

Quantum cryptography

Optical fibers to carry information

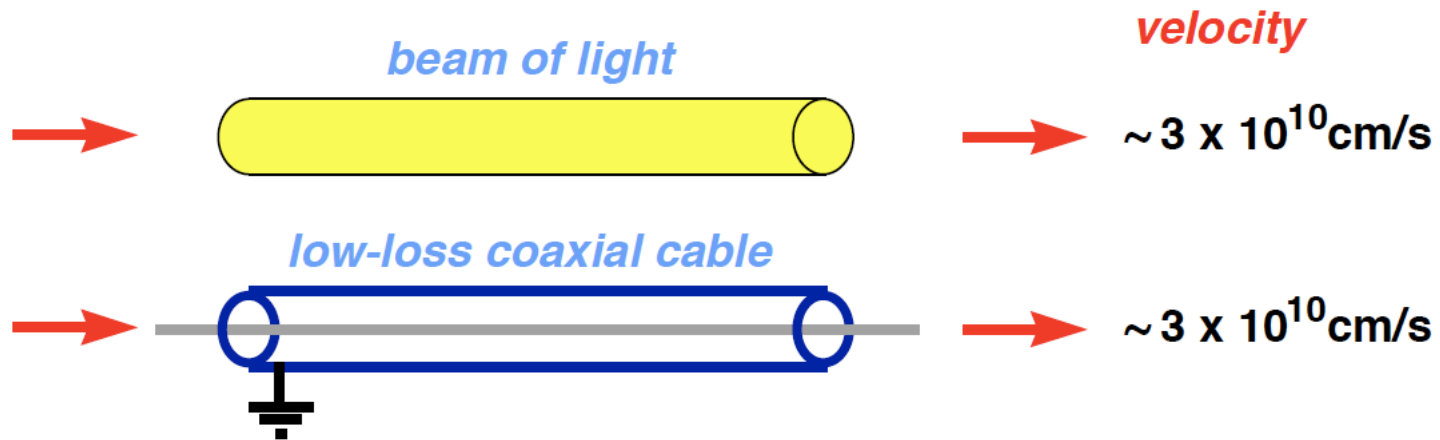


10 Kb/s



1Tb/s
 10^{12} b/s

Optical fibers vs electrical cables

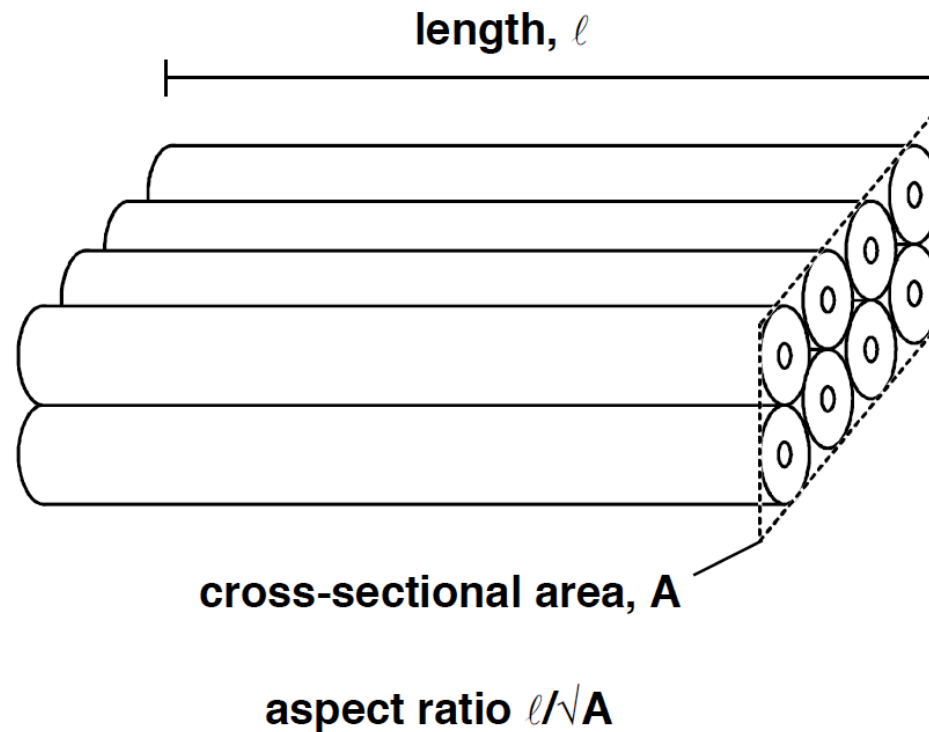


Frequency: 10^8 Hz vs 10^{15} Hz

Bit rate for electrical interconnections

$$B \propto B_0 \frac{A}{l^2}$$

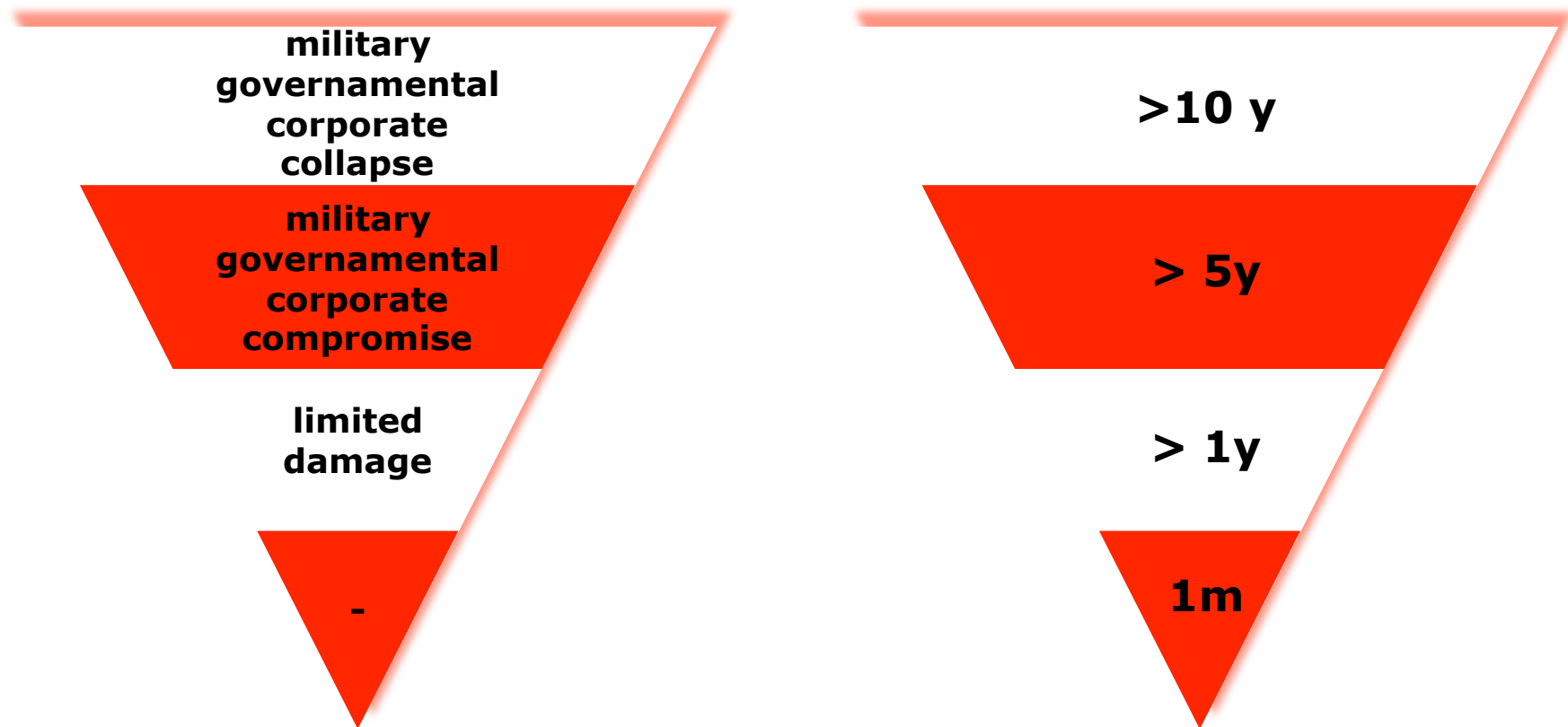
$$B_0 \approx 10^{15} \text{ bit} / \text{s}$$



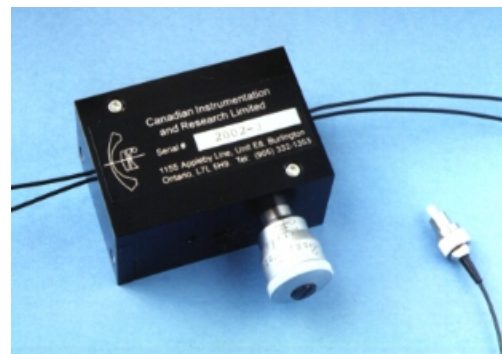
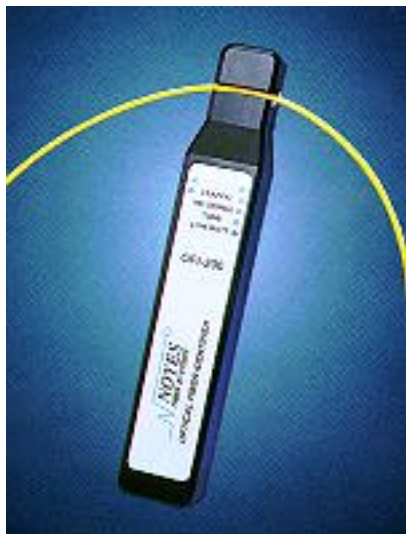
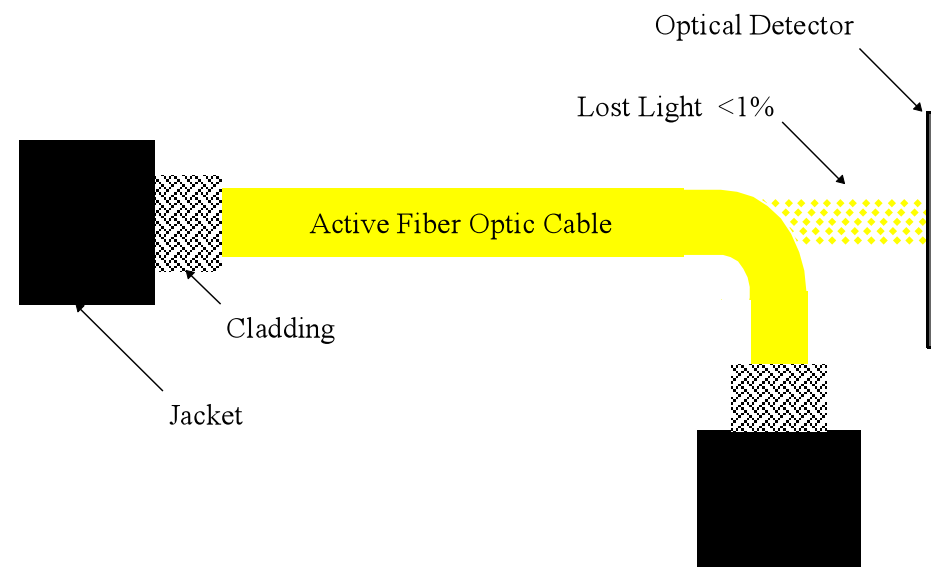
Problema: Tizio abita in Europa e per telefonare al suo amico Caio in America spende circa 0.1 €/minuto. Sapendo che la telefonata occupa una banda di circa 10kb/s, calcolare il ricavo di Sempronio, proprietario di una fibra da 1Tb/s posata nel fondo dell'oceano tra l'Europa e gli USA.

$$\begin{aligned} 1\text{Tb/s} &= 10^{12}\text{b/s} \\ &= 10^8 \text{ telefonate} \\ &= 10^7 \text{ € /minuto (dieci milioni al minuto!)} \\ &= 14.4 \cdot 10^9 \text{ € /giorno (quattordici miliardi al giorno!)} \end{aligned}$$

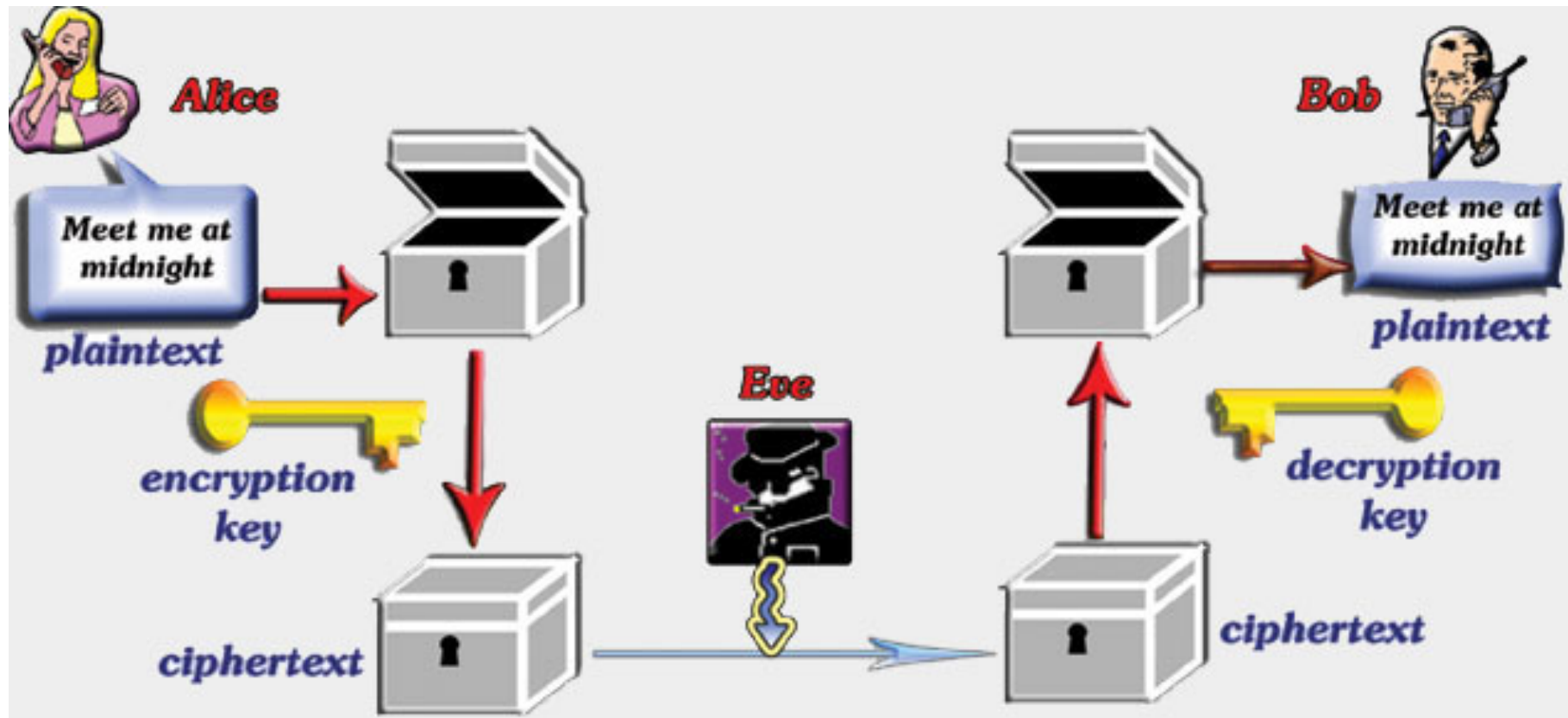
Privacy



How to tap a fiber

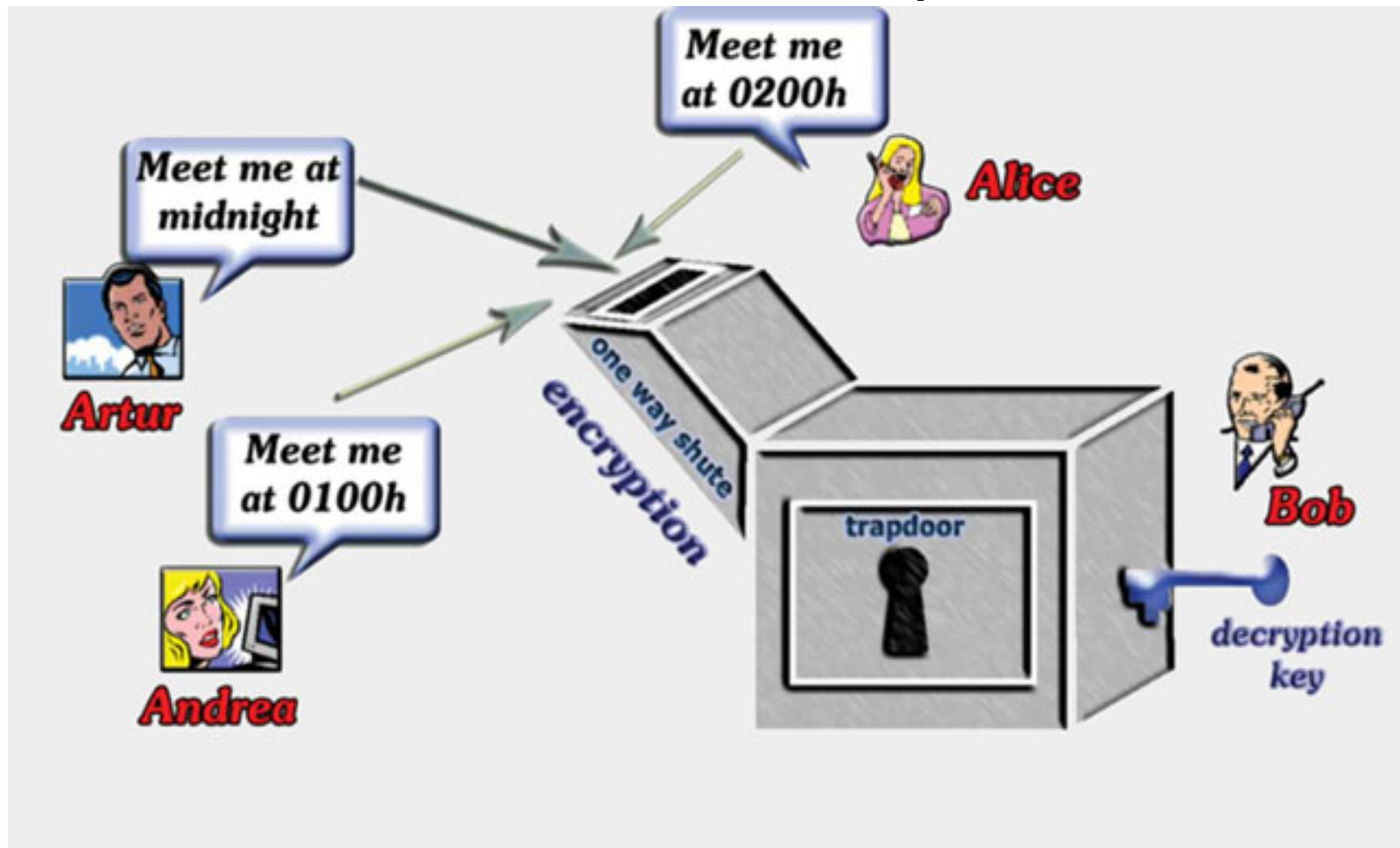


Private key cryptography (one time pad)



Secure but impractical, requires face-to-face meetings

Public key



RSA (Rivest, Shamir, Adleman):

- take two large prime numbers and multiply them to obtain $n=p \times q$
(128 o 256 bits)
- send n to Alice to encode
- to decode you will need p, q
 - only Bob knows them, **difficult for others** to retrieve

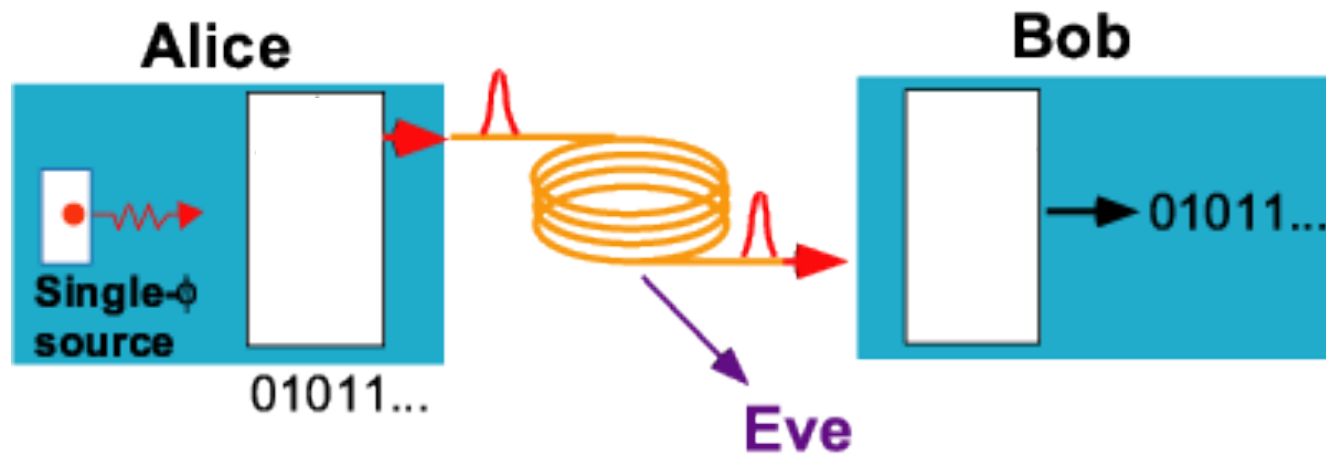
Quantum cryptography

How to distribute a private key through a public network

$$\begin{array}{c} \text{Quantum key distribution} \\ + \\ \text{Private key cryptography} \\ = \\ \text{Secure communication} \end{array}$$

Single photons

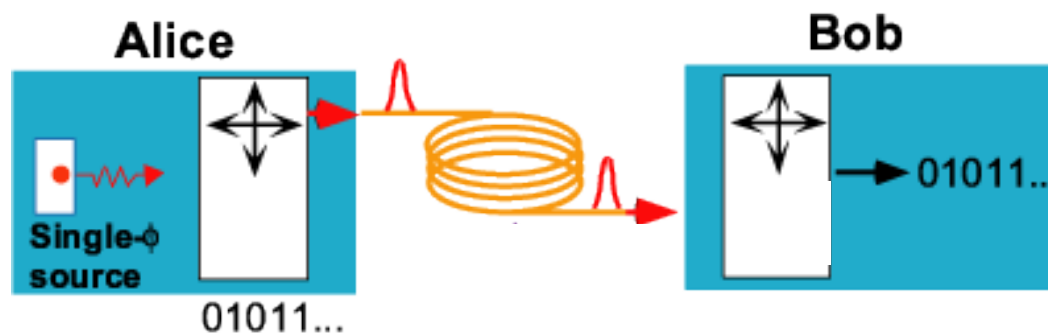
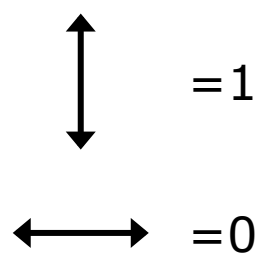
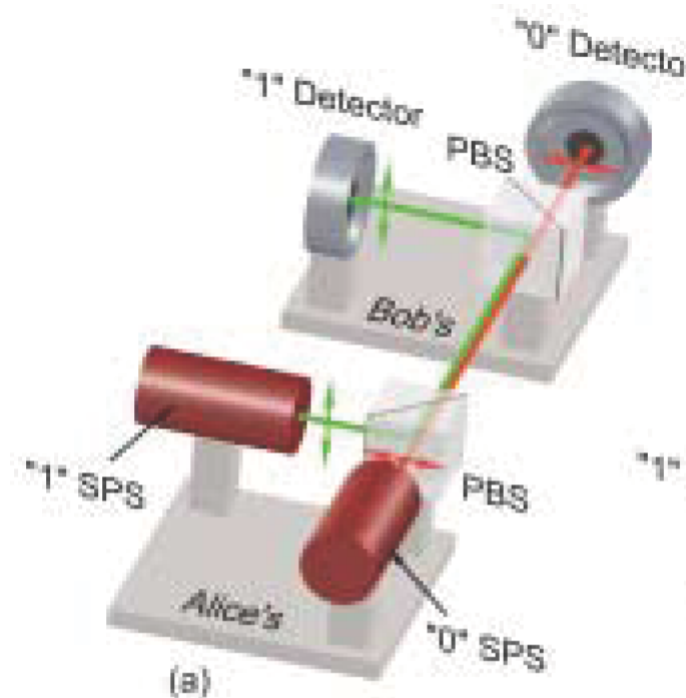
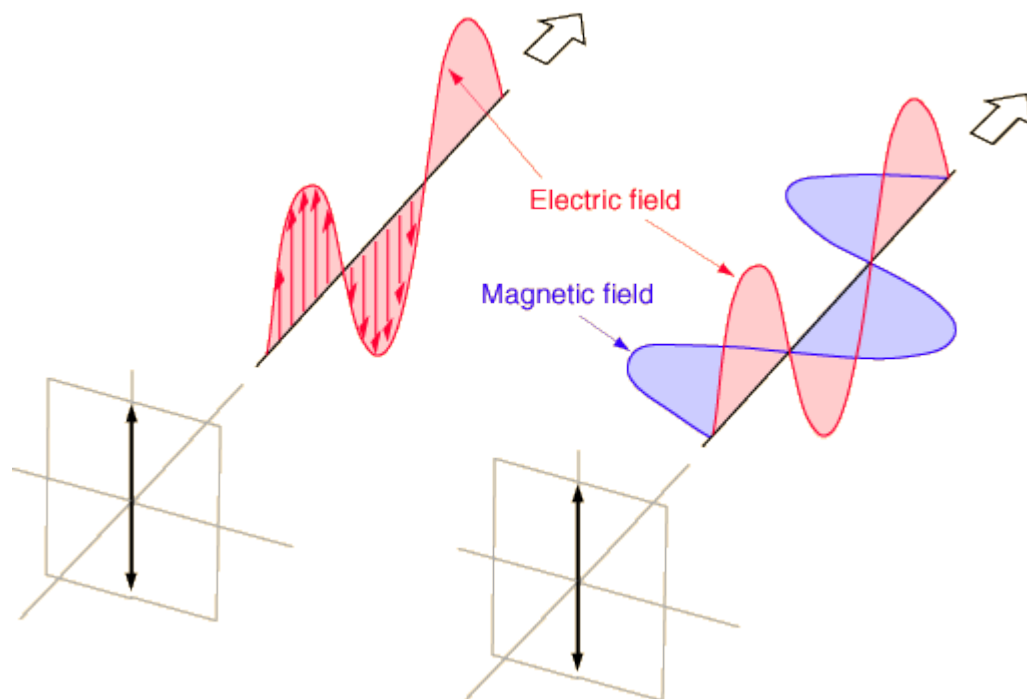
Alice sends one photon at time



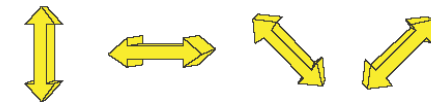
No split photon attack!

Fotoni e bit

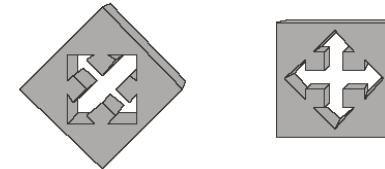
L'informazione è codificata nella direzione di polarizzazione



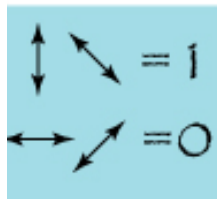
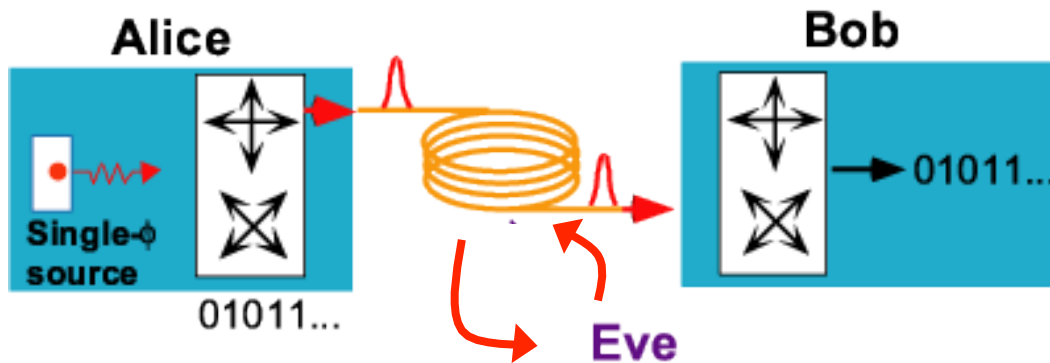
How to confuse Eve



Linear polarization states

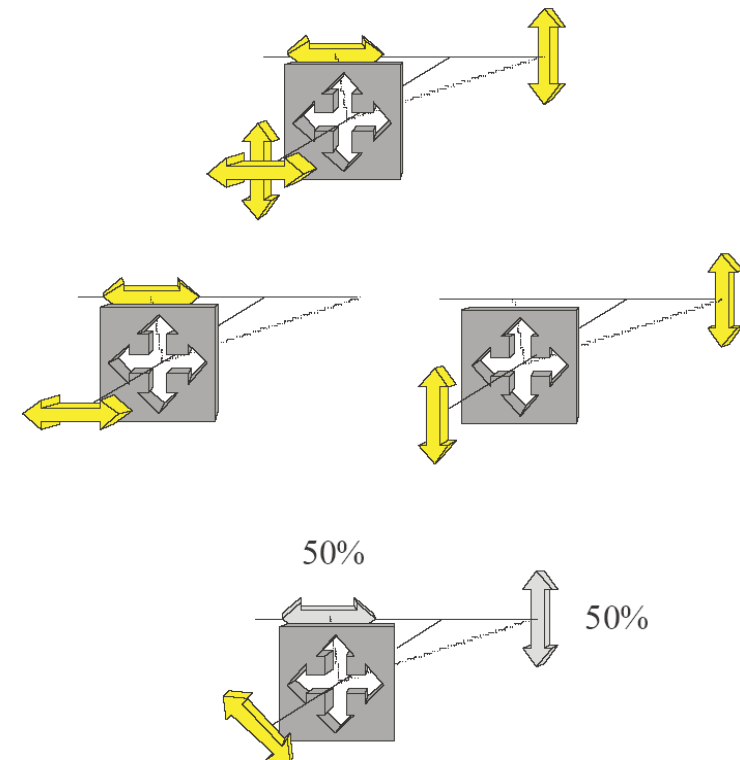


Filters



$$|\vartheta\rangle = \cos \vartheta |\uparrow\rangle + \sin \vartheta |\leftrightarrow\rangle$$

$$P_{\uparrow} = |\langle \vartheta | \uparrow \rangle|^2 = \cos^2 \vartheta$$



How to confuse Eve

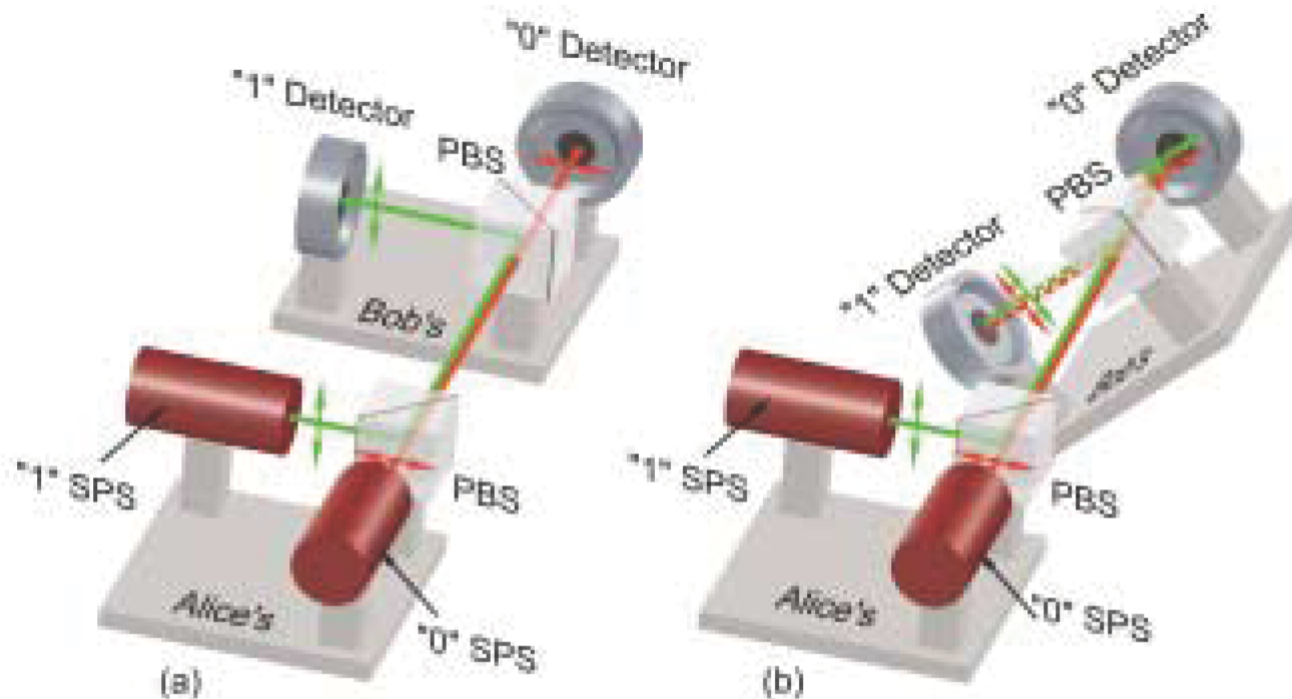


Figure 1. Alice can reliably communicate bit values to Bob only if they use the same basis for setting and measuring polarization state, as in (a). In this case, a horizontally polarized photon emitted by Alice's "0" single-photon source (SPS) is reliably directed to Bob's "0" detector, and similarly for a vertically polarized photon representing a "1." If Bob does not use the same basis as Alice, as in (b), then for a photon of either polarization, there is a non-zero probability that it will be directed to the wrong detector.

No cloning

Cannot copy an unknown quantum state without modifying it

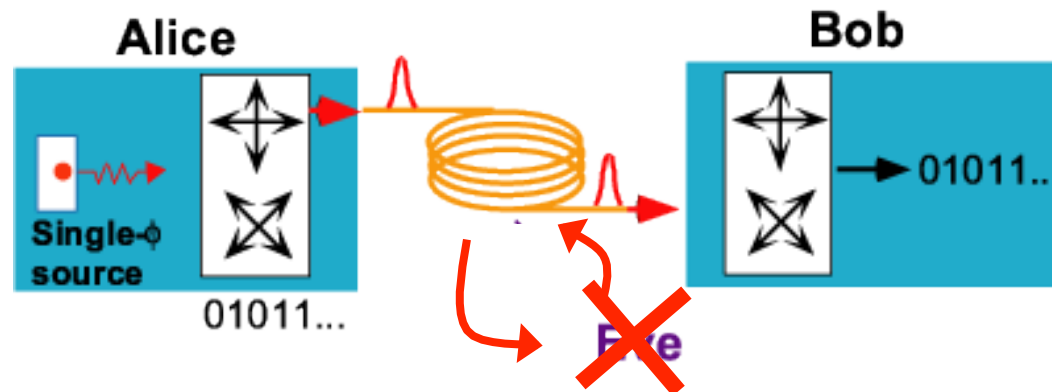
$$|\vartheta\rangle \otimes |\alpha\rangle$$

$$U(|\vartheta\rangle \otimes |\alpha\rangle) = |\vartheta\rangle \otimes |\vartheta\rangle$$

$$U(|\phi\rangle \otimes |\alpha\rangle) = |\phi\rangle \otimes |\phi\rangle$$

$$(\langle\phi| \otimes \langle\alpha|)U^\dagger = \langle\phi| \otimes \langle\phi|$$

























$$\langle\vartheta|\phi\rangle = (\langle\vartheta|\phi\rangle)^2 \Rightarrow |\vartheta\rangle = |\phi\rangle; |\vartheta\rangle \perp |\phi\rangle$$



BB84 protocol



Gilles Brassard (left) and Charles Bennett laid the foundations of quantum cryptography.

Emitter bit value	0	1	1	0	1	0	0	1
Emitter photon source								
<hr/>								
Receiver filter orientation								
Receiver photon detector								
Receiver bit value	1	1	0	0	1	0	0	1
<hr/>								
Sifted key	-	1	-	0	1	-	0	-

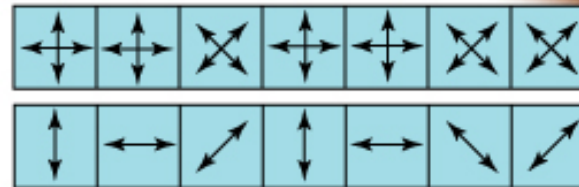
BB84 protocol



Alice sends photons using
A secret basis

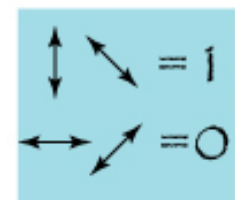
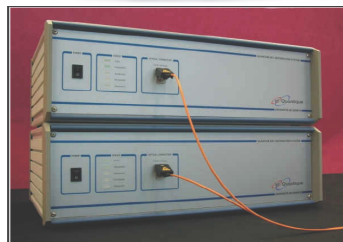


Bob uses a random detector
orientation to measure the
photons. He only gets some
correct.



Alice indicates to Bob what measurements will
be correct. These become the new key.

Bob phones Alice and tells
her over a public channel what
basis he used.



Error correction

Random deletion of photons:

- Absorption or scattering of the photons as they propagate from Alice to Bob
- Inefficient light collection so that some of the photons miss the detectors
- Detector inefficiency

No problem
Check detection timing

Birefringence

- polarization turns in random way during transmission
- same effect as eavesdropper

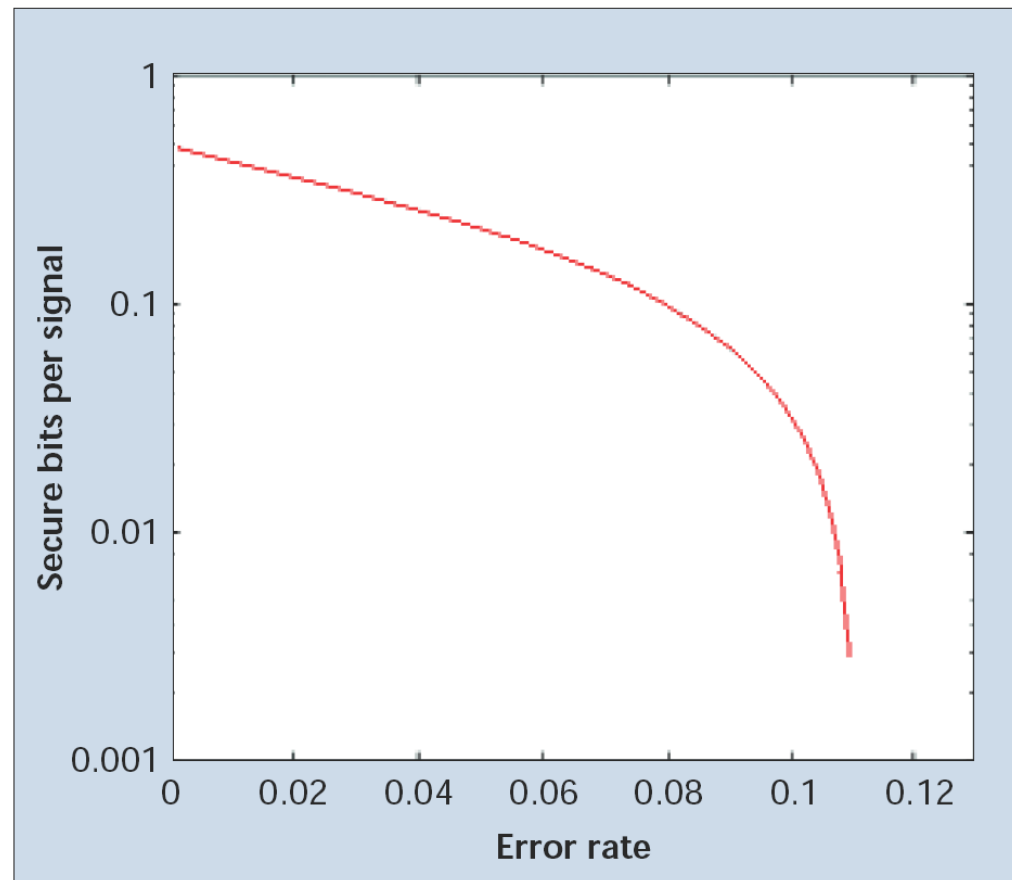
Keep small
Bundle bits

Errors and bit rate

$$N_{correction} = N \left[-\varepsilon \log_2 \varepsilon - (1 - \varepsilon) \log_2 (1 - \varepsilon) \right]$$

ε error probability, N number of bits

ε needs to be smaller than error introduced by Eve (0.25)



Identity verification

Man in the middle attack:

Eve pretends to be Bob, then sends Alice's message to Bob

Need to check Bob's identity carefully

Need a first face-by-face encounter to establish the first confidential key
(after that use it to establish Bob's ID and start quantum cryptography)

Single photon sources

- Make sure no more than 1 photon is in each pulse: $P(n>1) \ll P(n=1)$
($n>1$ decreases the error rate introduced by Eve)
- Attenuated coherent pulses from a laser
(low mean number of photons to keep $P(n>1)$ low)
- Best choice is genuine single photon guns

Free-space quantum cryptography

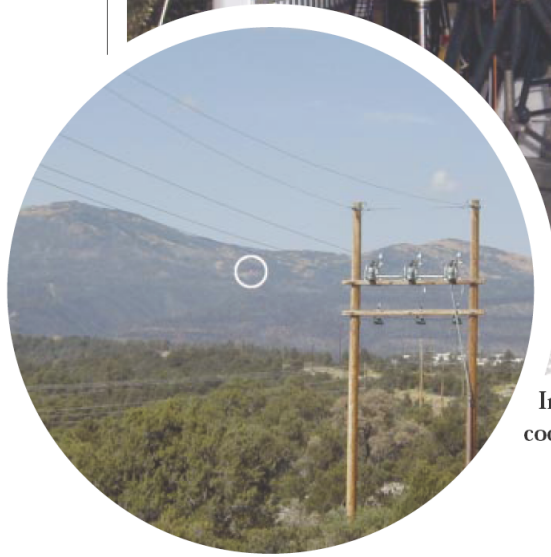
- Range 20 km
- Use telescopes to avoid diffraction
- Wavelength 600-900nm (low atmospheric losses, good detectors)
- Goal to communicate with satellites in low earth orbits.

Issues:

- Air turbulence
minimize with reference laser beam + adaptive optics)
- Stray light (sun, lamps...)
Minimize with spectral and temporal filters

Free-space quantum cryptography

LANL



In the air: Richard Hughes has sent a photon-encrypted code from a laser source (circled, inset) to a receiver.

Quantum cryptography in optical fibers

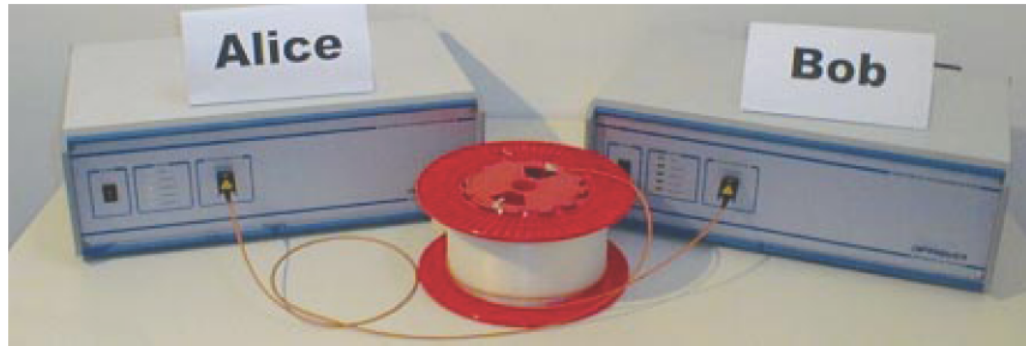
Features:

- Low losses
- No diffraction
- Widespread infrastructure
- Wavelengths 850nm, 1300nm, 1500nm

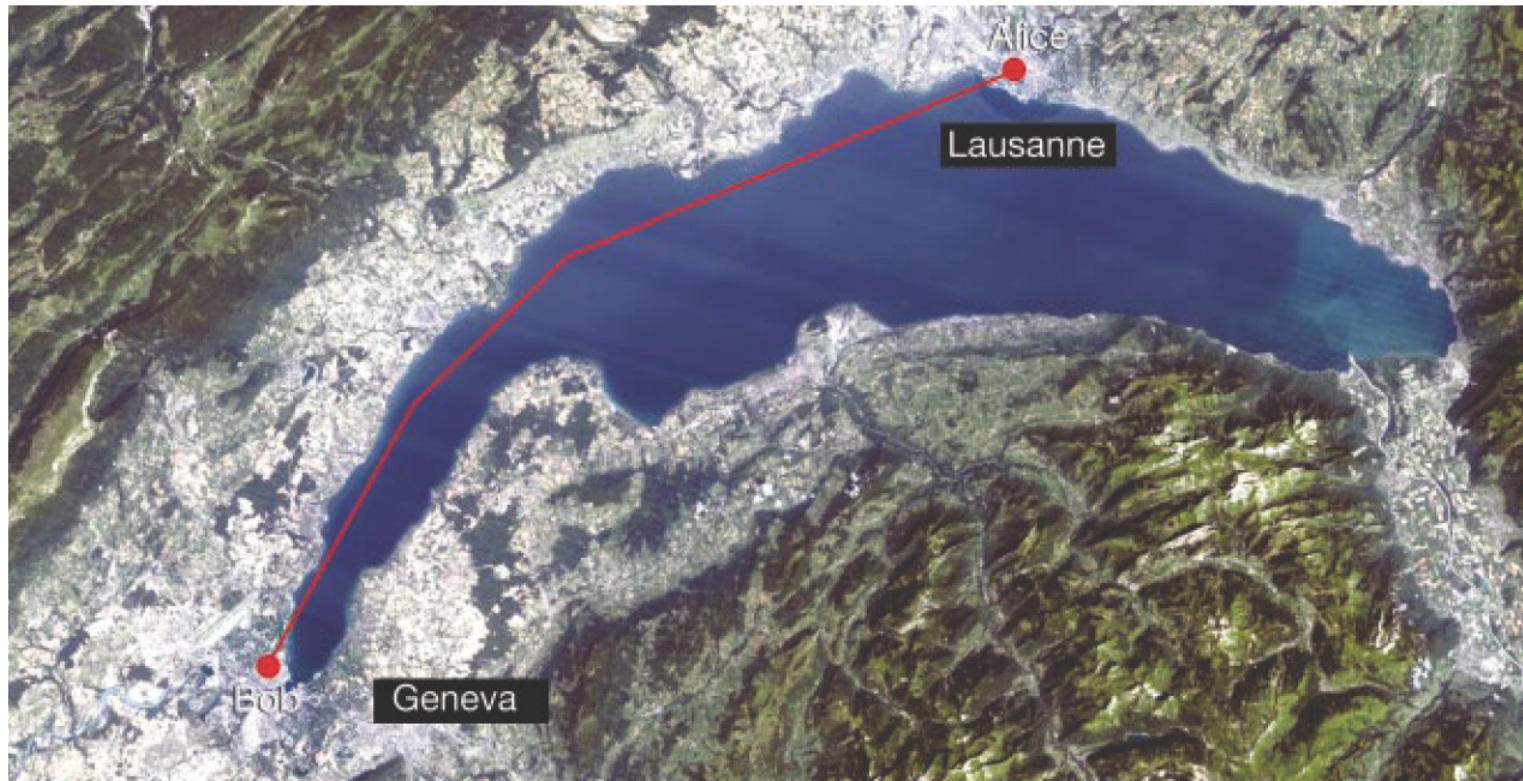
Issues:

- Optical losses
- Birefringence
- Detectors

Quantum cryptography in optical fibers



Light work: keys encoded using polarized photons have been sent between Alice and Bob (left) through 67 km of fibre-optic cable under Lake Geneva.



Exercises

1- Consider a BB84 quantum cryptography system which employs attenuated laser pulses as the source of Alice's photons.

(a) explain how Alice can produce photons with a particular polarization angle by placing suitable linear optical components after the laser.

(b) Devise a scheme for producing a stream of single photons with their polarization angles switching between angles 0° , 45° , 90° or 135° at choice by combining four such laser beams (Assume that Alice can turn the lasers on and off at will)

2- In a free space quantum cryptography experiment operating over a distance of 20 km, Alice uses a beam collimator with a diameter of 5 cm to send her photons to Bob. On the assumption that other losses are negligible, compare the fraction of the photons that are incident on Bob's detector when he uses a collection lens with a diameter of (a) 5 and (b) 25 cm.

3- In classical fiber-optic communication systems, the signals are amplified at regular intervals by repeaters to compensate for the decay in intensity due to scattering and absorption losses. Discuss whether it is possible to use repeaters to increase the range of a quantum cryptography system.