... rýchlosťou vetra


[The Great Days of Sail by Andrew Shewan; autor neznámy ~1886]

Daniel Nagaj

universität wien
SAV

... rýchlosťou svetla

[Chang'e 5 T1, Xinhua/CNSA, 2014]

Daniel Nagaj

universität wien

SAV

čudesné okamžité pôsobenie na diaľku?

Daniel Nagaj

universität wien

SAV

instantné správy

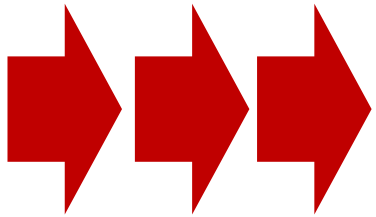
teleportácia

telepatia

[ESA/Rosetta/MPS for OSIRIS]

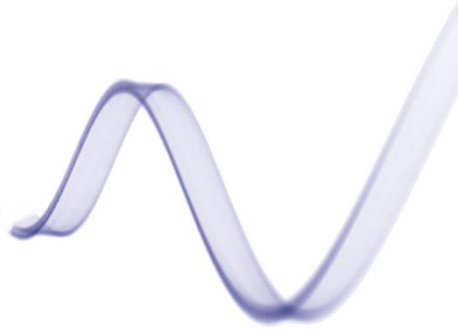
1 **run like the wind**

drahocenné informácie



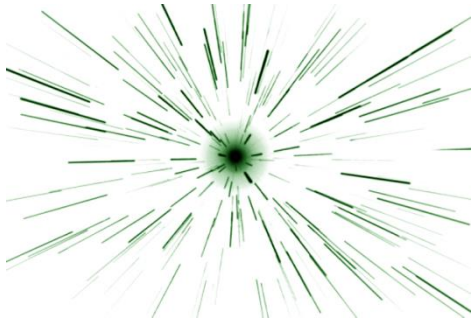
2 **traveling light**

chytáme elektromagnetické vlny



3 **warp speed**

čudesná kvantová mechanika



ako posielať správy?

1 Posielanie varovaní a správ

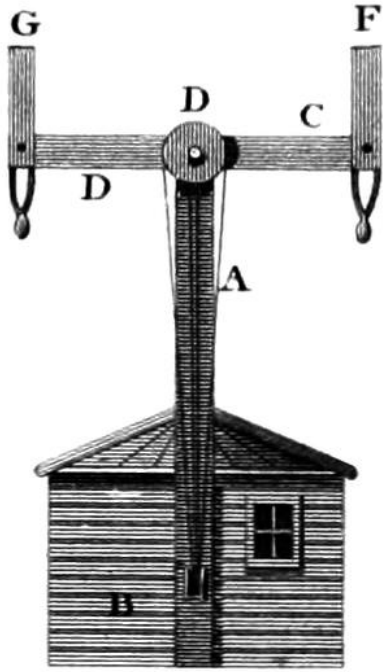
- strážne ohne
  rýchlosť?
  jediná správa: idú!
  farba ohňa? dym?
- bežec (Maratón)
  náročné na ľudí
- presedlávanie koní
  rýchlosť?
- hovoriace bubny
  zmeny frekvencií

1 Mechanické prepojenie

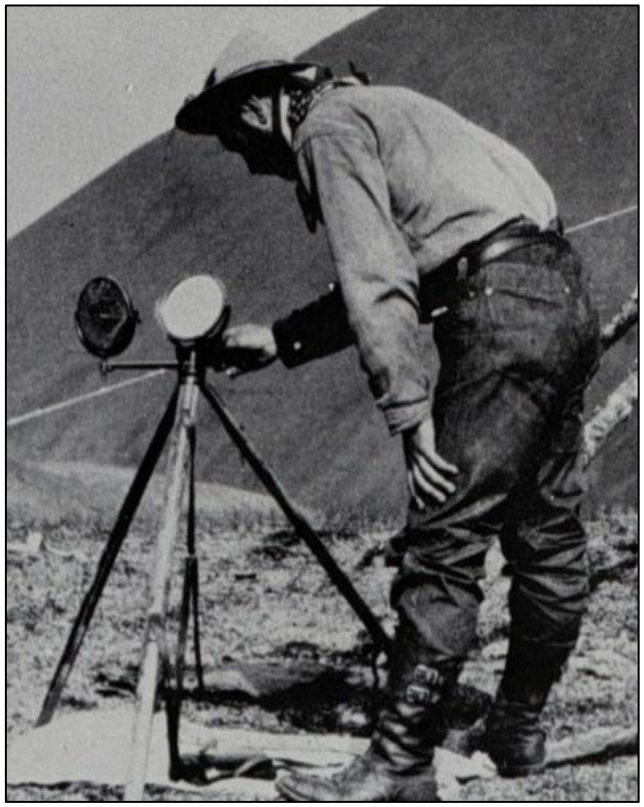
- píšťalový organ
  drevo, koža, kov
  láme sa to, starne
- dlhá tyč?
  mlátiť po koľajniciach?
  poťahovať za drôty?
  trenie, mráz
- pneumatický telegraf
  ťažké tlakovať, údržba

1 Vizuálne signály

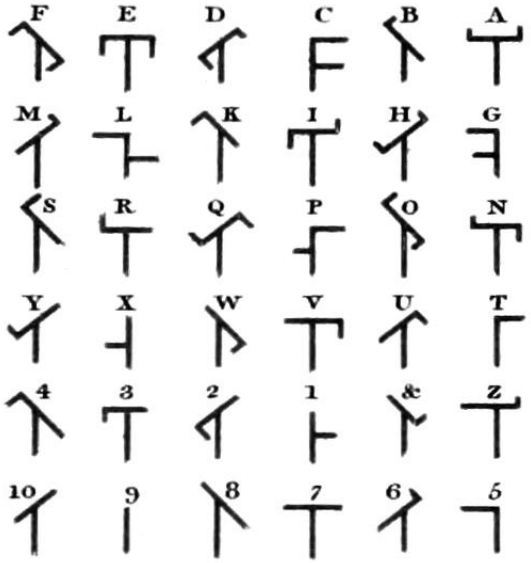
- semaforové systémy
  C. Chappe (1792, 556 veží, 4800 km)



- heliograf (GB až do 1960)



[US Nat'l Oceanic and Atmospheric Administration, 1910]



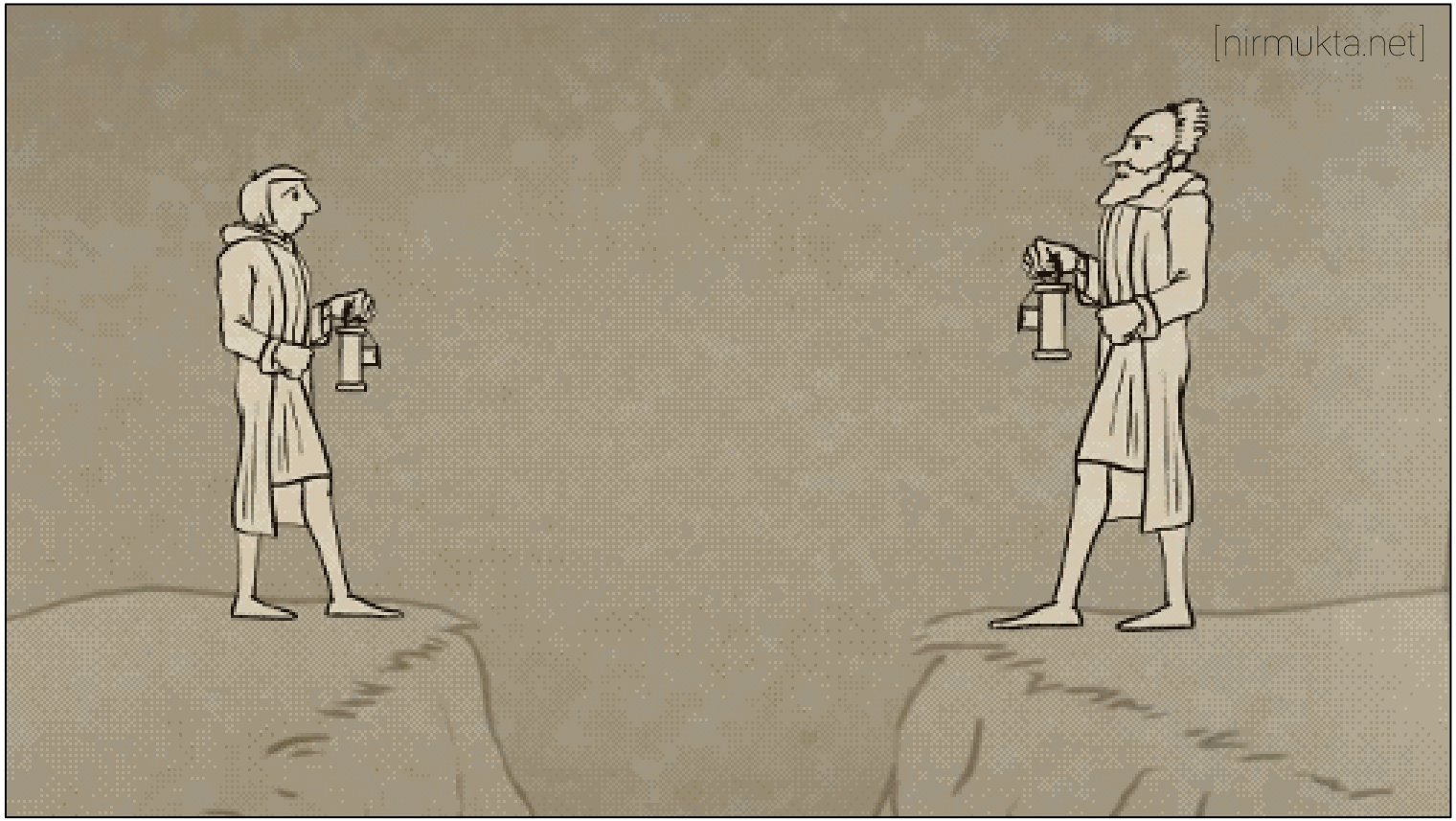
[John Farey, Jr., Rees's Cyclopædia Vol. IV, "TELEGRAPH", Fig. 4]

1 Svetlo je rýchle!

- Jára Cimrman: svetlo > zvuk (sviečka a zvonček)

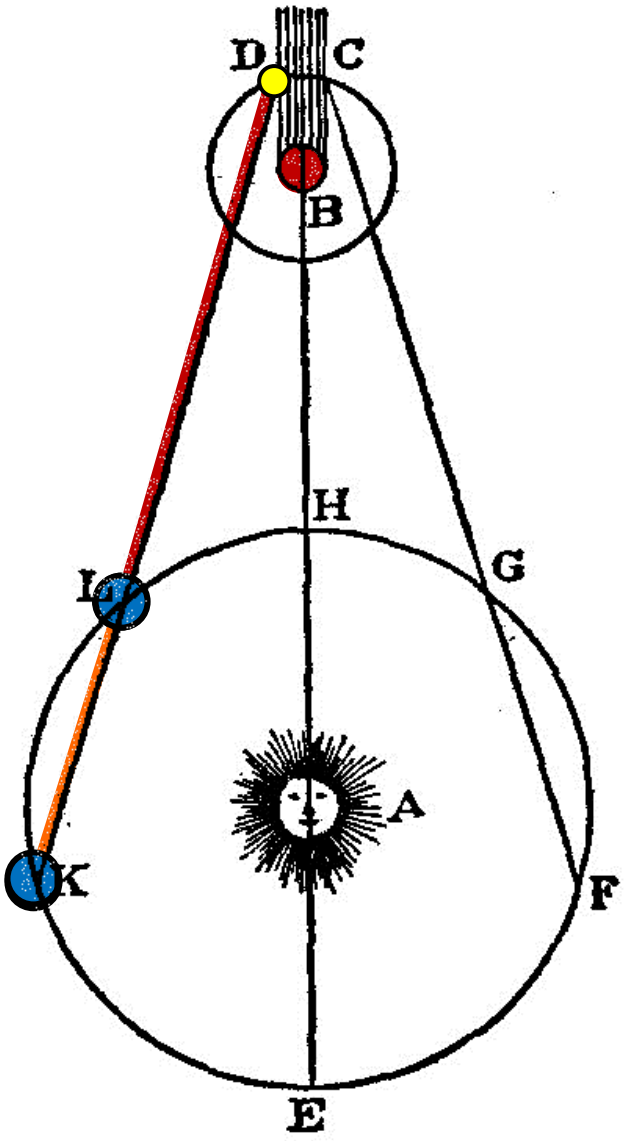
1 Svetlo je rýchle!

- Jára Cimrman: svetlo > zvuk (sviečka a zvonček)
- Galileo: zakrývanie a odkrývanie lampy



1 Konečná rýchlosť svetla

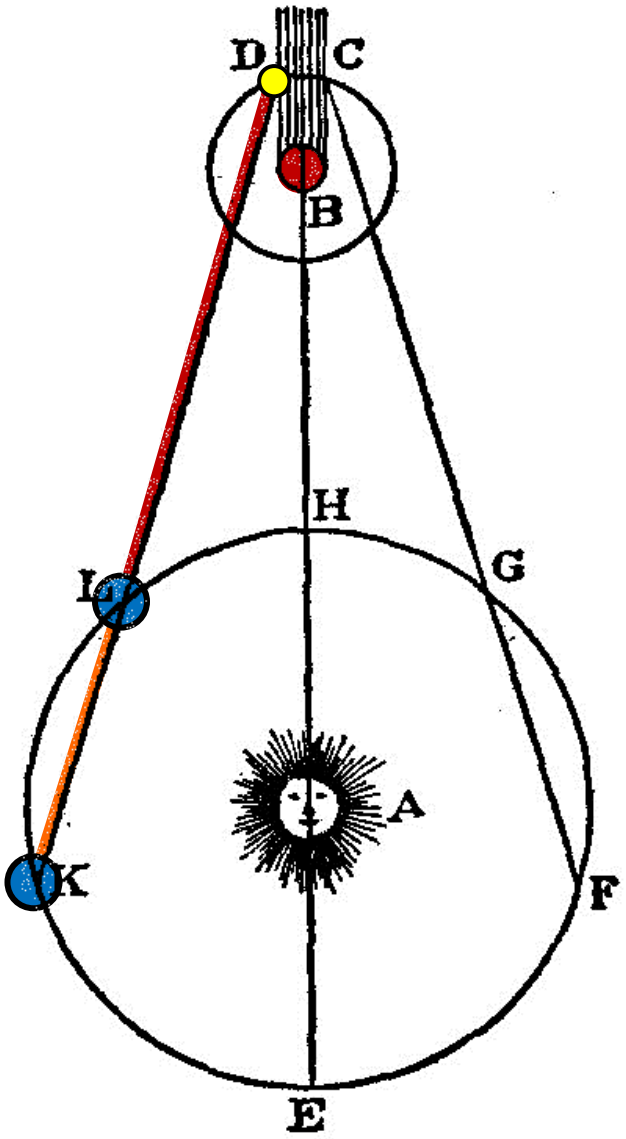
- Ole Rømer (1676)
  meškajúci Io (mesiac Jupitera)
  doba obehu ~42 hodín
  odhadnite meškanie



[J.P.Trap, Berømte danske mænd og kvinder]

1 Konečná rýchlosť svetla

- Ole Rømer (1676)
  meškajúci Io (mesiac Jupitera)
  doba obehu ~42 hodín
  odhadnite meškanie

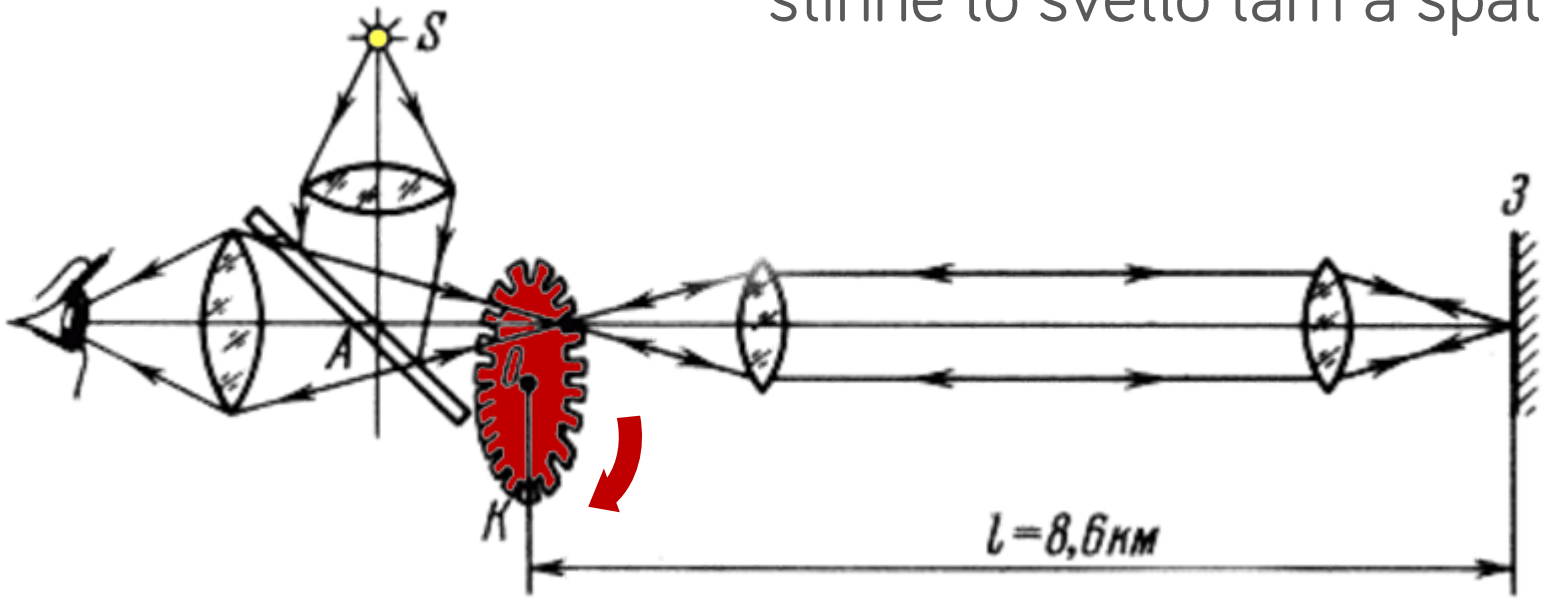


- Ch. Huygens
  $16\,^{2}/_{3}$ priemerov Zeme/sekunda

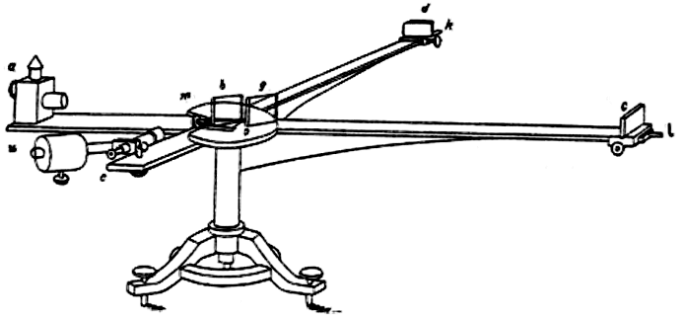
- I. Newton
  "For it is now certain from the phenomena of Jupiter's satellites … that light … requires about 7 or 8 minutes to travel from the sun to the earth." [Principia I, sec. XIV]

1 Meriame rýchlosť svetla na Zemi

- Hippolyte Fizeau (1849) roztočené ozubené koleso, stihne to svetlo tam a späť?



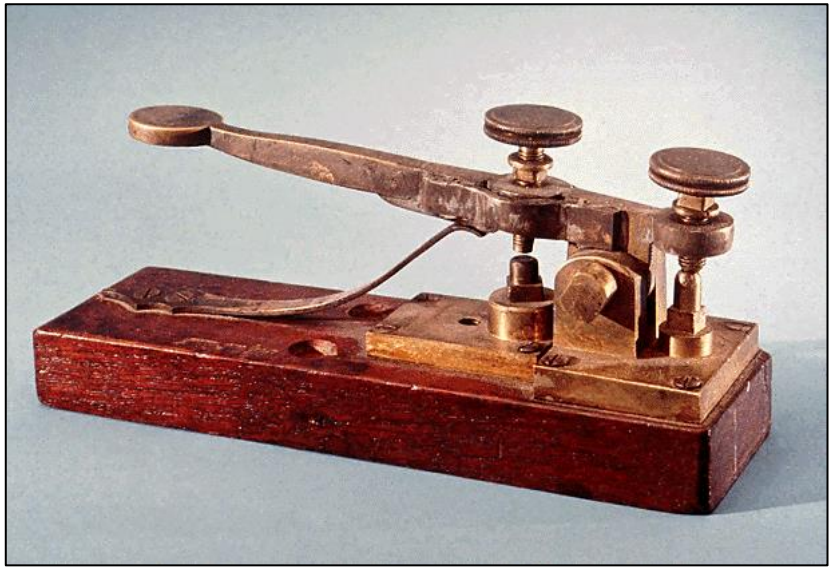
- Foucault: roztočíme zrkadlo



- Michelson/Morley: interferencia

1 Elektrický signál

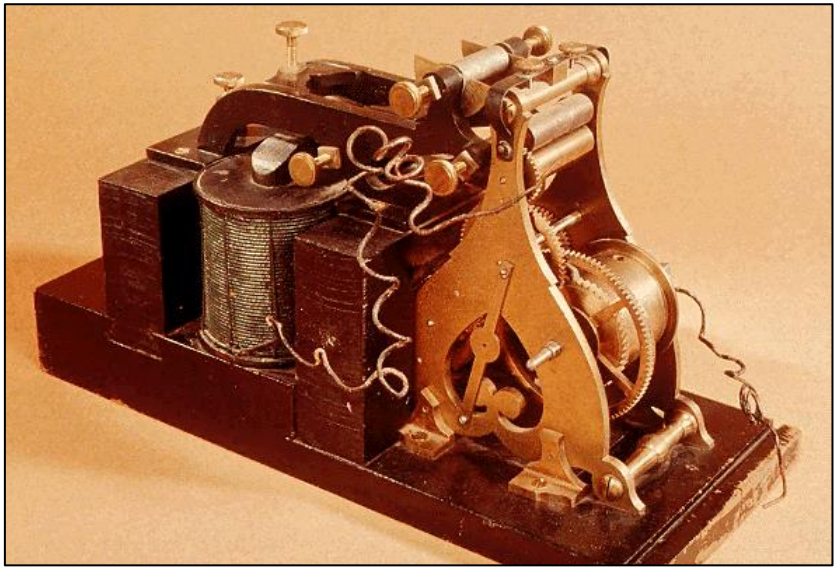
- von Sömmerring (1809)
  drôty, prúd, bublinky
- Wheatstone, Cooke (1839)
  vychýlené ručičky



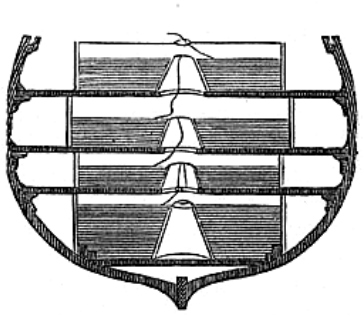
[Smithsonian National Museum]

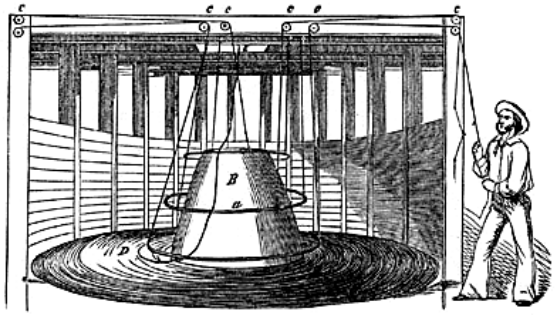
1 Elektrický signál

- von Sömmerring (1809)
  drôty, prúd, bublinky
- Wheatstone, Cooke (1839)
  vychýlené ručičky
- Morse (1837): telegraf
  len 2 drôty
  automatický zápis
- transatlantický kábel (1858, 1866)

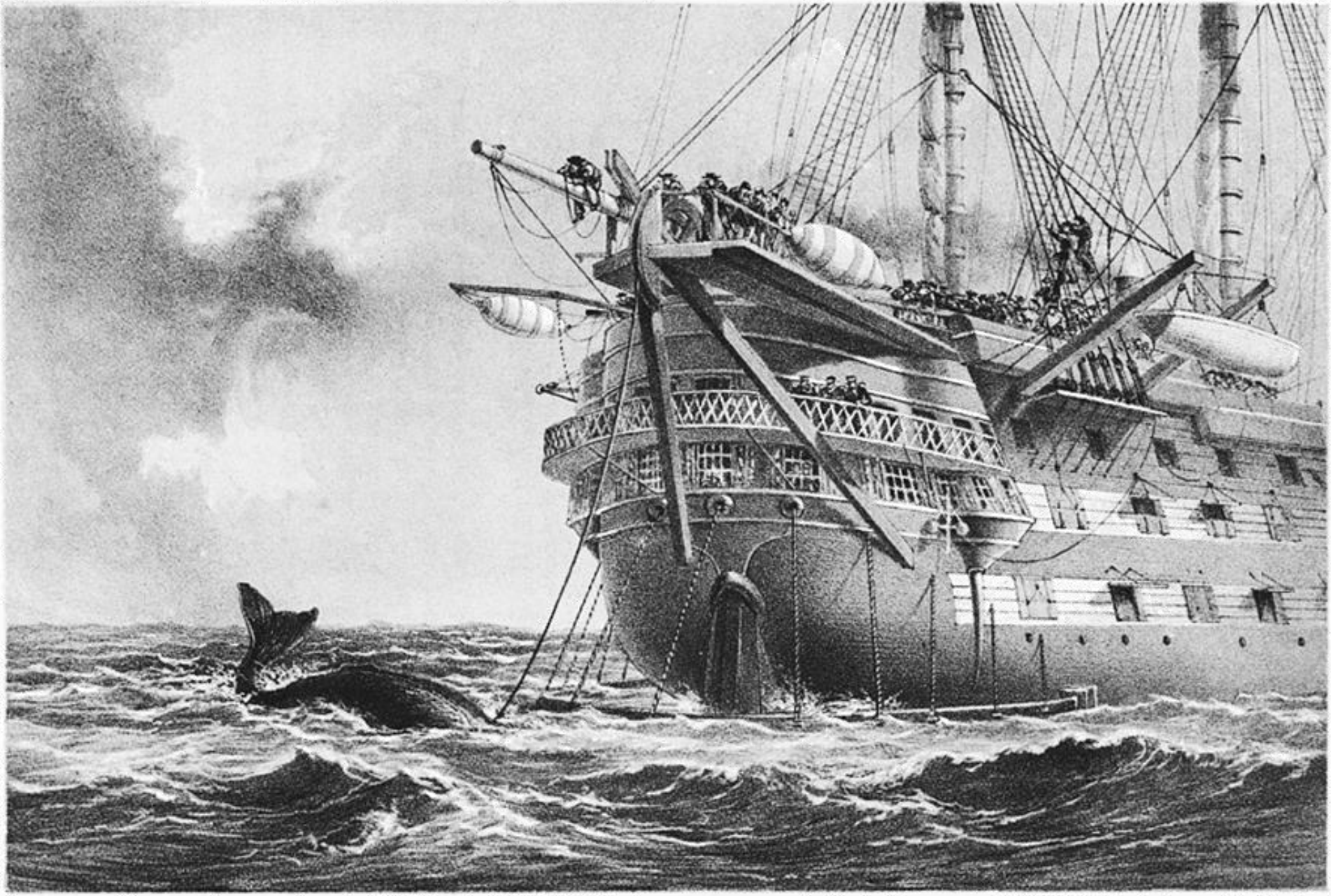


[Smithsonian National Museum]



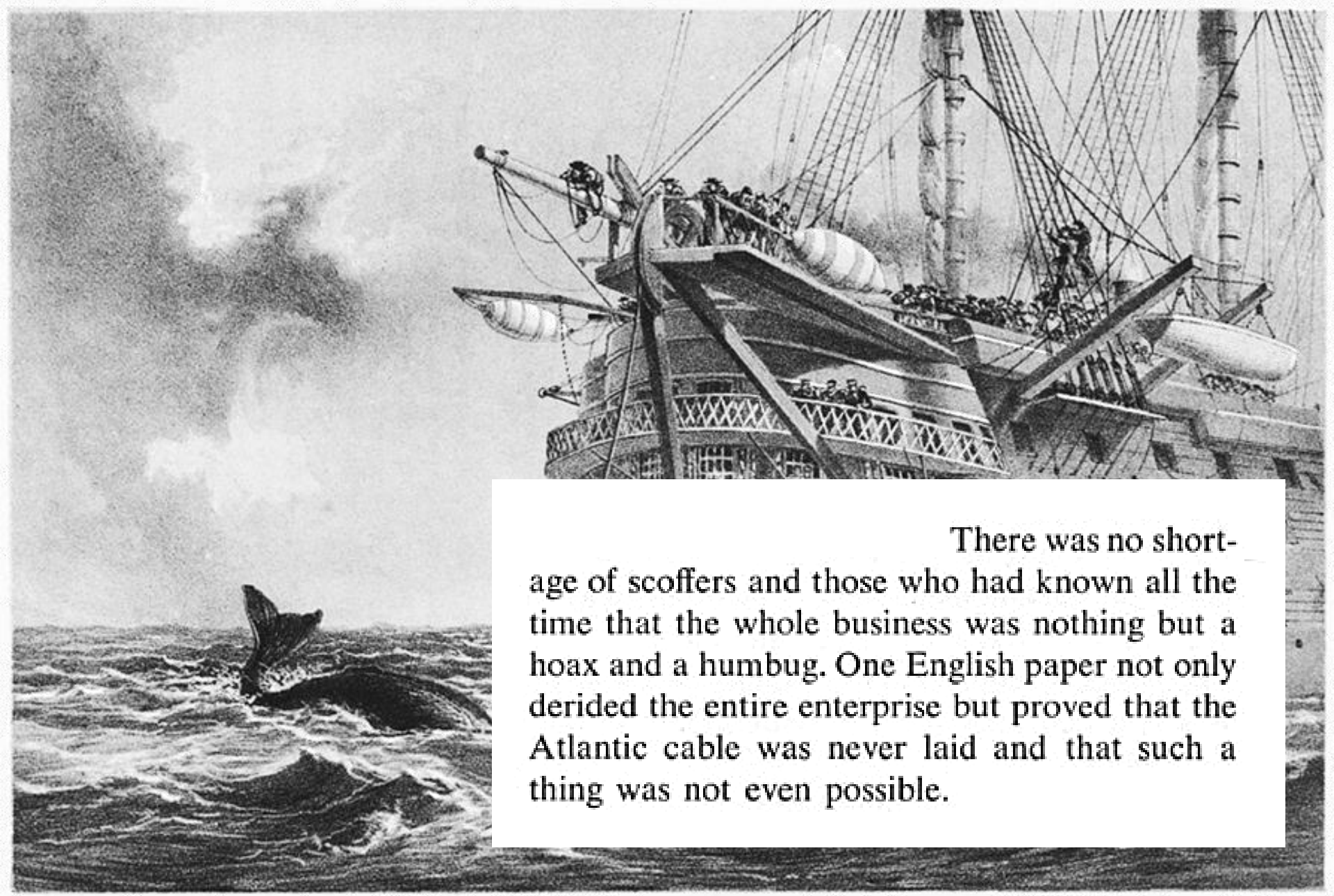


[Bern Dibner, The Atlantic Cable]



The stern of the Agamemnon with the cable issuing from the sheaves. The crew watches anxiously as a whale crosses the line. The "crinoline" about the rudder post was to keep the cable from being injured by the ship's propeller.

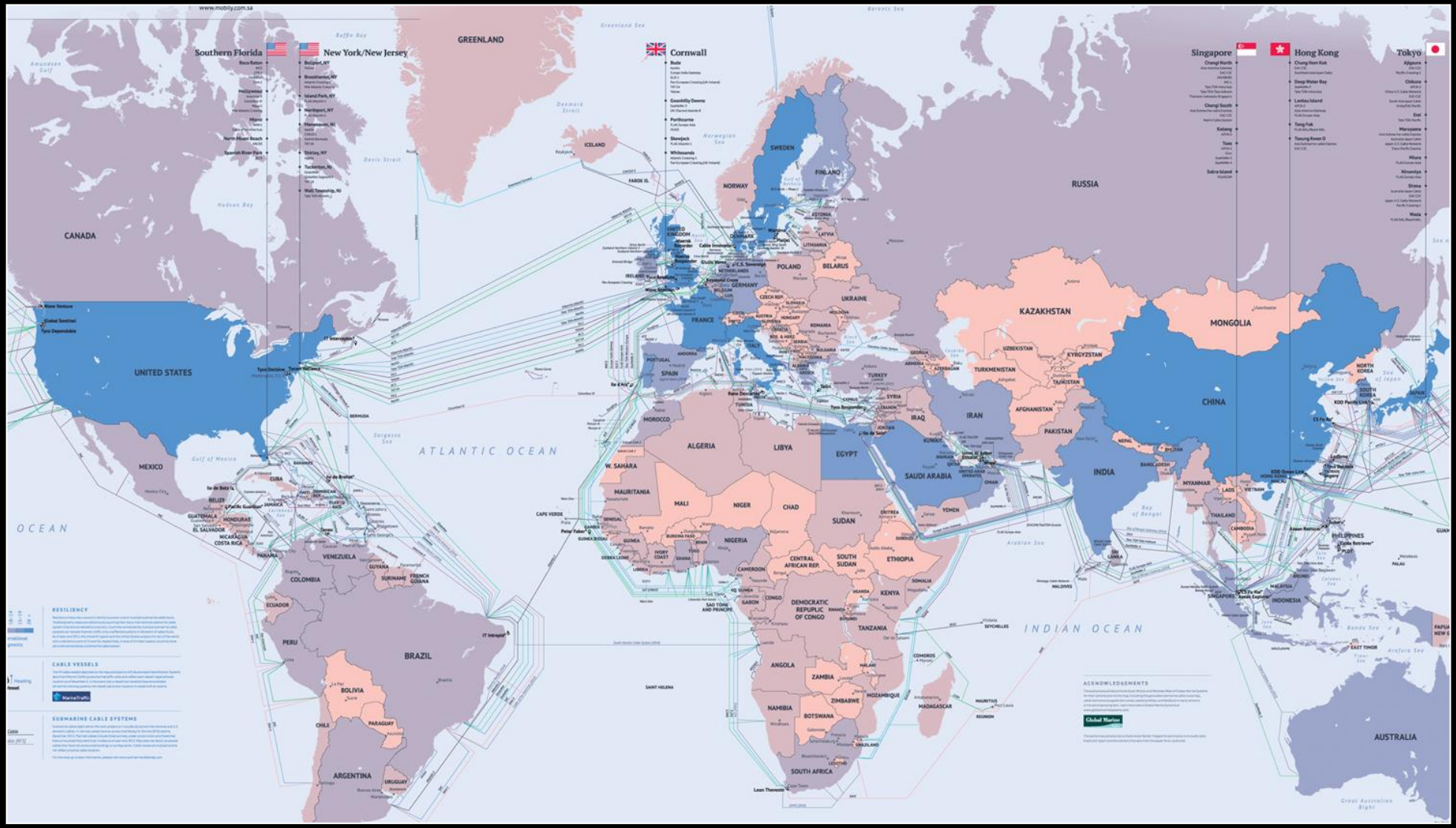
[Bern Dibner, The Atlantic Cable]



There was no shortage of scoffers and those who had known all the time that the whole business was nothing but a hoax and a humbug. One English paper not only derided the entire enterprise but proved that the Atlantic cable was never laid and that such a thing was not even possible.

The stern of the Agamemnon with the cable issuing from the sheaves. The crew watches anxiously as a whale crosses the line. The "crinoline" about the rudder post was to keep the cable from being injured by the ship's propeller.

[Bern Dibner, The Atlantic Cable]



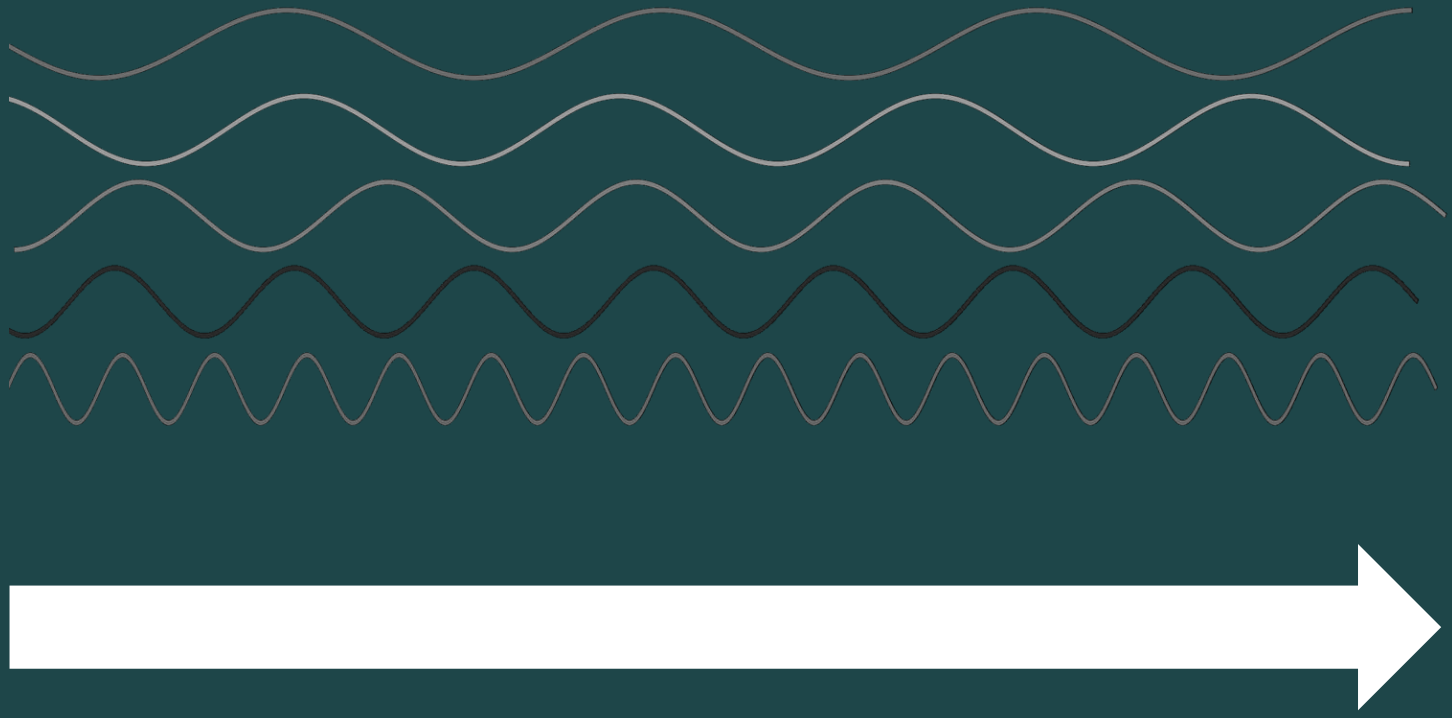
sieť podmorských optických káblov 2014 [TeleGeography]

žralok útočí na Google kábel, 15.8.2014 [youtube.com/watch?v=XMxkRh7sx84]

1 Grasshopper telegraphy (Edison's "in-flight wifi")

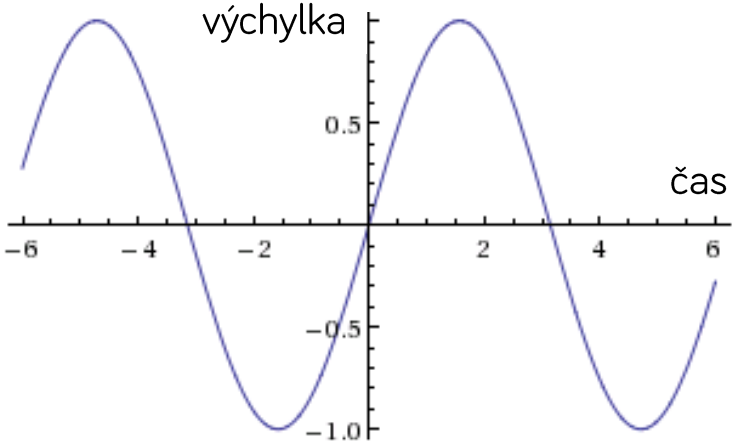
~1885, elmag. indukcia, preskok telegraf. signálu medzi vlakom a drôtmi pri trati

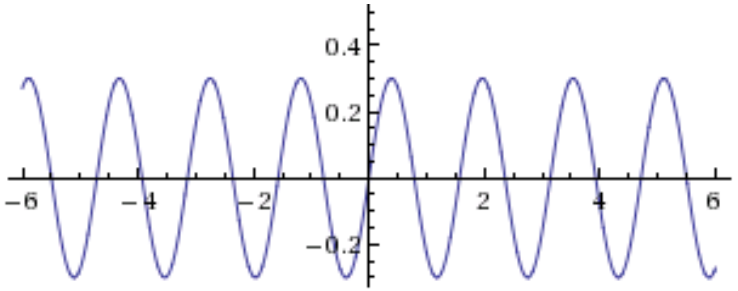
správy na vlnách (E&M)

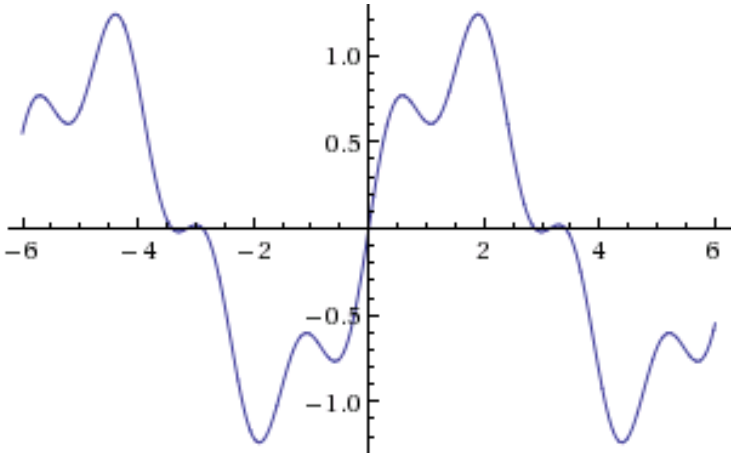


2 Zložitejšie signály?

- viac signálov naraz?
- reproduktor: dva tóny?

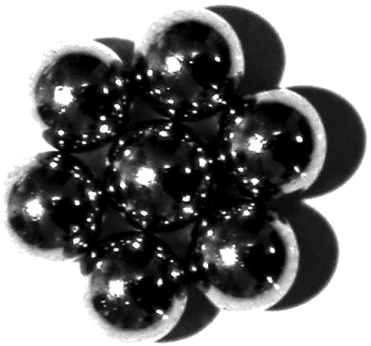


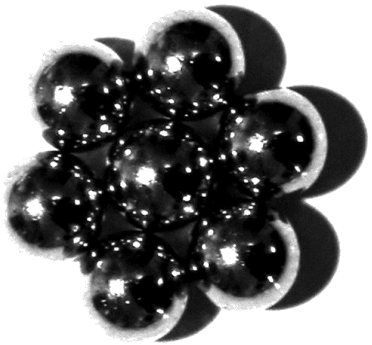




2 Elektromagnetické vlny

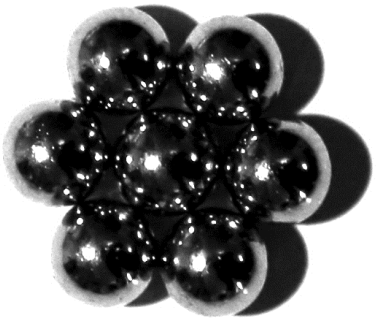
- pôsobenie na diaľku?

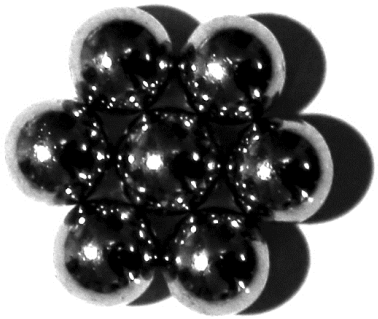




2 Elektromagnetické vlny

- pôsobenie na diaľku?

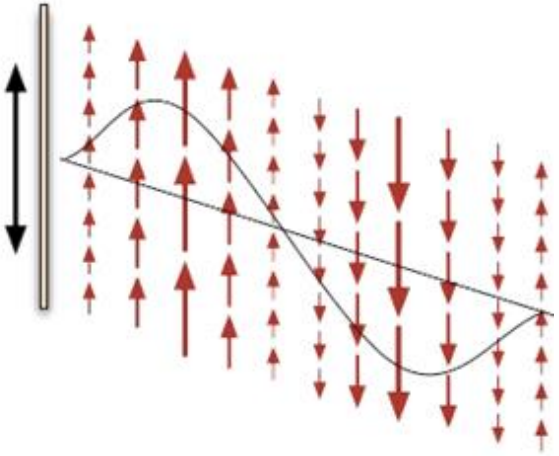




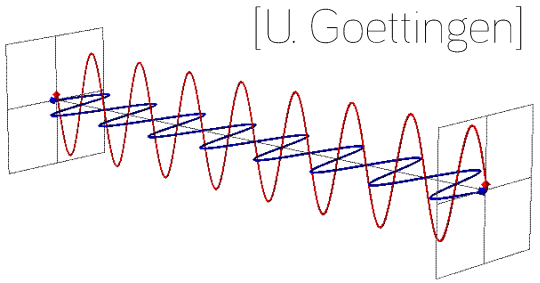
2 Elektromagnetické vlny

- pôsobenie na diaľku?

šírenie el-mag. signálu?



- J. C. Maxwell: predpoveď vĺn (1865)

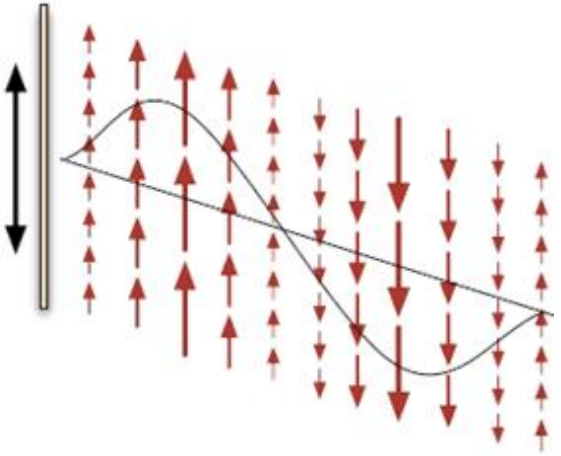


[U. Goettingen]

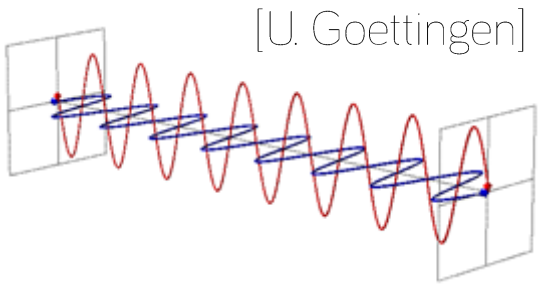
2 Elektromagnetické vlny

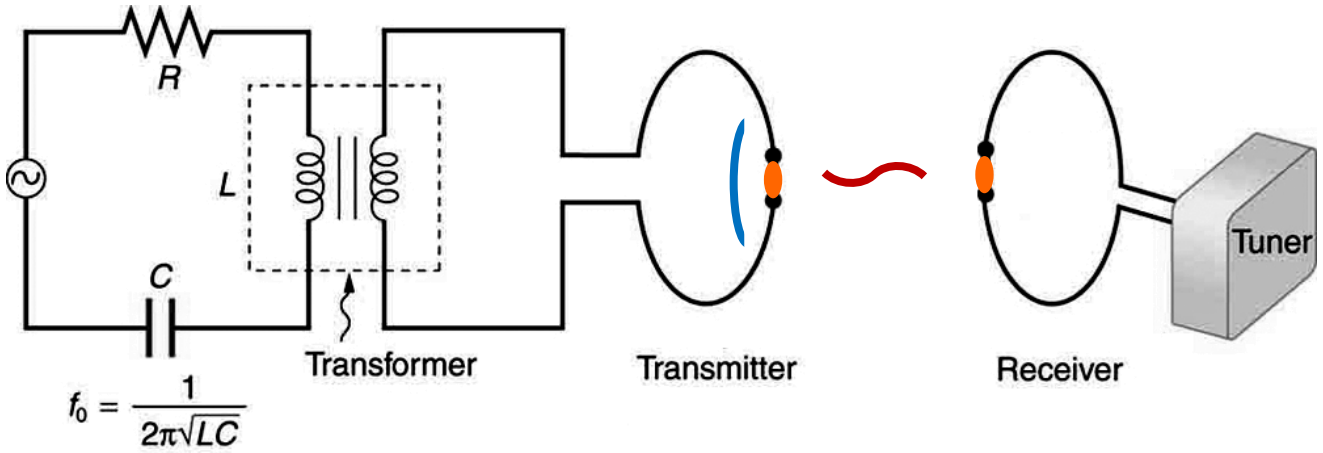
- pôsobenie na diaľku?

šírenie el-mag. signálu?



- J. C. Maxwell: predpoveď vĺn (1865)
  H. Hertz: overenie (1888)

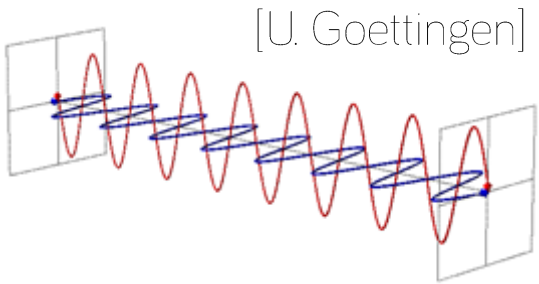


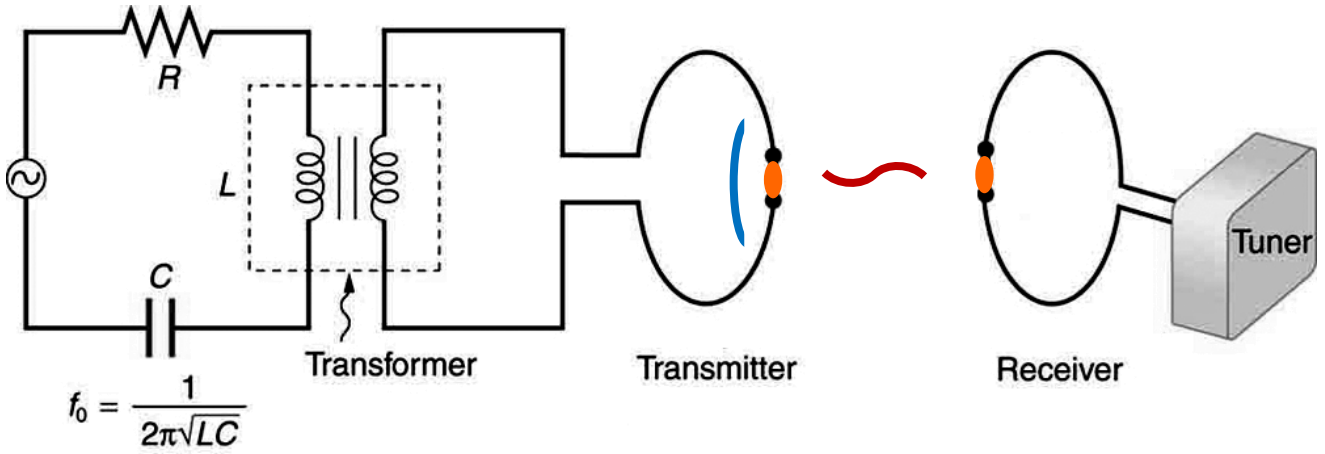


2 Elektromagnetické vlny

- k anténe pripojený detektor zo železných pilín (coherer)

- J. C. Maxwell: predpoveď vĺn (1865)
  H. Hertz: overenie (1888)



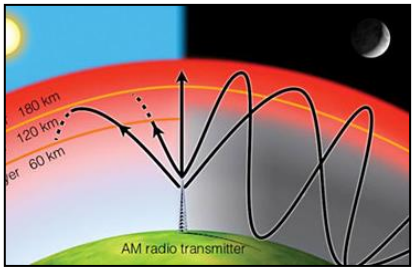


2 Bezdrôtový telegraf

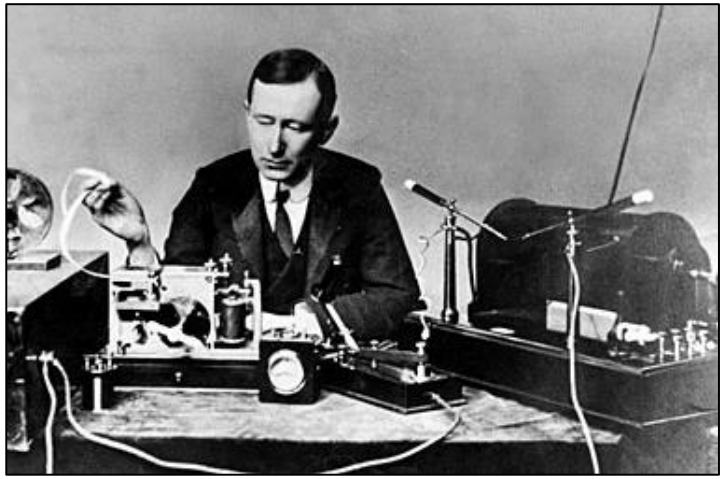
- k anténe pripojený detektor zo železných pilín (coherer)

- Hertz: je to nanič. N. Tesla: vzduchom nie, Zemou!

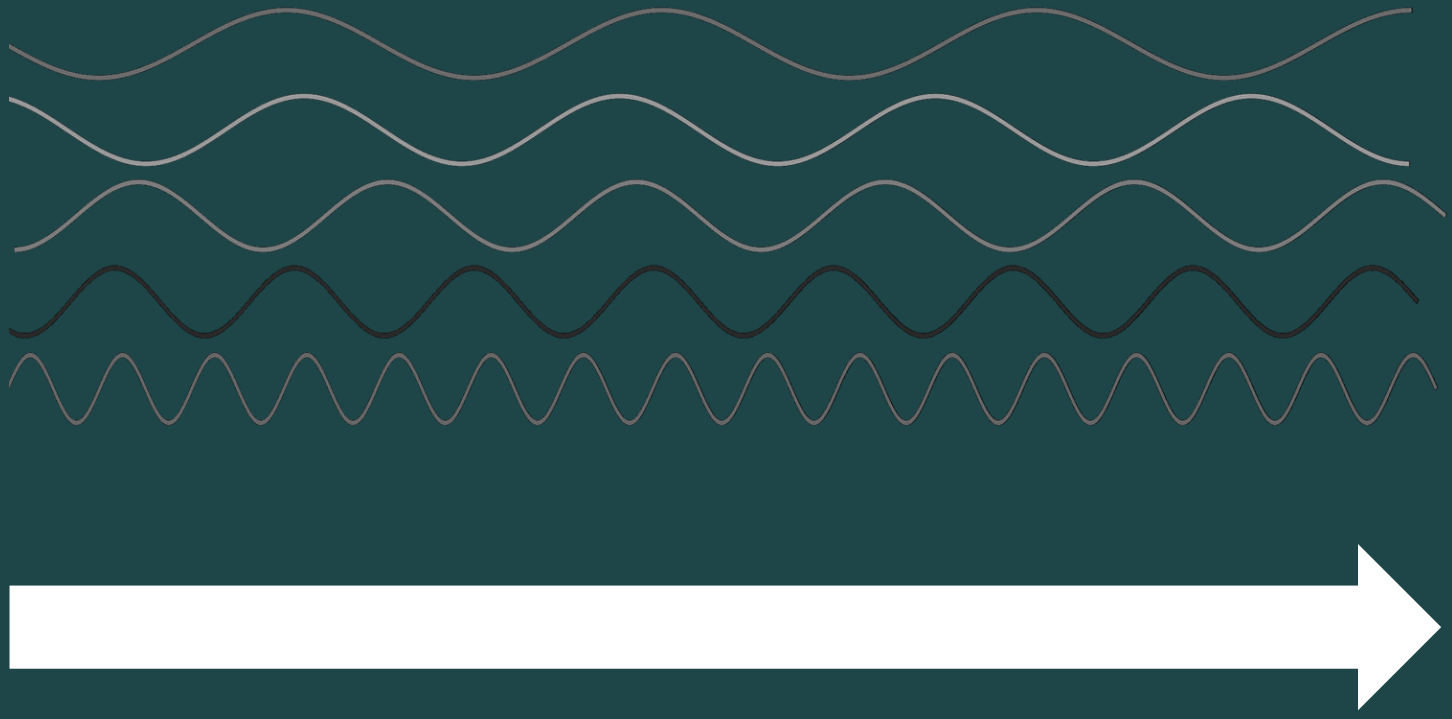
- G. Marconi (1903): ide to!
  odraz od ionosféry (>85km)



[Thompson Higher Ed.]

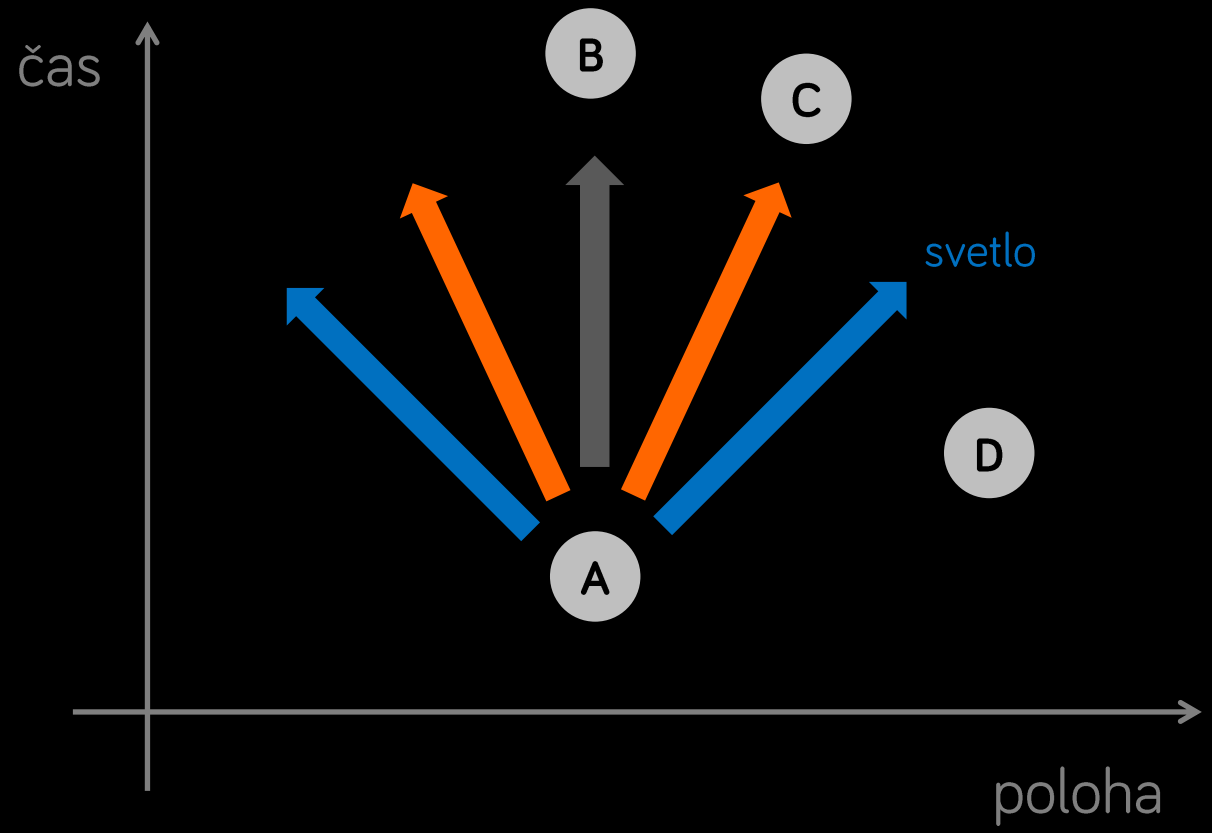


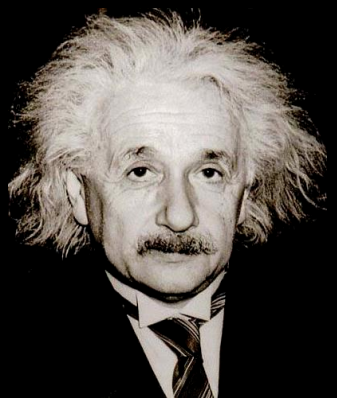
rýchlejšie ako svetlo?



2 Lokalita a kauzalita

- príčiny a dôsledky, kedy a kde sa niečo stalo?

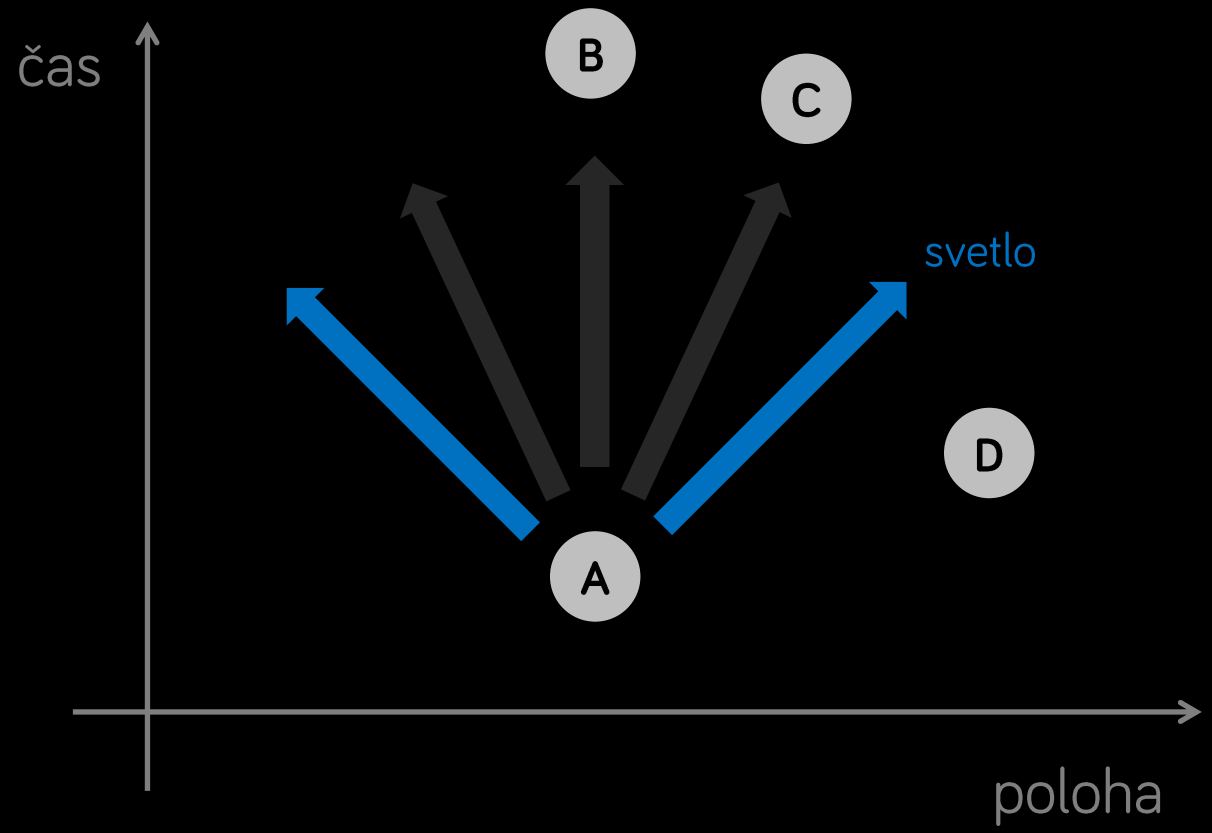


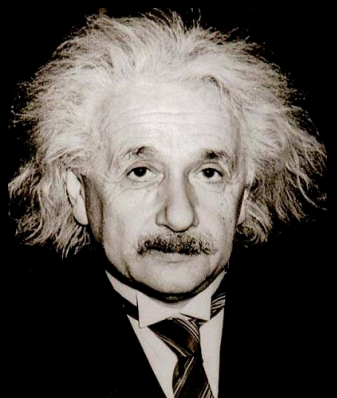


2 Lokalita a kauzalita

- nič nie je rýchlejšie ako svetlo

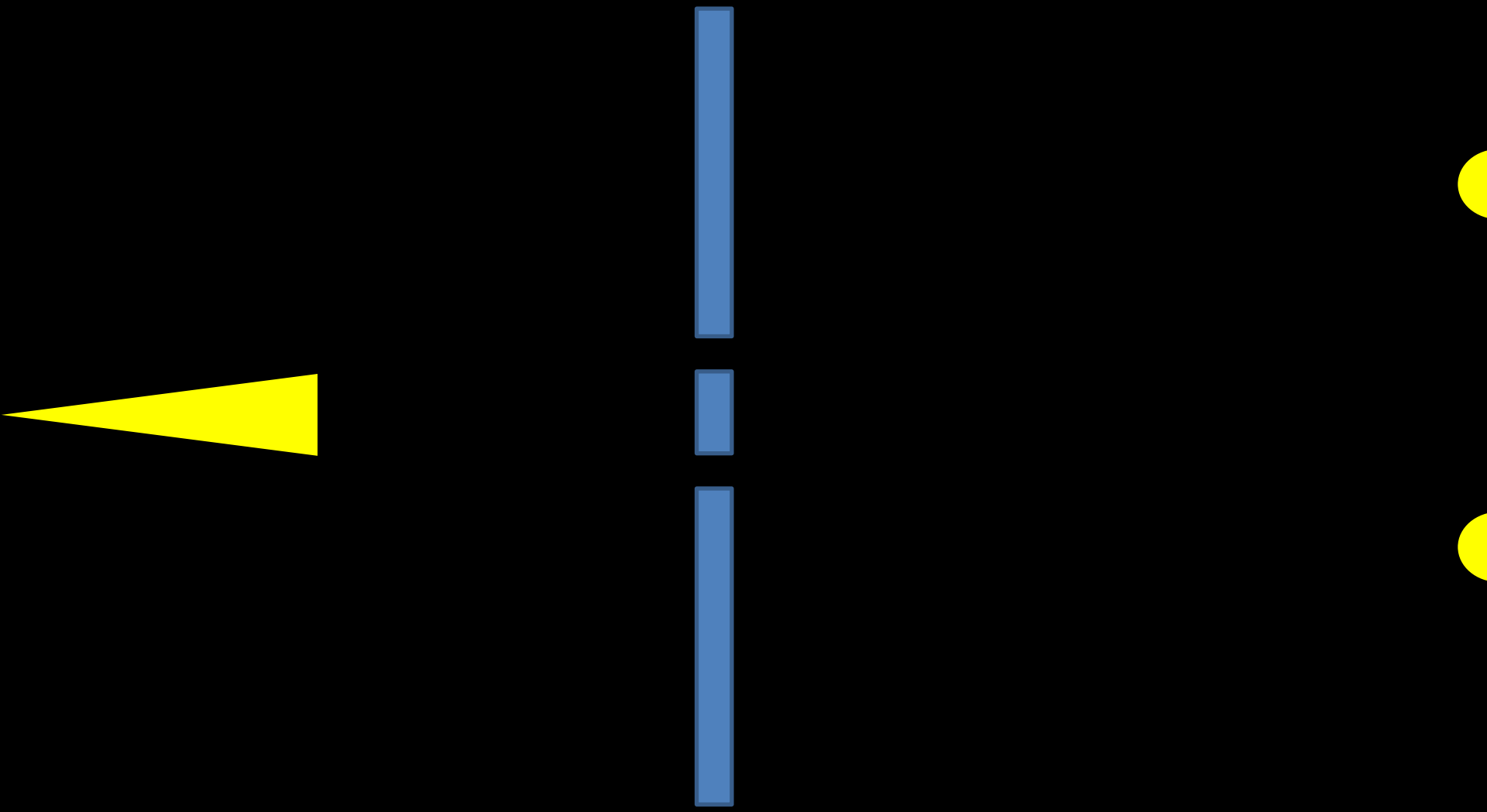
  priestoročasové intervaly, nezávislé udalosti





kvantová mechanika a jej čudné korelácie

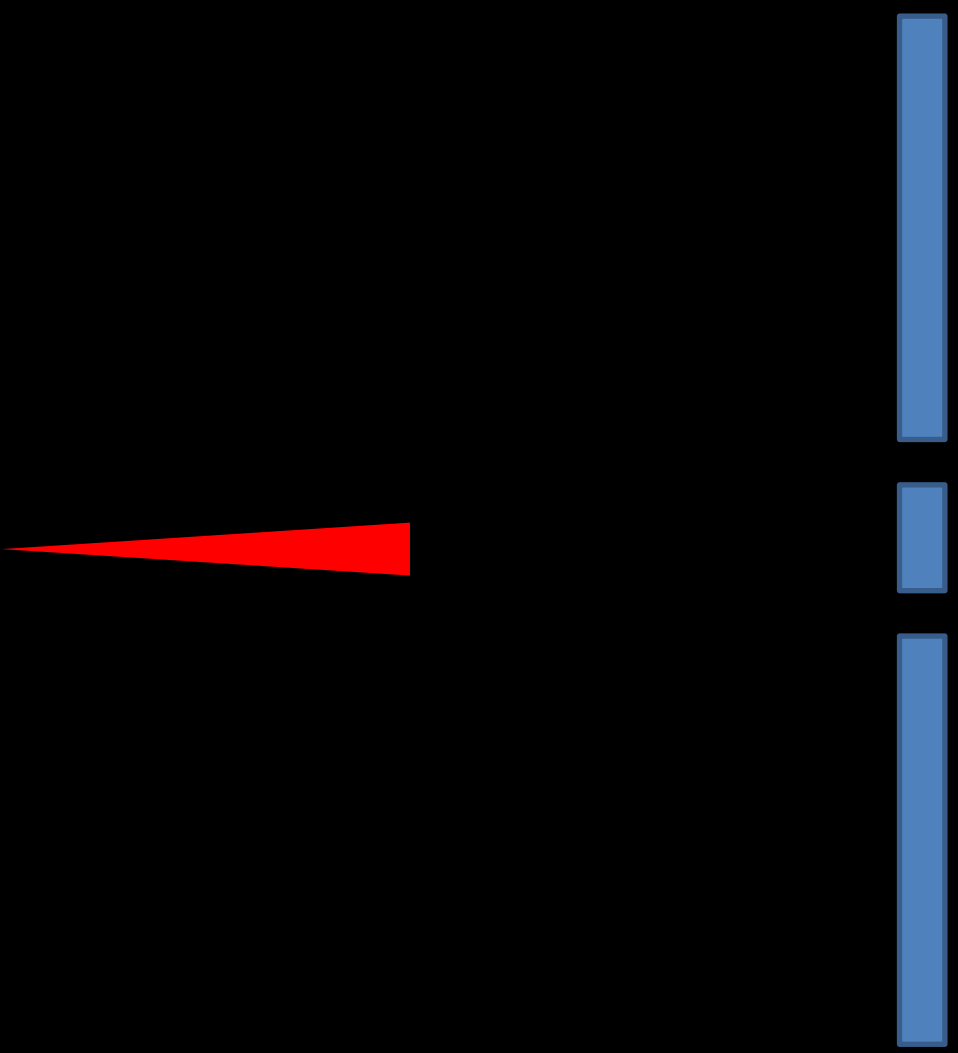
svetlo (baterka)



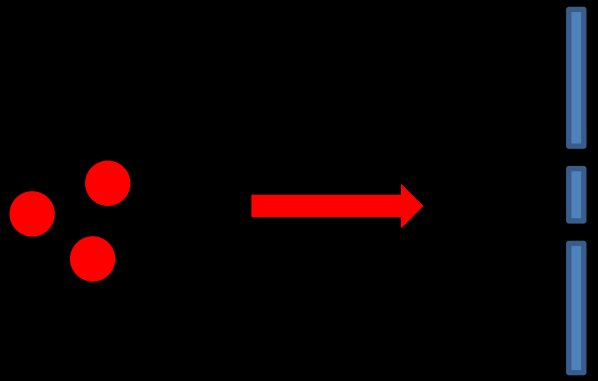
koherentné svetlo (laser)

interferencia

superpozícia



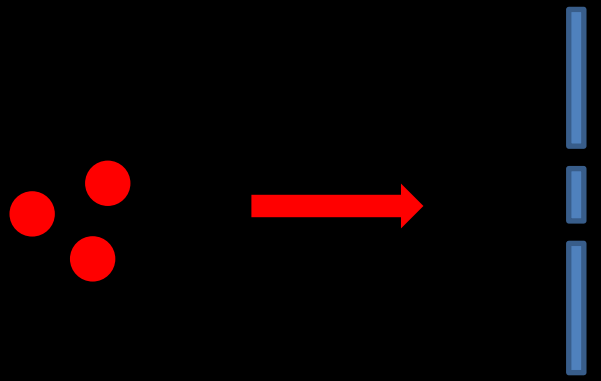
jednotlivé fotóny

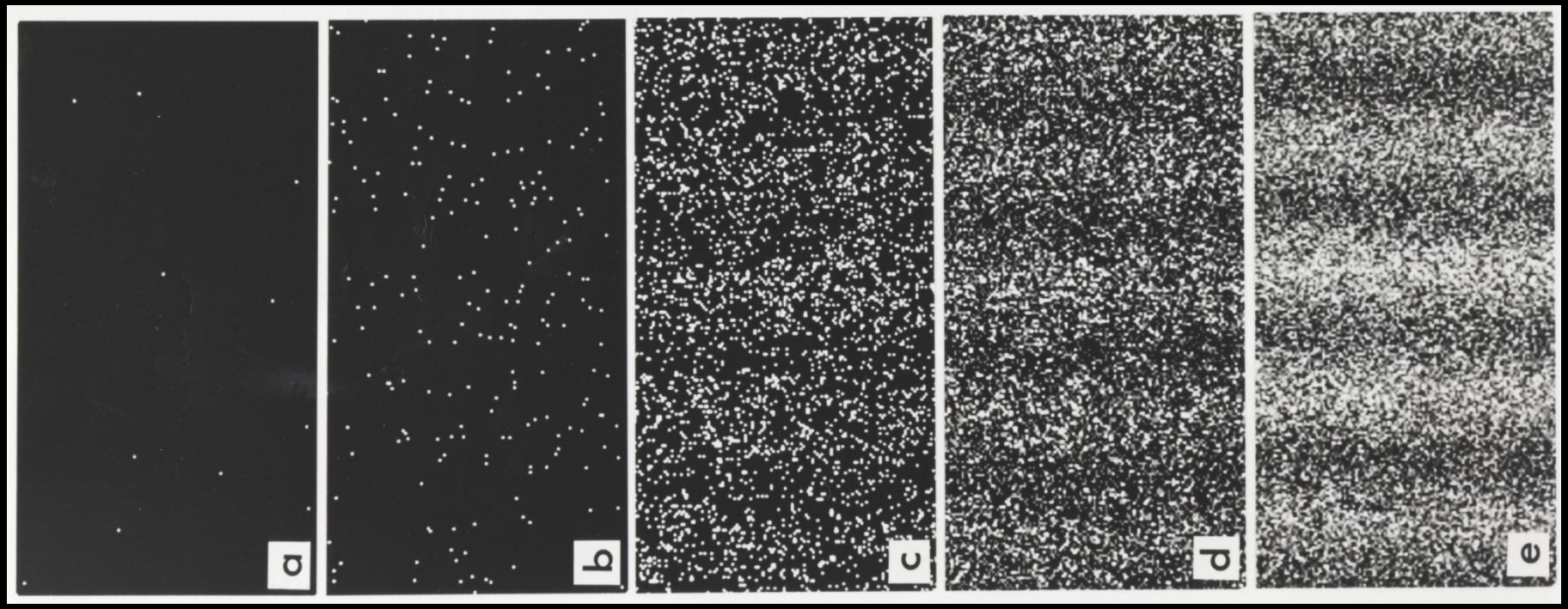


jednotlivé fotóny

interferencia

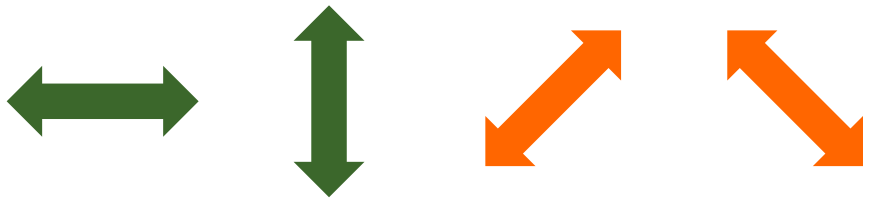
superpozícia



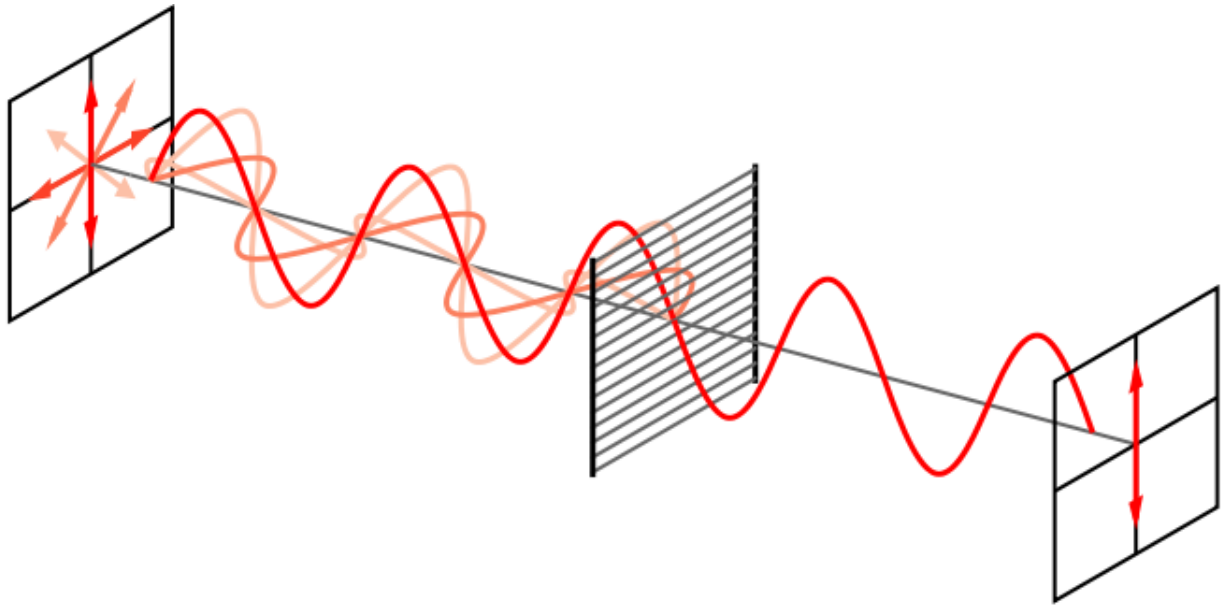


3 Svietime si po fotónoch

- vlny … jednotlivé fotóny
  rôzne polarizácie
  superpozície



- polarizačné filtre

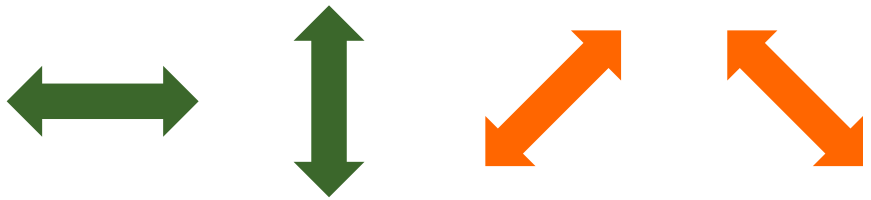


bez filtra

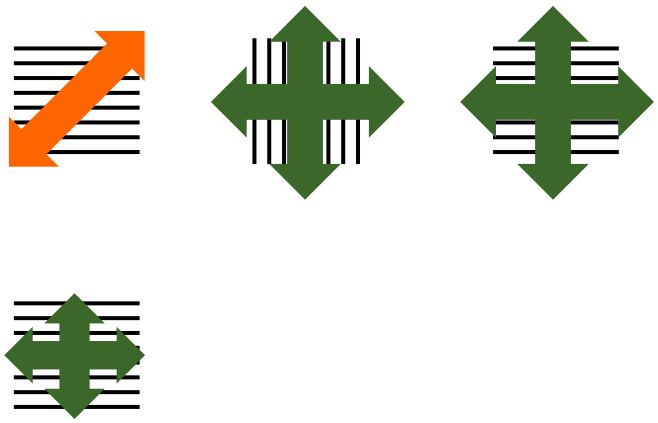
s filtrom

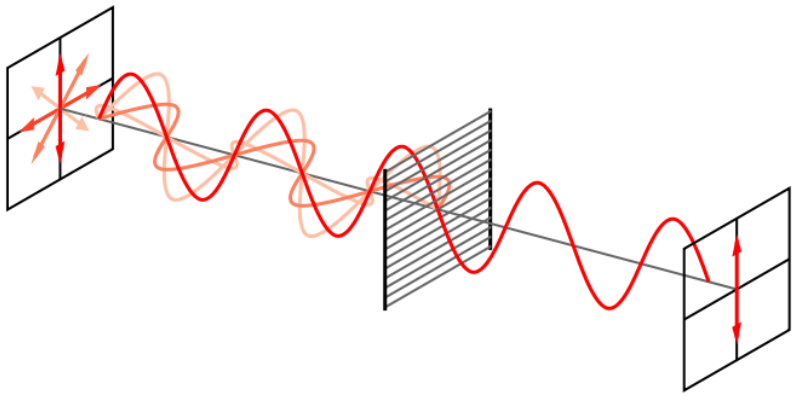
3 Svietime si po fotónoch

- vlny … jednotlivé fotóny
  rôzne polarizácie
  superpozície



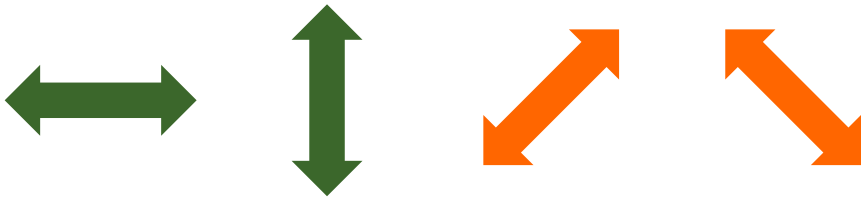
- polarizačné filtre
  čo robia so superpozíciami?



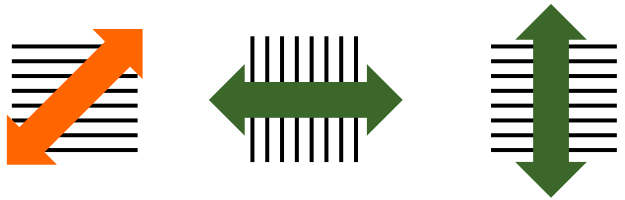


3 Svietime si po fotónoch

- vlny … jednotlivé fotóny
  rôzne polarizácie
  superpozície



- polarizačné filtre
  čo robia so superpozíciami?



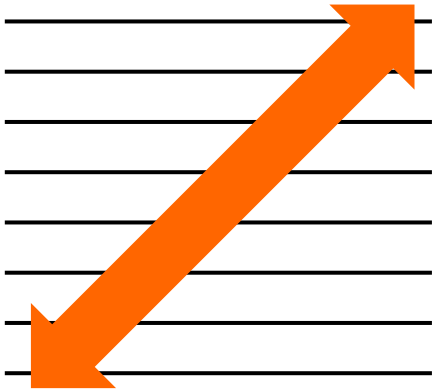
- polarizačný beamsplitter
  triedime polarizácie

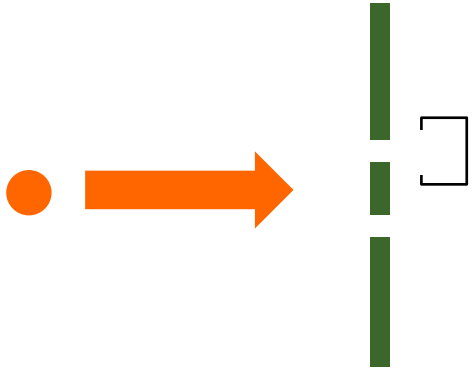
- jednofotónové detektory
  prenos informácie

3 Správanie superpozícií

- náhodné výsledky pri meraní

  kolaps vlnovej funkcie (toho, čo vieme o stave)





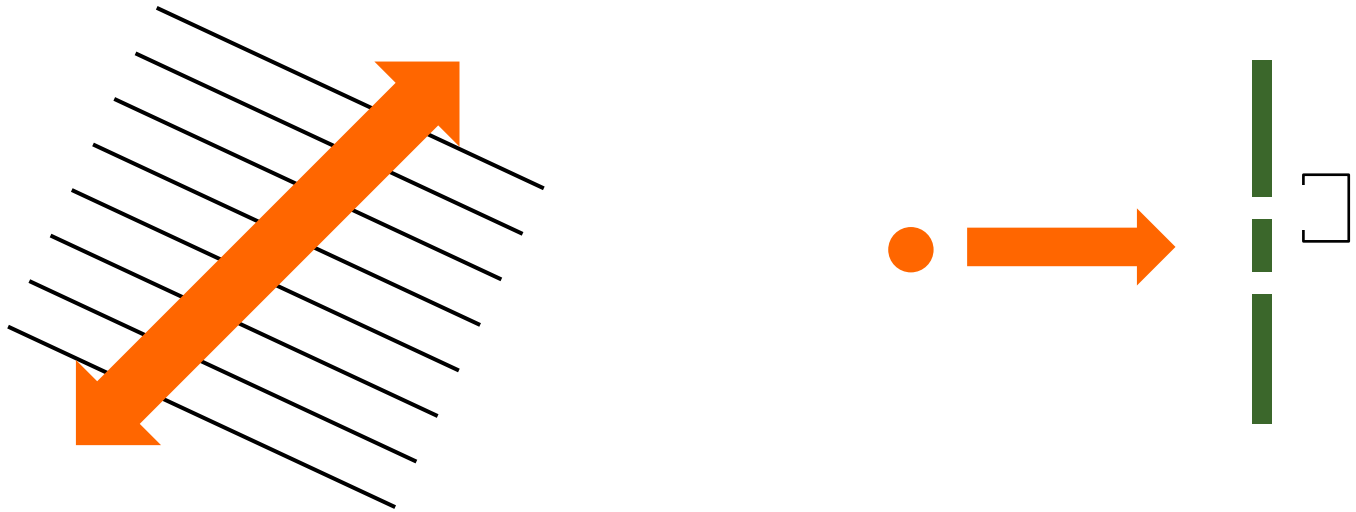
- princíp neurčitosti a nekompatibilné merania

  dá sa vedieť dve veci (všetko) naraz?

3 Správanie superpozícií

- náhodné výsledky pri meraní

  kolaps vlnovej funkcie (toho, čo vieme o stave)



- princíp neurčitosti a nekompatibilné merania

  dá sa vedieť dve veci (všetko) naraz?

- zaujímavé… je ale niečo za tým?

  vie niekto, ako to dopadne?

EPR

1935


P?

Q?

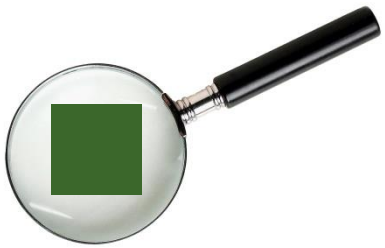
P?

P?

P?

Q?

Q?



Q?

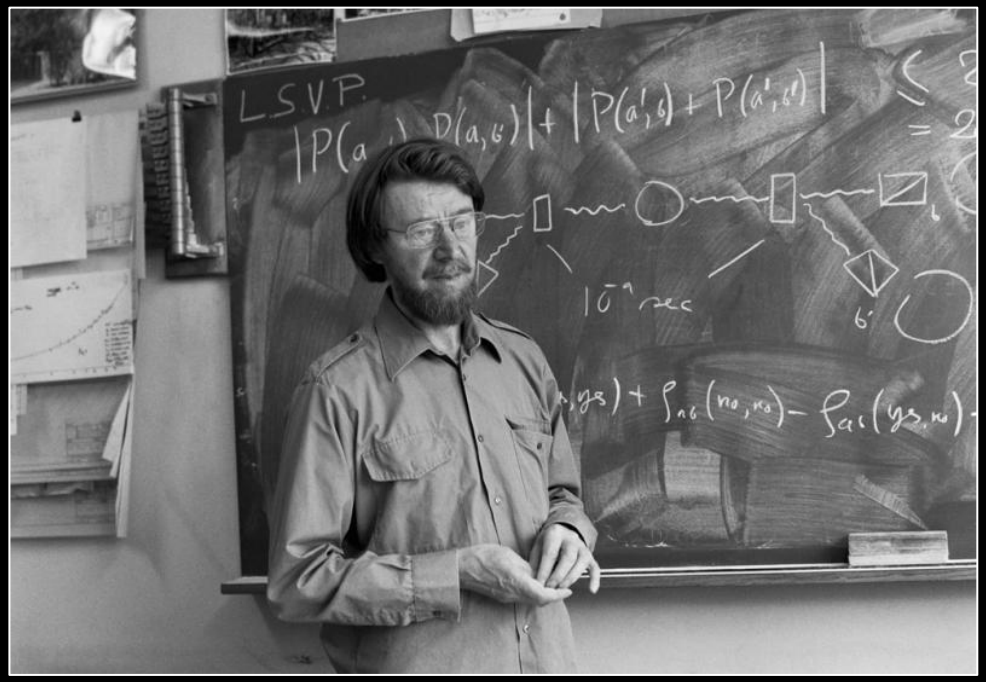
P?

kto pozná celú pravdu?

čo sa za tým skrýva?

čudesné okamžité pôsobenie na diaľku?

lokálna teória
skrytých premenných



BELL '64

TEST

3 Klasické korelácie: ponožky prof. Bertlmanna

BERTLMANN'S SOCKS AND THE NATURE OF REALITY

J.S. Bell

CERN - Geneva

Ref.TH.2926-CERN

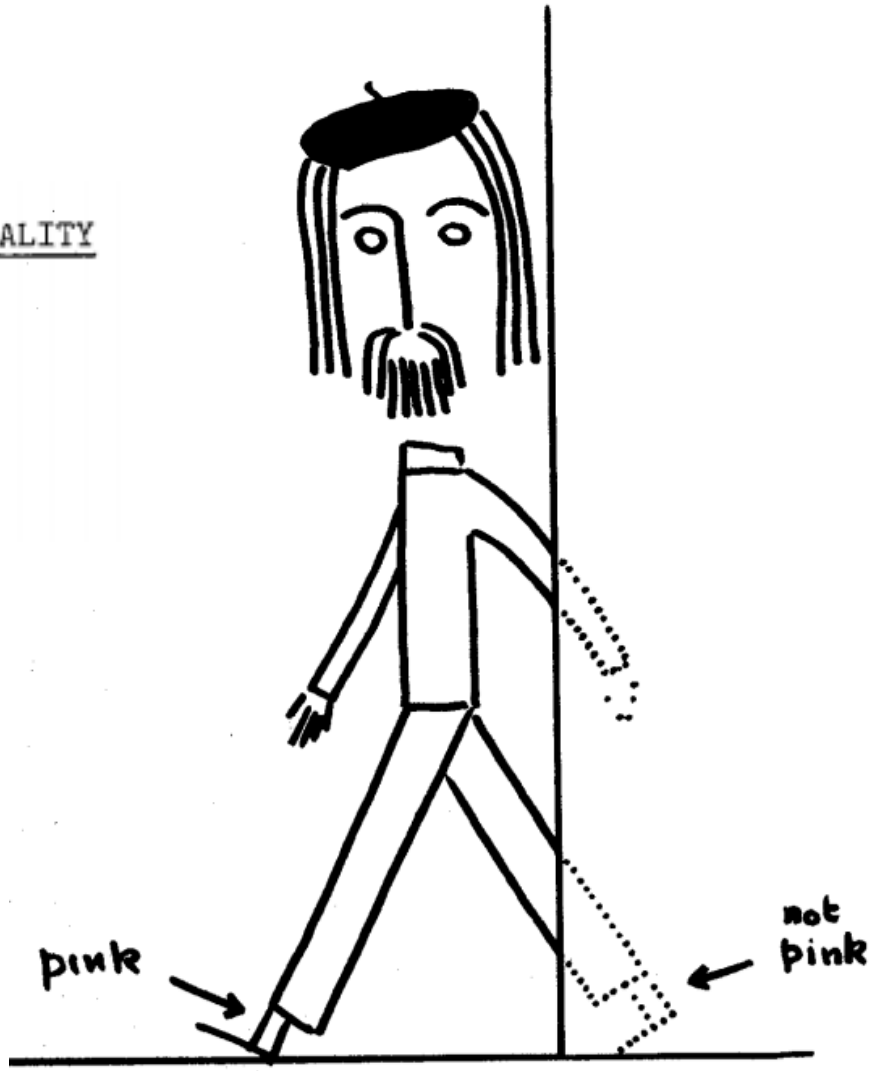
3 Klasické korelácie: ponožky prof. Bertlmanna

BERTLMANN'S SOCKS AND THE NATURE OF REALITY

J.S. Bell

CERN - Geneva

Ref.TH.2926-CERN



CHSH áno/nie pre 2 hráčov

zhodné odpovede na

A B

a B

a b

opačné odpovede na

A b

CHSH áno/nie pre 2 hráčov

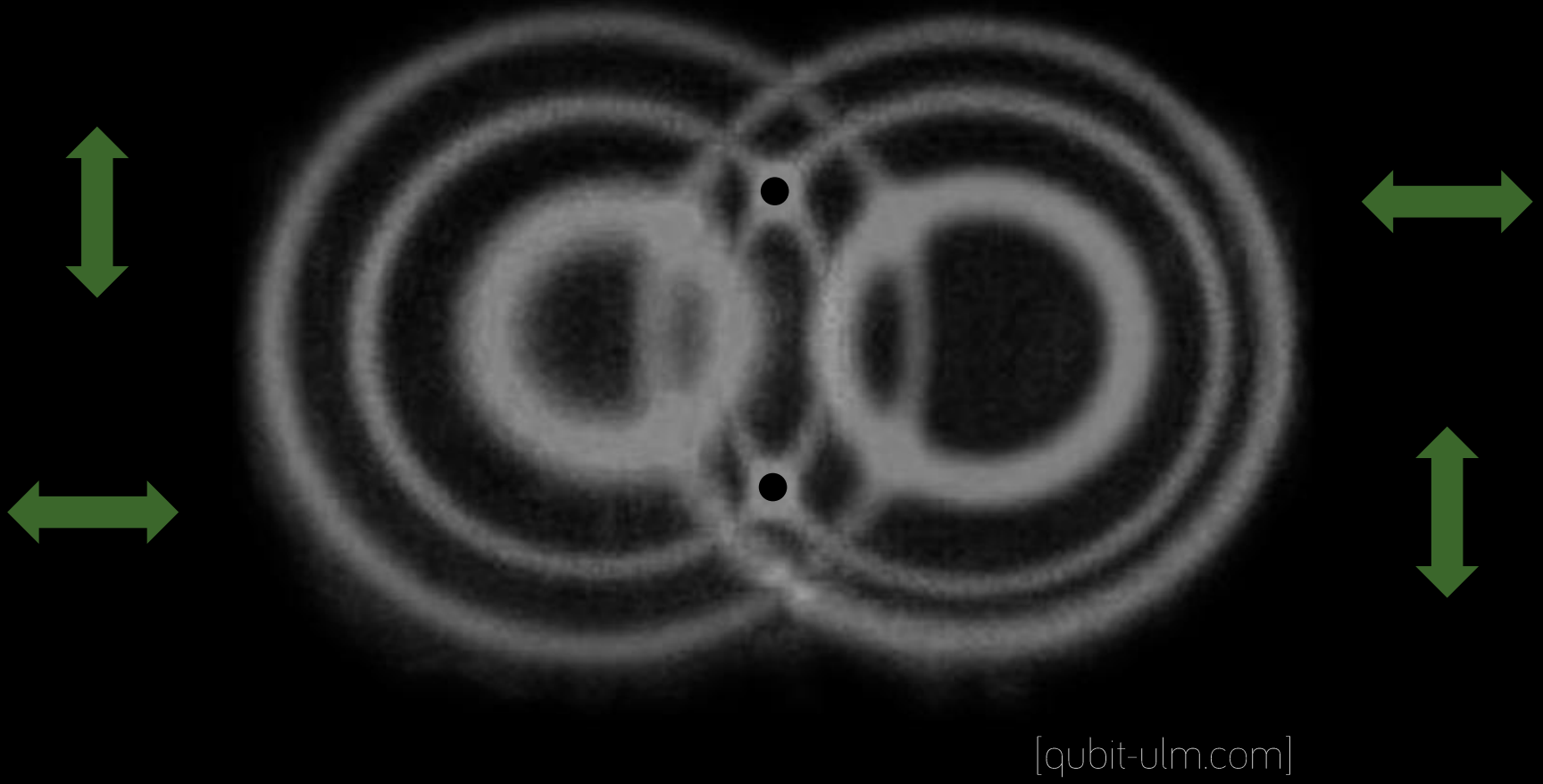
klasické premenné a korelácie:

$$\begin{aligned} A, a, B, b & \quad \pm 1 \\ (B-b, B+b) & \quad (0, \pm 2), (\pm 2, 0) \\ A(B-b) + a(B+b) & \quad \pm 2 \\ |AB + aB + ab - Ab| & \quad \leq 2 \end{aligned}$$

$$|\langle AB \rangle + \langle aB \rangle + \langle ab \rangle - \langle Ab \rangle| \leq 2$$

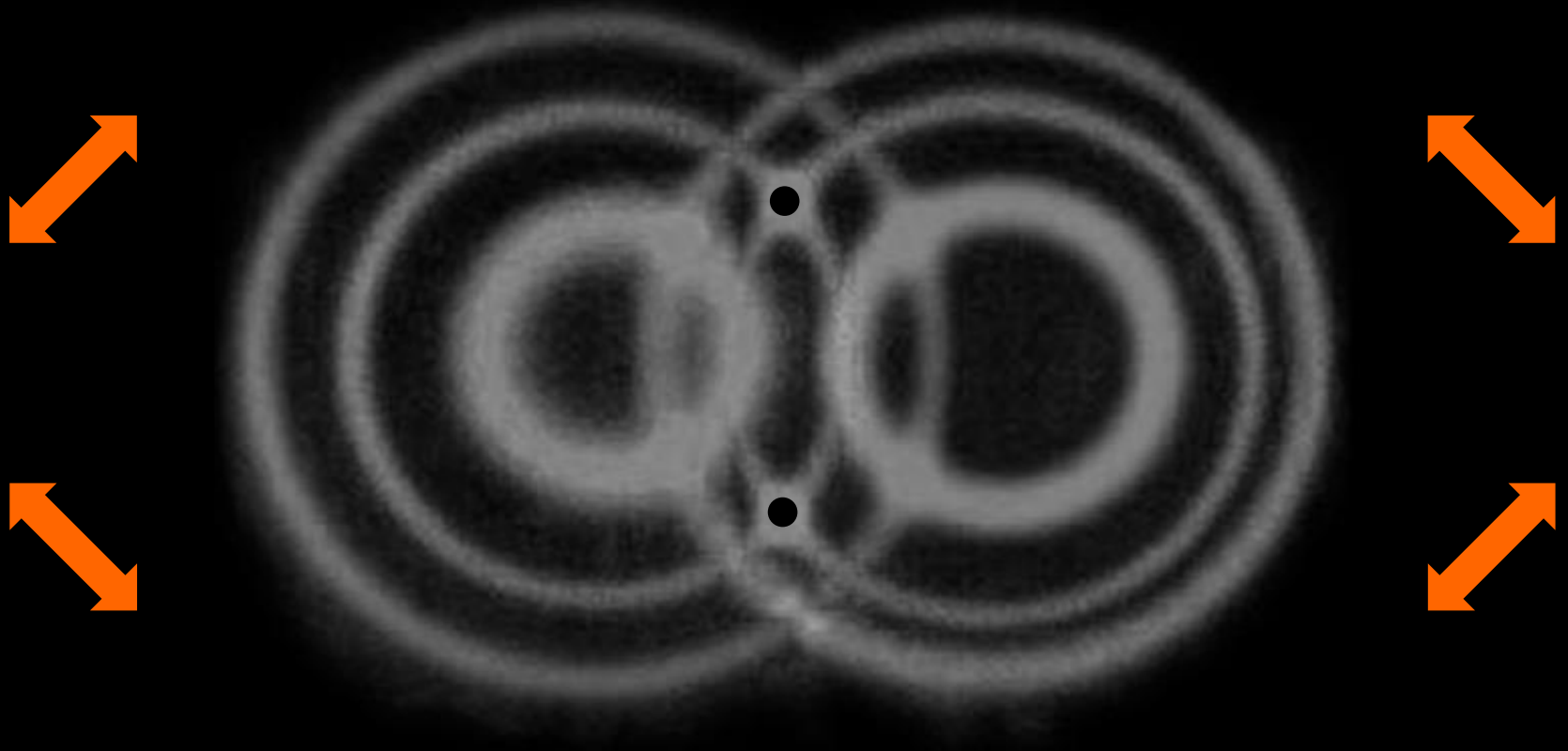
CHSH nerovnosť

3 Kvantové korelácie: previazané fotóny



[qubit-ulm.com]

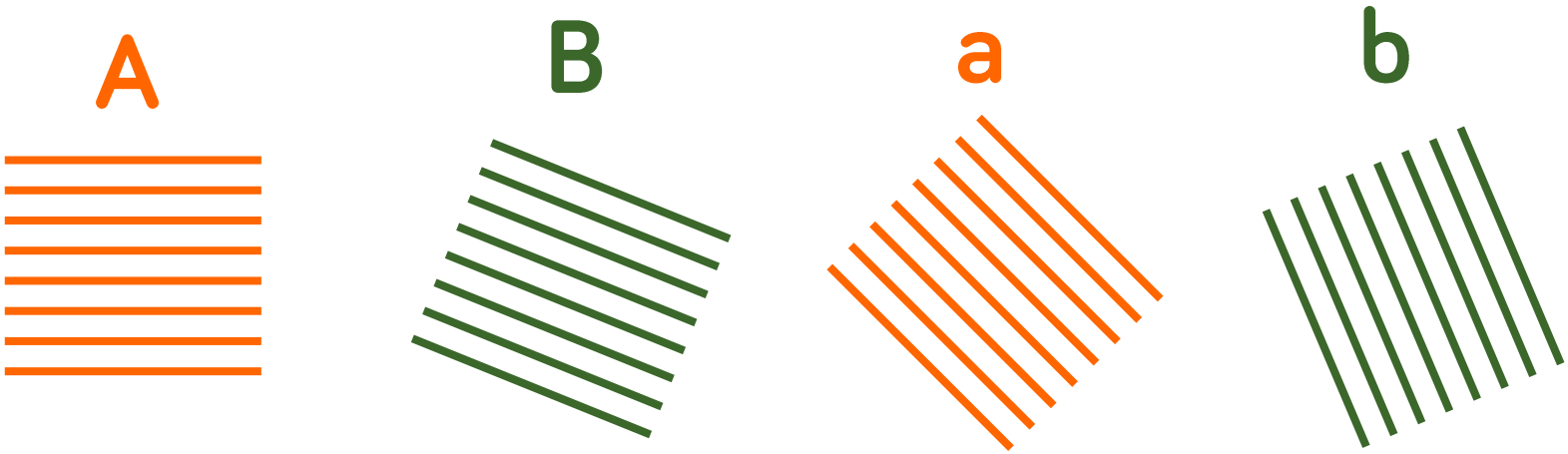
3 Kvantové korelácie: previazané fotóny



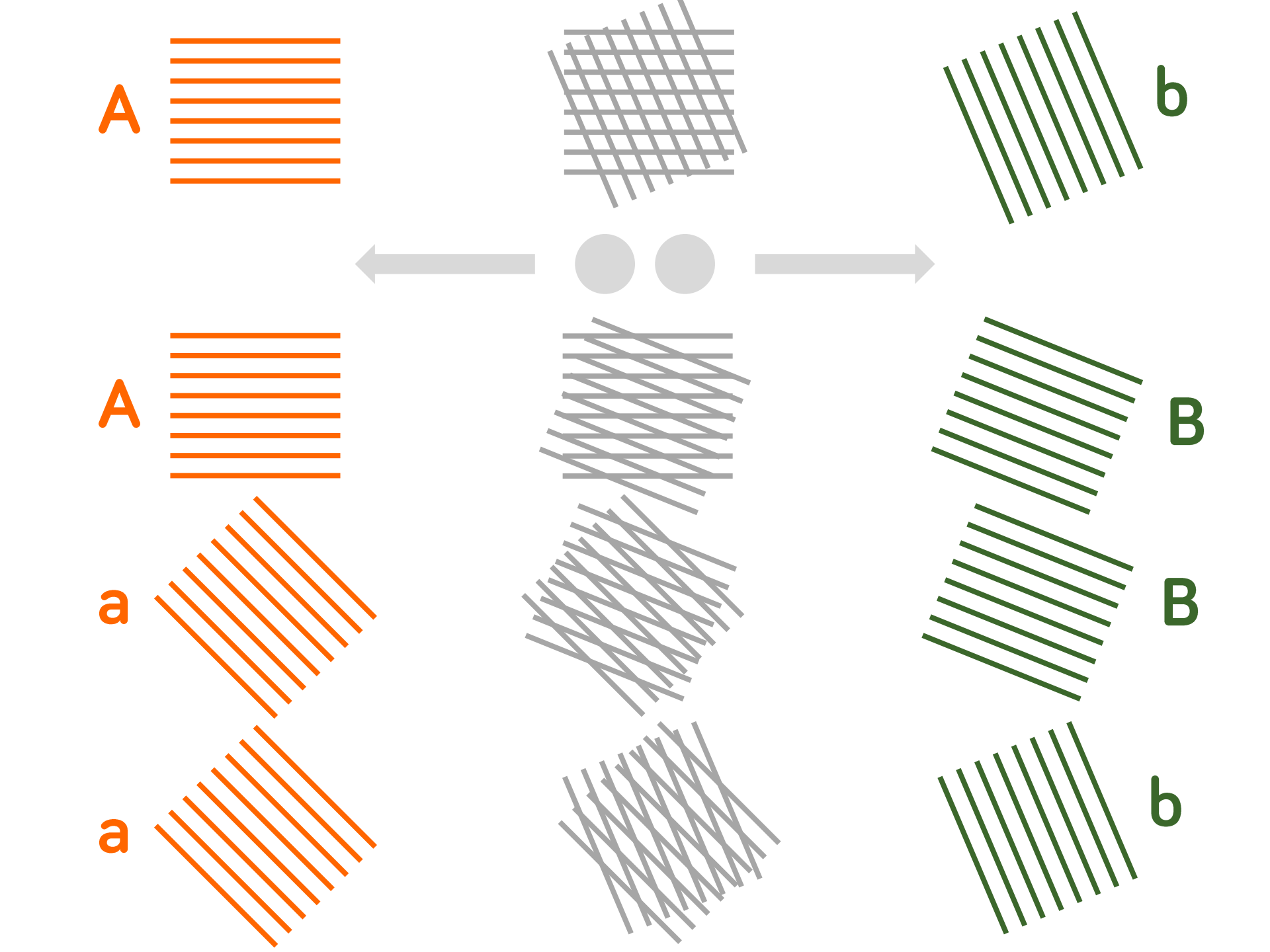
[qubit-ulm.com]

CHSH áno/nie pre 2 hráčov

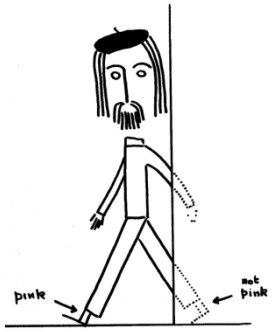
previazané fotóny



polarizačné filtre


A
b
A
B
a
B
a
b

3 QM dá viac!



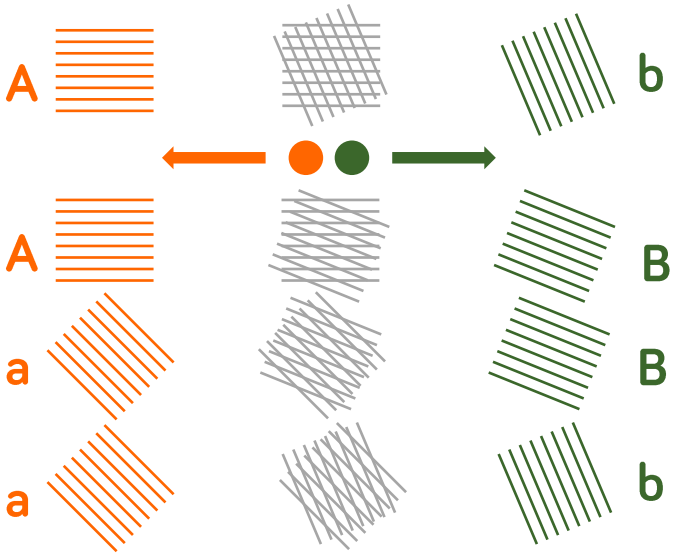
- Bellova (CHSH) nerovnosť

$$|\langle AB\rangle + \langle aB\rangle + \langle ab\rangle - \langle Ab\rangle| \leq 2$$

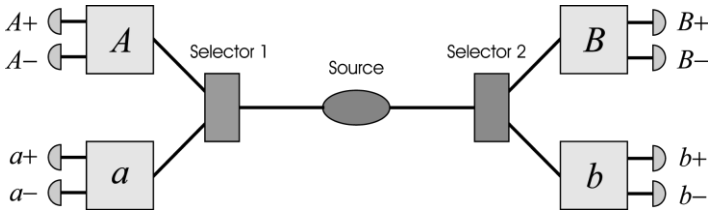
- kvantová mechanika dáva

$$|\langle AB\rangle + \langle aB\rangle + \langle ab\rangle - \langle Ab\rangle| = 2\sqrt{2}$$

Lokálne skryté premenné
také korelácie nevysvetlia!



- krásne experimenty
Clauser, Aspect, Zeilinger



SHUT UP

& CALCULATE

3 Fundamental fysiks group

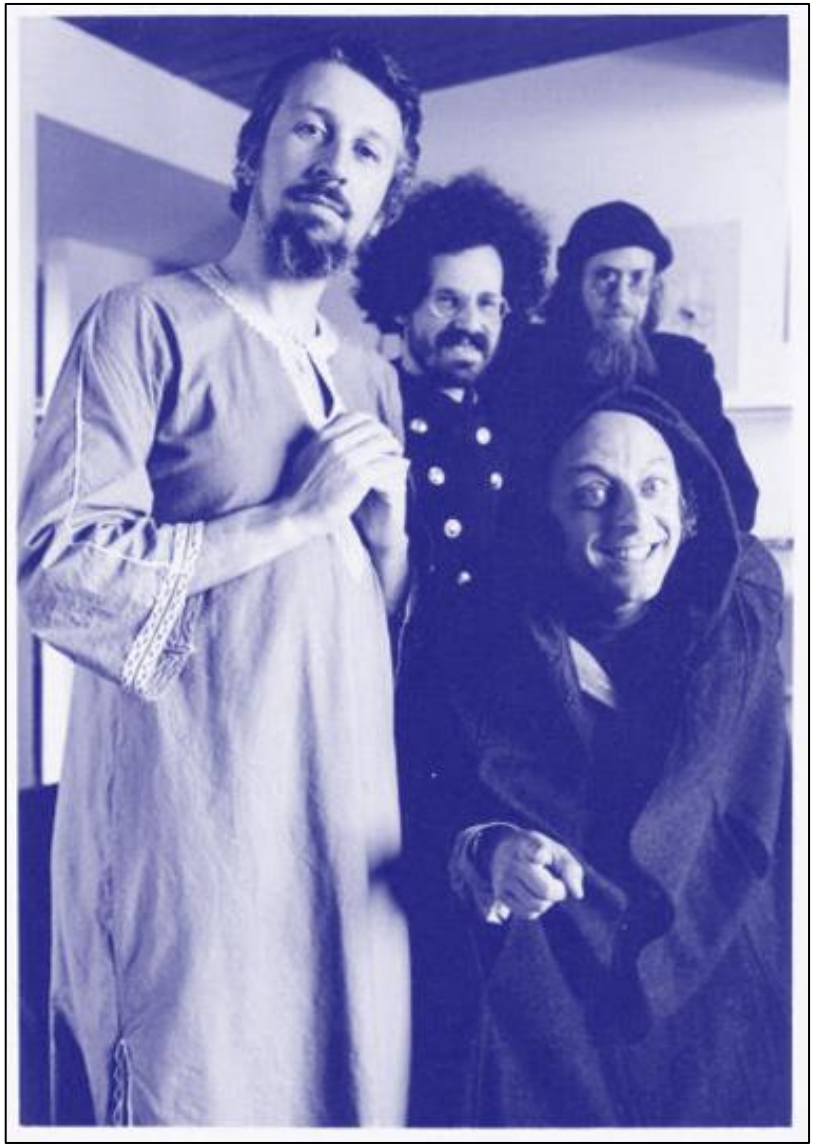
- filozofické otázky
  a špekulácie o QM

telepatia?

vedomie?

nadsvetelná
komunikácia?

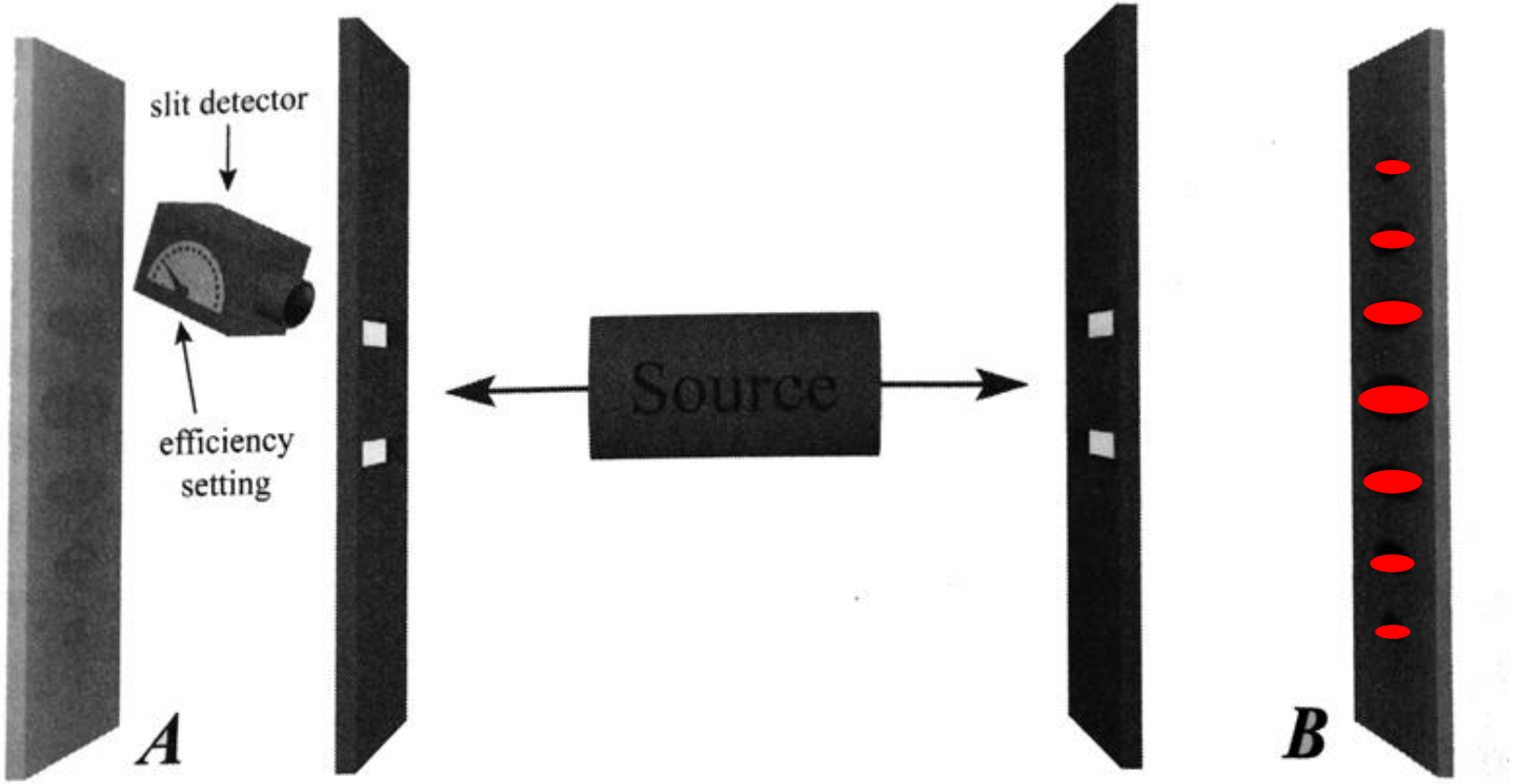
- inšpirácia: Bell



[Sarfati, Sirag, Herbert, Wolf, CityMagazine, 1975]

3 Fundamental fysiks group

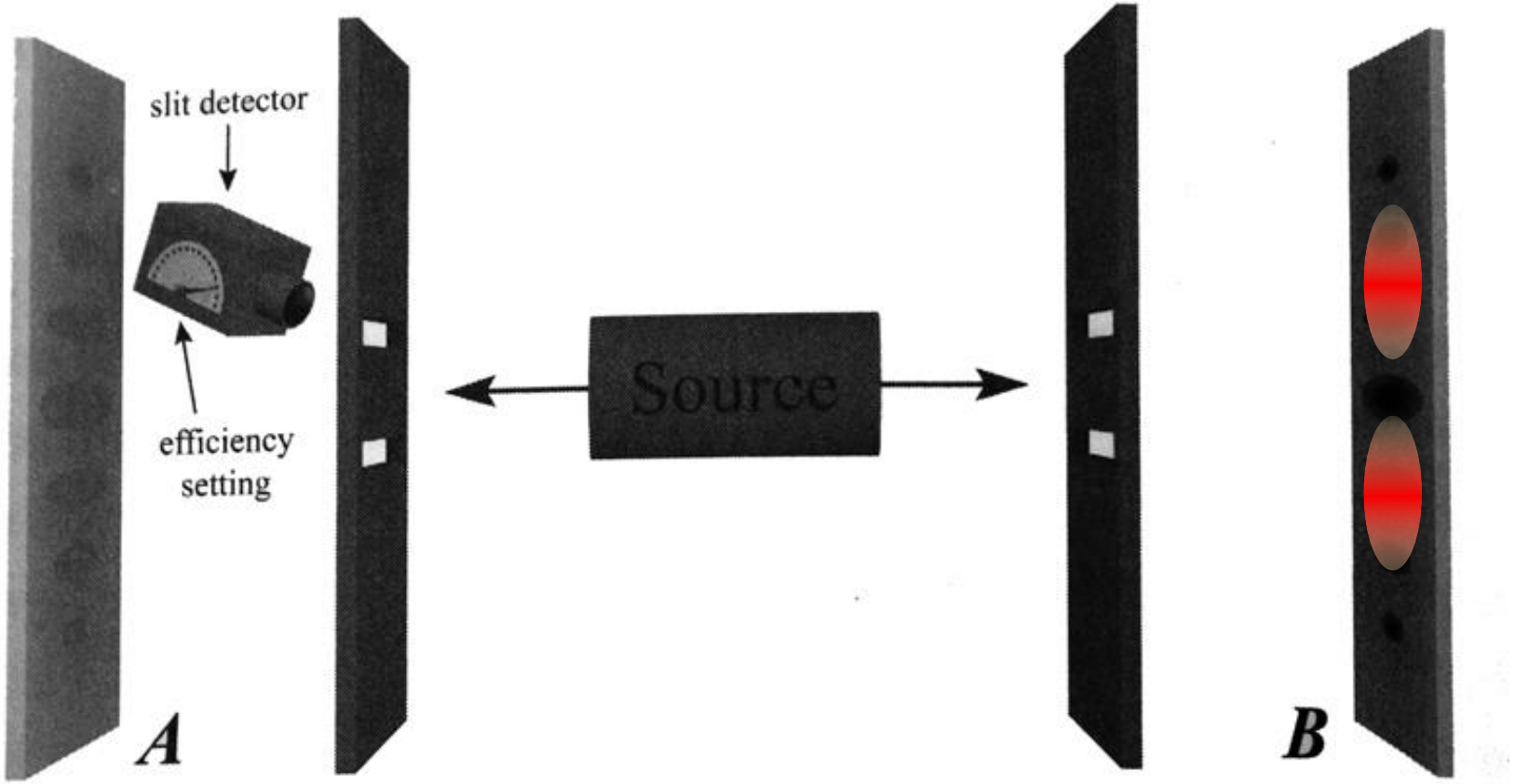
- Faster-than-light communication system (Sarfati '78)



[D. Kaiser, How the hippies saved physics]

3 Fundamental fysiks group

- Faster-than-light communication system (Sarfati '78)



[D. Kaiser, How the hippies saved physics]

Hippies believed that with enough LSD, everybody could be perfectly in tune with each other...

Charlie Bennett

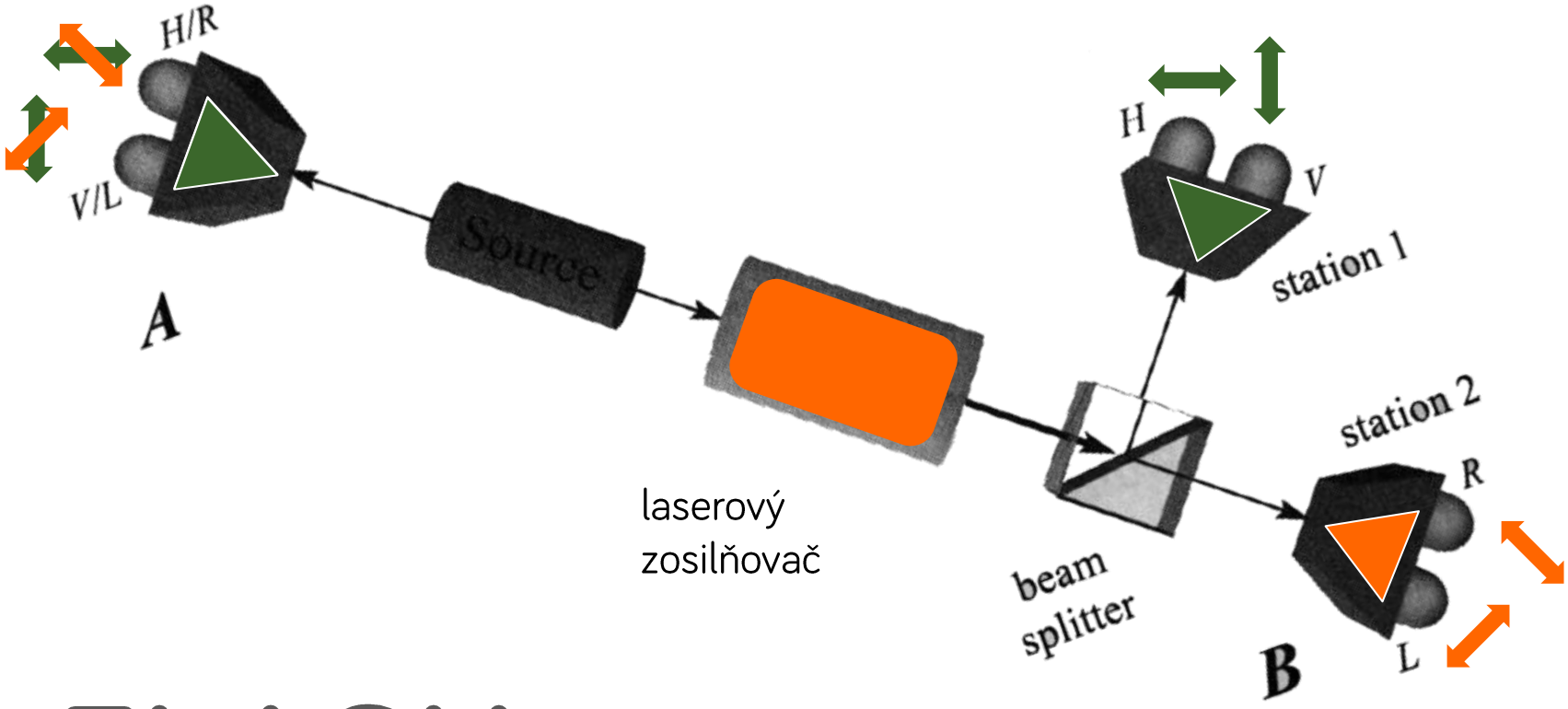
Entanglement allows two particles to be in a perfectly definite joint state, even though each one by itself is completely random.

Like two hippies who feel **perfectly in tune** with each other, even though neither has an opinion on anything.

Charlie Bennett

3 Fundamental fysiks group: nápady

- First Laser Amplified Superluminal Hookup (Herbert, ’79)



FLASH

[D. Kaiser, How the hippies saved physics]

3 Zabiják: nemožnosť klonovania

- klonovať (kopírovať, zosilňovať) hocaké fotóny sa nedá

letters to nature

Nature **299**, 802 - 803 (28 October 1982); doi:10.1038/299802a0

A single quantum cannot be cloned

W. K. WOOTTERS*[1] & W. H. ZUREK[2]

Communication by EPR devices

D. Dieks

Show more

doi:10.1016/0375-9601(82)90084-6

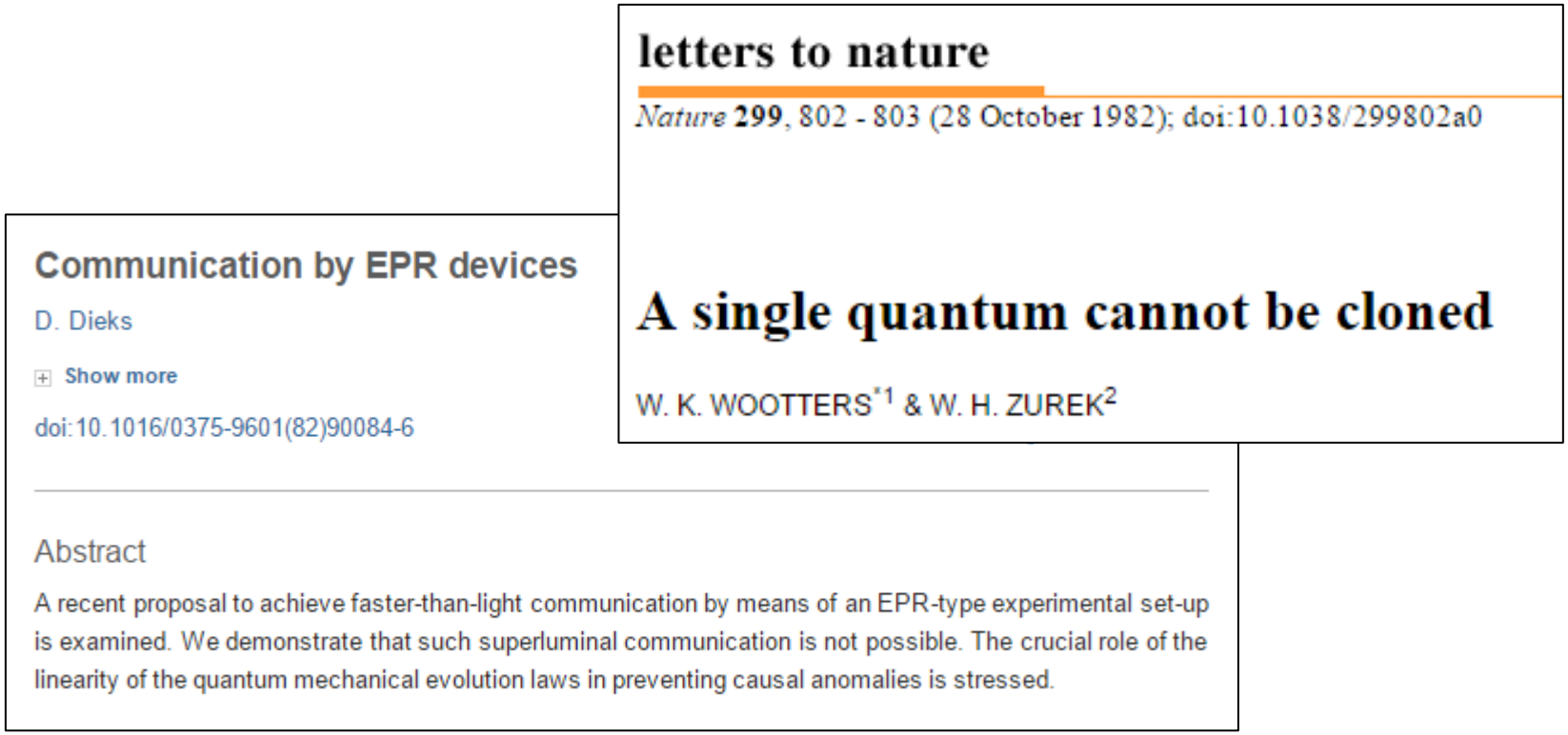
Abstract

A recent proposal to achieve faster-than-light communication by means of an EPR-type experimental set-up is examined. We demonstrate that such superluminal communication is not possible. The crucial role of the linearity of the quantum mechanical evolution laws in preventing causal anomalies is stressed.

- čo sa dá?

3 Zabiják: nemožnosť klonovania

- klonovať (kopírovať, zosilňovať) hocaké fotóny sa nedá



letters to nature

Nature **299**, 802 - 803 (28 October 1982); doi:10.1038/299802a0

A single quantum cannot be cloned

W. K. WOOTTERS*[1] & W. H. ZUREK[2]

Communication by EPR devices

D. Dieks

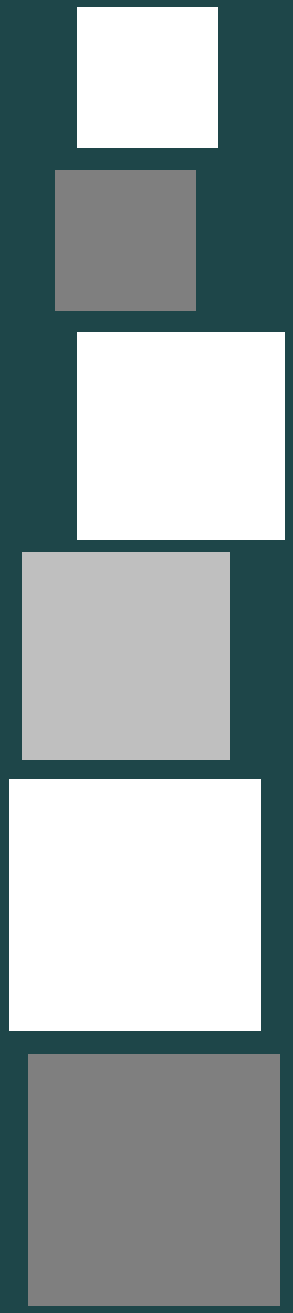
Show more

doi:10.1016/0375-9601(82)90084-6

Abstract

A recent proposal to achieve faster-than-light communication by means of an EPR-type experimental set-up is examined. We demonstrate that such superluminal communication is not possible. The crucial role of the linearity of the quantum mechanical evolution laws in preventing causal anomalies is stressed.

- čo sa dá?



na čo sú
tie divné
korelácie?

[Physics World]

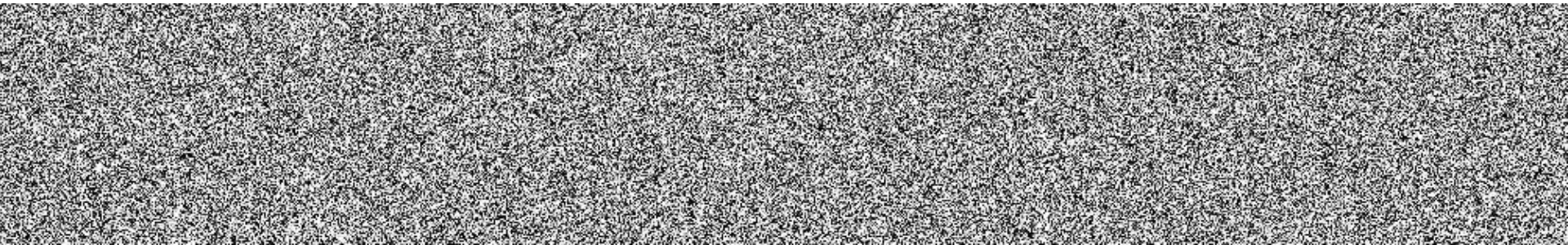
3 Unconditional security: one-time pad

$$P \longrightarrow C = P \oplus x$$

tajomstvo

šifra

kľúč



3 Unconditional security: one-time pad

$$P \longrightarrow C = P \oplus x$$

tajomstvo — šifra — kľúč

$$P = C \oplus x \oplus x$$

- na jedno použitie!

$$D = Q \oplus x$$

$$C \oplus D = P \oplus Q$$

3 Verejné zdieľanie hesla

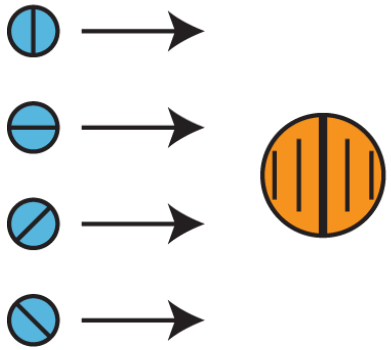
BB84 (bez previazania)

Alica

vyber si bázu

priprav fotón

pošli ho



Bob

vyber si bázu

zmeraj, čo prišlo

1

0

random

random

[Bennett & Brassard]

3 Verejné zdieľanie hesla

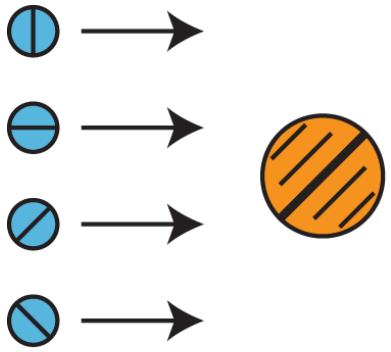
BB84 (bez previazania)

Alica

vyber si bázu

priprav fotón

pošli ho



Bob

vyber si bázu

zmeraj, čo prišlo

random

random

1

0

verejne si porovnajte výber báz

v rovnakej báze? korelované výsledky

korelované výsledky … váš **tajný kľúč**

[Bennett & Brassard]

3 Verejné zdieľanie hesla pomocou EPR

Ekert 91 (s previazaním)

Alica

priprav EPR pár

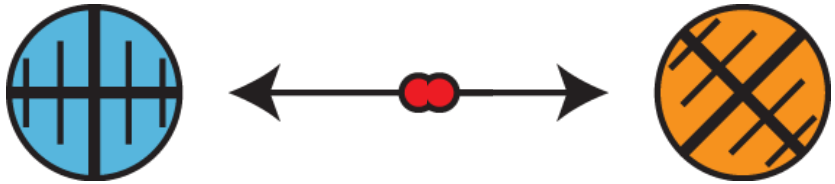
jeden fotón pošli B

vyber si bázu, zmeraj svoj fotón

Bob

vyber si bázu

zmeraj, čo prišlo



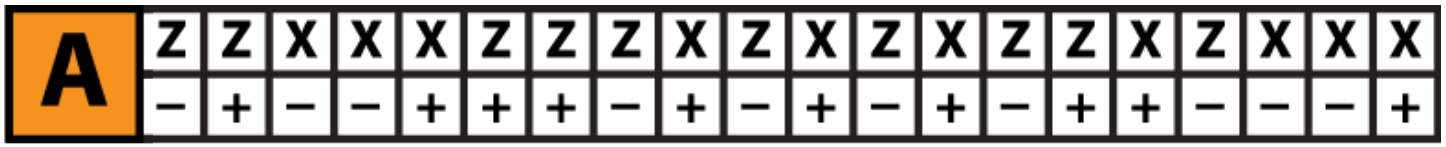
verejne si porovnajte výber báz

v rovnakej báze? **anti**korelované výsledky

detekcia špionáže: časť výsledkov zverejnite na Bell-testy

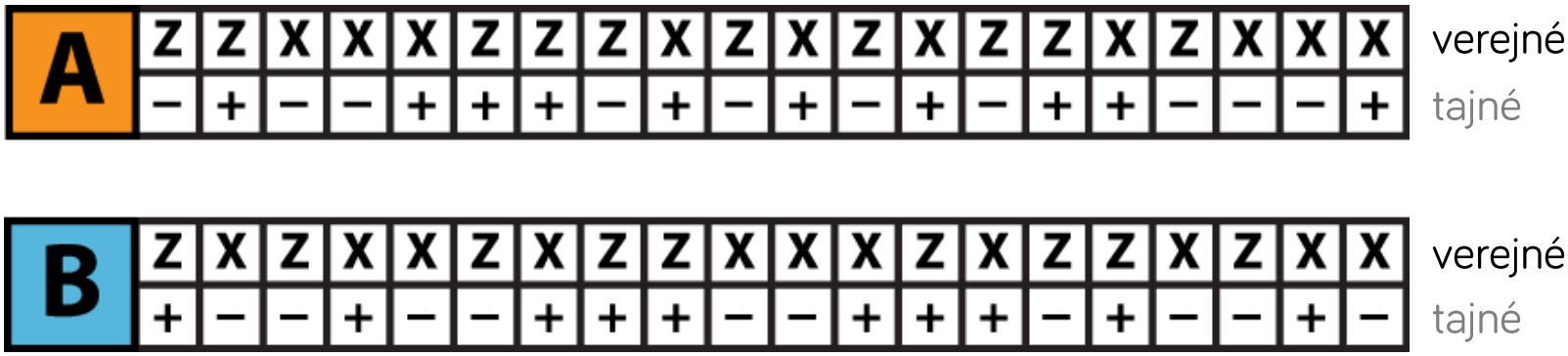
zvyšné výsledky … váš **tajný kľúč**

[Ekert]



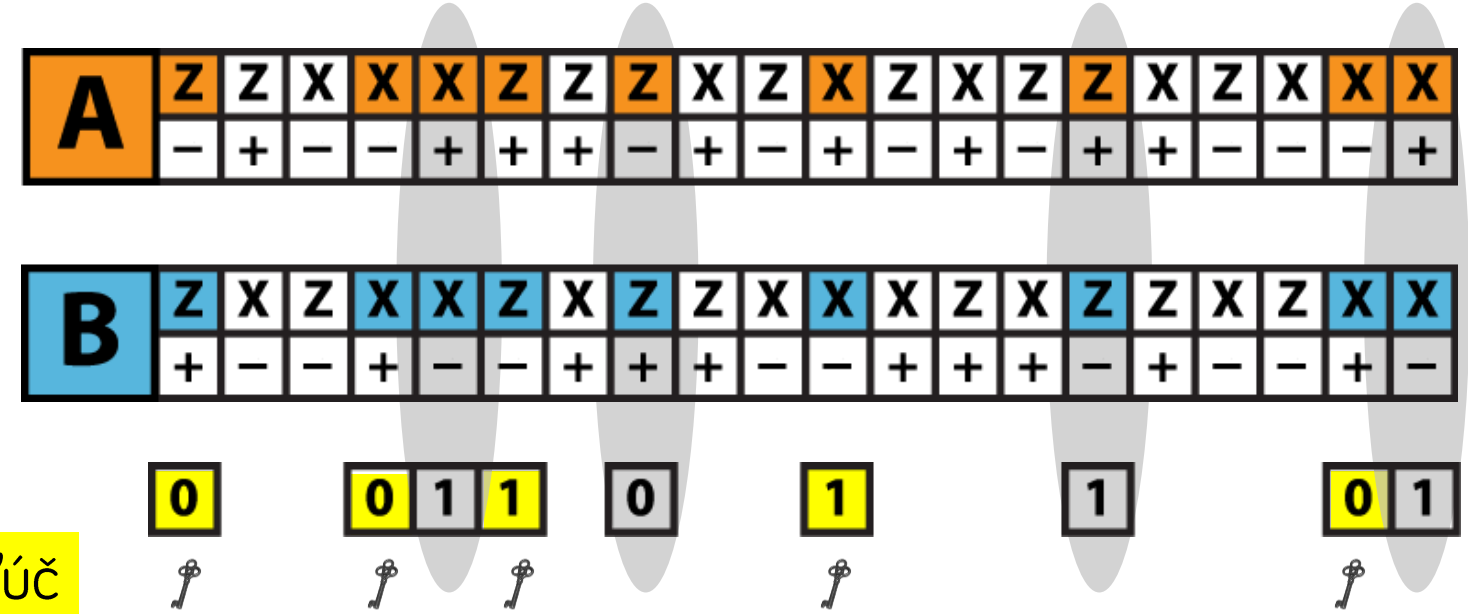
QKD

[Ekert91]


A
Z Z X X X Z Z Z X Z X Z X Z Z X Z X X X
− + − − + + + − + − + − + − + + − − − +
verejné
tajné
B
Z X Z X X Z X Z Z X X X Z X Z Z X Z X X
+ − − + − − + + + − − + + + − + − − + −
verejné
tajné

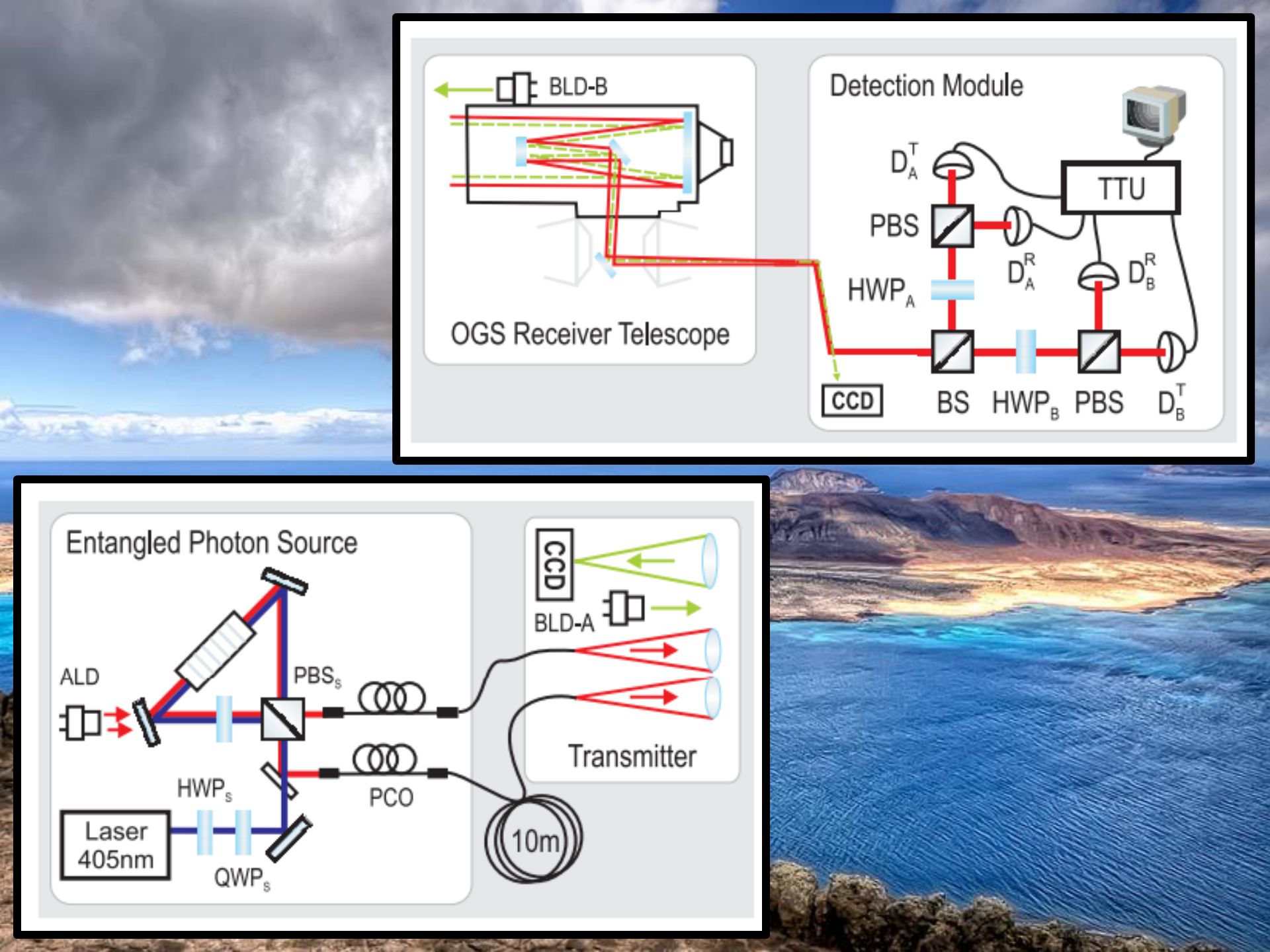
QKD

[Ekert91]


A
Z Z X X X Z Z Z X Z X Z X Z X Z X Z X X X
− + − − + + + − + − + − + − + + − − − +
B
Z X Z X X Z X Z Z X X X Z X Z Z X Z X X
+ − − + − − + + + − − + + + − + − − + −
0 0 1 1 0 1 1 0 1
kľúč

QKD

[Ekert91]


BLD-B
OGS Receiver Telescope
Detection Module
D_A^T
TTU
PBS
D_A^R
D_B^R
HWP_A
CCD
BS
HWP_B
PBS
D_B^T
Entangled Photon Source
ALD
PBS_S
HWP_S
PCO
Laser 405nm
QWP_S
10m
CCD
BLD-A
Transmitter

search

SWISS QUANTUM

PROJECT | NETWORK | PERFORMANCE | PARTNERS | STAY INFORMED | CONTACT

NEWS

SwissQuantum Project Completes Longest-Running Testbed of Quantum Crytography
Geneva, Switzerland - ID Quantique SA announced the successful completion (...)

read more

SwissQuantum network dismantled
The SwissQuantum network has been dismantled after almost two years of (...)

read more

Quantum encryption to secure World Cup link
In the first use of ultra secure quantum encryption at a world public (...)

read more

IDQ and UNIGE go one step further with the European research project QuRep
The SwissQuantum network highlights the reliability of Quantum Key (...)

SWISS QUANTUM

In January 2011 Swissquantum successfully completed the longest running project for testing Quantum Key Distribution (QKD) in a field environment. The main goal of the SwissQuantum network, installed in the Geneva metropolitan area in March 2009, was to validate the reliability and robustness of QKD in continuous operation in a network over a long time period in a field environment. The quantum layer ran stably for nearly 2 years, confirming the viability of QKD as a commercial encryption technology in telecommunication networks.

The network consisted of three nodes located in the Geneva metropolitan area.

This network served as a platform for:
- Research & Development
- Demonstration and
- Education

in the field of quantum communications.

This website presents the project, the technology used as well as the results of the extensive test campaign.

NATURE PHOTONICS | LETTER

Hacking commercial quantum cryptography systems by tailored bright illumination

Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar & Vadim Makarov

Nature Photonics **4**, 686–689 (2010)

3 Hackovane komerčnéhp QKD

Zmeraj, prepošli, oslep detektor a presvedč ho, nech meria, čo ty chceš.

[Gerhadt et al., NUS]

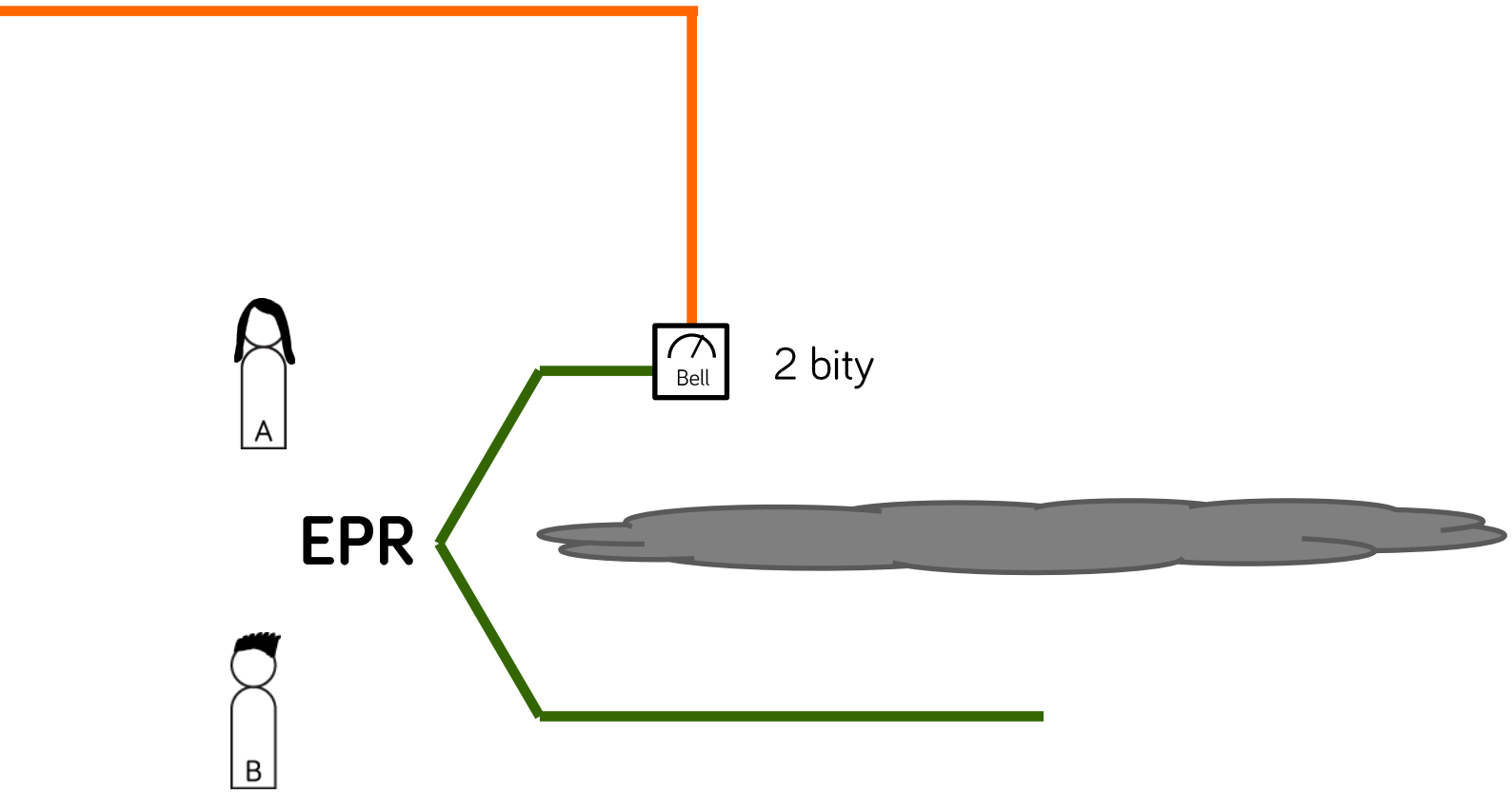
3 Kvantová teleportácia

[QIP 2012, UMontréal]

3 Kvantová teleportácia

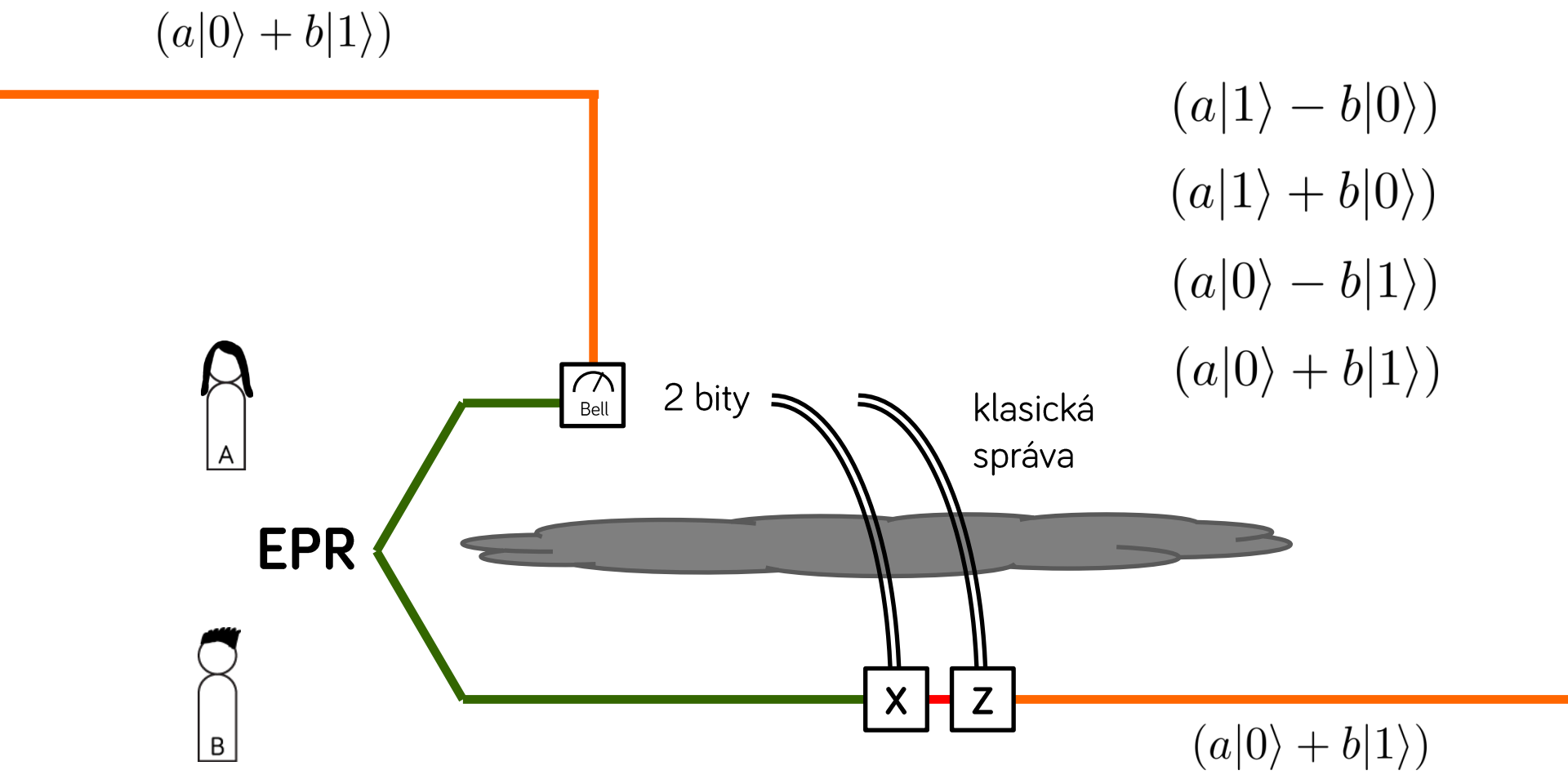
- posielanie kvantovej informácie pomocou predzdieľaného EPR páru

$$(a|0\rangle + b|1\rangle)$$



3 Kvantová teleportácia

- posielanie kvantovej informácie pomocou predzdieľaného EPR páru

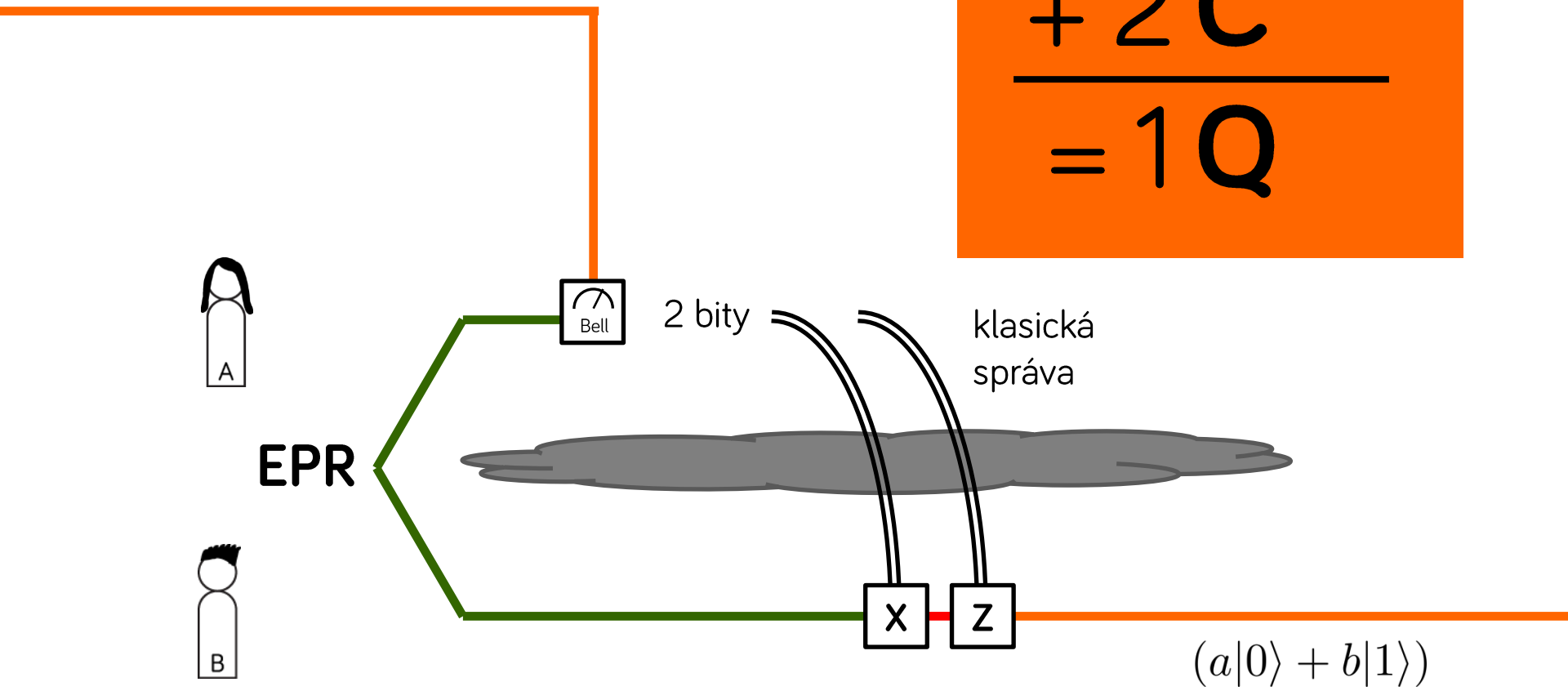


3 Kvantová teleportácia

- posielanie kvantovej informácie pomocou predzdieľaného EPR páru

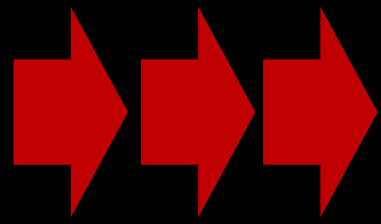
1 EPR
+ 2 C
= 1 Q

$(a|0\rangle + b|1\rangle)$



1 **run like the wind**

drahocenné informácie

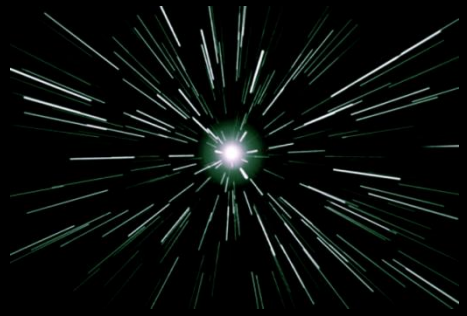


2 **traveling light**

chytáme elektromagnetické vlny

3 **warp speed**

čudesná kvantová mechanika



čudesné okamžité pôsobenie na diaľku

Daniel Nagaj

universität wien

SAV