id Quantique

A Quantum Leap for Cryptography

Quantum Cryptography
Beyond the buzz

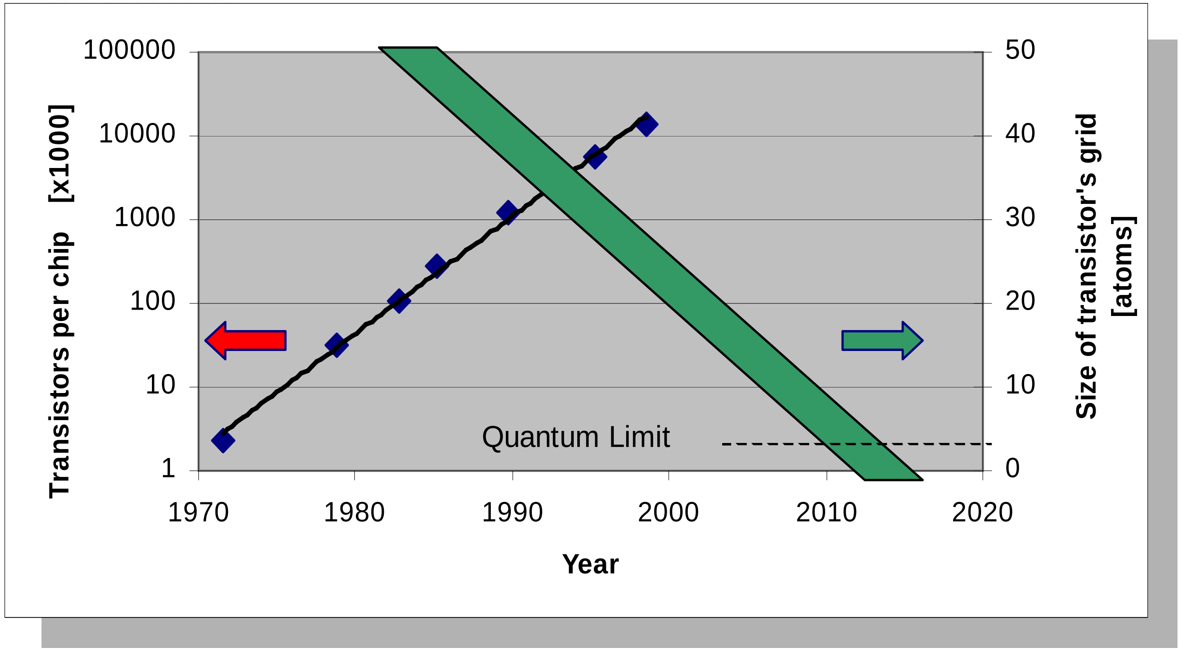
Grégoire Ribordy

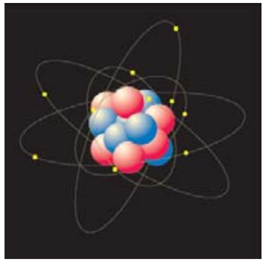
CERN, May 3rd 2006

Outline

- Quantum physics and information technology
- The limits of classical cryptography
- The principles of quantum cryptography
- Practical systems and applications
- Future directions

Moore’s law and quantum physics





Classical and Quantum physics

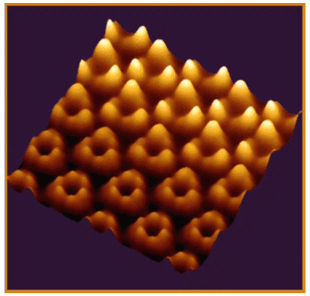
Classical physics

- … - 1900
- Describes the macroscopic world

- Deterministic
- Intuitive

Quantum physics

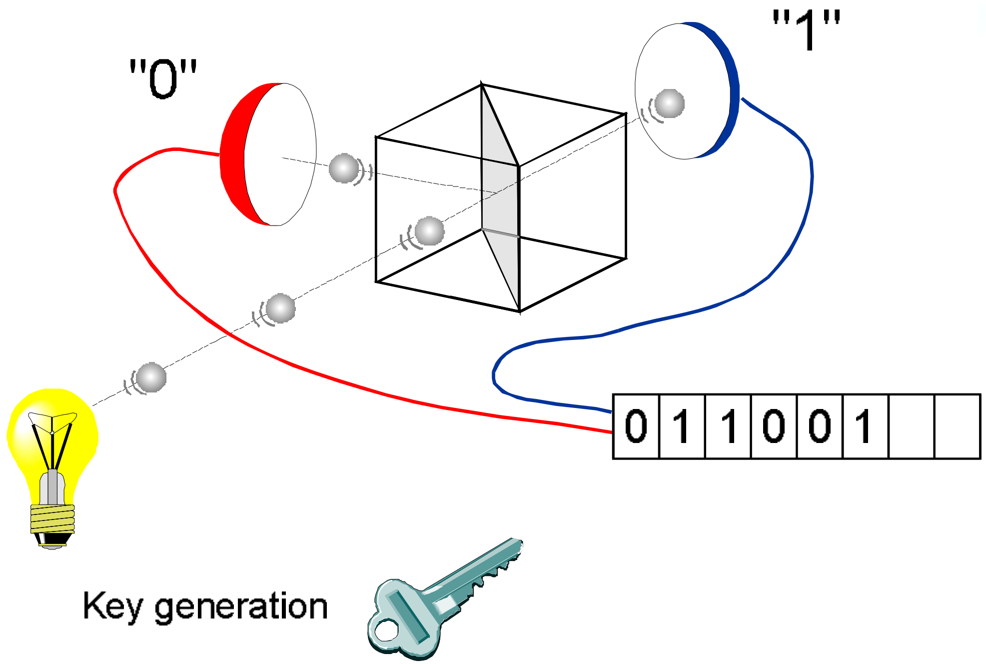
- 1900 - …
- Description of the microscopic world



- Probabilistic
- Central role of the observer
- Not very intuitive

Quantum physics → Novel information processing possibilities
→ Quantum Information Theory (QIT)

Generating random numbers with quantum physics



- High bit rate
  - 4 or 16 Mbits/s
- Continuous monitoring
- Main OS's supported

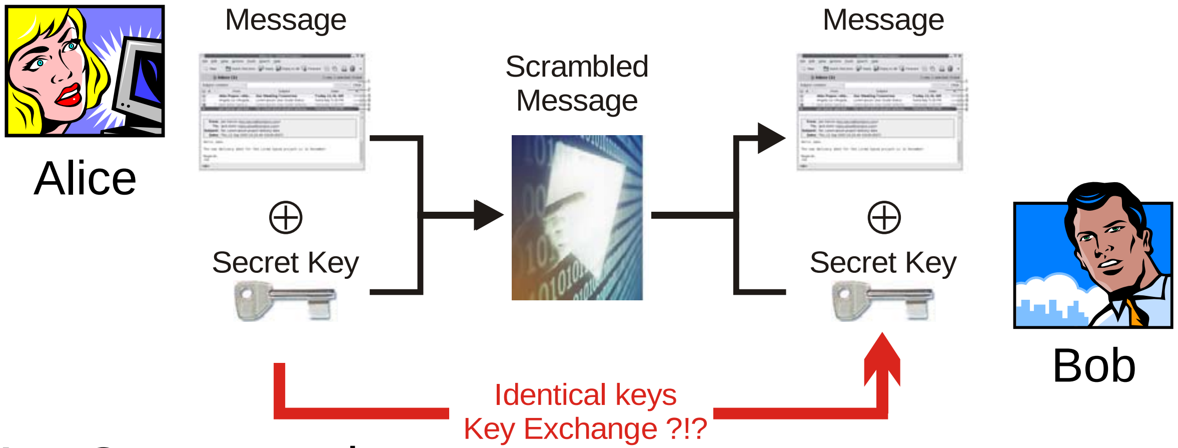
Microsoft Windows
LINUX POWERED
SOLARIS™

Outline

- Quantum physics and information technology
- The limits of classical cryptography
- The principles of quantum cryptography
- Practical systems and applications
- Future directions

Introduction: Classical Cryptography

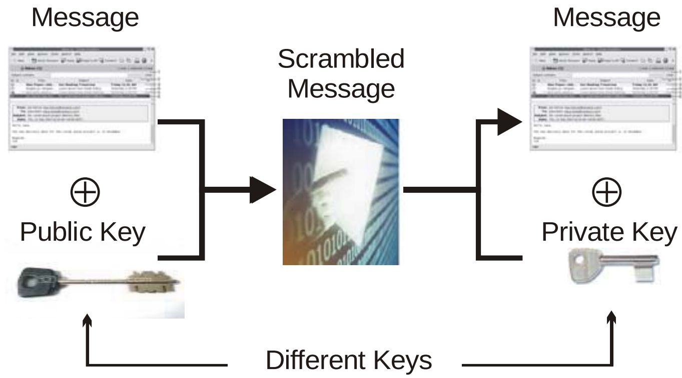
- Secret Key Cryptography



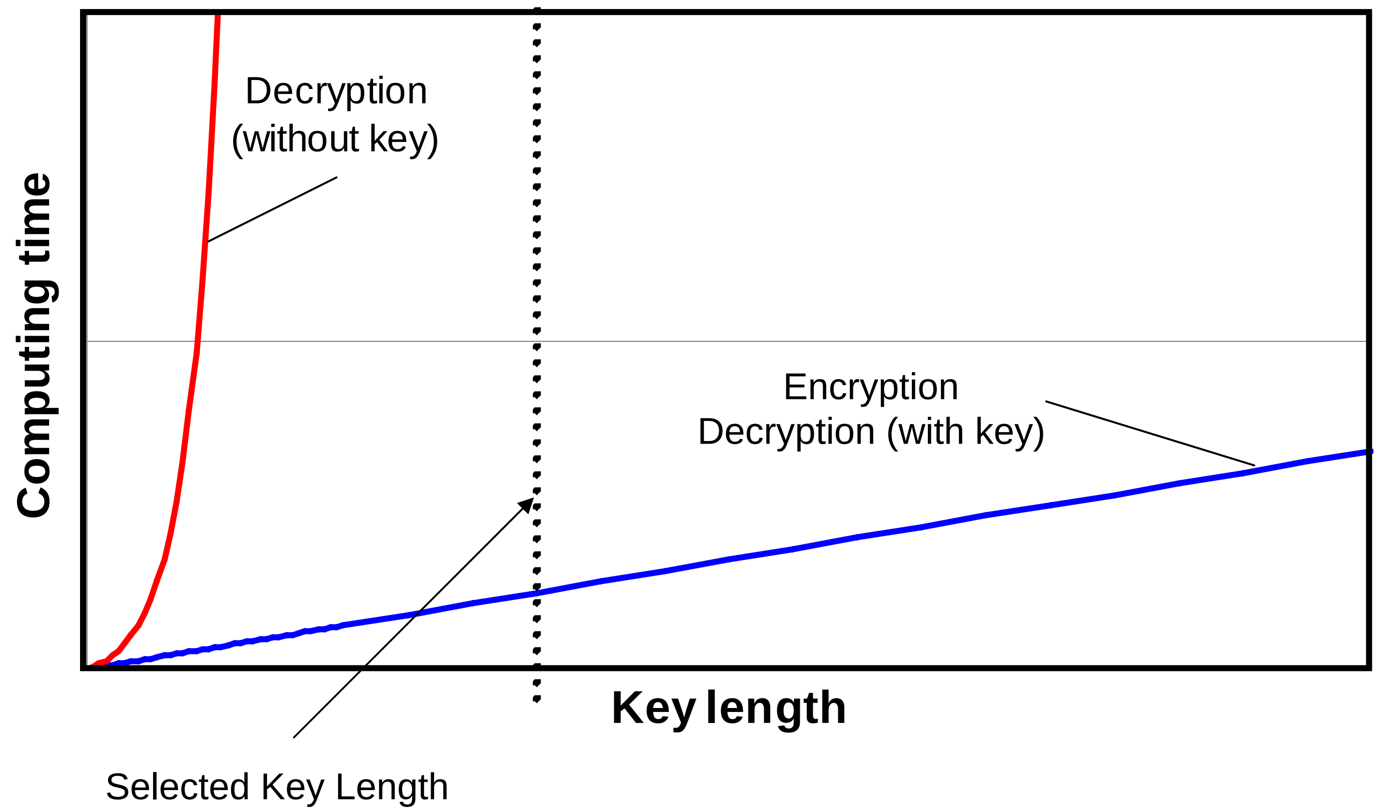
- Public Key Cryptography

Different keys
→ Key exchange solved

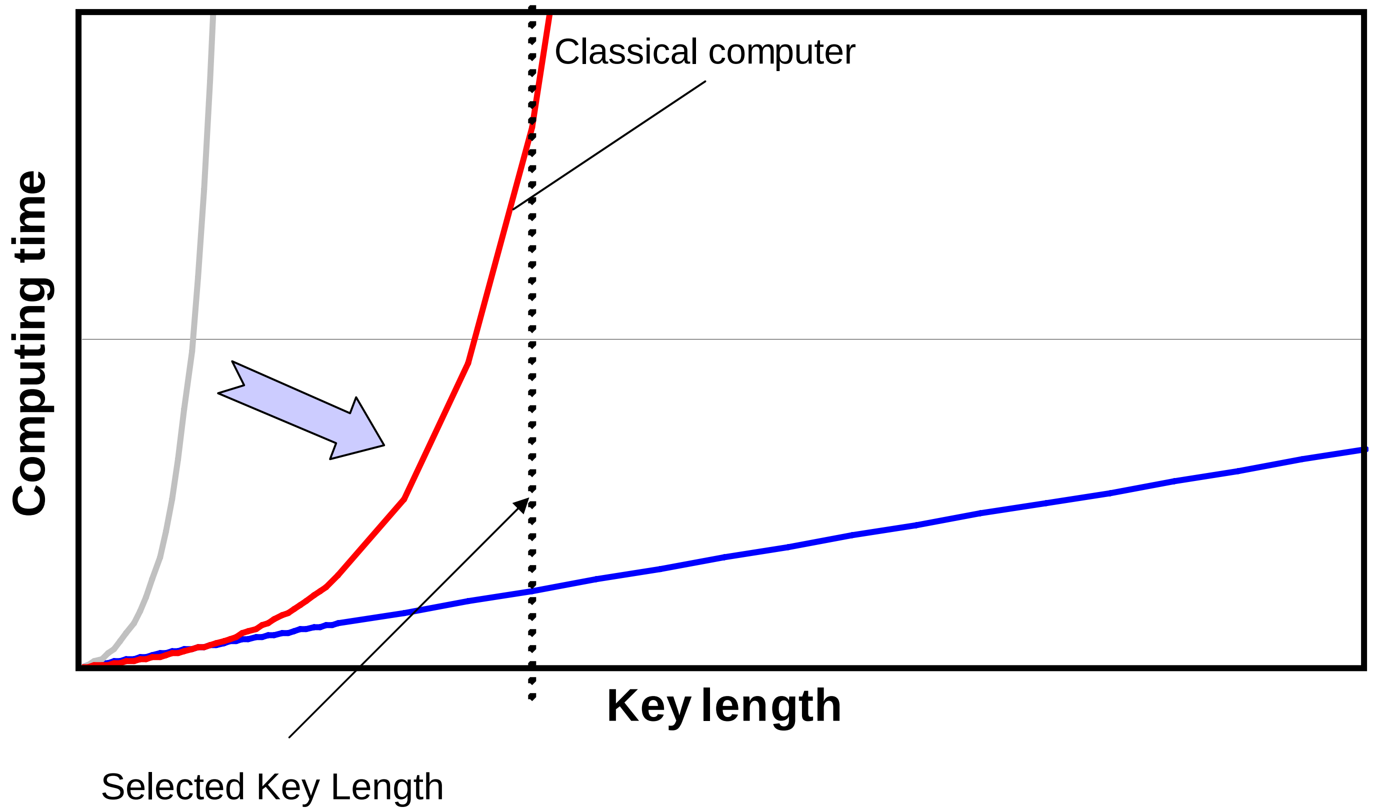
Vulnerabilities!!!



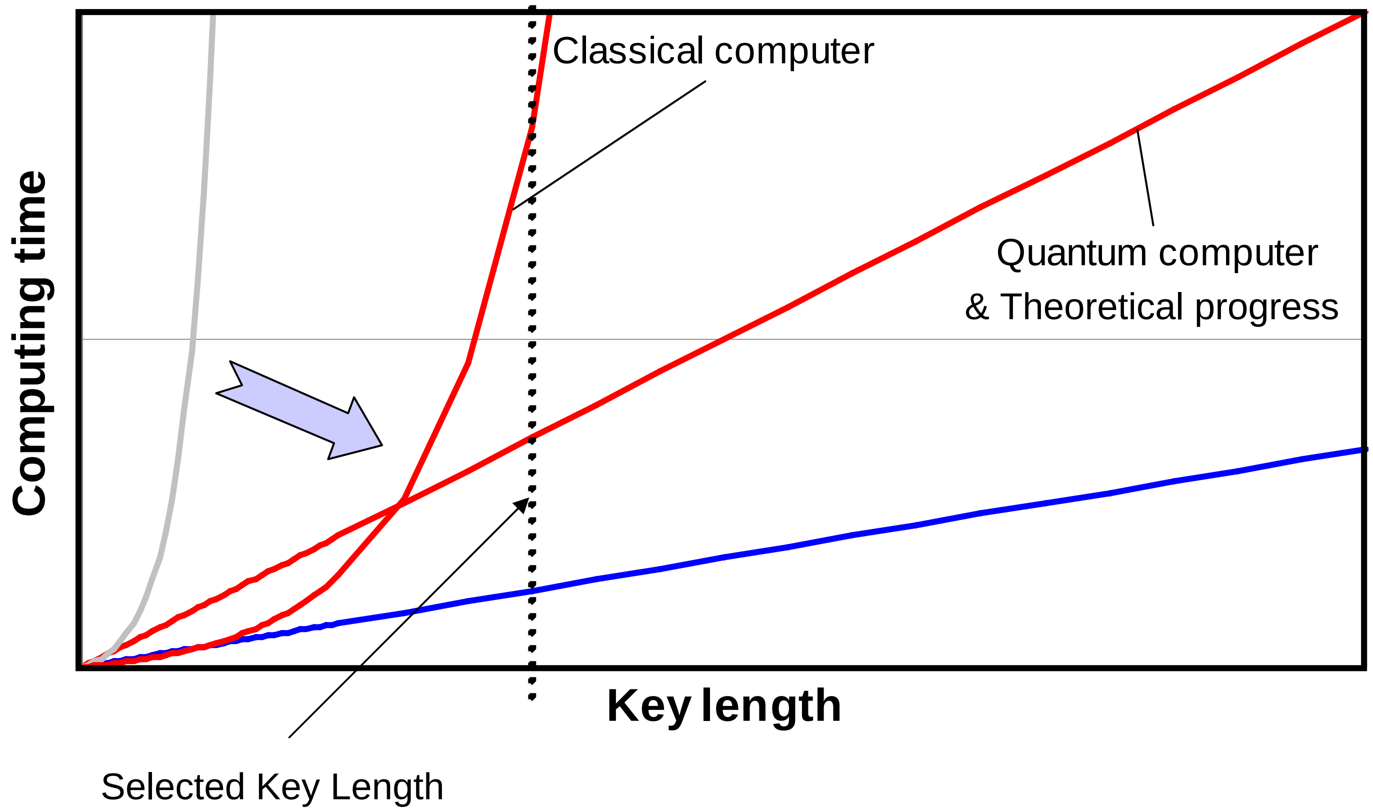
Security of public key cryptography



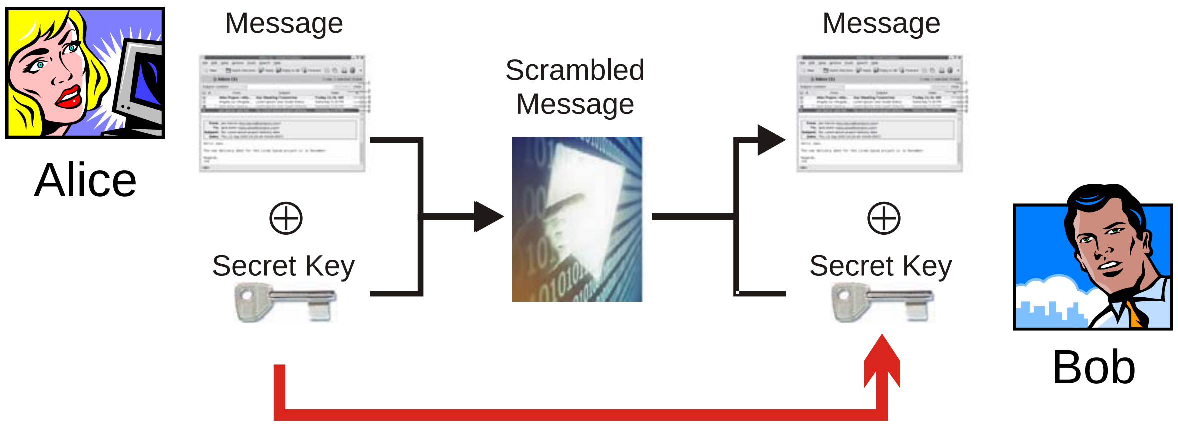
Vulnerabilities of public key cryptography



Vulnerabilities of public key cryptography



Where does Quantum Cryptography fit in?



Secret key exchange by quantum cryptography

Quantum Cryptography is a key distribution technique!

Quantum Key Distribution is a better name!!!

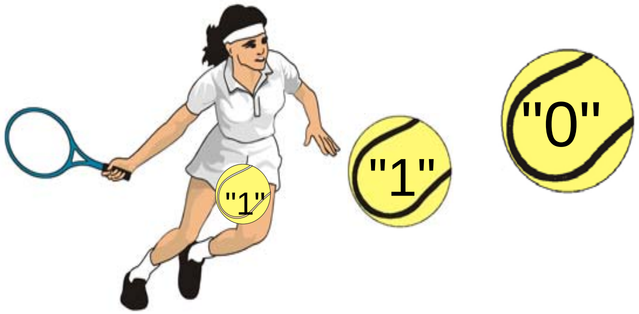
Outline

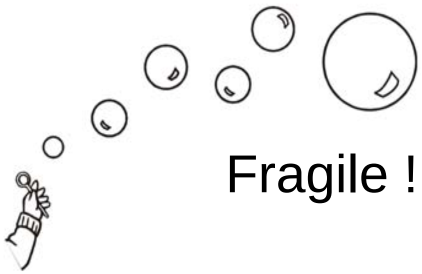
- Quantum physics and information technology
- The limits of classical cryptography
- The principles of quantum cryptography
- Practical systems and applications
- Future directions

Physical implementation of a data channel

Classical communication

Quantum communication

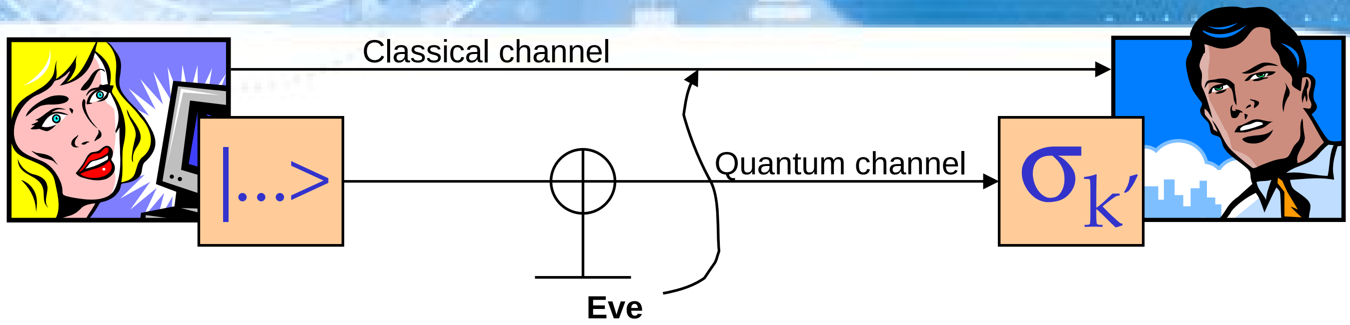




Fragile !

Security guaranteed by the laws of quantum physics

Quantum Cryptography: rules of the game



1. Details of the protocole publicly known
2. Goal: to produce a secret key or nothing

   ↔ « Eve cannot do better than cutting the line »

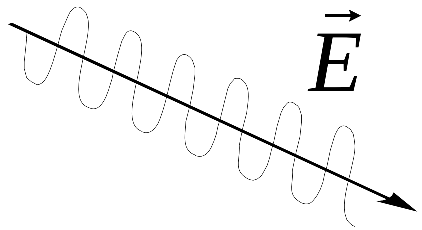
Alice and Bob: to estimate Eve's information on key

$$\begin{cases} I_{AE} \text{ small: Produce a key} \\ I_{AE} \text{ large: STOP} \end{cases}$$

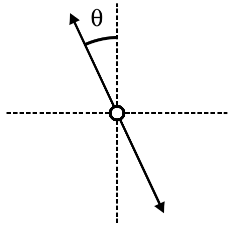
QUANTUM KEY DISTRIBUTION

Polarization of Photons

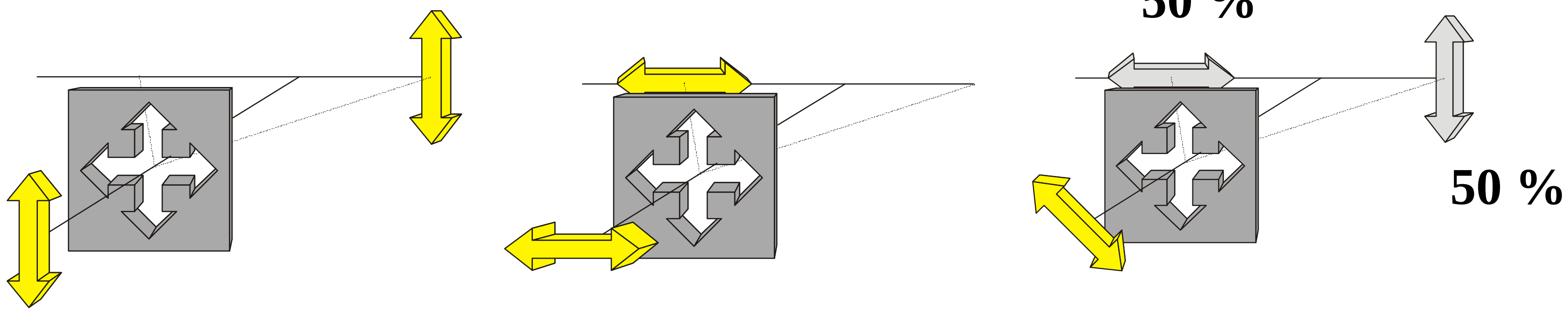
- Direction of oscillation of the electric field associated to a lightwave



- Polarization states

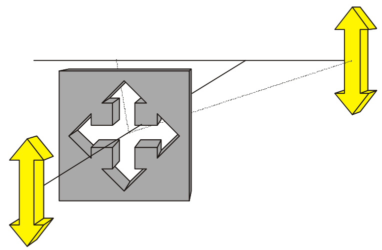


- What can we do with it ?

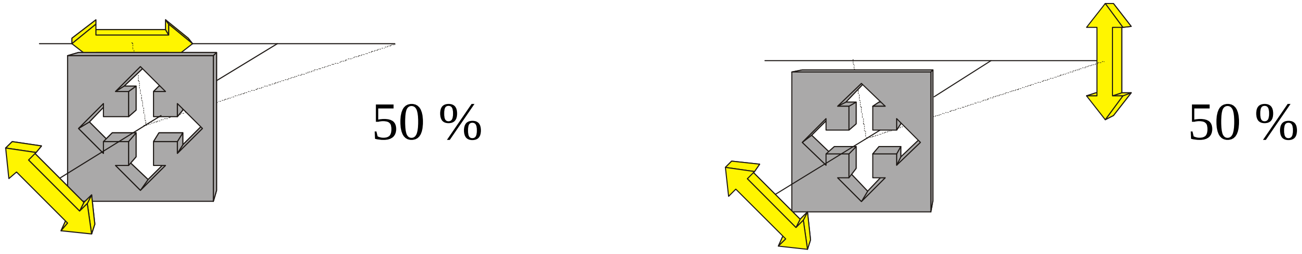


Irreversibility of Measurements

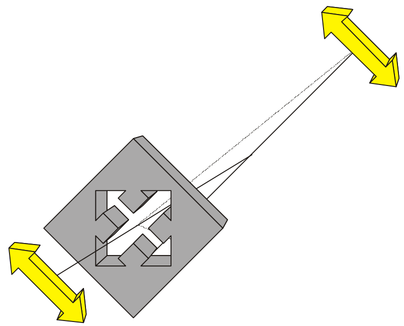
Incoming photon polarized at 90°



Incoming photon polarized at 45°



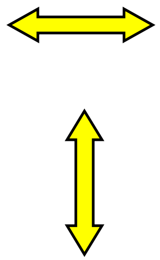
Rotation of polarizer



Quantum communications

- Transmitting information with a single-photon

- Use a quantum property to carry information



= "0" = $|0\rangle$

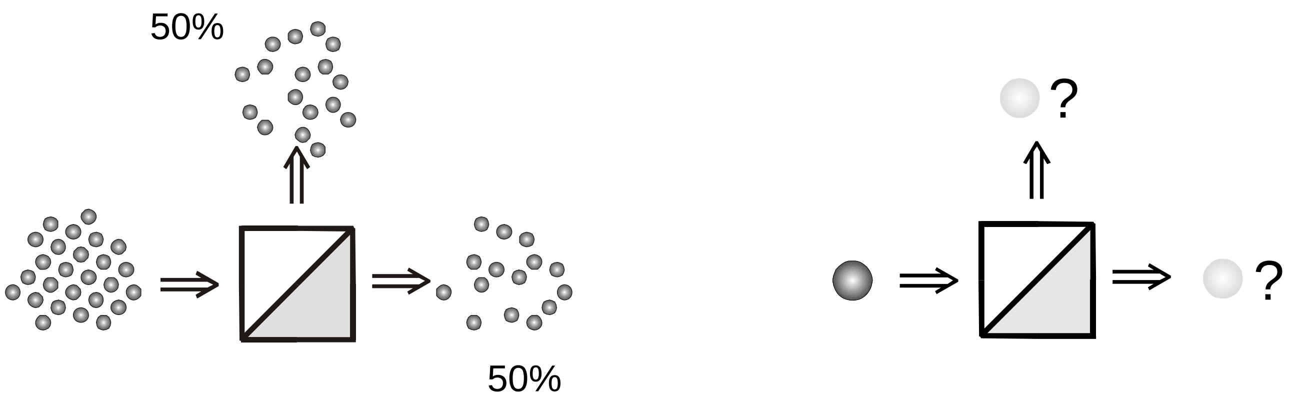
= "1" = $|1\rangle$

Eavesdropping (1)

- A single-photon constitutes an elementary quantum system

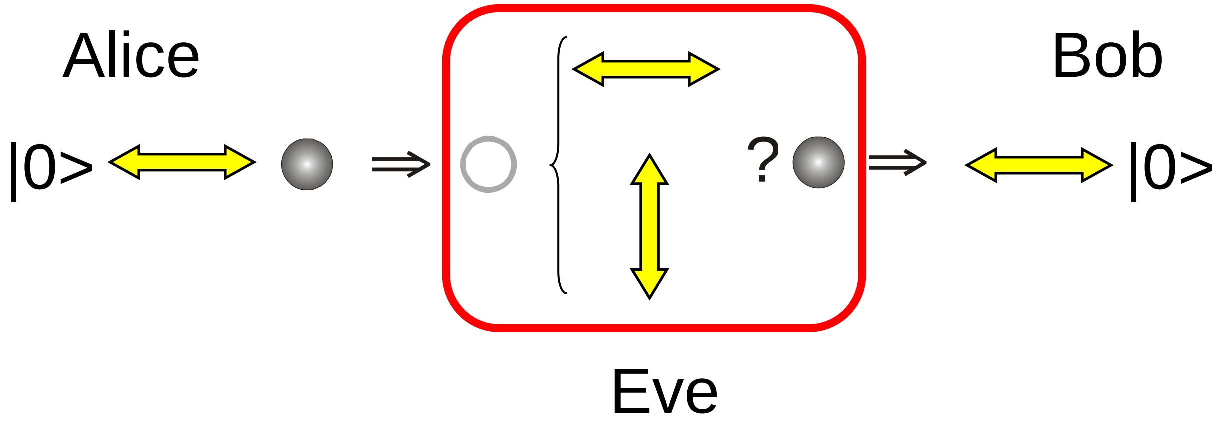
  It cannot be split

- Semi-transparent mirror



Eavesdropping (2)

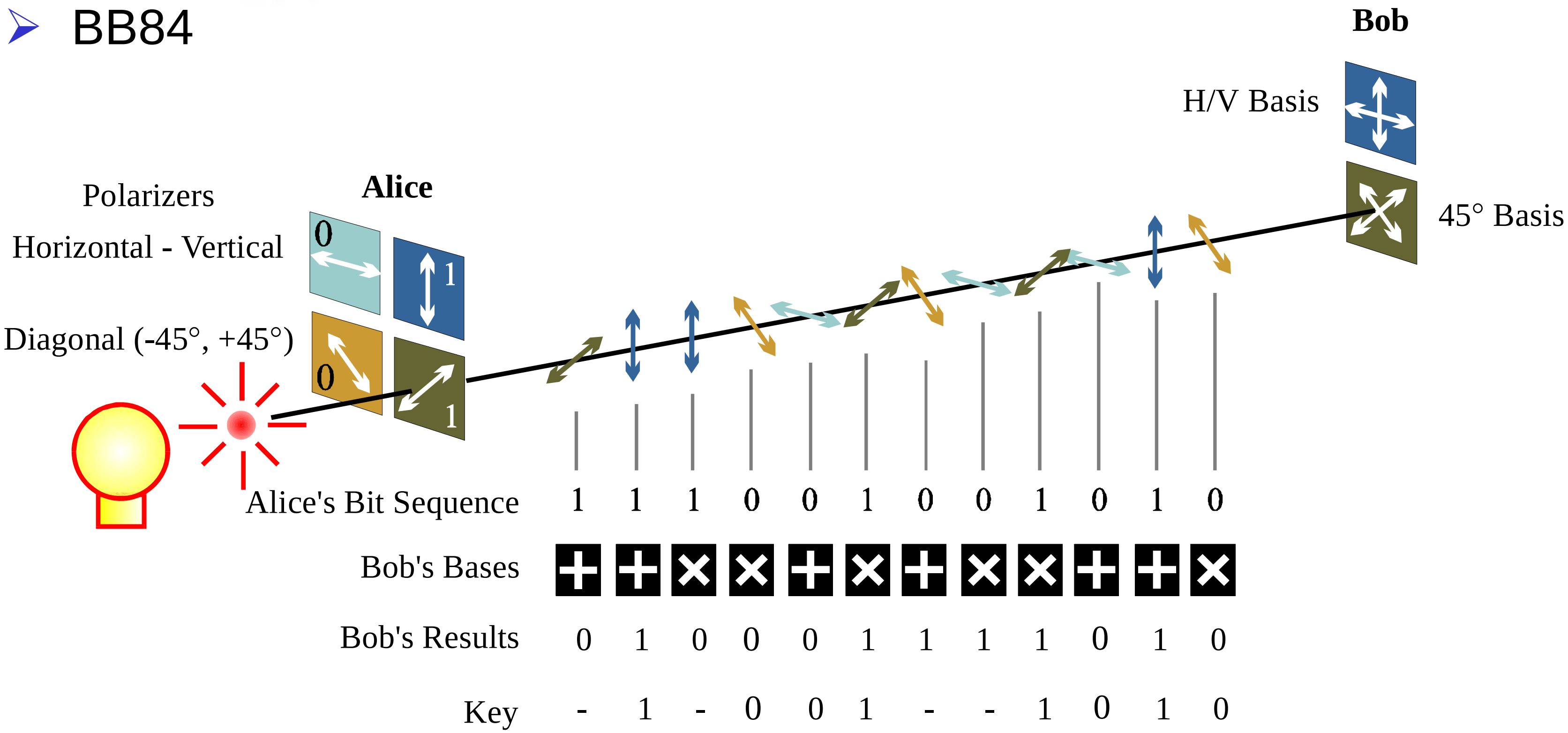
- Communication interception



- Use quantum physics to force spy to introduce errors in the communication

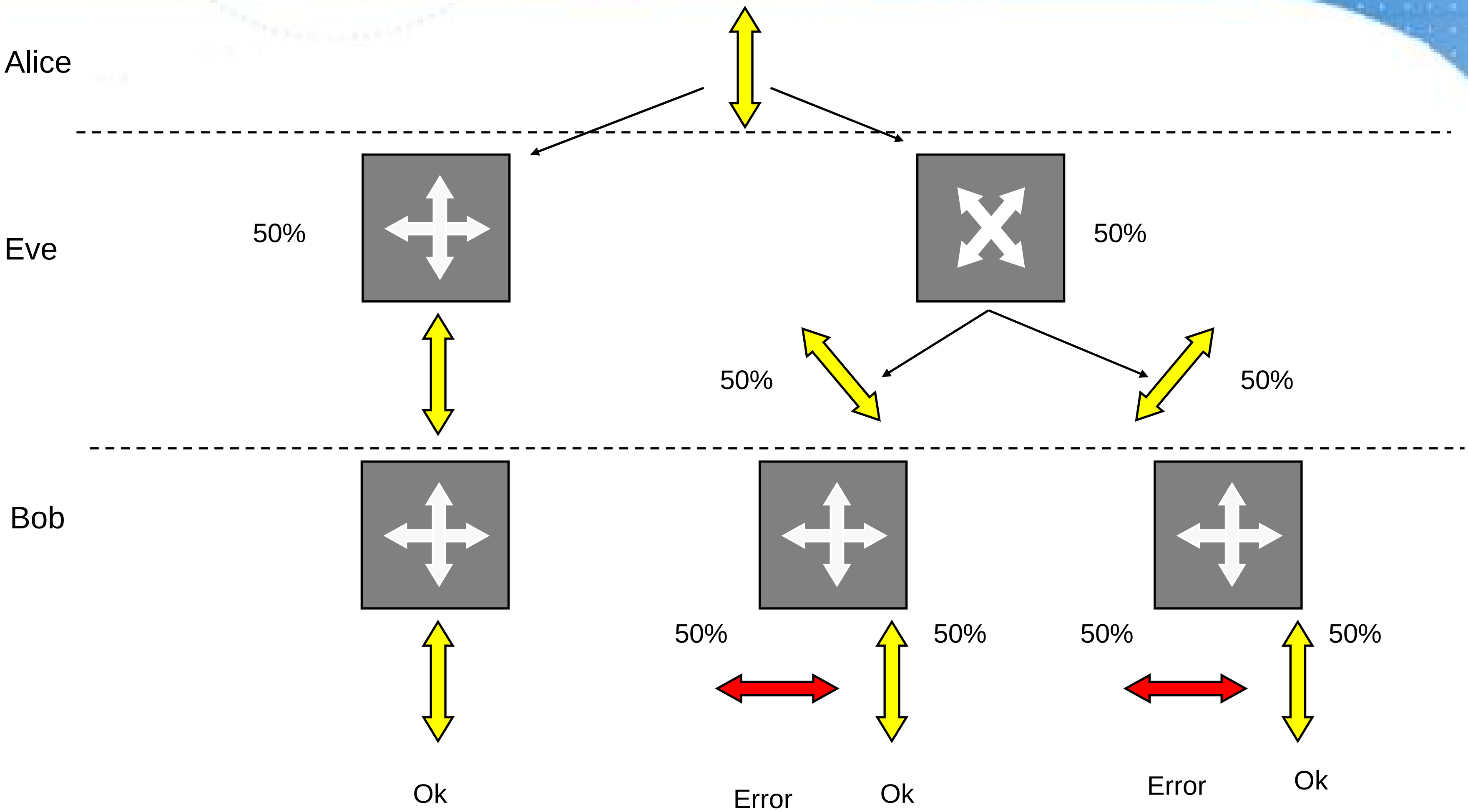
Quantum Cryptography Protocole

- BB84

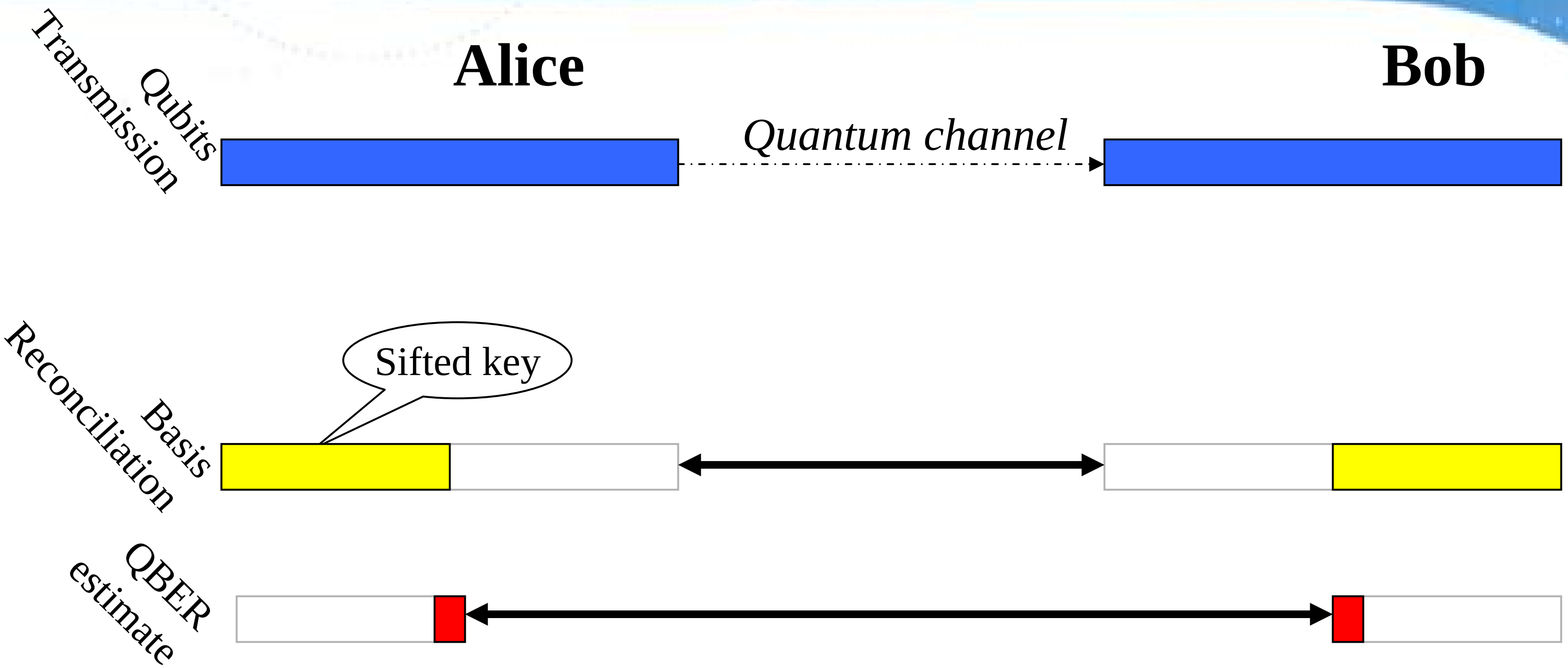


- A better name: *Quantum Key Distribution*

Eavesdropping (3)



Key Distillation (ideal case)

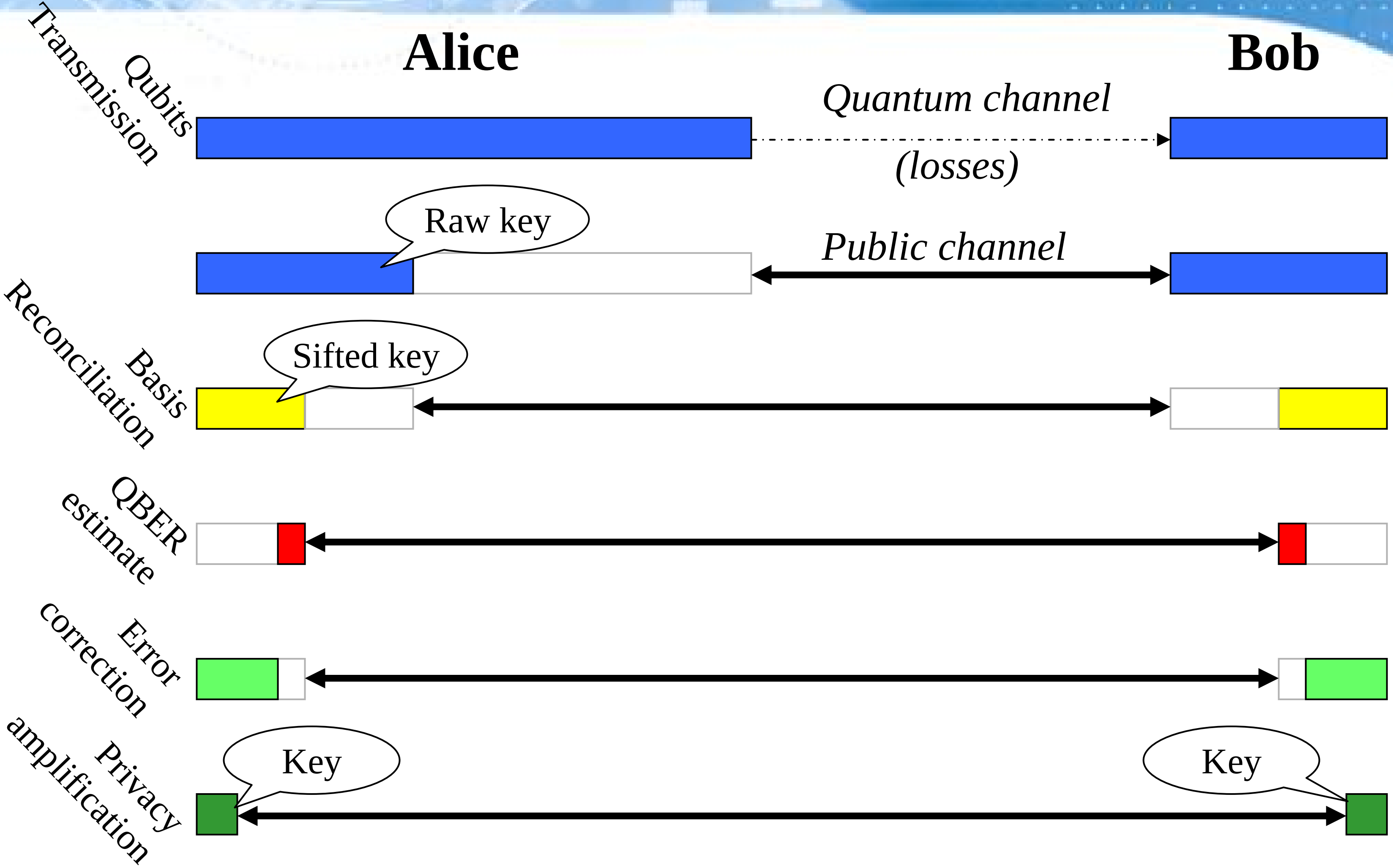


$$\text{QBER} = \begin{cases} 0 : \text{no eavesdropping} \\ > 0 : \text{eavesdropping} \end{cases}$$

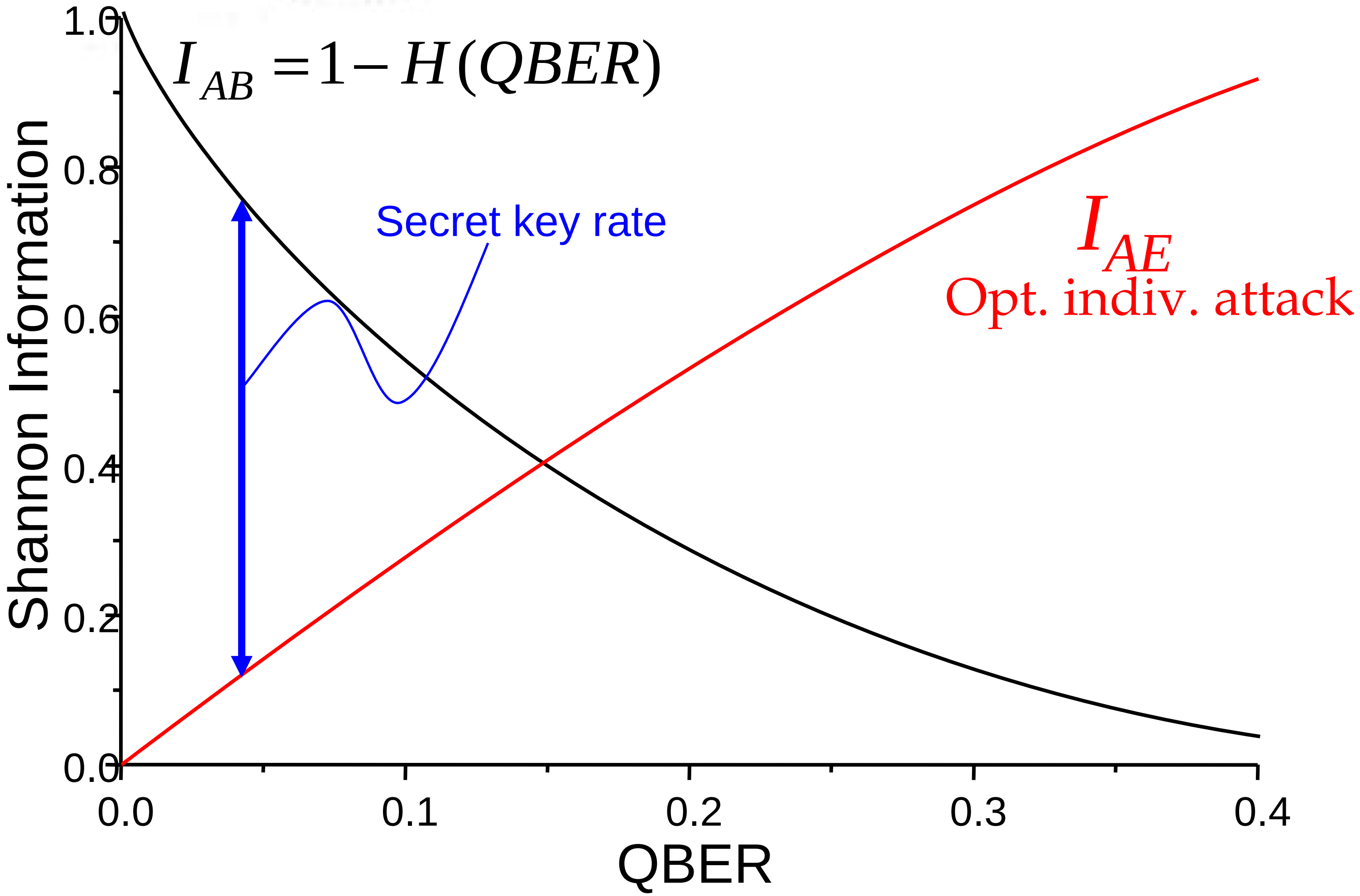
Reveals rather than prevents eavesdropping

A better name: quantum key distribution

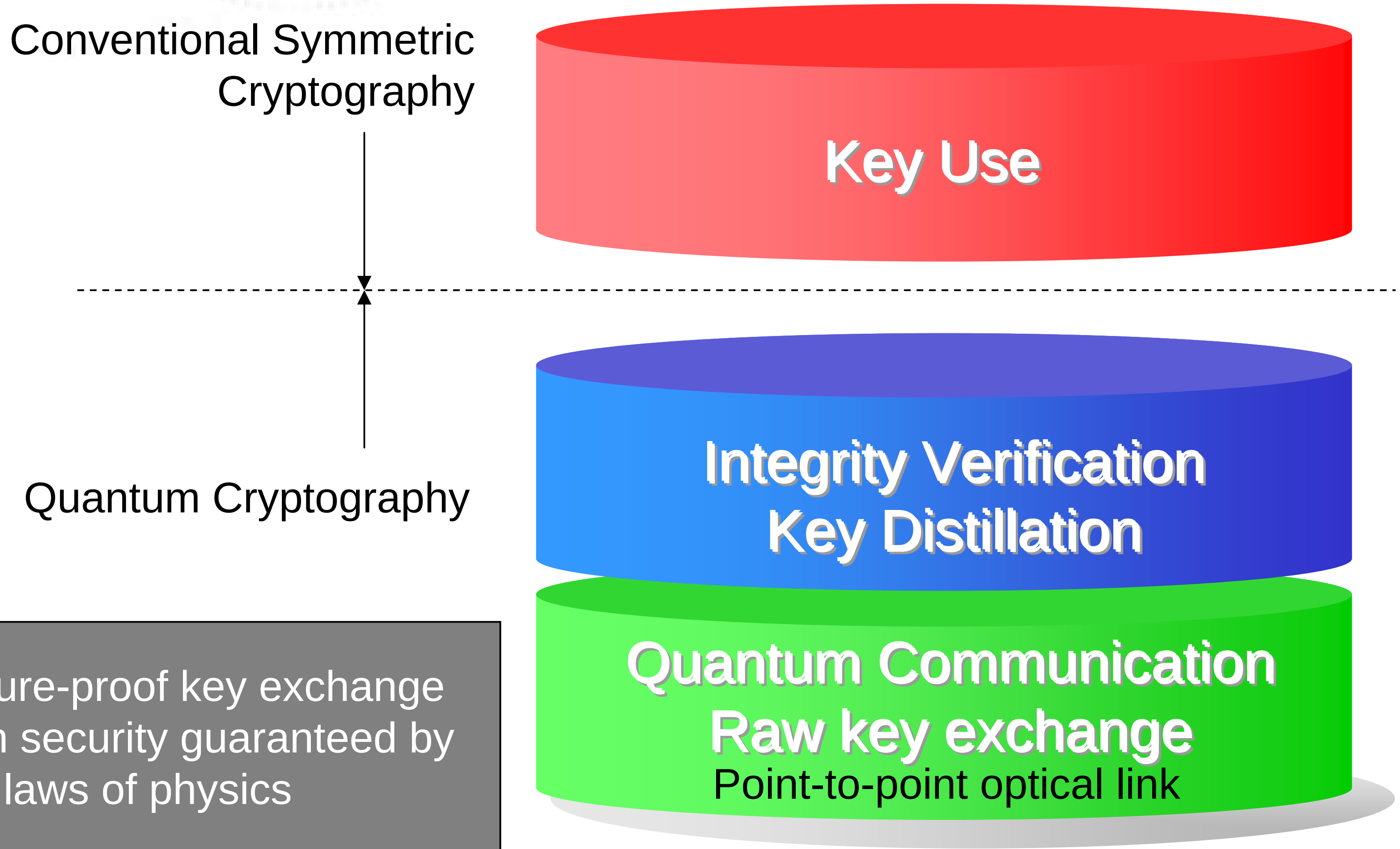
Key Distillation (realistic case)



Information curves



The Principles of Quantum Cryptography: Summary



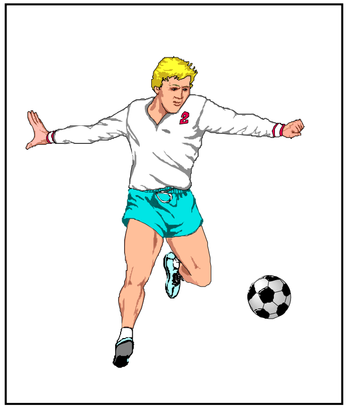
Future-proof key exchange with security guaranteed by the laws of physics

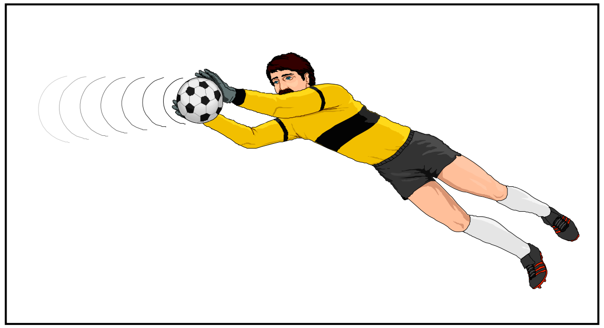
Outline

- Quantum physics and information technology
- The limits of classical cryptography
- The principles of quantum cryptography
- Practical systems and applications
- Future directions

Building a Quantum Key Distibution System

- Necessary components





Channel

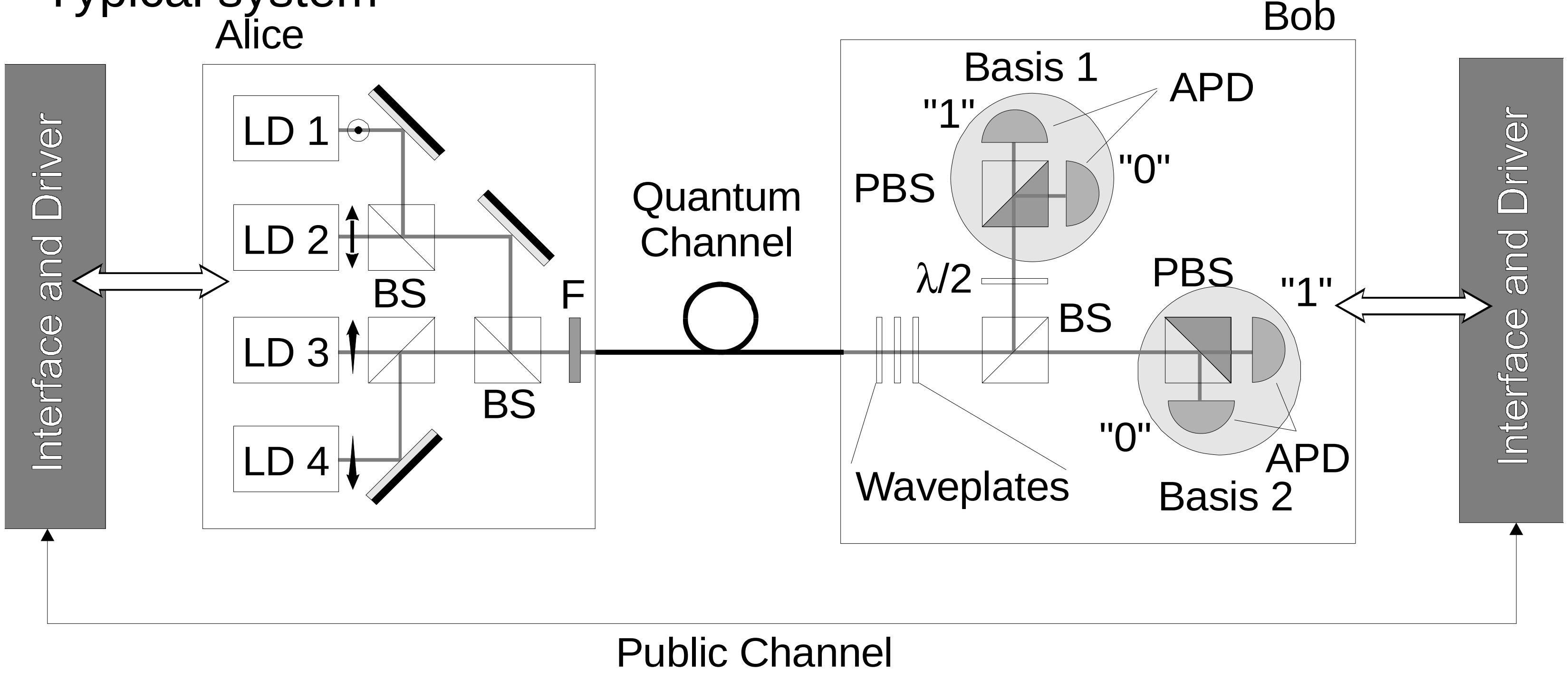
Single-Photon Source

Single-Photon Detector

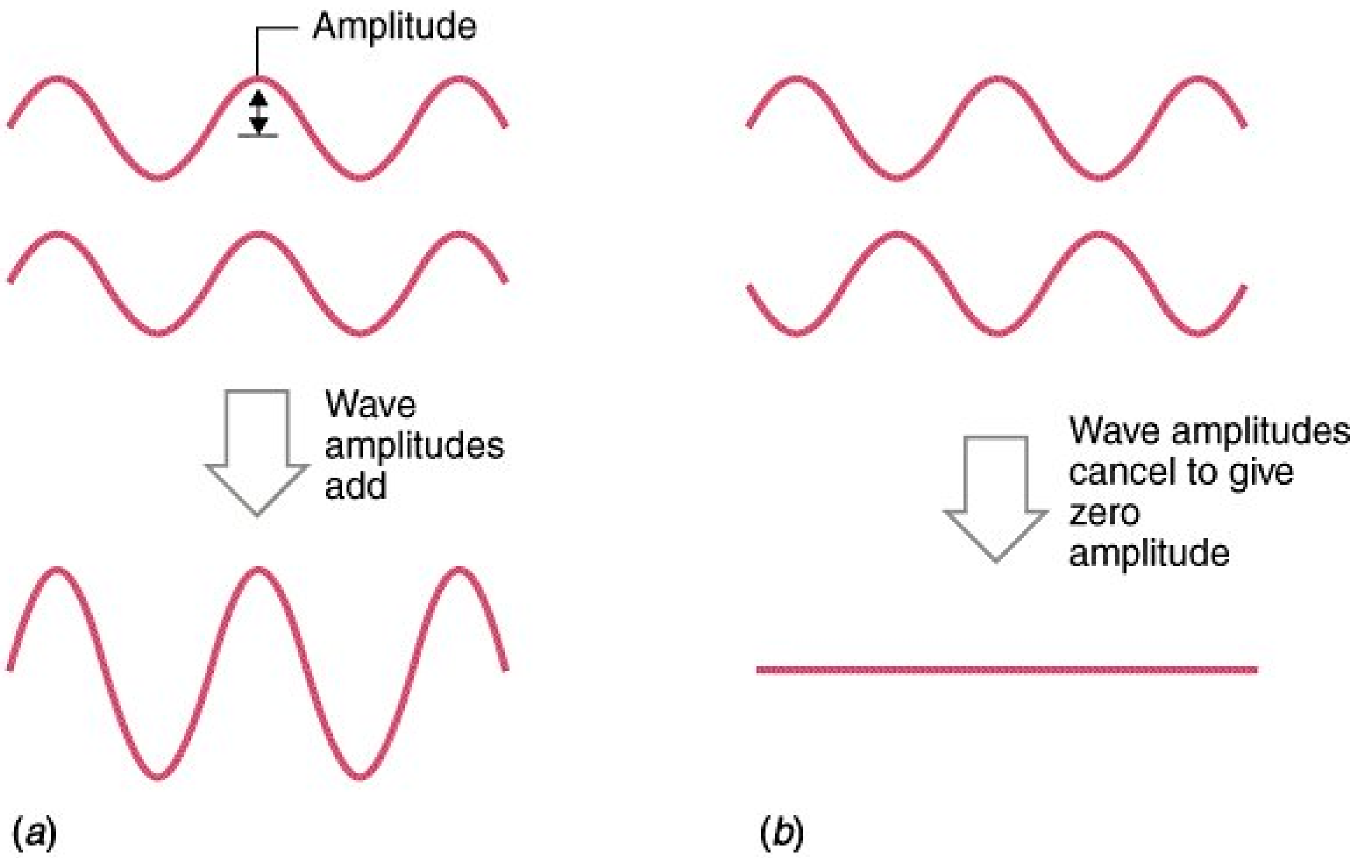
- “System approach”

Polarization Coding

- Typical system

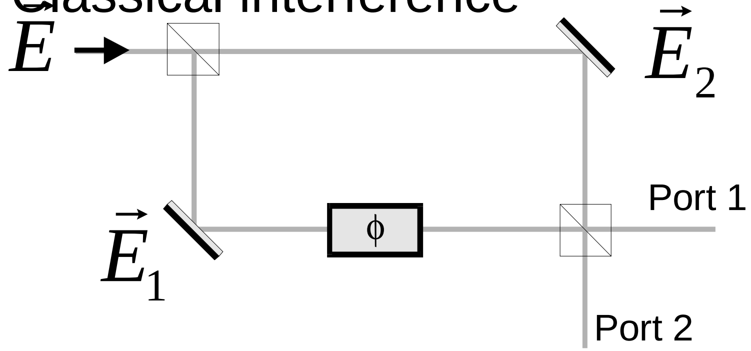


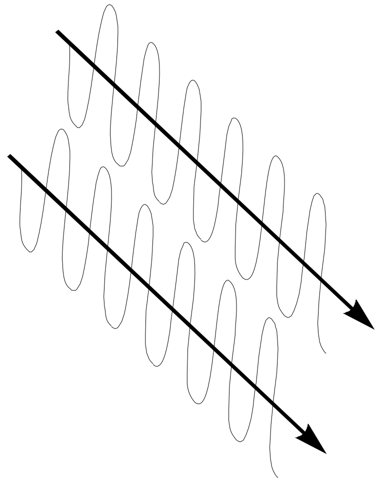
Interferences

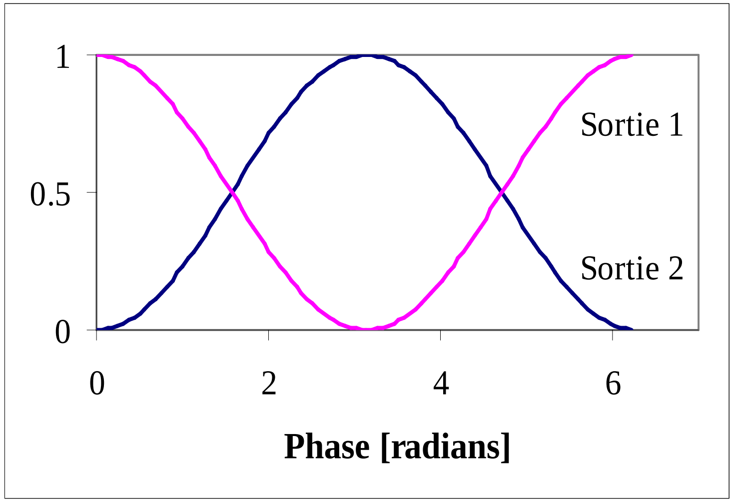


Interferometer

- Classical interference

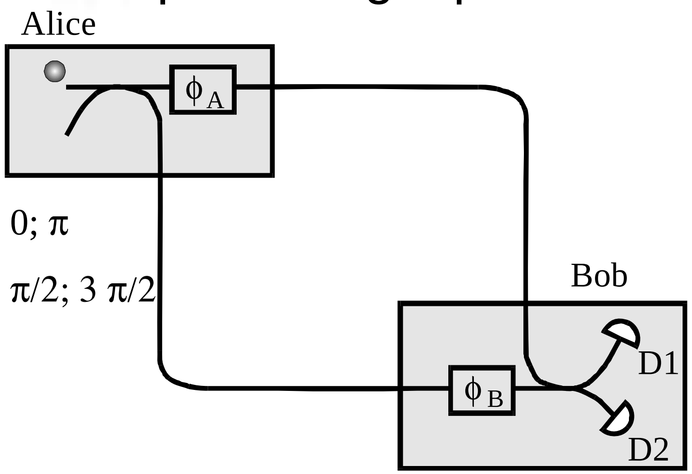






Phase encoding

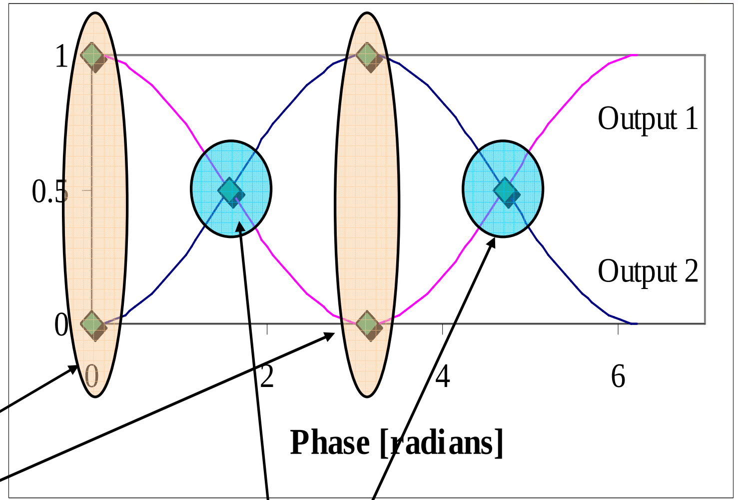
- Quantum optics: single-photon



Base 1: $\phi_A = 0; \pi$

Base 2: $\phi_A = \pi/2; 3\,\pi/2$

Basis choice: $\phi_B = 0; \pi/2$



Bases

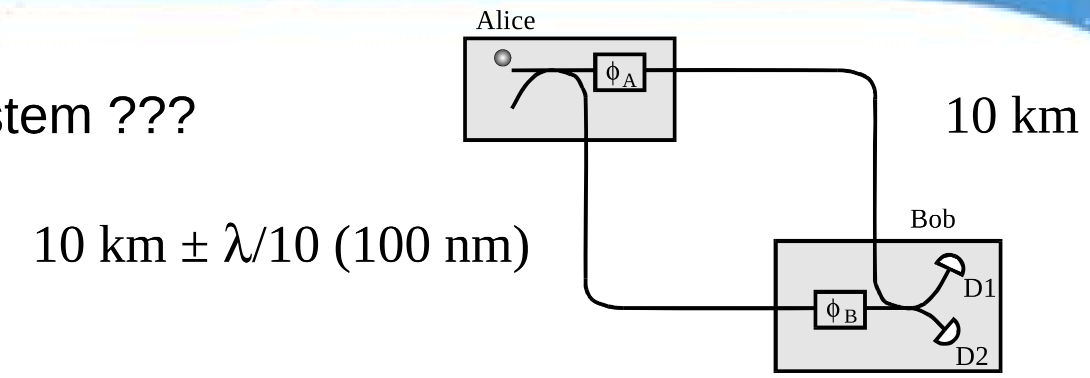
Compatible:	Alice $\phi_A \Rightarrow D_i$
$(\phi_A - \phi_B = n\pi)$	Bob $D_i \Rightarrow \phi_A$

Incompatible: Alice and Bob ??

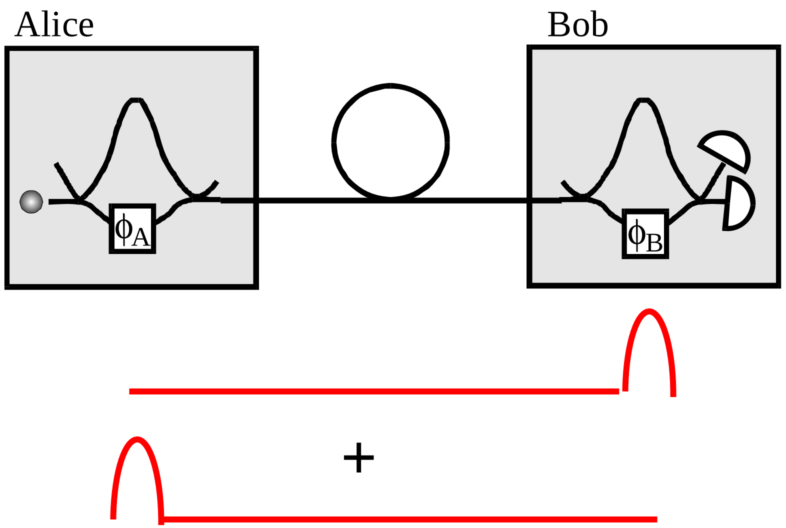
$(\phi_A - \phi_B = \pm\pi/2)$

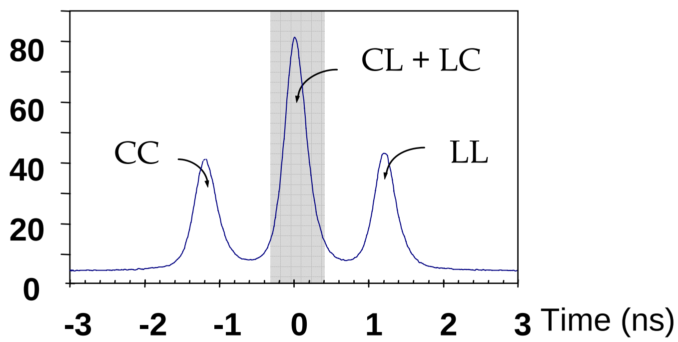
Phase encoding (2)

- Stability of such system ???



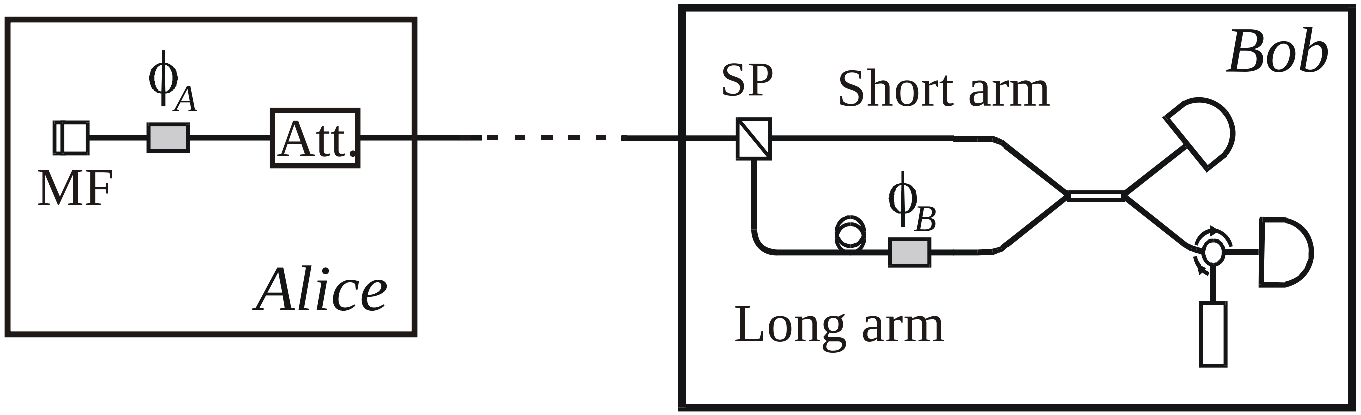
- In practice

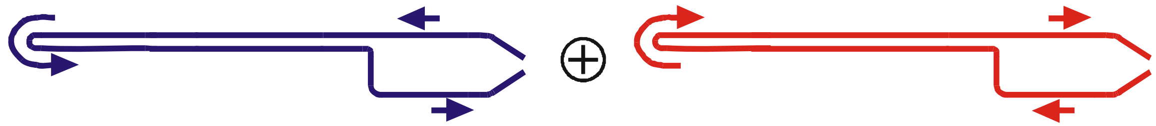




Auto-compensated set-up

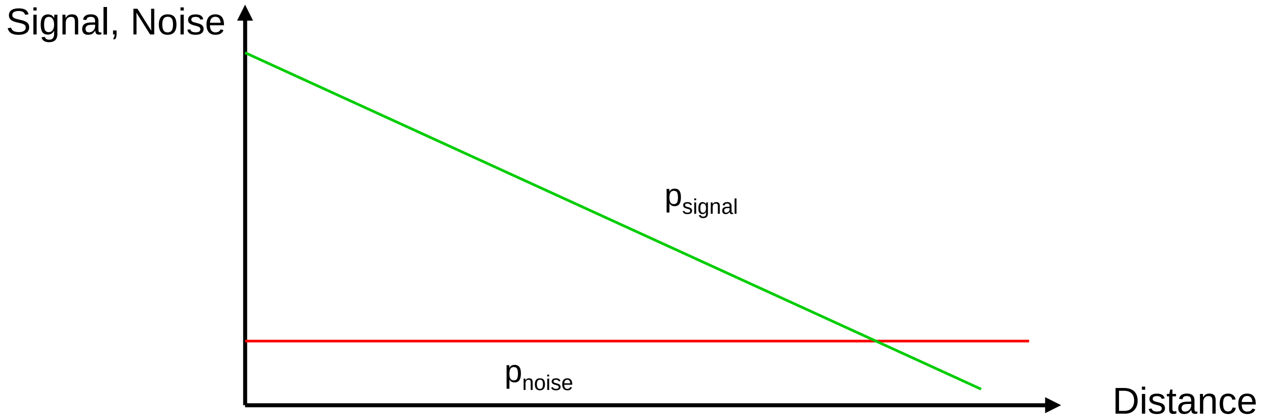
- Time multiplexing





Practical requirements

- Distance limitation < 100 km



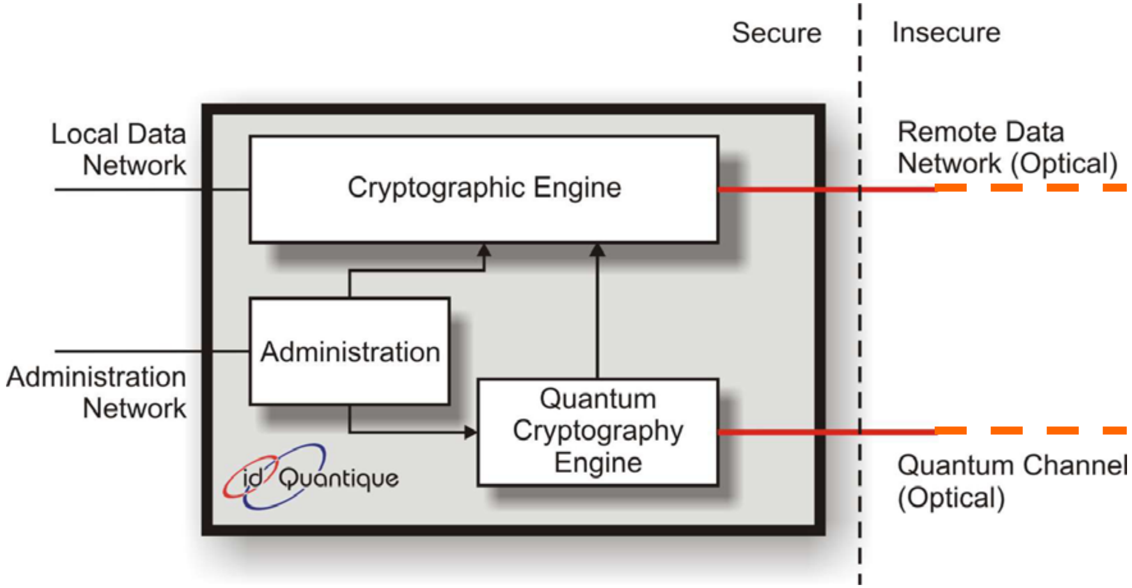
Current range is sufficient for a vast majority of MAN/SAN applications

- Point-to-point dark fiber
  - Amplifiers
  - Opto-electro-opto conversion

→perturbation of the quantum state of the photon

Link Encryptors with QKD

- Network Appliance
  - Point-to-point link encryption
  - Layer 2 device
  - Network protocole independent
  - Compatible with higher layer encryption



Specifications
- Encryption: AES (128, 192, 256 bits)
- Key rate as high as 100 keys / s
- Distance < 100 km (60 miles)
- Pair of dark fiber

Target Applications
MAN or SAN encryption

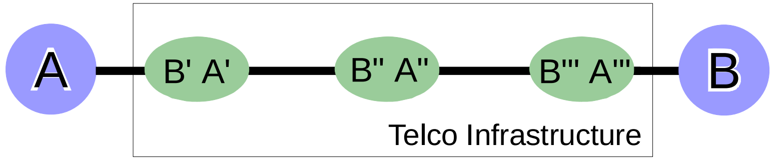
« Swiss Quantum » Pilot Site

Outline

- Quantum physics and information technology
- The limits of classical cryptography
- The principles of quantum cryptography
- Practical systems and applications
- Future directions

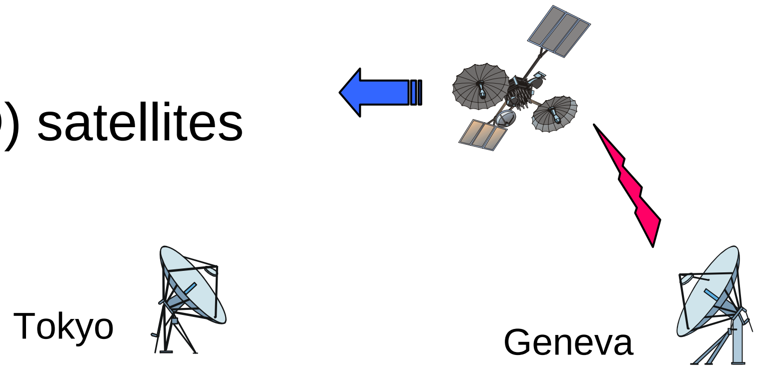
Extending the key distribution distance

- Chaining links



- Better components

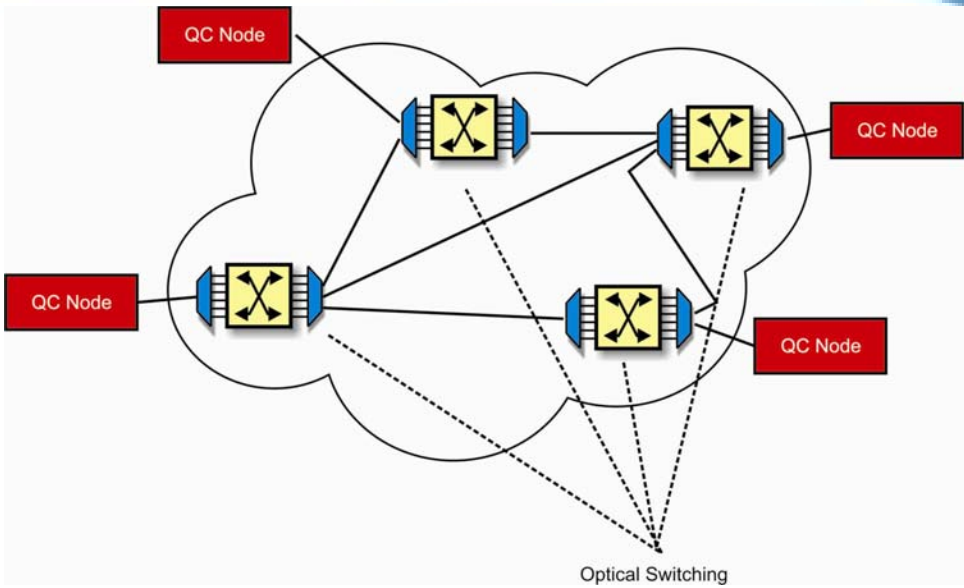
- Free space links to low-earth-orbit (LEO) satellites



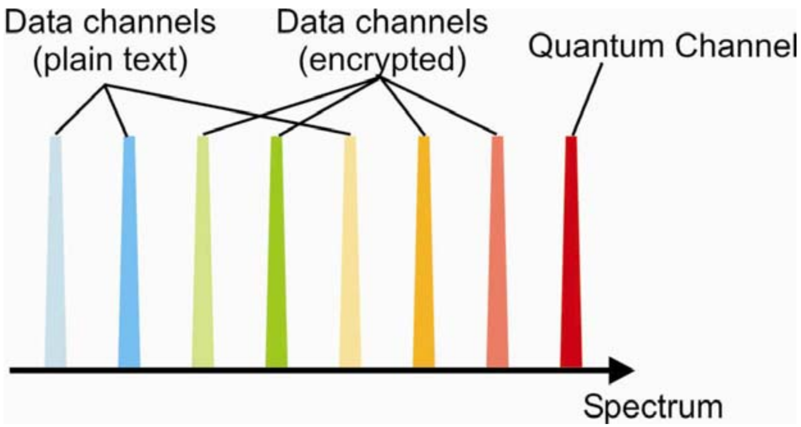
- Quantum relays and repeaters

Compatibility with conventional optical networks

- Optical switching



- WDM Links



Thank you very much for your attention

id Quantique SA
Chemin de la Marbrerie, 3
CH-1227 Carouge
Switzerland

Ph: +41 22 301 83 71
Fax: +41 22 301 83 79

info@idquantique.com
www.idquantique.com

Optical Taps

- Optical taps are cheap and simple to use

« Tapping a fibre-optic cable without being detected, and making sense of the information you collect isn't trivial but has certainly been done by intelligence agencies for the past seven or eight years. These days, it is within the range of a well funded attacker, probably even a really curious college physics major with access to a fibre optics lab and lots of time on his hands. »

John Pescatore, former NSA Analyst

The submarine « USS Carter » worth $4.1 bn will be able to tap and eavesdrop undersea cables.

Key use

- The key produced by a quantum cryptography system is used with conventional symmetric encryption algorithms
  - One-time pad → « unconditional security »
  - Other symmetric algorithms (AES, Tripe-DES, etc.) → enhanced security by frequent key change
- Why is Quantum Cryptography not used to transmit data?

1) Quantum Cryptography cannot guarantee that one particular bit will actually be received.

   With a random key, it is not a problem. With data, it is.

2) Quantum Cryptography does not prevent eavesdropping, but reveals it a posteriori. Sending a key and verifying its secrecy allows to prevent information leakage.

Device Authentication