Quantum Cryptography

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**

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

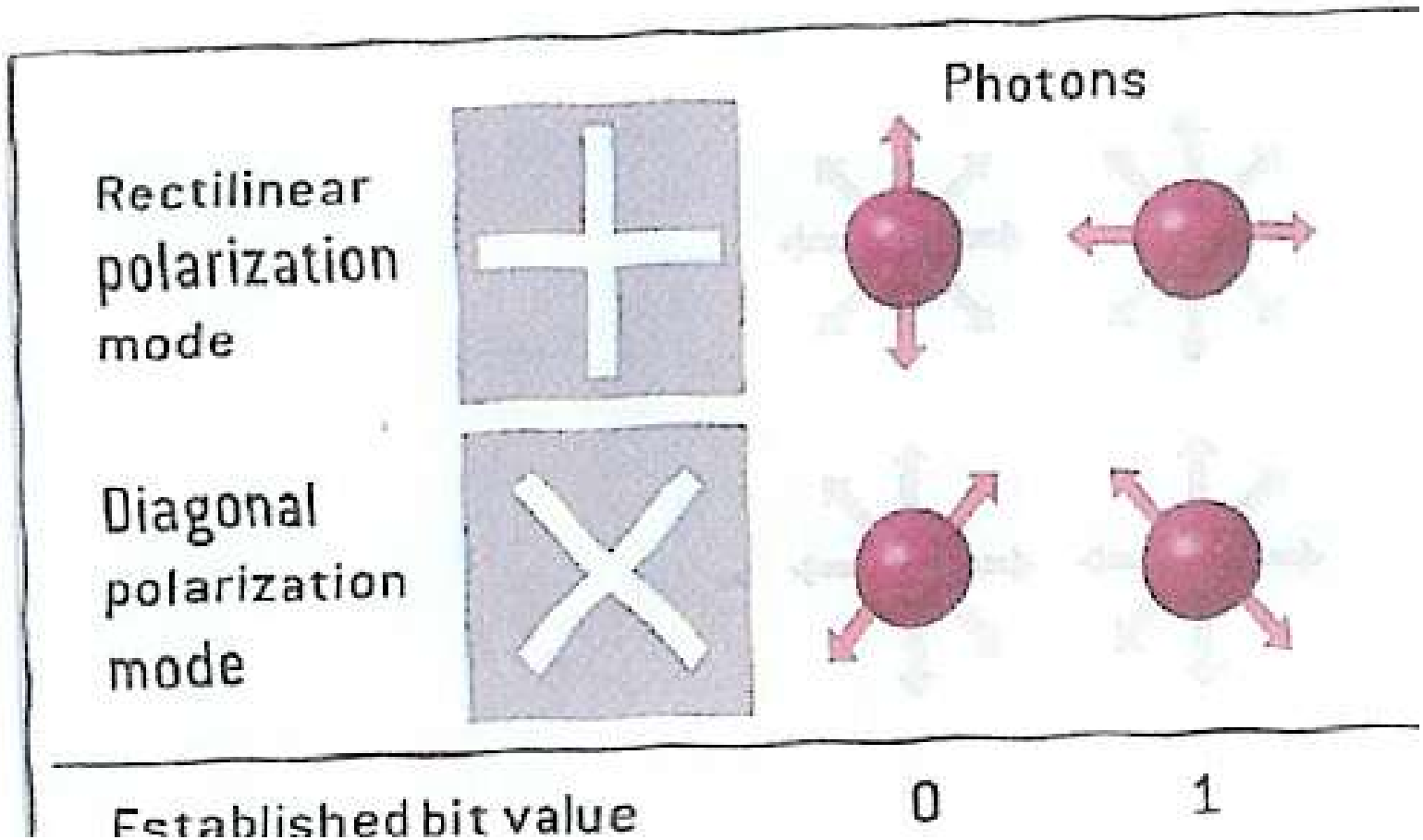
Once a quantum computer is built the RSA method would not be safe.

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

  a photon may pass through it or may not.
- We can use a detector to check of a photon has passed through a filter.

Photon polarization



Heisenberg Uncertainty Principle

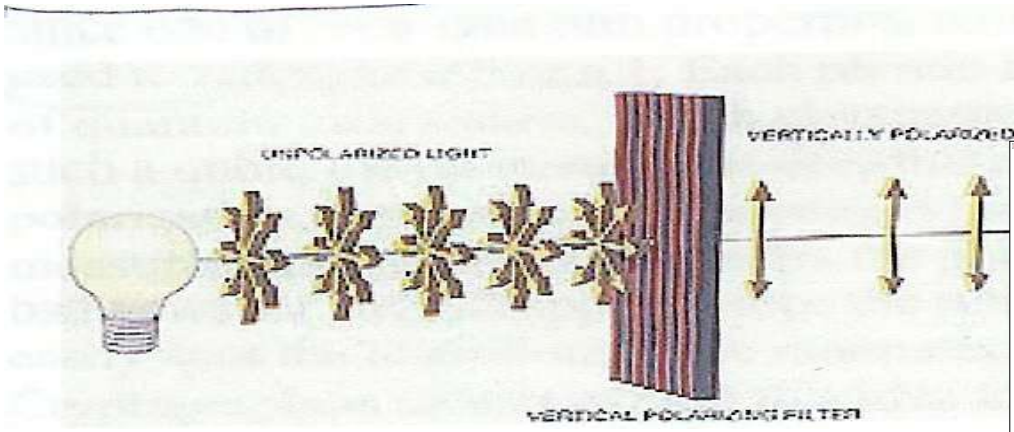
- Certain pairs of physical properties are related in such a way that measuring one property prevents the observer from knowing the value of the other.

  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



Vertical filter

Tilted filter at the angle θ

The probability of a photon appearing after the second filter depends on the angle θ and becomes 0 at θ = 90 degrees.

The first filter <u>randomizes</u> the measurements of the second filter.

Polarization by a filter

- A pair of orthogonal filters such as vertical/horizontal is called a basis.
- A pair of bases is conjugate if the measurement in the first basis completely randomizes the measurements in the second basis.
- As in the previous slide example for θ =45deg.

Sender-receiver of photons

- Suppose Alice uses 0-deg/90-deg polarizer sending photons to Bob. But she does not reveal which.
- Bob can determine photons by using filter aligned to the same basis.
- But if he uses 45deg/135 deg polarizer to measure the photon he will not be able to determine any information about the initial polarization of the photon.
- The result of his measurement will be completely random

Eavesdropper Eve

- If Eve uses the filter aligned with Alice's she can recover the original polarization of the photon.
- If she uses the misaligned filter she will receive no information about the photon .
- Also she will influence the original photon and be unable to retransmit it with the original polarization.
- Bob will be able to deduce Ave's presence.

Binary information

- Each photon carries one **qubit** of information
- Polarization can be used to represent a 0 or 1.
- In quantum computation this is called

  qubit.

To determine photon's polarization the recipient must measure the polarization by ,for example, passing it through a filter.

Binary information

- 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.

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.
- The method is called BB84.
- Once key is securely received it can be used to encrypt messages transmitted

  by conventional channels.

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.

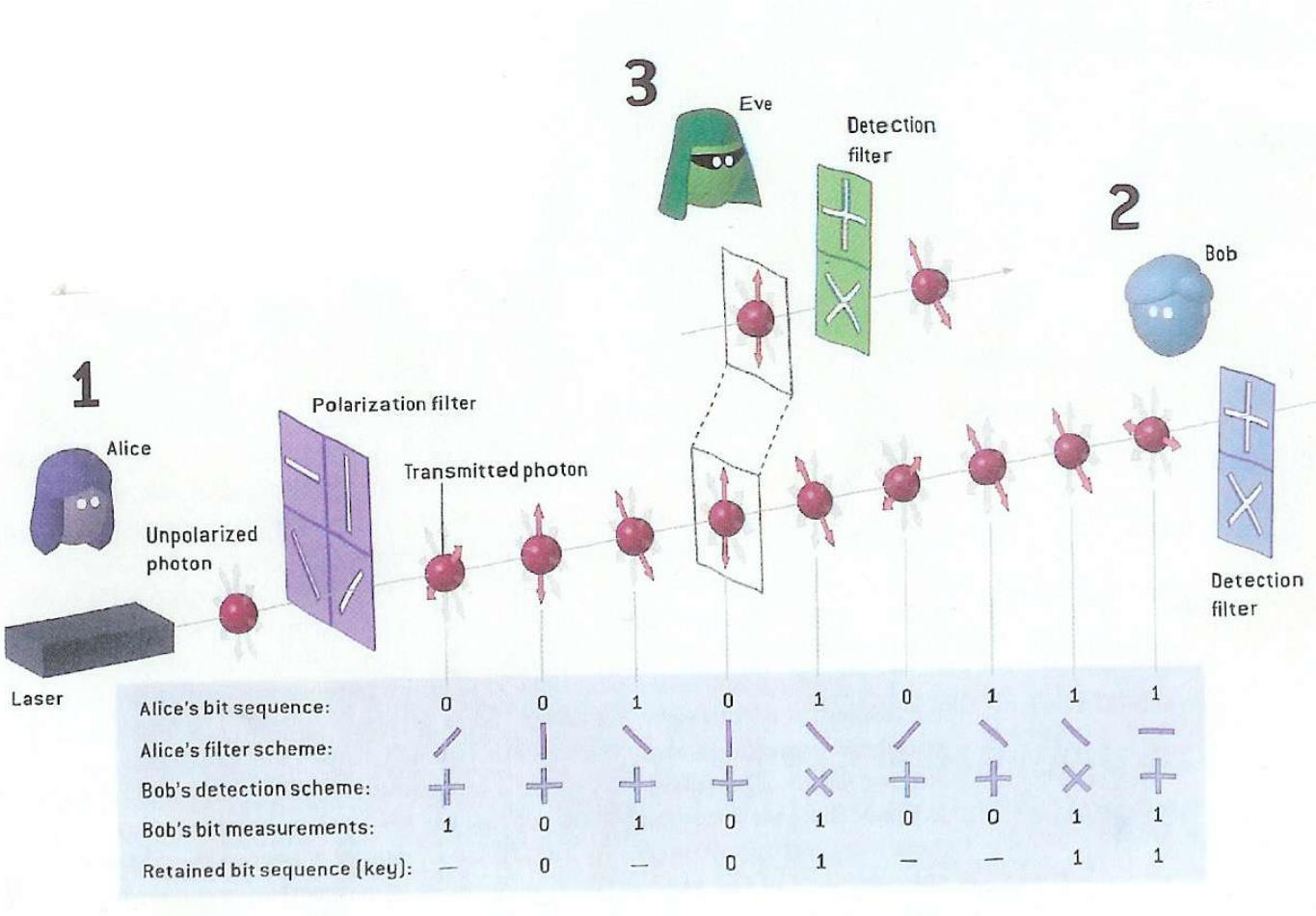
Quantum key distribution

- 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 (×) but not both simultaneously.

Example of key distribution



Security of quantum key distribution

- 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.

Noise

- The presence of noise can impact detecting attacks.
- Eavesdropper and noise on the quantum channel are indistinguishable.
- (1) Malicious eavesdropper can prevent communication.
- (2) Detecting eavesdropper in the presence of noise is hard.

State of the Quantum Cryptography technology.

- Experimental implementations have existed since 1990.
- Current (2004) QC is performed over distances of 30-40 kilometers using optical fiber.

In general we need two capabilities.

(1) Single photon gun.

(2) Being able to measure single photons.

State of the QC technology.

- Efforts are being made to use **Pulsed Laser Beam** with low intensity for firing single photons.
- Detecting and measuring photons is hard.
- The most common method is exploiting **Avalanche Photodiodes in the Geiger mode** where single photon triggers a detectable electron avalanche.

State of the QC technology.

- Key transmissions can be achieved for about 80 km distance (Univ of Geneva 2001).
- (2)For longer distances we can use repeaters. But practical repeaters are a long way in the future.
- Another option is using satellites.
- Richard Hughes at LOS ALAMOS NAT LAB (USA) works in this direction.
- The satellites distance from earth is in hundreds of kilometers.

NIST System

- Uses an infrared laser to generate photons
- and telescopes with 8-inch mirrors to send and receive photons over the air.
- Using the quantum transmitted key

  messages were encrypted at the rate

  1 million bits per second.

The speed was impressive but the distance between two NIST buildings was only 730 meters.

Commercial QC providers

- **id Quantique**, Geneva Switzerland
- Optical fiber based system
- Tens of kilometers distances
- **MagiQ Technologies, NY City**
- Optical fiber-glass
- Up to 100 kilometers distances
- **NEC Tokyo** 150 kilometers
- **QinetiQ** Farnborough, England
- Through the air 10 kilometers.
- Supplied system to BBN in Cambridge Mass.