Wprowadzenie do optycznej kryptografii kwantowej

o tym jak kryptografia kwantowa jest być może najważniejszym zastosowaniem współczesnej optyki kwantowej

prehistoria kryptografii kwantowej

1983 (1970 !)

Stephen Wiesner

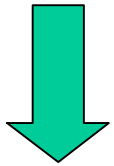
pierwszy opis kodowania kwantowego

- Jak drukować banknoty niefalsyfikowalne
- Jak połączyć 2-3 wiadomości tak, aby czytając jedną z nich automatycznie zniszczyć pozostałe

zakaz klonowania

(no-cloning theorem)
Wootters i Żurek oraz Dieks (1982)

- Tw. Nie można zrobić idealnej kopii nieznanego stanu kwantowego
- Tj. jedno z najbardziej fundamentalnych tw. mechaniki kwantowej



- *kryptografia kwantowa* jest bezpieczna
- *komunikacja nadświetlna* za p. stanów splątanych jest niemożliwa
- *teleportacja kwantowa* wydaje się też niemożliwa ???

zasada nieoznaczoności Heisenberga (1927)

dotyczy pomiaru wielkości komplementarnych (np. A i B)

pojedynczą wielkość można zmierzyć z dowolną dokładnością
ALE
dokładny pomiar A zaburza B tak, że mierząc
B otrzymujemy wartości przypadkowe

$$[\hat{A}, \hat{B}] = i\hat{C}$$

$$\operatorname{var}\hat{A}\,\operatorname{var}\hat{B} \geq \frac{1}{4}\left|\left\langle \hat{C} \right\rangle\right|^2$$

$$\text{np.}\quad \operatorname{var}\hat{x}\,\operatorname{var}\hat{p} \geq \frac{\hbar^2}{4}$$

➡ Tj. uzasadnienie bezpieczeństwa kryptografii kwantowej

zasada nieoznaczoności Heisenberga

➡ pasywny podsłuch jest niemożliwy

1. Można odróżnić 2 kierunki polaryzacji prostej $a = 0^o$ i 90^o
2. Można odróżnić 2 kierunki polaryzacji ukośnej $a = 45^o$ i 135^o
3. Można szybko przestawić ustawienie polarycji (np. w komórce Pockelsa)
4. ALE nie można zmierzyć jednocześnie $a = 0^o, 90^o, 45^o$ i 135^o

podsłuch układu klasycznego

2 etapy:

1. Ewa robi kopię „nośnika” informacji (tzw. klon)
2. i odczytuje informacje z kopii

pasywne monitorowanie informacji jest możliwe

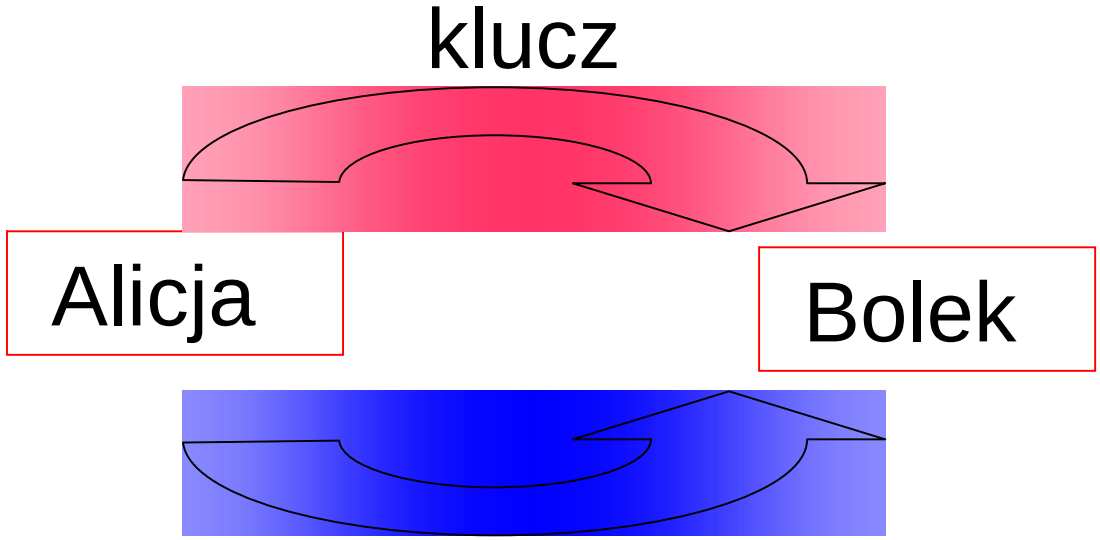
podsłuch układu kwantowego

Ewa nie może klonować informacji jeśli nie wie w jakim stanie jest „nośnik” informacji

monitorowanie zaburza informację kwantową

schemat Bennetta i Brassarda (1984)
= protokół BB84

dwa kanały:
1. kwantowy prywatny
2. klasyczny publiczny (np. internet)



BB84

2 etapy:

1. kwantowa dystrybucja klucza
2. klasyczny kryptaż wykorzystując np. algorytm Vernama

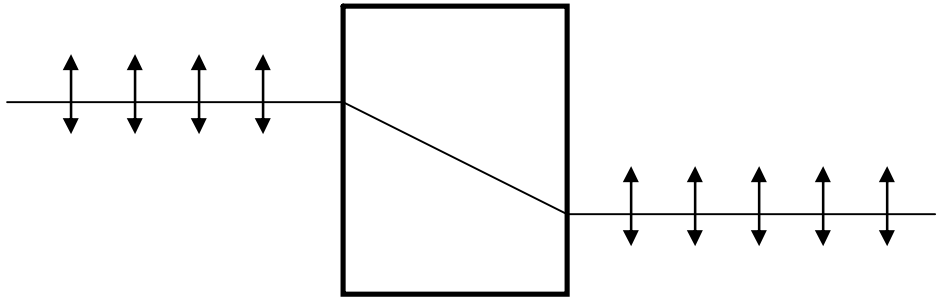
PROBLEM:

Jak ustalić wspólny klucz kwantowy?

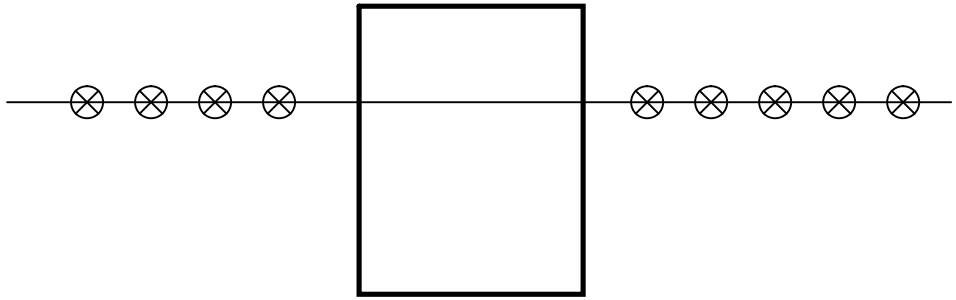
kryształy dwójłomne

umożliwiają rozróżnienie fotonów spolaryzowanych prostopadle względem siebie

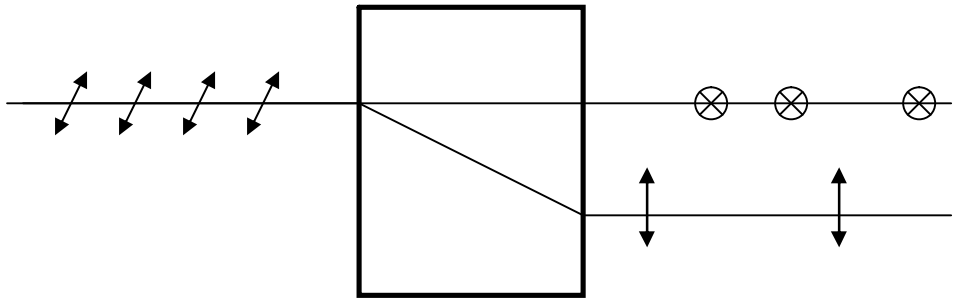
fotony spol. poziomo



fotony spol. pionowo



fotony spol. ukośnie



kryształ kalcytu

BB84 (1)

umowa | (a= 90º) i \ (a= 135º) => **bit 1**

- (a= 0º) i / (a= 45º) => **bit 0**

baza - proste lub ukośne ustawienie kryształu

1. Alicja wysyła fotony

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

+	+	x	+	x	x	x	+	x	+	+	x	x	+	x	**baza**
|	-	\	|	/	/	\	|	/	-	|	\	\	-	\	**pol.fotonu**
1	0	1	1	0	0	1	1	0	0	1	1	1	0	1	**bit**

BB84 (2)

2. Bolek losowo wybiera typ pomiaru (bazę)

```
01 02 03 04 05 06  07 08 09 10 11 12 13 14 15
| - \ | / / \ | / - | \ \ - \     pol.fotonu
                                    Alicji
+ x + + x x + + x + x x + + x     baza Bolka
| \ - | / / | | / - / \ - - \     pol.fotonu
                                    po pomiarze
```

BB84 (3)

3. Alicja i Bolek publicznie porównują bazy

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
+	+	x	+	x	x	x	+	x	+	+	x	x	+	x	bazy Alicji
+	x	+	+	x	x	+	+	x	+	x	x	+	+	x	bazy Bolka
z	n	n	z	z	z	n	z	z	z	n	z	n	z	z	test

BB84 (4)

4. Alicja i Bolek zatrzymują tylko te wyniki otrzymane przy zgodnych bazach

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
1	.	.	1	0	0	.	1	0	0	.	1	.	0	1	ciąg Alicji
1	.	.	1	0	0	.	1	0	0	.	1	.	0	1	ciąg Bolek

BB84 (5)

5.Testowanie wyników dla niektórych fotonów np. 1, 5, 10 i 14-go

01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
1	.	.	1	0	0	.	1	0	0	.	1	.	0	1	ciąg Alicji
1	.	.	1	0	0	.	1	0	0	.	1	.	0	1	ciąg Bolka
OK				OK					OK				OK		

BB84 (6)

6. odrzucamy wyniki dla testowanych fotonów

01 02 03 04 05 06 07 08 09 10 11 12 13 14 15

. . . 1 . 0 . 1 0 . . 1 . . 1 ciąg Alicji

. . . 1 . 0 . 1 0 . . 1 . . 1 ciąg Bolka

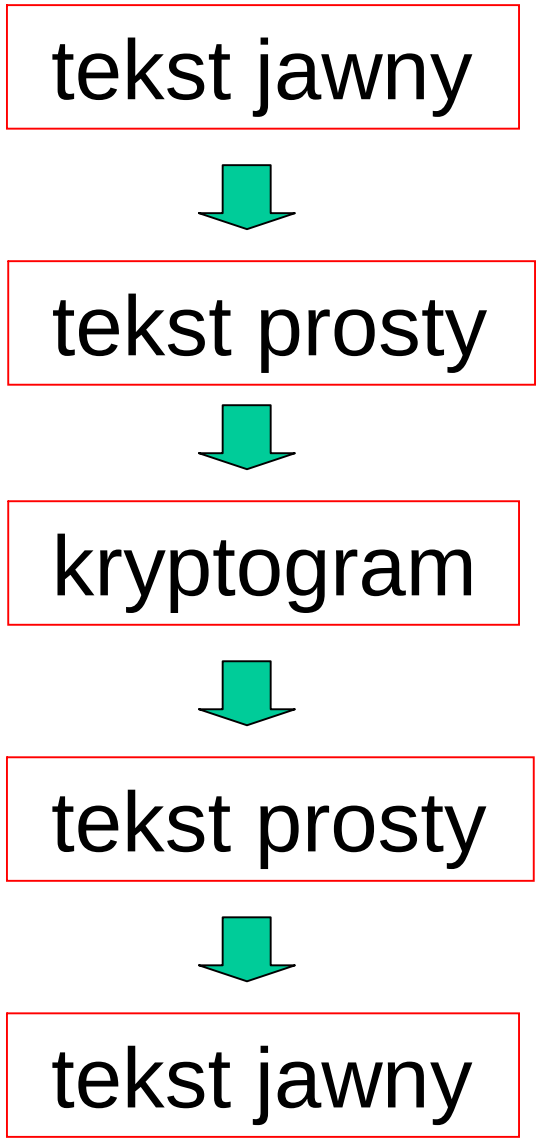
zatem kluczem jest ciąg

1 0 1 0 1 1

nasz alfabet cyfrowy

000001	01	A
000010	02	Ą
000011	03	B
000100	04	C
...		
100011	35	Ź
...		
101000	40	.

symetryczne algorytmy kryptograficzne



kryptaż kluczem *k*

dystrybucja klucza

dekryptaż tym samym kluczem *k*

szyfr Vernama (1918)

= szyfr Che Guevary

= one-time pad

= algorytm z kluczem jednorazowym

1) alfabet cyfrowy

01 A 02 Ą 03 B 04 C 05 Ć 06 D 07 E 08 Ę 09 F 10 G
11 H 12 I 13 J 14 K 15 L 16 Ł 17 M 18 N 19 Ń 20 O
21 Ó 22 P 23 Q 24 R 25 S 26 Ś 27 T 28 U 29 V 30 W
31 X 32 Y 33 Z 34 Ż 35 Ź 36 _ 37 - 38 ? 39 , 40 .

szyfr Vernama (II)

2) KLUCZ

wybrany losowo

fizycznie bezpieczny

nigdy nie używany powtórnie

długość klucza >= długość tekstu

3) ALGORYTM

dodawanie modulo N (np. 40)

szyfr Vernama (III)

klucz: 16 10 12 01 27 39 13 01 14 13 36 25 12 08 36 13 01 30 16
(losowy ciąg liczb)

tekst jawny	A D A M _ M I R A NO W I C Z _ ZO N
tekst prosty	01 06 01 17 36 17 13 24 0118 20 30 12 04 33 36 33 20 18

Suma: 17 16 13 18 63 56 26 25 15 31 56 55 24 12 69 49 34 50 34

Suma mod (40):

17 16 13 18 23 16 26 25 15 31 16 15 24 12 29 09 34 10 34

KRYPTOGRAM

Test zgodności

1. Alicja i Bolek porównują dowolnie wybrany podzbiór danych. Oczywiście ten podzbiór odrzucamy.
2. Jeśli podzbiór wykazuje ślady podsłuchu, to odrzucamy wszystkie dane i proces ponawiamy
3. Testowanie:

(a) bit po bicie

(b) porównywanie parzystości

np. 20 razy => $(1/2)^{20} \sim 0.000001$

4. Pogłębianie tajności (privacy amplification) schemat Bennetta-Brassarda-Roberta

strategia podsłuchu Ewy (I)

Jakie jest prawdopodobieństwo, że pojedynczy foton został zmierzony przez Ewę a Alicja i Bolek nie zauważyli podsłuchu ?

Odpowiedź:

P=3/4

optyczne protokoły dystrybucji klucza kwantowego

1984 schemat Ch. Bennetta i G. Brassarda (protokół BB84)

1991 schemat A. Ekerta z wykorzystaniem splątania kwantowego (protokół E91)

1992 schemat Ch. Bennetta (protokół B92)

strategia podsłuchu Ewy (II)

	Alicja	Ewa	Bob	
	+	+	+	
		1/2		= 1/2

	Alicja	Ewa	Bob	
Baza	+	x	+	
Polar.	|	/	|	
Prawd.		1/2*1/2	1/2	= 1/8

	Alicja	Ewa	Bob	
	+	x	+	
	|	\	|	
		1/2*1/2	1/2	= 1/8

bezpieczeństwo BB84

dla 1 fotonu $P_1=3/4$

dla n fotonów $P_n=(3/4)^n$

zatem

$P_2=(3/4)^2 \sim 0.56$

$P_{10}=(3/4)^{10} \sim 0.06$

$P_{20}=(3/4)^{20} \sim 0.003$

$P_{100}=(3/4)^{100} \sim 10^{-13}$

a dla 1000 fotonów

$P_{1000}=(3/4)^{1000} \sim 10^{-125}$

Informacja ma naturę fizyczną

„Information is inevitably tied to
a physical representation and
therefore to restrictions and possibilities
related to the laws of physics” (R. Landauer)

informatyka klasyczna
jest dziedziną matematyki

informatyka kwantowa
jest dziedziną fizyki

Wprowadzenie
do teleportacji kwantowej

Co to jest teleportacja ?

- ,,Fikcyjna metoda bezcielesnego transportu’’

- obiekt jest dematerializowany
  i następnie
  idealnie rekonstruowany w odległym miejscu

- 3D superfaks z niszczarką
  gdyż
  obiekt musi być zniszczony w czasie skanowania

Co to jest teleportacja kwantowa ?

- przekazanie całej informacji zakodowanej w jednej cząstce do innej cząstki

- przeniesienie stanu układu A do układu B poprzez pomiar wykonany na układzie A i operacje unitarne na układzie B

splątanie/splecenie kwantowe

[Schroedinger 1935]

= niem. Verschrankung, ang. entanglement

= korelacje typu EPR (Einsteina-Podolsky'ego-Rosena)

= nieseparowalność kwantowa

To są korelacje kwantowe między podukładami realizowane na 2 lub więcej sposobów

układ jest w stanie superpozycji różnych możliwości realizacji tych korelacji

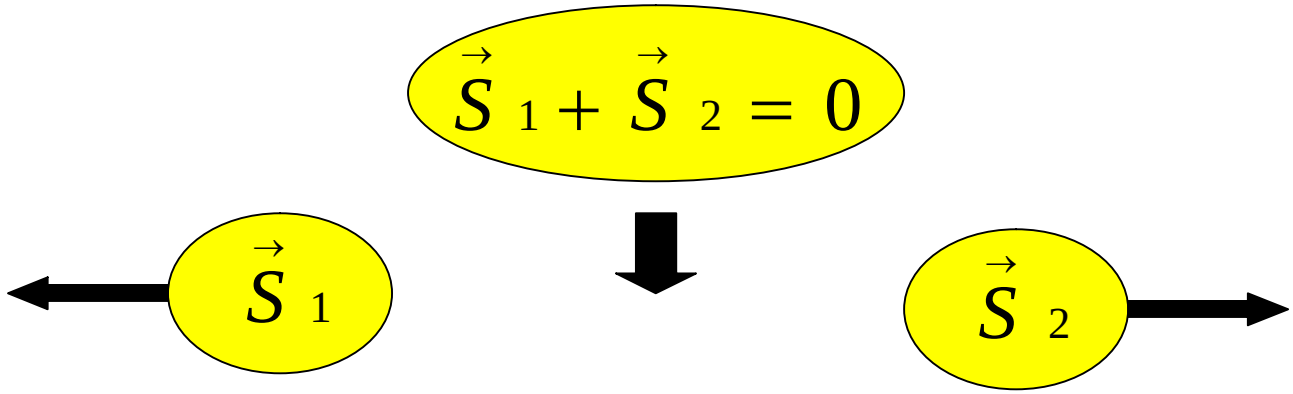
Stan układu złożonego z kilku podukładów jest splątany jeśli nie można go przedstawić w postaci iloczynu stanów dla każdego z podukładów

paradoks Einsteina-Podolsky'ego-Rosena

Jak obejść zasadę nieoznaczoności ?

Czy można zmierzyć dokładnie 2 składowe spinu ?

$$\mathrm{var}\,\hat{S}_{1x}\,\mathrm{var}\,\hat{S}_{1y} \geq \frac{\hbar^2}{4}\left|\left\langle \hat{S}_{1z} \right\rangle\right|^2$$



$$\hat{S}_{1x} + \hat{S}_{2x} = 0, \qquad \hat{S}_{1y} + \hat{S}_{2y} = 0$$

Zatem zmierzmy $\hat{S}_{1x}$ i $\hat{S}_{2y}$, aby wyznaczyć $\hat{S}_{2x}$ i $\hat{S}_{1y}$

stany Bella (stany EPR)

to są maksymalnie splecione stany 2 kubitów

$$|\Phi_A\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x|1\rangle_y - |1\rangle_x|0\rangle_y\right)$$

$$|\Phi_B\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x|1\rangle_y + |1\rangle_x|0\rangle_y\right)$$

$$|\Phi_C\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x|0\rangle_y - |1\rangle_x|1\rangle_y\right)$$

$$|\Phi_D\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_x|0\rangle_y + |1\rangle_x|1\rangle_y\right)$$

generacja stanów splątanych

- w wyniku rozpadu cząstki o spinie 0 na dwie cząstki o spinach 1

$$\left|\Phi\right\rangle_{xy} = \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_x\left|\downarrow\right\rangle_y \pm \left|\downarrow\right\rangle_x\left|\uparrow\right\rangle_y\right)$$

- za pomocą parametrycznego dzielnika częstotliwości (PDC II)

$$\left|\Phi\right\rangle_{xy} = \frac{1}{\sqrt{2}}\left(\left|H\right\rangle_x\left|V\right\rangle_y + e^{i\chi}\left|V\right\rangle_x\left|H\right\rangle_y\right)$$

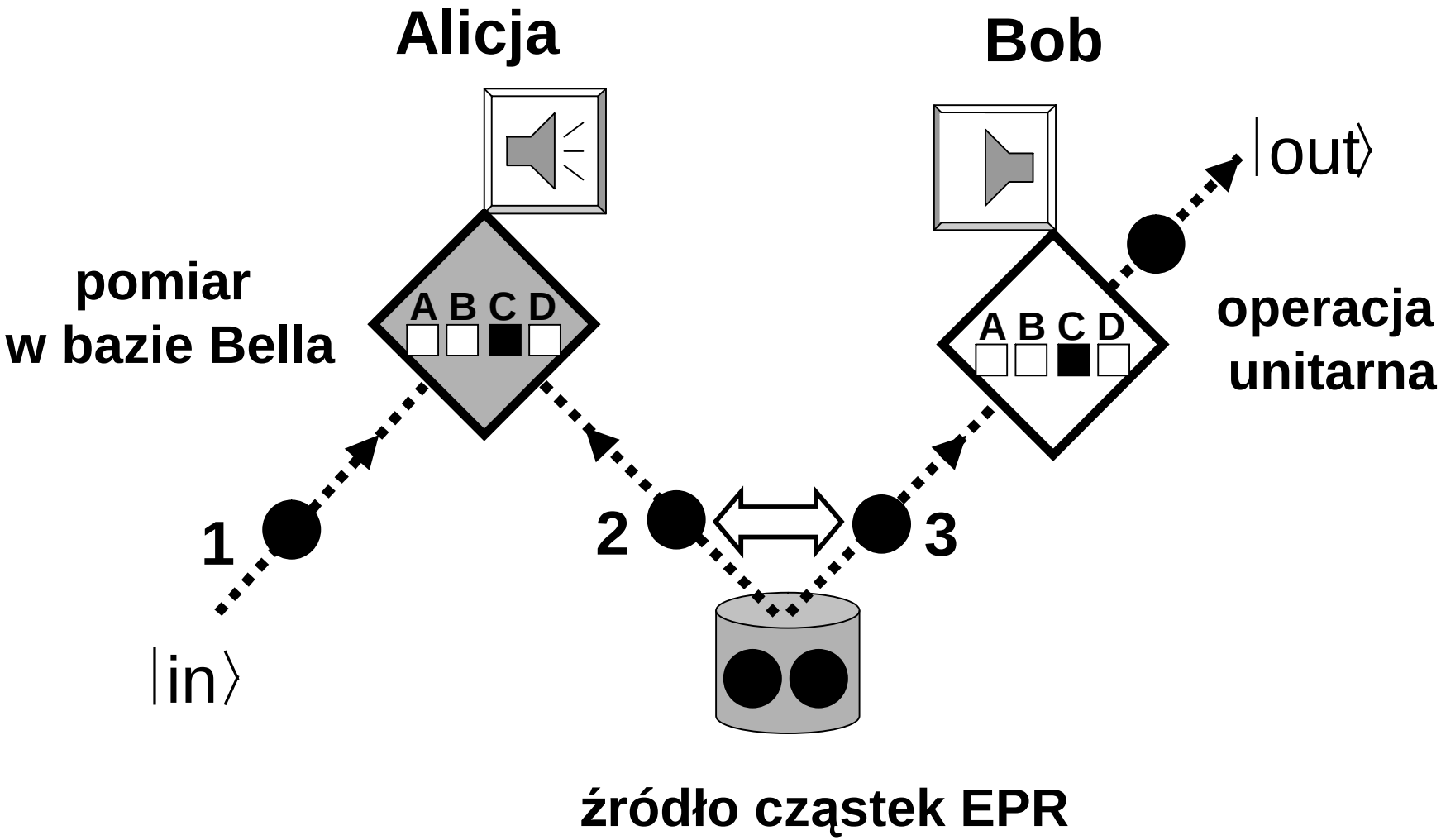
- za pomocą płytki światłodzielącej 50:50, gdy na wejściu jest jeden foton

$$\left|\Phi\right\rangle_{xy} = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle_x\left|1\right\rangle_y + \left|1\right\rangle_x\left|0\right\rangle_y\right)$$

- przez rzutowanie stanu niesplątanego na stan splątany

teleportacja kwantowa

[Bennett i in. (1993)]



uzasadnienie teleportacji

Problem: jak teleportować stan kubitu 1 do kubitu 3

Założenie: kubity 2 i 3 są splątane w stanie $\left|\Phi_A\right\rangle_{23}$

$$\left|\text{in}\right\rangle_1 \otimes \left|\Phi_A\right\rangle_{23} = \left(a\left|0\right\rangle_1 + b\left|1\right\rangle_1\right) \otimes \frac{\left|0\right\rangle_2\left|1\right\rangle_3 - \left|1\right\rangle_2\left|0\right\rangle_3}{\sqrt{2}}$$

$$= \frac{1}{2}\left|\Phi_A\right\rangle_{12} \otimes \left(a\left|0\right\rangle_3 + b\left|1\right\rangle_3\right) + \frac{1}{2}\left|\Phi_B\right\rangle_{12} \otimes \left(a\left|0\right\rangle_3 - b\left|1\right\rangle_3\right)$$

$$-\frac{1}{2}\left|\Phi_C\right\rangle_{12} \otimes \left(a\left|1\right\rangle_3 + b\left|0\right\rangle_3\right) + \frac{1}{2}\left|\Phi_D\right\rangle_{12} \otimes \left(a\left|1\right\rangle_3 - b\left|0\right\rangle_3\right)$$

pomiar w bazie Bella

$$\left|\Phi_A\right\rangle_{12} \Rightarrow \quad a\left|0\right\rangle_3 + b\left|1\right\rangle_3 \qquad \text{OK}$$

$$\left|\Phi_B\right\rangle_{12} \Rightarrow \quad \sigma_z\left(a\left|0\right\rangle_3 - b\left|1\right\rangle_3\right) \qquad \text{phase flip}\left|x\right\rangle \rightarrow (-1)^x\left|x\right\rangle$$

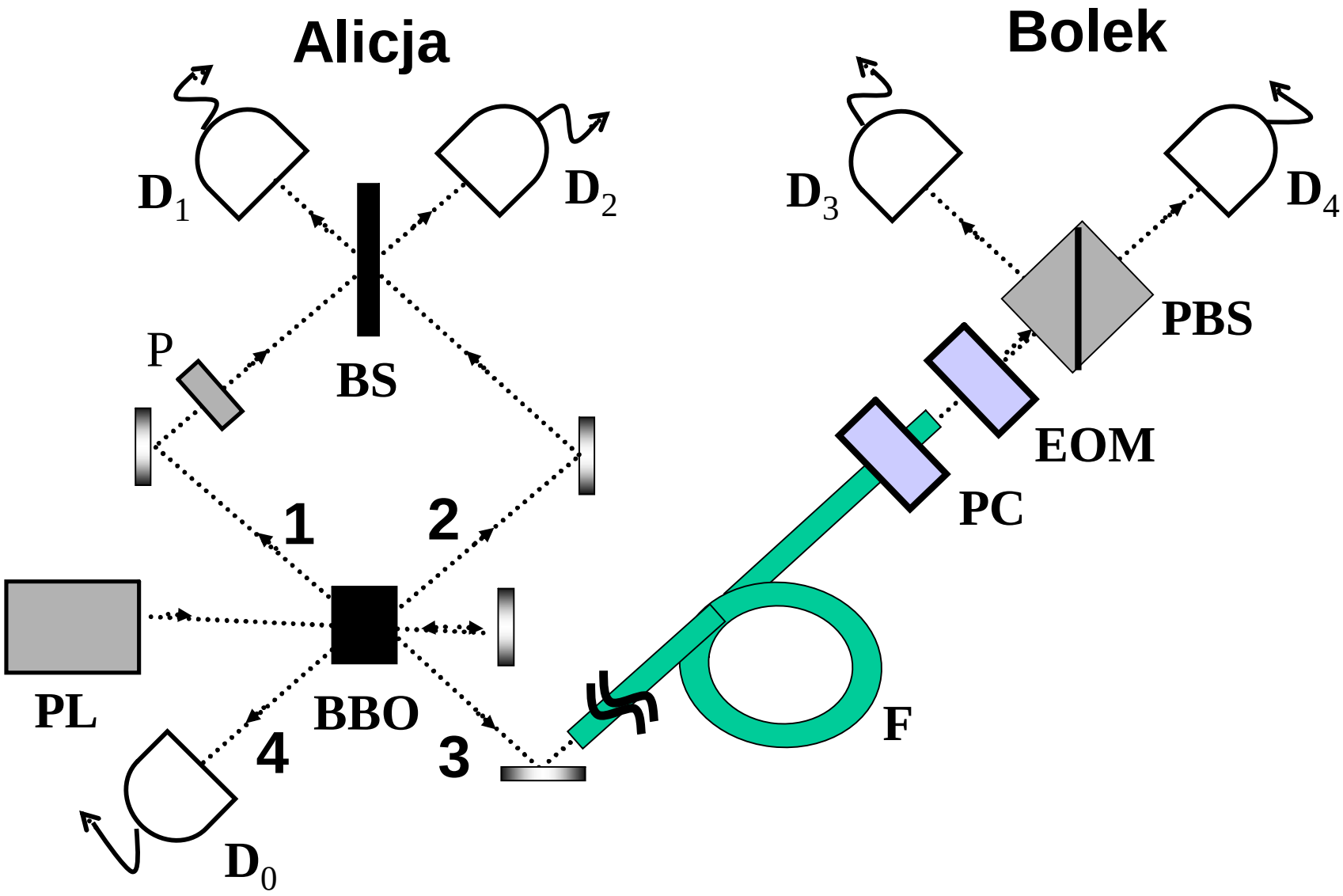
$$\left|\Phi_C\right\rangle_{12} \Rightarrow \quad -\sigma_x\left(-a\left|1\right\rangle_3 - b\left|0\right\rangle_3\right) \qquad \text{bit flip}\left|x\right\rangle \rightarrow -\left|x\oplus 1\right\rangle$$

$$\left|\Phi_D\right\rangle_{12} \Rightarrow \quad -i\sigma_y\left(a\left|1\right\rangle_3 - b\left|0\right\rangle_3\right) \qquad \text{phase flip} + \text{bit flip}$$

$$\left|x\right\rangle \rightarrow (-1)^{x+1}\left|x\oplus 1\right\rangle$$

bit flip = odwrócenie bitu
phase flip = odwrócenie fazy bitu

eksperyment Zeilingera



teleportacja pod Dunajem

teleportacja stanu polaryzacyjnego fotonu

eksperyment Zeilingera i in. (Nature 2004)

Legenda:

F - światłowód (fibre) o dł. 800m

PL - laser impulsowy emitujący światło o dł. 394 nm (fioletowe)

BBO - beta-boran baru - tj. parametryczny dzielnik częstotliwości

EOM - elektrooptyczny modulator <-> operacja unitarna Bolka

PC - kontroler/korektor polaryzacji

BS - płytka światłodzieląca (beam splitter)

PBS - polaryzacyjna płytka światłodzieląca (polarising beam splitter)

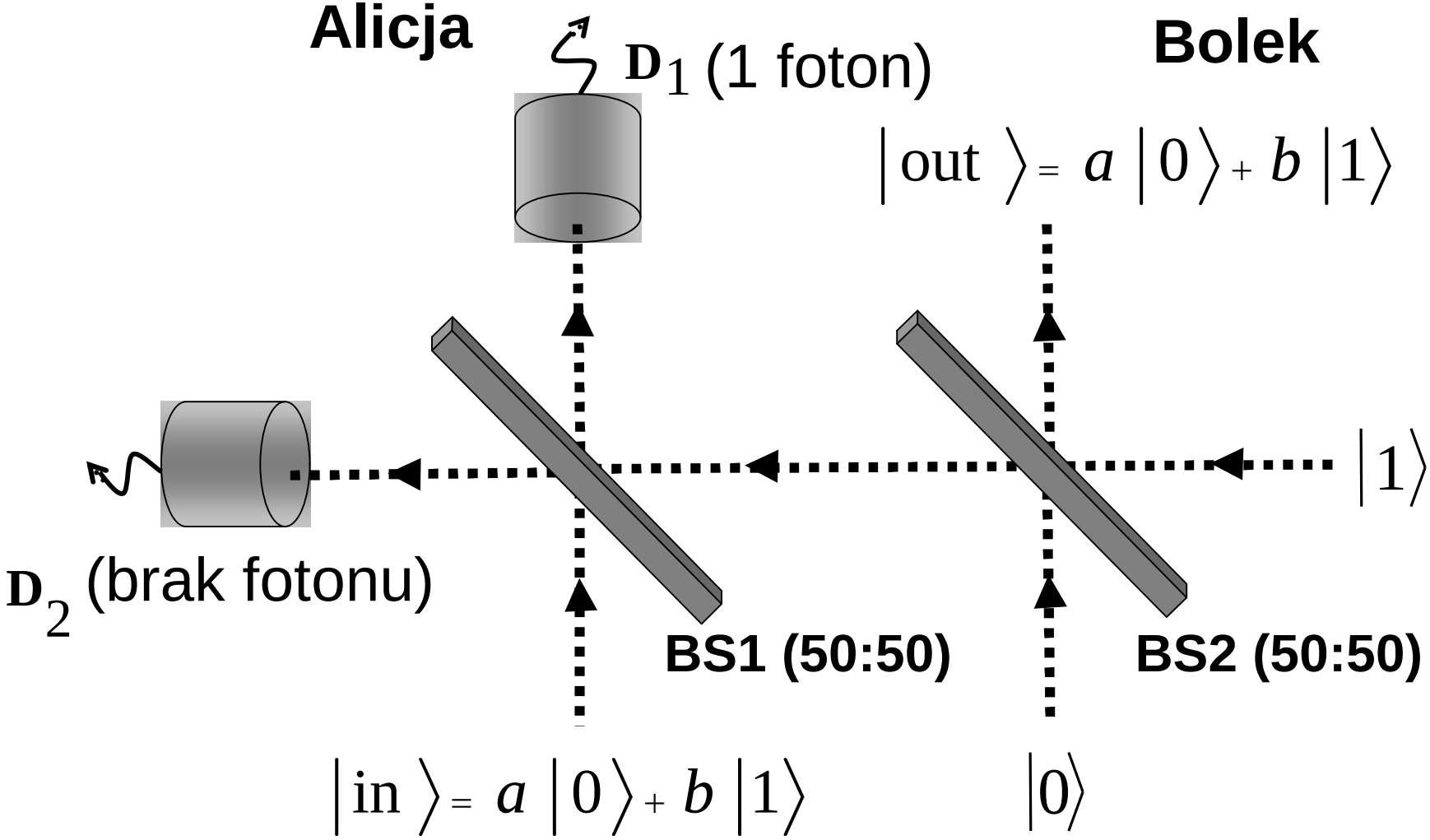
D_0, ... - detektory

kryształ BBO

padający foton `fioletowy' (394 nm) generuje w krysztale BBO typu II dwa splątane fotony `czerwone' (788 nm)

λ (nm)	*barwa światła*
650-790	czerwona
610-650	pomarańczowa
580-610	żółta
550-580	żółtozielona
505-550	zielona
485-505	zielononiebieska
440-485	niebieska
415-440	indygowa
380-415	fioletowa

teleporter Pegga i in.



nożyce kwantowe

przykład inżynierii optycznych stanów kwantowych za pomocą teleportacji

Wejście: stan koherentny

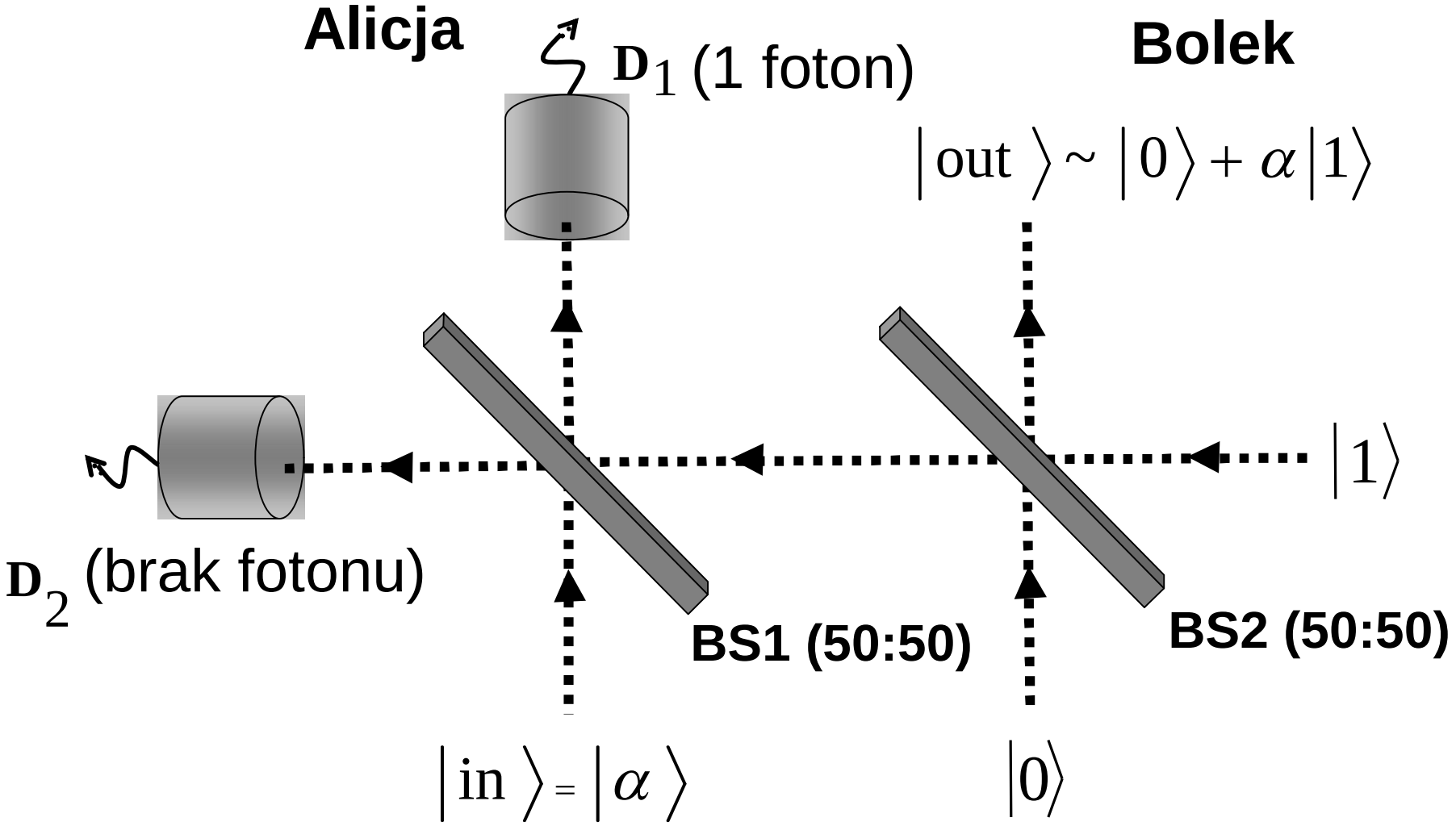
$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

$$= e^{-|\alpha|^2/2} \left\{ |0\rangle + \alpha|1\rangle + \frac{\alpha^2}{\sqrt{2}}|2\rangle + ... \right\}$$

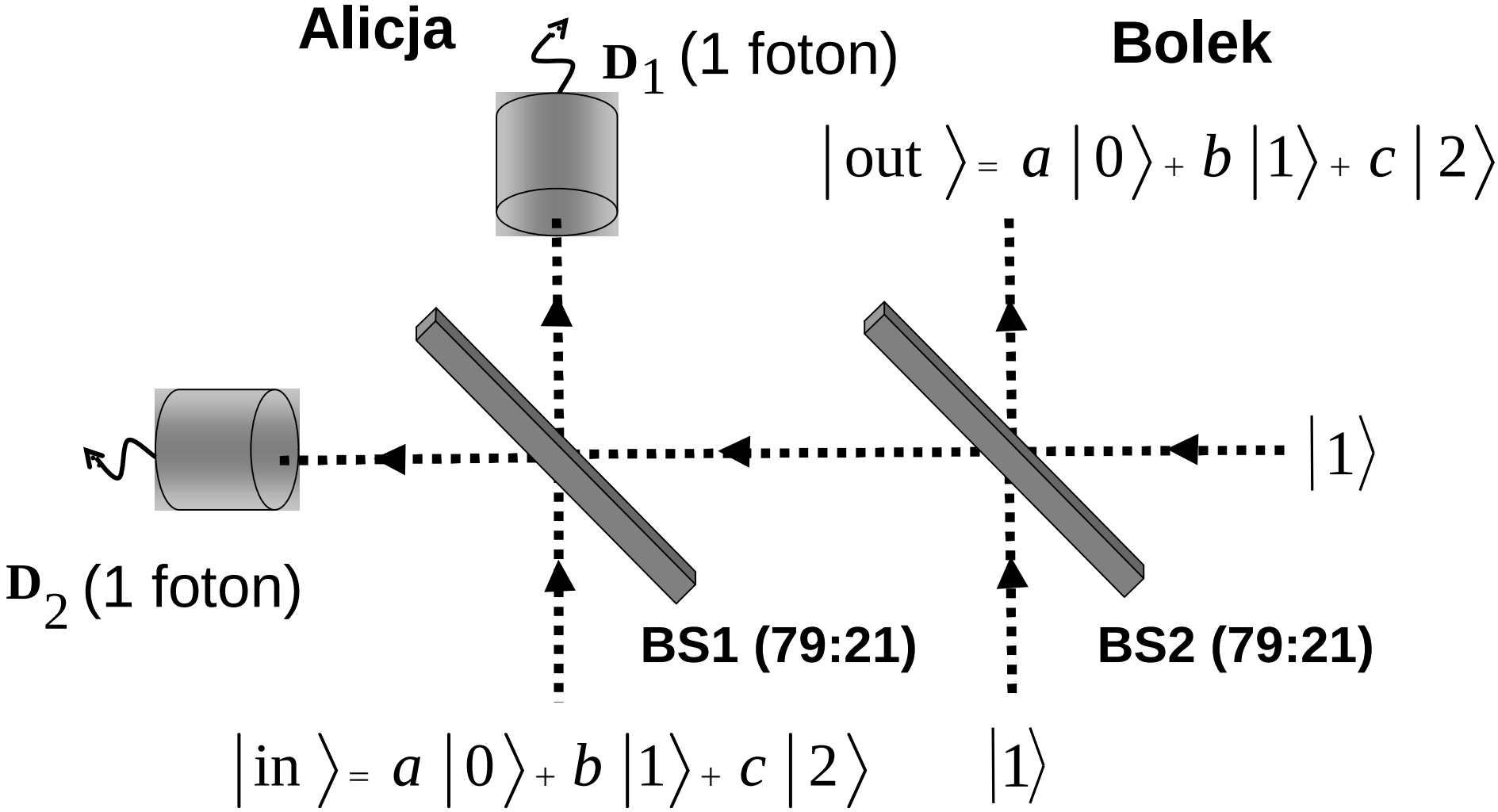
Wyjście: stan kubitowy

$$|\Phi\rangle = N\left(|0\rangle + \alpha|1\rangle\right) \quad \text{gdzie} \quad N = \frac{1}{\sqrt{1+|\alpha|^2}}$$

nożyce kwantowe Pegga i in.

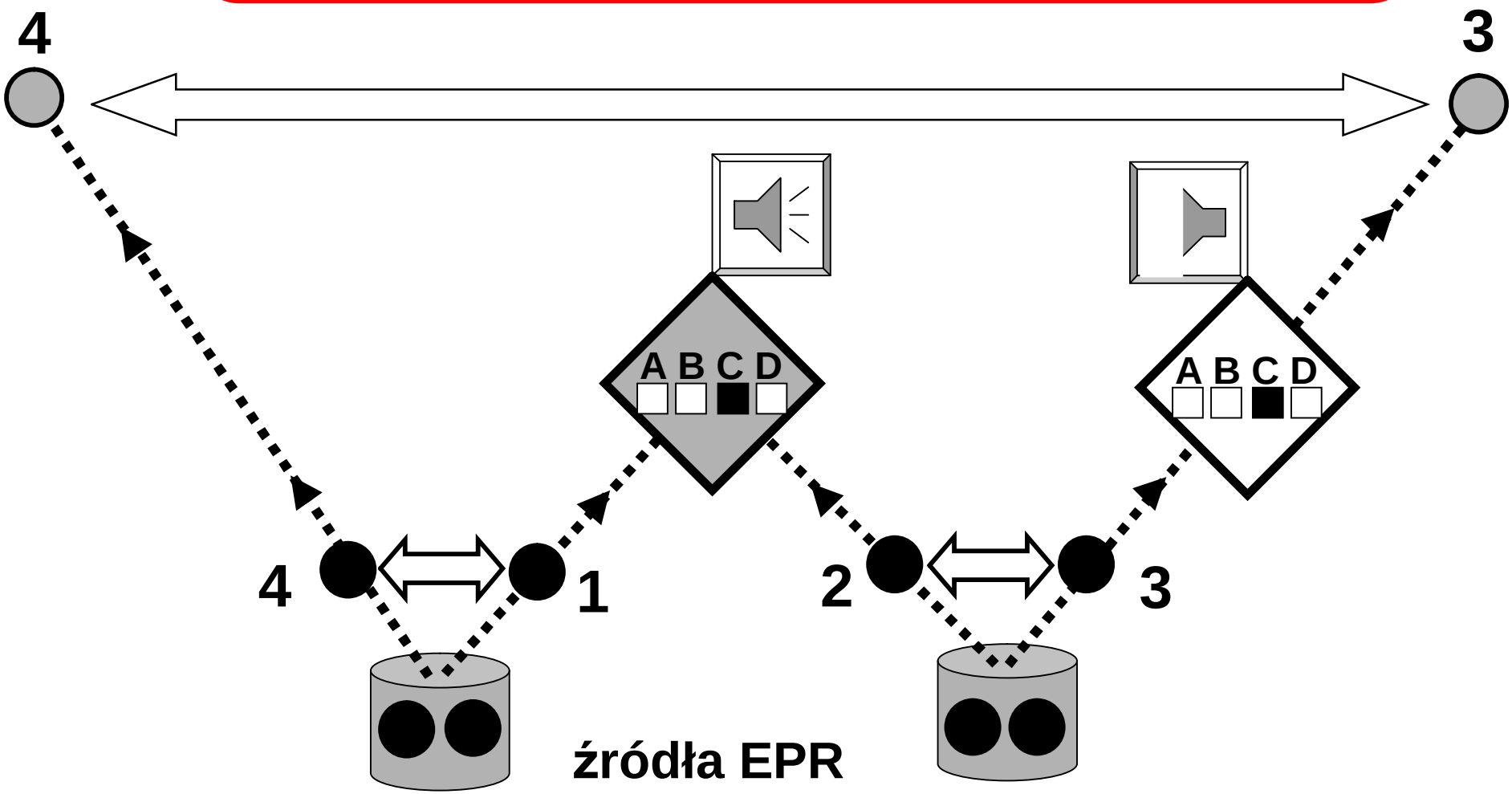


teleportacja kutritów



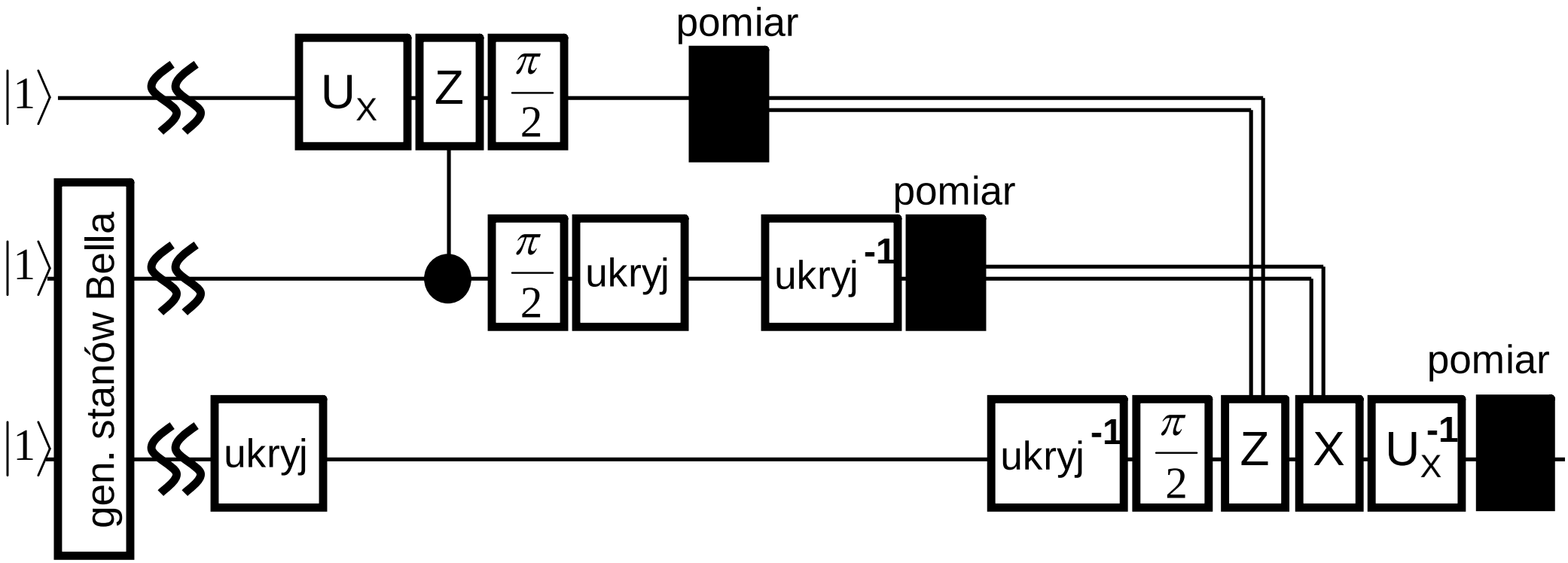
przeniesienie splątania

(entanglement swapping)



deterministyczna teleportacja stanów atomowych

eksperyment Blatta i in. (2004)



eksperyment Blatta i in. (2004)

- 3 jony $^{40}Ca^{+}$

  stany

$$|1\rangle \equiv S_{1/2}(m_J = -1/2)$$

$$|0\rangle \equiv D_{5/2}(m_J = -1/2)$$

$$|H\rangle \equiv D_{5/2}(m_J = -5/2)$$

- $U_x|1\rangle \rightarrow |1\rangle, |0\rangle, \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{i|0\rangle + |1\rangle}{\sqrt{2}}$

- $T_{teleport} = 2\,ms\,, T_{Bell\ .life} = 100\ ms\,, T_{delay} = 10\,ms$

- wierność: (66.7%<) 75% (<87%)

przełomowe odkrycia

T 1935 splątania kwantowe - Schroedinger oraz Einstein, Podolsky i Rosen

T 1982 zakaz klonowania Woottersa-Żurka

T 1993 teleportacja kwantowa - Bennett, Brassard, Crepeau, Jozsa, Peres, Wootters

T 1993 wymiana splątania - Żukowski, Zeilinger, Horne, Ekert

D 1997 optyczna teleportacja kwantowa - Zeilinger i in.

D 1998 bezwarunkowa optyczna teleportacja kwan. - Furusawa, Kimble, Polzik i in.

D 1998 optyczna wymiana splątania - Zeilinger et al..

T 1999 uniwersalne obliczenia kwan. za pomocą teleportacji - Gottesman, Chuang

D 2004 bezwarunkowa teleportacja stanów atomowych
- Barrett, Wineland i in. oraz Riebe, Blatt i in.

T - teoria, D - doświadczenie

Zastosowania teleportacji

- t. człowieka (10^{27} atomów) ? NIE!
- t. wirusa ? NIE
- t. w celu klonowania ? NIE
- t. w komunikacji nadświetlnej ? NIE
- t. w komputerach kwantowych ? TAK!

Chuang: ``*Dopiero zaczynamy rozumieć dlaczego teleportacja jest w ogóle możliwa*''