Quantum Cryptography

Umesh V. Vazirani

CS 161/194-1

November 28, 2005

Why Quantum Cryptography?

- Unconditional security

  - Quantum computers can solve certain tasks exponentially faster; including quantum factoring algorithm.
  - you can learn more about this in cs191.

- Measurement disturbs quantum state

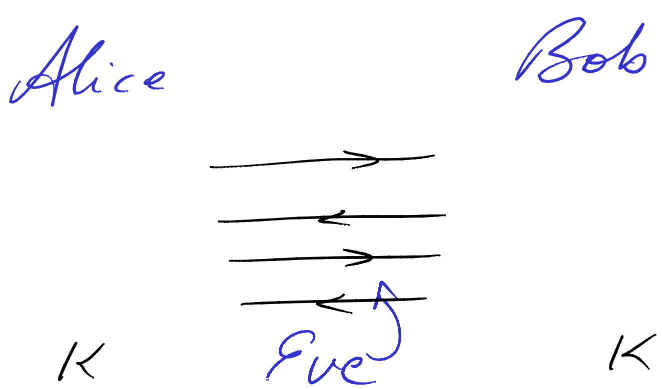
  - detecting eavesdropper

Quantum Mechanics

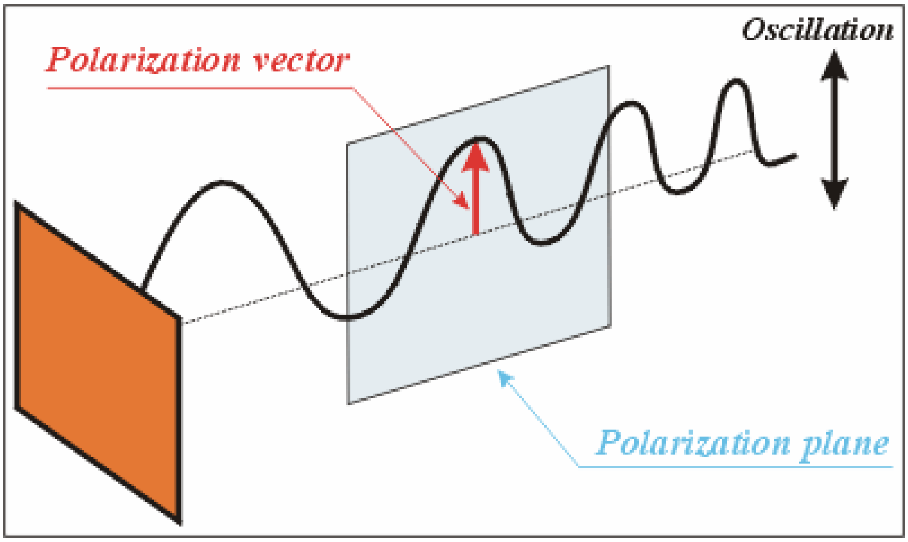
I think I can safely say that nobody understands quantum Mechanics.

-Richard Feynman

antum Ke Distribution.



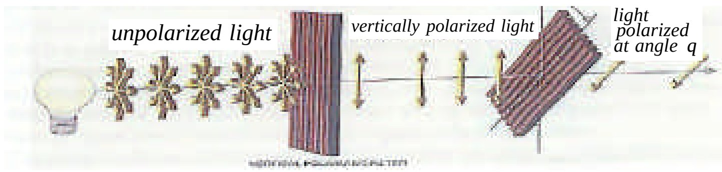
Polarization of Light



Photon Polarization

- **Light waves are propagated as discrete quanta called photons.**
- **The polarization of the photon is a direction in the plane normal to the direction of propagation.**
- **A polarizing filter blocks photons** whose polarization is perpendicular to the orientation of the filter and transmits photons whose polarization is aligned with the filter.

Photon Polarization

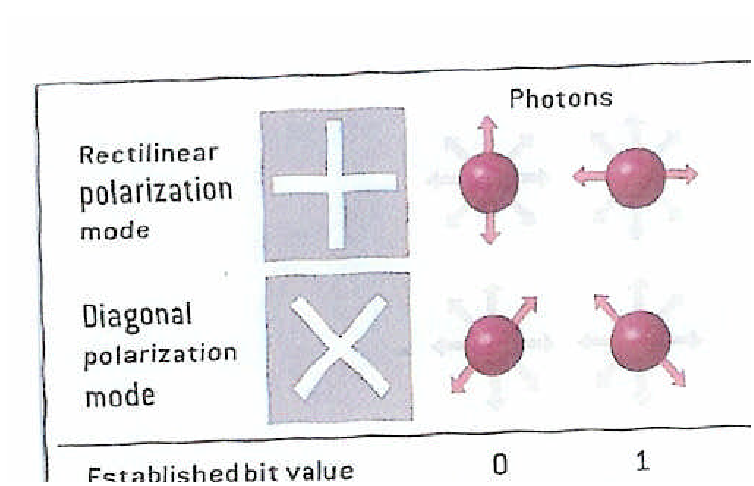


Vertical filter

Filter at angle q

The probability that the photon is transmitted by the second filter is $\cos^2 q$

Photon polarization



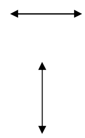
Transmitting a Bit

Rectilinear Polarization:

Alice

0

1



Bob

Vertical filter

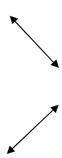
Transmitting a Bit

Diagonal Polarization:

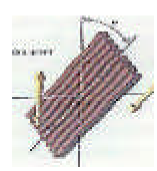
Alice

0

1



Bob



filter at 45^{o}

Transmitting a Bit

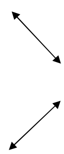
Diagonal Polarization:

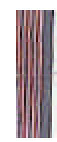
Alice

Bob

0

1





Vertical filter

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.
- Rectilinear and diagonal polarization constitute exactly such a pair of properties.

What does Eve learn?

Alice | Eve | Bob

0 ↔

1 ↕

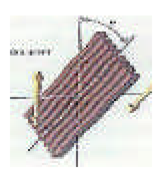
Vertical filter

What does Eve learn?

Alice | Eve | Bob

0 ↔

1 ↕



filter at 45^{o}

- Eve has a 50-50 chance of learning the bit
- If Eve chooses the wrong orientation for the filter, she learns no information about the bit. Moreover, she disturbs the state of the photon, and cannot retransmit it with original orientation.

BB84 Protocol for Key Distribution

Repeat 4N times:

Bennett & Brassard 1984

Alice picks a random bit b.

She transmits it to Bob randomly selecting rectilinear or diagonal polarization.

Bob measures the photon randomly selecting a vertical or diagonal filter.

Alice and Bob announce their respective choices – rectilinear or diagonal. Discard bit if choices different.

Alice ends up with about 2N bits $a_1a_2...a_{2N}$ and Bob with $b_1b_2...b_{2N}$. They select N positions at random and check that $a_i=b_i$. The remaining N bits are the secret key.

Security of BB84

- Since Eve does not know the correct orientation (rectilinear or diagonal), she cannot measure the polarization without disturbing it.
- So if the test for equality on N randomly chosen positions is passed, Alice and Bob can be confident there is no eavesdropper.
- The proof of unconditional security based on the axioms of quantum mechanics is difficult and dates back to about 2000.

Practical Considerations

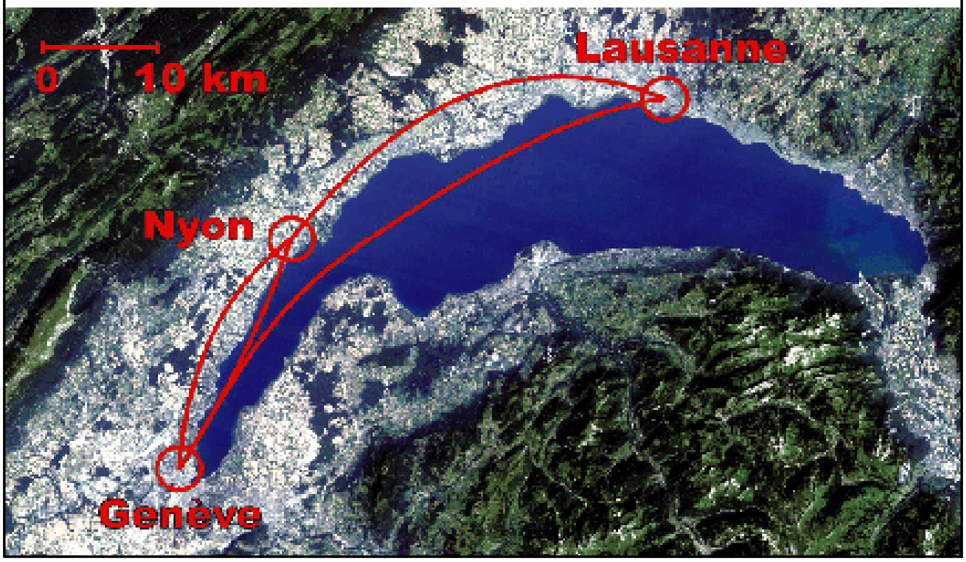
- Imperfect measurements, channel noise
  - $a_1a_2 \ldots a_{2N}$ and $b_1b_2 \ldots b_{2N}$ do not agree.
  - Alice and Bob exchange parity bits to correct their mismatches.
- Can only guarantee that Eve does not know too many bits out of the remaining N.
  - If Eve knows only 5% of the bits, then Alice and Bob hash the N bits down to .9N bits. Now Eve has practically no information about these .9N bits.

Practical Considerations

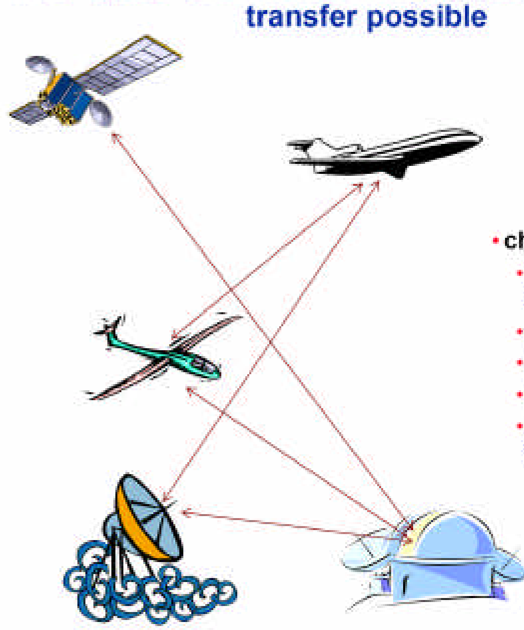
- Imperfect measurements, channel noise
  - $a_1a_2 \ldots a_{2N}$ and $b_1b_2 \ldots b_{2N}$ do not agree.
  - Alice and Bob exchange parity bits to correct their mismatches.
- Can only guarantee that Eve does not know too many bits out of the remaining N.

Example: Alice and Bob share bits a,b,c,d
Eve know one of these bits.
Alice and Bob extract key $a \oplus b, a \oplus c, a \oplus d$
The 3 bits of the key look random to Eve.

QKD over 64 Km Optical Fibre



Free-space QKD makes many types of secure key transfer possible



- challenges
  - photon production, transmission and detection
  - atmospheric optics
  - background photons
  - timing and synchronization
  - pointing, acquisition and tracking

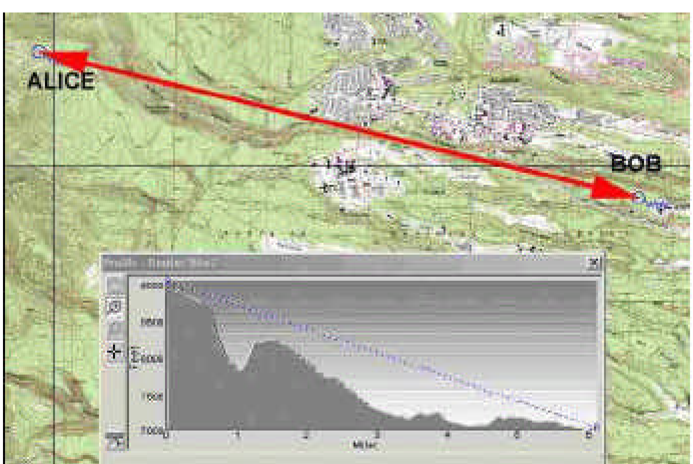
Los Alamos

Atmospheric photon transmission and detection

Challenge:

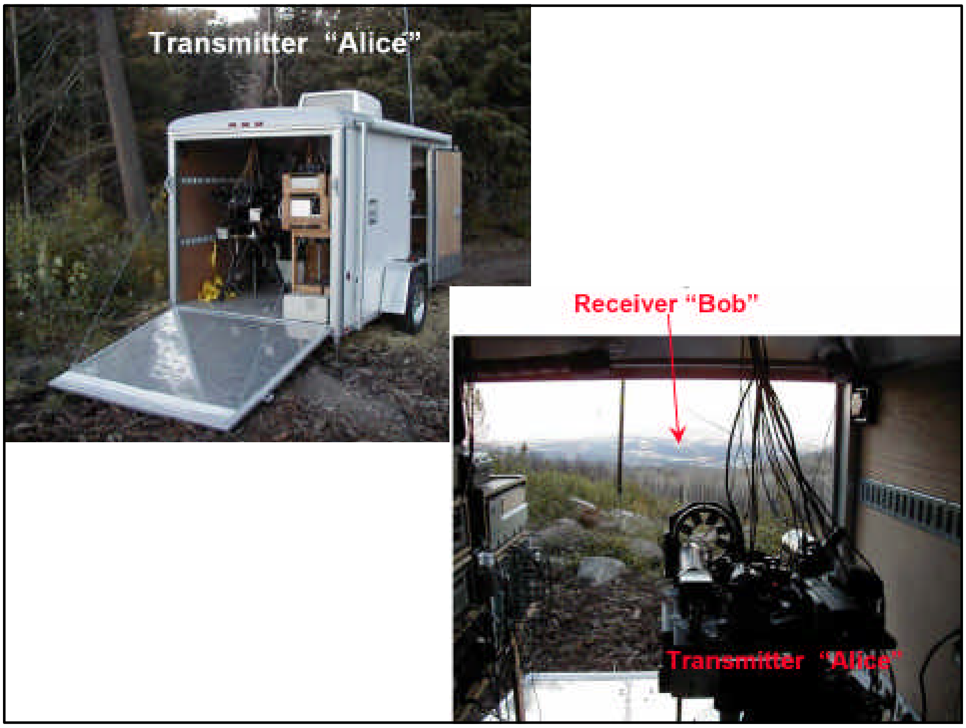
- Background photons
- daylight radiance = 10^{13} photons/s cm^2 A
  - temporal filtering: 1 ns
  - spectral filtering: .1 nm
  - spatial filtering: 220 *mrad*
- Night radiance = 10^5 photons/s cm2 A

10 km free-space QKD



From Pajarito Mtn., Los Alamos, NM to TA53, Los Alamos National Laboratory

Richard J. Hughes



Commercial Availability…

id Quantique

QKD is:

- Unconditionally secure.
- Implementable using current technology
- Early systems are commercially available.

But…

- It is not public-key cryptography.
- Currently very slow bit rates available. About 1KHz key rate.
- Distance limitations.
- Eve can jam the quantum channel.