

CZY JEST MOŻLIWE PRZETWARZANIE INFORMACJI BEZ ZUŻYCIA ENERGII?

dr inż. Andrzej Skorupski
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Zasilanie urządzeń cyfrowych

- ▣ Zasilacz pierwszego polskiego komputera UMC1 produkowanego seryjnie w ELWRO opracowanego w katedrze kierowanej przez prof. Kilińskiego ważył ponad 100kg
- ▣ Zasilanie współczesnych mobilnych urządzeń cyfrowych waży kilka gramów

Granice miniaturyzacji

- ▣ Technologie półprzewodnikowe wkrótce osiągną granice swojej stosowności
- ▣ Pierwsze scalone układy cyfrowe zawierały kilkanaście tranzystorów, współcześnie produkowane układy zawierają kilkanaście milionów tranzystorów

Układy VLSI

- ▣ Układ scalony procesora pobiera ok. 10W, układy VLSI (FPGA-CPLD) pobierają ok. 0.5W
- ▣ Trudności połączeń układów scalonych prowadzą w kierunku budowy systemów jednoukładowych

Oszczędność energii

- ▣ Zmniejszenie napięcia zasilania do 1.5V
- ▣ Zwiększenie pojemności baterii do 1.5Ah
- ▣ Zastosowanie trybu pracy oszczędzania

Poszukiwania nowych technologii

- ▣ Przerzucenie wiele funkcjonalności na oprogramowanie
- ▣ Zwiększanie pojemności pamięci wraz ze zmniejszeniem poboru mocy
- ▣ Poszukiwanie alternatywnych implementacji układów cyfrowych

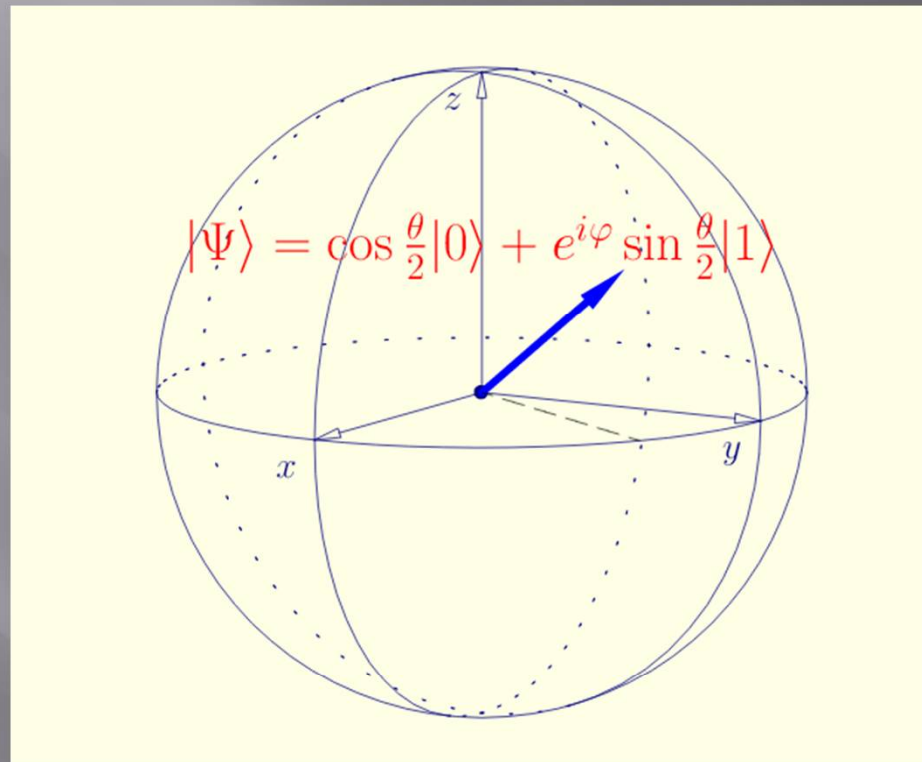
Układy cyfrowe przyszłości

Jeśli obecny trend w miniaturyzacji układów scalonych się utrzyma, to około roku 2020 jeden bit będzie reprezentowany przez jeden atom

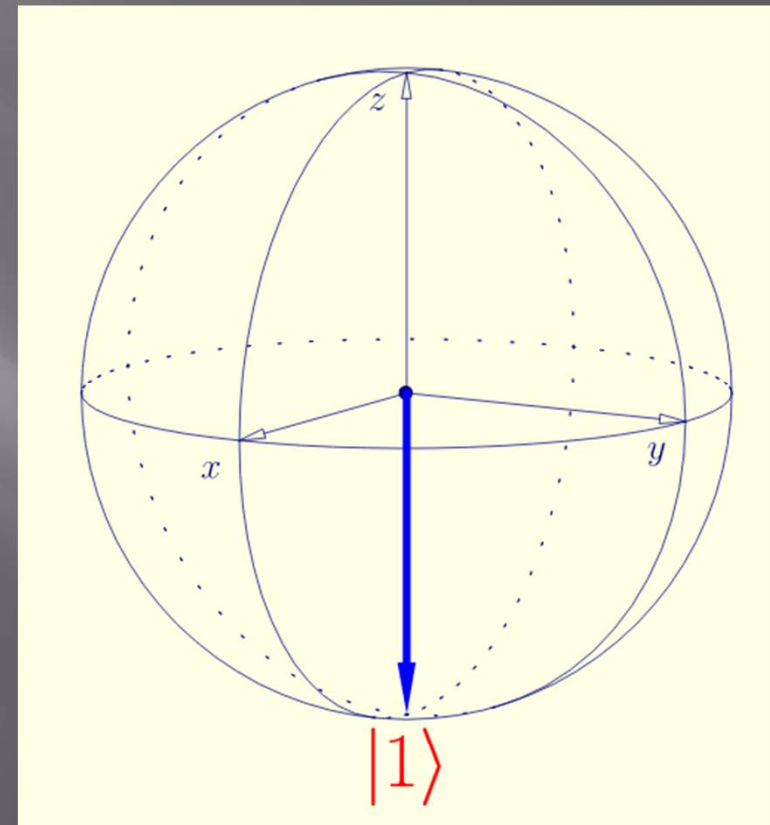
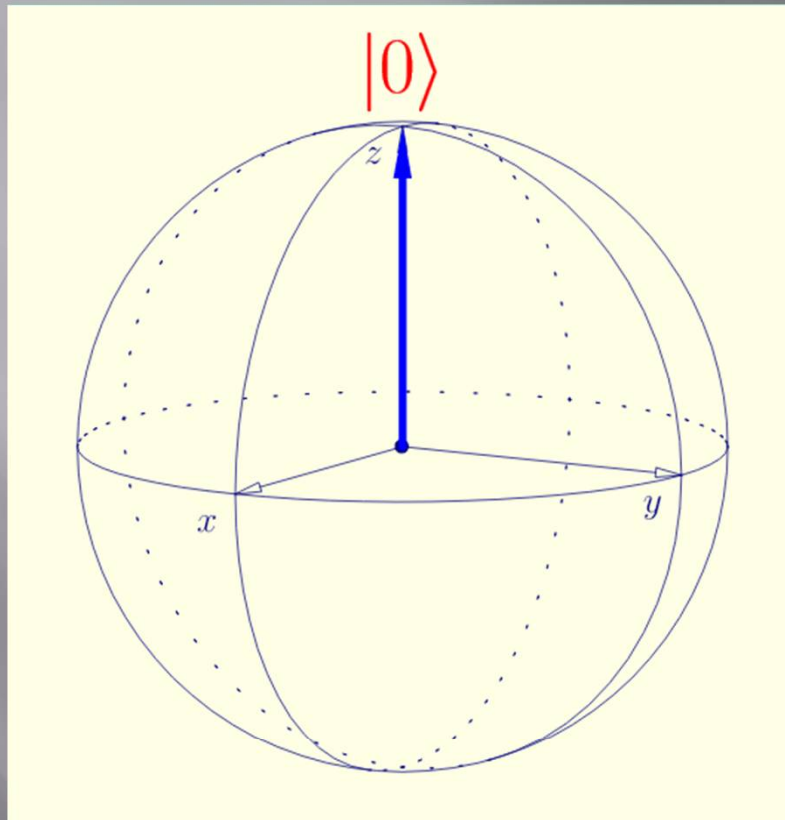
Technologia kwantowa

- ▣ Współczesne bramki logiczne realizują funkcje boolowskie czyli zero-jedynkowe
- ▣ Bramki kwantowe wykorzystują prawdopodobieństwo pojawienie się „0” lub „1”
- ▣ Z zasady Heisenberga wynika, że nie ma możliwości nieskończenie dokładnego pomiaru jednocześnie położenia i pędu cząstki

Położenie elektronu



Prawdopodobieństwo położenia elektronu



Bramki kwantowe

- ▣ Elementarnym nośnikiem kwantowej informacji w informatyce kwantowej jest kubit, tj. kwantowy odpowiednik bitu
- ▣ W najbardziej popularnym modelu kwantowego przetwarzania informacji, operacje na kubitach wykonywane są za pomocą bramek kwantowych
(jak zrobić bramkę?)

Prawo Landauera

Rolf Landauer (1961) wykazał, że strata (?) informacji jest procesem dyssypacyjnym, tj. w czasie „usuwania” informacji jest wydzielana pewna ilość ciepła

Ilość energii tracona podczas straty jednego bitu

- ▣ „Wymazanie” jednego bitu
powoduje wydzielenie energii:
 $kT \ln(2) = 3 \times 10^{-21} \text{J}$ w temp. 300K
- ▣ Jest to tzw. granica Landauera
(Landauer bound, Landauer limit)

Konsekwencja praw Landauera

Uniknięcie „strat” informacji spowoduje, że nie będzie wzrostu ciepła układu, entropia układu pozostanie wartością stałą

Uniknięcia „strat” informacji można zapewnić w procesach odwracalnych

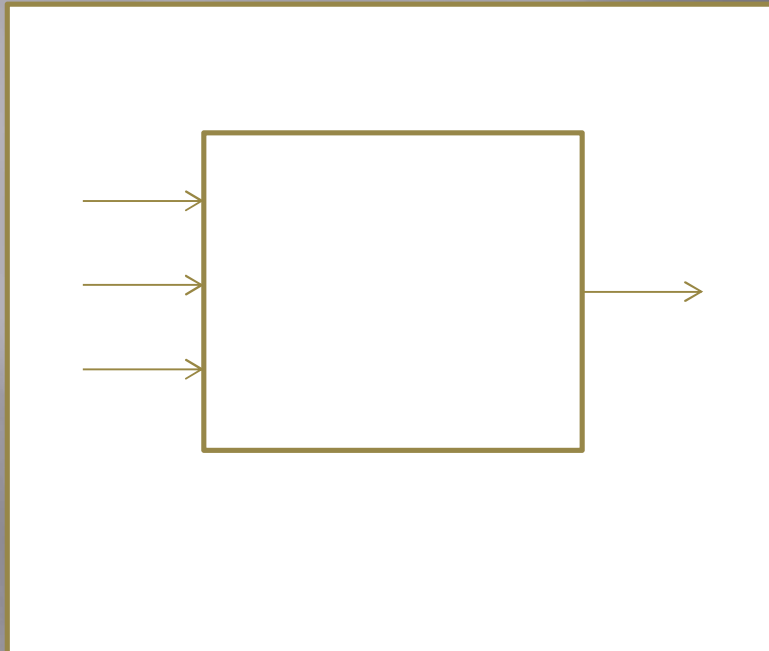
Proces odwracalny realizują układy odwracalne, tj. takie, w których na podstawie sygnałów wyjściowych da się odtworzyć sygnały wejściowe

Układy odwracalne

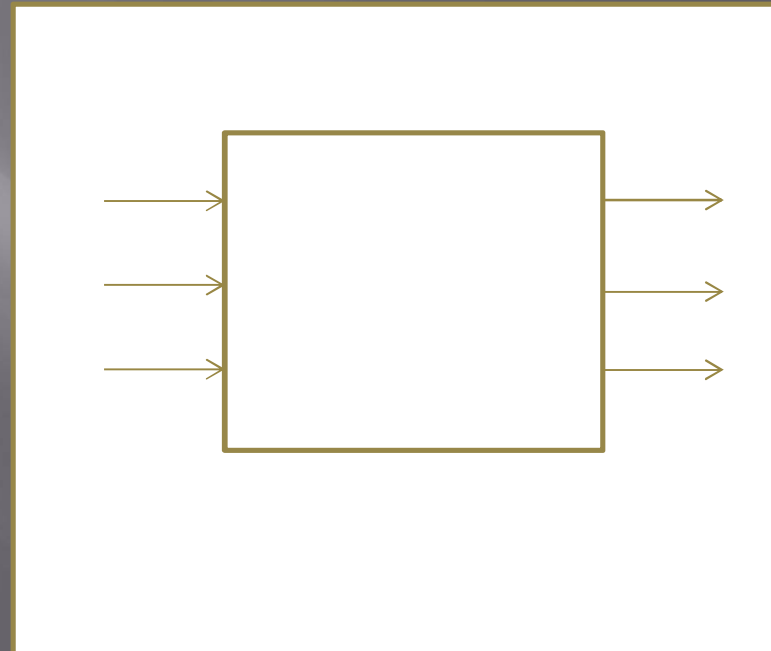
- ▣ Projektując układy odwracalne można spodziewać się, że nie będzie strat ciepła, a zatem poboru energii
- ▣ Jak zbudować (fizycznie i logicznie) bramkę odwracalną?

Porównanie układów

Układ nieodwracalny



Układ odwracalny



Warunki odwracalności

Każdemu z 2^n zerojedynkowych wektorów wejściowych odpowiada inny wektor wyjściowy (odwzorowanie wzajemnie jednoznaczne)

Każda z tych n funkcji składowych jest tzw. funkcją boolowską zrównoważoną, tj. dla 2^{n-1} wektorów wejściowych przyjmuje wartość „1” i dla pozostałych 2^{n-1} wektorów wejściowych przyjmuje wartość „0”

Przykładowa funkcja odwracalna

L.p.	wektor wejściowy $x_2x_1x_0$	wektor wyjściowy $y_2y_1y_0$
0	000	000
1	001	011
2	010	001
3	011	111
4	100	100
5	101	010
6	110	110
7	111	101

Liczba funkcji odwracalnych

Funkcja odwracalna odpowiada permutacji na zbiorze 2^n wektorów binarnych, więc dla n zmiennych istnieje $2^n!$ różnych funkcji odwracalnych

Dla $n=2$ liczba funkcji wynosi 24

Dla $n=3$ liczba funkcji wynosi 40320

Dla $n=4$ liczba funkcji wynosi 20×10^{12}

Dla $n=5$ liczba funkcji wynosi

Projektowanie układów odwracalnych

- ▣ Można zaprojektować trzy funkcje boolowskie za pomocą klasycznych bramek czyli bramek nieodwracalnych
- ▣ Wykorzystując koncepcję bramek kwantowych można przyjąć inny zestaw bramek

Bramki

Dowolną funkcję odwracalną można zbudować z bramek Toffoli'ego (XOR i AND)

Popularny zestaw bramek to 3 bramki NCT:

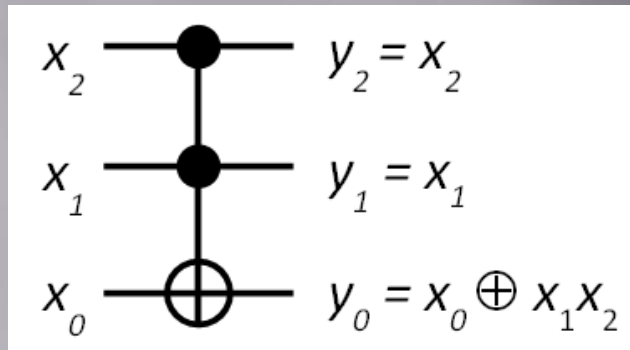
N – bramka negacji

C – bramka sterowana

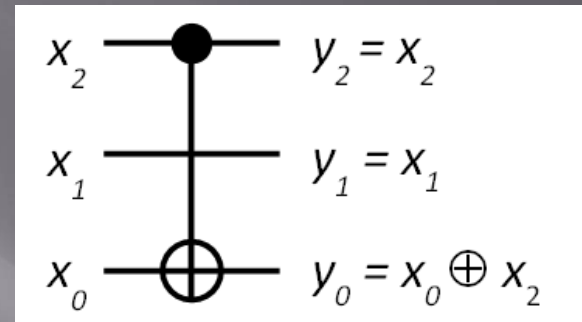
T – bramka Toffoli

Bramki odwracalne T C N

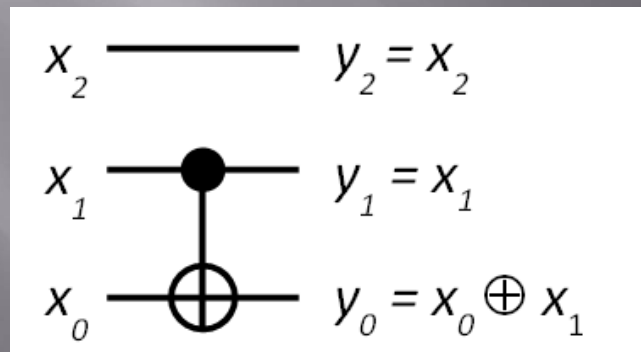
Bramka T



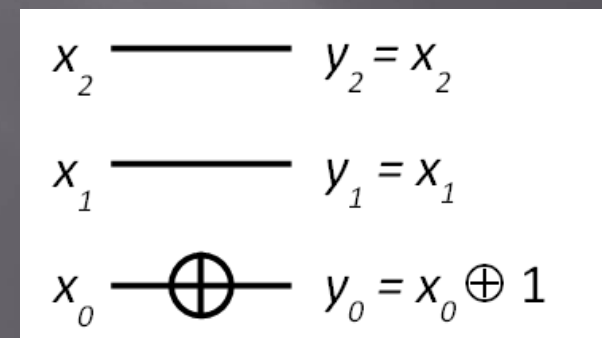
Bramka C(x_2)



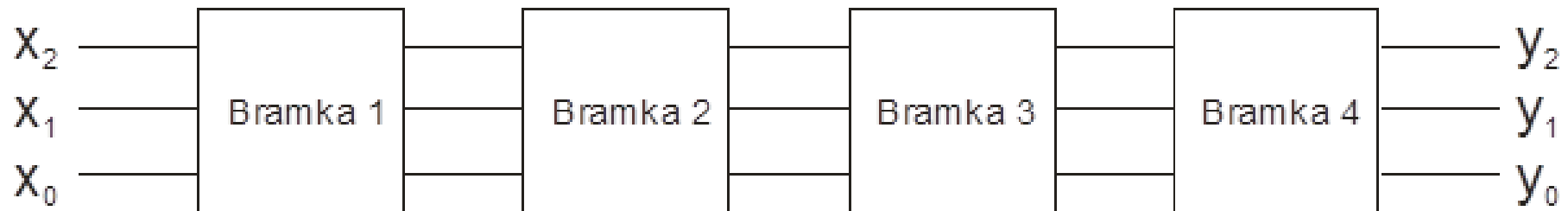
Bramka C(x_1)



Bramka N



Realizacje funkcji - kaskada bramek



Dowolną funkcję odwracalną można zrealizować za pomocą kaskady bramek NCT

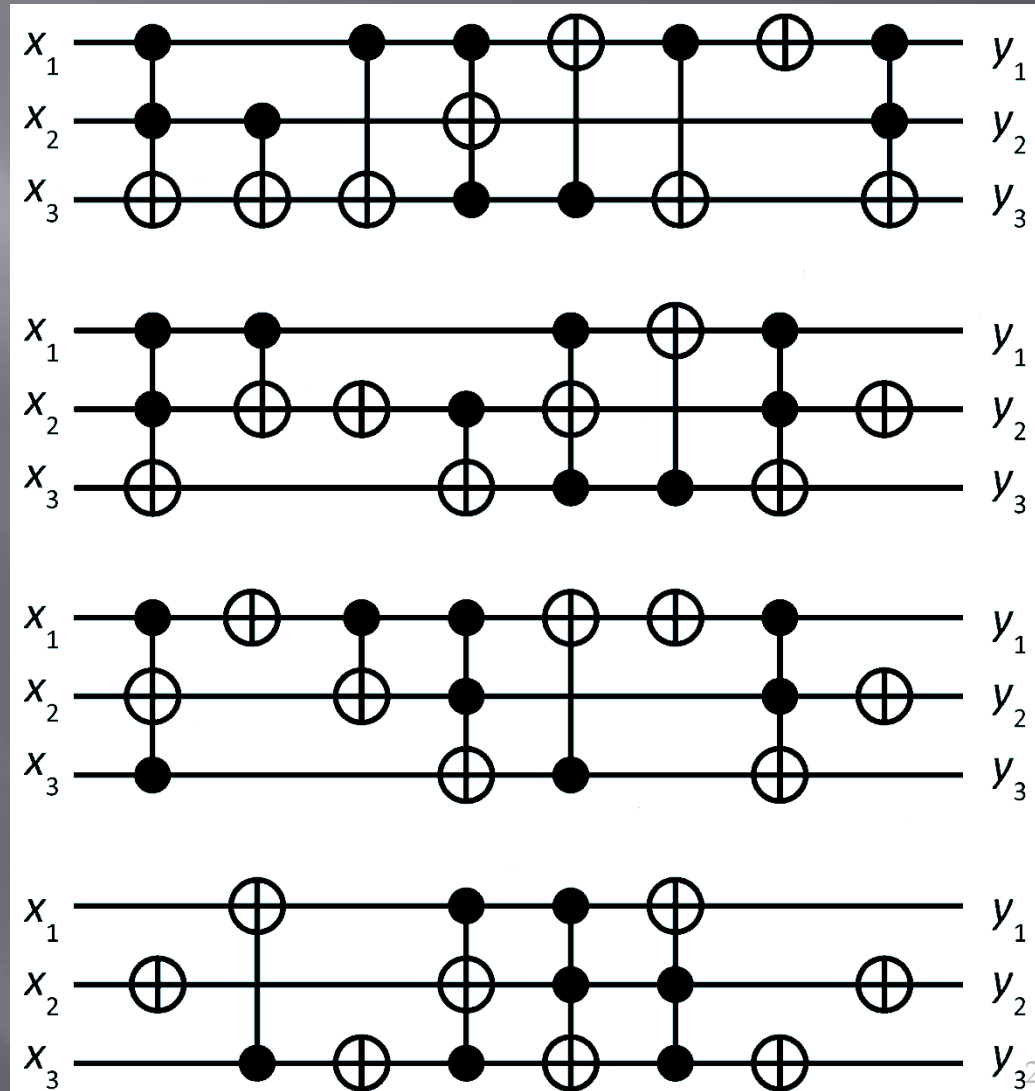
Optymalizacja rozwiązań

Rozwiązania optymalne (składające się z najmniejszej liczby bramek) dla 3 zmiennych są:
co najwyżej ośmiobramkowe

Rozwiązania optymalne dla 4 zmiennych są:
co najwyżej piętnastobramkowe

Cztery optymalne rozwiązania składające się z kaskady 8 bramek

x_3	x_2	x_1	y_3	y_2	y_1
0	0	0	0	0	1
0	0	1	1	0	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	0	0	0
1	0	1	1	1	0
1	1	0	1	0	0
1	1	1	0	1	1



Fizyczne realizacje bramek odwracalnych

- ▣ Bramki półprzewodnikowe
- ▣ Bramki NMR
- ▣ Bramki ION trap
- ▣ Bramki Quantum dots
- ▣ Bramki Optical lattices

Technologia półprzewodnikowa YBS

Realizacja bramek odwracalnych bazuje na technologii YBS (Y-branch switch)

Technologia wykorzystuje własności bardzo czystych półprzewodników

Ruch elektronów

Elektrony napotykają na swojej drodze różne przeszkody, które zmieniają kierunek jego ruchu

Przeszkody to:

- ▣ Defekty siatki
- ▣ Zanieczyszczenia
- ▣ Phonony – pseudocząsteczki (wibracje siatki)

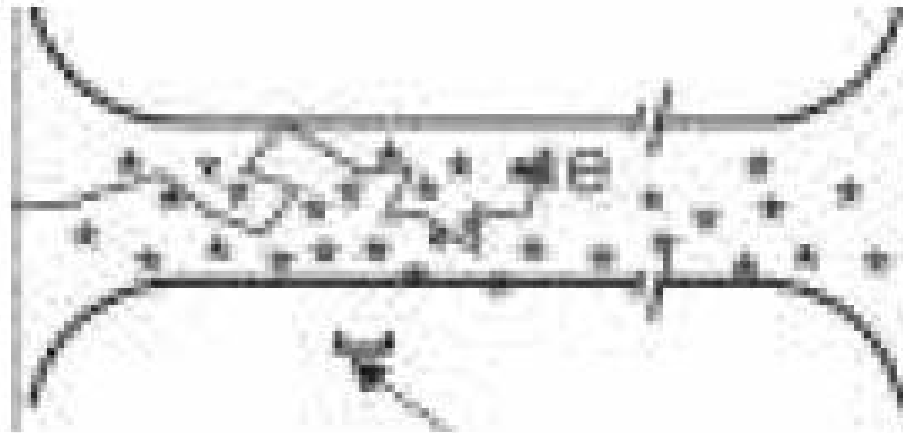
Średnia droga elektronu

Statystyczna średnia długość prostych odcinków jest zwana średnią swobodną drogą elektronu

W środowisku krzemu droga ta wynosi 5-10 nm

W środowisku wysokiej jakości półprzewodników (GaAs) dochodzi do 100-200 nm

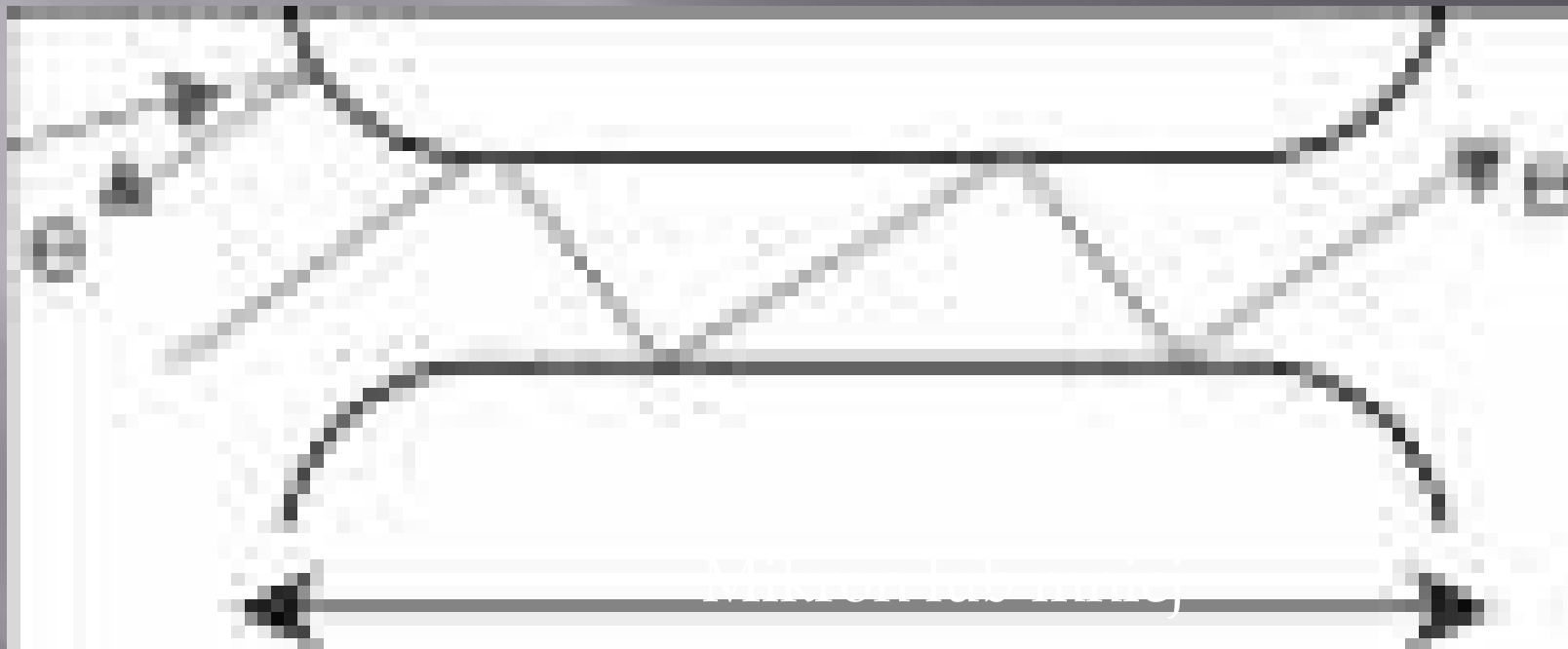
Makroskopowy przepływ elektronów



Scattering length

Fig. 1. Electron transport in macroscopic devices

Mesoskopowy przepływ elektronów



ok. 1 μm

Przepływ balistyczny

Przepływ elektronów w przyrządach, w których zderzenia elektronów następują o ścianki przyrządu jest nazywany przepływem balistycznym.

Przepływ taki pozwala na pracę w zakresie teraherców.

Prostownik balistyczny

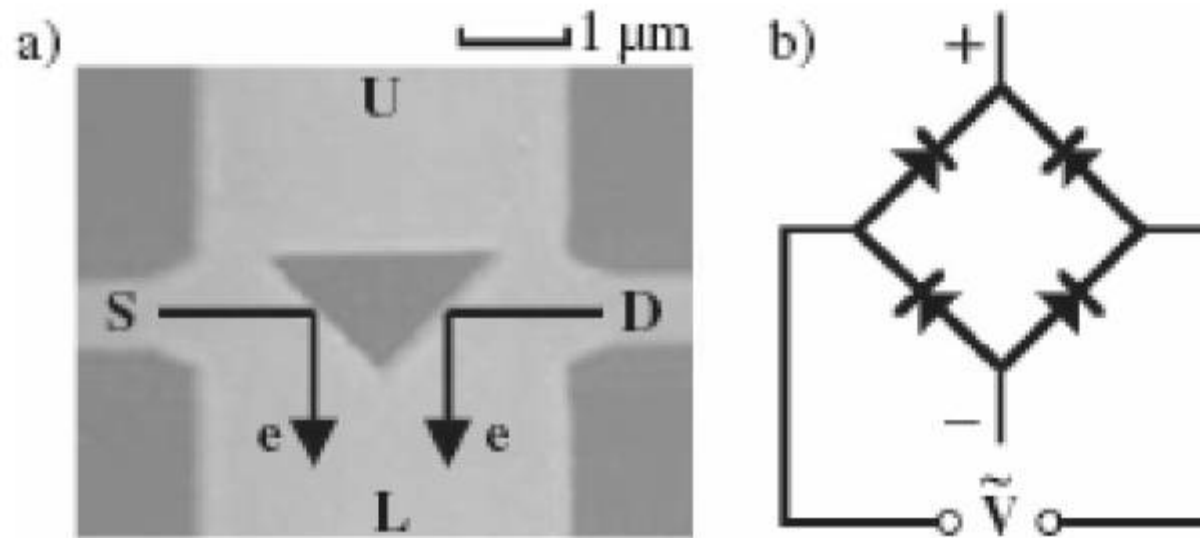


Fig. 4. Image of the a) Ballistic rectifier and b) Bridge rectifier

Element YBS

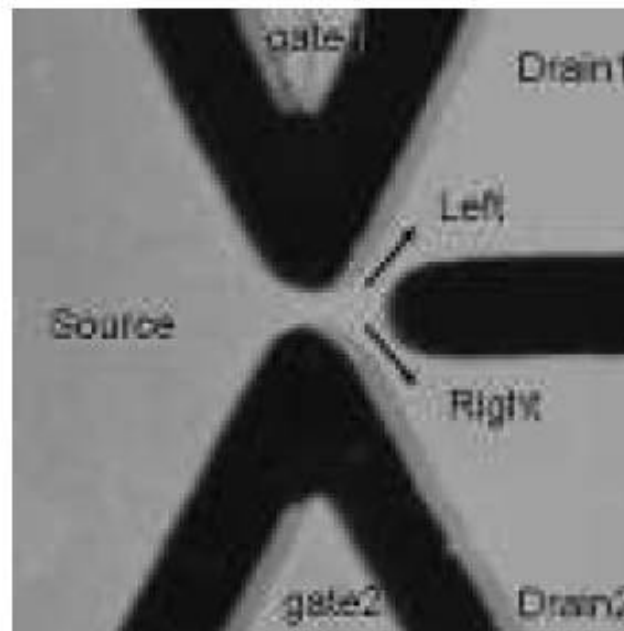


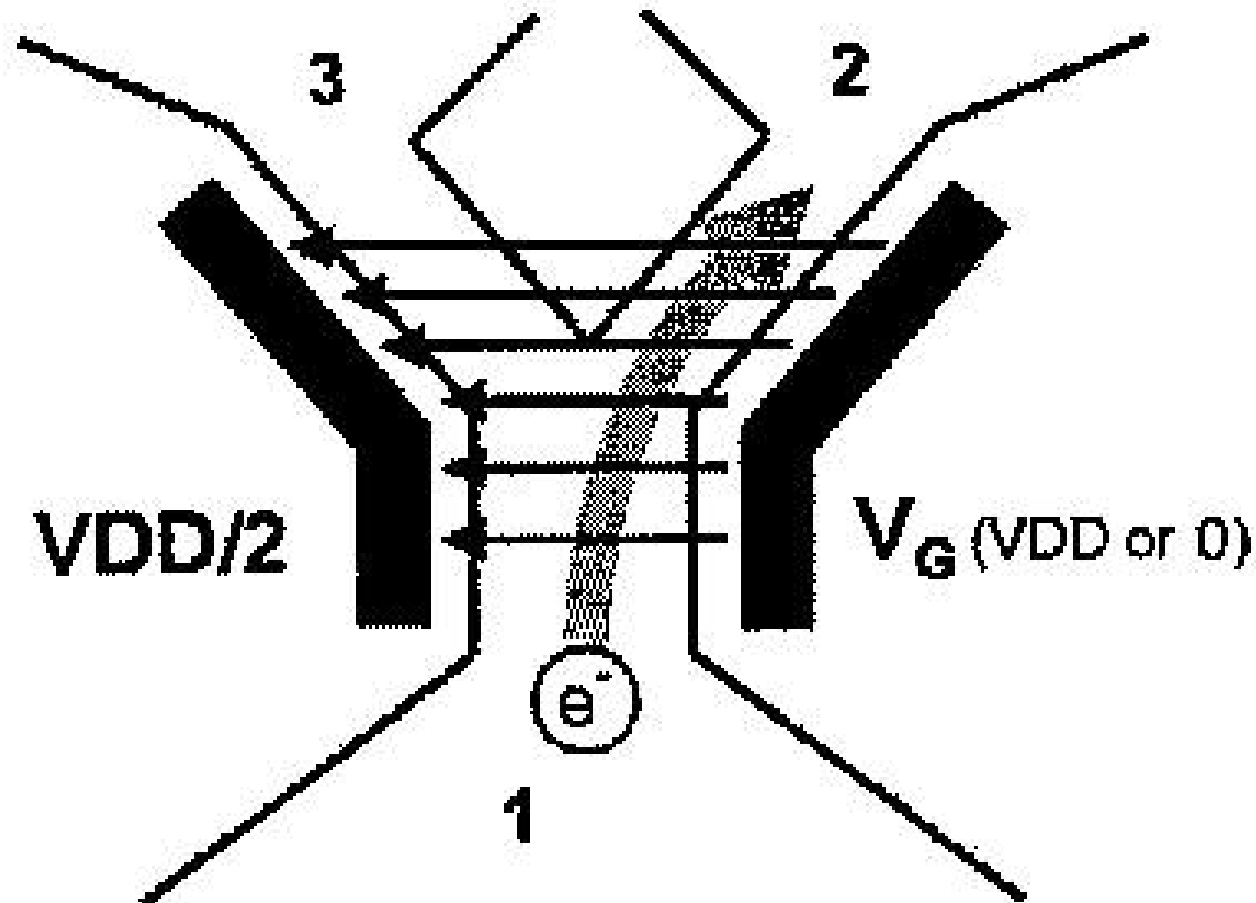
Fig. 7. Atomic force micrograph of a YBS with neck width of 76nm

Element YBS

Technologia YBS jest technologią bardzo małych mocy, która polega na przełączaniu polem elektromagnetycznym strumienia elektronów na dwa kierunki

Przepływ elektronów może być sterowany bardzo małą energią z dużą szybkością

Zasada działania YBS

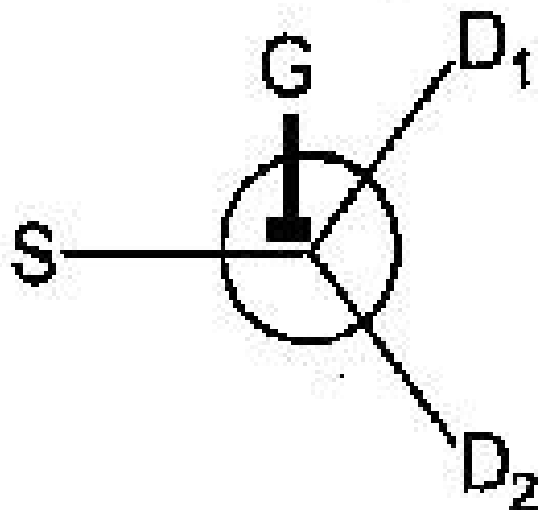


Parametry energetyczne YBS

Moc rozpraszana na pojedynczą operację wynosi
0.6 meV

Moc rozpraszana przez „stratę” 1 bitu w
temperaturze pokojowej wynosi 18meV
(30 x więcej)

Funkcja elementu YBS

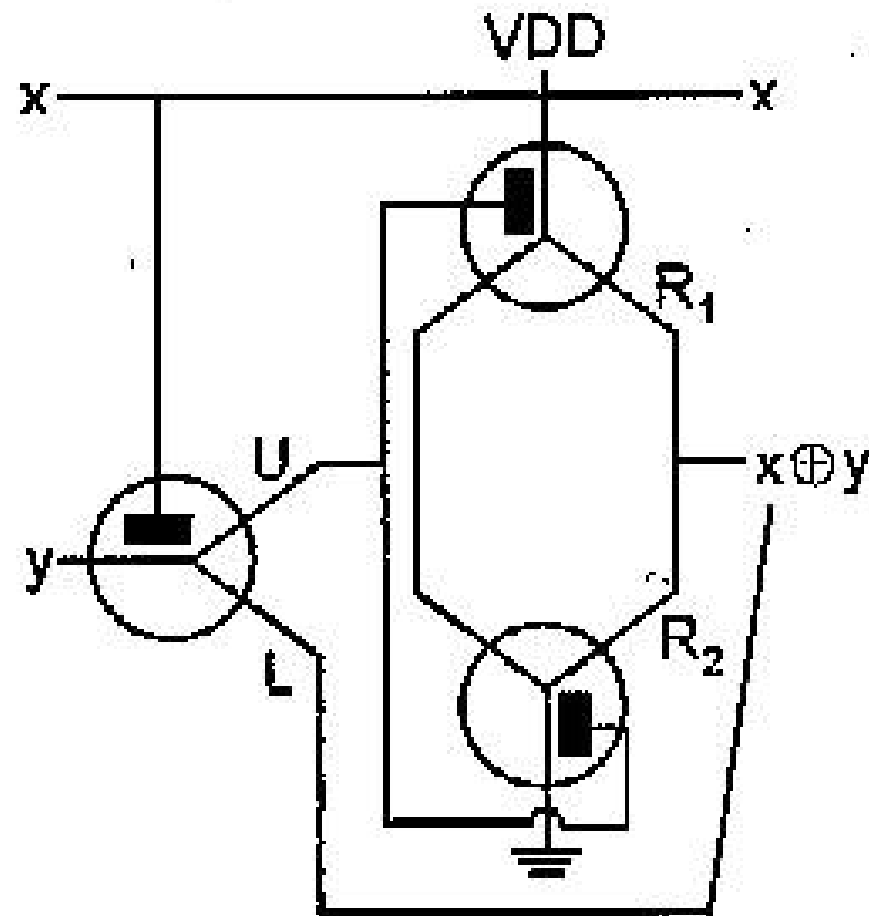


(a)

S	G	D ₁	D ₂
0	0	0	0
0	1	0	0
1	0	0	1
1	1	1	0

(b)

Dwubitowa bramka Toffoli



Przetwarzanie bez energii

Jeśli uda się zbudować kwantowe bramki odwracalne bez zużycia energii, to stanie się możliwe przetwarzanie informacji bez zasilania

Do czego potrzebne zasilanie?

Nawet przy zastosowaniu układów kwantowych, do wprowadzania i wyprowadzania informacji

**JEST POTRZEBNA
ENERGIA**

Komputery kwantowe

- ▣ Komputery kwantowe wykorzystują układy odwracalne
- ▣ Poszukuje się algorytmów wykorzystujących obliczenia kwantowe, np. algorytm Shore'a czyli rozkład liczby na czynniki pierwsze

Zastosowanie układów odwracalnych w kryptografii

Proste szyfrowanie podstawieniowe

Każda funkcja odwracana 8 zmiennych przypisuje bajtowi wejściowemu inny bajt wyjściowy.

Do realizacji szyfru potrzebna 8-wejściowa kaskada.

Kryptoanaliza

Jedną z technik łamania szyfrów jest analiza rozpraszanej mocy

SPA - *Simple Power Analysis*

DPA - *Differential Power Analysis*

Zmniejszenie mocy szyfratora utrudnia SPA i DPA

Dziękuję za uwagę