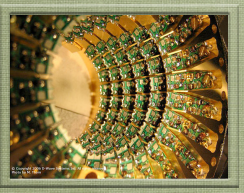


2110413 Computer Security

Lecture 9

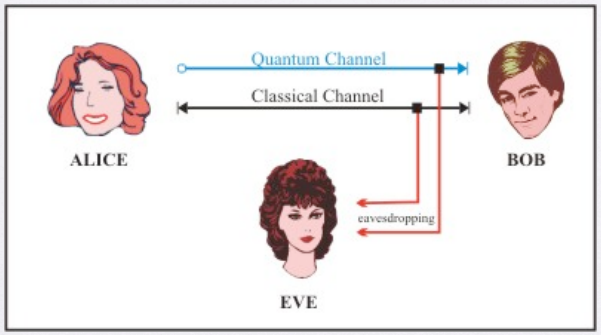
Quantum Key Distribution

Krerk Piromsopa, Ph.D.
Department of Computer Engineering
Chulalongkorn University

Outline

- Motivation
- About Quantum
- Algorithm
- Why does it secure?

Detailed Walkthrough



Message

H E L P

00111 00100 01011 01111

ALICE

BOB

0

Message

H E L P

00111 00100 01011 01111

ALICE

BOB

Message

H E L P

00111 00100 01011 01111

ALICE

BOB

EVE

Message

H E L P

00111 00100 01011 01111

ALICE

BOB

EVE

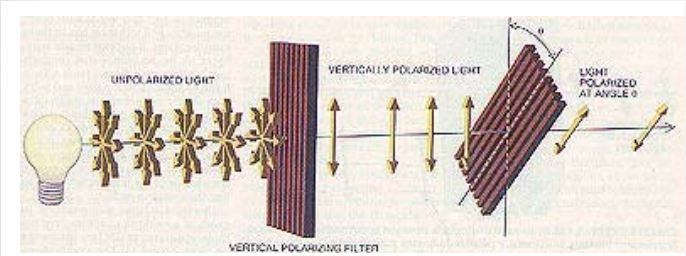
Private communication

Alice and Bob share a one-time pad
(secret random key).

	00111001000101101111	Message
$\oplus$	01110010011010010011	Key (random string)
	01001011011111111100	Coded message
$\oplus$	01110010011010010011	Key (random string)
	00111001000101101111	Message

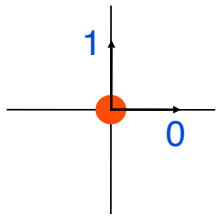
But where do Alice and Bob get the key?

Quantum

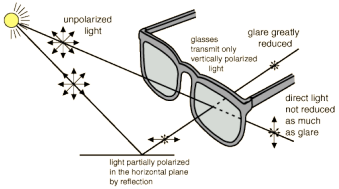


Qubits: Two-state quantum systems

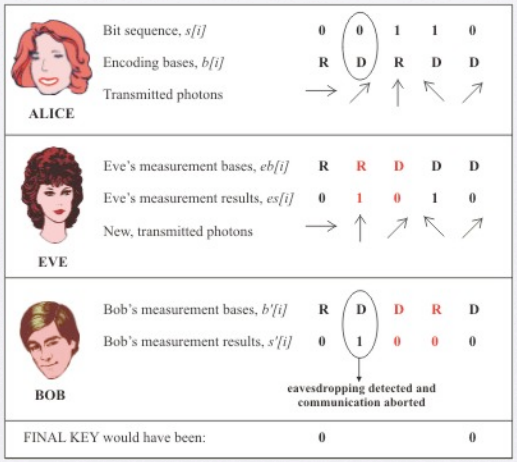
PHOTON



PHOTON POLARIZATION



How does it work?



"TWO-BIT" DEVICE

RULES

1. AN INTERLOCK MECHANISM PERMITS ONLY ONE BOX AT A TIME TO BE OPENED.
2. WHEN A BOX IS OPENED, THE INTERLOCK ALSO CAUSES A RANDOM BIT TO BE PLACED IN THE OTHER BOX.

INFORMATION CAPACITY = 1 BIT

IF YOU TRY TO SEND 2 BITS ENCODED IN WHICH BOX AND WHAT'S IN THAT BOX, YOU END UP SENDING ONLY HALF A BIT.

Secret key distribution

ALICE

BOB

X

Secret key distribution

ALICE

BOB

0

X

X Y

Secret key distribution

ALICE

BOB

X

Secret key distribution

ALICE

BOB

0

X

X Y

Secret key distribution

Alice

Bob

1 0 1 0 0 1 0 0 0 1

X X Y X Y Y Y X Y Y

r r r 0 r 1 r 0 0 r

Y Y X X X Y X X Y X

Alice and Bob announce their box sequences publicly and keep the bits only when the boxes agree. This process, called sifting, yields a shared secret key, in this case

0100

The key generation rate is 50% (1/2 bit per try).

Alice

1. Alice and Bob's sifted keys have an error rate of 25%. By sacrificing some key bits, they can detect Eve's presence through the error rate.
2. Eve knows 50% of each of their sifted keys.

Bob

1 0 1 0 0 1 0 0 0 1

X X Y X Y Y Y X Y Y

r r r 0 r s r s 0 r

Y Y X X X Y X X Y X

r r r 0 0 r 0 r

Y Y X X Y X

Heh, heh, heh.

Eve

Error correction and privacy amplification allow Alice and Bob to extract a secret key provided the error rate does not exceed 17.1%.

Flaw: If Eve can deactivate the interlock, she can open both boxes and determine the sifted key without introducing errors.

Secret key distribution

Alice

Quantum mechanics to the rescue! For quantum systems, the two rules are consequences of the laws of quantum mechanics: there is no hidden interlock mechanism to be de-activated.

Bob

Rats! Foiled again. I hate those quantum mechanicians.

Eve

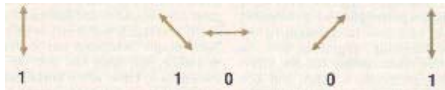
Alice sends photons with one of the four polarizations, chosen at random.

For each photon, Bob chooses at random the type of measurement: + or X

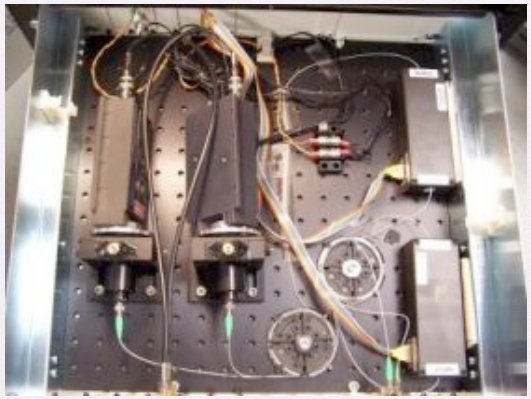
Bob records the result of his measurements, but keeps it a secret.

Bob tells Alice the measurement types used (but not results) in freespace.
Alice tells him which were correct.

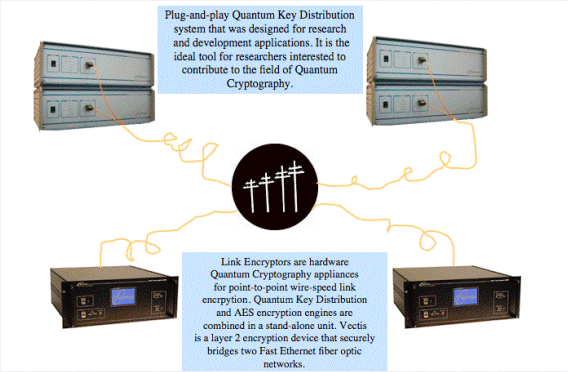
Alice and Bob keep correct cases and translate to 0's and 1's



Real Device



for Sale!



Why is quantum key distribution secure?

An unopened box has no bit value waiting to be discovered. Alice and Bob create the key by opening their boxes. Before that, there is no key for Eve to steal.

"There is no there there."
Gertrude Stein damning her native Oakland and inadvertently describing quantum systems.

Essential ingredient: Entanglement between qubits