QUANTUM KEY DISTRIBUTION (QKD)

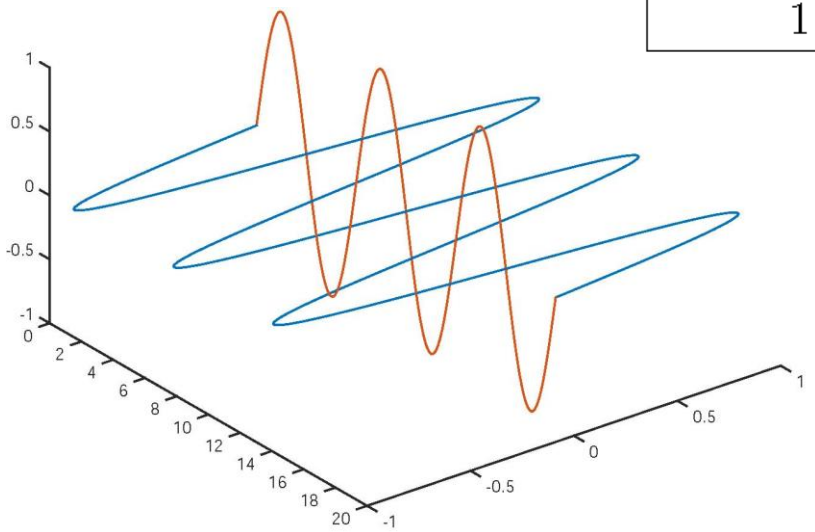
QUANTUM ENCODING

What are quantum communications?

- Use microscopic properties of light
  - Photon (quanta of light): carrier of data
- Medium is optical fiber or free space: UV or infrared
- Applications: quantum networking, distributed quantum computing and secret communications (photon detection changes its state)

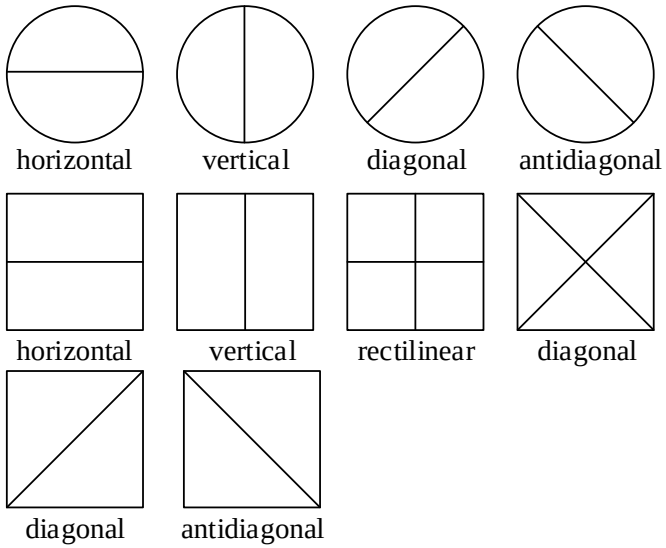
Polarization of photons

Horizontal (blue) and vertical (red)

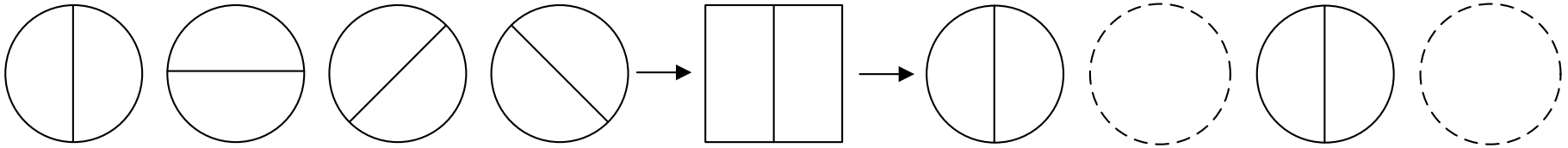


Bases, encoding and filters

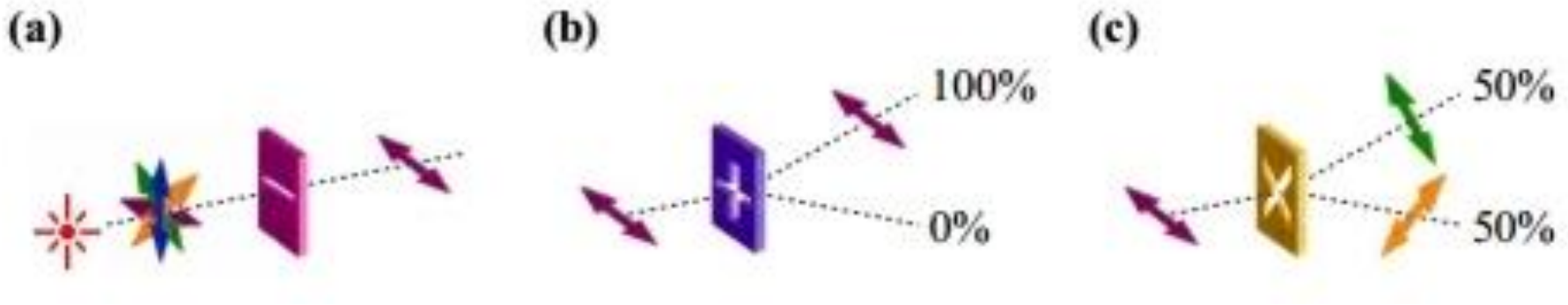
Binary value	Rectilinear basis	Diagonal basis
0	horizontal (0°)	diagonal (45°)
1	vertical (90°)	antidiagonal (135°)



Photon filtering example



Reorientation of polarity



Orthogonal vs non-orthogonal polarity

- Assuming a rectilinear filter
- Rectilinear photons are passed
- Diagonal photons are passed and reoriented
  - to vertical, with probability 50%, or
  - horizontal, with probability 50%
- Rectilinear and diagonal bases are not mutually orthogonal
- But, vertical and horizontal polarities are mutually orthogonal because there are no possible changes from one to the other

Non-cloning theorem

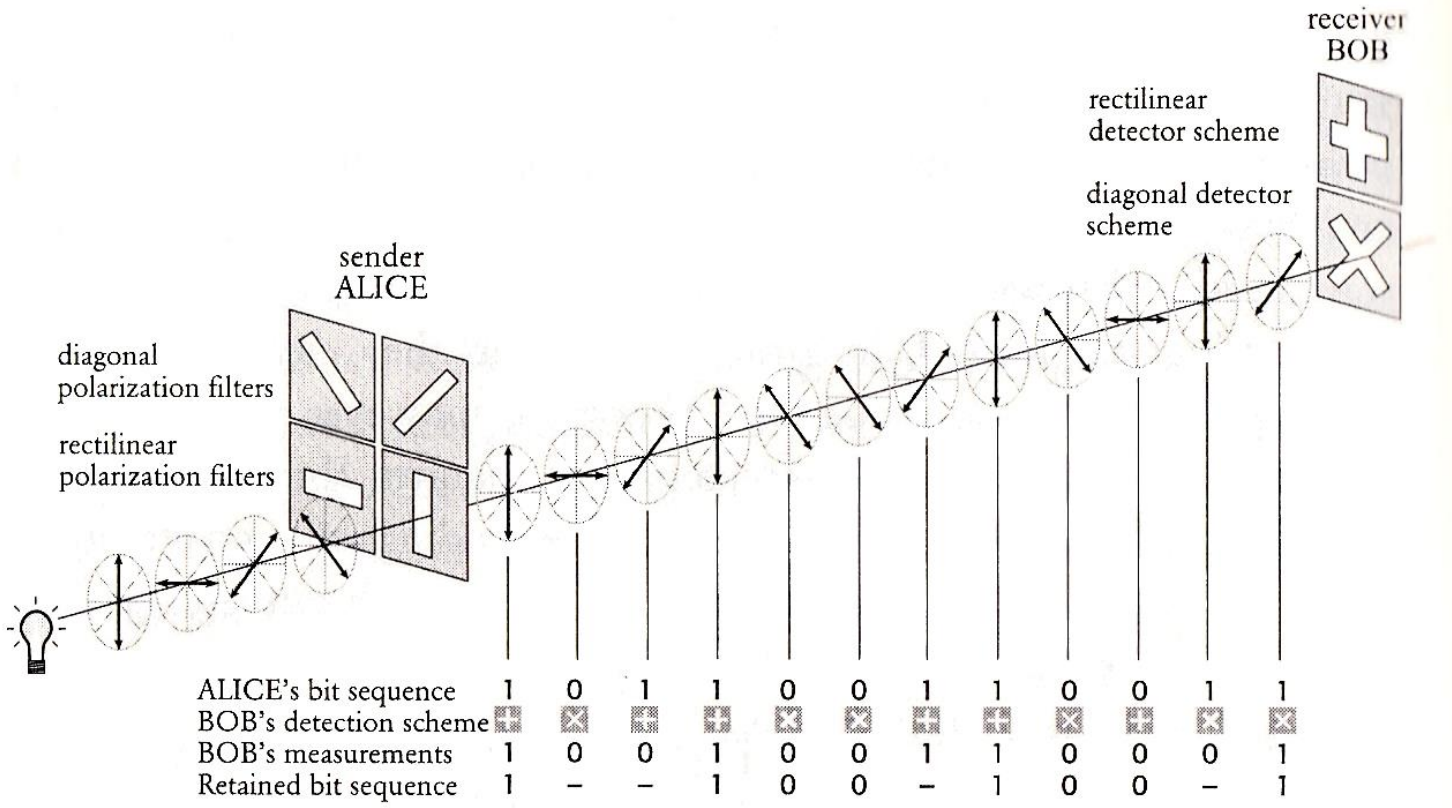
- Assuming polarities are not mutually orthogonal.
- A photon polarity (quantum state) is disturbed during measurement.
- It is impossible to make copies of photons in unknown polarities.
- An arbitrary photon polarity cannot be perfectly duplicated.

QUANTUM KEY DISTRIBUTION (QKD)

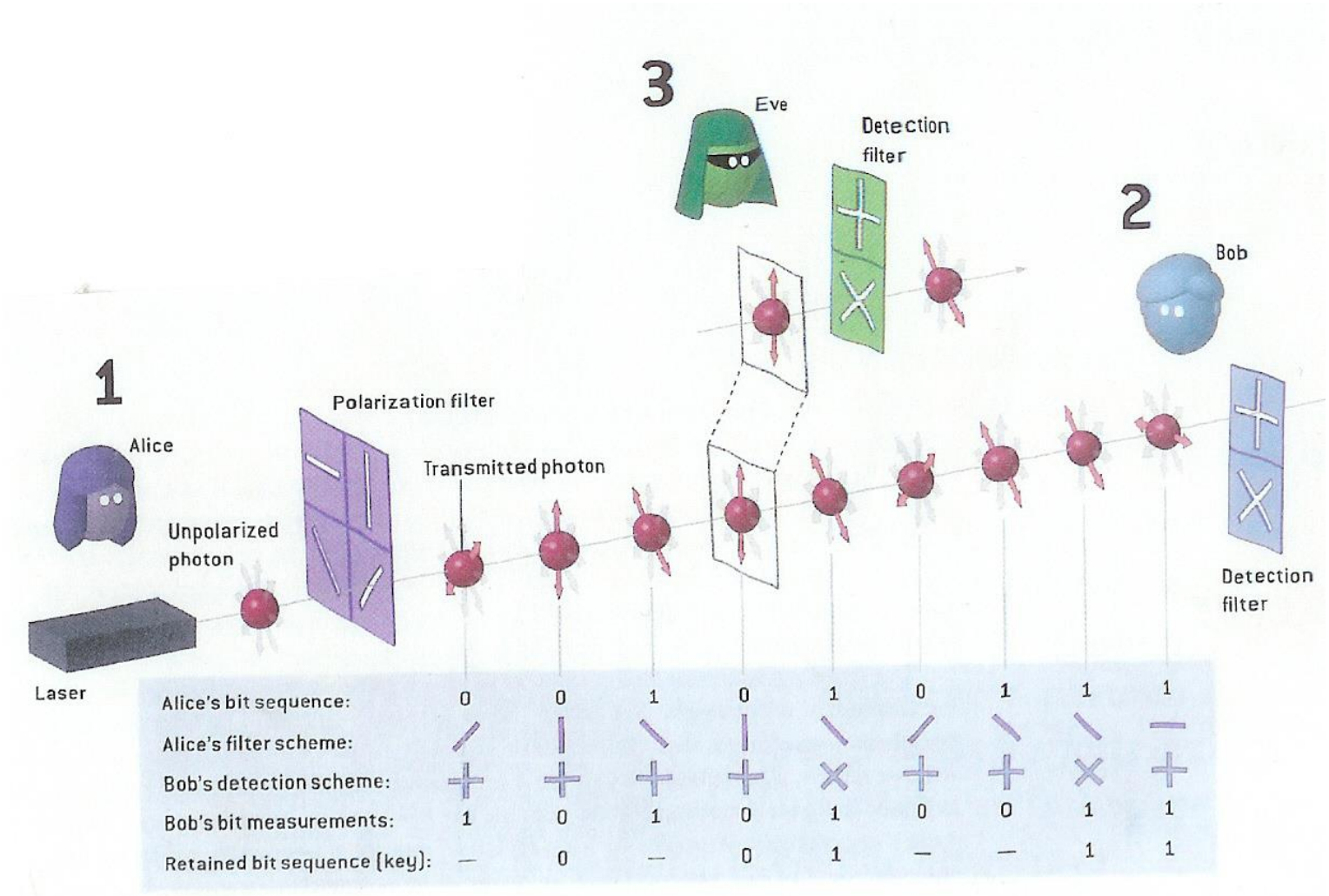
Quantum Key Distribution (QKD)

- Aka: BB84 (Bennet and Brassard 1984), quantum key expansion protocol
- Two parties (Alice & Bob)
  - Insecure photon (quantum) channel
  - Authenticated classical channel
  - Share a (relatively) short secret key
  - Can generate random numbers
- One adversary (Eve)
  - Can intercept & resend photons
  - Can eavesdrop, but not alter classical channel

QKD


receiver
BOB
rectilinear
detector scheme
diagonal detector
scheme
sender
ALICE
diagonal
polarization filters
rectilinear
polarization filters
ALICE's bit sequence 1 0 1 1 0 0 1 1 0 0 1 1
BOB's detection scheme
BOB's measurements 1 0 0 1 0 0 1 1 0 0 0 1
Retained bit sequence 1 – – 1 0 0 – 1 0 0 – 1

Interception by Eve



Practical QKD

- Ideal, qubit encoding using a single photon source not currently possible
- Practical, qubits are encoded into weak optical pulses (less than one *mean photon number (mpn)* per pulse)
  - E.g., 0.1 mpn, 90% 9% and 0.5% of pulses have one, two or more photons
  - Low mpn means low exposition to eavesdroppers
  - Pulse rate around 10 MHz

Practical QKD (cont'd)

- Single mode fiber
  - Wavelength is 1550 nm
  - Attenuation is 0.2 dB per km (distances up to 100 km)
- Free space
  - Wavelength is 880 nm
  - Depends on atmospheric conditions, line of sight, pointing and tracking mechanisms

Free space quantum communication

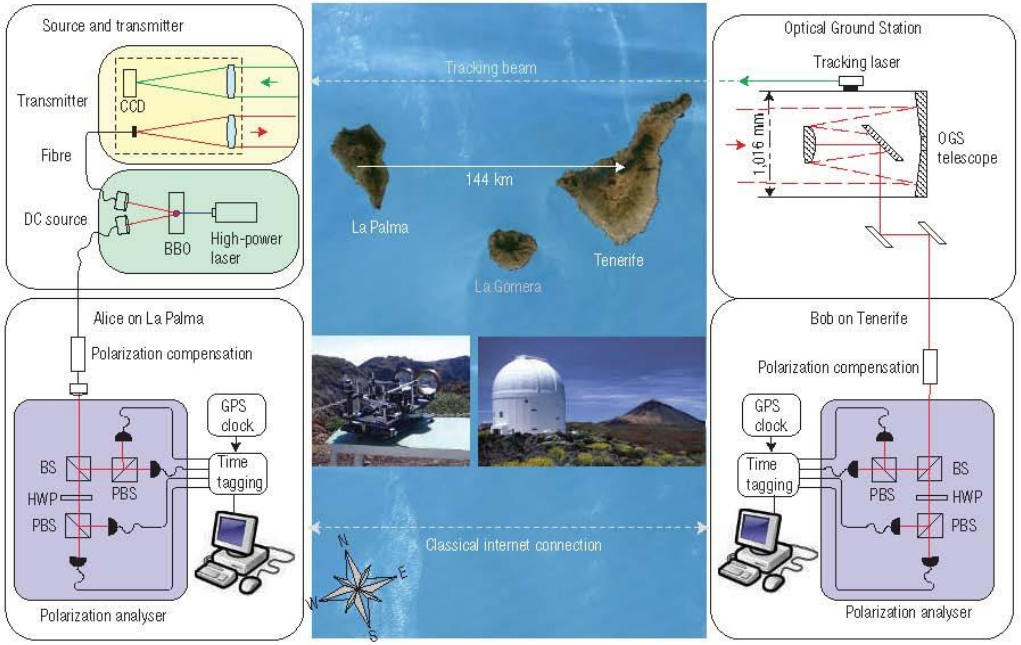


Figure 1 The free-space link between the Canary Islands La Palma and Tenerife in a picture taken from a satellite (clouds are shown here). Polarization-entangled photon pairs were produced in a type-II parametric down-conversion (DC) source by pumping a β-barium-borate crystal (BBO) with a high-power ultraviolet laser. One photon was measured locally on La Palma; the other one was sent through a 15 cm transceiver lens over the 144 km free-space optical link to the 1 m mirror telescope of the Optical Ground Station (OGS) on the island of Tenerife. The link was actively stabilized by analysing the direction of a tracking beam (532 nm) sent from OGS to La Palma, which was received in a second lens focusing it on a CCD (see Fig. 2). No optical cross-talk occurred in the quantum channel, because the tracking laser was sent in the opposite direction; additionally, interference filters were used. Both parties were using four-channel polarization analysers, consisting of a 50/50 beam-splitter (BS), a half-wave plate (HWP) and two polarizing beam-splitters (PBS), which analysed the polarization of an incident photon either in the H/V or in the +/− 45° basis, randomly split by the BS. Time-tagging units were used to record the individual times at which each detection event occurred relative to a timescale disciplined by the GPS. Already during data taking, Bob transmitted his time tags via a public internet channel to Alice. She found the coincident photon pairs in real time by maximizing the cross-correlation of these time tags using fast time-correlation software.

R. Ursin et al., Entanglement-based quantum communication over 144 km. Nature Physics, 3(7):481--486, 2007.

Commercial QKD

- ID Quantique (www.idquantique.com)
- MagiQ Technologies (www.magiqtech.com)
- QuantumCTek (www.quantum-info.com)
- Quintessence Labs (www.quintessencelabs.com)
- SeQureNet (www.sequrenet.com)
- Toshiba (www.toshiba.eu)