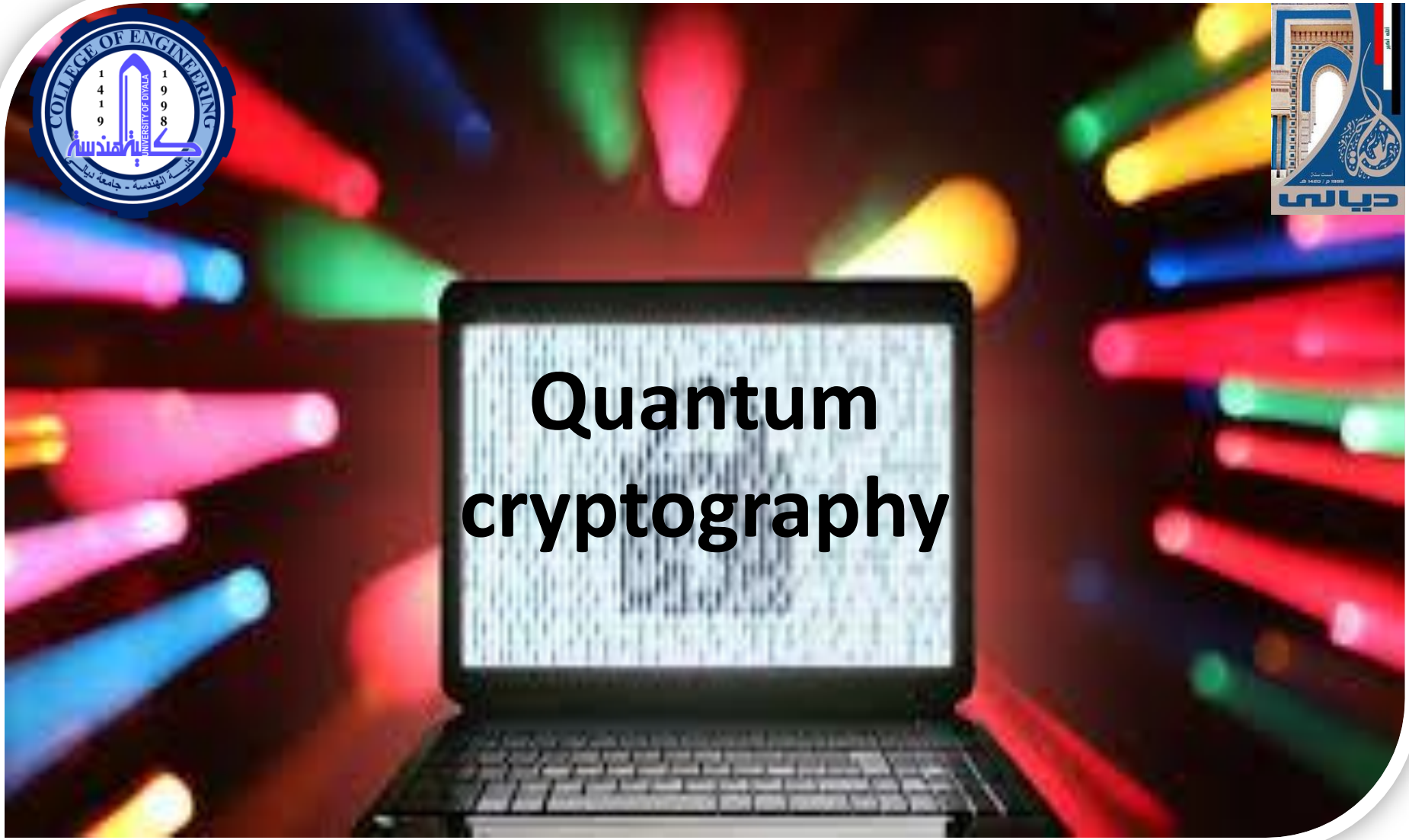


Presented by: Ass.Lec. Dhafer T. Shihab
University of Diyala
College of Engineering
Department of computer engineering

Introduction

- Cryptography is of increasing importance in our technological age using broadcast, network communications, Internet ,e-mail, cell phones which may transmit sensitive information related to finances, politics, business and private confidential matters.

- **Quantum cryptography**, or **quantum key distribution** (QKD), uses **quantum mechanics** to guarantee secure communication. It enables two parties to produce a shared random bit string known only to them, which can be used as a **key** to encrypt and decrypt messages

Quantum mechanics

- **Quantum mechanics** (quantum physics or quantum theory) including quantum field theory, is a fundamental branch of physics concerned with processes involving, for example, **atoms** and **photons**.

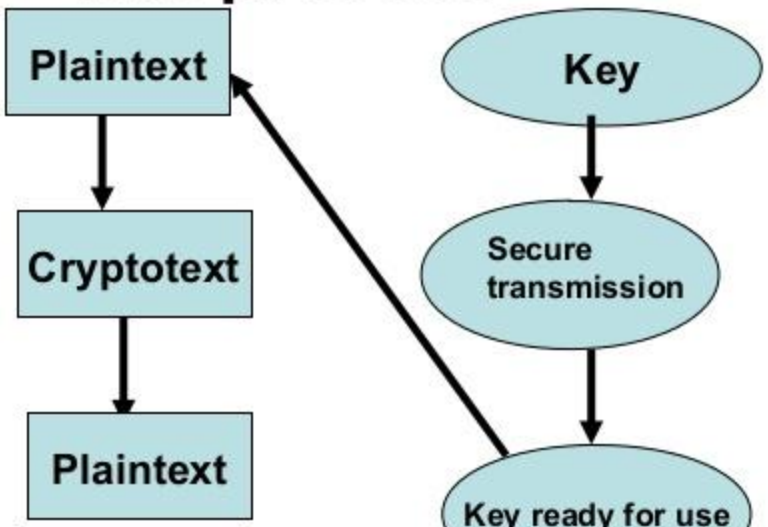
The process

- Sender

Encryption

Decryption

Recipient



Message encryption

Secure key distribution

Hard Problem for conventional encryption

The classical cryptography

- Encryption algorithm and related key are kept secret.
- Breaking the system is hard due to large numbers of possible keys.
- For example: for a key 128 bits long
- there are

$$2^{128} \approx 10^{38}$$

keys to check using **brute force**

The fundamental difficulty is **key distribution** to parties who want to exchange messages.

PKC: The Modern Cryptography

- In 1970s the Public Key Cryptography emerged.
- Each user has two mutually inverse keys,
- The encryption key is published;
- The decryption key is kept secret.
- Anybody can send a message to Bob but only Bob can read it.

PKC: RSA (cont..)

- The most widely used PKC is the RSA algorithm based on the difficulty of
- factoring a product out two large primes.

- Easy Problem

  Given two large primes p and q compute $n = p \times q$

Hard Problem

Given n compute p and q.

Factoring A Product Of Two Large Primes

- The best known conventional algorithm requires the solution time proportional to:

$$T(n) = \exp[c(\ln n)^{1/3} (\ln \ln n)^{2/3}]$$

i.e. scales exponentially with the input size

for p & q 65 digits long T(n) is approximately one month using cluster of workstations.

for p & q 200 digits long T(n) is astronomical.

Quantum Computing Algorithm For Factoring

- In 1994 Peter Shor from the AT&T Bell Laboratory showed that in principle a quantum computer could factor a very long product of primes in seconds.
- Shor's algorithm time computational complexity is

$$T(n) = O[(\ln n)^3]$$

Once a quantum computer is built the RSA method would not be safe.

Need of quantum cryptography

- Classical Cryptography relies heavily on the complexity of factoring integers.
- Quantum Computers can use Shor's Algorithm to efficiently break today's cryptosystems.
- We need a new kind of cryptography!

Perfect Secrecy and the OTP

- There exist perfect cryptosystems.

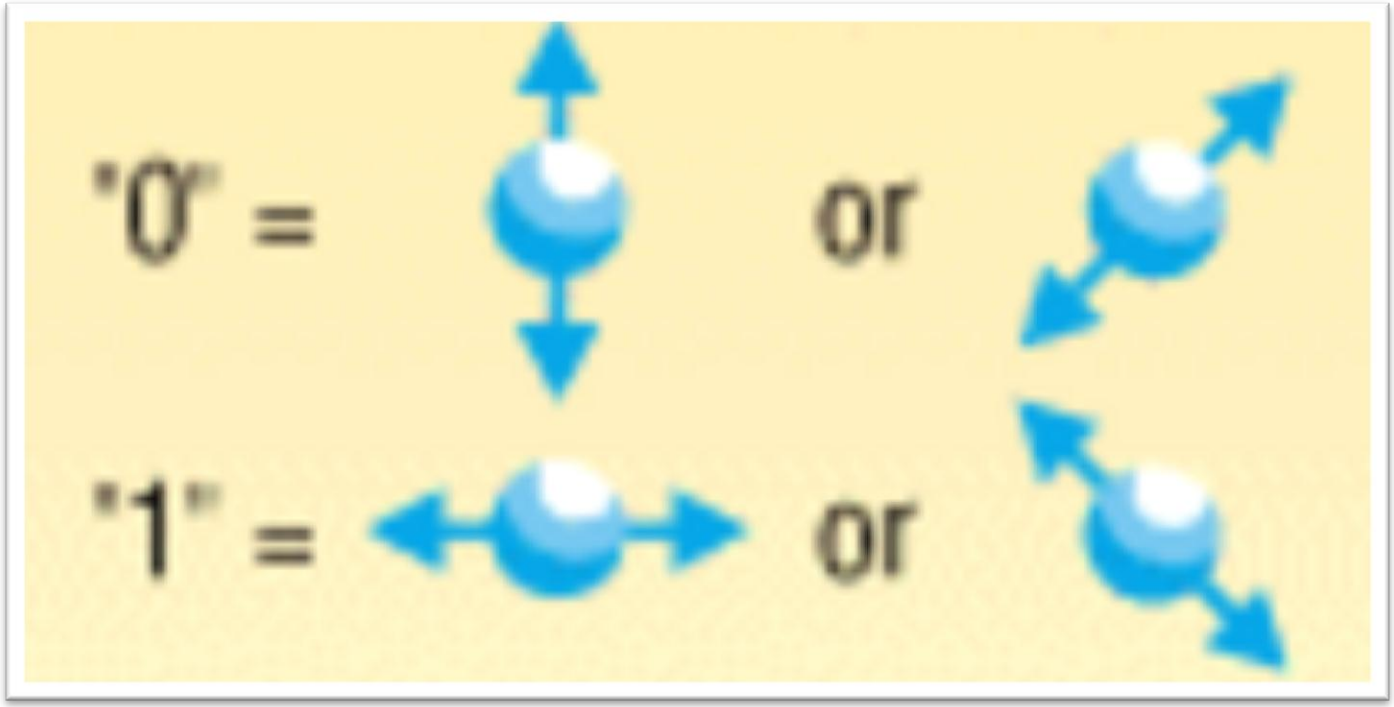
  Example: One-Time Pad (OTP)
- The problem of distributing the keys in the first place remains.
- QKD: Quantum Key Distribution
- Using quantum effects, we can distribute keys in perfect secrecy!
- The Result: The Perfect Cryptosystem,

  QC = QKD + OTP

Elements of the Quantum Theory

- Light waves are propagated as discrete quanta called photons.
- They are massless and have energy, momentum and angular momentum called spin.
- Spin carries the polarization.
- If on its way we put a polarization filter(polarizer) a photon of a specific polarization pass and blocks others.

Photon polarization



Binary Information & quantum information

- Each photon carries one qubit of information
- Polarization can be used to represent a qubit information.
- To determine photon’s polarization the recipient must measure the polarization by ,for example, passing it through a filter.

Binary Information & quantum information (cont..)

- A user can suggest a key by sending a stream of randomly polarized photons.
- This sequence can be converted to a binary key.
- If the key was intercepted it could be discarded and a new stream of randomly polarized photons sent.

Heisenberg Uncertainty Principle

- Certain pairs of physical properties are related in such a way that measuring one property prevents the observer from knowing the value of the other.

- When measuring the polarization of a photon, the choice of what direction to measure, affects all subsequent measurements.

- If a photon passes through a vertical filter it will have the vertical orientation regardless of its initial direction of polarization.

Photon Polarization

When a photon passes through the correct filter, its polarization does not change.

When a photon passes through the incorrect filter, its polarization is modified randomly.

Quantum Key Distribution

(a)Alice communicates with Bob via a quantum channel sending him photons.

(b) Then they discuss results using a public channel.

(c) After getting an encryption key, Bob can encrypt his messages and send them by any public channel.

Quantum Key Distribution (cont..)

- Both Alice and Bob have two polarizers each.
- One with the 0-90 degree basis (+) and one with 45-135 degree basis (×)

(a) Alice uses her polarizers to send randomly photons to Bob in one of the four possible polarizations 0,45,90,135 degree.

(b) Bob uses his polarizers to measure each polarization of photons he receives.

He can use the(+)basis or the (×) basis but not both simultaneously.

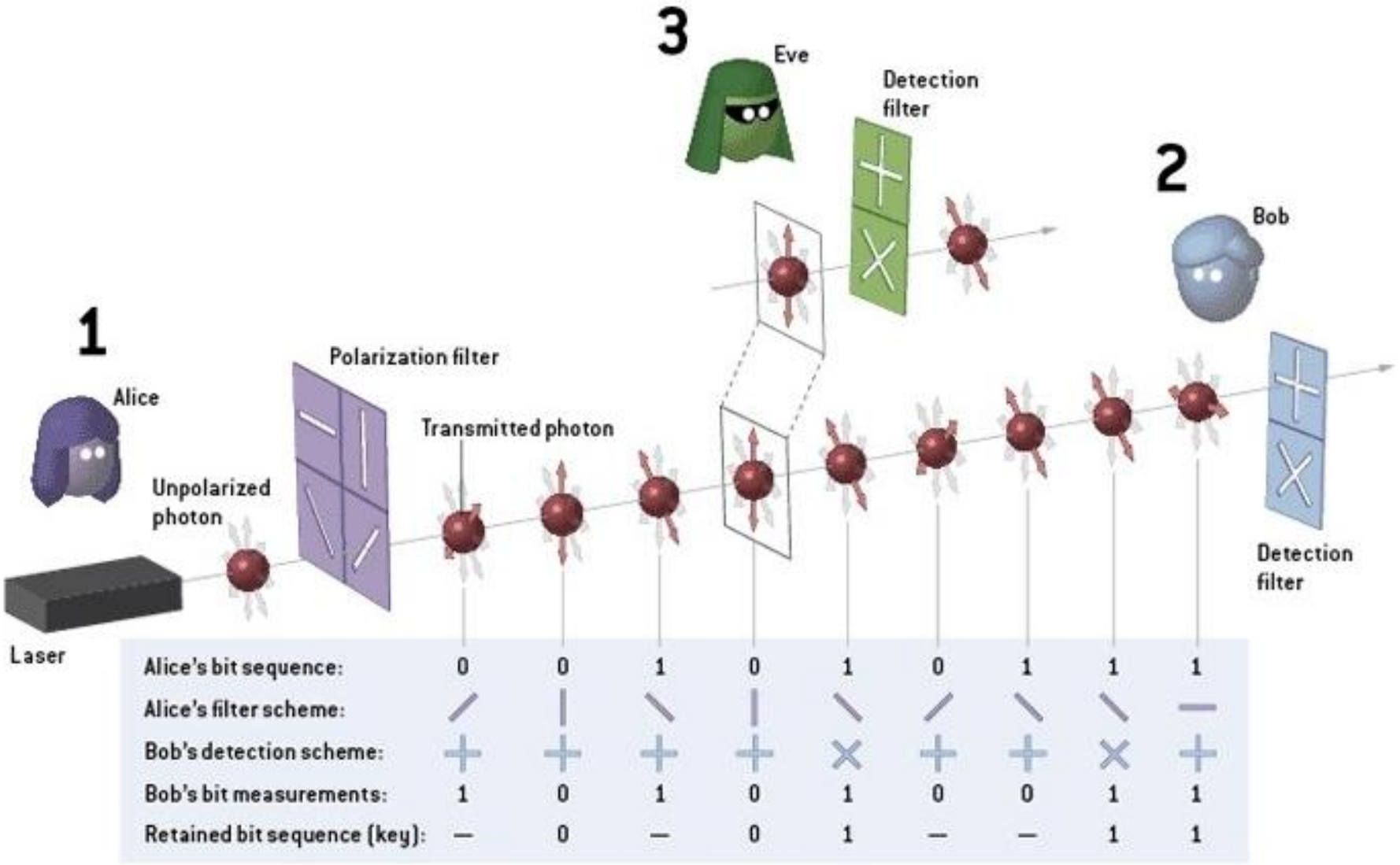
QKD Protocols

- A security protocol is a special protocol designed to ensure security properties are met during communications.
- There are three main security protocols for QKD: BB84, B92, and Entanglement-Based QKD.
- We will only discuss BB84 here.

QKD Protocols: (BB84)

- BB84 was the first security protocol implementing Quantum Key Distribution.
- BB84 invented by Charles Bennett and Gilles Brassard during 1980s
- It uses the idea of photon polarization.
- The key consists of bits that will be transmitted as photons.
- Each bit is encoded with a random polarization basis!

Example of Key Distribution



QKD (BB84)

1- To begin creating a key, Alice sends a photon through either the 0 or 1 slot of the rectilinear or diagonal polarizing filters, while making a record of the various orientations.

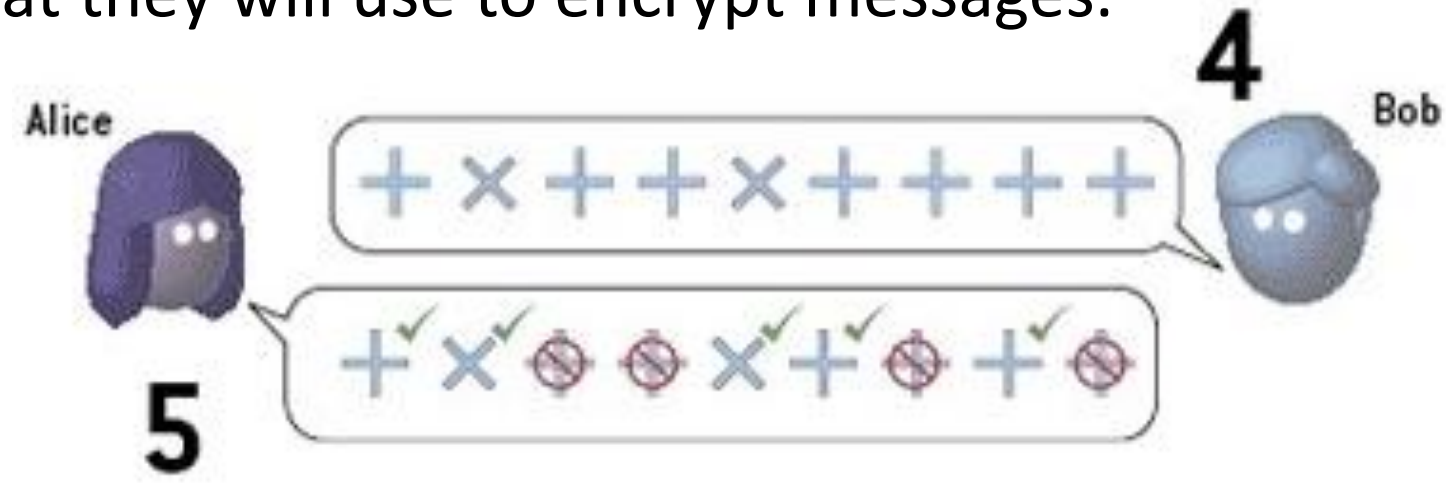
2- For each incoming bit, Bob chooses randomly which filter slot he uses for detection and writes down both the polarization and the bit value.

3- If Eve the eavesdropper tries to spy on the train of photons, quantum mechanics prohibits her from using both filters to detect the orientation of a photon. If she chooses the wrong filter, she may create errors by modifying their polarization.

QKD (BB84)

4- After all the photons have reached Bob, he tells Alice over a public channel, perhaps by telephone or an e-mail, the sequence of filters he used for the incoming photons, but not the value of the photons.

5- Alice tells Bob during the same conversation which filters he chose correctly. Those instances constitute the bits that Alice and Bob will use to form the key that they will use to encrypt messages.



BB84 with eavesdropping

- **If an eavesdropper Eve tries to tap the channel,** this will automatically show up in Bob's measurements.

- As Eve intercepts Alice's photons, **she has to measure them** with a random basis and send new photons to Bob.`

- The photon states cannot be cloned **(non-cloneability).**

- Eve's presence is always detected: **measuring** a quantum system **irreparably alters its state.**

The Main contribution of Quantum Cryptography.

- It solved the key distribution problem.
- Unconditionally secure key distribution method proposed by: Charles Bennett and Gilles Brassard in 1984.
- Once key is securely received it can be used to encrypt messages transmitted by conventional channels.

Conclusion

- Quantum cryptography is a major achievement in security engineering.
- Quantum cryptography obtains its fundamental security from the fact that each qubit is carried by a single photon, and each photon will be altered as soon as it is read.
- This makes impossible to intercept message without being detected.
- As it gets implemented, it will allow perfectly secure bank transactions, secret discussions for government officials, and well-guarded trade secrets for industry!

Thank you