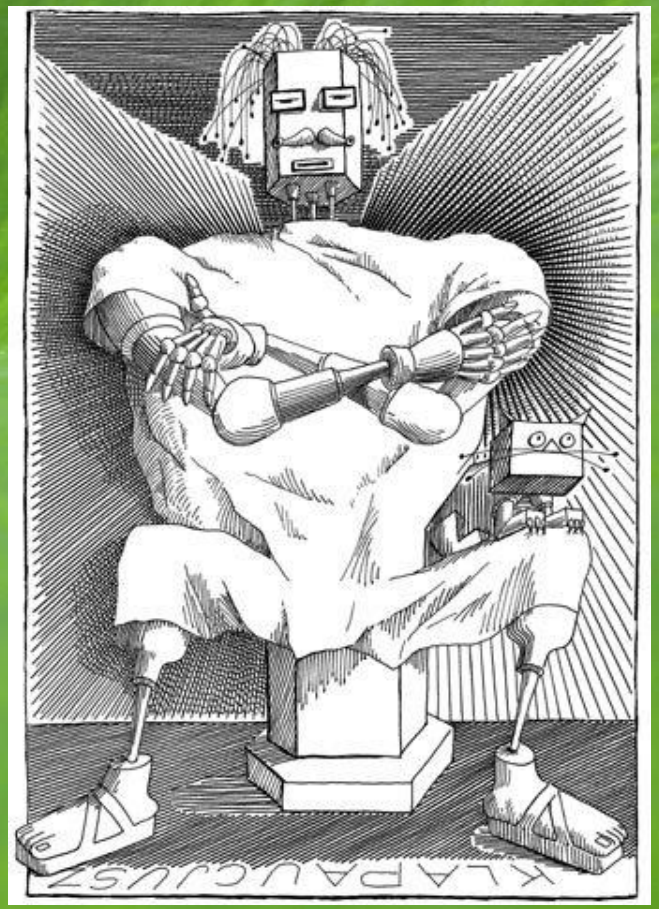
Wolność, prywatność i bezpieczeństwo – o polskiej szlachcie, Internecie, komputerach kwantowych i teleportacji



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

Edukacja przez badania

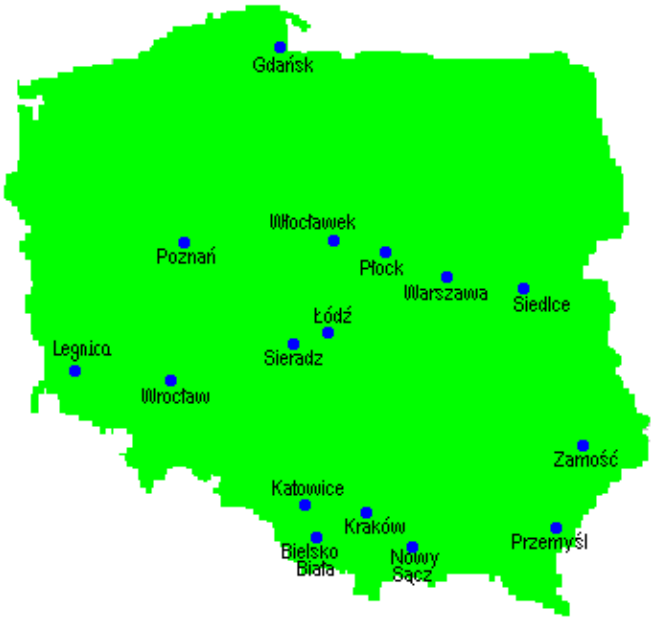
Hoża 69: 1921-2014 r.

WYDZIAŁ FIZYKI
UNIWERSYTET WARSZAWSKI

inżynieria nanostruktur

Internet dla Szkół – 20 lat!

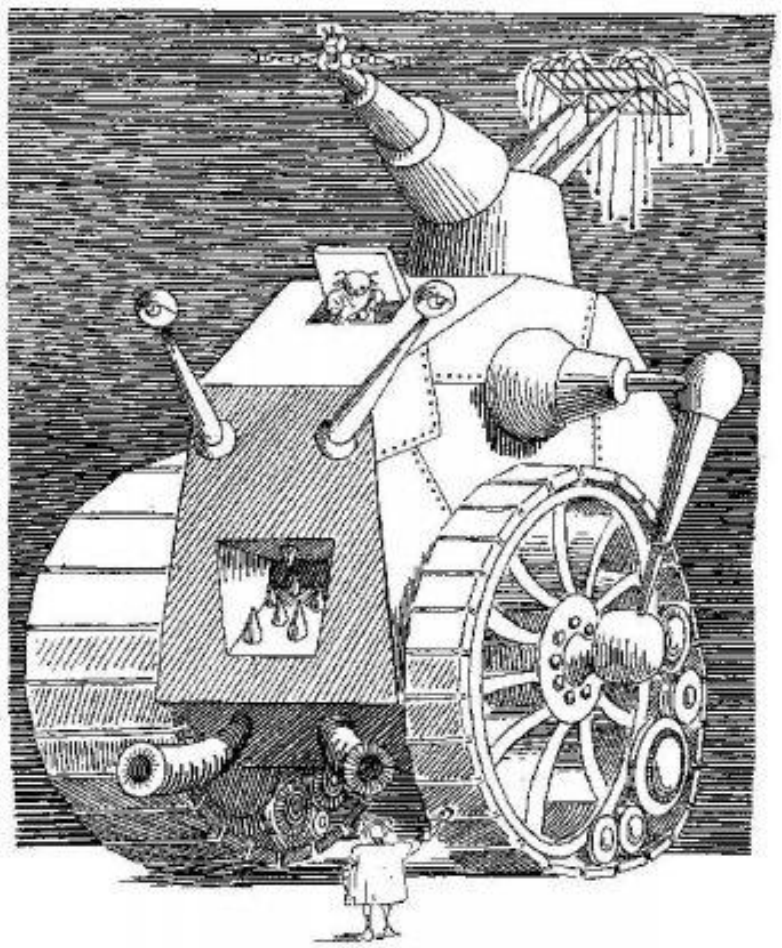
Pierwsze podłączenie Internetu w Polsce:
sierpień 1991, Wydział Fizyki UW
Ul. Hoża 69
http://www.internet10.pl/



Polskie szkoły w Internecie w 1997 r.

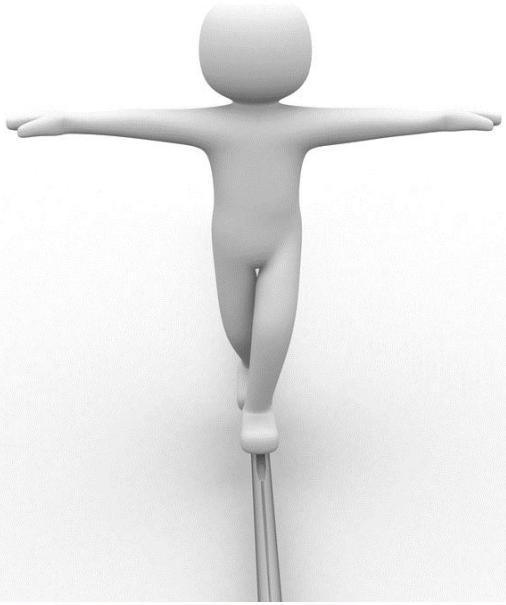
1994-2005 Wydział Fizyki UW
1997-2000(?) Fundacja Rozwoju Demokracji Lokalnej

Wolność, prywatność, bezpieczeństwo

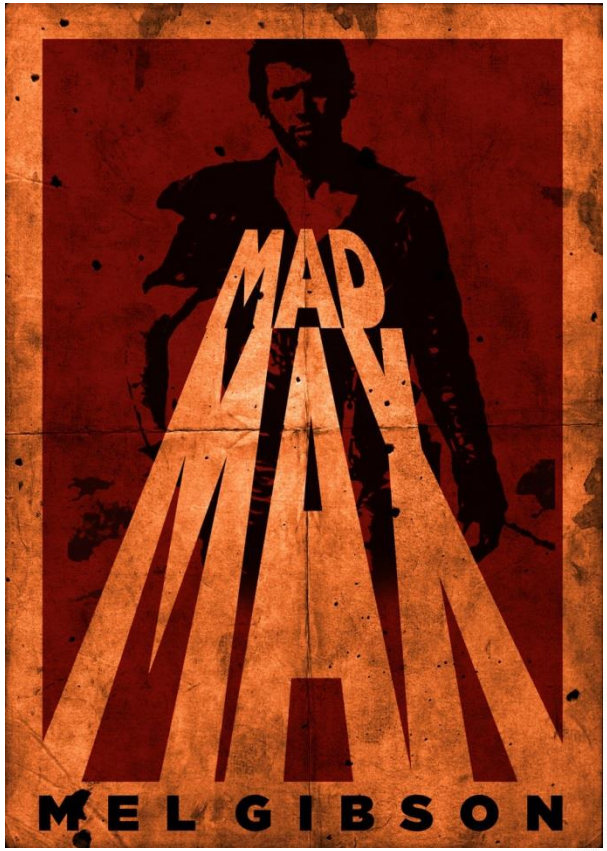


„Wolność”, " vs. „bezpieczeństwo”

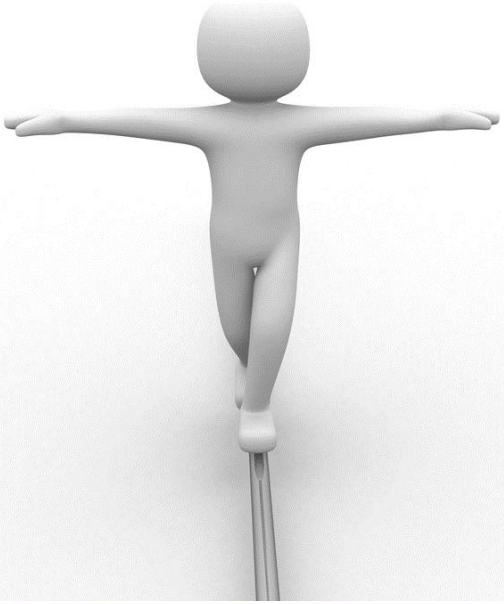
Prywatność

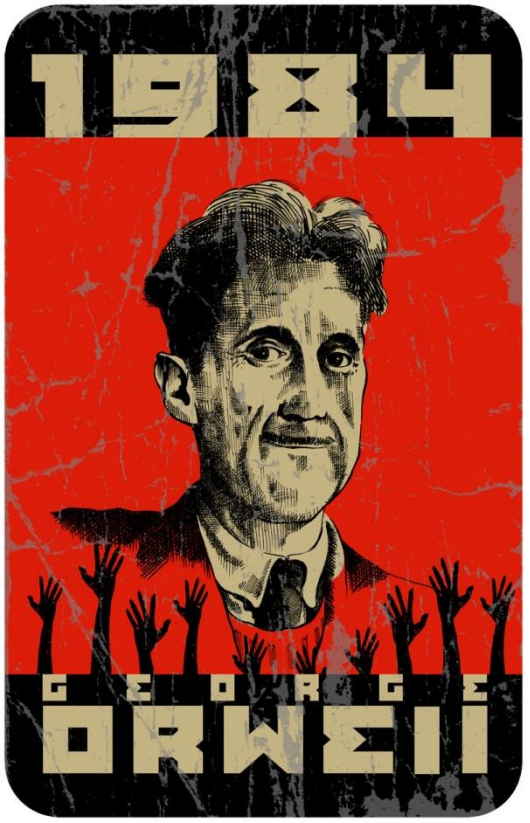


„Wolność”, " vs. „bezpieczeństwo”



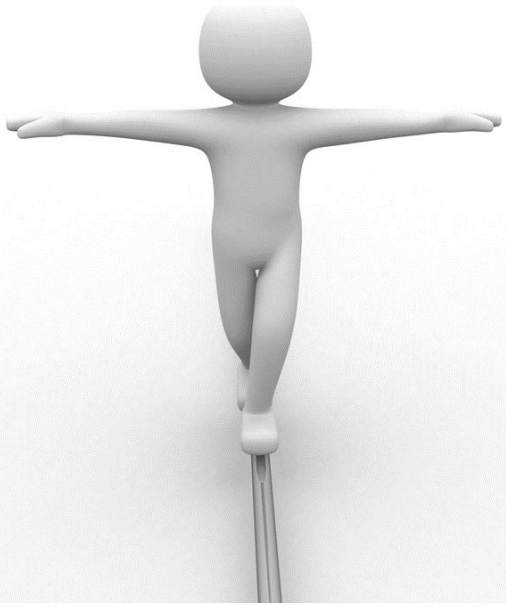
Prywatność





„Wolność”, " vs. „bezpieczeństwo”

Prywatność

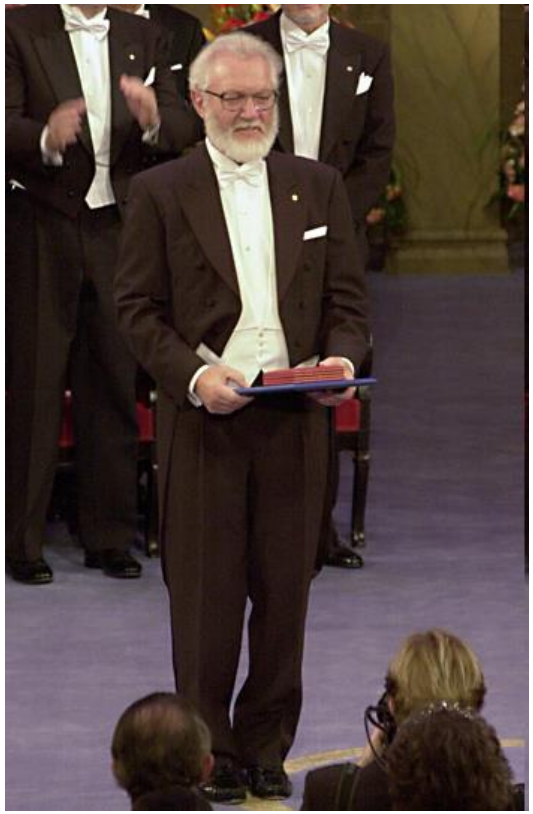


„Wolność”, " vs. „bezpieczeństwo”

„Wolność”, " vs. „bezpieczeństwo”

Nowe technologie

The Nobel Prize in Physics 2000



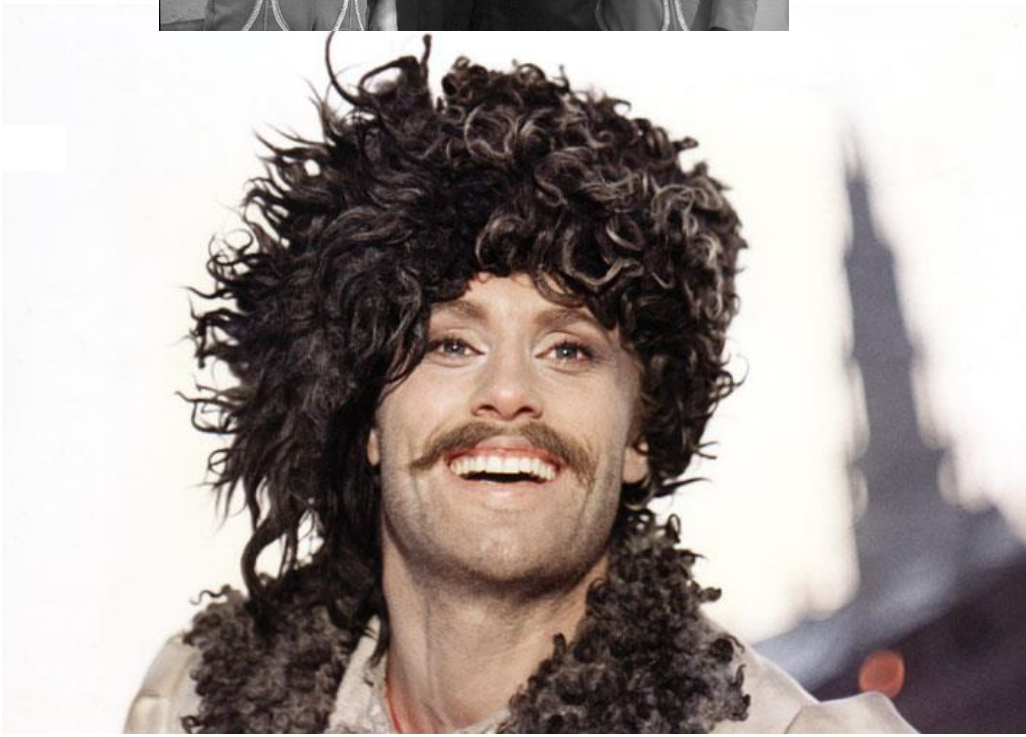
"The principal applications of any sufficiently new and innovative technology always have been - and will continue to be - applications created by that technology."

Herbert Krömer

"Główne zastosowanie każdej nowej i innowacyjnej technologii zawsze było – i nadal będzie – zastosowaniem stworzonym przez tą technologię"

http://en.wikipedia.org/wiki/Herbert_Kroemer

Wolność, prywatność, bezpieczeństwo



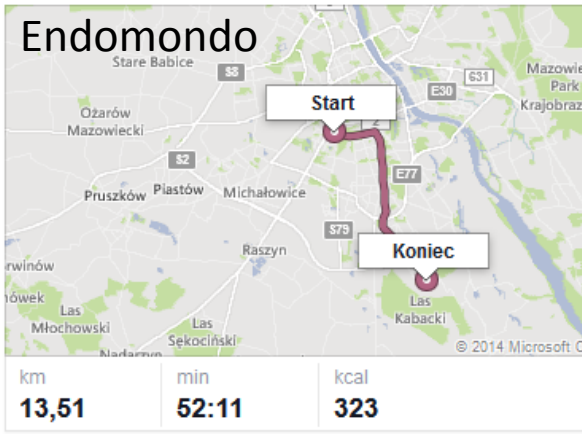
Wolność, prywatność, bezpieczeństwo

Wolność, prywatność, bezpieczeństwo

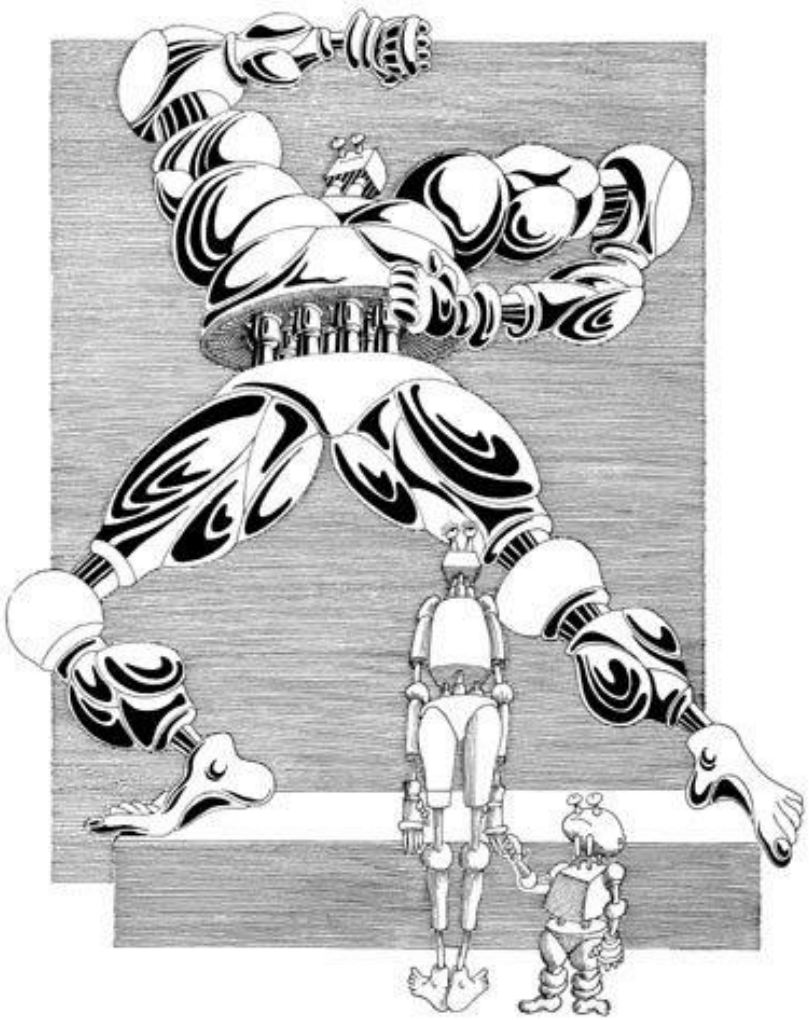
Wolność, prywatność, bezpieczeństwo

Wolność, prywatność, bezpieczeństwo

http://crowdfunding.pl/2011/05/04/prywatnosc-na-portalach-spolecznosciowych-raport/

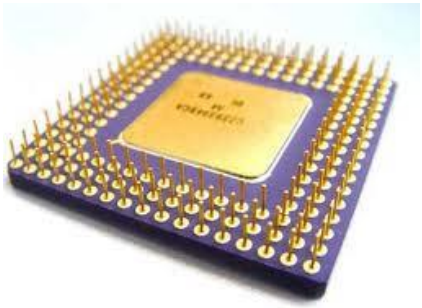


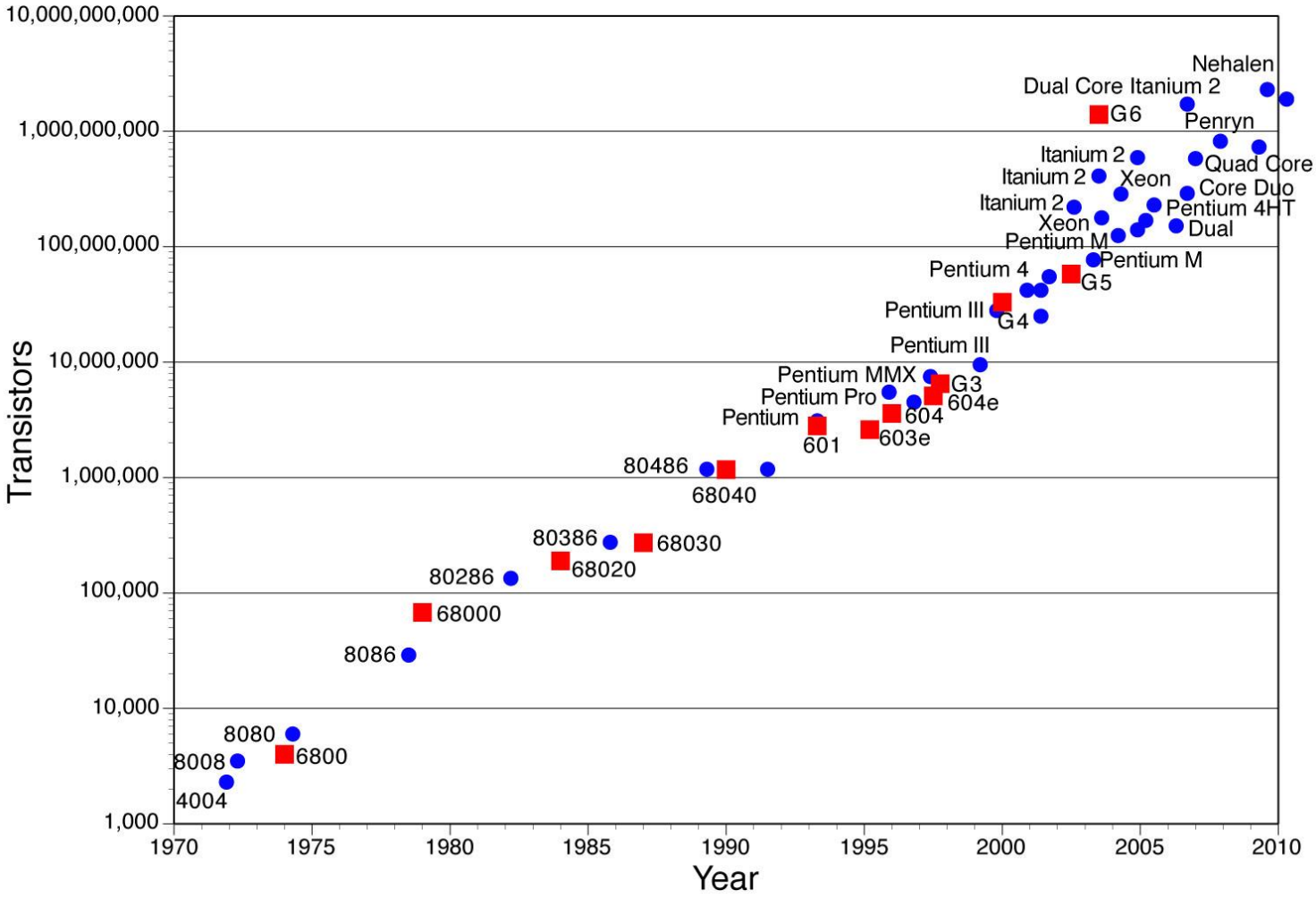
Postęp techniczny



TRENDY: Prawo Moore'a

Ilość komponentów (tranzystory, połączenia, izolacje itd.) w IC podwaja się co około 18 miesięcy.





20 lat

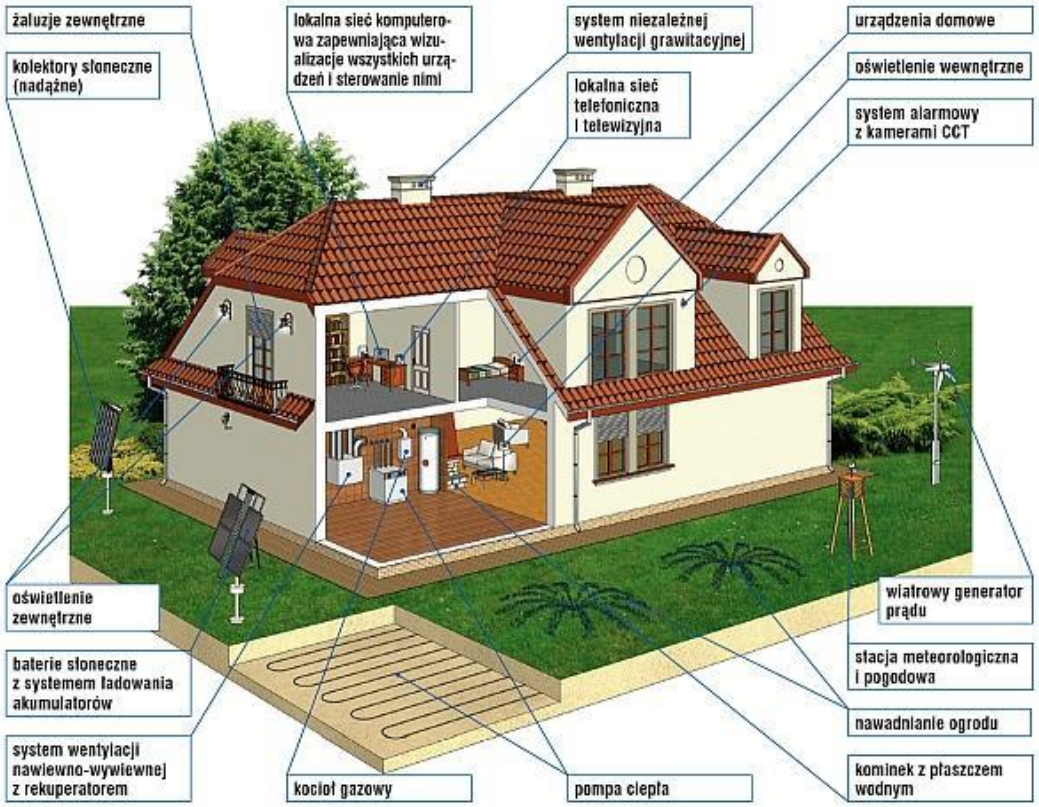
„Maksymalna paranoja nie polega na przekonaniu, że wszyscy są przeciwko tobie, lecz że wszystko jest przeciwko tobie. Zamiast mówić „Moj szef spiskuje przeciwko mnie”, mówisz wtedy: „Telefon mojego szefa spiskuje przeciwko mnie”

(Philip K. Dick, *Galaxy*, czerwiec 1953)

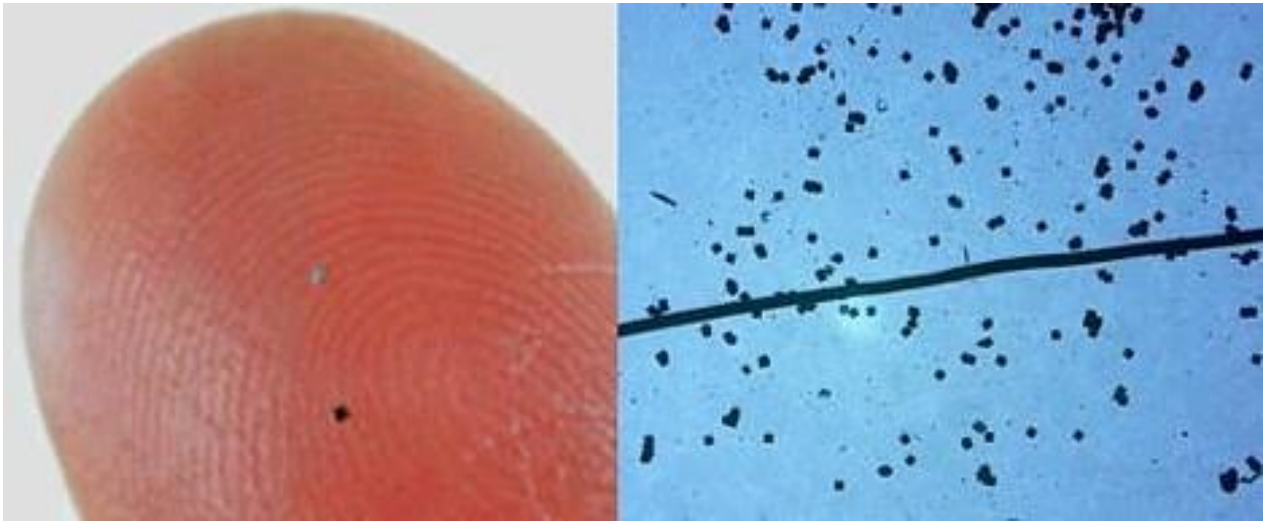
Inteligentny dom

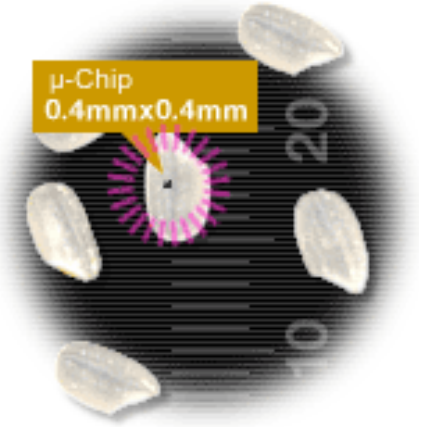
„Maksymalna paranoja nie polega na przekonaniu, że wszyscy są przeciwko tobie, lecz że wszystko jest przeciwko tobie. Zamiast mówić „Moj szef spiskuje przeciwko mnie”, mówisz wtedy: „Telefon mojego szefa spiskuje przeciwko mnie”

(Philip K. Dick, *Galaxy*, czerwiec 1953)



RFID





Hitachi's new RFID chips (pictured on right, next to a human hair) are 64 times smaller than their mu-chips (left)

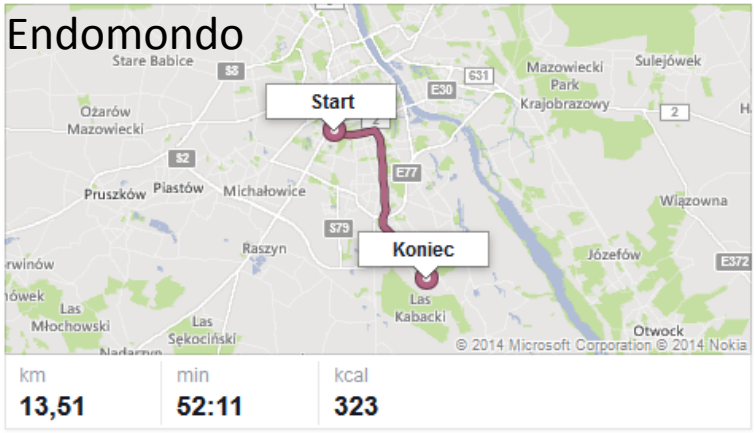
Pieniądze


MasterCard
paypass
5412 7512 3412 3456
JAN KOWALSKI
55 ZŁ
NFC

Big Data


ABSA
platinum
VISA
MasterCard


support
cloud
Database
storage
analize
information
tools
statistics
Big Data
mobile
processing
terabytes
NoSQL
compression


Endomondo
Start
Koniec
Stare Babice
Ożarów Mazowiecki
Pruszków
Piastów
Michałowice
Raszyn
Mazowiecki Park Krajobrazowy
Sulejówek
Wiązowna
Józefów
Las Kabacki
Las Młochowski
Las Sękociński
Otwock
© 2014 Microsoft Corporation © 2014 Nokia
km
13,51
min
52:11
kcal
323

Druk 3D

Inżynieria nanostruktur, UW

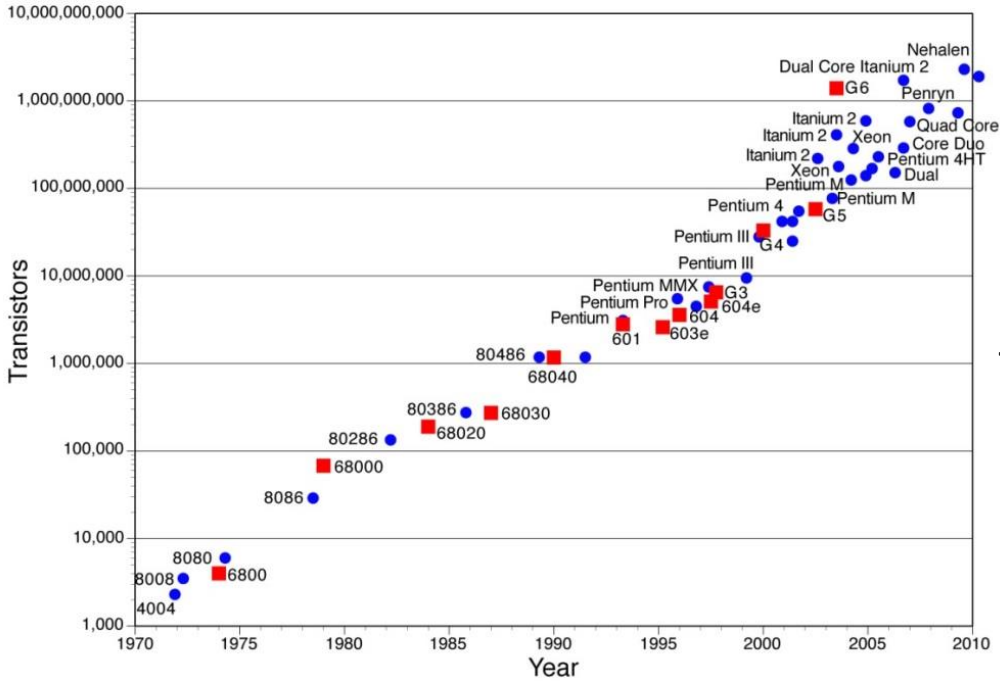
Prywatność

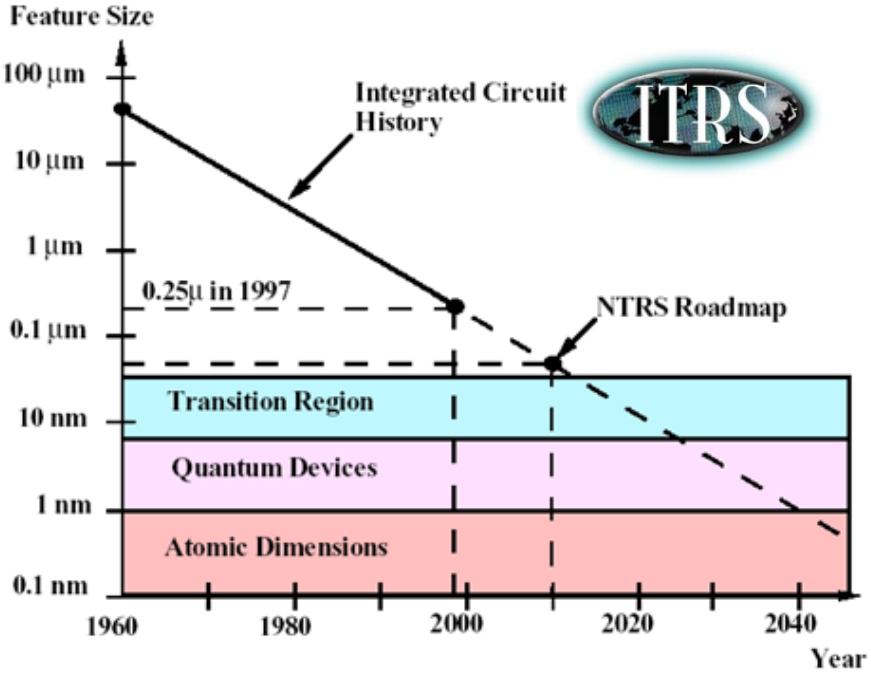
Kilka lat temu użytkownicy internetu zaczęli zdawać sobie sprawę że gdy jakaś usługa jest darmowa, to my przestajemy być klientami. Stajemy się produktem.

Tim Cook, 2014

TRENDY: Prawo Moore'a

Ilość komponentów (tranzystory, połączenia, izolacje itd.) w IC podwaja się co około 18 miesięcy. Rozmiar liniowy komponentów również zmniejsza się wykładniczo w czasie.





Te trendy nie mogą być kontynuowane w nieskończoność.

- **Co zastąpi technologię Si?**
- **Z czego będzie wynikała ta zmiana technologii?**

Źródło: Intel

Obliczenia kwantowe

Komputery kwantowe

1. **Bity, P-bity, Q-bity**
2. **Bramki Qbitowe**
3. **Kwantowe procedury**
4. **Poważny problem**
5. **Jak zbudować taki komputer?**

D-Wave
The Quantum Computing Company™

Bity, P-bity, Q-bity

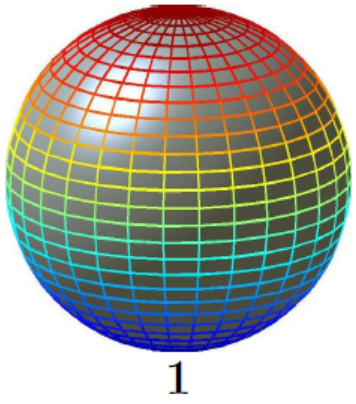
Bit

States: 0 or 1

Pbit

$\{p{:}0, (1-p){:}1\}$

Qubit

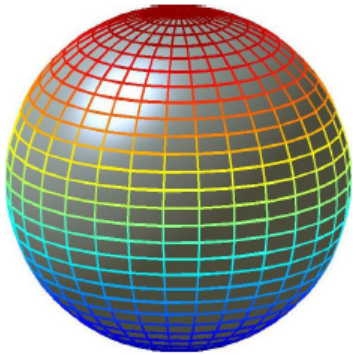


$\alpha|0\rangle + \beta|1\rangle$

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

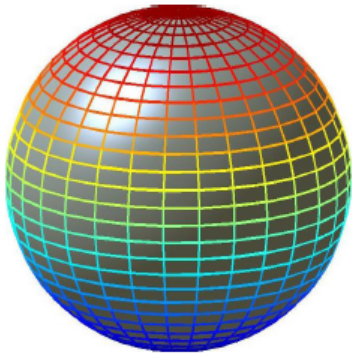
> komputery (maszyny Turinga)
> standardowe programy
> ▌

Bity, P-bity, Q-bity

Bit	Pbit	Qubit
0	0	0
		
1	1	1
States: 0 or 1	$\{p{:}0, (1-p){:}1\}$	$\alpha\|0\rangle + \beta\|1\rangle$ $\|\alpha\|^2 + \|\beta\|^2 = 1$

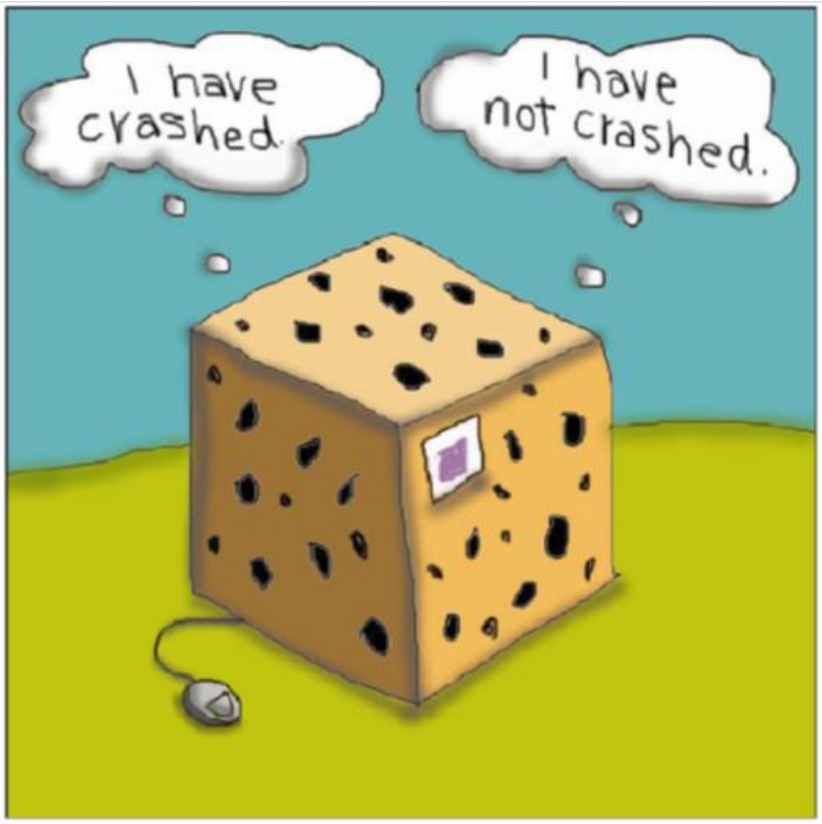
> „logika rozmyta”
> metody obliczeniowe typu Monte Carlo
> algorytmy genetyczne
> metody optymalizacji

Bity, P-bity, Q-bity

	Bit	Pbit	Qubit
	0	0	0
			
	1	1	1
States:	o or ı	$\{p$:o, $(1-p)$:ı$\}$	$\alpha\|\text{o}\rangle + \beta\|\text{ı}\rangle$
			$\|\alpha\|^2 + \|\beta\|^2 = 1$

> komputery kwantowe
> algorytmy kwantowe
> ▌

Obliczenia kwantowe



Schrödinger's computer. —Sally O. Lee

Obliczenia kwantowe

Pierwszy komercyjny komputer kwantowy - sprzedany - Mozilla Firefox

Plik Edycja Widok Historia Zakładki Narzędzia Pomoc

Pierwszy komercyjny komputer kwanto...

http://technologie.gazeta.pl/internet/1,104530,9684065,Pierwszy_komercyjny_komputer_kwantowy__sprzedany.html

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

Gazeta.pl Technologie

Szukaj

Program TV | Newsletter

Wiadomości | Sport | Biznes | Kultura | Technologie | Moto | Kobieta | Plotki

Wiadomości | Testy | Porady | Telewizory | Mobile | Audio | Internet | Rankingi | Komputer w firmie | Teleinformatyka

Polecamy | Aplikacje mobilne | Tablety | Komputer w firmie

Strefa 51: zobacz, nad czym w tajemnicy pracowała armia USA

Volkswagen Aqua - poduszkowiec dla Chin

Czy Samsung D7000 jest idealny? [test]

Janusz A. Urbanowicz | 28.05.2011 15:27

Pierwszy komercyjny komputer kwantowy - sprzedany

Lubię to! 126

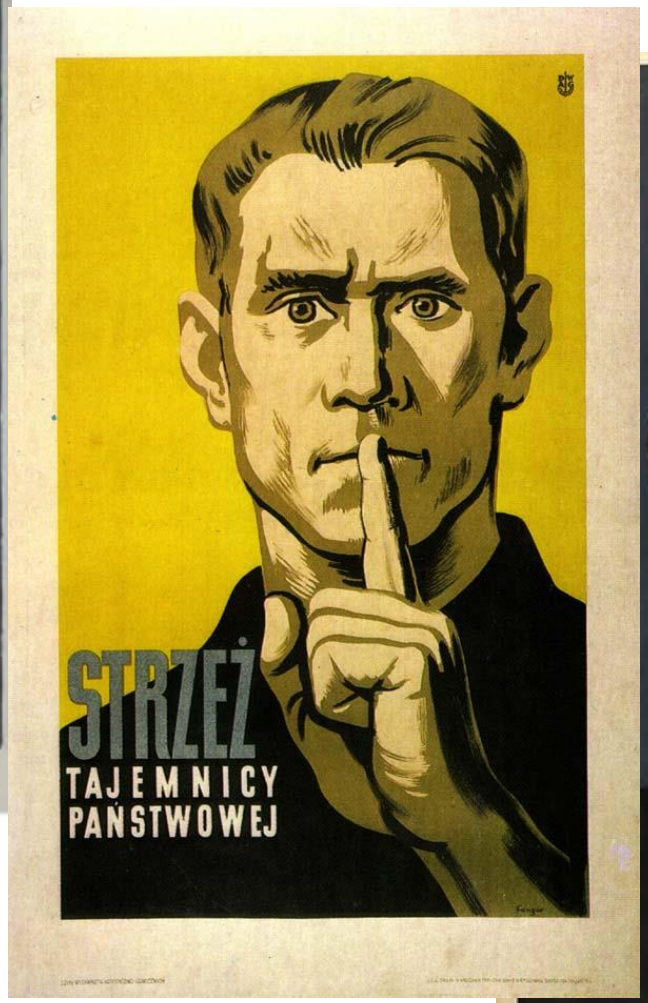
Komentuj, dodawaj zdjęcia i znajomych!

Zaloguj się | Nie masz u nas konta? Zarejestruj się

Najczęściej czytane

1. 10 najbardziej pożądanych gadżetów lat 80 (i czy ich jeszcze
2. Włamanie do Lockheed-Martin okazuje się być robotą
3. Pierwszy komercyjny komputer kwantowy - sprzedany
4. Felieton gościnny: Empik.com - prawie jak Amazon.com
5. Samsung i Apple: wojna na pozwy

Kryptografia



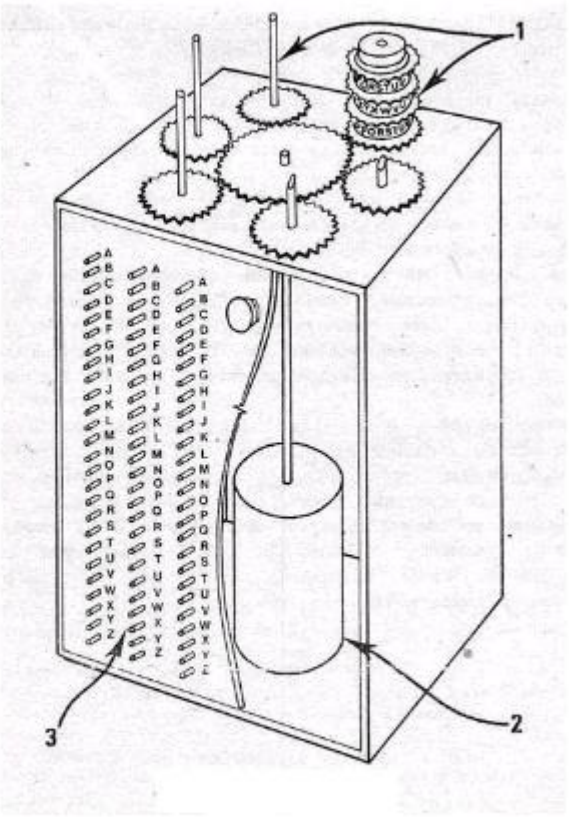
Kryptografia

Jerzy
Różycki

Marian
Rejewski

Henryk
Zygalski

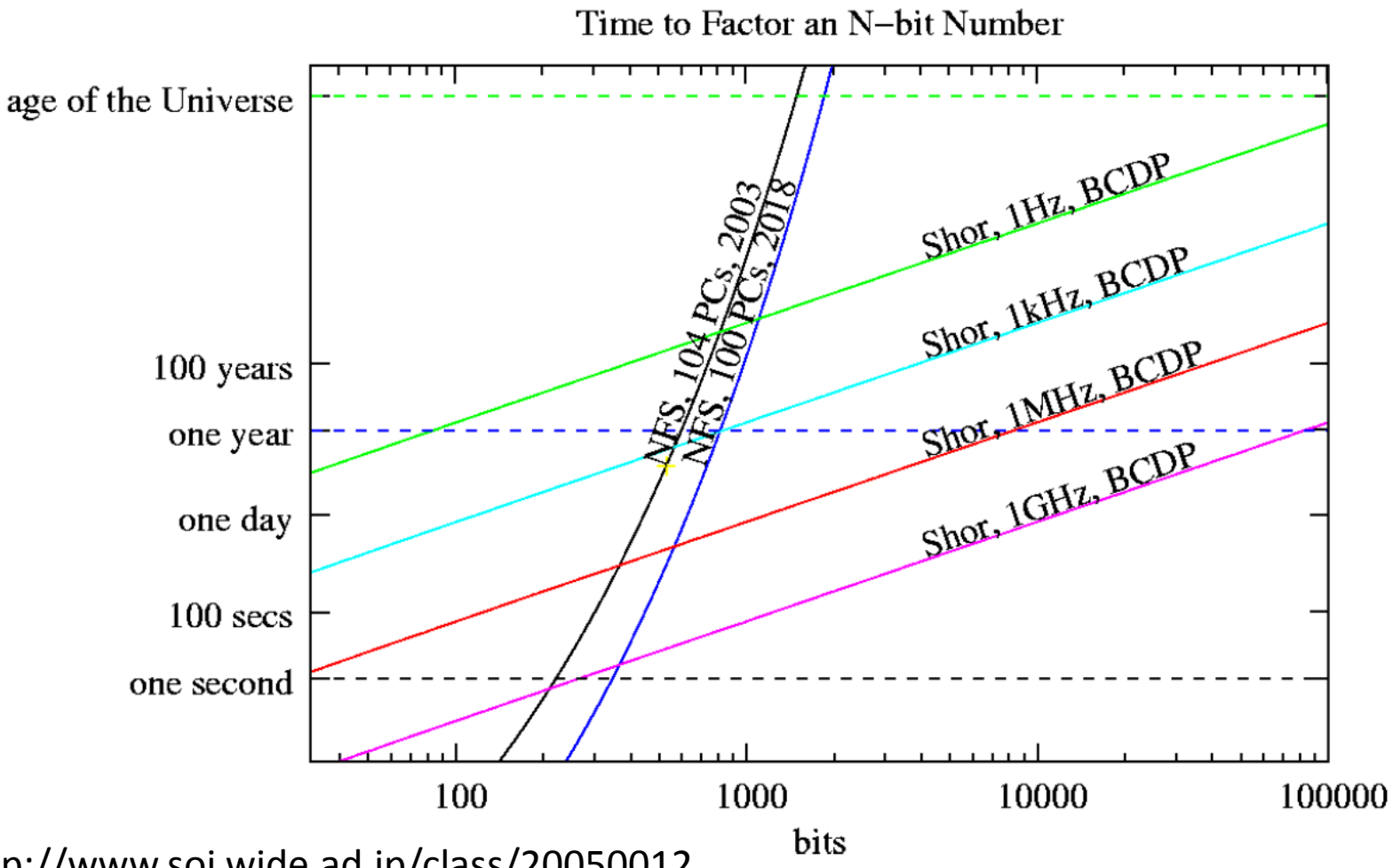
Enigma 1918/1923



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

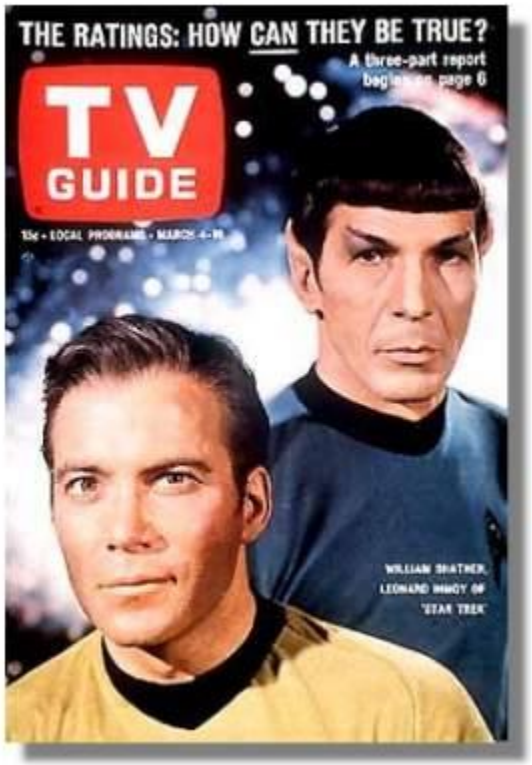
Algorytm Shora

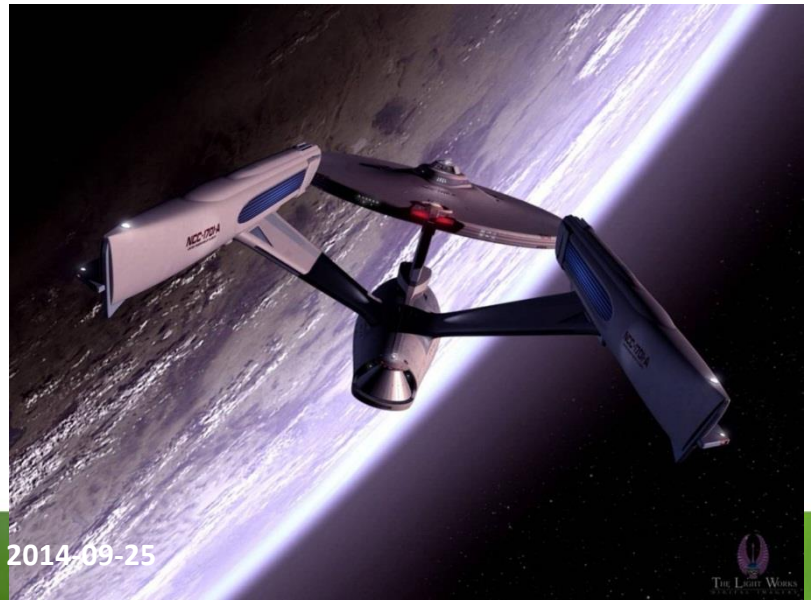
Factoring Larger Numbers



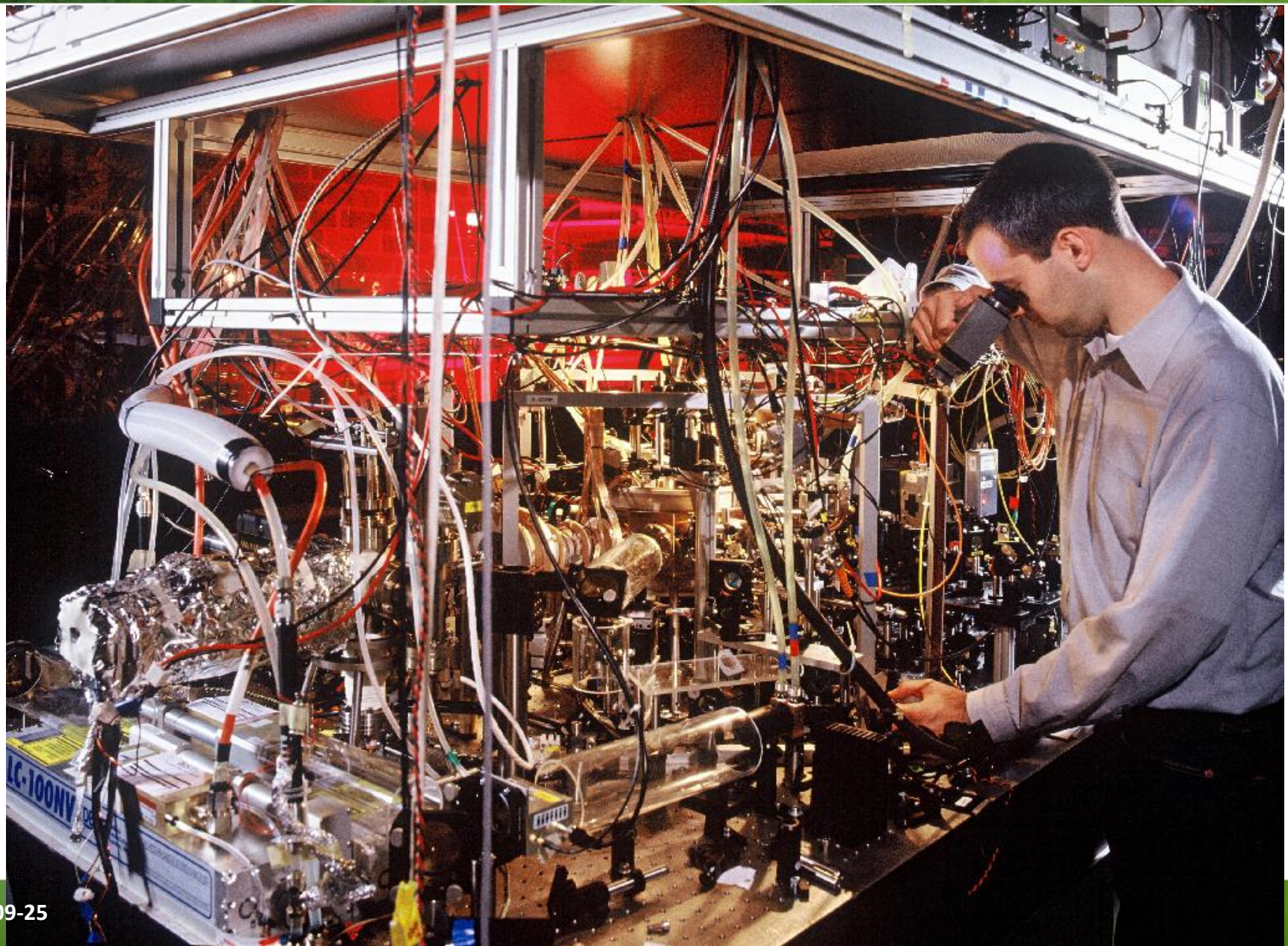
http://www.soi.wide.ad.jp/class/20050012

Kwantowa teleportacja



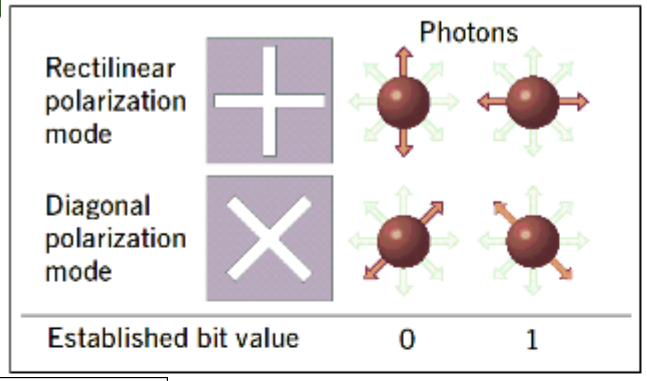


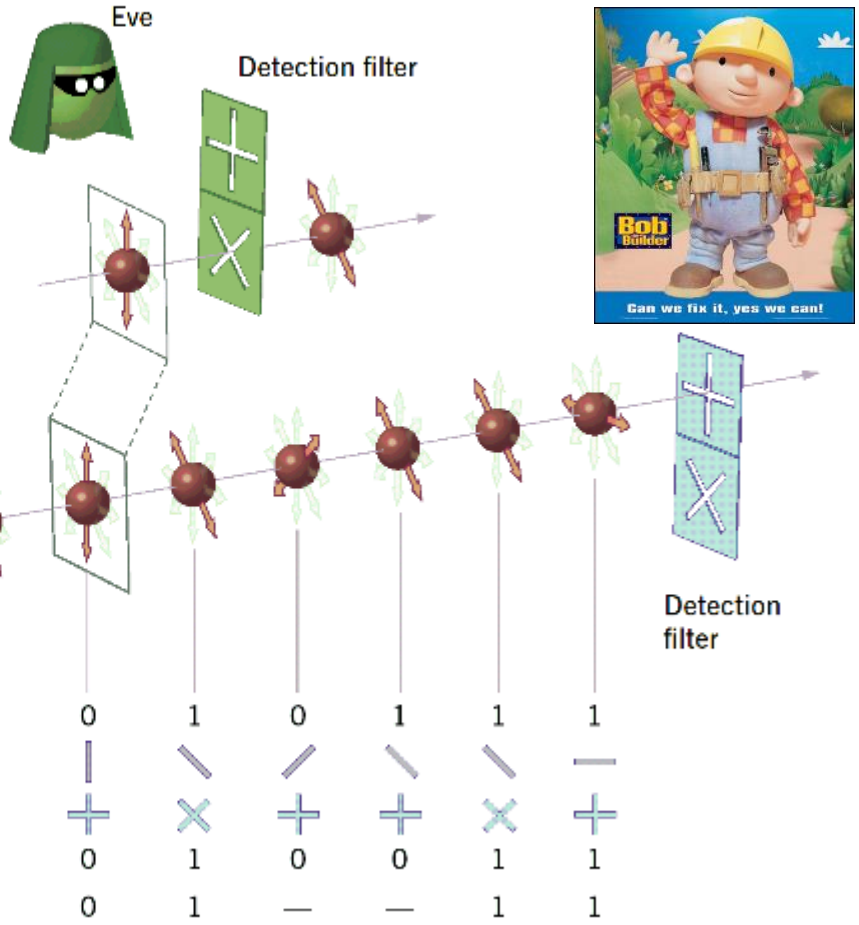
Maszyna do teleportacji



Kryptografia kwantowa

Protokół BB84 (Bennett, Brassard, 1984)

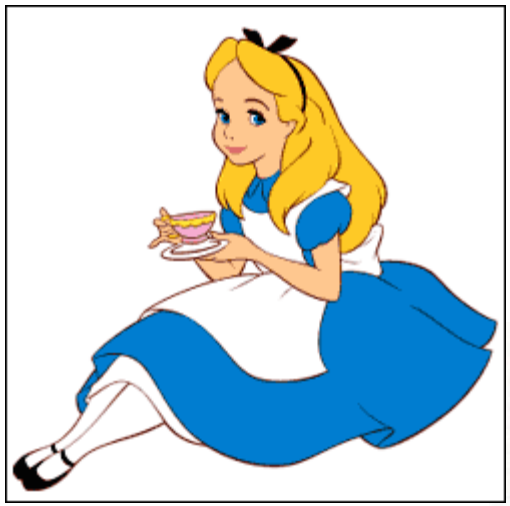




Bolek publicznie informuje Alicje jakiej bazy uzywał, zaś Alicja informuje go czy była to baza właściwa czy nie.

Kryptografia kwantowa

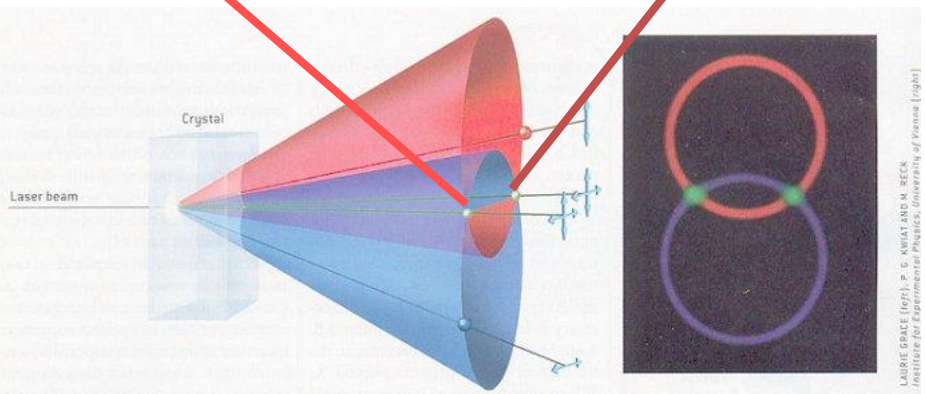
Prof. Artur Ekert

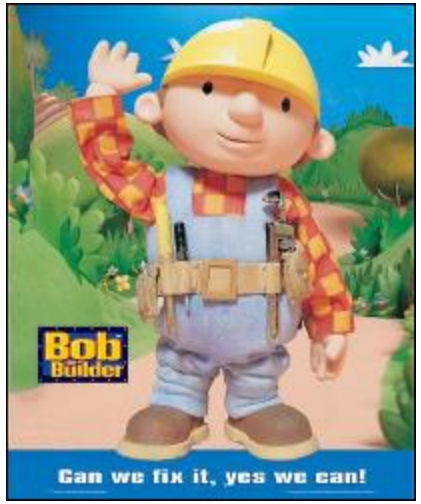


Alice

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

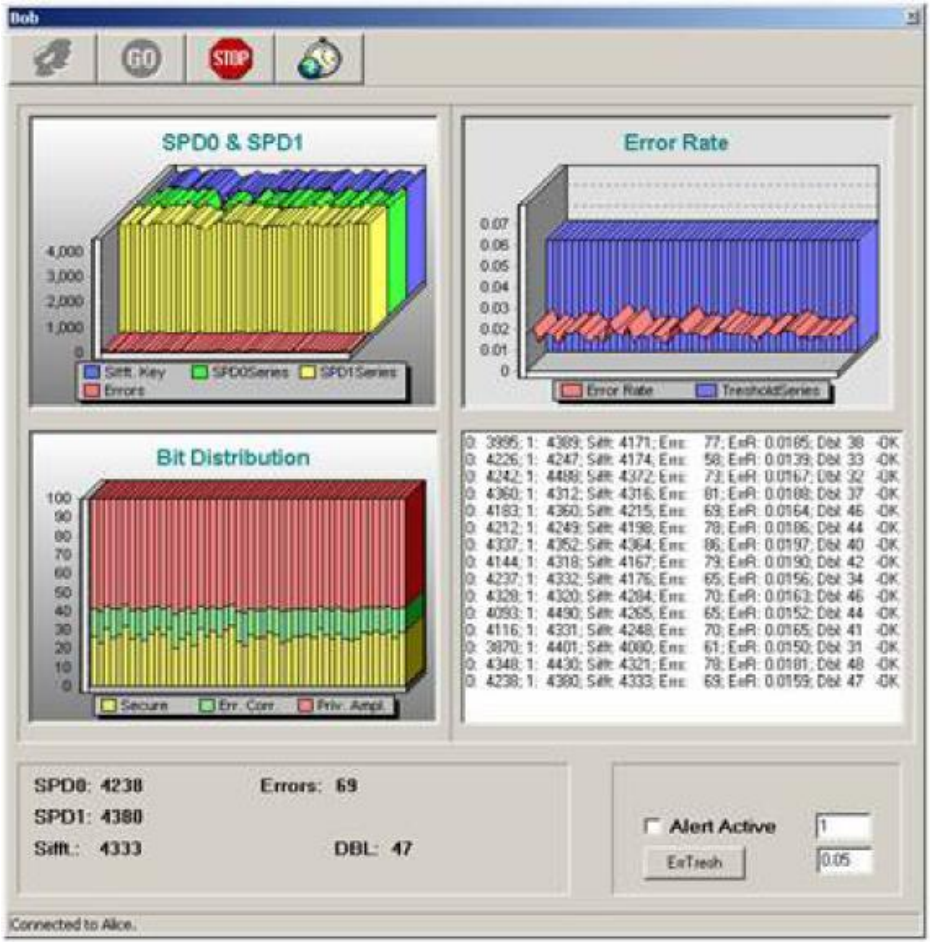
jawne

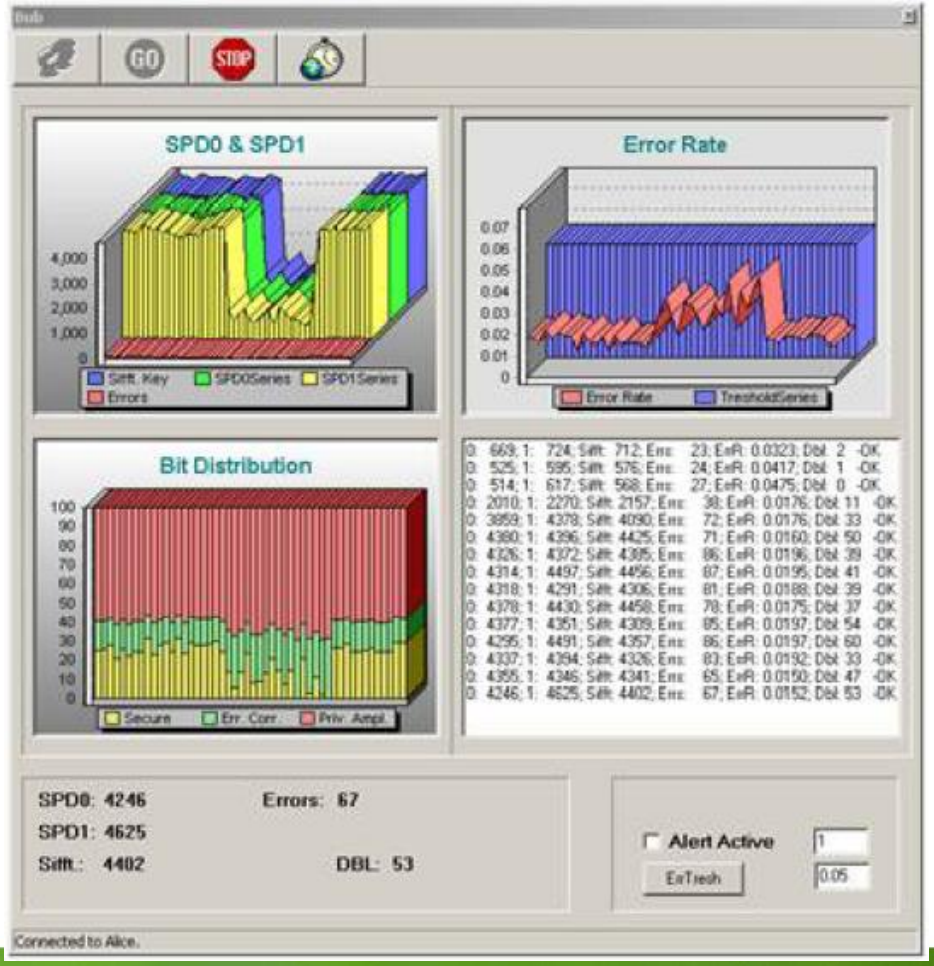
jawne

test (jawny)

Klucz: 0100101011…

Produkty


Bob
GO
STOP
SPD0 & SPD1
Error Rate
Bit Distribution
SPD0: 4238
Errors: 69
SPD1: 4380
Sift.: 4333
DBL: 47
Alert Active
EnTresh
Connected to Alice.


Bob
GO
STOP
SPD0 & SPD1
Error Rate
Bit Distribution
SPD0: 4246
Errors: 67
SPD1: 4625
Sift.: 4402
DBL: 53
Alert Active
EnTresh
Connected to Alice.

Jak TO działa?

Czwartki 17:00-18:30 **Pasteura 5, Wydział Fizyki**

http://www.fuw.edu.pl/~szczytko

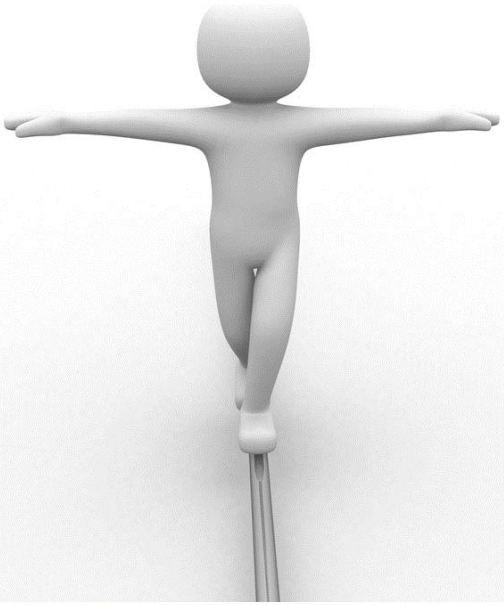
Google: **Jacek Szczytko**

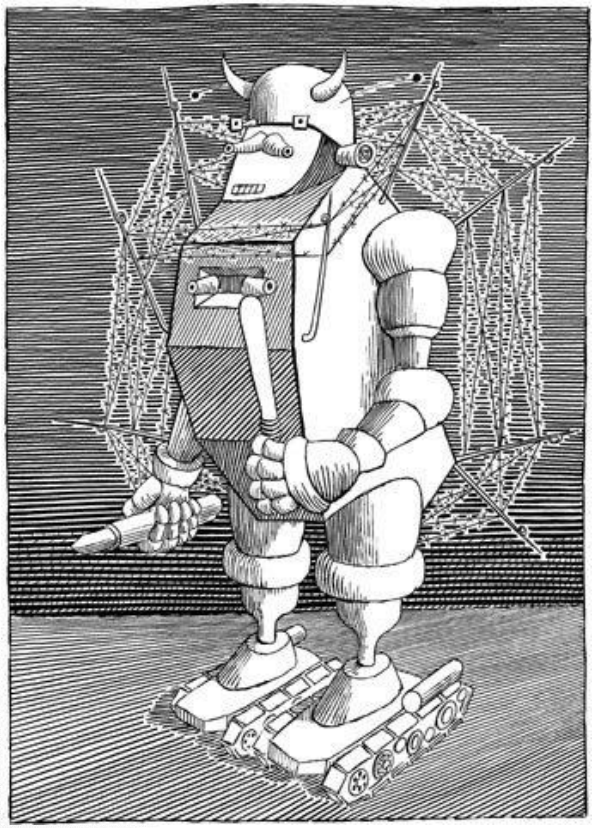
Login: **student**

Hasło: *******

„Wolność”, " vs. „bezpieczeństwo”

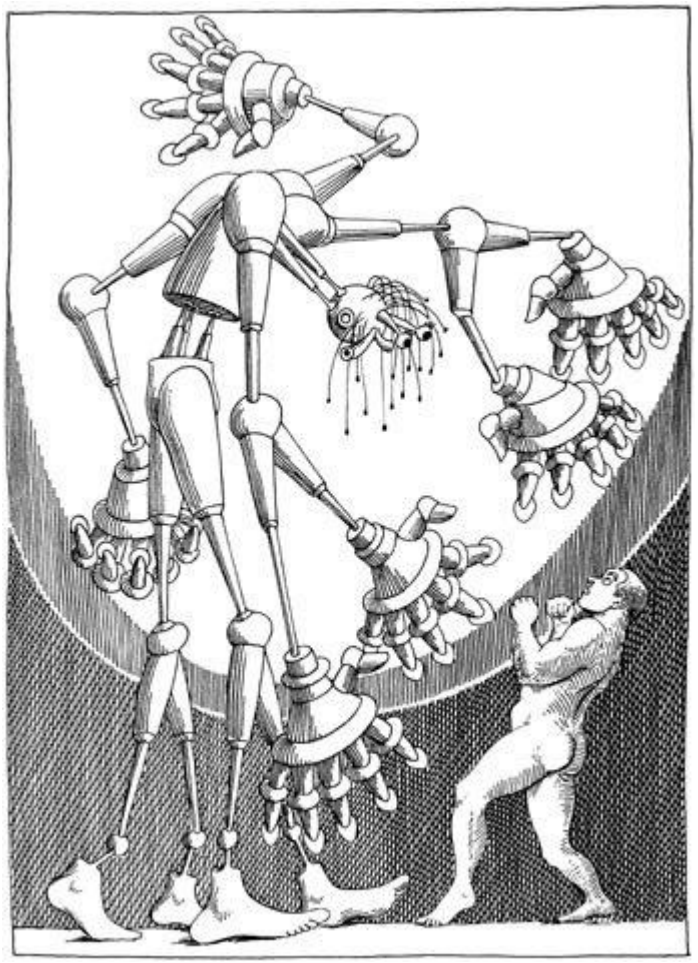
Prywatność





Podziękowania

Dziękuję panu Szymonowi Wójcikowi (Safeinternet.pl) za zaproszenie i moim studentom za inspiracje.



W prezentacji wykorzystano ilustracje Daniela Mroza do książki Stanisława Lema „Cyberiada”.