



# **Jak kwantowe bity dodają** ~~**dwa do dwóch**~~ **jeden do jednego**

**czyli obliczenia kwantowe**

**Jerzy Kamiński**

**Katedra Optyki Kwantowej i Fizyki Atomowej  
Instytut Fizyki Teoretycznej  
Wydział Fizyki Uniwersytetu Warszawskiego**

# PLAN

- Aspekty społeczny, finansowo-gospodarczy i technologiczny
- Fizyczne właściwości informacji
- Mechanika kwantowa i jej dziwne konsekwencje
- Bramki kwantowe
- Kwantowa równoległość obliczeń
- Algorytmy kwantowe
- Procesory kwantowe – czy możliwe ?

# Szyfrowanie kluczem publicznym

Twórcy idei: J. Ellis – W. Brytania (1969)

W. Diffie i M. Hellman – Stany Zjednoczone (1973)

Praktyczna implementacja:

R. A. Rivest (USA), A. Shamir (Izrael)

L. Adleman (USA)

Stąd metoda RSA



Jedna z metod:

rozkład dużych liczb naturalnych na czynniki pierwsze

# RSA

Podstawą algorytmu jest stwierdzenie, że jest bardzo liczb pierwszych oraz rozkład dużej liczby na czynniki pierwsze jest bardzo czasochłonny

$$N \approx \frac{n}{\ln(n)}$$

Jeśli  $n=10^{160}$ , to  $N \approx 3 \cdot 10^{157}$

Gdyby każda liczba pierwsza mniejsza od  $10^{160}$  była zachowana przez jeden atom to nie starczyłoby atomów we Wszechświecie

# Problem RSA160

n=2152741102718889701896015201312825429257773588845675980\\  
1704976767781331452188591356730110597734910596024979071\\  
11585214302079314665202840140619946994927570407753

$$n=p*q$$

p=4542789285848139407168619064973883165613714577846979325\\  
0959984709250004157335359

q=473880906038320161966338323037889519732689229210409579\\  
44741354648812028493909367

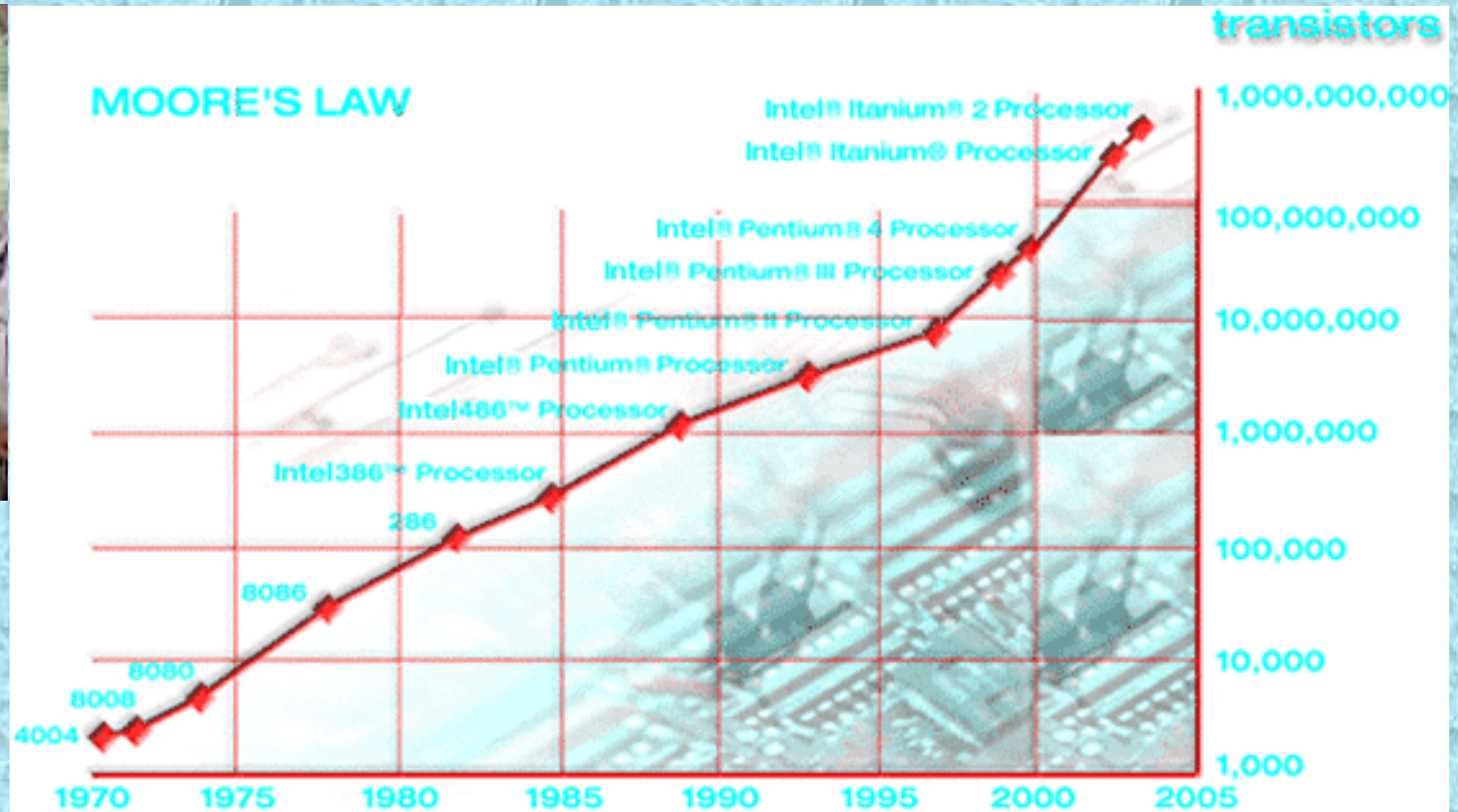
Rozwiązany w 2003 po dwóch tygodniach obliczeń  
na około stu komputerach

# Prawo Moore'a

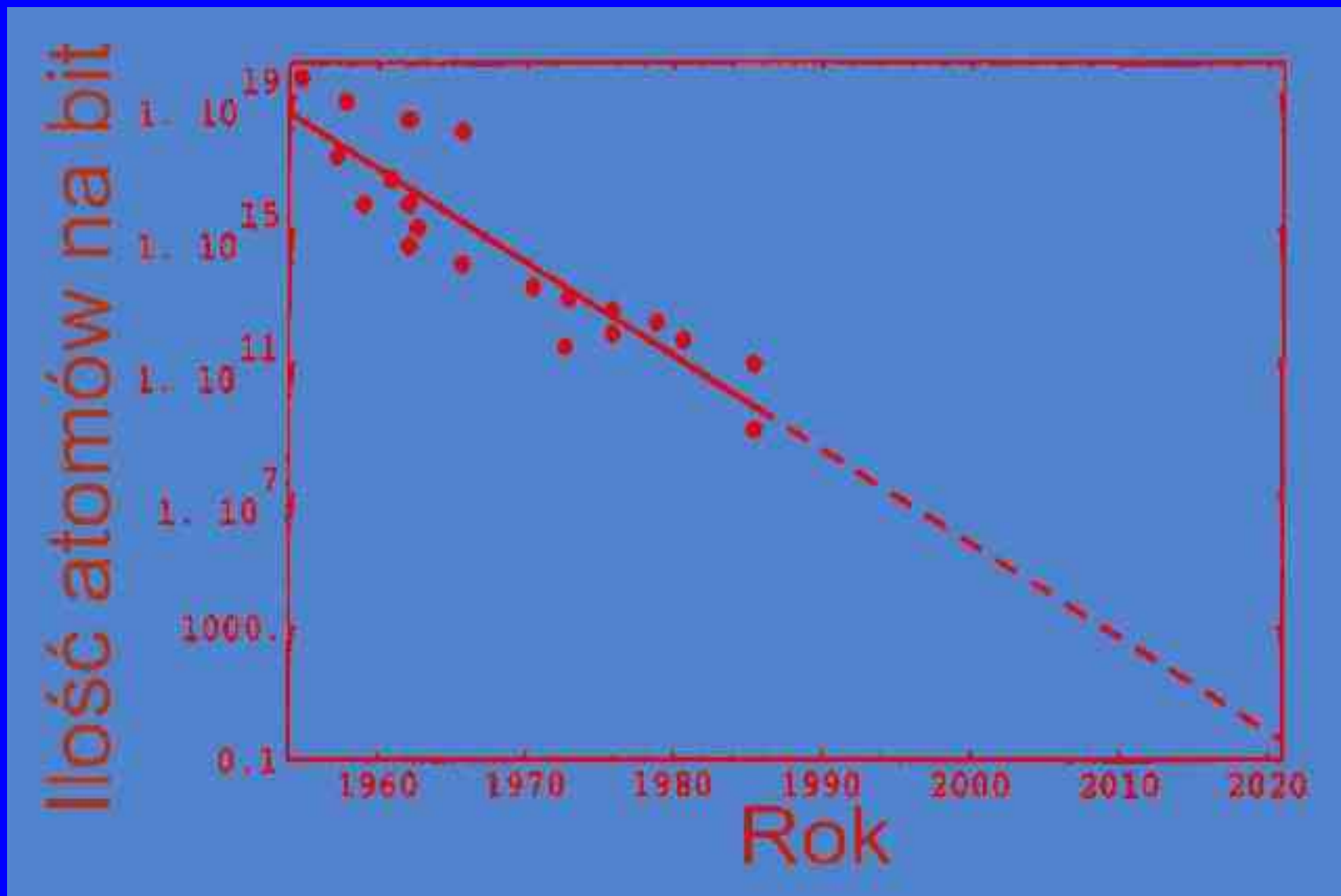
Ilość tranzystorów w układzie scalonym podwaja się w przybliżeniu co dwa lata



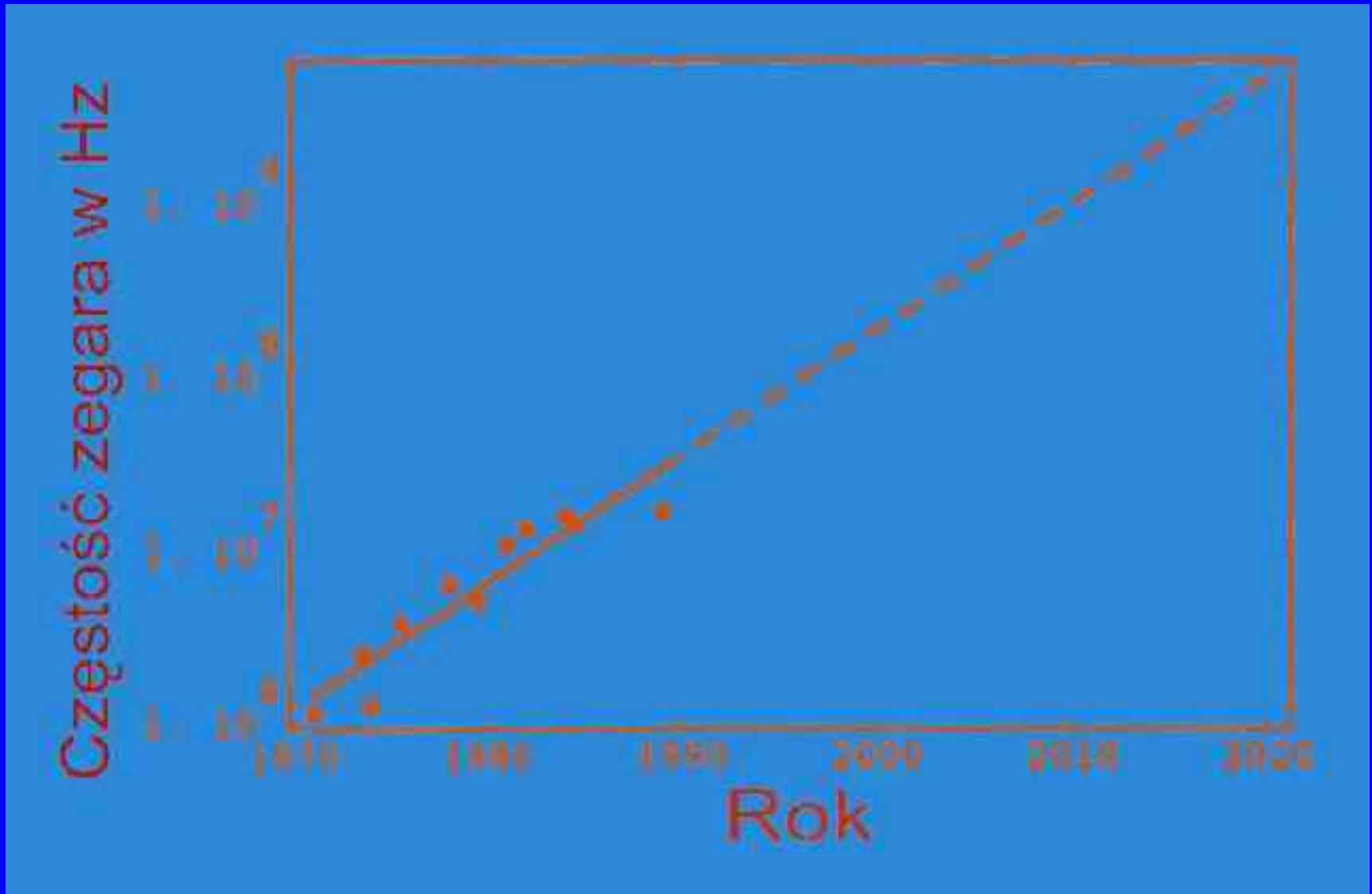
Gordon E. Moore



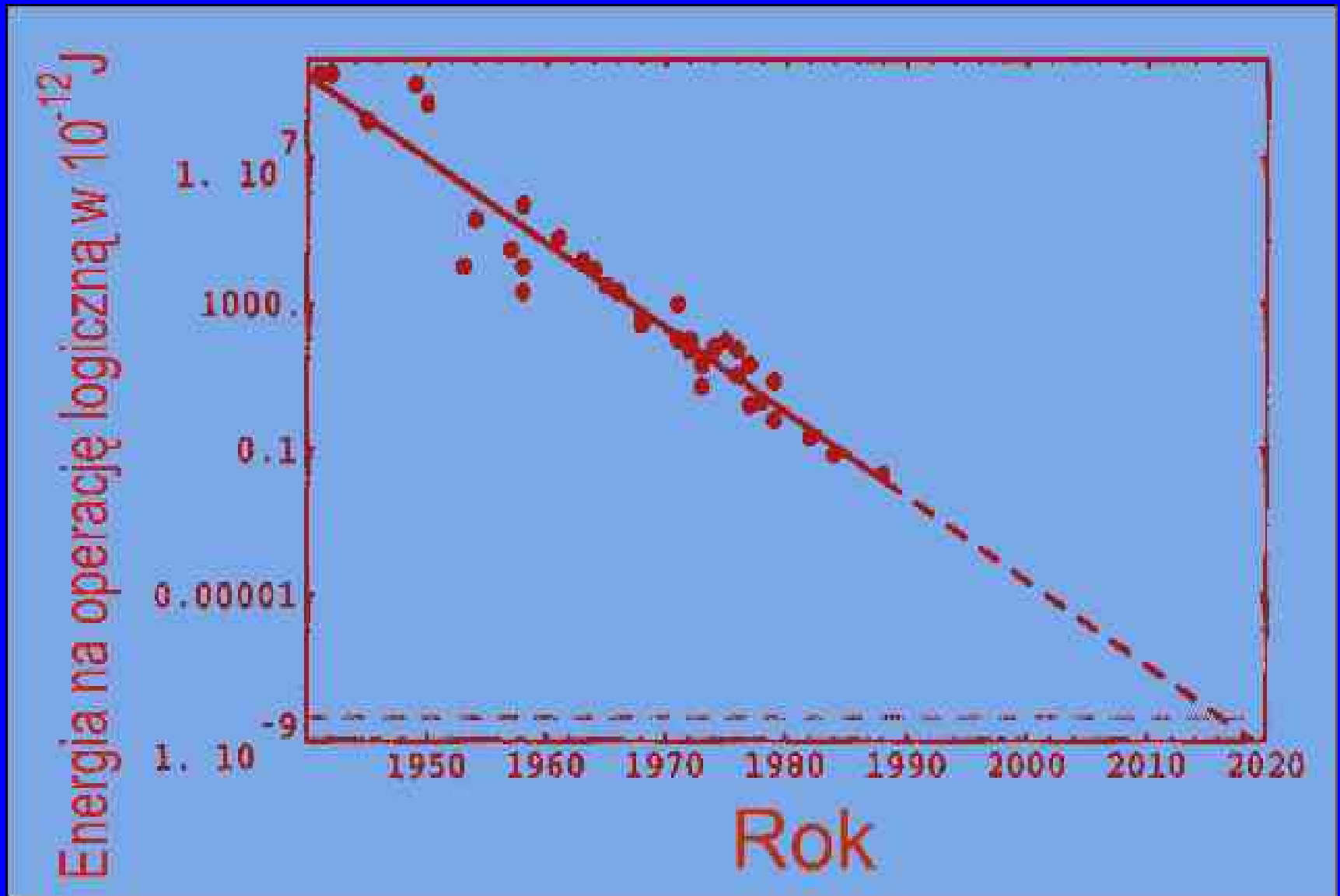
# Oszczędność materiałów



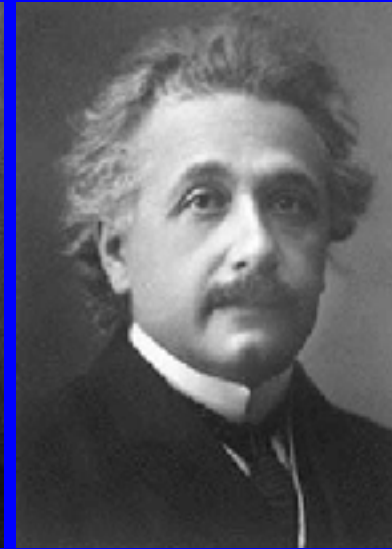
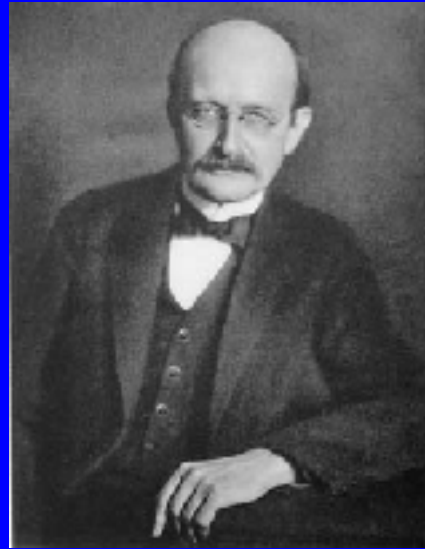
# Oszczędność czasu



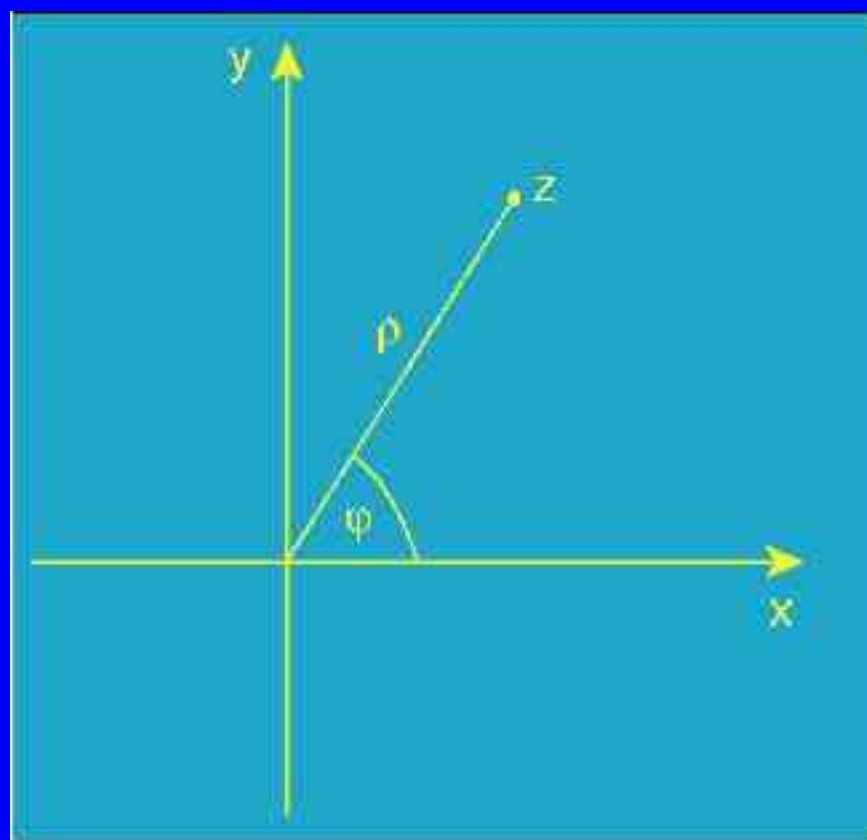
# Oszczędność energii



# Twórcy mechaniki kwantowej



## Liczby zespolone



$$i = \sqrt{-1}$$

$$z = x + iy$$

$$z = \rho(\cos \varphi + i \sin \varphi)$$

$$z = \rho e^{i\varphi}$$

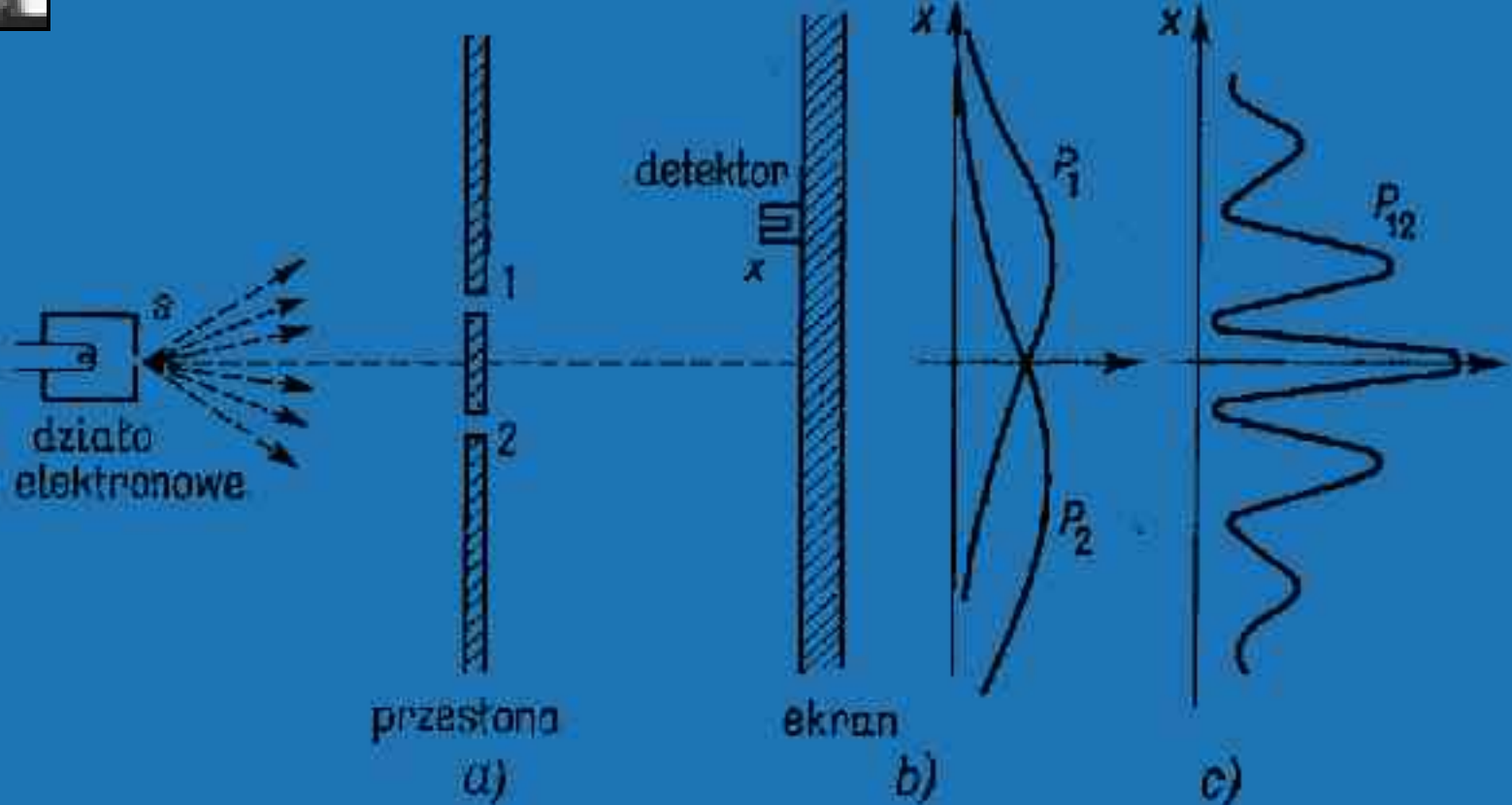
$$|z| = \sqrt{x^2 + y^2} = \rho$$

$$z_1 = \rho_1 e^{i\varphi_1} \text{ oraz } z_2 = \rho_2 e^{i\varphi_2}$$

$$|z_1 + z_2|^2 = \rho_1^2 + \rho_2^2 + 2\rho_1\rho_2 \cos(\varphi_1 - \varphi_2)$$



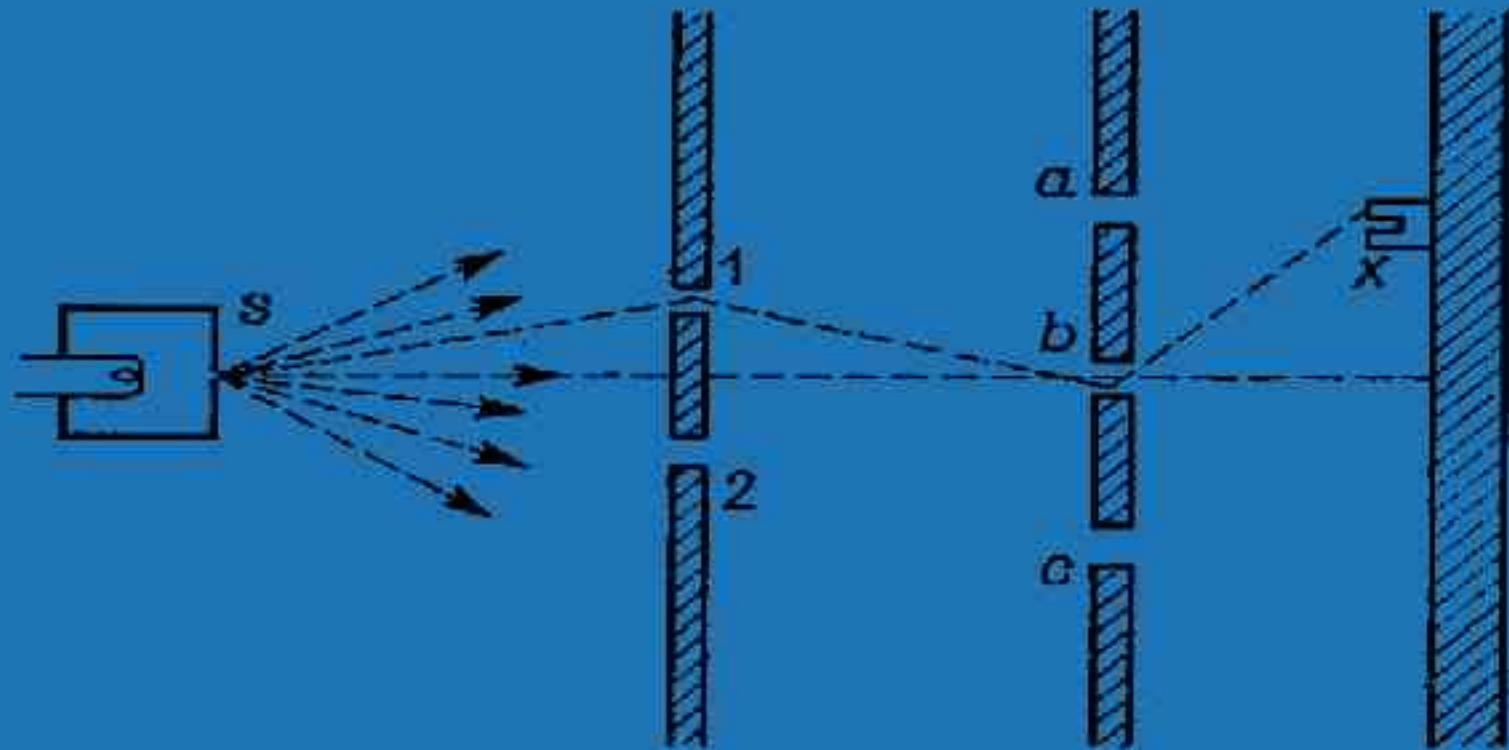
# Interferencja przez dwie szczeliny



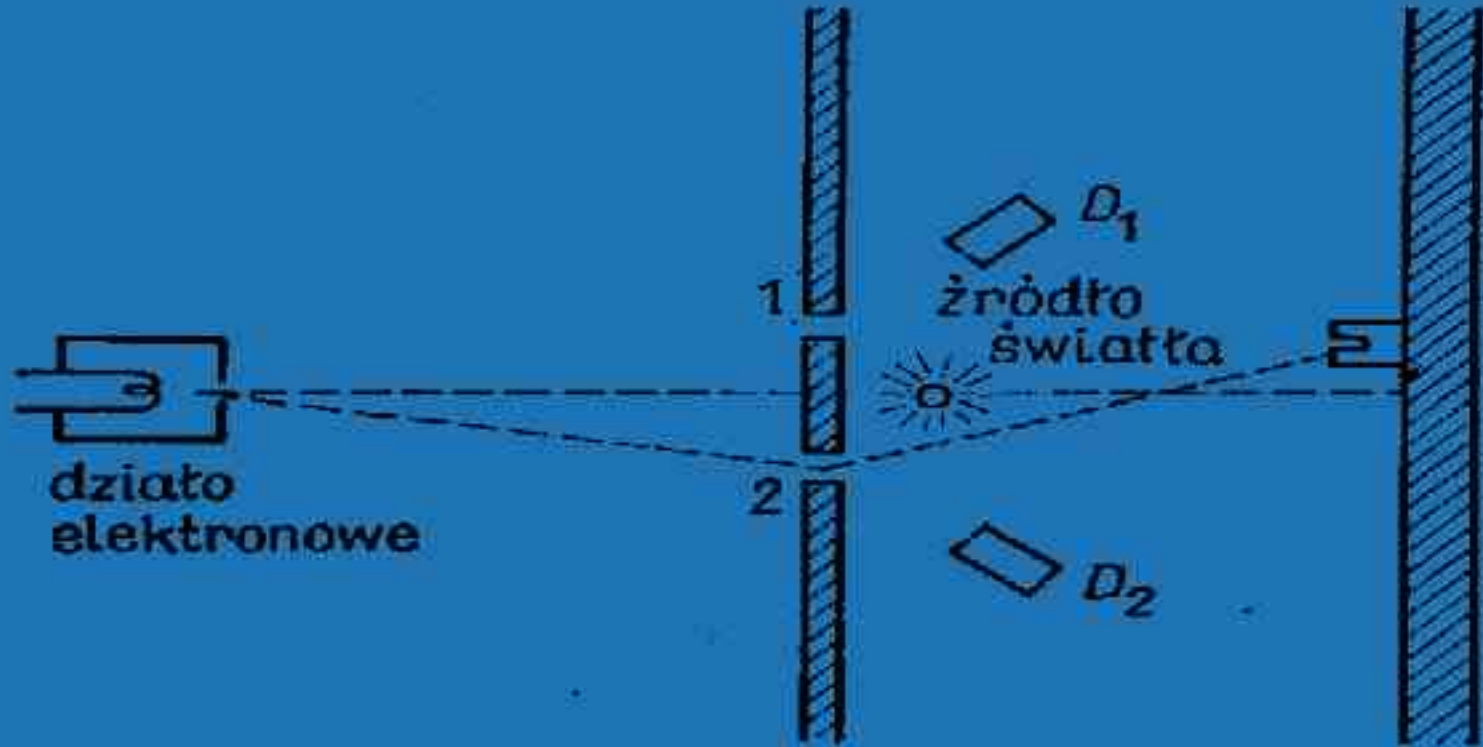
Eksperyment interferencyjny z elektronami

# Interferencja z wieloma drogami

3.2. Bardziej skomplikowany eksperyment interferencyjny



# Interferencja z podglądaniem



3.3. Eksperyment mający na celu określenie przez którą szczelinę przechodzi elektron

# Kubit

Kubitem jest jakikolwiek układ fizyczny, który może znajdować się dwóch stanach:  $|0\rangle$  lub  $|1\rangle$

Może się on znaleźć także w superpozycji tych stanów

$$\alpha|0\rangle + \beta|1\rangle$$

Zespolone liczby  $\alpha$  i  $\beta$  nazywamy amplitudami prawdopodobieństwa

# Dwa kubity i stany splątane

Najprostrzy stan dwu-kubitowy  $|a\rangle \otimes |b\rangle$

Stan splątany  $\alpha|0\rangle \otimes |1\rangle + \beta|1\rangle \otimes |0\rangle$

gdzie  $|\alpha|^2 + |\beta|^2 = 1$

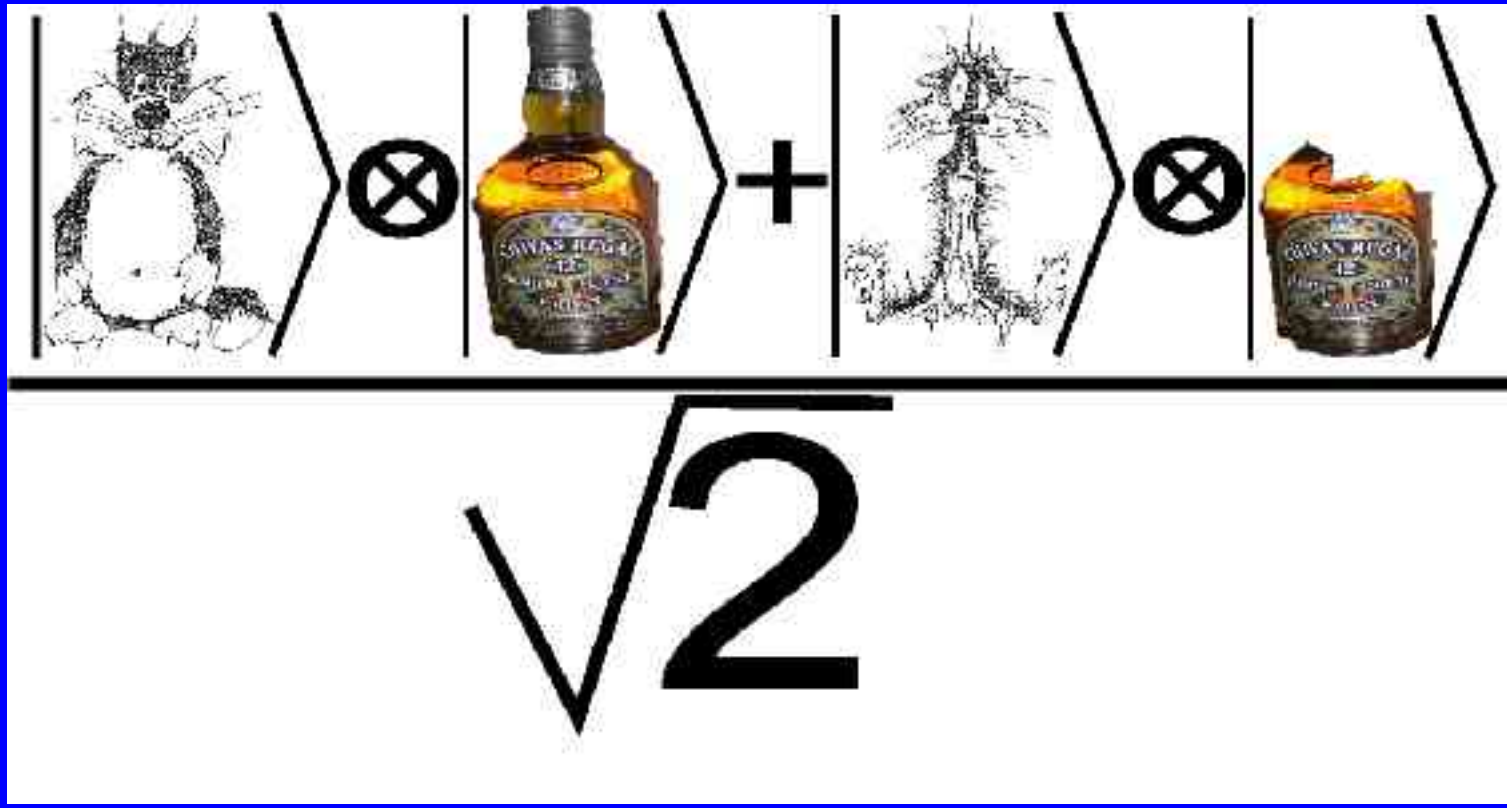
Jeśli  $|\alpha|^2 = |\beta|^2 = \frac{1}{\sqrt{2}}$ , to  
stany te nazywamy  
stanami Bella



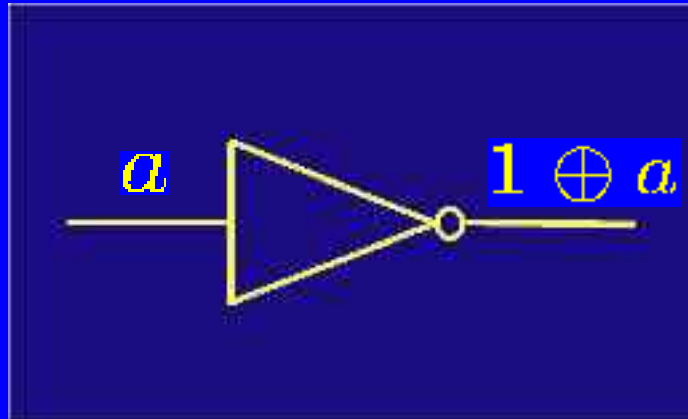
J. Bell



# Kot Schrödingera



# Podstawowe bramki komputera klasycznego



$p$	$q$	$p \text{ lub } q$	$p \oplus q$
0	0	0	0
1	0	1	0
0	1	1	0
1	1	1	1



# System dwójkowy



W systemie dziesiętnym liczbę  
 $2 \times 10^2 + 5 \times 10^1 + 8 \times 10^0$  zapisujemy  
 w skrócie w postaci **258**

W systemie dwójkowym liczbę  
 $1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$   
 zapisujemy w skrócie w postaci **1001**

$$\begin{array}{c|cc}
 + & 0 & 1 \\
 \hline
 0 & 0 & 1 \\
 1 & 1 & 0
 \end{array} \Rightarrow a \oplus b$$

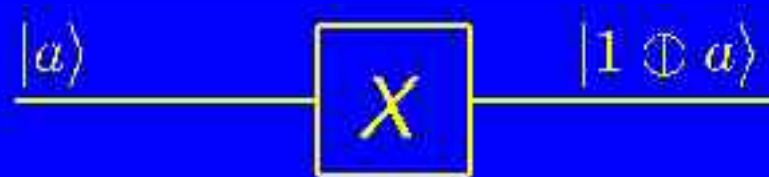
$$\begin{array}{c|cc}
 \times & 0 & 1 \\
 \hline
 0 & 0 & 0 \\
 1 & 0 & 1
 \end{array}$$



# Bramki jedno-kubitowe

Bramka zaprzeczenie NOT:  $0 \Rightarrow 1$   $1 \Rightarrow 0$

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$



Bramka fazy

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$$



Bramka Hadamarda: ze stanów 0 lub 1 generuje ich superpozycję

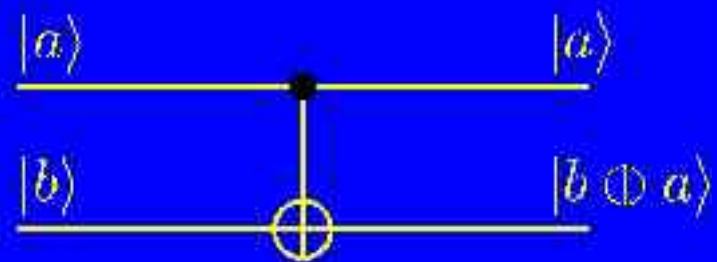
$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



# Bramki dwu-kubitowe

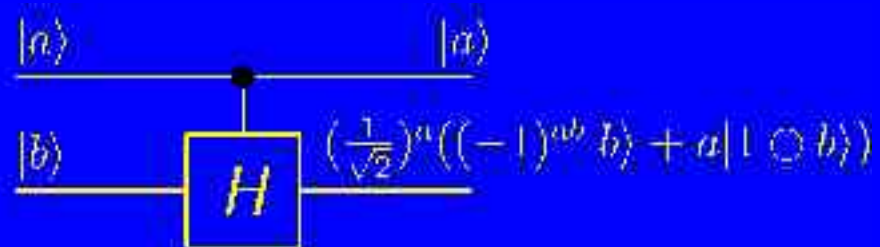
## Sterowane zaprzeczenie

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



## Sterowana bramka Hadamarda

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 0 & 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix}$$



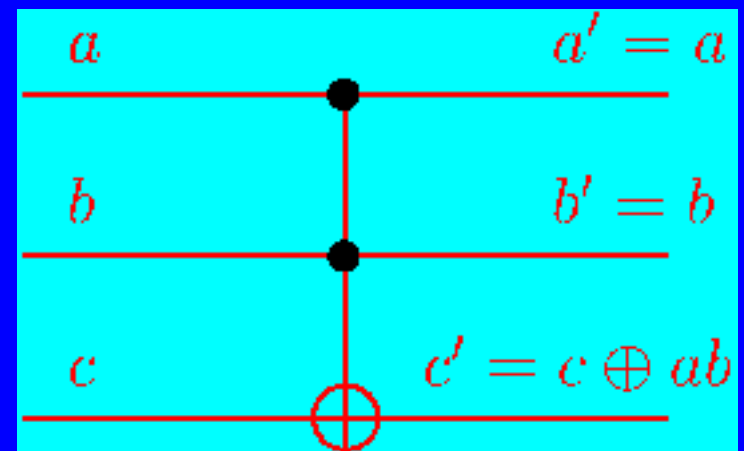
# Bramki trzy-kubitowe

## Bramka Toffoli'ego

Tablica prawdy

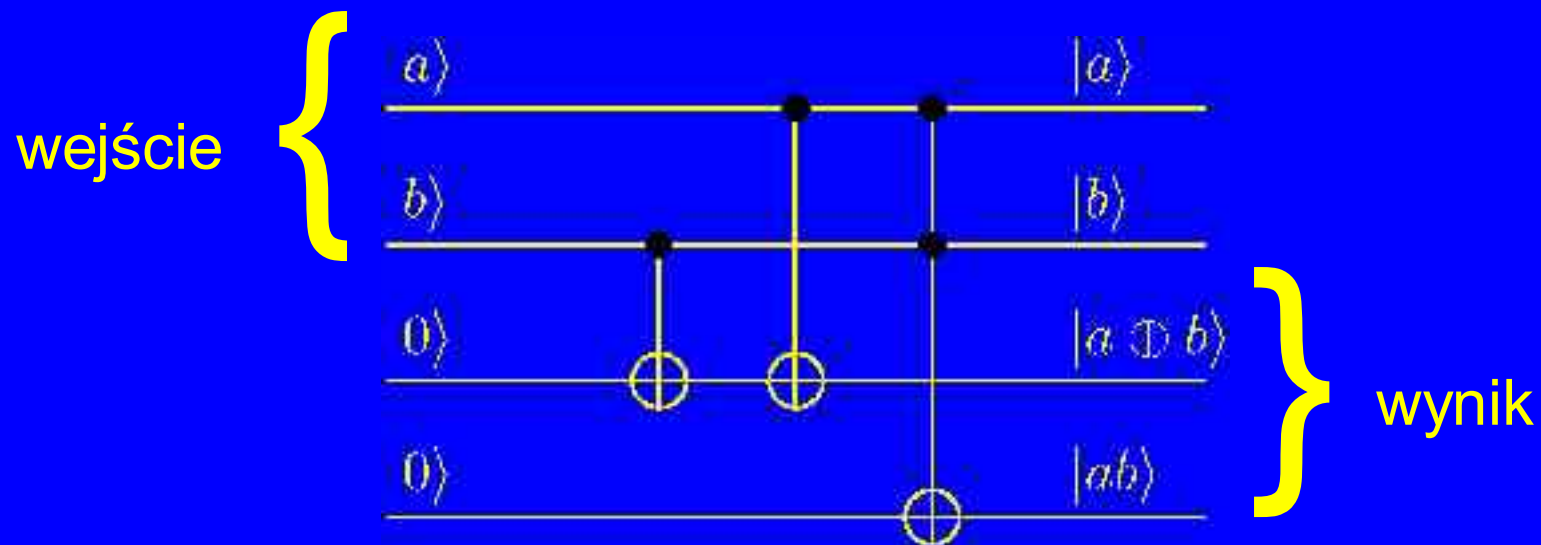
wejście			wyjście		
$a$	$b$	$c$	$a'$	$b'$	$c'$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Przedstawienie graficzne



Z wielu takich bramek można zbudować komputer wykonujący dowolne obliczenie

# Bramka dodająca dwa kubity



$$|0\rangle \otimes |0\rangle \otimes |b\rangle \otimes |a\rangle \Rightarrow |ab\rangle \otimes |a \oplus b\rangle \otimes |b\rangle \otimes |a\rangle$$

$$00\ 00 \Rightarrow 00\ 00 \text{ czyli } 0+0=0$$

$$00\ 01 \Rightarrow 01\ 01 \text{ czyli } 1+0=1$$

$$00\ 10 \Rightarrow 01\ 10 \text{ czyli } 0+1=1$$

$$00\ 11 \Rightarrow 10\ 11 \text{ czyli } 1+1=2$$

# Równoległość obliczeń kwantowych

$$|0\rangle \otimes |0\rangle \otimes \left( \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right) \otimes \left( \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \right)$$



$$\frac{1}{2} \left( |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle \otimes |1\rangle \otimes |0\rangle \right. \\ \left. + |0\rangle \otimes |1\rangle \otimes |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle \otimes |1\rangle \otimes |1\rangle \right)$$

# Algorytmy kwantowe



P. Shor

Odkrywca kwantowego algorytmu rozkładu na czynniki pierwsze bardzo dużych liczb naturalnych

**Zastosowanie:** łamanie szyfrów z kluczem publicznym



L. Grover

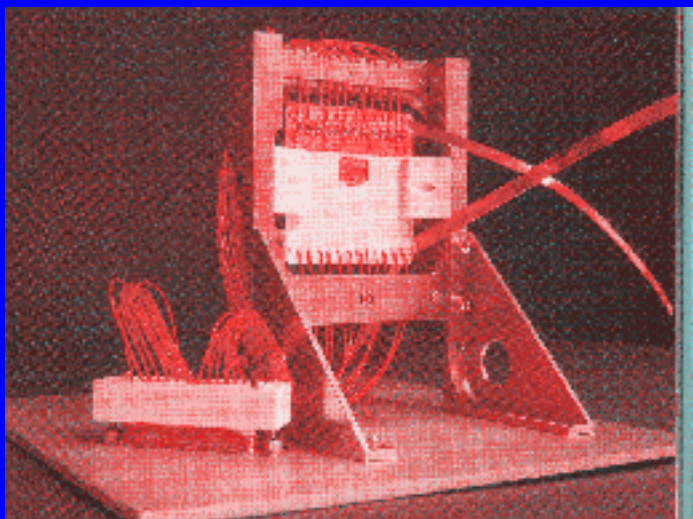
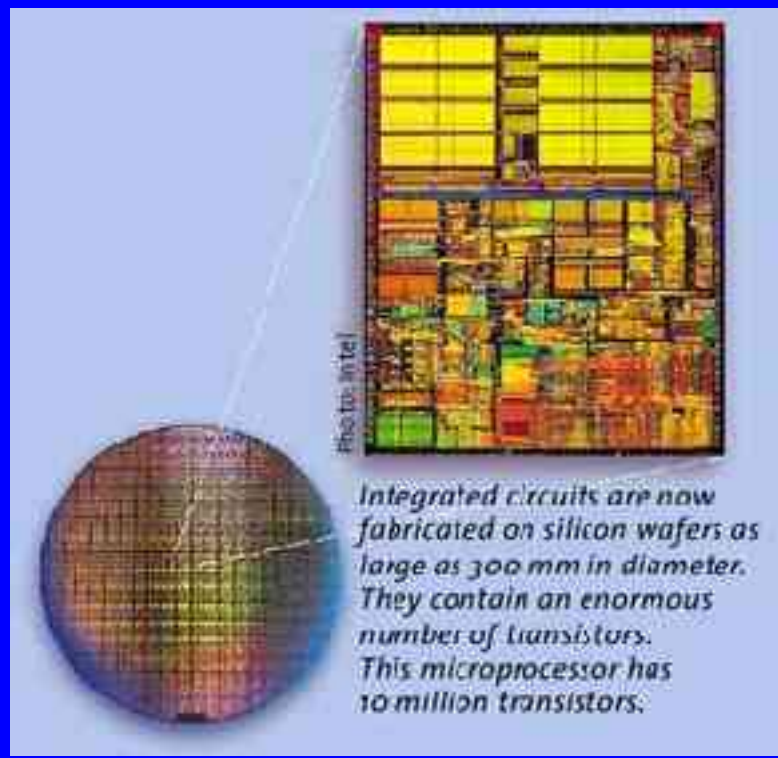
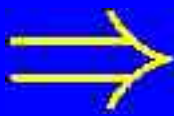
Odkrywca kwantowego algorytmu sortowania i wyszukiwania

**Zastosowania:** łamanie szyfrów z kluczem symetrycznym



# Procesory

## klasyczny



## kwantowy



# Oszczędność materiałów I





# Kot Schrödingera



---

$$\sqrt{2}$$