a bit-string at random: 10101001

Choses a random set of basis with the same length

Prepares each qubit to correspond to the bit value in that basis

	$\|0,1\rangle$	$\|+,-\rangle$
0	$\|0\rangle$	$\|+\rangle$
1	$\|1\rangle$	$\|-\rangle$

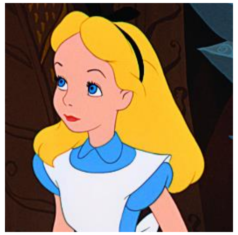
Bob measures the each qubit from Alice in a random basis

If for any of the qubits their basis doesn't match they both discard the corresponding bit from the key

End result: a key that only Alice and Bob have access to

Quantum Key Distribution (QKD)

Why is it secure?



Let's assume we have an eavesdropper: Eve

- Based on the laws of quantum mechanics Eve cannot copy the qubit state
- So she has to measure in a random basis and send Bob a new qubit
- If she does that, Alice and Bob can figure out how much of the key Eve knows
- If Eve knows too much, Alice and Bob will discard the key