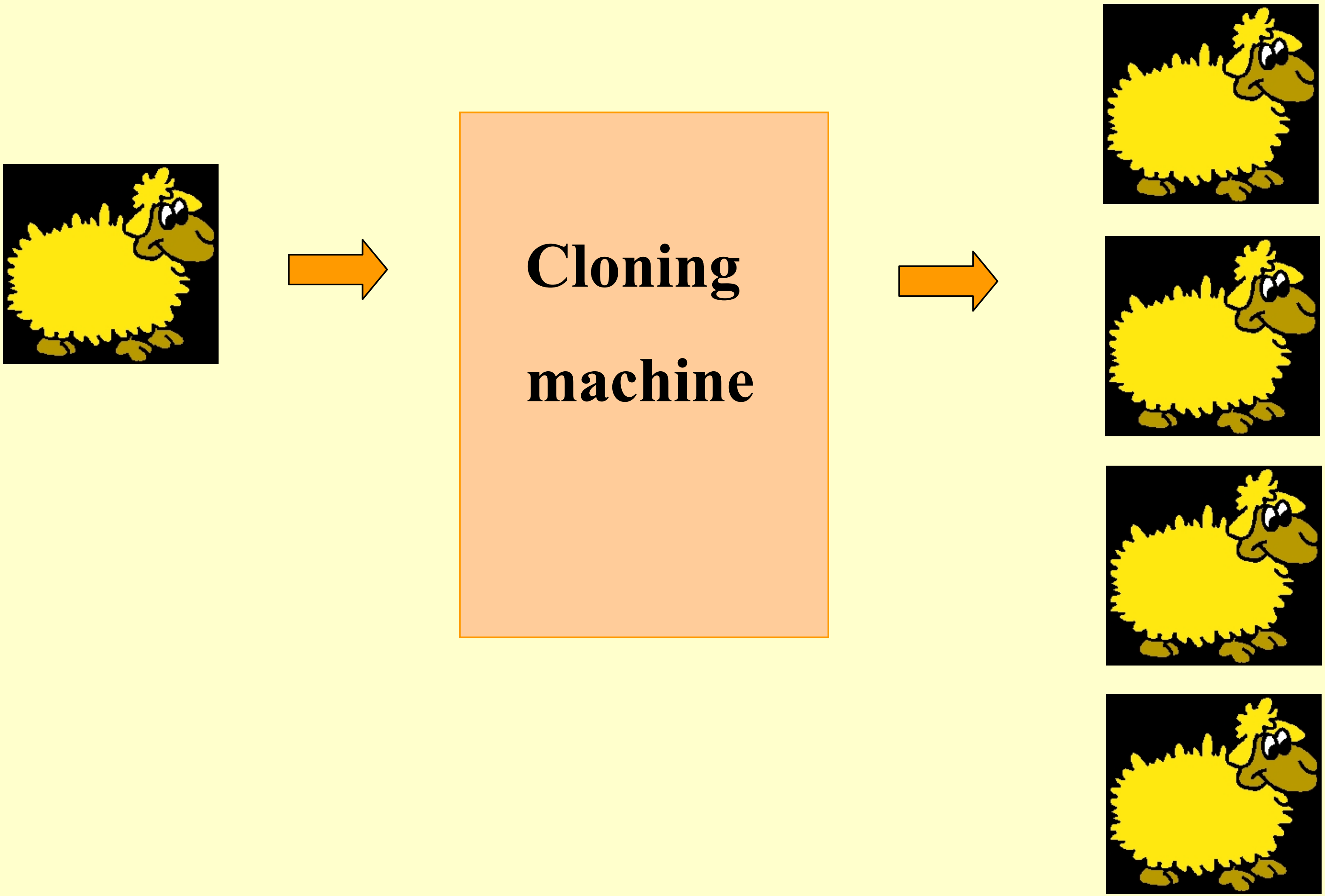
QUANTUM CLONING

Chiara Macchiavello

University of Pavia

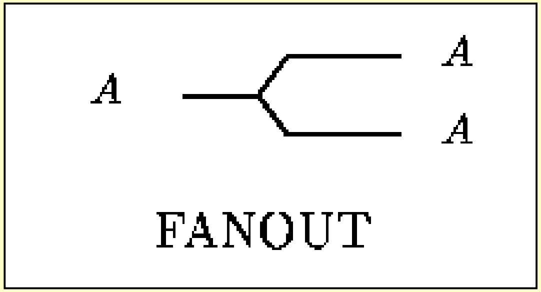
quantum information theory group

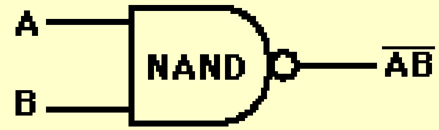
CLONING



IN CLASSICAL INFORMATION

Computing with bits (0 and 1)





A	B	Out
0	0	1
0	1	1
1	0	1
1	1	0

FANOUT and **NAND** are **universal gates for classical computation**

Measurements: bits can be measured perfectly

IN QUANTUM INFORMATION

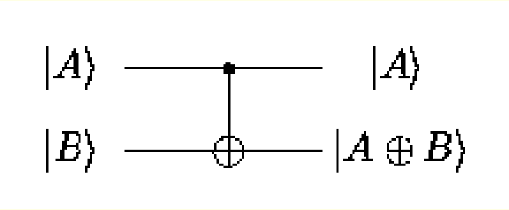
Qubits: $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ $\qquad |a|^2 + |b|^2 = 1$

NO CLONING THEOREM:

an unknown quantum state cannot be perfectly cloned

CONTROLLED NOT

Universal gate for quantum computation (with single qubit transformations)



$$|0\rangle\,|0\rangle \longrightarrow |0\rangle\,|0\rangle$$
$$|0\rangle\,|1\rangle \longrightarrow |0\rangle\,|1\rangle$$
$$|1\rangle\,|0\rangle \longrightarrow |1\rangle\,|1\rangle$$
$$|1\rangle\,|1\rangle \longrightarrow |1\rangle\,|0\rangle$$

With B=0 perfect cloning for a classical bit, but:

$$(a\,|0\rangle + b\,|1\rangle)\,|0\rangle \longrightarrow a\,|0\rangle\,|0\rangle + b\,|1\rangle|1\rangle \neq |\psi\rangle\,|\psi\rangle$$

NO CLONING THEOREM

Fundamental theorem in quantum information, with consequences for:

Quantum measurements

Quantum error correction

Superluminal communications

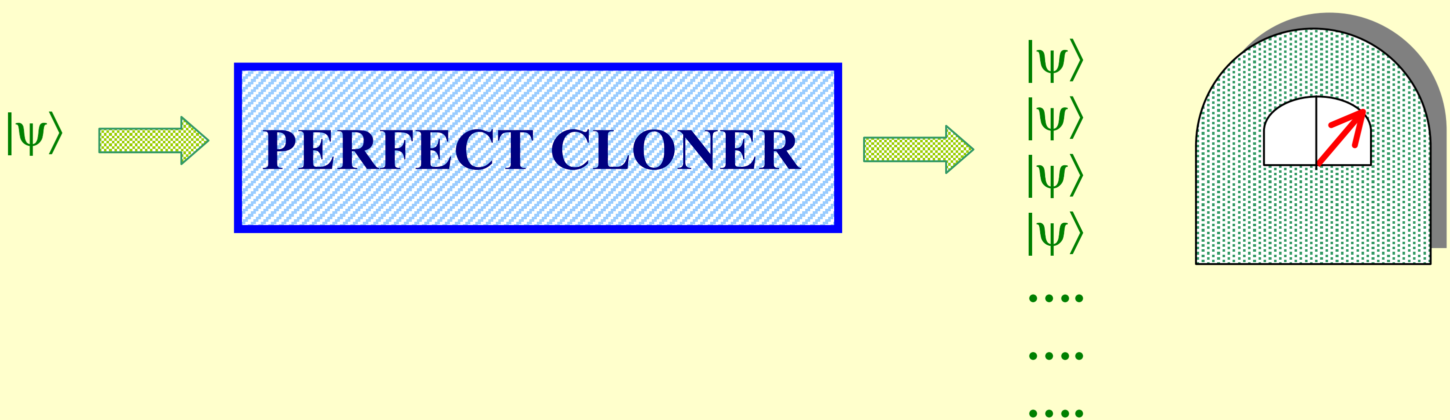
Secure communications

……………

QUANTUM MEASUREMENTS

No cloning ⟺ **No perfect measurability of a single quantum system**

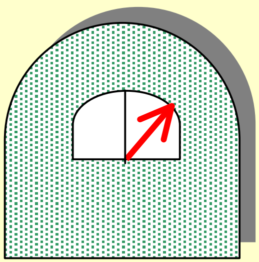
Perfect cloning ⟹ **Perfect measurements**



QUANTUM MEASUREMENTS

Perfect measurements → **Perfect cloning**

$|\psi\rangle$

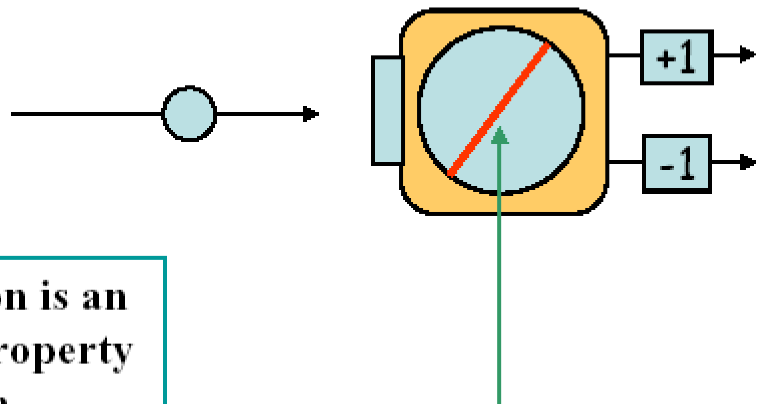


Full information on the state

Repreparation of $|\psi\rangle$

$|\psi\rangle$
$|\psi\rangle$
$|\psi\rangle$
$|\psi\rangle$

POLARIZATION



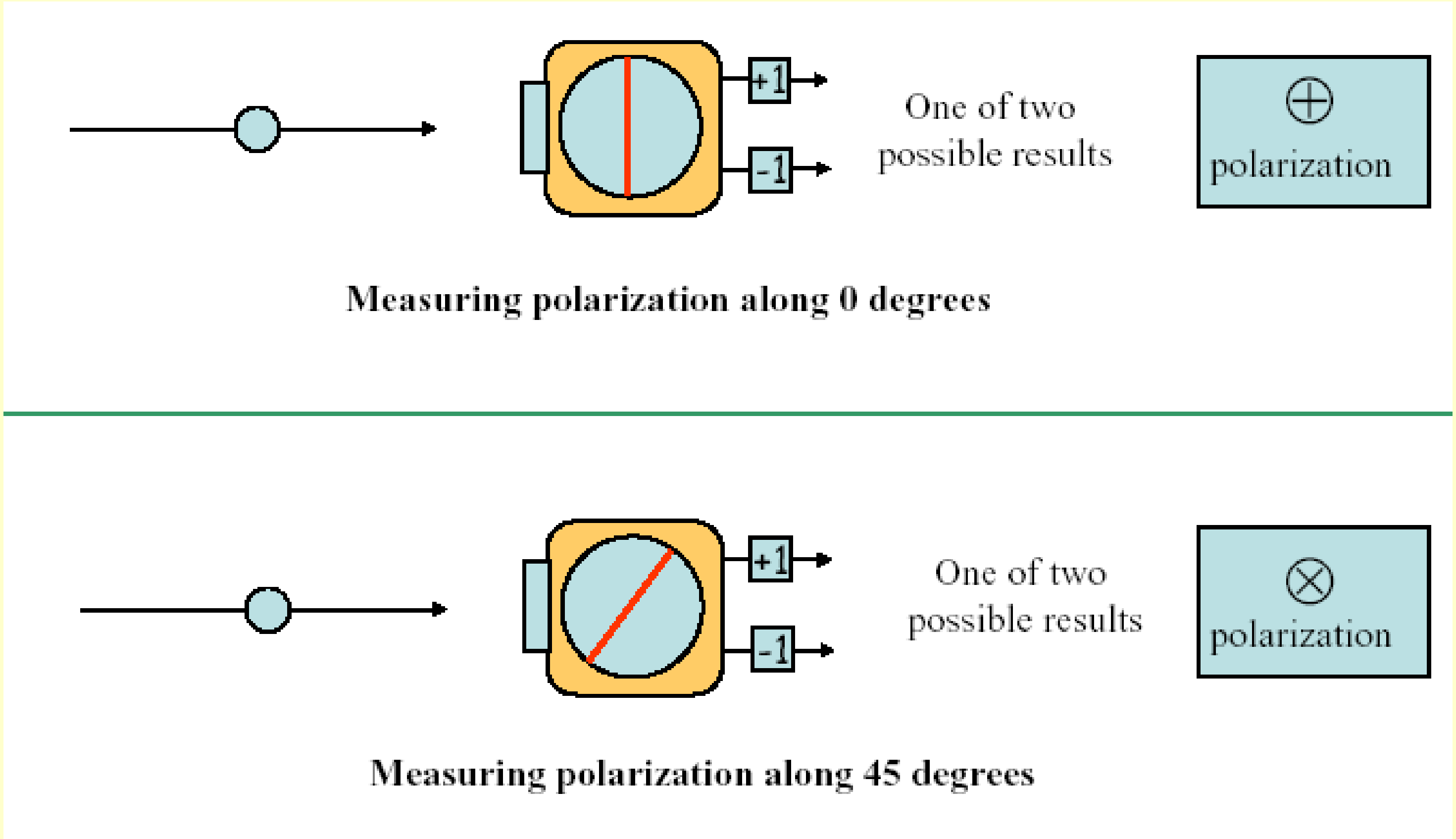
In any measurement
we can get only
two results: +1 or -1

(in units of $\hbar = 1.05 \times 10^{-34}$ Js)

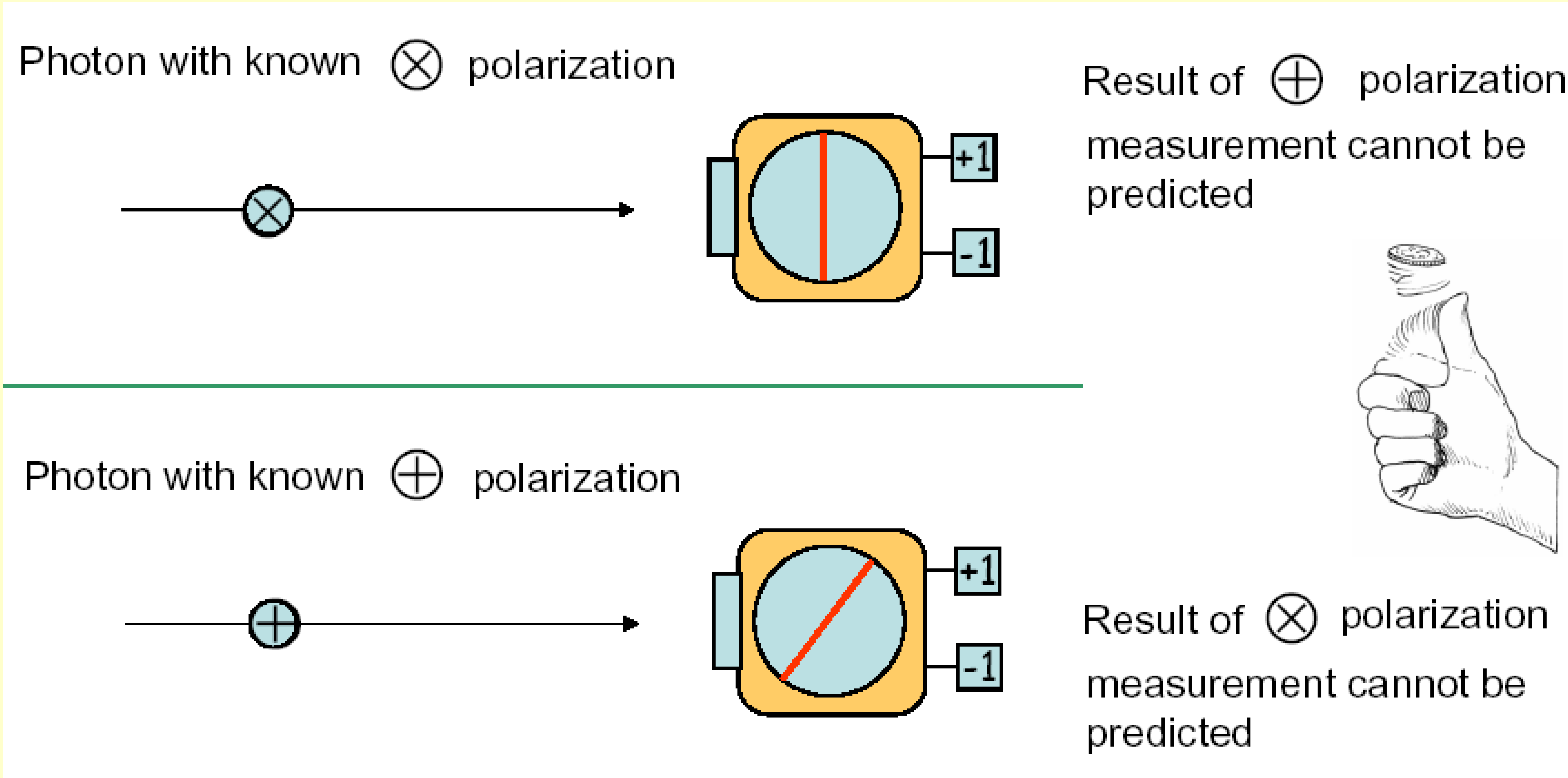
Polarization is an intrinsic property of a photon

We cannot just "measure polarization". We can only measure polarization with respect to some specified direction

POLARIZATION MEASUREMENT



COMPLEMENTARY PROPERTIES



A photon cannot have definite ⊕ and ⊗ polarization at the same time

ENTANGLEMENT

Entangled state for two qubits A and B:

$$|\Psi_{AB}\rangle \neq |\psi_A\rangle|\psi_B\rangle$$

E.g.: singlet state

$$(|\rightarrow\uparrow\rangle - |\uparrow\rightarrow\rangle)/\sqrt{2}$$

If the polarizations of A and B are measured along the same direction they always give opposite results

Strong correlations, with nonlocal character (q. teleportation)

SUPERLUMINAL COMMUNICATIONS

Perfect cloning would allow superluminal communications:

Alice ← $|\uparrow\rightarrow\rangle - |\rightarrow\uparrow\rangle$ → **Bob**

Information encoded into the type of measurement

Perfect cloner

Measure ⊕ ⟹ ↑ or →

Measure ⊗ ⟹ ↗ or ↘

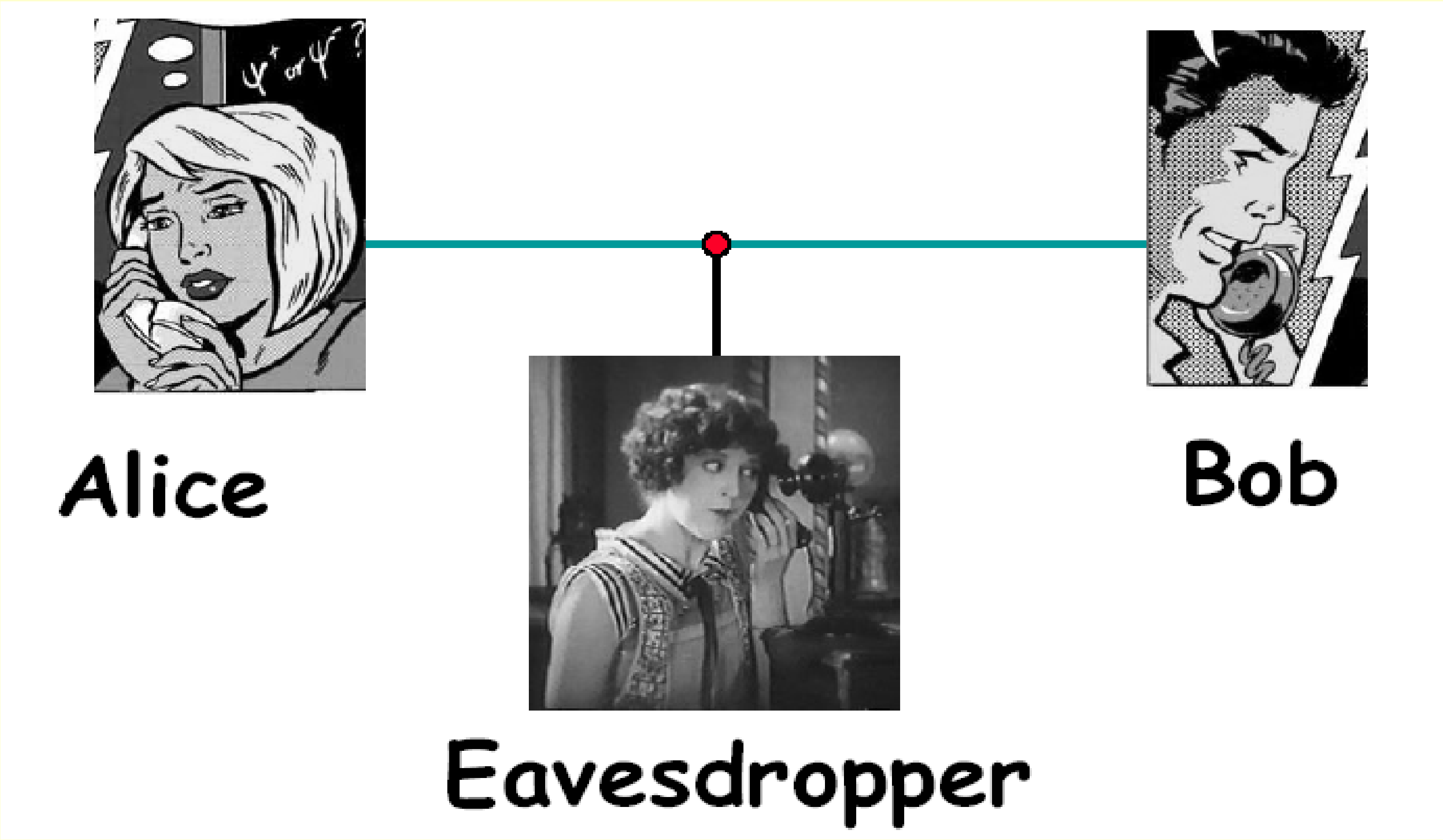
QUANTUM CRYPTOGRAPHY

Why is it important?

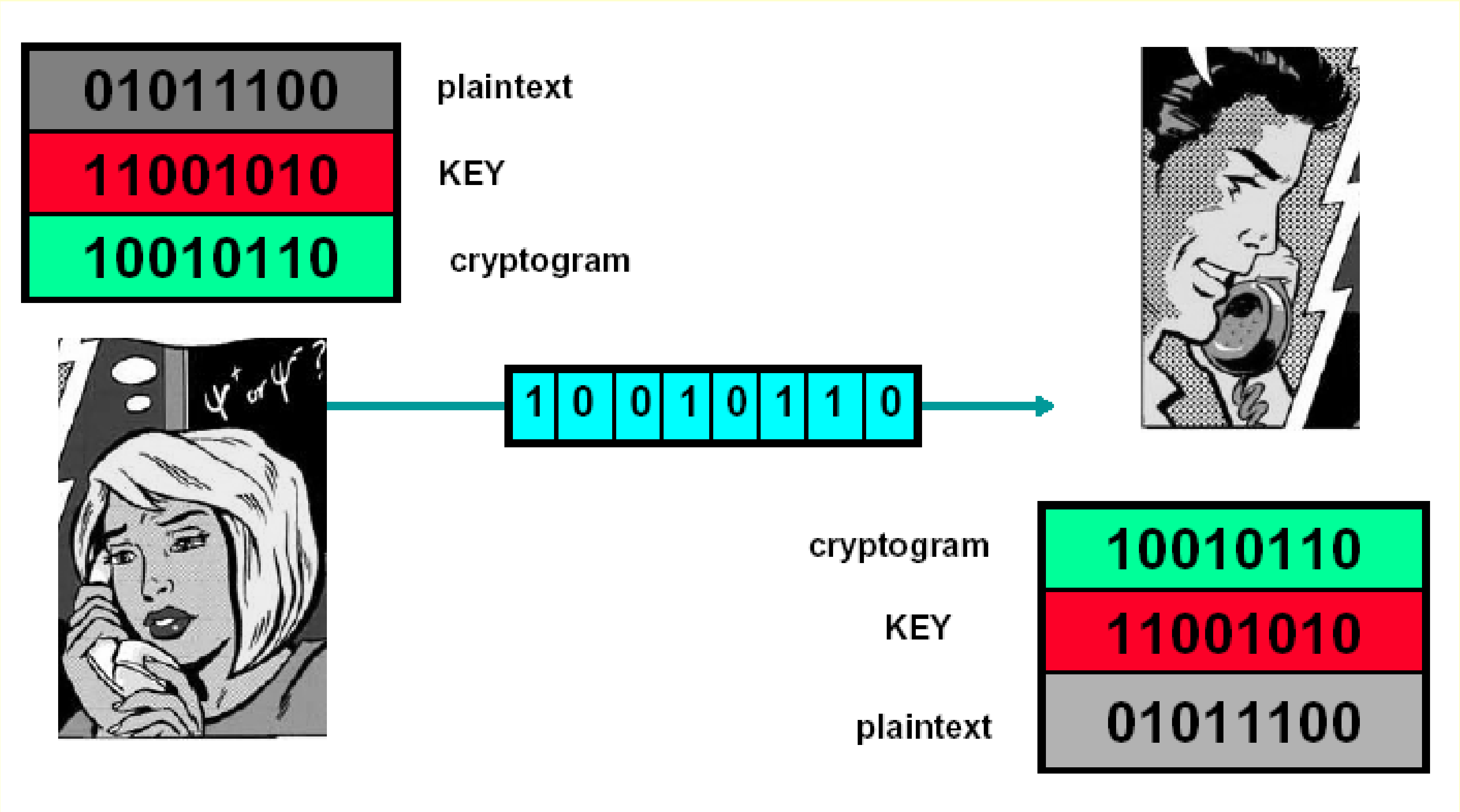
It solves the problem of the security of key distribution in classical protocols

In the presence of a quantum computer, public key cryptosystems like the RSA would be insecure

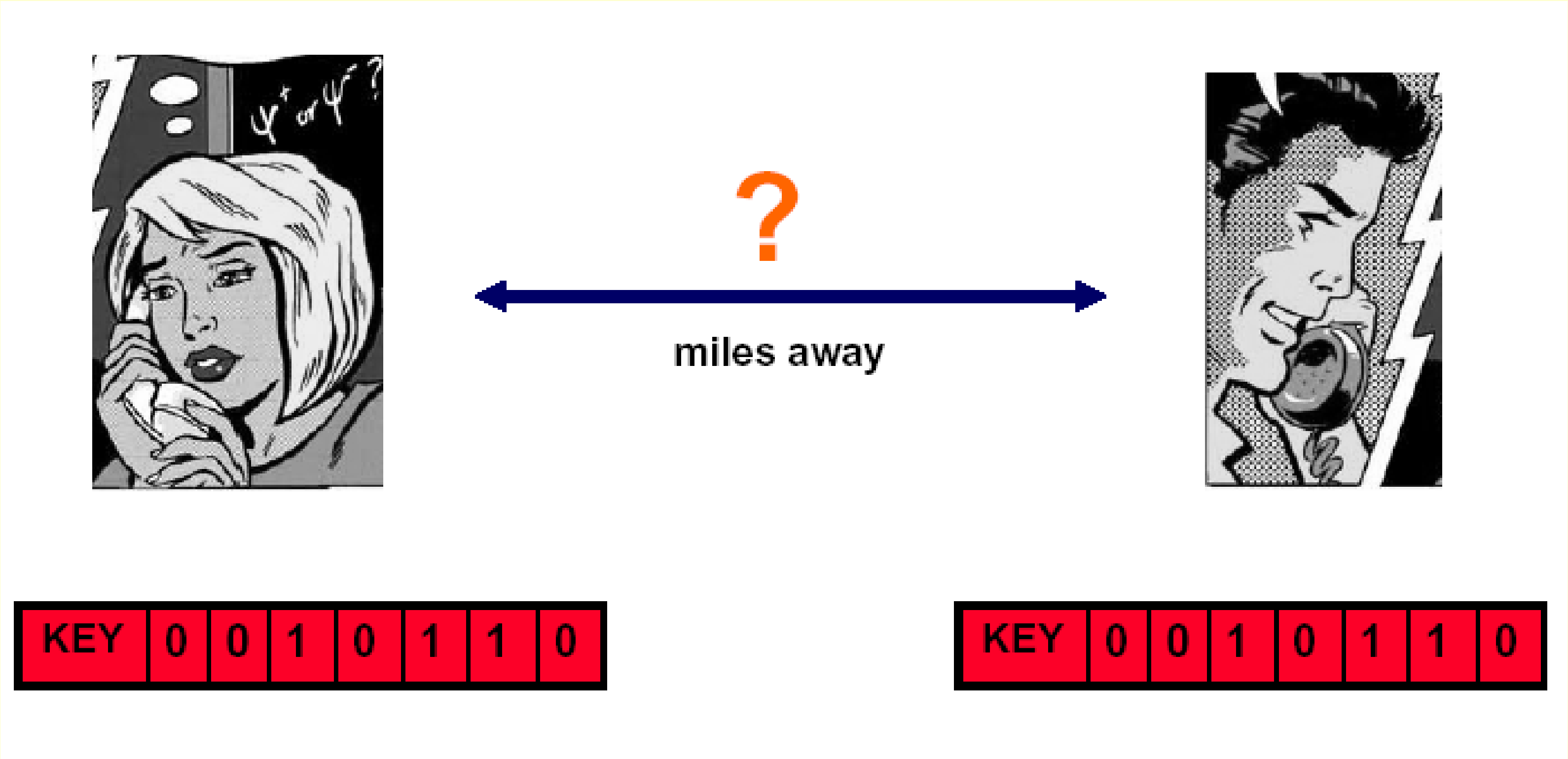
SCENARIO



ONE-TIME PAD


01011100
plaintext
11001010
KEY
10010110
cryptogram
1 0 0 1 0 1 1 0
cryptogram
10010110
KEY
11001010
plaintext
01011100

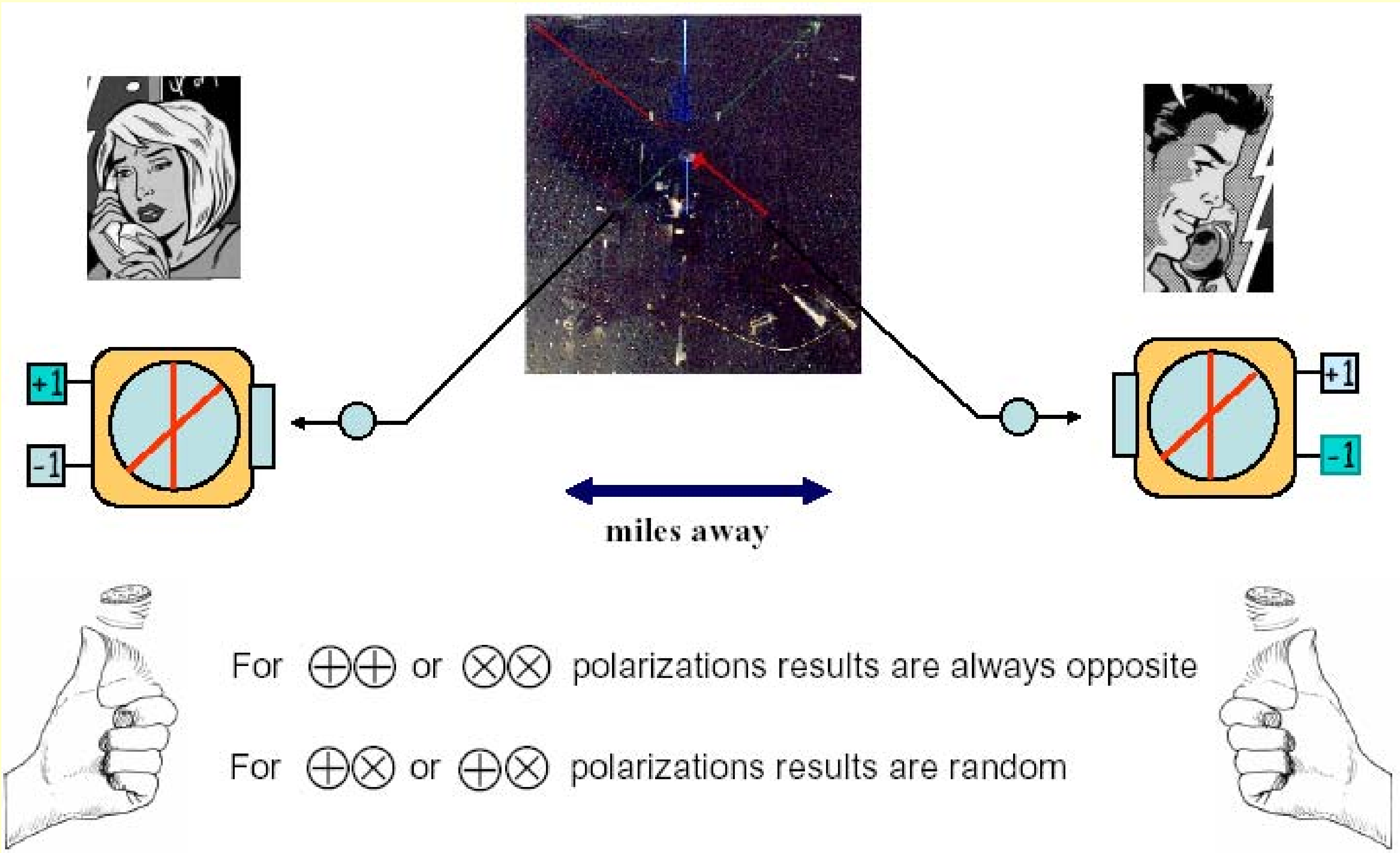
KEY DISTRIBUTION PROBLEM



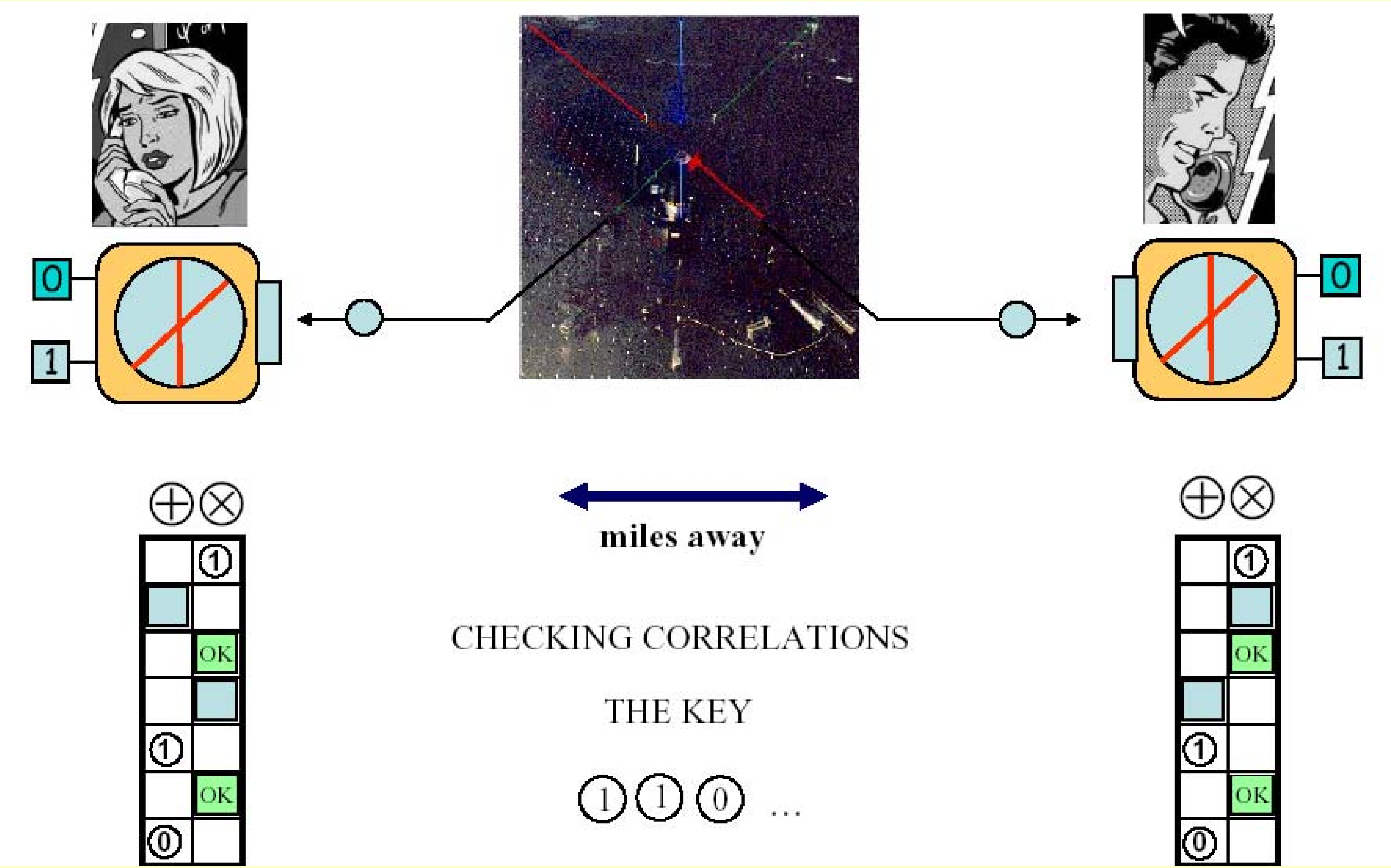
Quantum schemes: **Single particles (Bennett & Brassard 84)**

Entanglement (Ekert 91)

WITH ENTANGLEMENT



QUANTUM KEY DISTRIBUTION

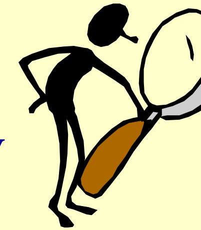


SECURITY

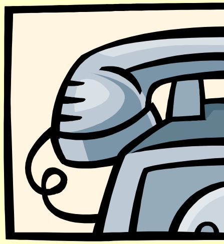
If perfect cloning were possible, the eavesdropper would recover complete information about the state shared by Alice and Bob

Any eavesdropping attempt disturbs the systems and introduces errors that can be detected

IN SUMMARY



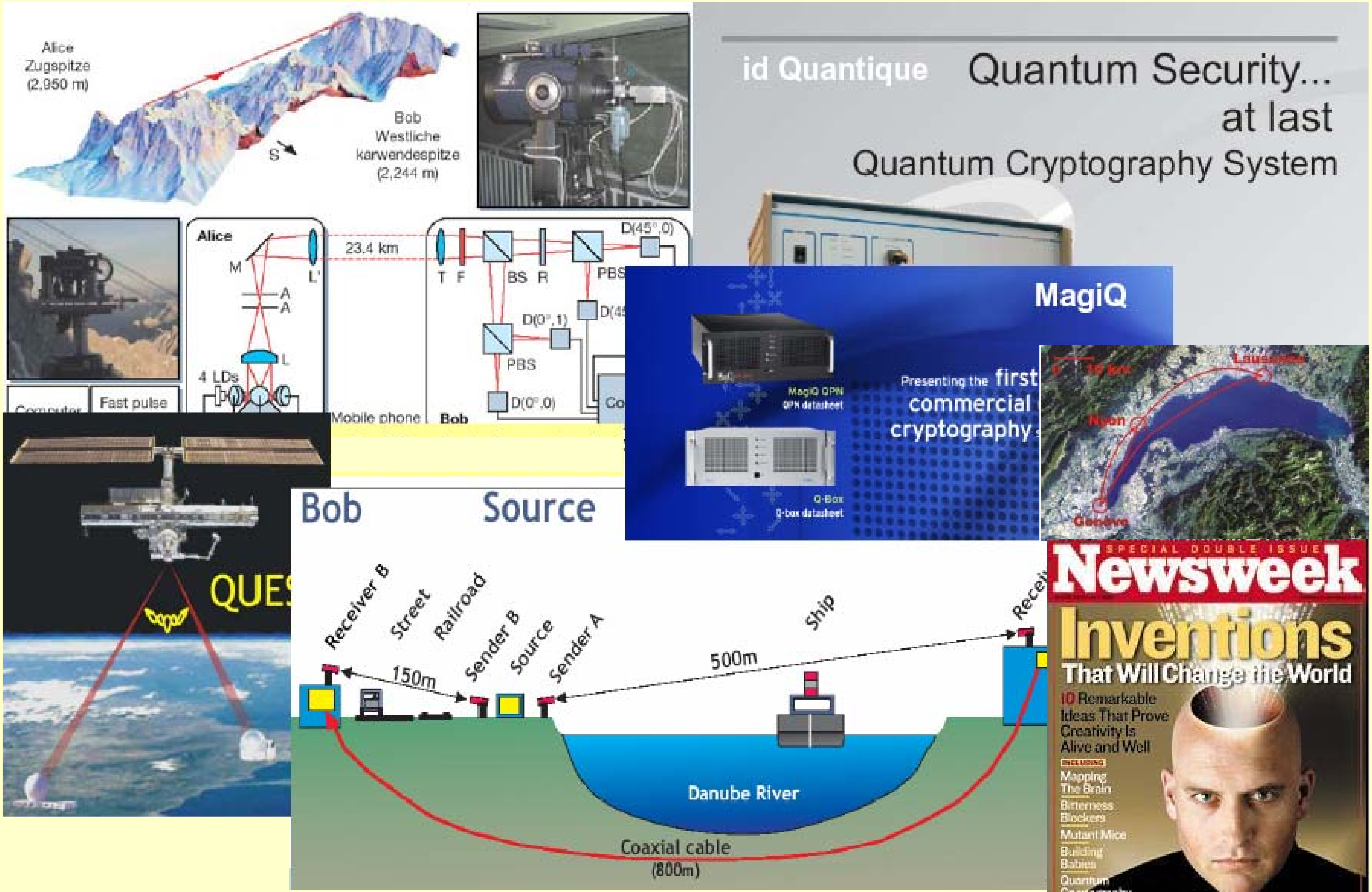
Measurements: Alice and Bob measure the polarization with setting $\oplus$ or $\otimes$ chosen at random and independently



Classical communication: the type of measurement is revealed classically and only matching cases are selected

Security test: subsets of data are used to test the presence of an eavesdropper

TODAY


Alice
Zugspitze
(2,950 m)
Bob
Westliche
karwendespitze
(2,244 m)
S
Alice
M
L'
A
A
L
4 LDs
23.4 km
Fast pulse
Mobile phone
Bob
T
F
BS
R
PBS
D(45°,0)
D(0°,1)
PBS
D(0°,0)
id Quantique
Quantum Security...
at last
Quantum Cryptography System
MagiQ
MagiQ QPN
QPN datasheet
Q-Box
Q-box datasheet
Presenting the first
commercial
cryptography
Lausanne
Nyon
Geneva
Newsweek
SPECIAL DOUBLE ISSUE
Inventions
That Will Change the World
10 Remarkable
Ideas That Prove
Creativity Is
Alive and Well
Mapping
The Brain
Bitterness
Blockers
Mutant Mice
Building
Babies
Bob
Source
Receiver B
Street
Railroad
Sender B
Source
Sender A
Ship
150m
500m
Danube River
Coaxial cable
(800m)