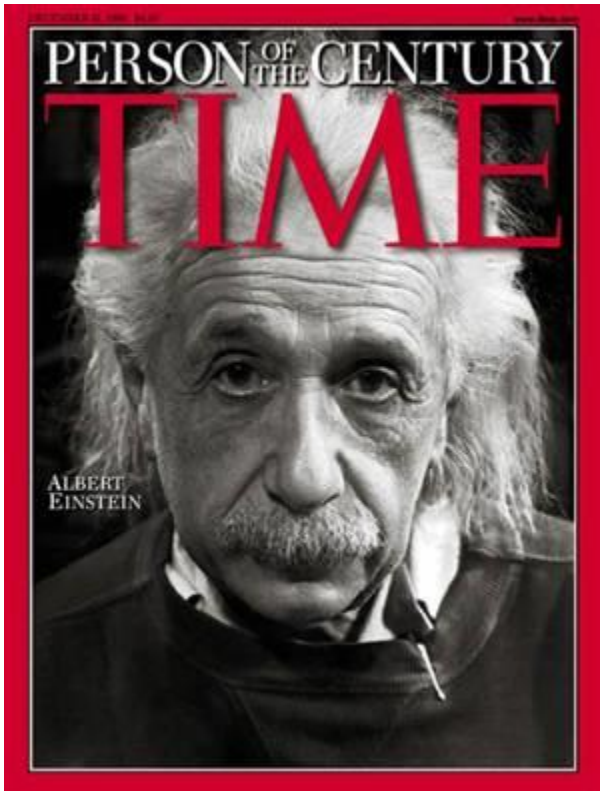
Czy można się teleportować?

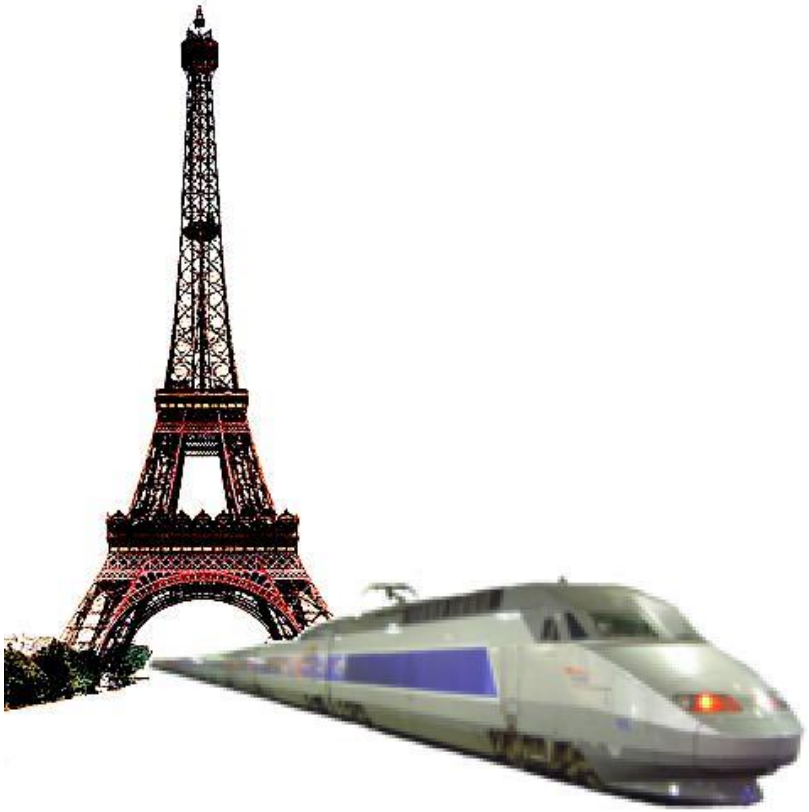
Jacek.Szczytko@fuw.edu.pl Wydział Fizyki UW

Sprawy bieżące

1. Esej na temat przyszłości – do 10 stycznia!
2. Nowy przedmiot „**Od pomysłu do patentu - Trendy, nowe technologie i zarządzanie innowacjami**” (Jacek Szczytko, Piotr Nieżurawski)– kwalifikacje na podstawie EGZAMINU! 1100-2`TNT (2 i 3 rok FIZ), 3 ECTS

Szczególna teoria względności





Doświadczenie: w naszym Wszechświecie największą prędkością w dowolnym układzie współrzędnych jest prędkość światła *c*.

Wniosek: nie ma zdarzeń jednoczesnych we wszystkich układach współrzędnych!

Świat klasyczny i kwantowy

Uwaga 4: (tzw. *redukcja f. falowej*)

tzw. ***stany własne*** (*ortogonalne*, ang. *eigen states*)

dwa poziomy atomu $\{|g\rangle, |e\rangle\}$ np. $g = 1s$, $e = 2s$

spin elektronu $\{|\uparrow\rangle, |\downarrow\rangle\}$

foton o dwóch wzajemnie ortogonalnych stanach polaryzacji $\{|\rightarrow\rangle, |\uparrow\rangle\}$

Jeśli cząstka jest w superopozycji stanów A i B, to z definicji (tzw. *ortogonalność stanów*) nie może być zaobserwowana w obu z nich na raz!

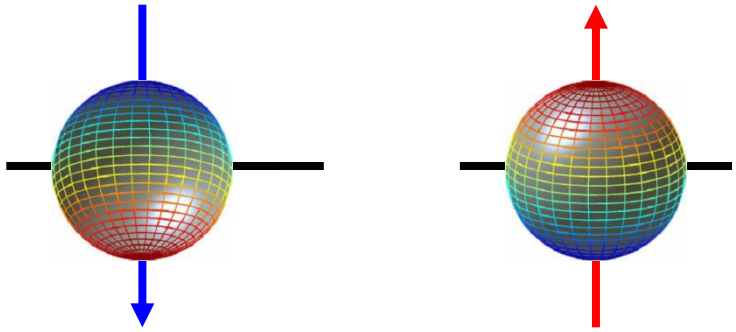
$$\Psi = A\Psi_A + B\Psi_B$$

Splątane stany - EPR.

Układ cząstek

$$\Psi_{n_1,n_2,n_3,\ldots}(r_1,r_2,r_3,\ldots t) \stackrel{?}{=} |n_1\rangle |n_2\rangle |n_3\rangle \ldots$$

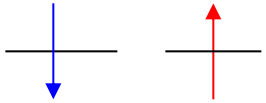
Np. spiny elektronów



Opis wielu cząstek kwantowych

Jeden elektron:

baza: $\left|\downarrow\right\rangle, \left|\uparrow\right\rangle$



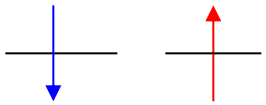
$$\left|\Psi\right\rangle = \alpha_0 \left|\downarrow\right\rangle + \alpha_1 \left|\uparrow\right\rangle$$

$$\alpha_0^2 + \alpha_1^2 = 1$$

Opis wielu cząstek kwantowych

Jeden elektron:

baza: $\left|\downarrow\right\rangle, \left|\uparrow\right\rangle$

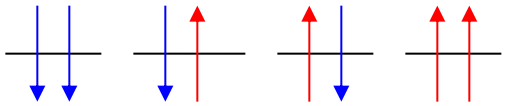


$$\left|\Psi\right\rangle = \alpha_0 \left|\downarrow\right\rangle + \alpha_1 \left|\uparrow\right\rangle$$

$$\alpha_0^2 + \alpha_1^2 = 1$$

Dla dwóch elektronów:

baza: $\left|\downarrow\right\rangle\left|\downarrow\right\rangle, \left|\downarrow\right\rangle\left|\uparrow\right\rangle, \left|\uparrow\right\rangle\left|\downarrow\right\rangle, \left|\uparrow\right\rangle\left|\uparrow\right\rangle$



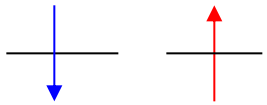
$$\left|\Psi\right\rangle = \alpha_{00}\left|\downarrow\right\rangle\left|\downarrow\right\rangle + \alpha_{01}\left|\downarrow\right\rangle\left|\uparrow\right\rangle + \alpha_{10}\left|\uparrow\right\rangle\left|\downarrow\right\rangle + \alpha_{11}\left|\uparrow\right\rangle\left|\uparrow\right\rangle$$

$$\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$$

Opis wielu cząstek kwantowych

Jeden elektron:

baza: $|\downarrow\rangle, |\uparrow\rangle$

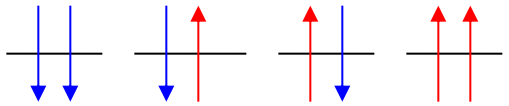


$$|\Psi\rangle = \alpha_0|\downarrow\rangle + \alpha_1|\uparrow\rangle$$

$$\alpha_0^2 + \alpha_1^2 = 1$$

Dla dwóch elektronów:

baza: $|\downarrow\rangle|\downarrow\rangle, |\downarrow\rangle|\uparrow\rangle, |\uparrow\rangle|\downarrow\rangle, |\uparrow\rangle|\uparrow\rangle$



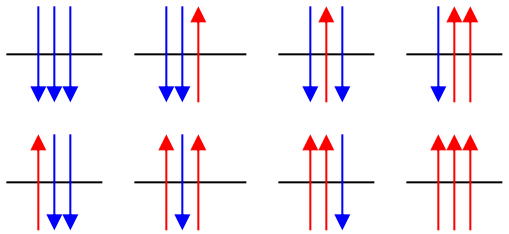
$$|\Psi\rangle = \alpha_{00}|\downarrow\rangle|\downarrow\rangle + \alpha_{01}|\downarrow\rangle|\uparrow\rangle + \alpha_{10}|\uparrow\rangle|\downarrow\rangle + \alpha_{11}|\uparrow\rangle|\uparrow\rangle$$

$$\alpha_{00}^2 + \alpha_{01}^2 + \alpha_{10}^2 + \alpha_{11}^2 = 1$$

Dla trzech elektronów:

baza: $|\downarrow\rangle|\downarrow\rangle|\downarrow\rangle, |\downarrow\rangle|\downarrow\rangle|\uparrow\rangle, |\downarrow\rangle|\uparrow\rangle|\downarrow\rangle, |\downarrow\rangle|\uparrow\rangle|\uparrow\rangle,$

$|\uparrow\rangle|\downarrow\rangle|\downarrow\rangle, |\uparrow\rangle|\downarrow\rangle|\uparrow\rangle, |\uparrow\rangle|\uparrow\rangle|\downarrow\rangle, |\uparrow\rangle|\uparrow\rangle|\uparrow\rangle,$



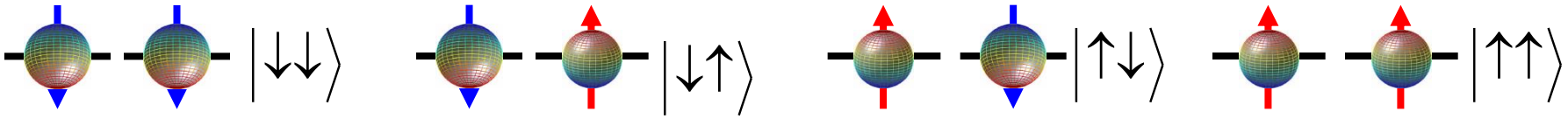
$$|\Psi\rangle = \alpha_{000}|\downarrow\rangle|\downarrow\rangle|\downarrow\rangle + \alpha_{001}|\downarrow\rangle|\downarrow\rangle|\uparrow\rangle + \alpha_{010}|\downarrow\rangle|\uparrow\rangle|\downarrow\rangle + \alpha_{011}|\downarrow\rangle|\uparrow\rangle|\uparrow\rangle +$$

$$+ \alpha_{100}|\uparrow\rangle|\downarrow\rangle|\downarrow\rangle + \alpha_{101}|\uparrow\rangle|\downarrow\rangle|\uparrow\rangle + \alpha_{110}|\uparrow\rangle|\uparrow\rangle|\downarrow\rangle + \alpha_{111}|\uparrow\rangle|\uparrow\rangle|\uparrow\rangle$$

itd..

$$\alpha_{000}^2 + \alpha_{001}^2 + \alpha_{010}^2 + \alpha_{011}^2 + \alpha_{100}^2 + \alpha_{101}^2 + \alpha_{110}^2 + \alpha_{111}^2 = 1$$

Opis wielu cząstek kwantowych



Stany Bella

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow\rangle + |\uparrow\uparrow\rangle\right) \qquad |\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle + |\uparrow\downarrow\rangle\right)$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow\rangle - |\uparrow\uparrow\rangle\right) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle - |\uparrow\downarrow\rangle\right)$$

po prostu inna baza...

np:

$$|\downarrow\downarrow\rangle = \frac{1}{\sqrt{2}}\left(|\Phi^+\rangle + |\Phi^-\rangle\right)$$

Opis wielu cząstek kwantowych

Motto na dziś:

Stany splątane są splątane (w każdej bazie)

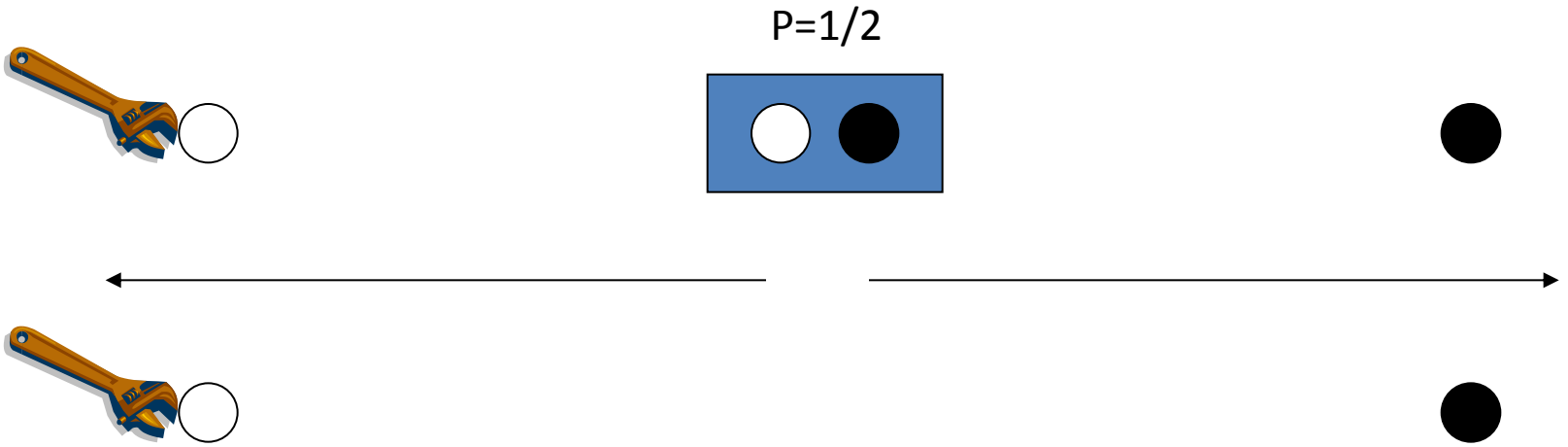
$$\left|\downarrow_\theta\right\rangle = \cos\theta\left|\downarrow\right\rangle + \sin\theta\left|\uparrow\right\rangle$$
$$\left|\uparrow_\theta\right\rangle = -\sin\theta\left|\downarrow\right\rangle + \cos\theta\left|\uparrow\right\rangle$$

$$\left|\downarrow\right\rangle = \cos\theta\left|\downarrow_\theta\right\rangle - \sin\theta\left|\uparrow_\theta\right\rangle$$
$$\left|\uparrow\right\rangle = \sin\theta\left|\downarrow_\theta\right\rangle + \cos\theta\left|\uparrow_\theta\right\rangle$$

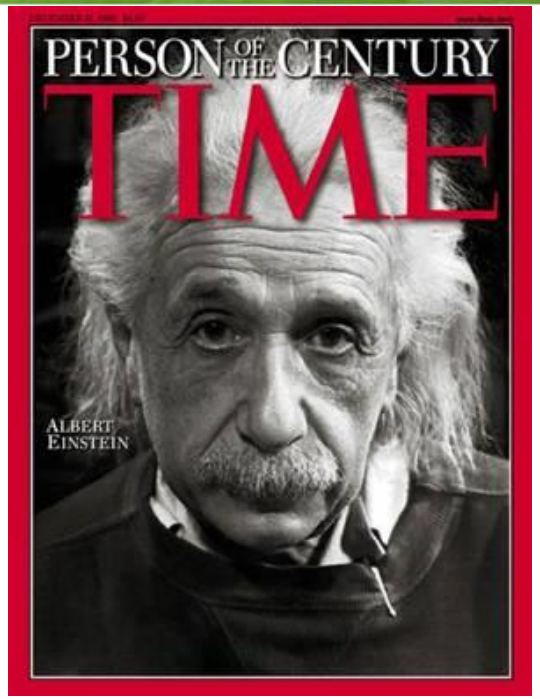
$$\left|\downarrow_\theta\downarrow_\theta\right\rangle + \left|\uparrow_\theta\uparrow_\theta\right\rangle = \left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle$$

Splątane stany - EPR

Problem:
Czy cząstki splątane mają określone cechy (takie jak spin, polaryzacja itp.) już w momencie „narodzin”, czy nabywają je dopiero w chwili pomiaru?

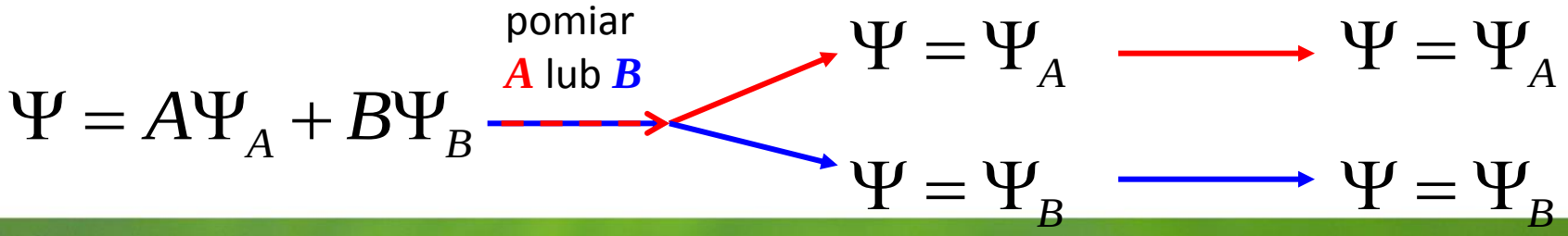


Splątane stany - EPR



Einstein:
1. informacja w przyrodzie nie porusza się szybciej niż światło w próżni
2. nie ma absolutnej równoczesności zdarzeń

MQ: ewolucja funkcji falowej jest DETERMINISTYCZNA. Jednak w momencie pomiaru „dowiadujemy" się w jakim stanie jest funkcja (tzw. *redukcja f. falowej*)



Nierówność Bella.

John Bell

A: mężczyźni
B: wzrost powyżej 185
C: oczy niebieskie

ilość obiektów, które posiadają cechę A ale nie mają B +
ilość obiektów, które posiadają cechę B ale nie mają C
jest większa bądź równa
ilość obiektów, które posiadają cechę A ale nie mają C

ilość(A, not B) + ilość(B, not C) ≥ ilość(A, not C)

Bell pokazał, że w pewnych przypadkach mechanika kwantowa daje

ilość(A, not B) + ilość(B, not C) < ilość(A, not C)

!

http://www.upscale.utoronto.ca/PVB/Harrison/BellsTheorem/BellsTheorem.html

Nierówność Bella.

Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,[a] and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France

(Received 27 September 1982)

Correlations of linear polarizations of pairs of photons have been measured with time-varying analyzers. The analyzer in each leg of the apparatus is an acousto-optical switch followed by two linear polarizers. The switches operate at incommensurate frequencies near 50 MHz. Each analyzer amounts to a polarizer which jumps between two orientations in a time short compared with the photon transit time. The results are in good agreement with quantum mechanical predictions but violate Bell's inequalities by 5 standard deviations.

PACS numbers: 03.65.Bz, 35.80.+s

Bell's inequalities apply to any correlated measurement on two correlated systems. For instance, in the optical version of the Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*,[1] a source emits pairs of photons (Fig. 1). Measurements of the correlations of linear polarizations are performed on two photons belonging to the same pair. For pairs emitted in suitable states, the correlations are strong. To account for these correlations, Bell[2] considered theories which invoke common properties of both members of the

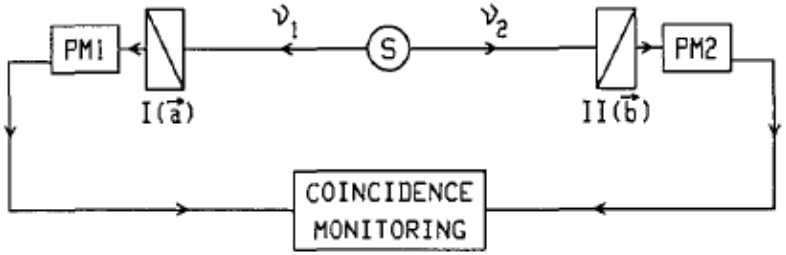
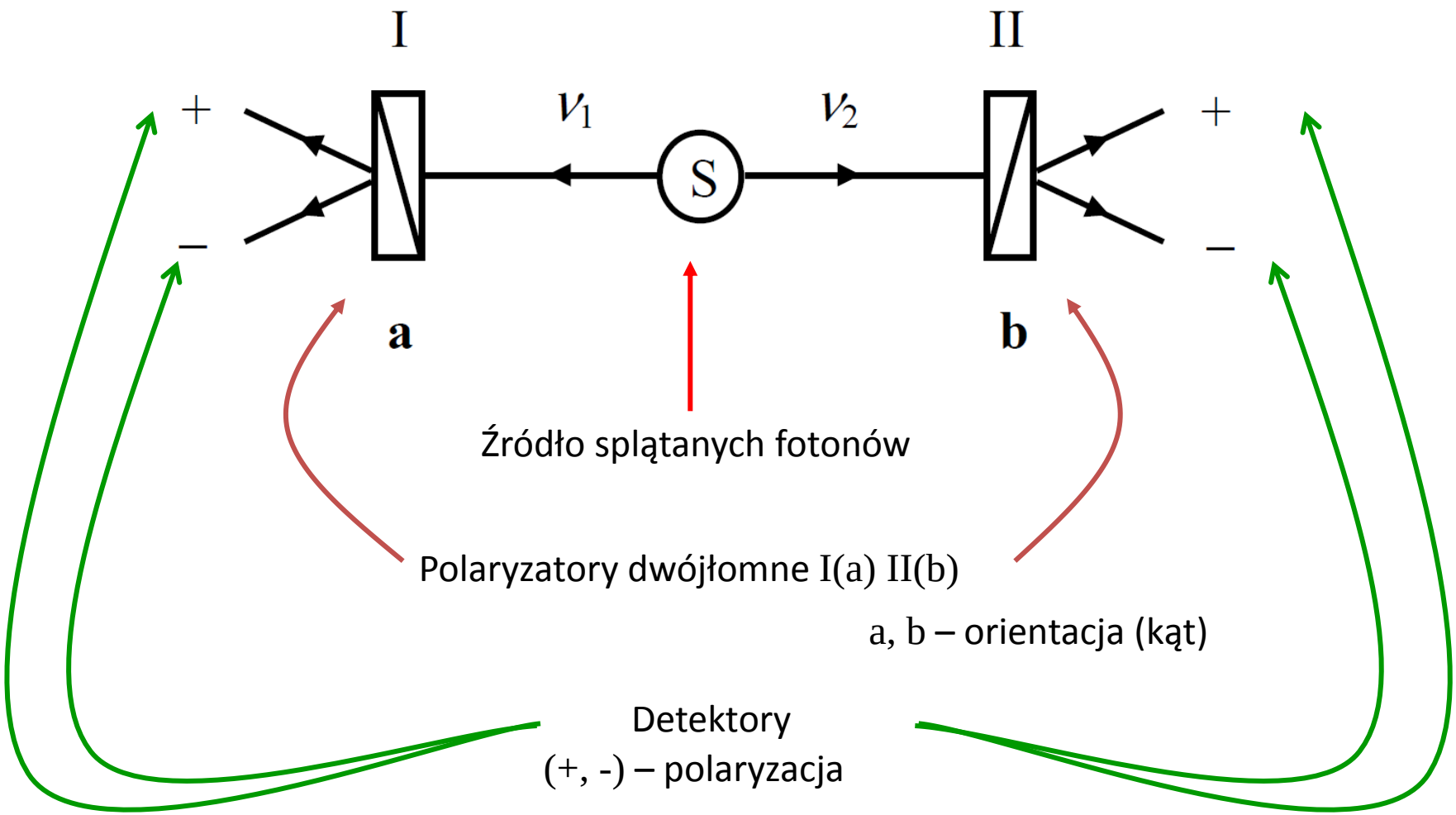


FIG. 1. Optical version of the Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*. The pair of photons ν_1 and ν_2 is analyzed by linear polarizers I and II (in orientations $\vec{a}$ and $\vec{b}$) and photomultipliers. The coincidence rate is monitored.

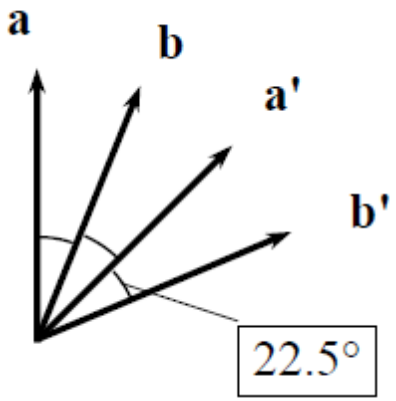
Nierówność Bella.

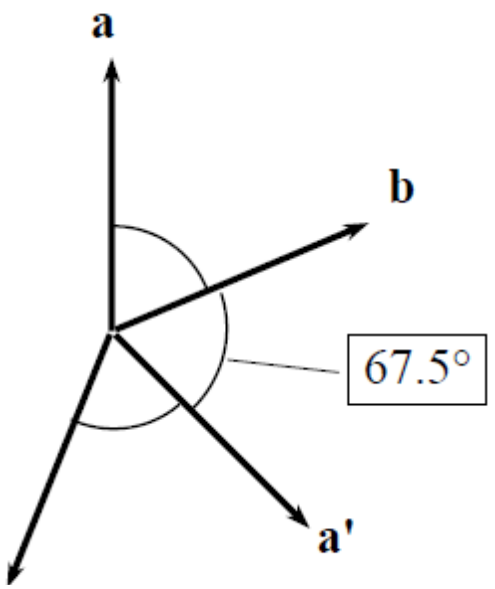


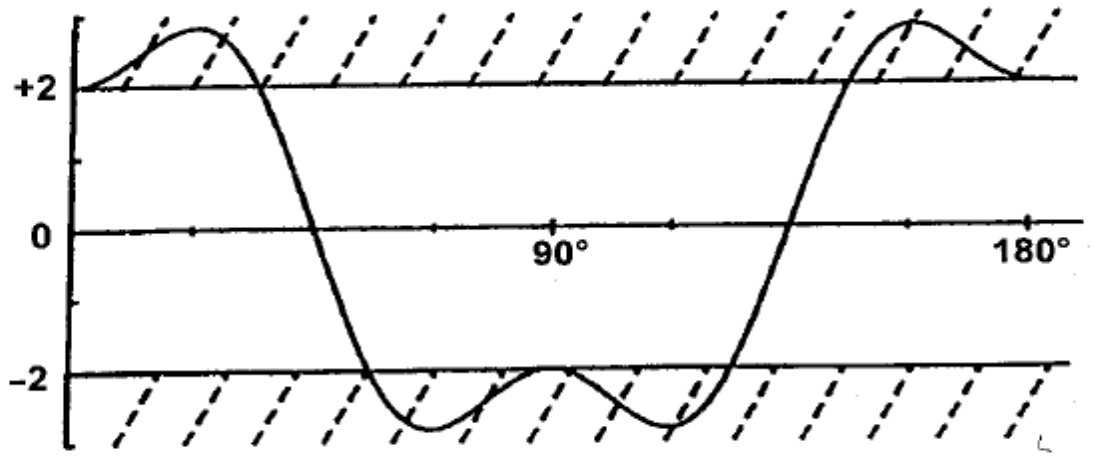
Nierówność Bella.

$$S_{MQ} = 2\sqrt{2} \quad \text{for} \quad \theta = \pm\frac{\pi}{8}$$

$$S_{MQ} = -2\sqrt{2} \quad \text{for} \quad \theta = \pm\frac{3\pi}{8}$$





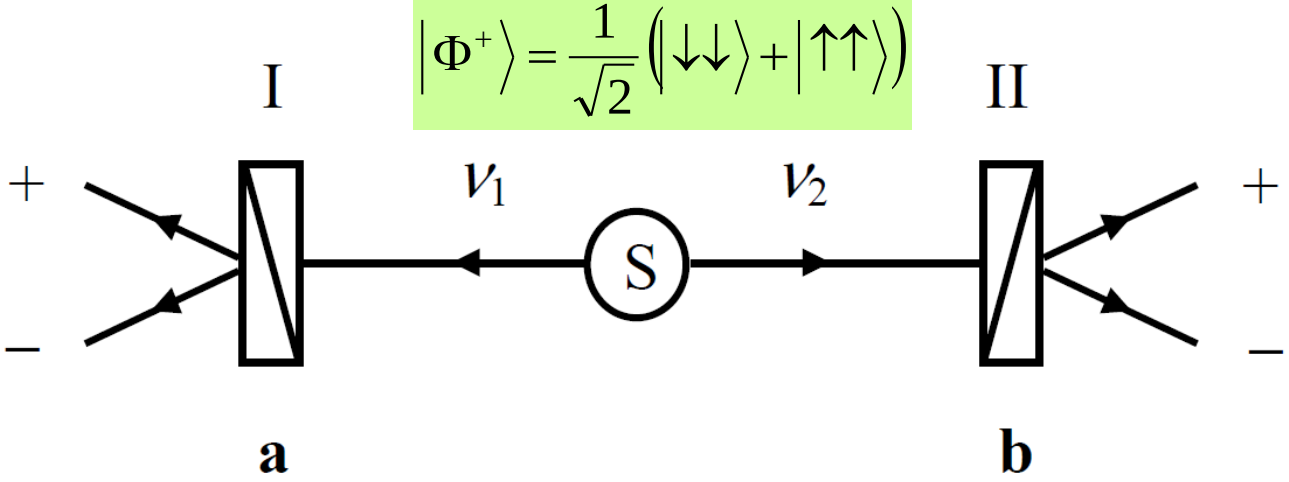


$$S_{QM} = 2\sqrt{2}$$

Figure 5 *- S(θ) as predicted by Quantum Mechanics for EPR pairs. The conflict with Bell's inequalities happens when |S| is larger than 2, and it is maximum for the sets of orientations of Figure 4.*

Nierówność Bella.

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$



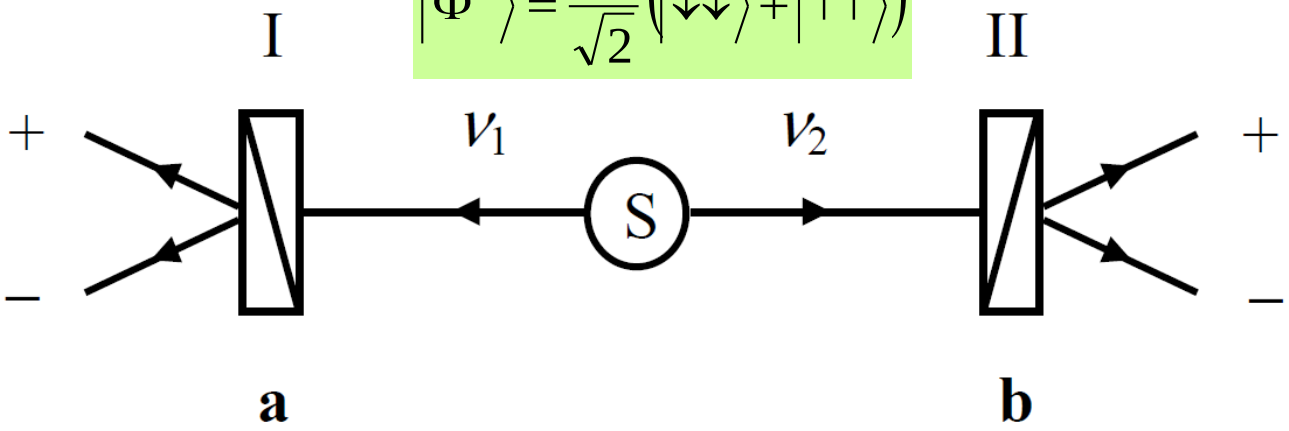
Kluczowe założenie odnośnie parametrów λ: **LOKALNOŚĆ**, czyli wynik pomiaru $A(\lambda,\mathbf{a})$ nie zależał od wyniku $B(\lambda,\mathbf{b})$ oraz rozkład prawdopodobieństwa parametru λ nie zależał od orientacji polaryzatorów **a** i **b**.

Wnioski:

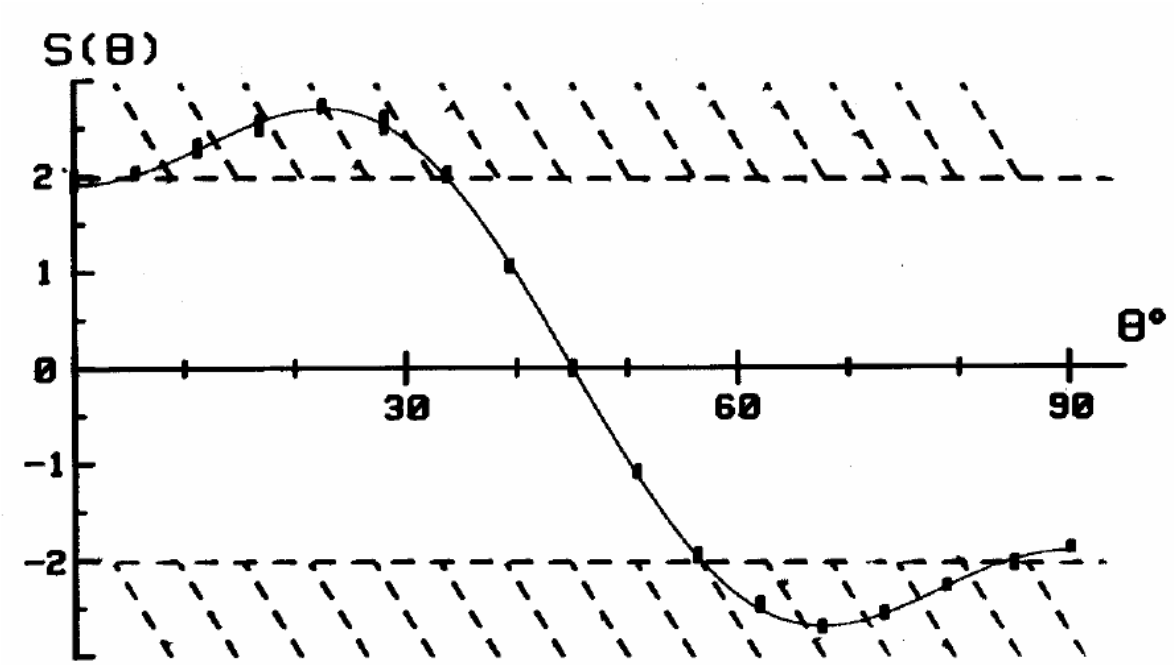
1. Stan kwantowy splątanych cząstek nie jest ustalony oddzielnie dla każdej z nich.
2. Redukcja funkcji falowej następuje w momencie pomiaru.

Nierówność Bella.

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$



Eksperyment:



Nierówność Bella.

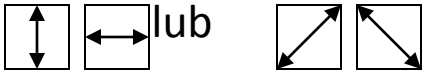
Załóżmy, że dysponujemy stanem

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$

np. dwa fotony.

Wtedy $\left|\downarrow\right\rangle, \left|\uparrow\right\rangle$

oznaczają dwie ortogonalne polaryzacje:

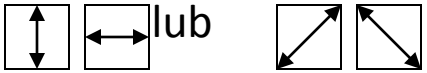


Nierówność Bella.

Załóżmy, że dysponujemy stanem

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$

np. dwa fotony.
Wtedy $\left|\downarrow\right\rangle, \left|\uparrow\right\rangle$
oznaczają dwie ortogonalne polaryzacje:



Załóżmy, że możemy na tym stanie wykonać trzy różne pomiary:
$\boldsymbol{A}$, $\boldsymbol{B}$ i $\boldsymbol{C}$,
które dają wyniki „1” lub „0” z prawdopodobieństwem ½.

np. polaryzatory w pozycji

0°, 60°, 120°
$\boldsymbol{A}$, $\boldsymbol{B}$ i $\boldsymbol{C}$

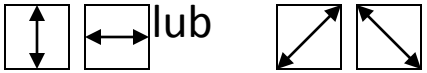
<u>Uwaga</u> (ale bez znaczenia)
W tym przykładzie wybraliśmy stan Bella w taki sposób, że wyniki TYCH SAMYCH pomiarów na OBU składnikach pary są w pełni skorelowane (np. pomiar A na obu daje w wyniku tylko pary „00” lub „11”). Ale mogliśmy też wybrać pełną anty-korelację („01” lub „10”) – nie ma to znaczenia.

Nierówność Bella.

Załóżmy, że dysponujemy stanem

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$

np. dwa fotony.
Wtedy $\left|\downarrow\right\rangle, \left|\uparrow\right\rangle$
oznaczają dwie ortogonalne polaryzacje:



Załóżmy, że możemy na tym stanie wykonać trzy różne pomiary:
$\boldsymbol{A}$, $\boldsymbol{B}$ i $\boldsymbol{C}$,
które dają wyniki „1” lub „0” z prawdopodobieństwem ½.

np. polaryzatory w pozycji

0°, 60°, 120°
$\boldsymbol{A}$, $\boldsymbol{B}$ i $\boldsymbol{C}$

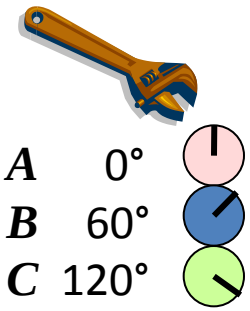
Możemy teraz odseparować oba składniki stanu splątanego i niezależnie wykonać na nich pomiary $\boldsymbol{A}$, $\boldsymbol{B}$ i $\boldsymbol{C}$,

pierwszy

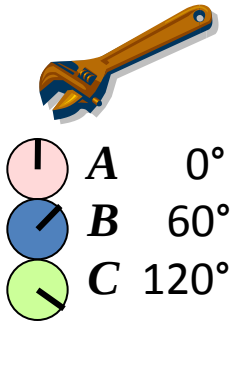
drugi

Nierówność Bella.

pierwszy



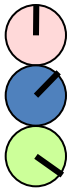
$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$



drugi

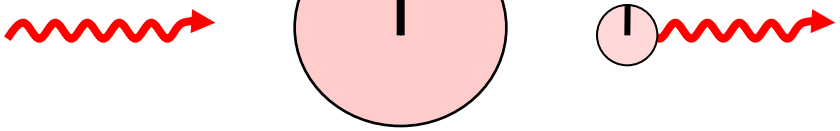
Nierówność Bella.

A 0°
B 60°
C 120°



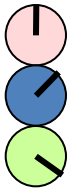
<u>Uwaga</u>:
Możemy wykonać na raz tylko JEDEN z pomiarów (różne polaryzacje nie są współmierzalne).

<u>Nie</u>spolaryzowany foton.



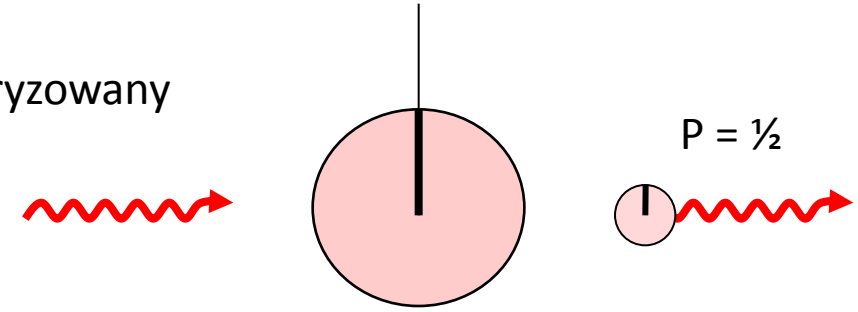
Nierówność Bella.

A 0°
B 60°
C 120°

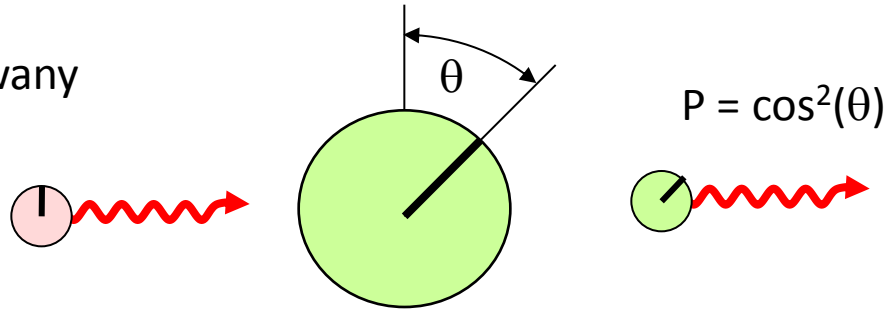


<u>Uwaga</u>:
Możemy wykonać na raz tylko JEDEN z pomiarów (różne polaryzacje nie są współmierzalne).

<u>Nie</u>spolaryzowany foton.

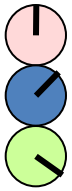


Spolaryzowany foton.



Prawo Malusa

Nierówność Bella.

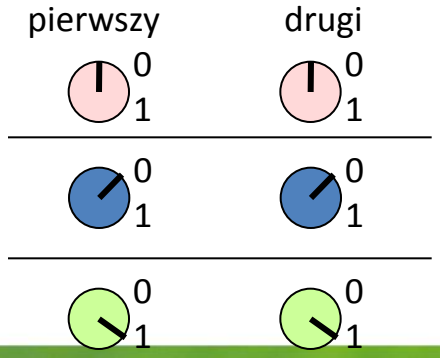


Uwaga:
Możemy wykonać na raz tylko JEDEN z pomiarów (różne polaryzacje nie są współmierzalne).

Dla stanu:

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$

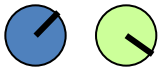
1. Pomiar dokonany tylko na jednej cząstce daje wynik „1” lub „0” z prawdopodobieństwem ½
2. Jeśli oba pomiary zostały wykonane dla tej samej polaryzacji, to oba wyniki sa skorelowane



Mechanika kwantowa o pkt 2. „dba sama”. W mechanice klasycznej my musimy o to zadbać (ukryte parametry)!

Nierówność Bella.

Skoro możemy na tym stanie wykonać trzy różne pomiary $\boldsymbol{A}$, $\boldsymbol{B}$ i $\boldsymbol{C}$, które dają wyniki „1” lub „0” z prawdopodobieństwem ½, to jak wyglądają korelacje między nimi?

Np. pytamy: jeśli na <u>pierwszym</u> składniku wynik był „1” dla $\boldsymbol{A}$ 
to znaczy, że dla <u>drugiego</u> był:
„1” dla $\boldsymbol{A}$  ,
i dowolny („0” lub „1”) dla $\boldsymbol{B}$ i $\boldsymbol{C}$ 
z prawd. $P = \cos^2(\theta)$

$\cos^2(\theta) = \cos^2(60°) = \cos^2(120°) = ¼$

drugi

pierwszy

1	¼	¼
¼	1	¼
¼	¼	1

KWANTOWO:

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$

Średni rozkład = (***3*** × 1 + ***6*** × ¼) / 9 = ½

Gdy oba eksperymenty wybrane zostaną przypadkowo

Nierówność Bella.

Załóżmy że stan kwantowy splątanych cząstek jest ustalony oddzielnie dla każdej z nich, a redukcja funkcji falowej nastąpiła w momencie rozdzielenia cząstek. Jakie są „klasyczne” wyniki pomiaru?

pierwszy

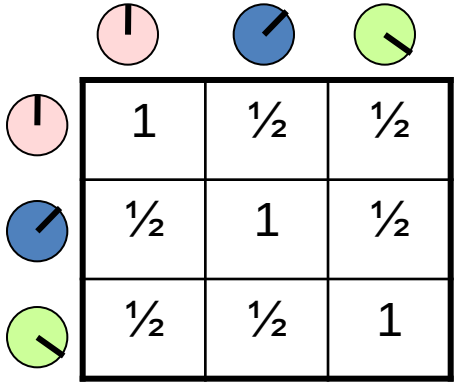
A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1



1	½	½
½	1	½
½	½	1

Średni rozkład = (***3*** × 1 + ***6*** × ½) / 9 = 2/3

Nierówność Bella.

Załóżmy że stan kwantowy splątanych cząstek jest ustalony oddzielnie dla każdej z nich, a redukcja funkcji falowej nastąpiła w momencie rozdzielenia cząstek. Jakie są „klasyczne” wyniki pomiaru?

pierwszy

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

1	½	½
½	1	½
½	½	1

Średni rozkład = (***3*** × 1 + ***6*** × ½) / 9 = 2/3

Nierówność Bella.

Załóżmy że stan kwantowy splątanych cząstek jest ustalony oddzielnie dla każdej z nich, a redukcja funkcji falowej nastąpiła w momencie rozdzielenia cząstek. Jakie są „klasyczne” wyniki pomiaru?

pierwszy

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

1	½	½
½	1	½
½	½	1

Średni rozkład = (***3*** × 1 + ***6*** × ½) / 9 = 2/3

Nierówność Bella.

Załóżmy że stan kwantowy splątanych cząstek jest ustalony oddzielnie dla każdej z nich, a redukcja funkcji falowej nastąpiła w momencie rozdzielenia cząstek. Jakie są „klasyczne” wyniki pomiaru?

pierwszy

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

1	1	½	½
½	½	1	½
½	½	½	1

Średni rozkład = (***3*** × 1 + ***6*** × ½) / 9 = 2/3

Nierówność Bella.

Załóżmy że stan kwantowy splątanych cząstek jest ustalony oddzielnie dla każdej z nich, a redukcja funkcji falowej nastąpiła w momencie rozdzielenia cząstek. Jakie są „klasyczne” wyniki pomiaru?

pierwszy

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

1	½	½
½	1	½
½	½	1

Średni rozkład = (***3*** × 1 + ***6*** × ½) / 9 = 2/3

Nierówność Bella.

Załóżmy że stan kwantowy splątanych cząstek jest ustalony oddzielnie dla każdej z nich, a redukcja funkcji falowej nastąpiła w momencie rozdzielenia cząstek. Jakie są „klasyczne” wyniki pomiaru?

pierwszy

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

1	½	½
½	1	½
½	½	1

Średni rozkład = (***3*** × 1 + ***6*** × ½) / 9 = 2/3

Nierówność Bella.

Załóżmy że stan kwantowy splątanych cząstek jest ustalony oddzielnie dla każdej z nich, a redukcja funkcji falowej nastąpiła w momencie rozdzielenia cząstek. Jakie są „klasyczne” wyniki pomiaru?

pierwszy

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

1	½	½
½	1	½
½	½	1

Średni rozkład = (***3*** × 1 + ***6*** × ½) / 9 = 2/3

Nierówność Bella.

(QM) = a+b+g+h = ¼

pierwszy

A, B i C

a	0	0	0
b	0	0	1
c	0	1	0
d	0	1	1
e	1	0	0
f	1	0	1
g	1	1	0
h	1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

	1	¼	½
	¼	1	½
	½	½	1

Nierówność Bella.

(QM) = a+b+g+h = ¼

(QM) = a+c+f+h = ¼

pierwszy

A, B i C

a	0	0	0
b	0	0	1
c	0	1	0
d	0	1	1
e	1	0	0
f	1	0	1
g	1	1	0
h	1	1	1

drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

	1	¼	¼
	¼	1	½
	¼	½	1

Nierówność Bella.

(QM) = a+b+g+h = ¼

(QM) = a+c+f+h = ¼

(QM) = a+d+e+h = ¼

pierwszy

A, B i C

a	0	0	0
b	0	0	1
c	0	1	0
d	0	1	1
e	1	0	0
f	1	0	1
g	1	1	0
h	1	1	1

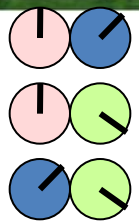
drugi

A, B i C

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

	1	¼	¼
	¼	1	¼
	¼	¼	1

Nierówność Bella.



(QM) = a+b+g+h = ¼

(QM) = a+c+f+h = ¼

(QM) = a+d+e+h = ¼

= a+b+g+h + a+c+f+h + a+d+e+h =

= 2(a+h) + (a+b+c+d+e+f+g+h) = ¾

2(a+h) + (a+b+c+d+e+f+g+h) = ¾

2(a+h) + ~~1~~ = ¾

a+h = ~~1~~/8 < 0

Nie ma klasycznych prawdopodobieństw dla NIEZALEŻNYCH zdarzeń

Żadna LOKALNA teoria parametrów ukrytych nie może odtworzyć wyników QM.

Nierówność Bella.

John Bell

A: mężczyźni
B: wzrost powyżej 190
C: oczy niebieskie

ilość obiektów, które posiadają cechę A ale nie mają B +
ilość obiektów, które posiadają cechę B ale nie mają C
jest większa bądź równa
ilość obiektów, które posiadają cechę A ale nie mają C

ilość(A, not B) + ilość(B, not C) ≥ ilość(A, not C)

Nierówność Bella (*Bell's inequality*)

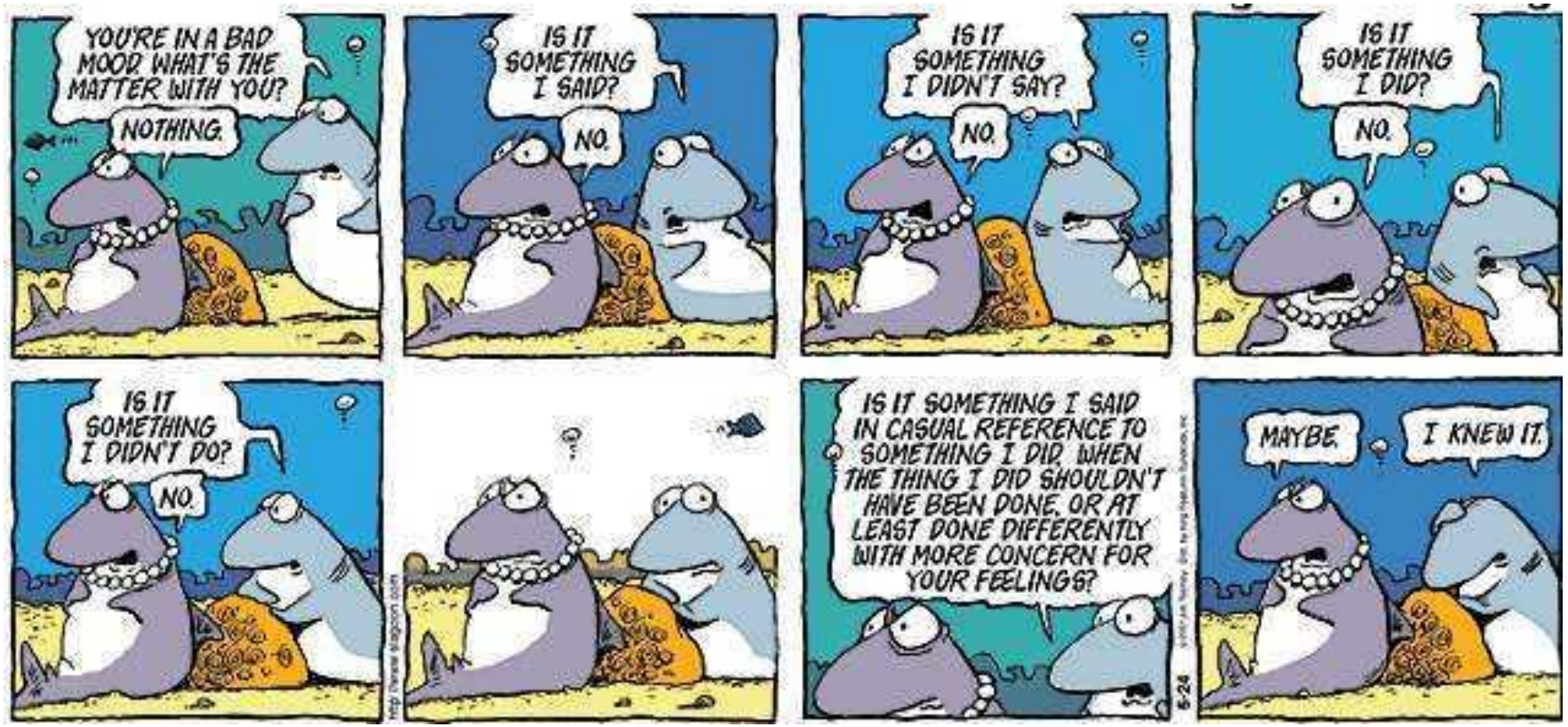
Cechy A, B i C nie istnieją równocześnie (niezależnie od siebie) w QM.

A: polaryzacja 
B: polaryzacja 
C: polaryzacja 

Za to stają się określone w momencie pomiaru (w przypadku stanów splątanych niezależnie od dzielącej cząstki odległości)! Mechanika kwantowa jest NIELOKALNA.

Splątane stany - EPR

POJEDYNCZE POMIARY NIE DAJĄ INFORMACJI O CAŁEJ FUNKCJI FALOWEJ

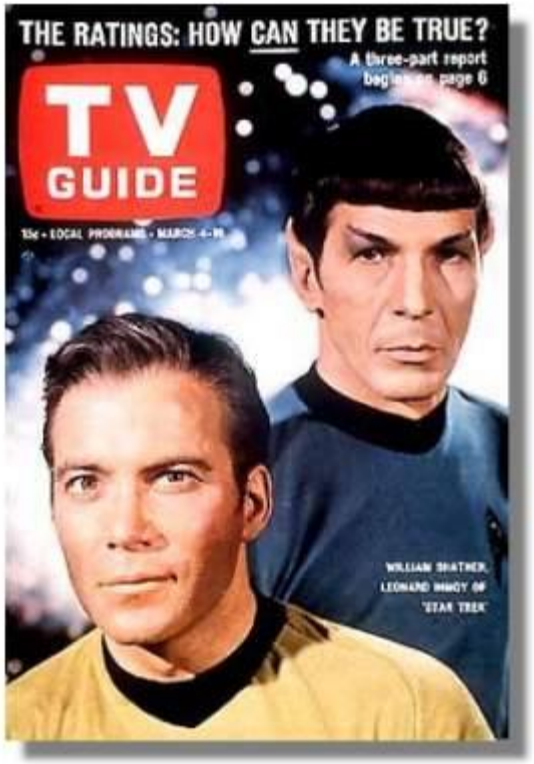


odpowiedź probabilistyczna

Teleportacja – za tydzień!

Jacek Szczytko, Wydział Fizyki UW

a. Poplątane stany.
   i. Eksperyment EPR.
   ii. Eksperyment Bella
b. Star-Trec, czyli teleportujcie mnie!
   i. Co wlasciwie teleportujemy
   ii. Ile kosztuje ubezpieczenie
c. Kryptografia kwantowa
   i. Czy są szyfry nie do złamania
   ii. Klucze duże i małe
   iii. Alice i Bob w świecie kwantów
   iv. Ewa chce posłuchać



Dialog z przyrodą musi być prowadzony w języku matematyki, w przeciwnym razie przyroda nie odpowiada na nasze pytania.

Michał Heller

Sprawy bieżące

1. Esej na temat przyszłości – do 10 stycznia!
2. Nowy przedmiot „**Od pomysłu do patentu - Trendy, nowe technologie i zarządzanie innowacjami**” (Jacek Szczytko, Piotr Nieżurawski)– kwalifikacje na podstawie EGZAMINU! 1100-2`TNT (2 i 3 rok FIZ), 3 ECTS

Przełom w kwantowej teleportacji - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

Przełom w kwantowej teleportacji | UNSW: The University of New South ...

http://technologie.gazeta.pl/internet/1,104530,9458065,Przelom_w_kwantow

Gazeta.pl | Technologie | Poczta | Forum | Blogi | Wyborcza.pl

Gazeta.pl Technologie

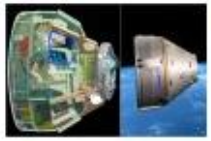
Szukaj

Program TV | Ne

Technologie | Biznes | Kultura | Sport | Plotki

Wiadomości | Testy | Telewizory | Mobile | Audio | Internet | Rankingi | F

Polecamy | Aplikacje mobilne | Tablety | Komputer w firmie



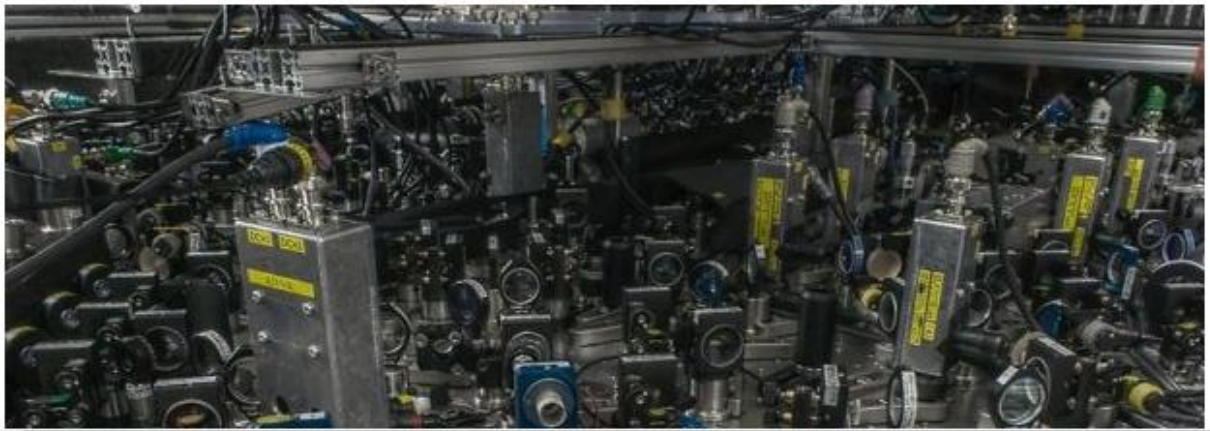
Co po promach kosmicznych? Cztery pierwsze projekty

Top 10 aplikacji do pracy na Androida

Polecą w polskie nieb

Janusz A. Urbanowicz | 18.04.2011 17:26

Przełom w kwantowej teleportacji



Komentuj, dodawaj zdjęcia i znajom

Zaloguj się | Nie masz u nas konta? Zarejestruj

Reklamy na tej stronie sprzedawane sa przez w
AdTaily.com (PLBLOADTAILY0001)

Sondaż

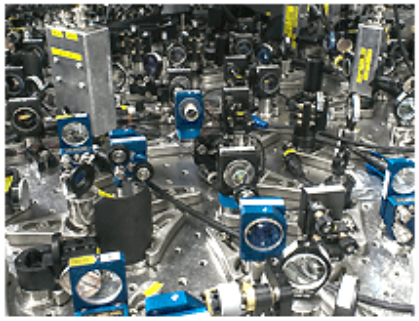
Jaki mobilny OS jest najle dla firm?

- Symbian
- iOS
- Android
- WP7

Quantum teleporter breakthrough

15th April 2011

Researchers have achieved a breakthrough in quantum communications and computing using a teleporter and a paradoxical cat.



Beam me up ... the teleporter in the lab of Professor Akira Furusawa at the University of Tokyo

The breakthrough is the first-ever transfer, or teleportation, of a particular complex set of quantum information from one point to another, opening the way for high-speed, high-fidelity transmission of large volumes of information, such as quantum encryption keys, via quantum communications networks.

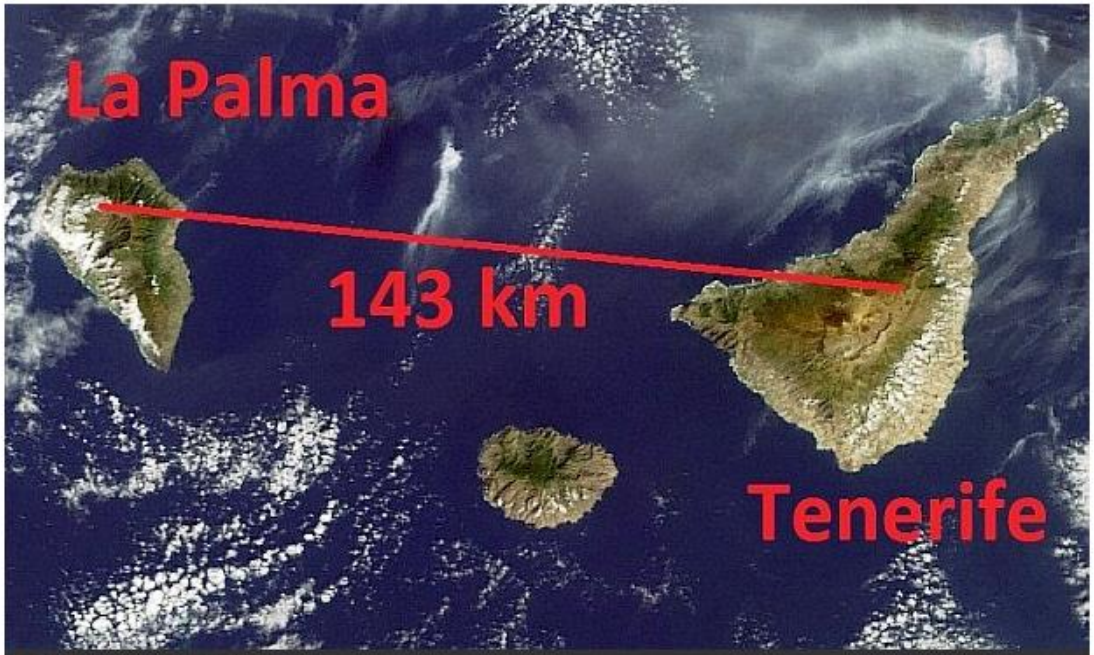
Teleportation – the transfer of quantum information from one location to another using normal, "classical" communications - is one of the fundamental quantum communication techniques.

The cat in the equation was not a living, breathing feline but rather "wave packets" of light representing the famous "thought experiment" known as Schrodinger's Cat. Schrodinger's Cat was a paradox proposed by early 20th century physicist Erwin Schrodinger to describe the situation in which normal, "classical" objects can exist in a quantum "superposition" - having two states at once.

Professor Elanor Huntington, in the School of Engineering and Information Technology at UNSW's Canberra campus at the Australian Defence Force Academy (ADFA), was part of a team led by University of Tokyo researchers. She said the

Naukowcy teleportowali "obiekt" na rekordową odległość

lmc | 07.09.2012 15:19



Z La Palma na Teneryfę (fot. ESA)

Nawet dzieci wiedzą - wystarczy klepnąć w komunikator i wypowiedzieć magiczną formułkę - "Scotty, beam me up". Pewnie nie było to aż tak proste, ale naukowcom rzeczywiście udało się teleportować "obiekt" na aż 143 kilometry!

Rzeczonym obiektem był stan kwantowy. Niestety, technologia, która pozwalałaby na teleportowanie materii lub nawet niewielkich dawek energii po prostu jeszcze nie istnieje. Mimo to, naukowcy nie poddają się, opracowując coraz to sprawniejsze metody teleportacji.

Najczęściej czytane

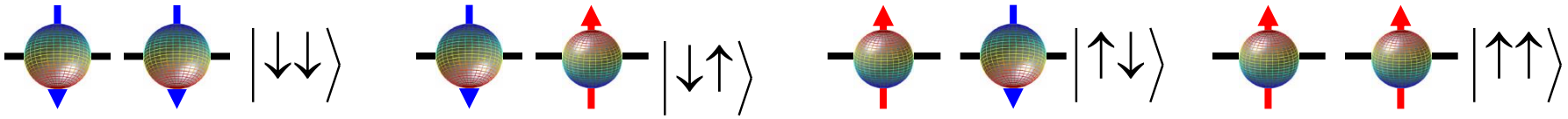
1. Naukowcy teleportowali "obiekt" na rekordową odległość
2. W Estonii nawet pierwszaki będą się uczyć programowania
3. Kosmiczna samotność Voyagera 1 [Galeria]
4. Samsung pozywa LG. Za wyciek technologii dot. wyświetlaczy
5. Zamiast żony - Siri, zamiast wczoraj i jutra - dziś
6. Najlepsze, najdziwniejsze i najbardziej zaskakujące z targów

Najczęściej szukane

Lotto

Wyniki Lotto z dnia 06.09.2012

Opis wielu cząstek kwantowych



Stany Bella

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow\rangle + |\uparrow\uparrow\rangle\right) \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle + |\uparrow\downarrow\rangle\right)$$

$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow\rangle - |\uparrow\uparrow\rangle\right) \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle - |\uparrow\downarrow\rangle\right)$$

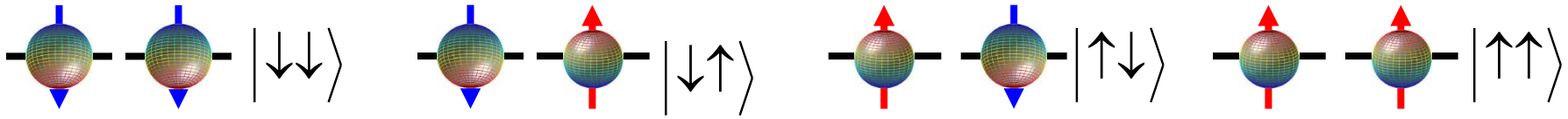
Ale stanów Bella nie da się przedstawić w postaci iloczynu dwóch funkcji

jednocząstkowych typu: $|\beta\rangle = |\varphi_1\rangle|\varphi_2\rangle$ gdzie $|\varphi_i\rangle = a_{i1}|\uparrow\rangle + a_{i2}|\downarrow\rangle$

Stany Bella są **SPLĄTANE**

spiny, polaryzacja fotonów, atom + foton, dwa atomy, atom w różnych stanach...

Opis wielu cząstek kwantowych



Stany Bella

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow\rangle + |\uparrow\uparrow\rangle\right) \qquad |\beta_{10}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\downarrow\rangle - |\uparrow\uparrow\rangle\right) \qquad |\beta_{01}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle + |\uparrow\downarrow\rangle\right) \qquad |\beta_{11}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow\uparrow\rangle - |\uparrow\downarrow\rangle\right)$$

Observation of entanglement between a single trapped atom and a single photon

B. B. Blinov, D. L. Moehring, L.- M. Duan & C. Monroe

NATURE | VOL 428 | 11 MARCH 2004 | www.nature.com/nature

PHYSICAL REVIEW A **69**, 042316 (2004)

Atom-photon entanglement generation and distribution

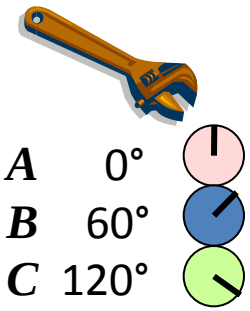
B. Sun, M. S. Chapman, and L. You

School of Physics, Georgia Institute of Technology, Atlanta, Georgia 30332, USA

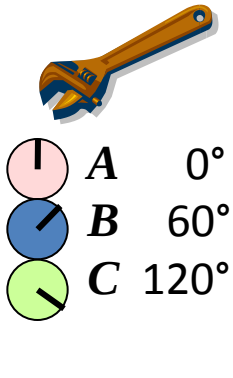
(Received 21 August 2003; published 21 April 2004)

Nierówności Bella.

pierwszy



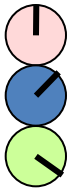
$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow\uparrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$



drugi

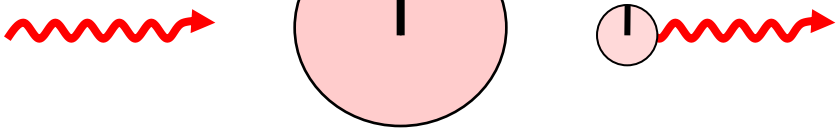
Nierówności Bella.

A 0°
B 60°
C 120°

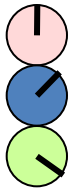


<u>Uwaga</u>:
Możemy wykonać na raz tylko JEDEN z pomiarów (różne polaryzacje nie są współmierzalne).

<u>Nie</u>spolaryzowany foton.



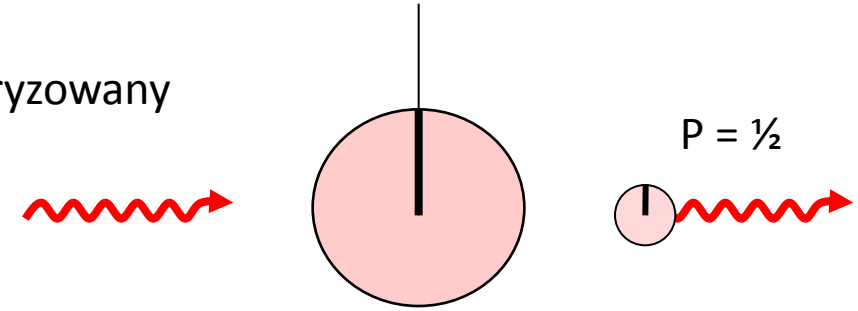
Nierówności Bella.



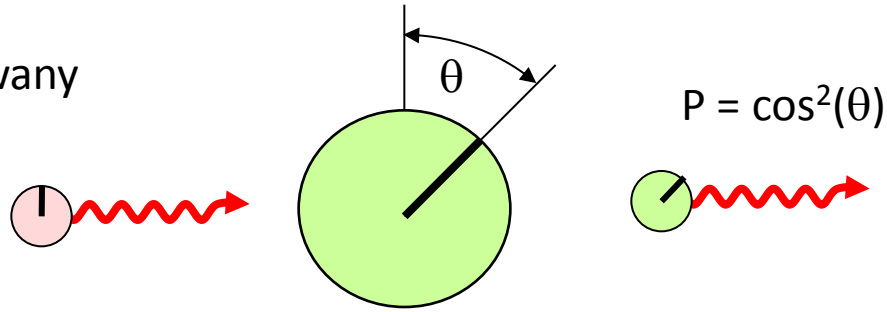
A 0°
B 60°
C 120°

<u>Uwaga</u>:
Możemy wykonać na raz tylko JEDEN z pomiarów (różne polaryzacje nie są współmierzalne).

<u>Nie</u>spolaryzowany foton.



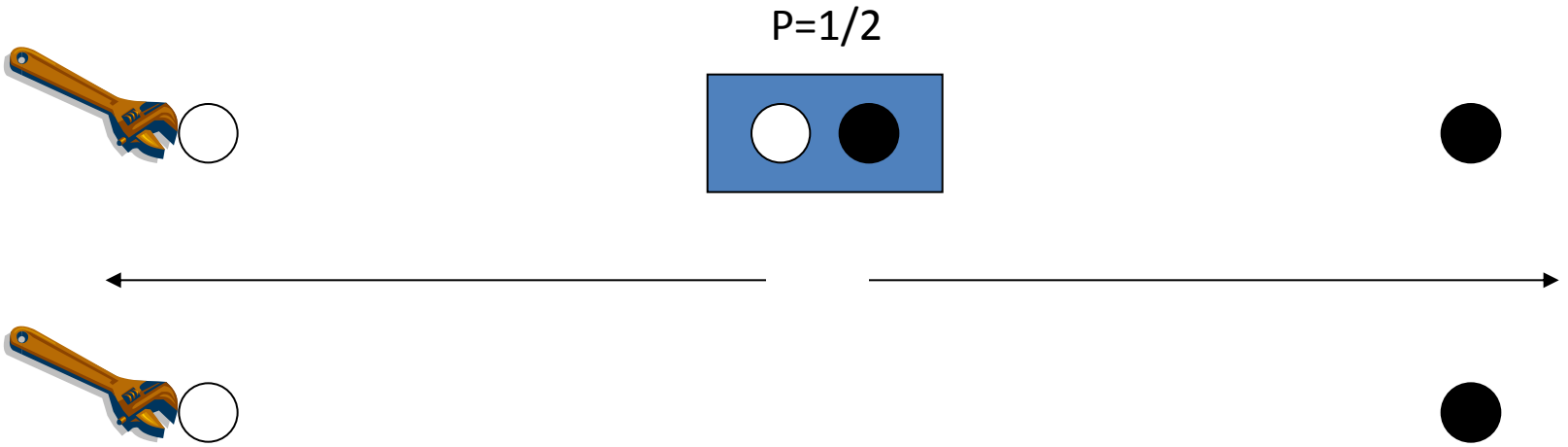
Spolaryzowany foton.



Prawo Malusa

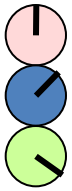
Splątane stany - EPR

Problem:
Czy cząstki splątane mają określone cechy (takie jak spin, polaryzacja itp.) już w momencie „narodzin”, czy nabywają je dopiero w chwili pomiaru?



Nierówności Bella.

A 0°
B 60°
C 120°

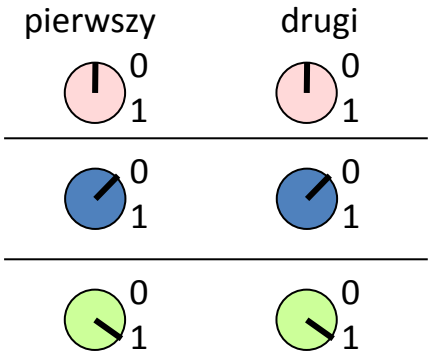


<u>Uwaga</u>:
Możemy wykonać na raz tylko JEDEN z pomiarów (różne polaryzacje nie są współmierzalne).

Dla stanu:

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$

1. Pomiar dokonany tylko na jednej cząstce daje wynik „1” lub „0” z prawdopodobieństwem ½
2. Jeśli oba pomiary zostały wykonane dla tej samej polaryzacji, to oba wyniki sa skorelowane



Mechanika kwantowa o pkt 2. „dba sama”. W mechanice klasycznej my musimy o to zadbać (ukryte parametry)!

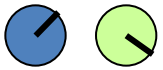
Nierówności Bella.

Skoro możemy na tym stanie wykonać trzy różne pomiary $\boldsymbol{A}$, $\boldsymbol{B}$ i $\boldsymbol{C}$, które dają wyniki „1” lub „0” z prawdopodobieństwem ½, to jak wyglądają korelacje między nimi?

Np. pytamy: jeśli na <u>pierwszym</u> składniku wynik był „1” dla $\boldsymbol{A}$ 

to znaczy, że dla <u>drugiego</u> był:

„1” dla $\boldsymbol{A}$  ,

i dowolny („0” lub „1”) dla $\boldsymbol{B}$ i $\boldsymbol{C}$ 

z prawd. $P = \cos^2(\theta)$

$\cos^2(\theta) = \cos^2(60°) = \cos^2(120°) = ¼$

KWANTOWO:

$$\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right)$$

drugi

pierwszy

1	¼	¼
¼	1	¼
¼	¼	1

Średni rozkład = (***3*** × 1 + ***6*** × ¼) / 9 = ½

Gdy oba eksperymenty wybrane zostaną przypadkowo

Zakaz klonowania

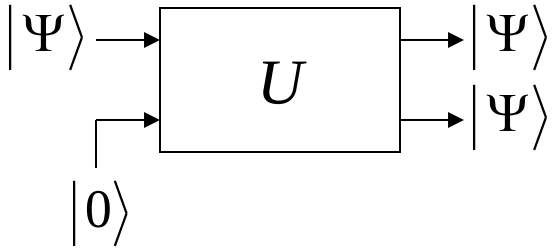
Źródło: Lucas Film

Zakaz klonowania

Źródło: internet

Klonowanie stanów kwantowych

$$|\Psi\rangle \rightarrow |\Psi\rangle, |\Psi\rangle, |\Psi\rangle, |\Psi\rangle, |\Psi\rangle, |\Psi\rangle, |\Psi\rangle \ldots$$



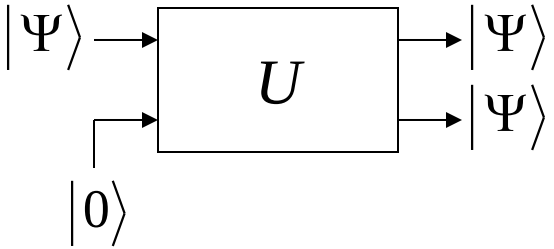
„czysta kartka”

Zakaz klonowania

Źródło: internet

Klonowanie stanów kwantowych

$$|\Psi\rangle \rightarrow |\Psi\rangle, |\Psi\rangle, |\Psi\rangle, |\Psi\rangle, |\Psi\rangle, |\Psi\rangle, |\Psi\rangle \ldots$$



„czysta kartka”

Wtedy $U|\Psi\rangle|0\rangle = |\Psi\rangle|\Psi\rangle$

$U|0\rangle|0\rangle = |0\rangle|0\rangle$

$U|1\rangle|0\rangle = |1\rangle|1\rangle$

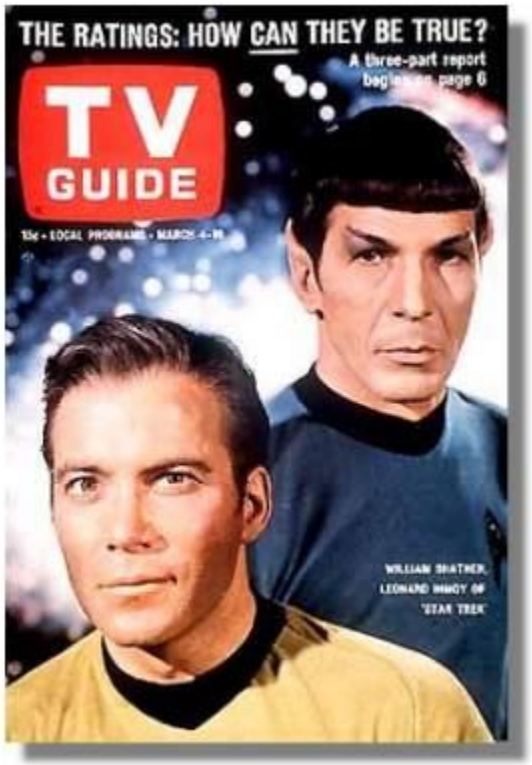
Ale dla $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ Dostajemy sprzeczność bo:

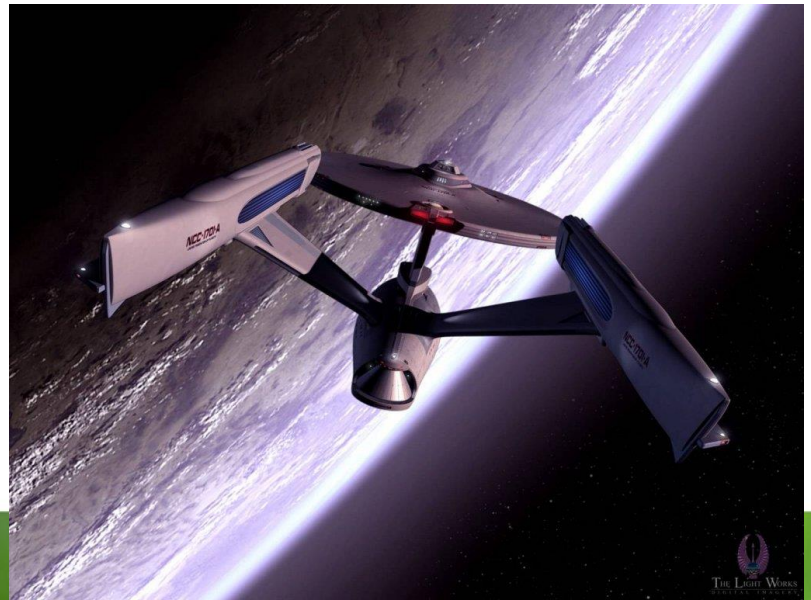
$$U|\Psi\rangle|0\rangle = U(\alpha|0\rangle + \beta|1\rangle)|0\rangle = \alpha U|0\rangle|0\rangle + \beta U|1\rangle|0\rangle = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \neq |\Psi\rangle|\Psi\rangle$$

!

bo $|\Psi\rangle|\Psi\rangle = \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle$

Kwantowa teleportacja





Kwantowa teleportacja

IBM CREW Six researchers--Richard Jozsa, William K. Woolters, Charles H. Bennett *(back row, left to right)* Gilles Brassard, Claude Crepeau and Asher Peres *(front row)*--proposed quantum teleportation in 1993.

Kwantowa teleportacja

PHYSICAL REVIEW
LETTERS

VOLUME 70 | 29 MARCH 1993 | NUMBER 13

Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels

Charles H. Bennett,[1] Gilles Brassard,[2] Claude Crépeau,[2,3]
Richard Jozsa,[2] Asher Peres,[4] and William K. Wootters[5]
[1] *IBM Research Division, T.J. Watson Research Center, Yorktown Heights, New York 10598*
[2] *Département IRO, Université de Montréal, C.P. 6128, Succursale "A", Montréal, Québec, Canada H3C 3J7*
[3] *Laboratoire d'Informatique de l'École Normale Supérieure, 45 rue d'Ulm, 75230 Paris CEDEX 05, France*[a]
[4] *Department of Physics, Technion–Israel Institute of Technology, 32000 Haifa, Israel*
[5] *Department of Physics, Williams College, Williamstown, Massachusetts 01267*
(Received 2 December 1992)

An unknown quantum state $|\phi\rangle$ can be disassembled into, then later reconstructed from, purely classical information and purely nonclassical Einstein-Podolsky-Rosen (EPR) correlations. To do so the sender, "Alice," and the receiver, "Bob," must prearrange the sharing of an EPR-correlated pair of particles. Alice makes a joint measurement on her EPR particle and the unknown quantum system, and sends Bob the classical result of this measurement. Knowing this, Bob can convert the state of his EPR particle into an exact replica of the unknown state $|\phi\rangle$ which Alice destroyed.

Kwantowa teleportacja

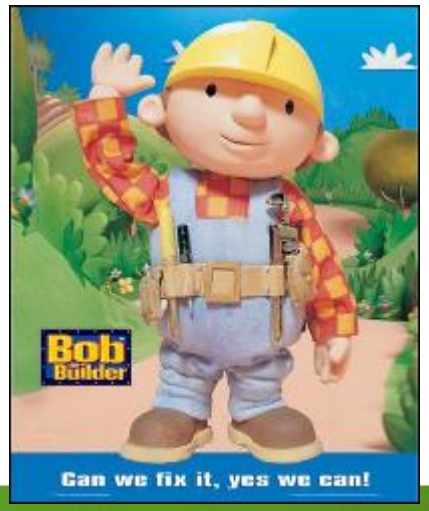
Dwucząstkowe stany splątane, baza Bella

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle + \left|\uparrow\uparrow\right\rangle\right) \qquad \left|\Psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\uparrow\right\rangle + \left|\uparrow\downarrow\right\rangle\right)$$

$$\left|\Phi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\downarrow\right\rangle - \left|\uparrow\uparrow\right\rangle\right) \qquad \left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\uparrow\right\rangle - \left|\uparrow\downarrow\right\rangle\right)$$

Alice

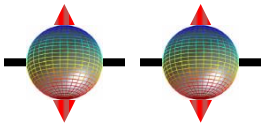
Bob



Kwantowa teleportacja

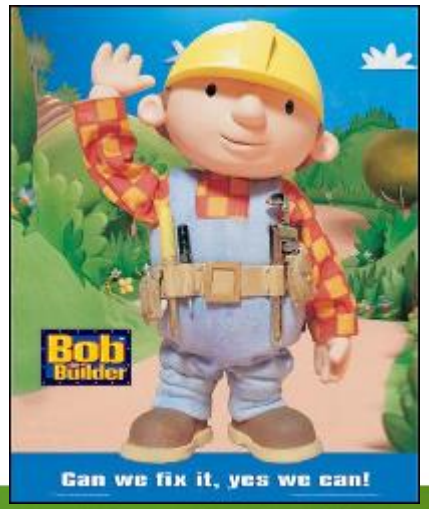
$$|\phi\rangle = a|\uparrow_1\rangle + b|\downarrow_1\rangle$$

$$|\Psi^-_{2,3}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow_2\uparrow_3\rangle - |\uparrow_2\downarrow_3\rangle\right)$$



Alice

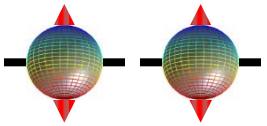
Bob



Kwantowa teleportacja

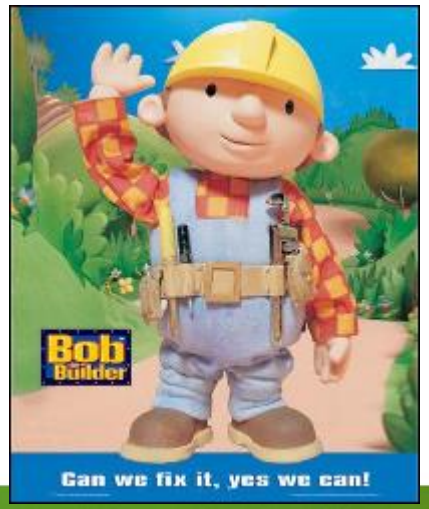
$$|\phi\rangle = a|\uparrow_1\rangle + b|\downarrow_1\rangle$$

$$|\Psi^-_{2,3}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow_2\uparrow_3\rangle - |\uparrow_2\downarrow_3\rangle\right)$$



Alice

Bob

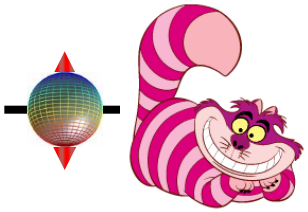


Kwantowa teleportacja

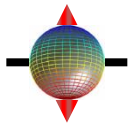
$$|\phi\rangle = a|\uparrow_1\rangle + b|\downarrow_1\rangle$$

$$|\Psi^-_{2,3}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow_2 \blacksquare\rangle - |\uparrow_2 \blacksquare\rangle\right)$$

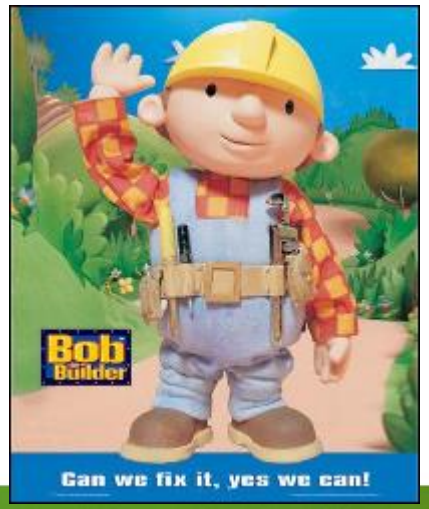
$$|\Psi^-_{2,3}\rangle = \frac{1}{\sqrt{2}}\left(|\blacksquare\uparrow_3\rangle - |\blacksquare\downarrow_3\rangle\right)$$



Alice



Bob

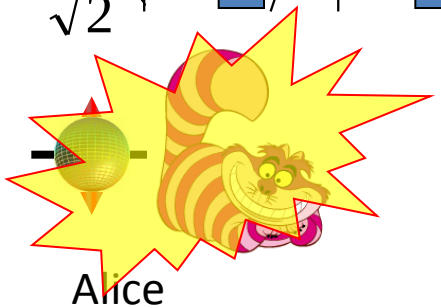


Kwantowa teleportacja

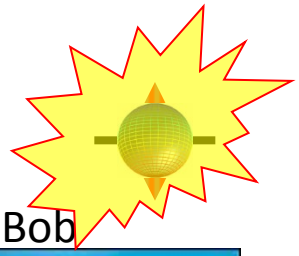
$$|\phi\rangle = a|\uparrow_1\rangle + b|\downarrow_1\rangle$$

$$|\Psi^-_{2,3}\rangle = \frac{1}{\sqrt{2}}\left(|\downarrow_2 \blacksquare\rangle - |\uparrow_2 \blacksquare\rangle\right)$$

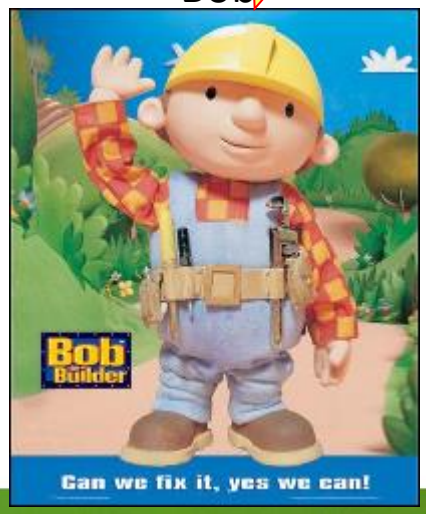
$$|\Psi^-_{2,3}\rangle = \frac{1}{\sqrt{2}}\left(|\blacksquare\uparrow_3\rangle - |\blacksquare\downarrow_3\rangle\right)$$



Alice



Bob

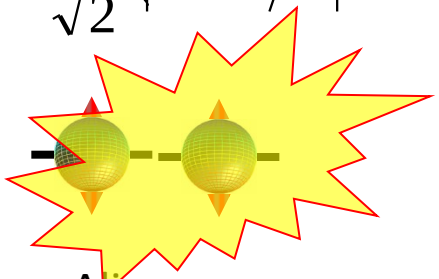


Kwantowa teleportacja

pufff...

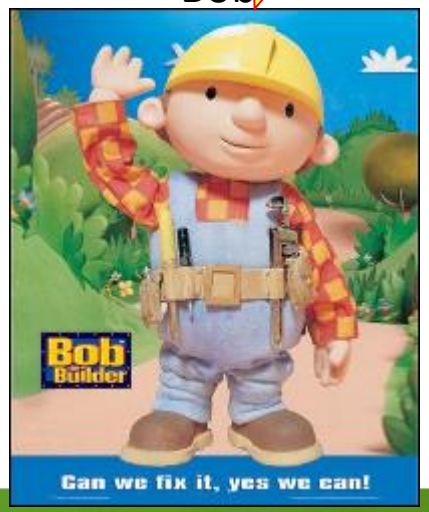
$$\left|\Psi_{2,1}^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow_2\uparrow_1\right\rangle - \left|\uparrow_2\downarrow_1\right\rangle\right)$$

$$\left|\phi\right\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\left(a\left|\uparrow_3\right\rangle + b\left|\downarrow_3\right\rangle\right)$$



Alice

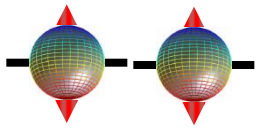
Bob



Kwantowa teleportacja

$$\left|\Psi_{2,1}^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow_2\uparrow_1\right\rangle - \left|\uparrow_2\downarrow_1\right\rangle\right)$$

$$\left|\phi\right\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\left(a\left|\uparrow_3\right\rangle + b\left|\downarrow_3\right\rangle\right)$$



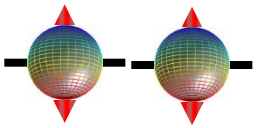
Alice

Bob

Kwantowa teleportacja

$$\left|\Psi^{-}_{2,1}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow_2\uparrow_1\right\rangle - \left|\uparrow_2\downarrow_1\right\rangle\right)$$

$$\left|\phi\right\rangle = a\left|\uparrow_3\right\rangle + b\left|\downarrow_3\right\rangle$$

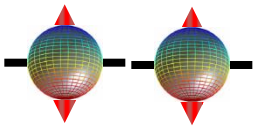


Alice

Bob

Kwantowa teleportacja

1. Przekazywana jest stan obiektu, a nie sam obiekt fizyczny.
2. Obiekt nie jest skopiowany (por. zasada Heisenberga, *zakaz klonowania*)
3. Informacja nie porusza się szybciej niż światło.
4. Trudności w pomiarze wszystkich czterech stanów Bella (wydajność).



Alice

Bob

Kwantowa teleportacja

Anton Zeilinger

Institute of Experimental Physics, University of Vienna,

Teleportacja stanów fotonowych

Nature, **390**, 575 (1997)

Experimental quantum teleportation

Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter & Anton Zeilinger

Institut für Experimentalphysik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria

Quantum teleportation—the transmission and reconstruction over arbitrary distances of the state of a quantum system—is demonstrated experimentally. During teleportation, an initial photon which carries the polarization that is to be transferred and one of a pair of entangled photons are subjected to a measurement such that the second photon of the entangled pair acquires the polarization of the initial photon. This latter photon can be arbitrarily far away from the initial one. Quantum teleportation will be a critical ingredient for quantum computation networks.

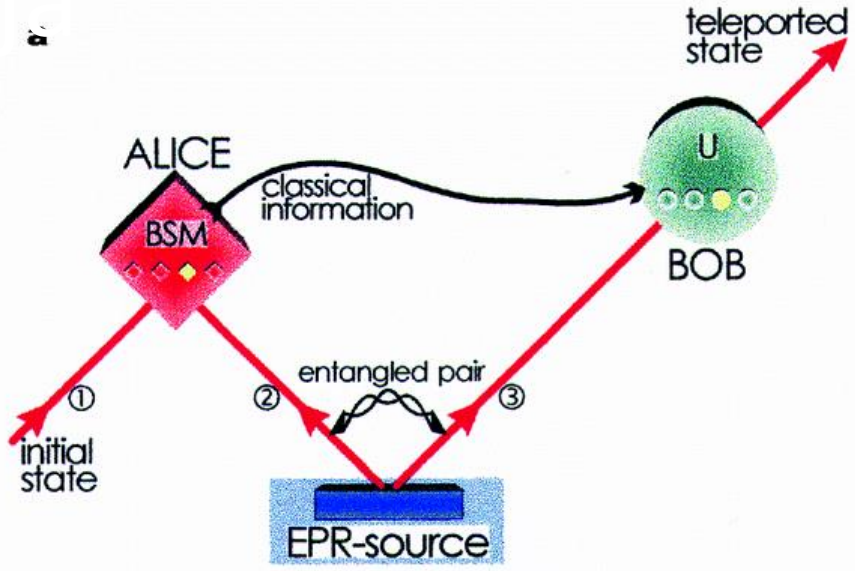
Kwantowa teleportacja

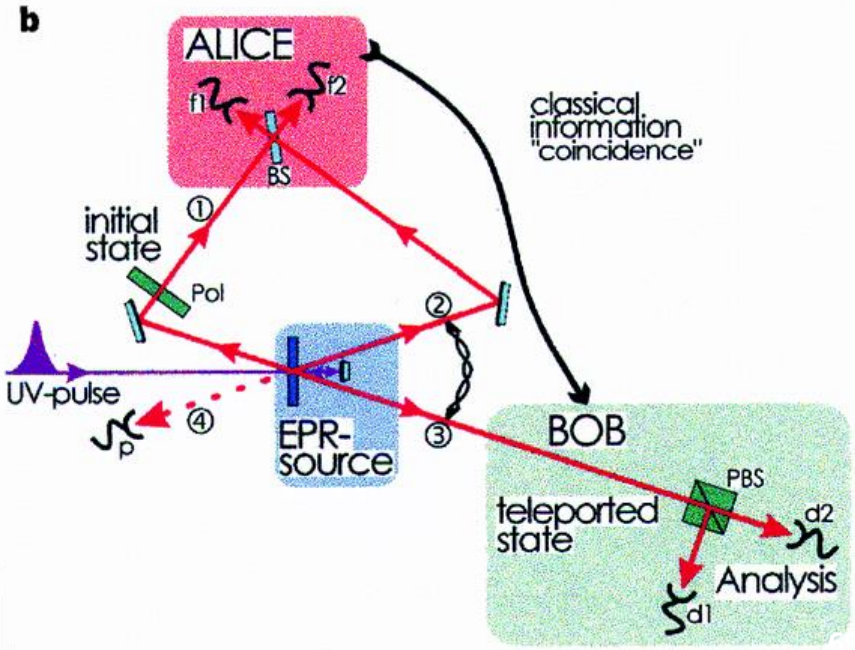
Anton Zeilinger

Institute of Experimental Physics, University of Vienna,

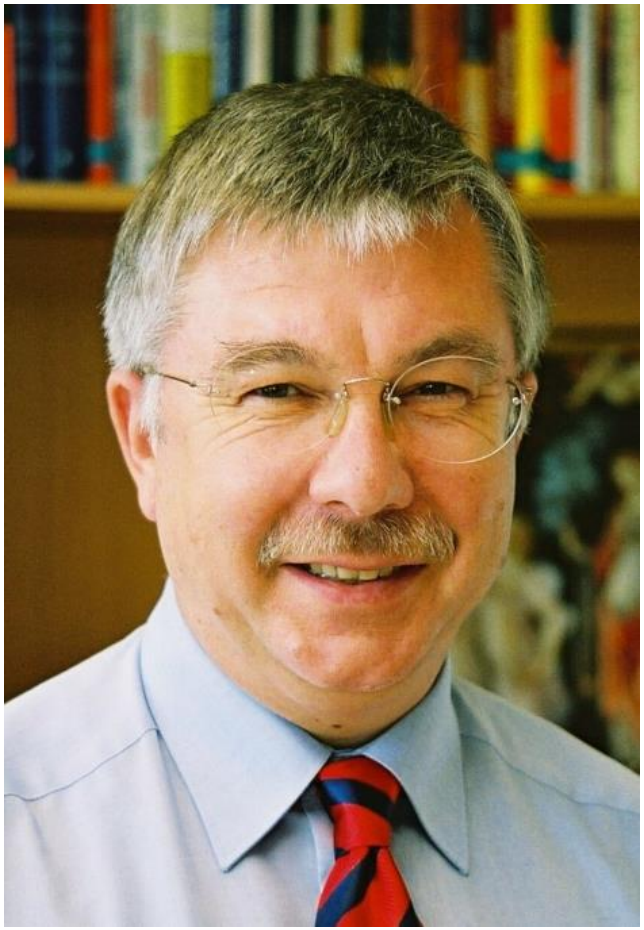
Teleportacja stanów fotonowych

Nature, **390**, 575 (1997)





Kwantowa teleportacja



Deterministic quantum teleportation with atoms

M. Riebe[1], H. Häffner[1], C. F. Roos[1], W. Hänsel[1], J. Benhelm[1], G. P. T. Lancaster[1], T. W. Körber[1], C. Becher[1], F. Schmidt-Kaler[1], D. F. V. James[2] & R. Blatt[1,3]

[1]*Institut für Experimentalphysik, Universität Innsbruck, Technikerstraße 25, A-6020 Innsbruck, Austria*
[2]*Theoretical Division T-4, Los Alamos National Laboratory, Los Alamos NM 87545, USA*
[3]*Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, Technikerstraße 25, A-6020 Innsbruck, Austria*

Teleportacja stanów kwantowych jonów $^{40}Ca^{+}$ w pułapce jonowej

Nature, **429**, 734 (2004)

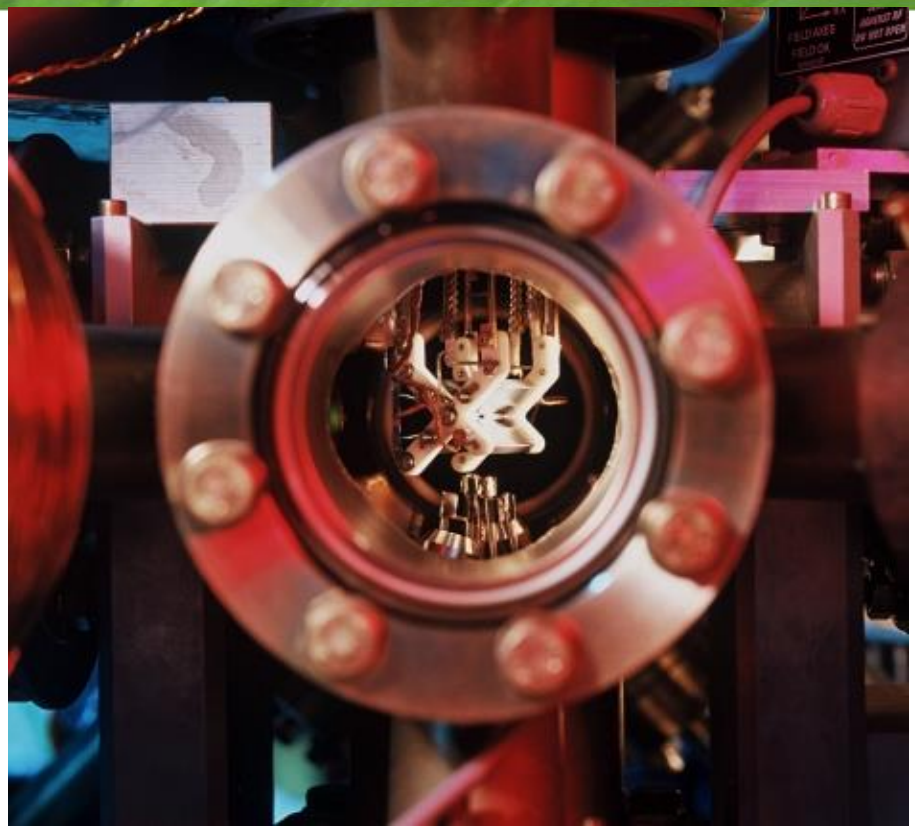
Reiner Blatt

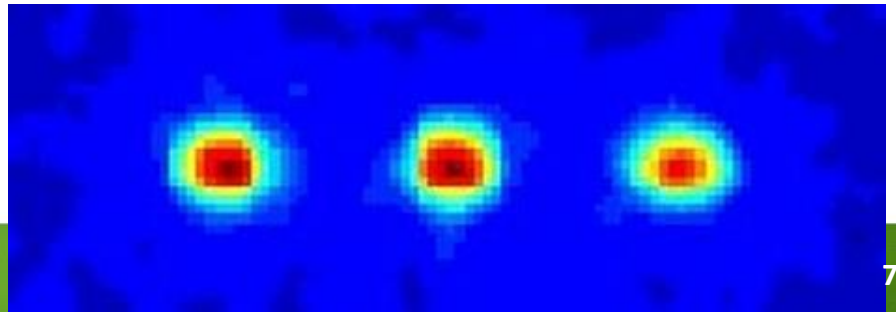
Institute of Experimental Physics, University of Insbruck,

Kwantowa teleportacja

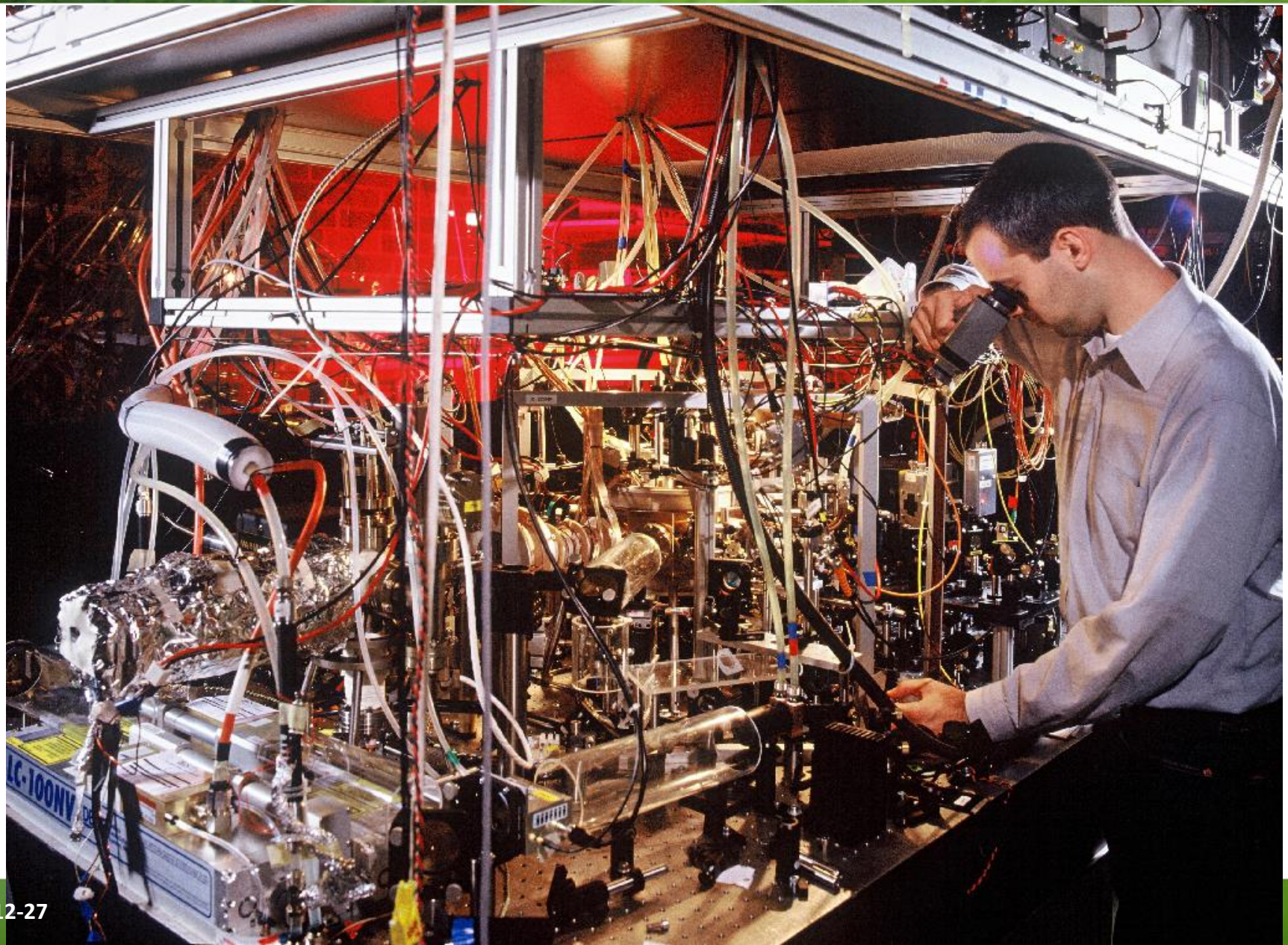
Table 1 **Pulse sequence of the teleportation protocol.**

	Action	Comment
1	Light at 397 nm	Doppler preparation
2	Light at 729 nm	Sideband cooling
3	Light at 397 nm	Optical pumping
Entangle		
4	$R_3^{+}(\pi/2,3\pi/2)$	Entangle ion 3 with motional qubit
5	$R_2^{C}(\pi,3\pi/2)$	Prepare ion 2 for entanglement
6	$R_2^{+}(\pi,\pi/2)$	Entangle ion 2 with ion 3
7	Wait for 1 μs – 10,000 μs	Standby for teleportation
8	$R_3^{H}(\pi,0)$	Hide target ion
9	$R_1^{C}(\vartheta_\chi,\varphi_\chi)$	Prepare source ion 1 in state χ
Rotate into Bell basis		
10	$R_2^{+}(\pi,3\pi/2)$	Get motional qubit from ion 2
11	$R_1^{+}(\pi/\sqrt{2},\pi/2)$	Composite pulse for phasegate
12	$R_1^{+}(\pi,0)$	Composite pulse for phasegate
13	$R_1^{+}(\pi/\sqrt{2},\pi/2)$	Composite pulse for phasegate
14	$R_1^{+}(\pi,0)$	Composite pulse for phasegate
15	$R_1^{C}(\pi,\pi/2)$	Spin echo on ion 1
16	$R_3^{H}(\pi,\pi)$	Unhide ion 3 for spin echo
17	$R_3^{C}(\pi,\pi/2)$	Spin echo on ion 3
18	$R_3^{H}(\pi,0)$	Hide ion 3 again
19	$R_2^{+}(\pi,\pi/2)$	Write motional qubit back to ion 2
20	$R_1^{C}(\pi/2,3\pi/2)$	Part of rotation into Bell basis
21	$R_2^{C}(\pi/2,\pi/2)$	Finalize rotation into Bell basis
Read out		
22	$R_2^{H}(\pi,0)$	Hide ion 2
23	PMDetection for 250 μs	Read out of ion 1 with photomultiplier
24	$R_1^{H}(\pi,0)$	Hide ion 1
25	$R_2^{H}(\pi,\pi)$	Unhide ion 2
26	PMDetection for 250 μs	Read out of ion 2 with photomultiplier
27	$R_2^{H}(\pi,0)$	Hide ion 2
28	Wait 300 μs	Let system rephase; part of spin echo
29	$R_3^{H}(\pi,\pi)$	Unhide ion 3
30	$R_3^{C}(\pi/2,3\pi/2+\phi)$	Change basis
Reconstruction		
31	$R_3^{C}(\pi,\phi)$	$\left.\begin{matrix} i\sigma_x \\ -i\sigma_y \end{matrix}\right\} = -i\sigma_z$ conditioned on PM detection 1
32	$R_3^{C}(\pi,\pi/2+\phi)$	
33	$R_3^{C}(\pi,\phi)$	$i\sigma_x$ conditioned on PM detection 2
34	$R_2^{C}(\vartheta_\chi,\varphi_\chi+\pi+\phi)$	Inverse of preparation of χ with offset ϕ
35	Light at 397 nm	Read out of ion 3 with camera

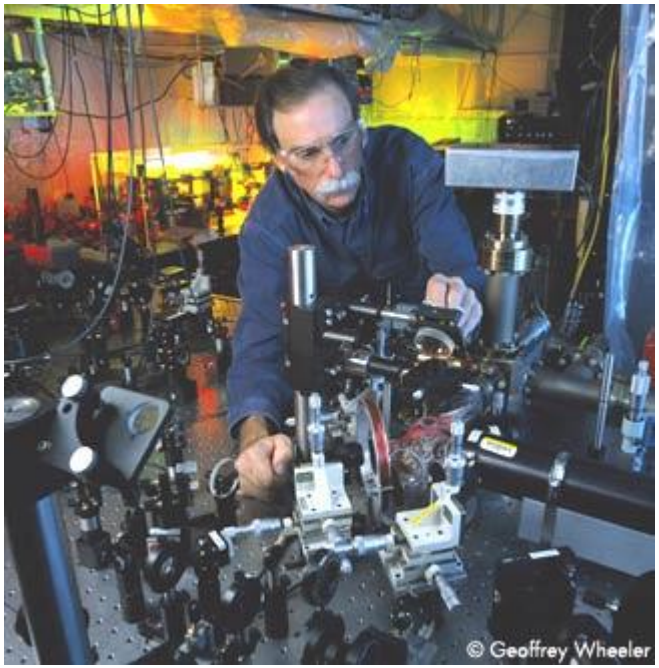




Maszyna do teleportacji



Kwantowa teleportacja



David Wineland
National Institute of Standards and Technology

Deterministic quantum teleportation of atomic qubits

M. D. Barrett[1]*, J. Chiaverini[1], T. Schaetz[1], J. Britton[1], W. M. Itano[1], J. D. Jost[1], E. Knill[2], C. Langer[1], D. Leibfried[1], R. Ozeri[1] & D. J. Wineland[1]

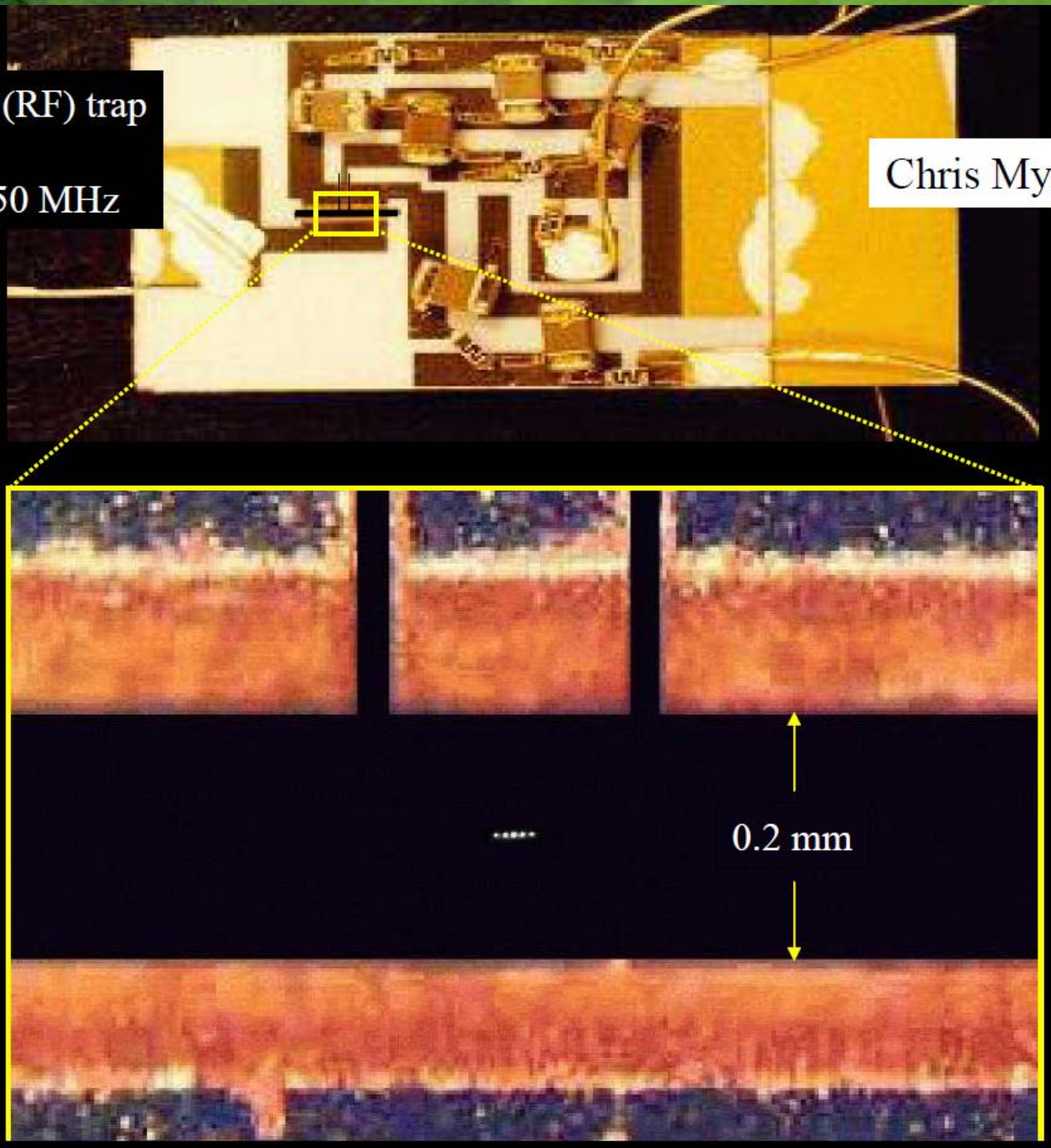
[1]*Time and Frequency Division, NIST, Boulder, Colorado 80305, USA*
[2]*Mathematical and Computational Sciences Division, NIST, Boulder, Colorado 80305, USA*

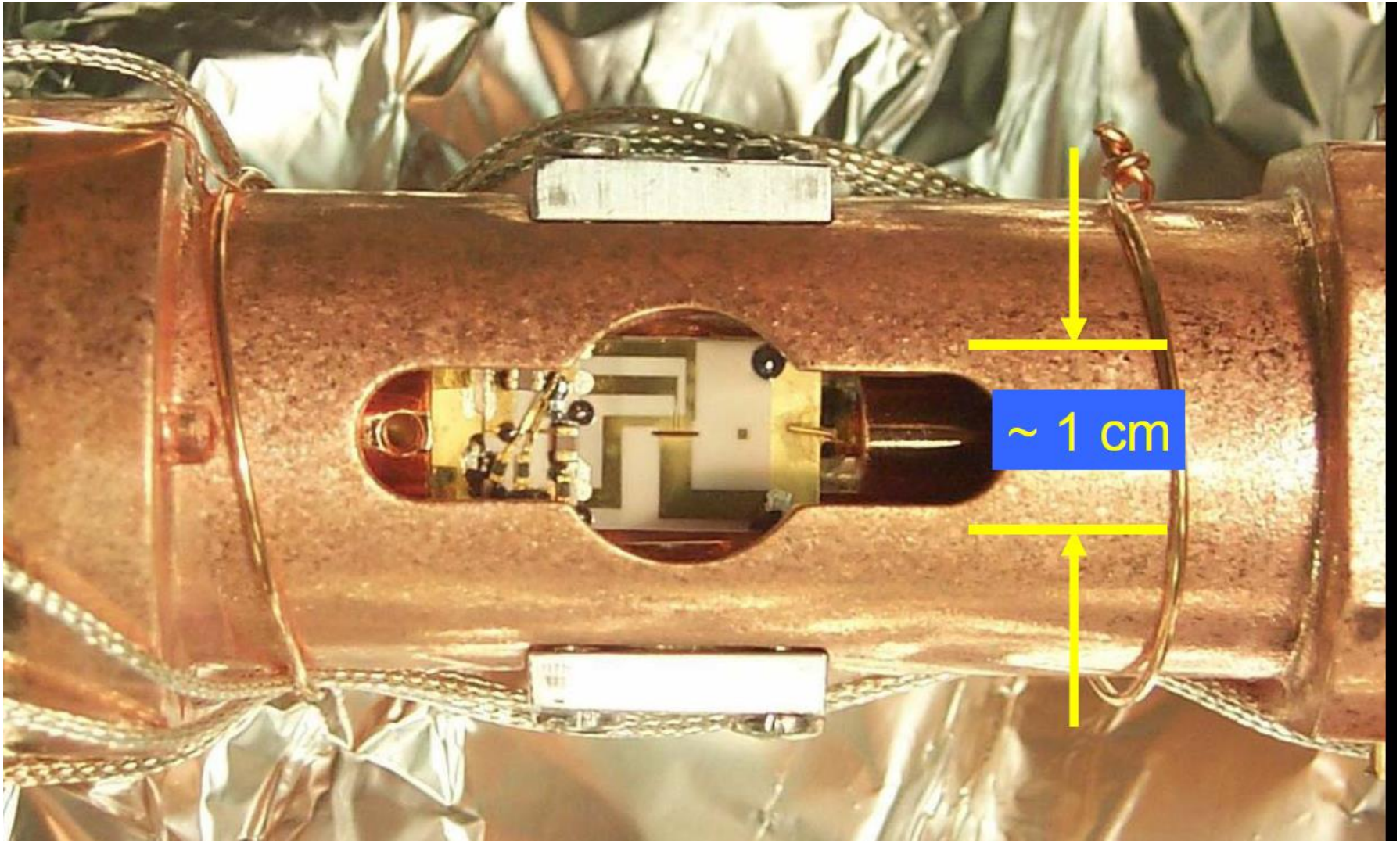
* Present address: Department of Physics, University of Otago, PO Box 56, Dunedin, New Zealand

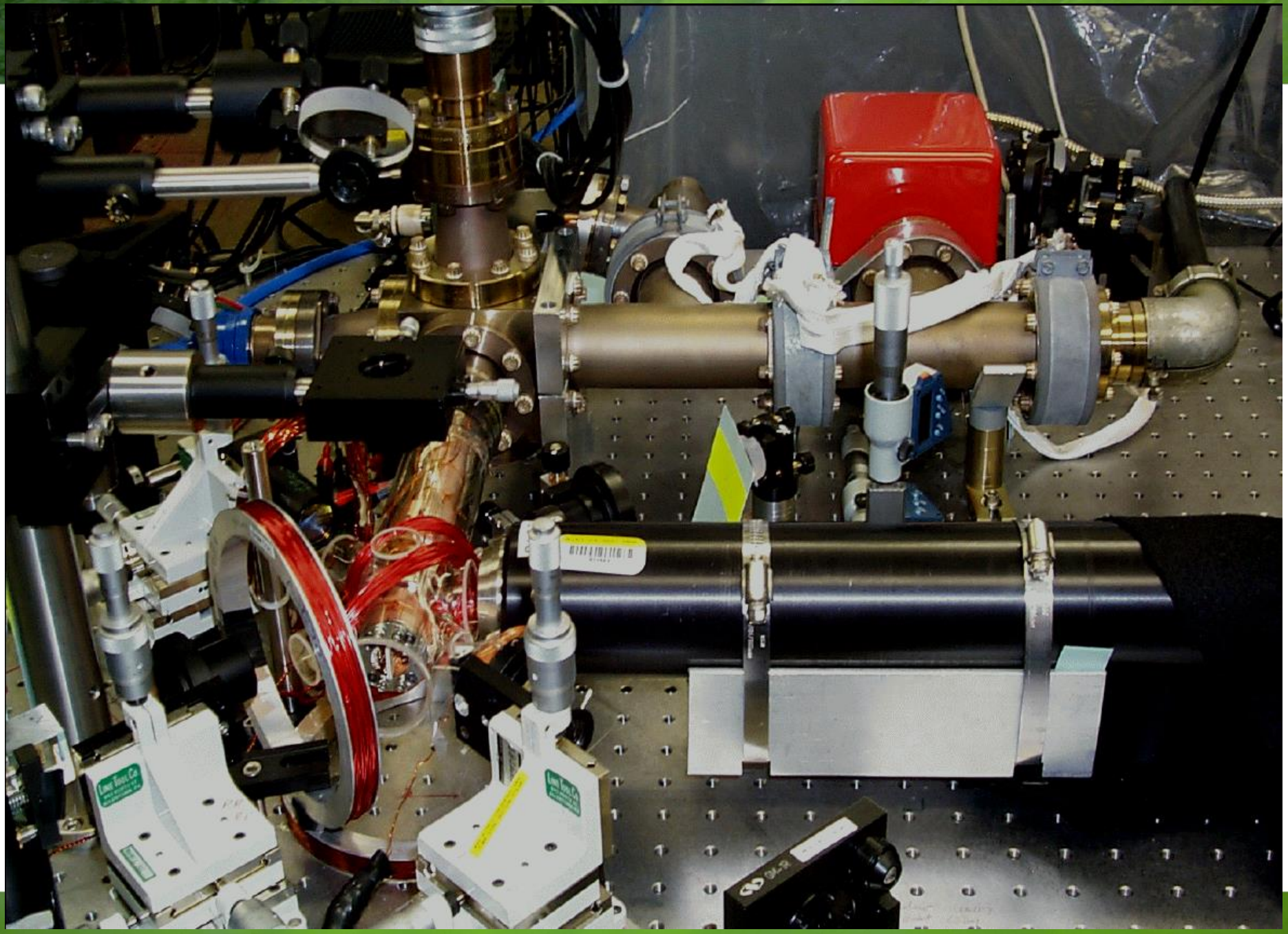
Teleportacja stanów kwantowych jonów $^{9}Be^{+}$ w pułapce jonowej

Nature, **429**, 737 (2004)

"linear" Paul (RF) trap
V_{RF} ~ 500 V
Ω_{RF} ~ 50 – 250 MHz




~ 1 cm



Kwantowa teleportacja

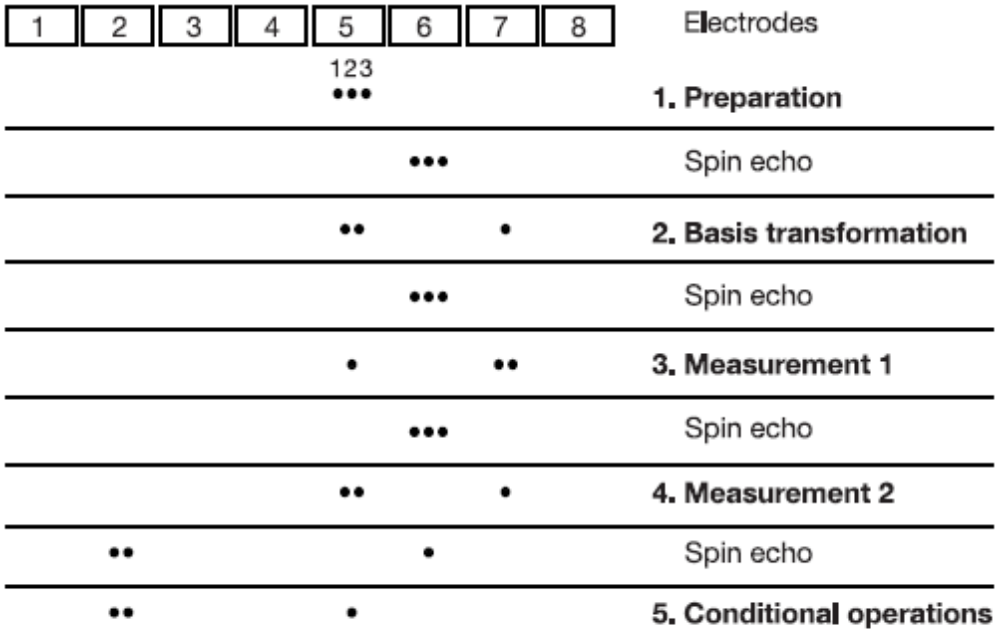
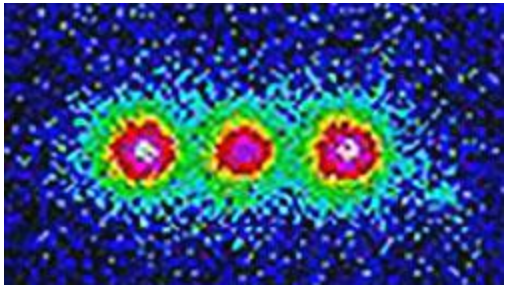


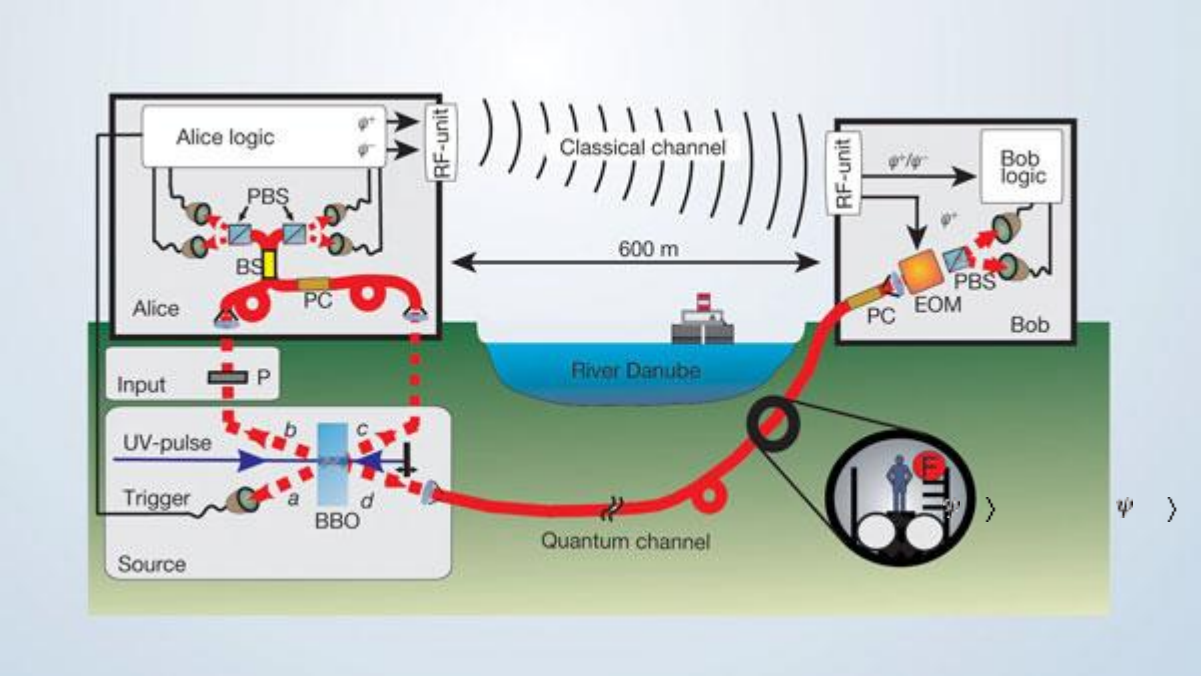
Figure 1 Schematic representation of the teleportation protocol. The ions are numbered left to right, as indicated at the top, and retain their order throughout. Positions, relative to the electrodes, are shown at each step in the protocol. The widths of the electrodes vary, with the width of the separation electrode (6) being the smallest at 100 μm. The spacing between ions in the same trap is about 3 μm, and laser-beam spot sizes (in traps 5 and 6) at the position of the ions are approximately 30 μm. In step 1 we prepare the outer ions in an entangled (singlet) state and the middle ion in an arbitrary state (equation (1)). Steps 2–4 constitute a measurement in a Bell-basis for ions 1 and 2 (Alice's qubits), teleporting the state of ion 2 onto ion 3 (Bob's qubit), up to unitary operations that depend on the measurement outcomes. In step 5 we invoke these conditional operations, recovering the initial state. Interspersed are spin-echo pulses applied in trap 6 that protect the state from de-phasing due to fluctuating magnetic fields but do not affect the teleportation protocol.



This colorized image shows the fluorescence from three trapped beryllium ions illuminated with an ultraviolet laser beam. Credit: NIST

Kwantowa teleportacja

Rupert Ursin, Thomas Jennewein, Markus Aspelmeyer, Rainer Kaltenbaek, Michael Lindenthal, Philip Walther and Anton Zeilinger Nature **430**, 849 (19 August 2004)



800 m

The quantum channel (fibre F) rests in a sewage-pipe tunnel below the river in Vienna, while the classical microwave channel passes above it. A pulsed laser (wavelength, 394 nm; rate, 76 MHz) is used to pump a - barium borate (BBO) crystal that generates the entangled photon pair *c* and *d* and photons *a* and *b* (wavelength, 788 nm) by spontaneous parametric down-conversion. The state of photon *b* after passage through polarizer P is the teleportation input; *a* serves as the trigger. Photons *b* and *c* are guided into a single-mode optical-fibre beam splitter (BS) connected to polarizing beam splitters (PBS) for Bell-state measurement. Polarization rotation in the fibres is corrected by polarization controllers (PC) before each run of measurements. The logic electronics identify the Bell state as either $|\Psi^-\rangle_{bc}$ or $|\Psi^+\rangle_{bc}$ and convey the result through the microwave channel (RF unit) to Bob's electro-optic modulator (EOM) to transform photon *d* into the input state of photon *b*.

Quantum Teleporation: The Math

Three qubit joint state of Alice, Bob, and "Victor" who prepared $|\psi\rangle$:

$$|\chi\rangle = |\psi\rangle_V \otimes |\Phi^{(+)}\rangle_{AB} = (\alpha|0\rangle_V + \beta|1\rangle_V) \otimes (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$$

$$= \frac{1}{2}\Big[(|0\rangle_V \otimes |0\rangle_A + |1\rangle_V \otimes |1\rangle_A) \otimes (\alpha|0\rangle_B + \beta|1\rangle_B) + (|0\rangle_V \otimes |0\rangle_A - |1\rangle_V \otimes |1\rangle_A) \otimes (\alpha|0\rangle_B - \beta|1\rangle_B)$$

$$+ (|0\rangle_V \otimes |1\rangle_A + |1\rangle_V \otimes |0\rangle_A) \otimes (\alpha|1\rangle_B + \beta|0\rangle_B) + (|0\rangle_V \otimes |1\rangle_A - |1\rangle_V \otimes |0\rangle_A) \otimes (\alpha|1\rangle_B - \beta|0\rangle_B)\Big]$$

$$|\chi\rangle = \frac{1}{2}\left(|\Phi^{(+)}\rangle_{VA} \otimes |\psi\rangle_B + |\Phi^{(-)}\rangle_{VA} \otimes Z|\psi\rangle_B + |\Psi^{(+)}\rangle_{VA} \otimes X|\psi\rangle_B - i|\Psi^{(-)}\rangle_{VA} \otimes Y|\psi\rangle_B\right)$$

A measurement by Alice in Bell-basis leaves Bob's qubit in one of four states:

$$\left\{|\psi\rangle_B,\ Z|\psi\rangle_B,\ X|\psi\rangle_B,\ Y|\psi\rangle_B\right\}$$

Alice uses the classical channel to tell Bob which Bell state she found.
Bob can then put his qubit in the unknown state, through application of a Pauli.

Kwantowa teleportacja

VOLUME 88, NUMBER 1 PHYSICAL REVIEW LETTERS 7 JANUARY 2002

Experimental Nonlocality Proof of Quantum Teleportation and Entanglement Swapping

Thomas Jennewein, Gregor Weihs, Jian-Wei Pan, and Anton Zeilinger
Institut für Experimentalphysik, Universität Wien Boltzmanngasse 5, 1090 Wien, Austria
(Received 15 August 2001; published 18 December 2001)

Quantum teleportation strikingly underlines the peculiar features of the quantum world. We present an experimental proof of its quantum nature, teleporting an entangled photon with such high quality that the nonlocal quantum correlations with its original partner photon are preserved. This procedure is also known as entanglement swapping. The nonlocality is confirmed by observing a violation of Bell's inequality by 4.5 standard deviations. Thus, by demonstrating quantum nonlocality for photons that never interacted, our results directly confirm the quantum nature of teleportation.

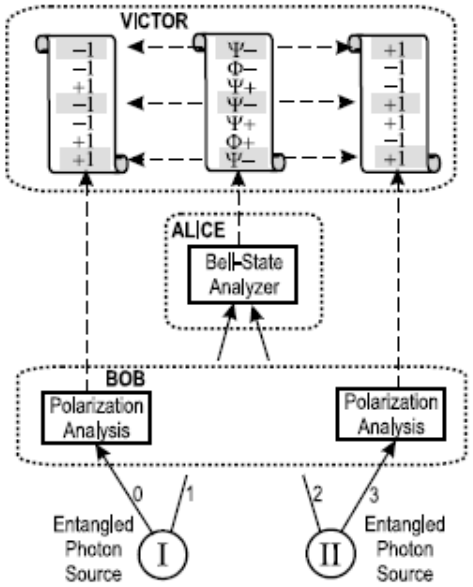


FIG. 1. Entanglement swapping version of quantum teleportation. Two entangled pairs of photons 0–1 and 2–3 are produced in the sources I and II, respectively. One photon from each pair is sent to Alice who subjects them to a Bell-state measurement, projecting them randomly into one of four possible entangled states. Alice records the outcome and hands it to Victor. This

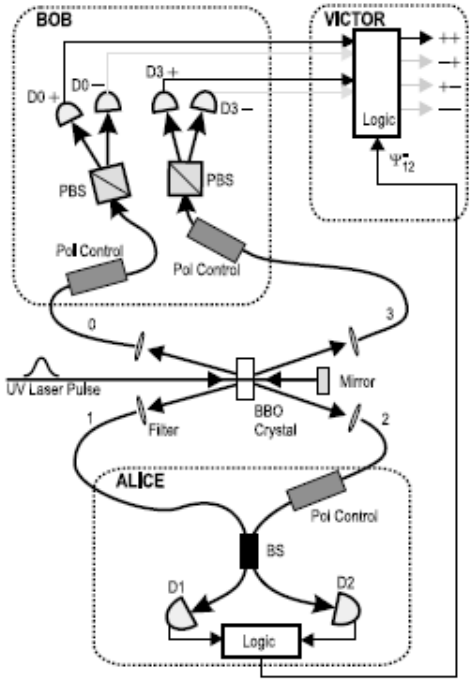


FIG. 2. Setup of the experiment. The two entangled photon pairs were produced by down-conversion in barium bo-

Kwantowa teleportacja

VOLUME 88, NUMBER 1 PHYSICAL REVIEW LETTERS 7 JANUARY 2002

Experimental Nonlocality Proof of Quantum Teleportation and Entanglement Swapping

Thomas Jennewein, Gregor Weihs, Jian-Wei Pan, and Anton Zeilinger
Institut für Experimentalphysik, Universität Wien Boltzmanngasse 5, 1090 Wien, Austria
(Received 15 August 2001; published 18 December 2001)

Quantum teleportation strikingly underlines the peculiar features of the quantum world. We present an experimental proof of its quantum nature, teleporting an entangled photon with such high quality that the nonlocal quantum correlations with its original partner
also known as entanglement swapping. The nonlocality is cont
inequality by 4.5 standard deviations. Thus, by demonstratin
never interacted, our results directly confirm the quantum natu

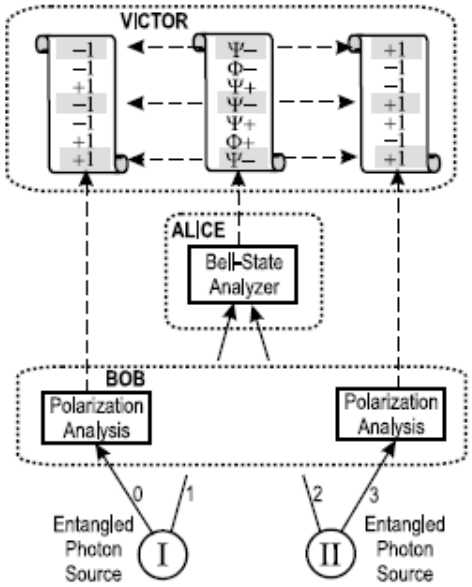


FIG. 1. Entanglement swapping version of quantum teleportation. Two entangled pairs of photons 0–1 and 2–3 are produced in the sources I and II, respectively. One photon from each pair is sent to Alice who subjects them to a Bell-state measurement, projecting them randomly into one of four possible entangled states. Alice records the outcome and hands it to Victor. This

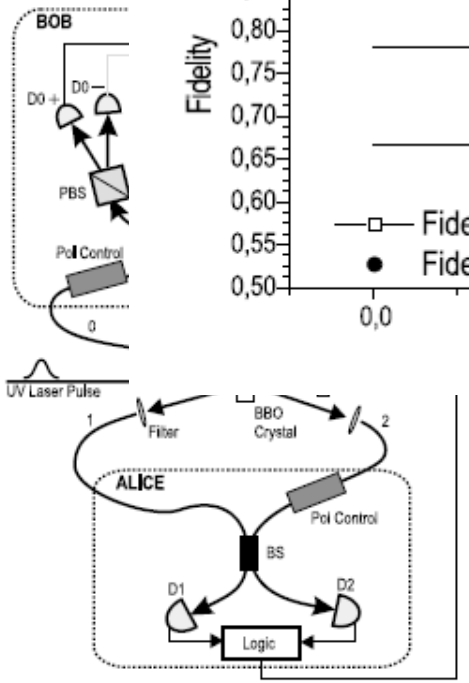
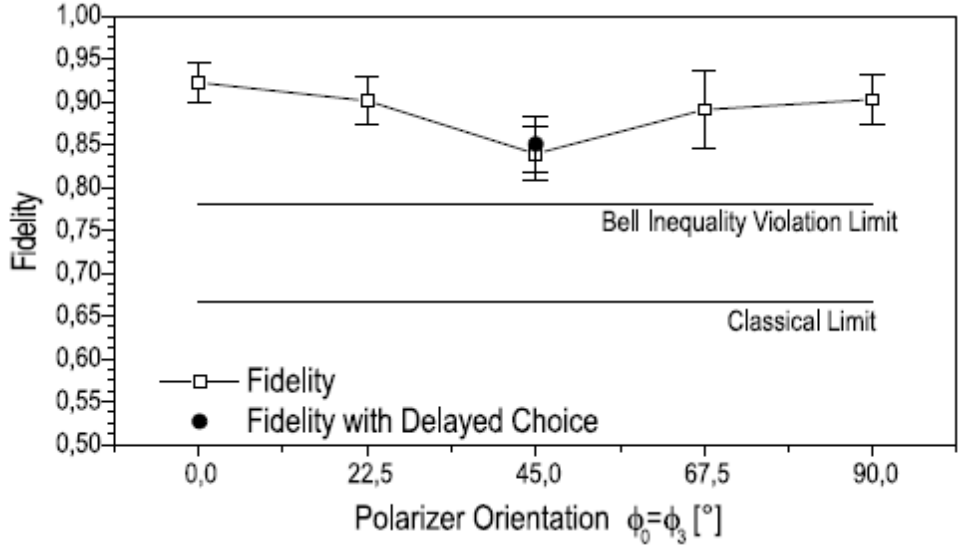
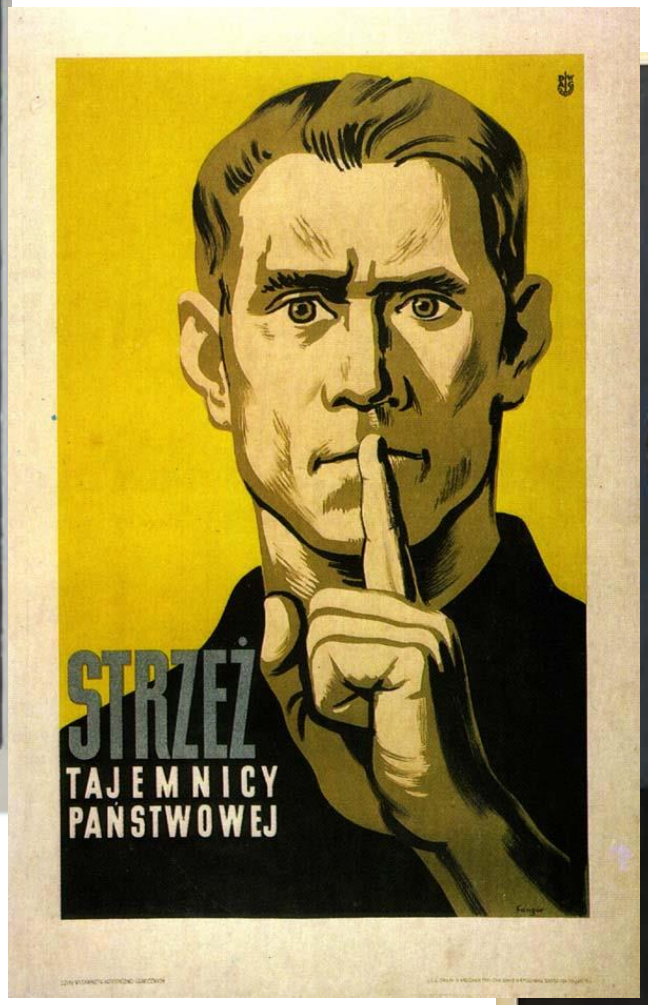


FIG. 2. Setup of the experiment. The two entangled photon pairs were produced by down-conversion in barium bo-



Sprawność 40%

Kryptografia Kwantowa



Kryptografia Kwantowa

- http://zon8.physd.amu.edu.pl/~tanas/

1.4 Proste szyfry

Szyfr Cezara

szyfr podstawieniowy monoalfabetyczny

A B C D E F G H I J K L M N O P R S T U V W X Y Z
D E F G H I J K L M N O P R S T U V W X Y Z A B C

tekst jawny $\longrightarrow$ K R Y P T O G R A F I A
kryptogram $\longrightarrow$ N U B T W S J U D I L D

- http://zon8.physd.amu.edu.pl/~tanas/

Kryptografia Kwantowa

- http://zon8.physd.amu.edu.pl/~tanas/

Szyfr Vigenère'a

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y

klucz $\longrightarrow$ S Z Y M P A N S S Z Y M

tekst $\longrightarrow$ K R Y P T O G R A F I A

krypt. $\longrightarrow$ C P W C I O U I S E G M

Kryptografia Kwantowa

Szyfr Vernama (one-time pad)

tekst jawny	⟶	S	Z	Y	F	R
binarnie	⟶	01010011	01011010	01011001	01000110	01010010
klucz	⟶	01110010	01010101	11011100	10110011	00101011
kryptogram	⟶	00100001	00001111	10000101	11110101	01111001

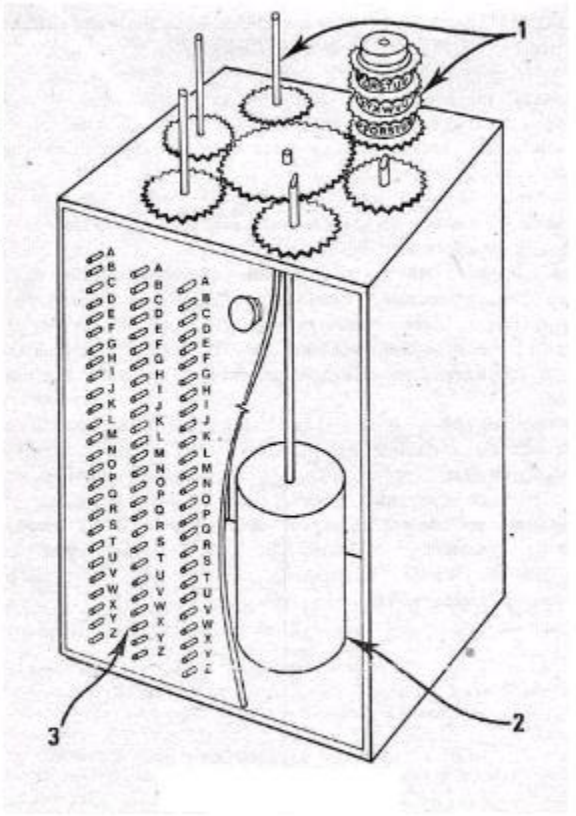
- Klucz jest losowym ciągiem bitów.
- Kryptogram jest także losowym ciągiem bitów i jeśli nie znamy klucza to nie dowiemy się niczego o tekście jawnym.
- Jeśli klucz jest tak długi jak wiadomość i użyty tylko raz, to szyfr ten gwarantuje bezpieczeństwo absolutne.
- Współczesne metody kryptograficzne sprowadzają się do obliczeń w systemie binarnym, czyli operacji na bitach.

Kryptografia Kwantowa

Jerzy Różycki

Marian Rejewski

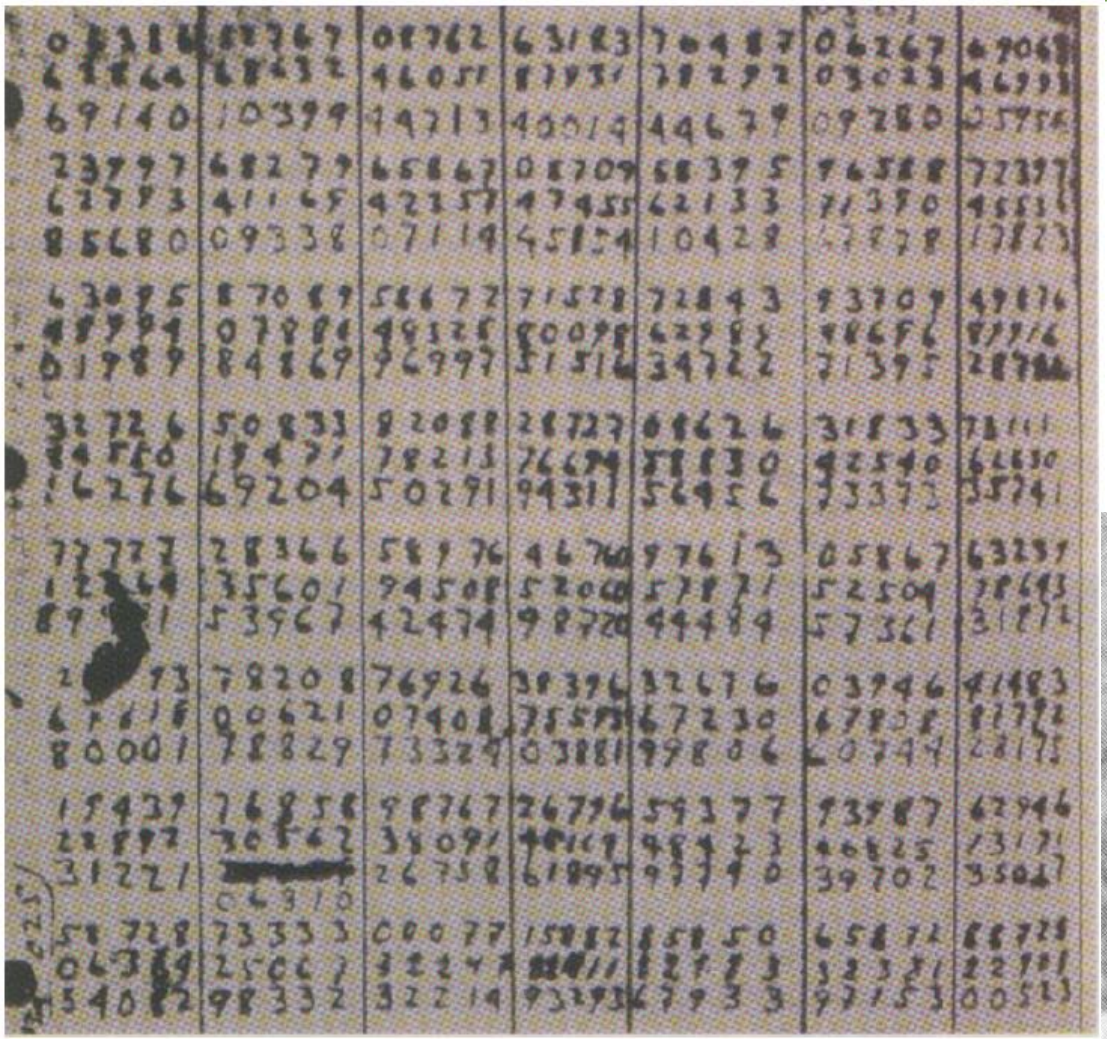
Henryk Zygalski



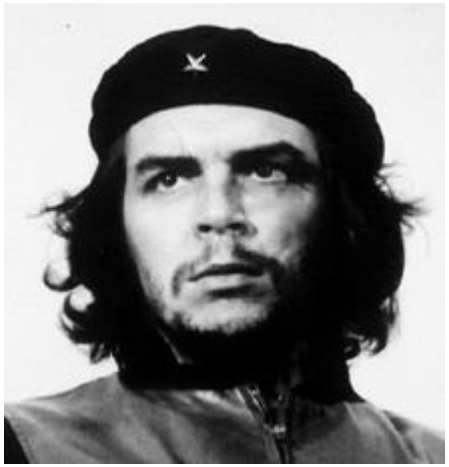
Enigma 1918/1923

images from http://www.armyradio.com/publish/Articles/The_Enigma_Code_Breach/

Szyfry nie do złamania

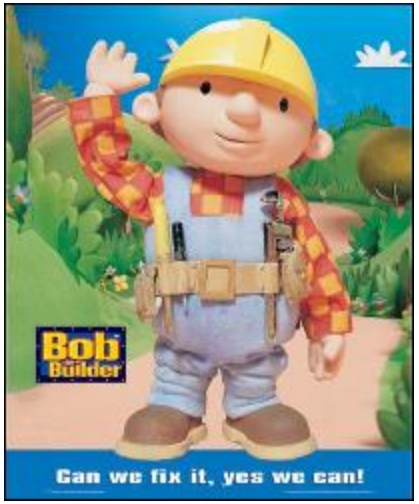


Klucze jednorazowe – nie do złamania!



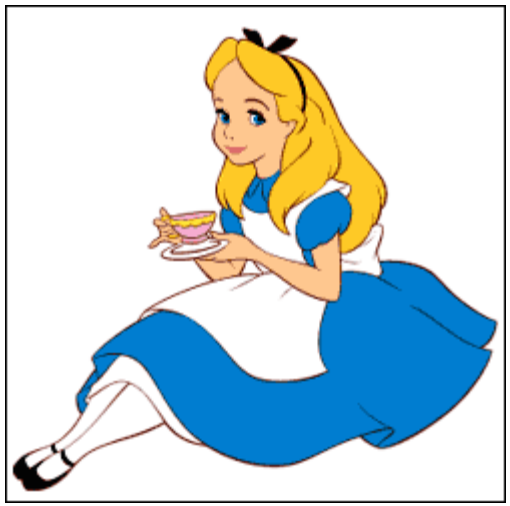
Kryptografia

Alice

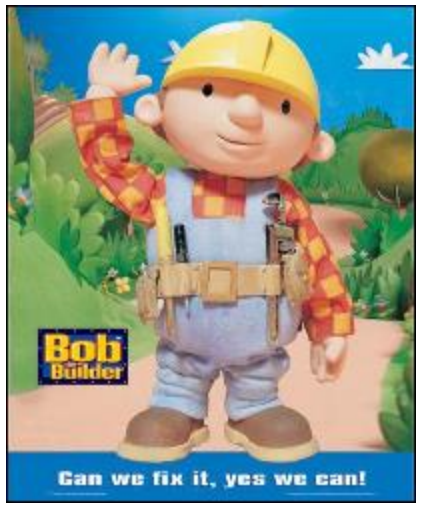


Bob

Kryptografia



Alice

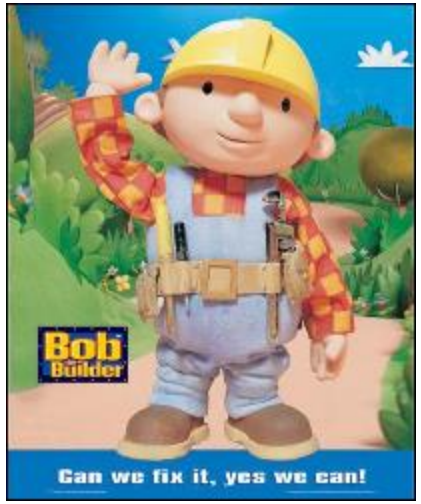


Bob

Eve (eavesdropper)

Kryptografia

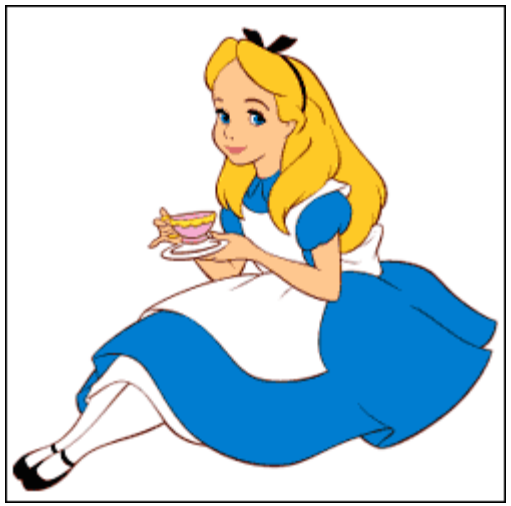
Alice



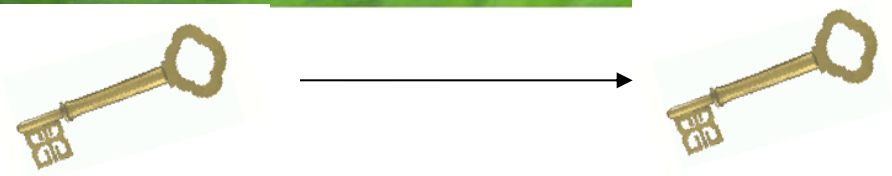
Bob

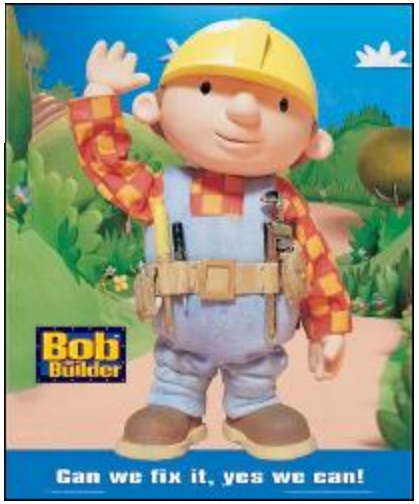
Eve

Kryptografia



Alice



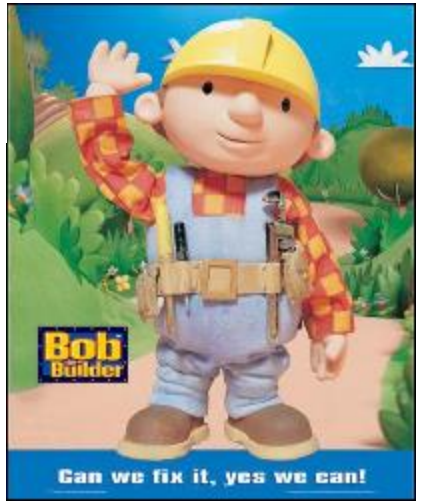


Bob

Eve

Kryptografia

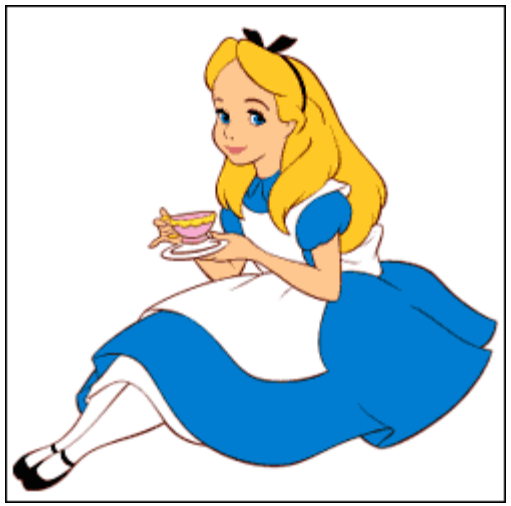
Alice



Bob

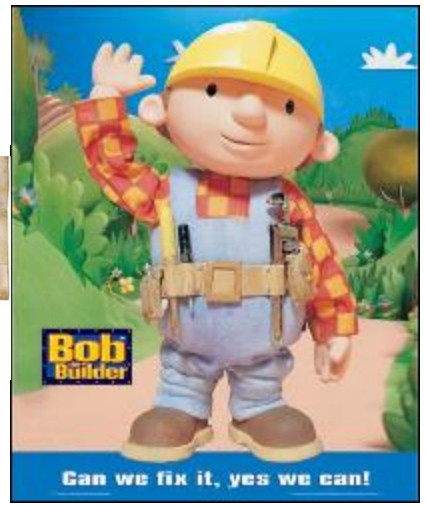
Eve

Kryptografia



Alice

Aby mieć bezpieczny kanał łączności trzeba mieć bezpieczny kanał łączności...

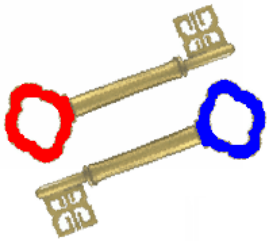


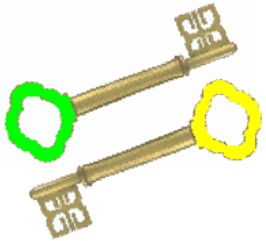
Bob

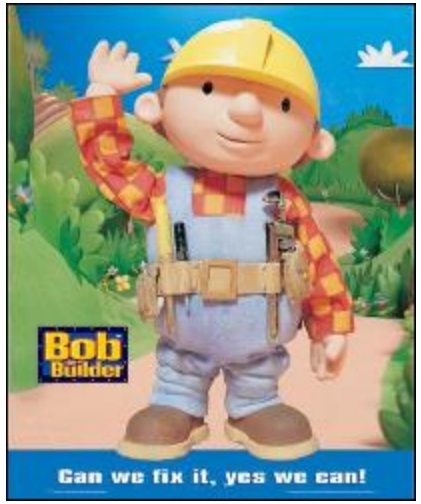
Eve

Kryptografia klucza publicznego

Alice

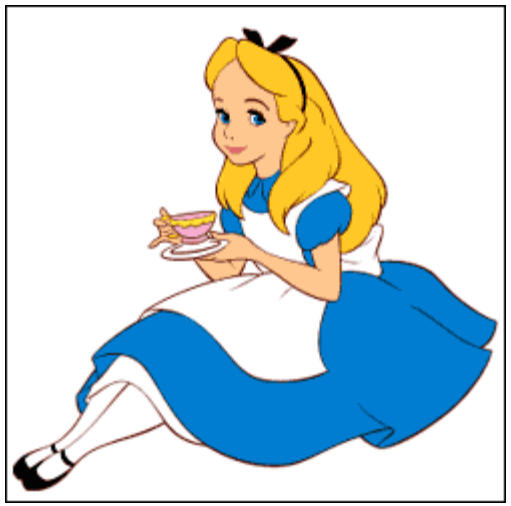




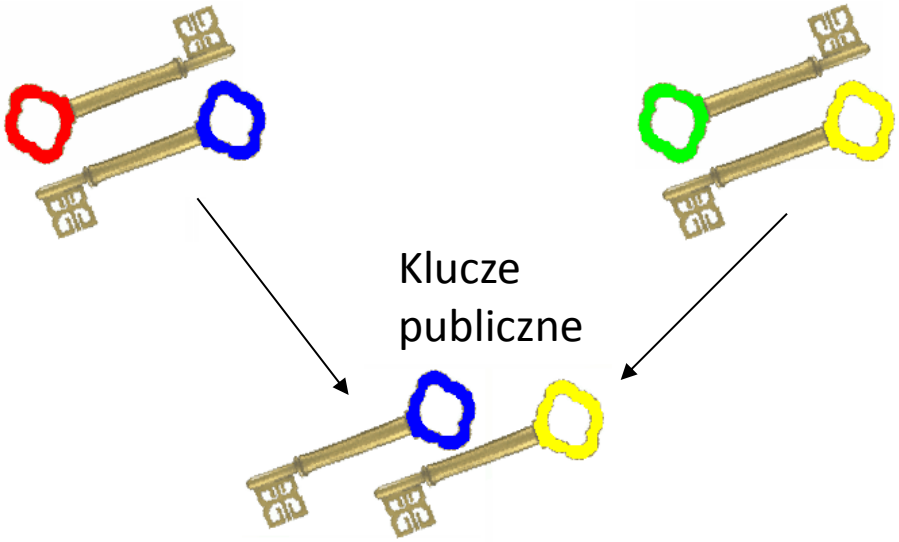


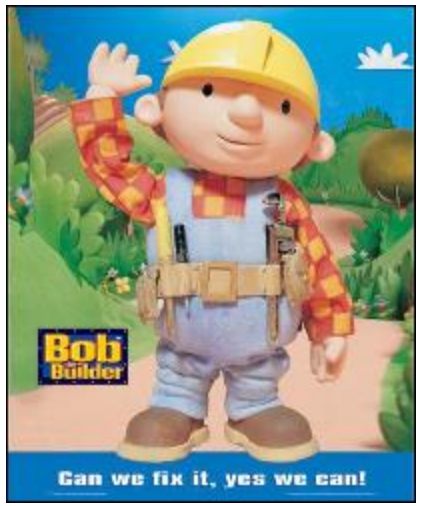
Bob

Kryptografia klucza publicznego



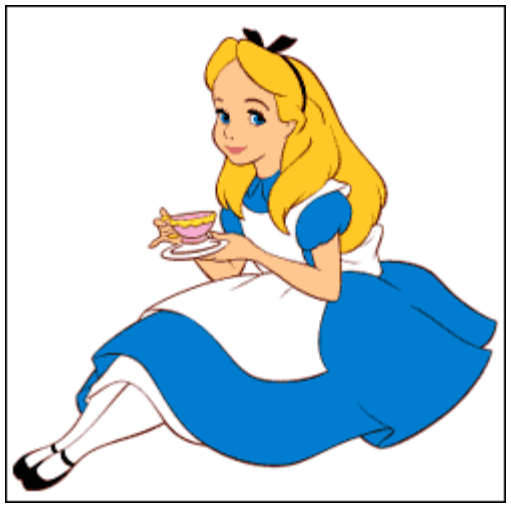
Alice



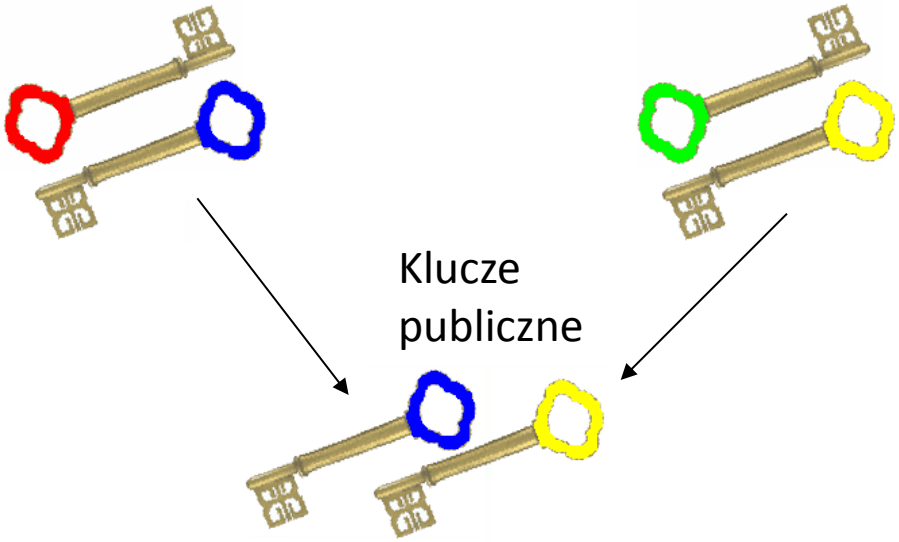


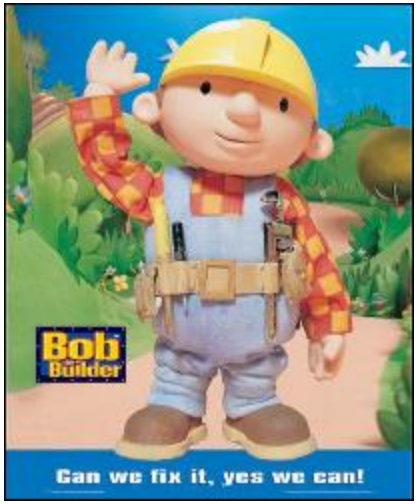
Bob

Kryptografia klucza publicznego



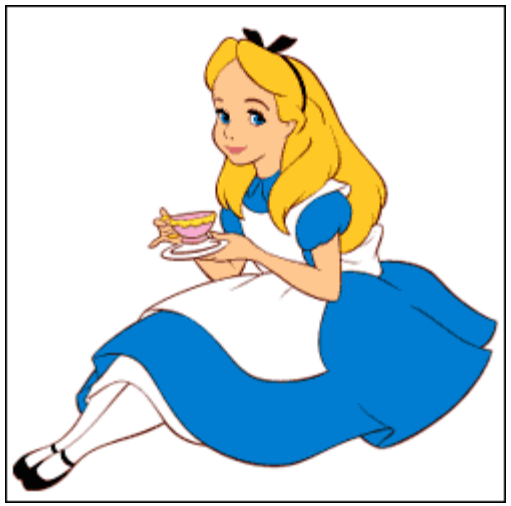
Alice



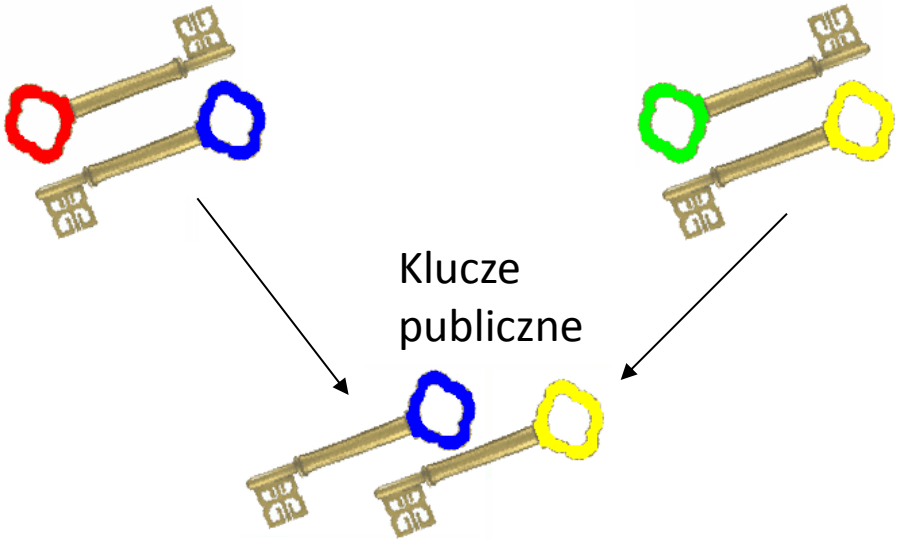


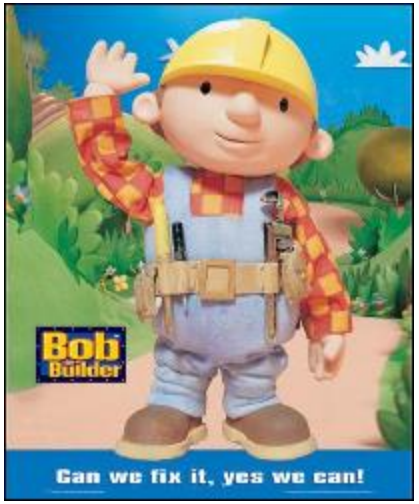
Bob

Kryptografia klucza publicznego

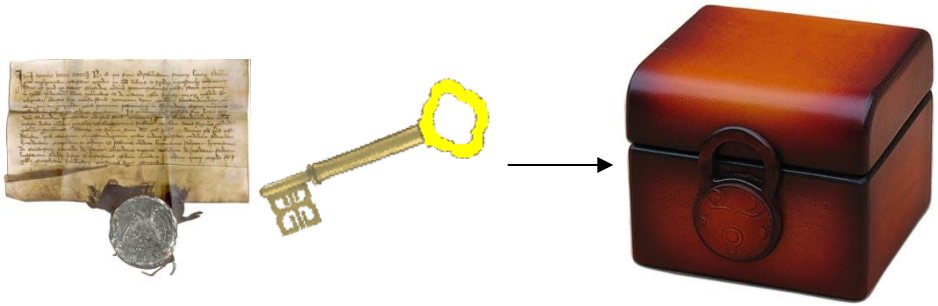


Alice

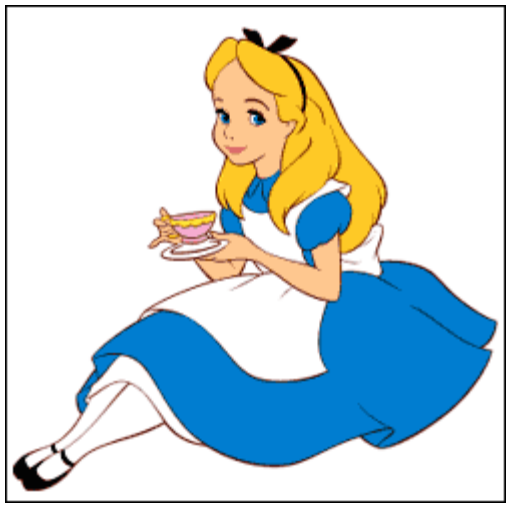




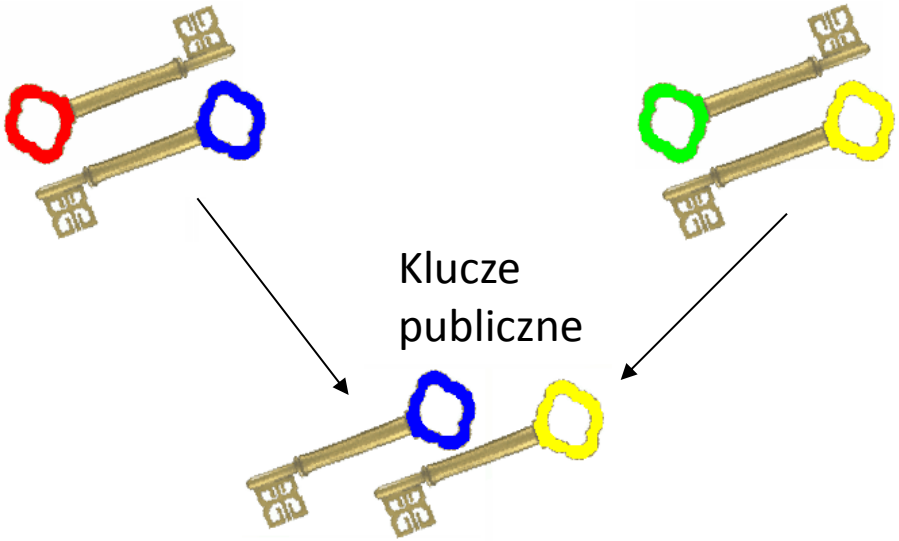
Bob

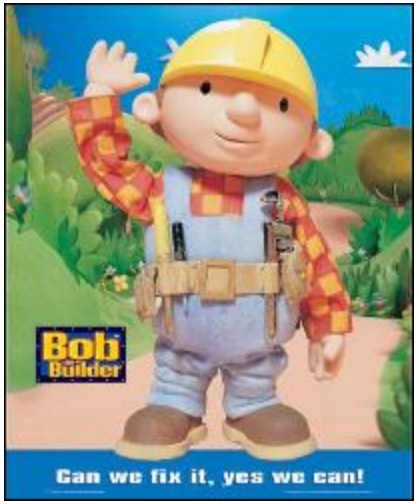


Kryptografia klucza publicznego

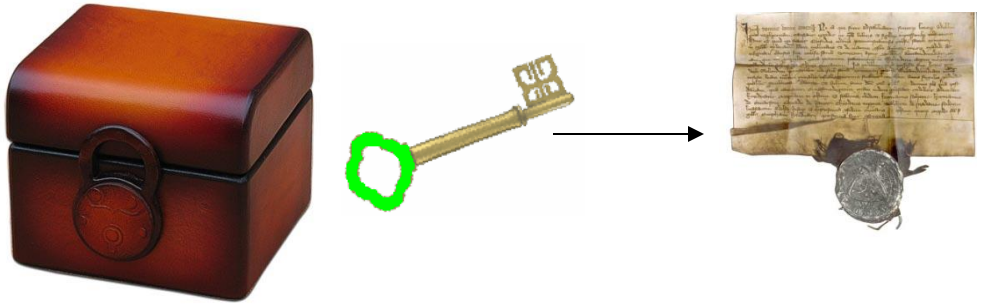


Alice

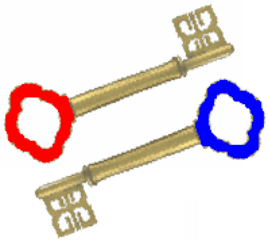
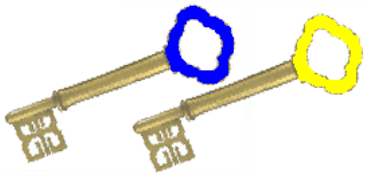


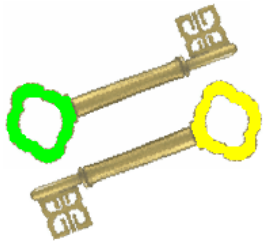


Bob



Kryptografia klucza publicznego

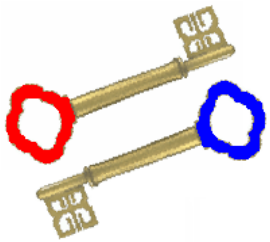
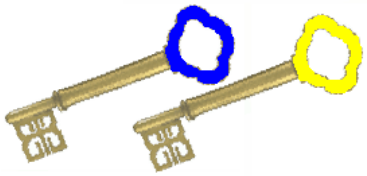



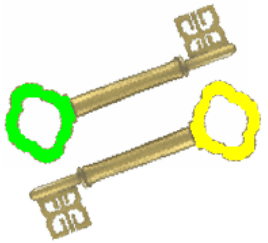
•Bezpieczenstwo systemu kryptograficznego z kluczem publicznym jest oparte na istnieniu funkcji jednostronnych, dla których znalezienie wartosci samej funkcji jest łatwe zas znalezienie argumentu funkcji kiedy znamy jej wartosc jest obliczeniowo trudne (jak trudne to zalezy od aktualnego stanu wiedzy i rozwoju techniki)

•Najbardziej znany kryptosystem z kluczem publicznym, RSA, opiera sie na trudnosci z rozkładem liczby na czynniki (faktoryzacja)

•Systemy takie nie gwarantuja pełnego bezpieczenstwa. Nie mozna wykluczyc, ze ktoś znajdzie efektywny algorytm faktoryzacji liczb.
W istocie taki algorytm juz istnieje. Jest to algorytm Shora! Wymaga on jednak komputera kwantowego!.

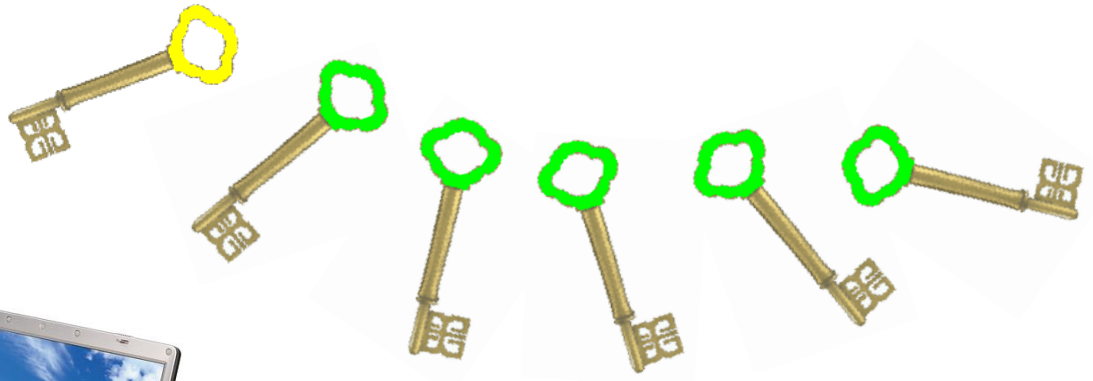
Kryptografia klucza publicznego

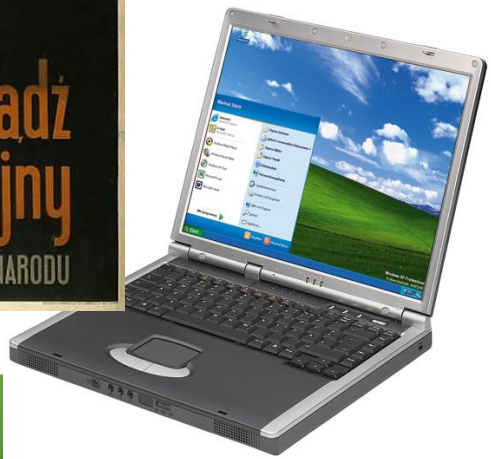



W 1994 r. RSA 129 został złamany na 1600 stacjach roboczych w ciagu 8 miesiecy

Eve





Kryptografia kwantowa

Wielokrotna i bezpieczna procedura uzgadniania klucza jednorazowego

http://wug.physics.uiuc.edu/courses/phys214/fall04/

Kryptografia kwantowa

Charles Bennett

Gilles Brassard

Wielokrotna i bezpieczna procedura uzgadniania klucza jednorazowego

QUANTUM CRYPTOGRAPHY: PUBLIC KEY DISTRIBUTION AND COIN TOSSING

Charles H. Bennett (IBM Research, Yorktown Heights NY 10598 USA)
Gilles Brassard (dept. IRO, Univ. de Montreal, H3C 3J7 Canada)

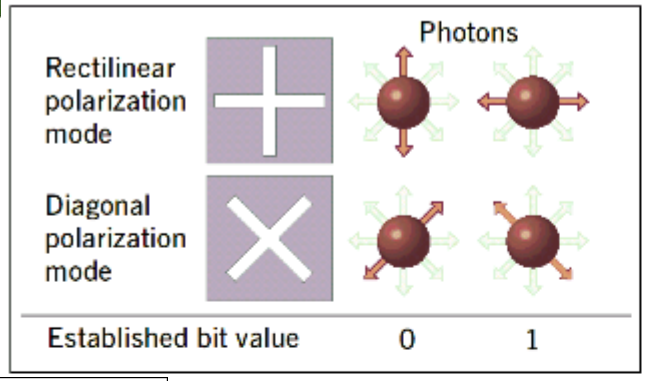
International Conference on Computers, Systems & Signal Processing Bangalore, India December 10-12, 1984

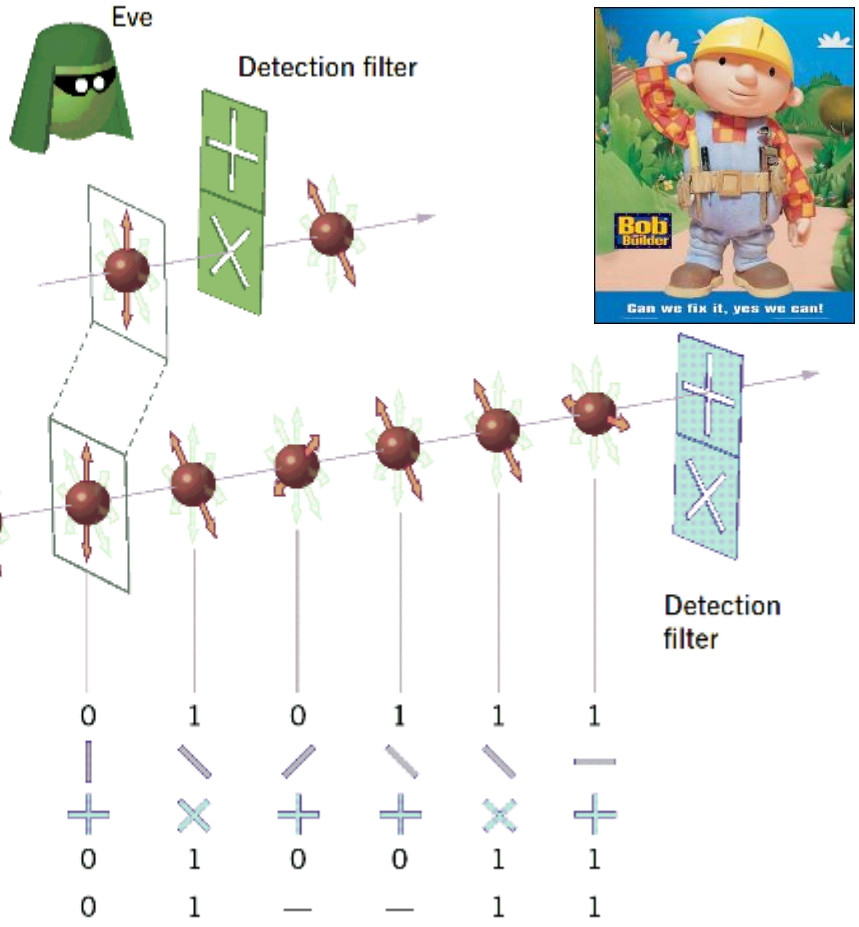
When elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomena unachieveable with traditional transmission media, e.g. a communications channel on which it is impossible in principle to eavesdrop without a high probability of disturbing the transmission in such a way as to be detected. Such a quantum channel can be used in conjunction with ordinary insecure classical channels to distribute random key information between two users with the assurance that it remains unknown to anyone else, even when the users share no secret information initially. We also present a protocol for coin-tossing by exchange of quantum messages, which is secure against traditional kinds of cheating, even by an opponent with unlimited computing power, but ironically can be subverted by use of a still subtler quantum phenomemon, the Einstein-Podolsky-Rosen paradox.

principle impossible to counterfeit, and multiplexing two or three messages in such a way that reading one destroys the others. More recently [BBBW], quantum coding has been used in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Here we show that quantum coding by itself achieves one of the main advantages of public key cryptography by permitting secure distribution of random key information between parties who share no secret information initially, provided the parties have access, besides the quantum channel, to an ordinary channel susceptible to passive but not active eavesdropping. Even in the presence of active eavesdropping, the two parties can still distribute key securely if they share some secret information initially, provided the eavesdropping is not so active as to suppress communications completely. We also present a protocol for coin tossing by exchange of quantum messages. Except where otherwise noted the protocols

Kryptografia kwantowa

Protokół BB84 (Bennett, Brassard, 1984)



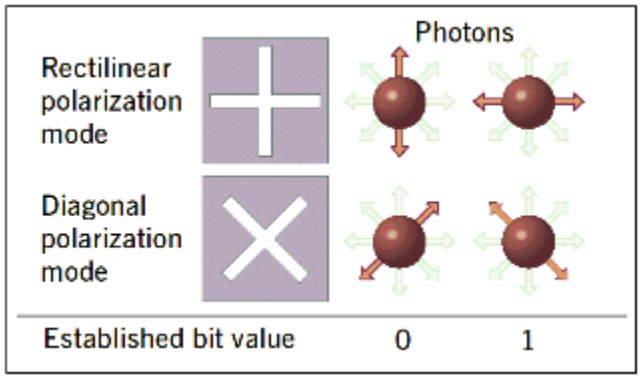


Bolek publicznie informuje Alicje jakiej bazy uzywał, zaś Alicja informuje go czy była to baza właściwa czy nie.

Kryptografia kwantowa

Uwagi:
Porównując bity wysłane przez Alicję z bitami zarejestrowanymi przez Bolka możemy podzielić bity zarejestrowane przez Bolka na trzy kategorie:
– bity pewne (średnio 50 %) — te dla których Bolek wybrał prawidłową bazę i które mogą być traktowane jako klucz kryptograficzny;
– bity prawidłowe pomimo złego wyboru bazy (średnio 25 %);
– bity nieprawidłowe (srednio 25 %).

Zatem prawdopodobieństwo tego, że zarejestrowany bit będzie prawidłowy (taki sam jak bit wysłany) jest równe 3/4
• Prawdopodobieństwo zarejestrowania bitu nieprawidłowego wynosi wiec 1/4



Kryptografia kwantowa

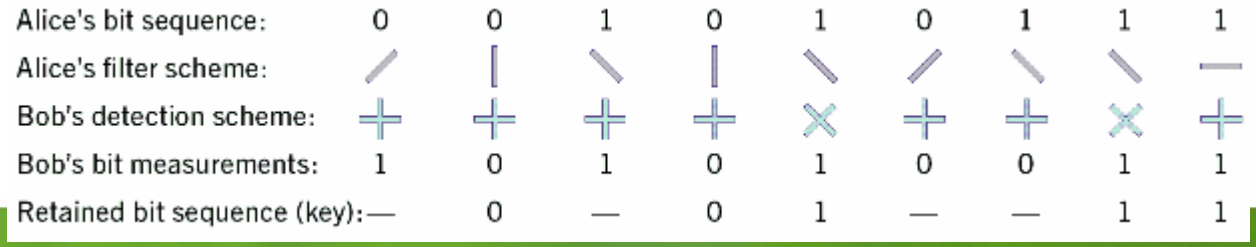
Uwagi:
Jeśli Ewa podsłuchuje stosując strategię tzw. *nieprzezroczystego podsłuchu*, to wybiera losowo bazę prostą lub ukośną, dokonuje pomiaru polaryzacji w tej bazie i następnie przesyła do Bolka foton o takiej polaryzacji jaką zmierzyła.

- Dokonywane przez Ewę pomiary muszą wprowadzić błędy, które Alicja i Bolek mogą wykryć przy uzgadnianiu klucza.

Takie błedy Alicja i Bolek mogą wykryć wybierając losowo pewną liczbę bitów klucza i porównując publicznym kanałem ich wartości. Te bity oczywiście następnie się wyrzuca.

- Jeśli liczba błędów przekracza założony poziom to uznaje się, że kanał był podsłuchiwany i procedurę uzgadniania klucza rozpoczyna się od nowa.

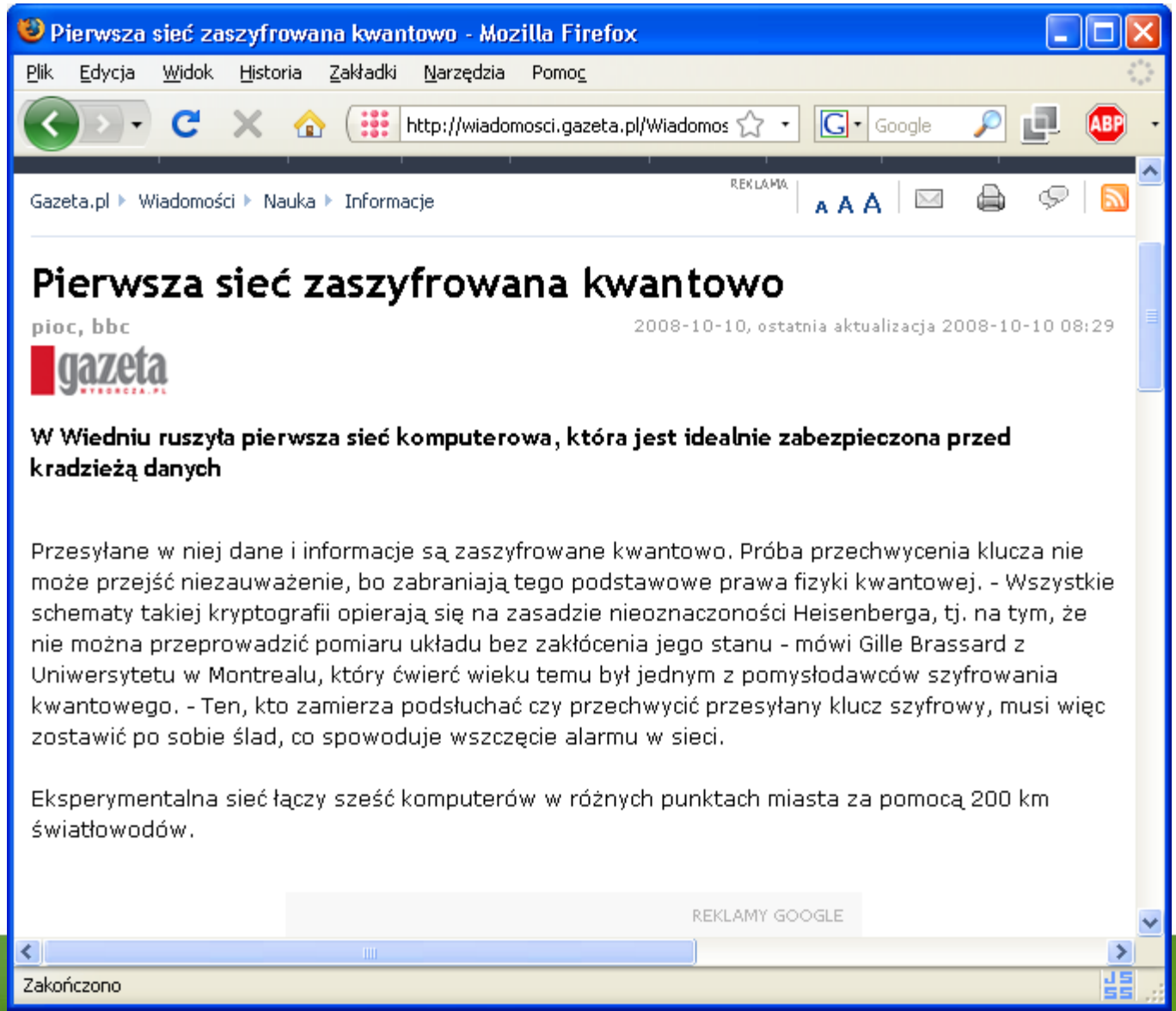
- **Mechanika kwantowa nie dopuszcza możliwości pasywnego podsłuchu. Bezpieczeństwo kwantowego systemu kryptograficznego gwarantowane jest przez prawa fizyki!**



Produkty


ID QUANTIQUE - Mozilla Firefox
Plik Edycja Widok Przejdź Zakładki Narzędzia Pomoc
http://www.idquantique.com/
Idź
Getting Started Latest Headlines Gazeta.pl Murator :: Indeks Tabela NBP Slownik Ang. Slownik Fra. Google Desktop
id Quantique
Products Ordering Support Company News Contact Site Map
SWISS MADE
Are you protected against industrial espionage?
DO YOU TRUST THE SECURITY OF YOUR DATA NETWORK ?
Is your sensitive data as secure as you think?
Latest news
June 05:
A turnkey service to secure communications, based on QC, is now available in Switzerland. Strategic partnership between Fibrelac and idQ (pdf, English or French).
Network Security
Quantum Cryptography [QC] Systems
Vectis
[commercial applications]
Clavis
[research applications]
Overview of idQ's product offering in the field of QC.
Reasons why QC is the most secure technology.
Understanding QC: an introduction (pdf).
Securing networks with the Vectis Link Encryptor (pdf).
Future-proof data confidentiality with QC (pdf).
Random Number Generators [RNGs]
Quantis
Random numbers generation using Quantum Physics (pdf).
Algorithmic randomness, quantum physics and incompleteness (pdf).
Operating Systems supported by Quantis-PCI cards.
What makes Quantis a unique random number generator?
Optical Instrumentation
Photon counters - VIS
Counter arrays - VIS
Photon counters - NIR
Short pulse laser sources
Products overview
Besides its strong focus on Network Security applications, id Quantique is also a leading provider of Optical Instrumentation Products. The company's innovative photonic solutions are used in industrial, commercial and research applications.
© copyright 2005 id Quantique SA, All rights reserved
Zakończono
Disabled
& Events | Partners
s for the Real World.
Company Information
MagiQ at NITSL 2005
MagiQ Celebrates Five Years of Progress
Quantum Cryptography Gets Practical by Bob Gelfond
CIO Ask the Expert: Bob Gelfond
QPN Data Sheet
MagiQ and Cavium

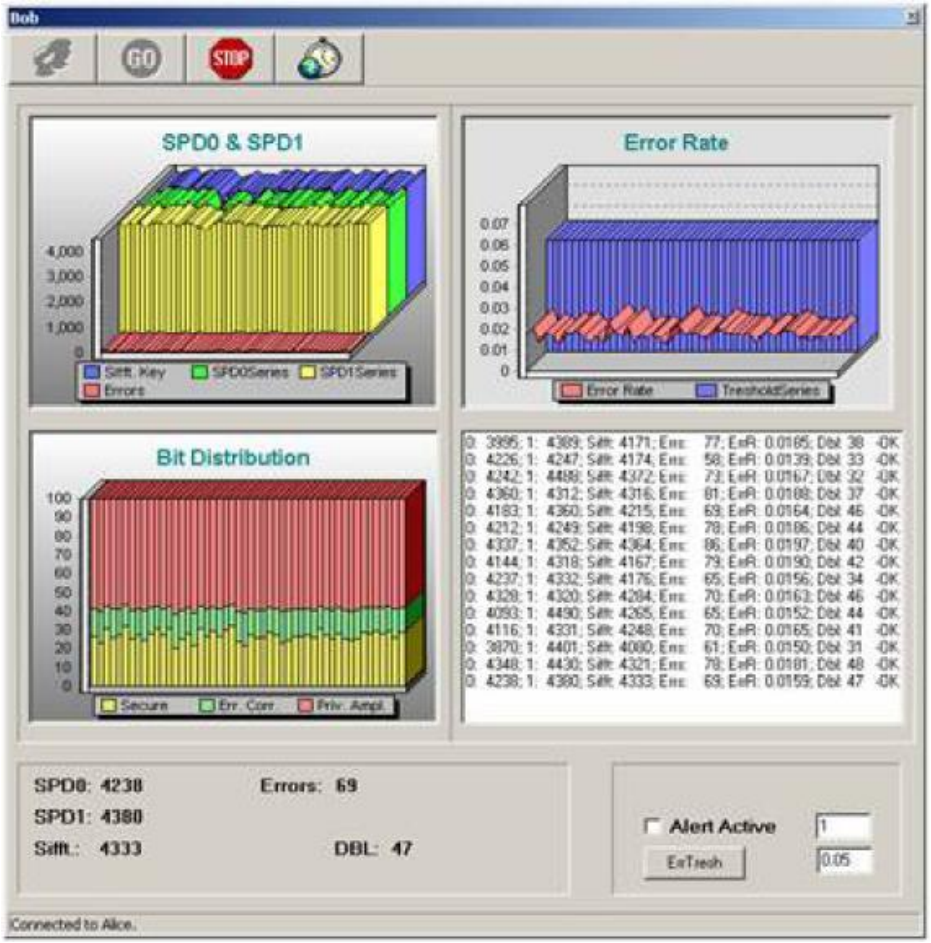
Produkty

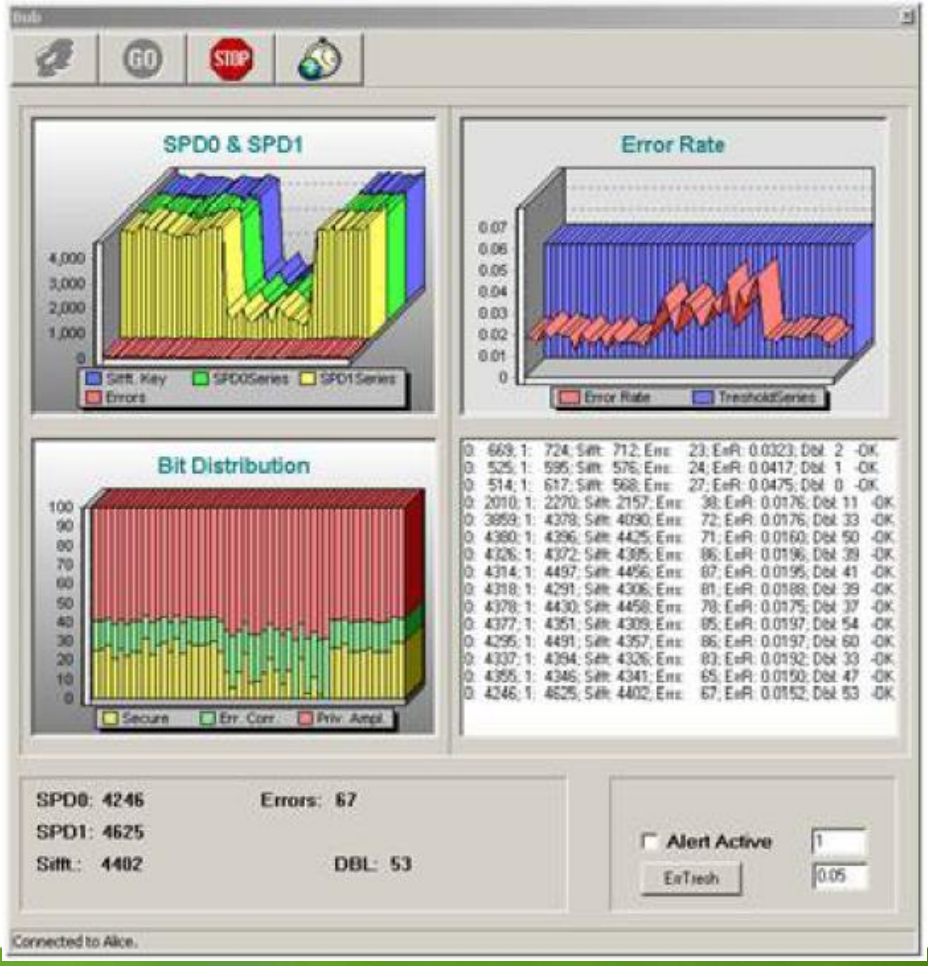

Pierwsza sieć zaszyfrowana kwantowo - Mozilla Firefox
Plik Edycja Widok Historia Zakładki Narzędzia Pomoc
http://wiadomosci.gazeta.pl/Wiadomos
Google
Gazeta.pl ▸ Wiadomości ▸ Nauka ▸ Informacje
REKLAMA
A A A
Pierwsza sieć zaszyfrowana kwantowo
pioc, bbc
2008-10-10, ostatnia aktualizacja 2008-10-10 08:29
gazeta
W Wiedniu ruszyła pierwsza sieć komputerowa, która jest idealnie zabezpieczona przed kradzieżą danych
Przesyłane w niej dane i informacje są zaszyfrowane kwantowo. Próba przechwycenia klucza nie może przejść niezauważenie, bo zabraniają tego podstawowe prawa fizyki kwantowej. - Wszystkie schematy takiej kryptografii opierają się na zasadzie nieoznaczoności Heisenberga, tj. na tym, że nie można przeprowadzić pomiaru układu bez zakłócenia jego stanu - mówi Gille Brassard z Uniwersytetu w Montrealu, który ćwierć wieku temu był jednym z pomysłodawców szyfrowania kwantowego. - Ten, kto zamierza podsłuchać czy przechwycić przesyłany klucz szyfrowy, musi więc zostawić po sobie ślad, co spowoduje wszczęcie alarmu w sieci.
Eksperymentalna sieć łączy sześć komputerów w różnych punktach miasta za pomocą 200 km światłowodów.
REKLAMY GOOGLE
Zakończono

Produkty


MagiQ Technologies - Mozilla Firefox
Plik Edycja Widok Przejdź Zakładki Narzędzia Pomoc
http://www.magiqtech.com/index.php
Idź
Getting Started Latest Headlines Gazeta.pl Murator :: Indeks Tabela NBP Slownik Ang. Slownik Fra. Google Desktop
MagiQ™
Products & Solutions | Research | About MagiQ | Press & Events | Partners
Search
Quantum Information Solutions for the Real World.
News
CSO
Quantum Physics to the Rescue
More...
The Register
Quantum crypto moves out of the lab
More...
Forbes.com
Next-Generation Networks: The Hacker-Proof Network
More...
CNET News.com
Quantum crypto firm charts way to mainstream
More...
Scientific American
Best-Kept Secrets: Quantum Cryptography from Theory to Laboratory
More...
The Industrial Physicist
Quantum Key Distribution
More...
MagiQ QPN
QPN datasheet
QPN™ Research
QPN datasheet
Presenting the first commercial quantum cryptography solutions.
Press Releases
MagiQ Solves Quantum Cryptography Geomagnetic Interference Problem
MagiQ Announces New, Next Generation Quantum Cryptography Solution
MagiQ and Cavium
Product Information
QPN Overview Presentation
New Weapon to Protect Online Privacy
QPN Executive Summary
QPN Data Sheet
Company Information
MagiQ at NITSL 2005
MagiQ Celebrates Five Years of Progress
Quantum Cryptography Gets Practical by Bob Gelfond
CIO Ask the Expert: Bob Gelfond

Produkty


Bob
GO
STOP
SPD0 & SPD1
Sift. Key
SPD0Series
SPD1Series
Errors
Error Rate
Error Rate
TresholdSeries
Bit Distribution
Secure
Err. Corr
Priv. Ampl
SPD0: 4238
Errors: 69
SPD1: 4380
Sift.: 4333
DBL: 47
Alert Active
ErrTresh
Connected to Alice.


Bob
GO
STOP
SPD0 & SPD1
Sift. Key
SPD0Series
SPD1Series
Errors
Error Rate
Error Rate
TresholdSeries
Bit Distribution
Secure
Err. Corr
Priv. Ampl
SPD0: 4246
Errors: 67
SPD1: 4625
Sift.: 4402
DBL: 53
Alert Active
ErrTresh
Connected to Alice.

PHYSICAL REVIEW
LETTERS

VOLUME 67 5 AUGUST 1991 NUMBER 6

Quantum Cryptography Based on Bell's Theorem

Artur K. Ekert

Merton College and Physics Department, Oxford University, Oxford OX1 3PU, United Kingdom

(Received 18 April 1991)

Practical application of the generalized Bell's theorem in the so-called key distribution process in cryptography is reported. The proposed scheme is based on the Bohm's version of the Einstein-Podolsky-Rosen *gedanken experiment* and Bell's theorem is used to test for eavesdropping.

Kryptografia kwantowa

VOLUME 67 NUMBER 6

Q

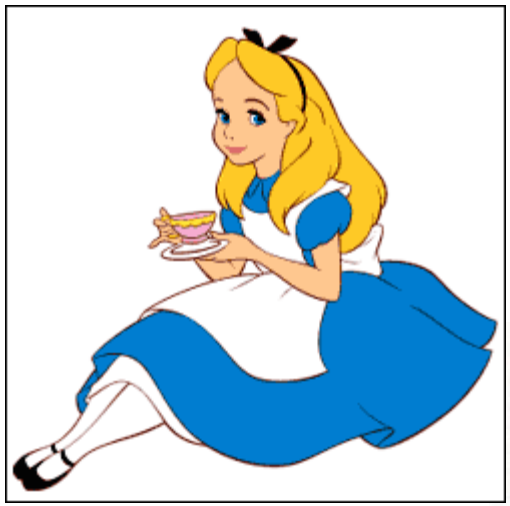
Merton College ar *ed Kingdom*

Practical applicatio process in cryp-
tography is reported. nstein-Podolsky-
Rosen *gedanken exper*

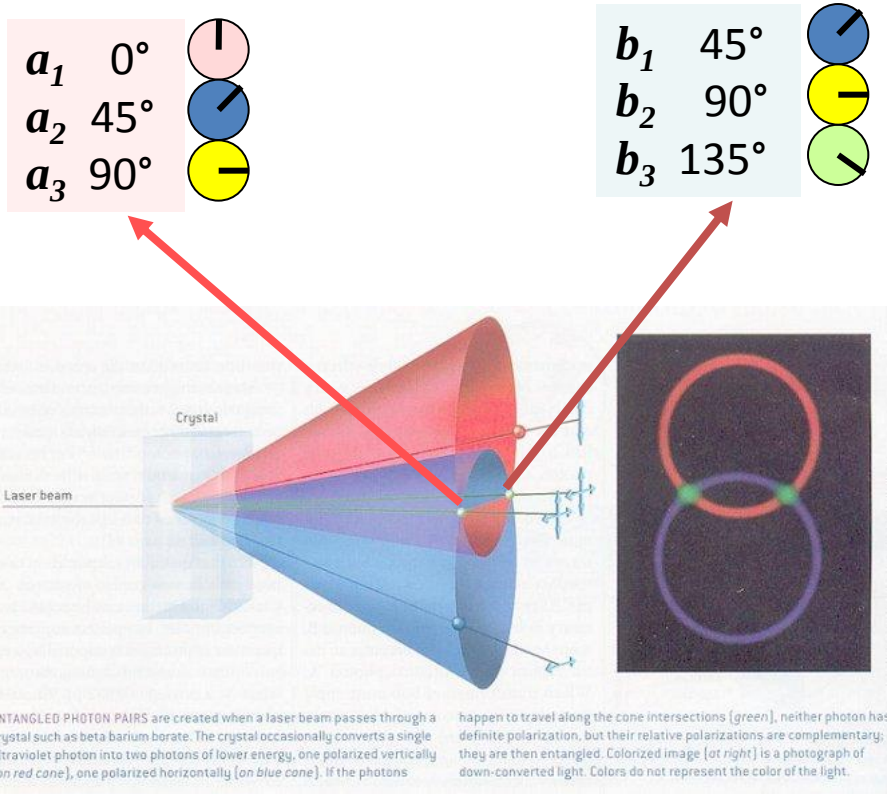
Artur Ekert

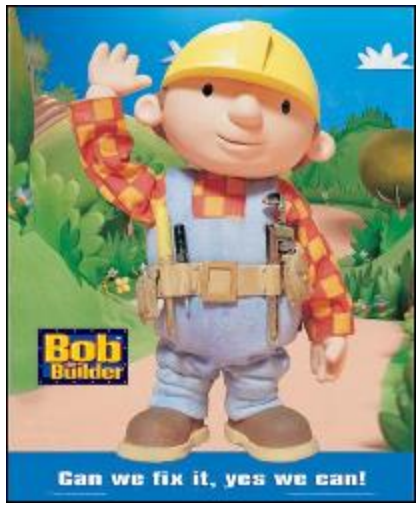
Kryptografia kwantowa

Artur Ekert



Alice

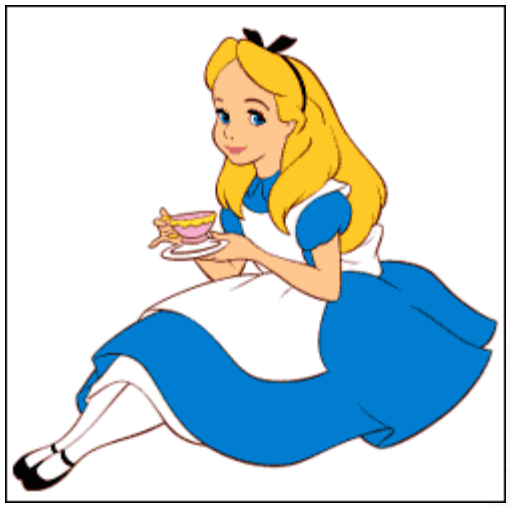




Bob

Kryptografia kwantowa

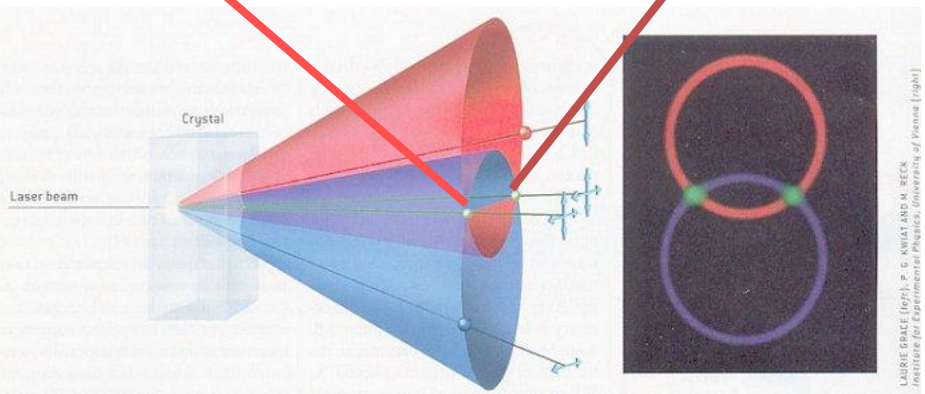
Artur Ekert

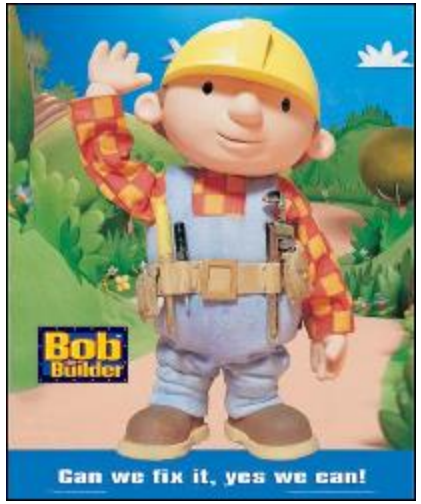


Alice

a_1 0°
a_2 45°
a_3 90°

b_1 45°
b_2 90°
b_3 135°





Bob

a																					
	1	0	1	1	0	0	0	1	0	1	x	1	0	1	1	0	0	1	1	1	0
b																					
	1	0	0	0	1	1	0	1	1	1	0	0	0	0	0	1	0	1	0	1	1
	t	0	1	t	0	0	t	1	0	1	x	t	0	1	t	t	t	1	t	t	t

jawne

jawne

test (jawny)

Klucz: 0100101011…

After the transmission has taken place, Alice and Bob can announce in public the orientations of the analyzers they have chosen for each particular measurement and divide the measurements into two separate groups: a first group for which they used different orientation of analyzers, and a second group for which they used the same orientation of their analyzers. They discard all measurements in which either or both of them failed to register a particle at all. Subsequently, Alice and Bob can reveal publicly the results they obtained but within the first group of measurements only. This allows them to establish the value of S, which, if the particles were not directly or indirectly "disturbed," should reproduce the result of Eq. (4). This assures the legitimate users that the results they obtained within the second group of measurements are anticorrelated and can be converted into a secret string of bits—the key. This secret key may be then used in a conventional cryptographic communication between Alice and Bob.

$$S=E(\mathbf{a}_1,\mathbf{b}_1)-E(\mathbf{a}_1,\mathbf{b}_3)+E(\mathbf{a}_3,\mathbf{b}_1)+E(\mathbf{a}_3,\mathbf{b}_3)\,. \tag{3}$$

Again, quantum mechanics requires

$$S=-2\sqrt{2}\,. \tag{4}$$

The eavesdropper cannot elicit any information from the particles while in transit from the source to the legitimate users, simply because there is no information encoded there. The information "comes into being" only after the legitimate users perform measurements and communicate in public afterwards. The eavesdropper may try to substitute his own prepared data for Alice and Bob to misguide them, but as he does not know which orientation of the analyzers will be chosen for a given pair of particles, there is no good strategy to escape from being detected.

$$S=\int \rho(\mathbf{n}_a,\mathbf{n}_b)\,d\mathbf{n}_a\,d\mathbf{n}_b[\sqrt{2}\mathbf{n}_a\cdot\mathbf{n}_b]\,, \tag{6}$$

which implies

$$-\sqrt{2}\le S\le\sqrt{2}\,, \tag{7}$$

Kryptografia kwantowa

PHYSICAL REVIEW A VOLUME 56, NUMBER 2 AUGUST 1997

Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy

Christopher A. Fuchs,[1] Nicolas Gisin,[2] Robert B. Griffiths,[3] Chi-Sheng Niu,[3] and Asher Peres[4,*]
[1]*Norman Bridge Laboratory of Physics 12-33, California Institute of Technology, Pasadena, California 91125*
[2]*Group of Applied Physics, University of Geneva, CH 1211 Geneva 4, Switzerland*
[3]*Department of Physics, Carnegie-Mellon University, Pittsburgh, Pennsylvania 15213*
[4]*Institute for Theoretical Physics, University of California, Santa Barbara, California 93106*
(Received 31 January 1997)

We consider the Bennett-Brassard cryptographic scheme, which uses two conjugate quantum bases. An eavesdropper who attempts to obtain information on qubits sent in one of the bases causes a disturbance to qubits sent in the other basis. We derive an upper bound to the accessible information in one basis, for a given error rate in the conjugate basis. Independently fixing the error rates in the conjugate bases, we show that both bounds can be attained simultaneously by an optimal eavesdropping probe. The probe interaction and its subsequent measurement are described explicitly. These results are combined to give an expression for the optimal information an eavesdropper can obtain for a given average disturbance when her interaction and measurements are performed signal by signal. Finally, the relation between quantum cryptography and violations of Bell's inequalities is discussed. [S1050-2947(97)01708-3]

Kryptografia kwantowa

We take the framework for our problem directly from quantum cryptography. In order to take advantage of Alice's delayed information on the basis that was used, Eve's optimal strategy is the following: she lets a probe, initially in some standard state $|\psi_0\rangle$, interact unitarily with the qubit sent by Alice. (There is no loss of generality in this, because any physical nonunitary interaction is equivalent to a unitary one with a higher dimensional probe.) Eve's probe is then stored until Alice announces the basis that was used, and only after that is it measured by Eve.

In a convenient notation, if Alice sends state $|x\rangle$, the result may be written as

$$|x\rangle \otimes |\psi_0\rangle \rightarrow |X\rangle, \qquad (1)$$

where $|X\rangle$ is an entangled state of the probe and the photon that Alice sent to Bob. Likewise, for the other signals that Alice may send, the results of Eve's intervention are entangled states, $|Y\rangle$, $|U\rangle$, and $|V\rangle$. Since the interaction is unitary, it follows from

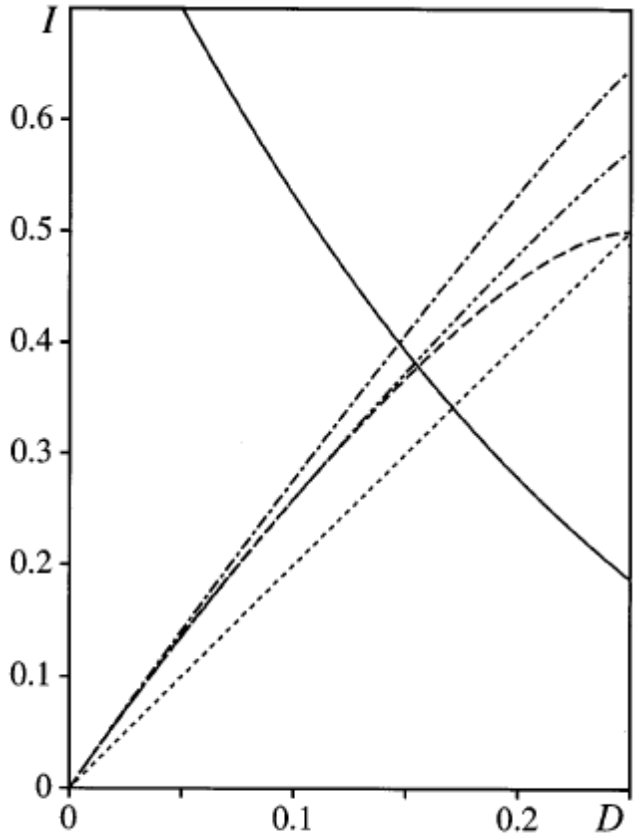


FIG. 2. Information vs disturbance for various eavesdropping methods.


DO PRACY
ZGŁASZAJ SIĘ
TRZEŹWY i WYPOCZĘTY