

Komputery kwantowe – ostateczni zabójcy bezpieczeństwa informacji?

Jan Anisimowicz CRISC, CISM, PMP

Sebastian Burgemeister CISA, CISM, CRISC, CDPSE, CCAK (...)

Kilka słów o nas. Zapraszamy do kontaktu!



Jan Anisimowicz

C&F SA

Board Member of ISACA Warszawa

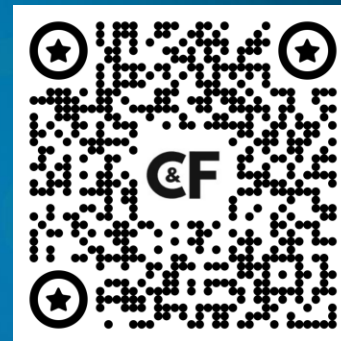
IIA Warszawa

Jan.Anisimowicz@candf.com



www.adaptivegrc.com
www.candf.com

Skontaktuj się ze mną na LinkedIn!



Sebastian Burgemeister

BW Advisory Sp. z o.o.

IIA UAE (Dubai)

Former President of IIA Polska

s.burgemejster@itgrc.pl



www.itgrc.pl
www.akademiaitgrc.pl

Skontaktuj się ze mną na LinkedIn!



O czym dzisiaj powiemy

01

Z czego zbudowany jest komputer kwantowy

04

Kryptografia postkwantowa.

02

Jak działa komputer kwantowy

05

Podsumowanie

03

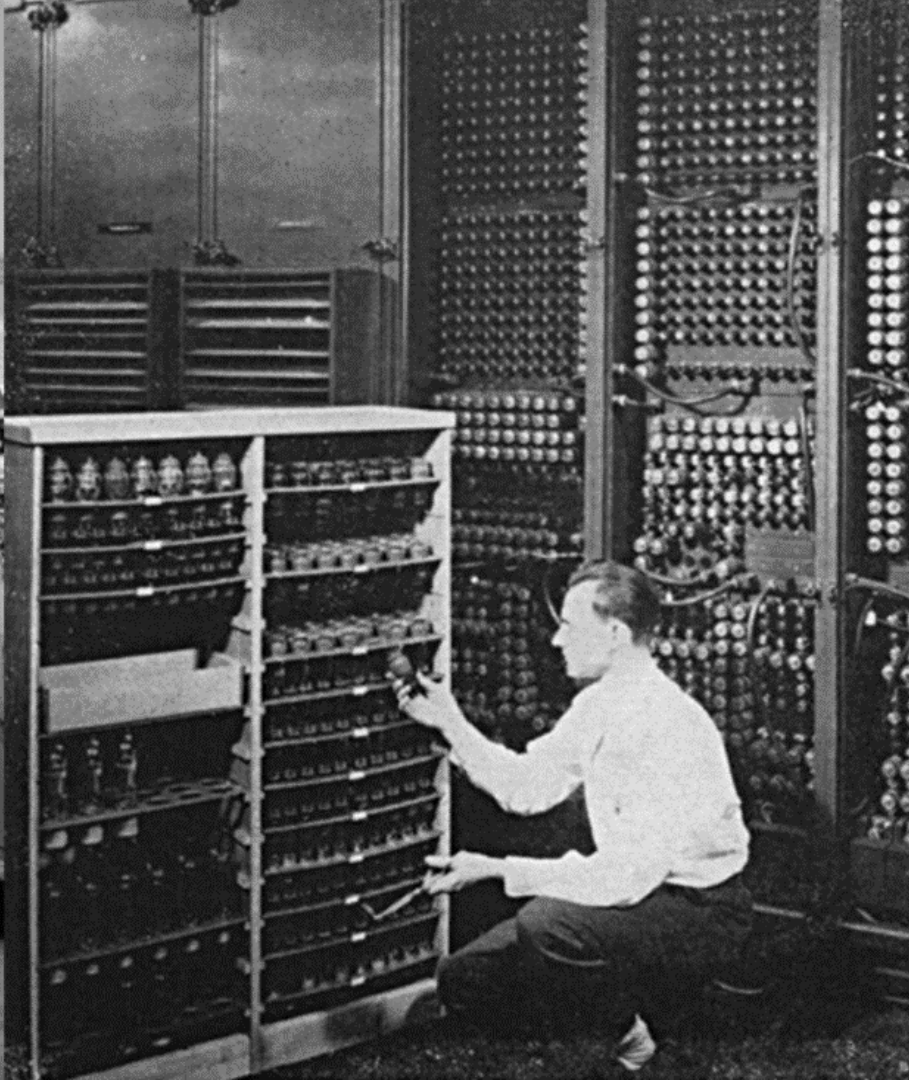
Algorytmy kwantowe

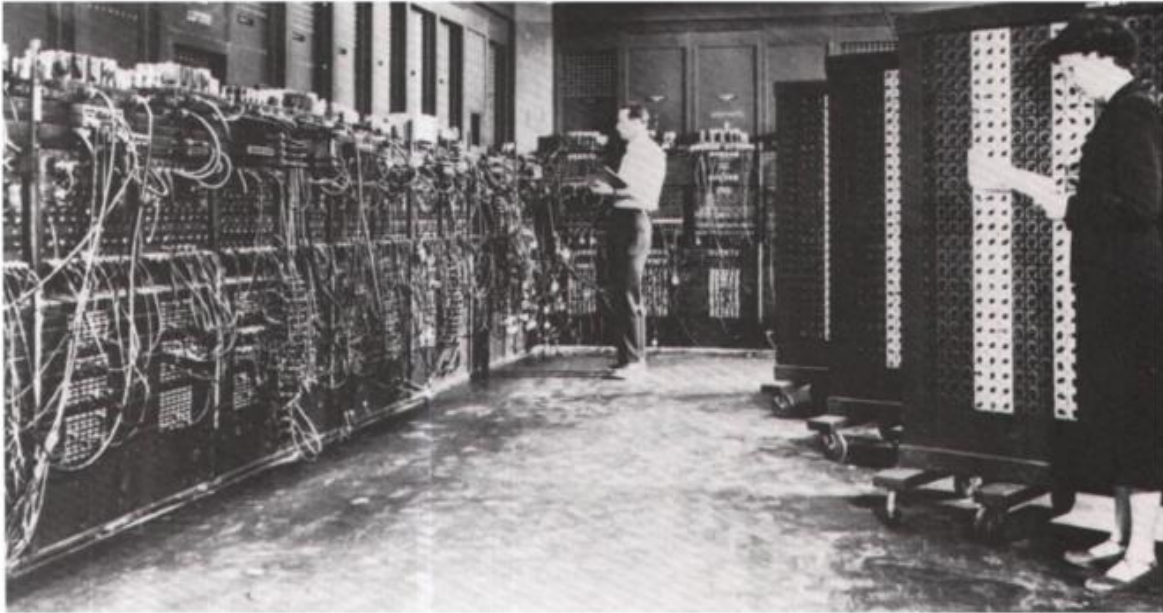
06

Pytania i odpowiedzi.

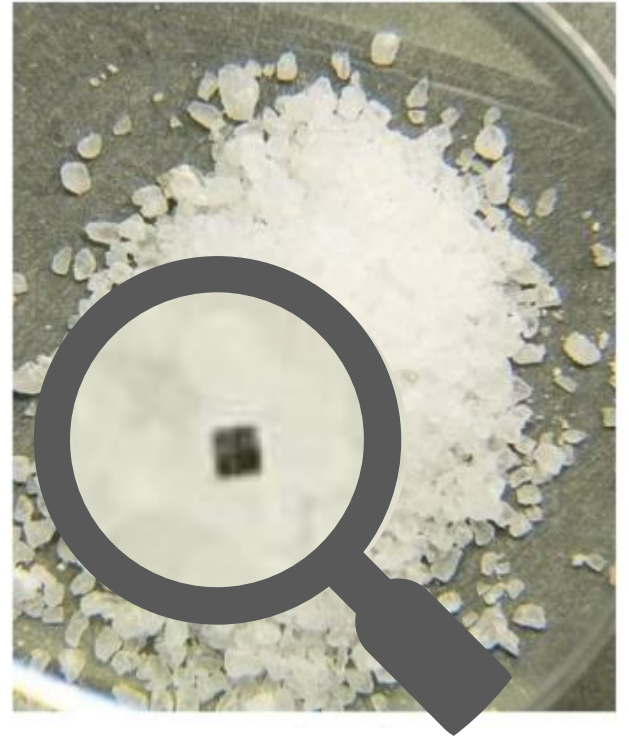
The background features a complex network of glowing green and blue lines and spheres, resembling a molecular structure or a data visualization. The lines are thin and intersect to form various shapes, while the spheres are larger and more prominent, with some appearing as bright, multi-colored nodes. The overall effect is a dynamic and futuristic aesthetic.

Zanim zaczniemy
Trochę historii i definicji





Eniac: **7M\$**

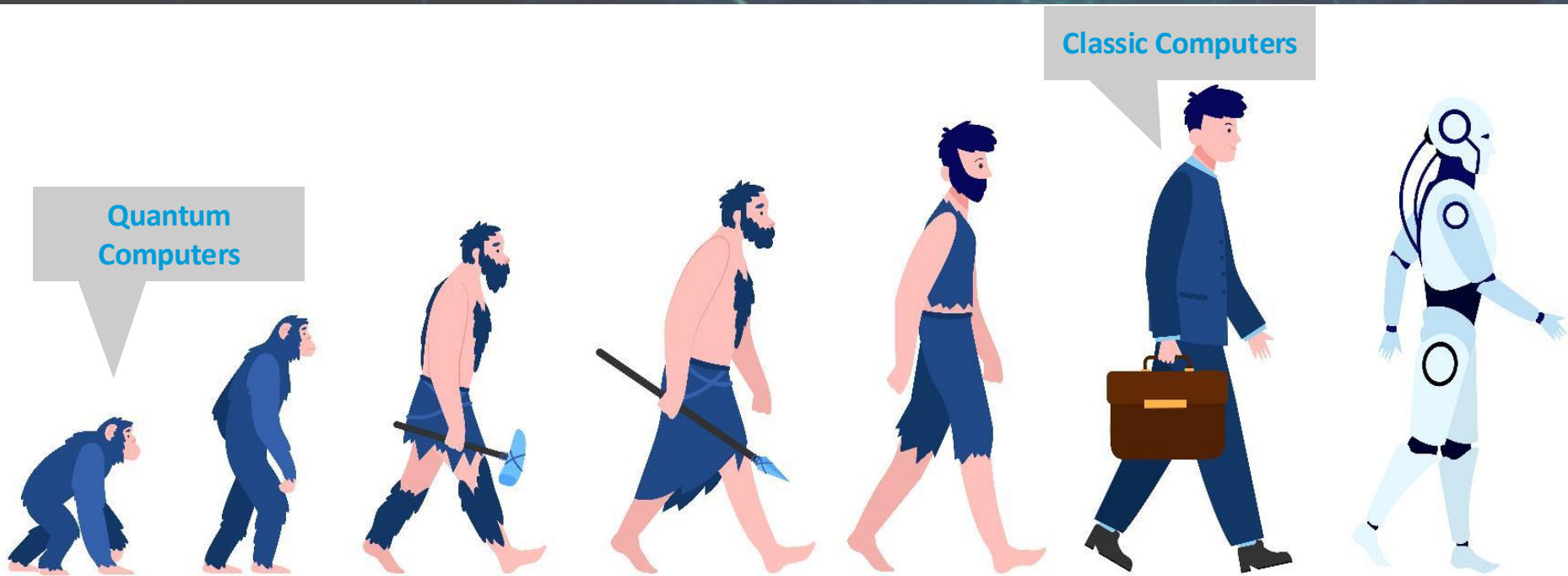


Chip: **0,1\$ (Dzisiaj)**



70 lat historii i taka zmiana

Current status of Quantum Computing maturity




Przydatne Definicje

1. **PQC (Post-Quantum Cryptography)** – Kryptografia postkwantowa, która opiera się na problemach matematycznych trudnych do rozwiązania nawet dla komputerów kwantowych.
2. **CRQC (Cryptographically Relevant Quantum Computer)** – Komputer kwantowy zdolny do łamania obecnie stosowanych algorytmów kryptograficznych, takich jak RSA i ECC.
3. **RSA (Rivest–Shamir–Adleman)** – Algorytm szyfrowania asymetrycznego oparty na trudności faktoryzacji liczb całkowitych.
4. **ECC (Elliptic Curve Cryptography)** – Kryptografia oparta na krzywych eliptycznych, oferująca mniejsze rozmiary kluczy w porównaniu z RSA, ale również zagrożona przez komputery kwantowe.
5. **LWE (Learning with Errors)** – Problem matematyczny polegający na rozwiązywaniu układów równań liniowych z losowymi błędami. Uważany za trudny do rozwiązania zarówno dla komputerów klasycznych, jak i kwantowych. Wykorzystywany w algorytmach takich jak CRYSTALS-Kyber.
6. **MLWE (Module Learning with Errors)** – Uogólnienie problemu LWE, stosowane w kryptografii opartej na kratkach modułowych. Wykorzystuje kratki o strukturze modułowej, co pozwala na efektywne operacje z dużymi wymiarami.
7. **NTT (Number Theoretic Transform)** – Algorytm używany w kryptografii opartej na kratkach do efektywniejszego wykonywania operacji na wielomianach, szczególnie przyspieszający mnożenie wielomianów w transformacji Fourierskiej.
8. **Hash-Based Signatures** – Podpisy cyfrowe oparte na funkcjach skrótu, takie jak SPHINCS+ i XMSS, które są odporne na ataki kwantowe.
9. **CRYSTALS-Kyber** – Algorytm wymiany kluczy oparty na MLWE, odporny na ataki komputerów kwantowych.
10. **CRYSTALS-Dilithium** – Algorytm podpisu cyfrowego oparty na MLWE, odporny na ataki kwantowe.
11. **SPHINCS+ (SLH-DSA)** – Stateless Hash-Based Digital Signature Algorithm, statelessowy algorytm podpisu cyfrowego oparty na funkcji skrótu, zaprojektowany do odporności na ataki kwantowe.
12. **LMS (Leighton-Micali Signature)** – Algorytm podpisu cyfrowego oparty na funkcji skrótu, używany w systemach oprogramowania i sprzętu.
13. **CNSA 2.0 (Commercial National Security Algorithm Suite 2.0)** – Zestaw algorytmów kryptograficznych opracowanych przez NSA do ochrony systemów bezpieczeństwa narodowego przed zagrożeniami kwantowymi.
14. **AES (Advanced Encryption Standard)** – Symetryczny algorytm szyfrowania blokowego, używany w CNSA 2.0 do szyfrowania danych.
15. **SHA (Secure Hash Algorithm)** – Rodzina funkcji skrótu, wykorzystywanych w kryptografii do zapewnienia integralności danych.

Przydatne Definicje

1. **XMSS (eXtended Merkle Signature Scheme)** – Algorytm podpisu cyfrowego oparty na drzewach Merkle'a, zapewniający odporność na ataki kwantowe.
2. **WOTS+ (Winternitz One-Time Signature Plus)** – Jednorazowy algorytm podpisu cyfrowego używany w schematach opartych na funkcjach skrótu, takich jak XMSS i SPHINCS+.
3. **Merkle Tree (Drzewo Merkle'a)** – Struktura danych wykorzystywana w kryptografii do efektywnego weryfikowania poprawności podpisów cyfrowych.
4. **Isogeny-Based Cryptography** – Kryptografia oparta na izogeniach między krzywymi eliptycznymi, jedna z potencjalnych ścieżek rozwoju kryptografii.
5. **Hybrid Cryptography** – Podejście do kryptografii polegające na łączeniu klasycznych algorytmów kryptograficznych z algorytmami postkwantowymi, aby zachować kompatybilność wsteczną i zwiększyć bezpieczeństwo.
6. **Kratki (Lattices)** – Struktury matematyczne w przestrzeni n-wymiarowej, używane w kryptografii postkwantowej (np. w algorytmach opartych na MLWE). Problemy takie jak najkrótszy wektor (SVP) są uważane za trudne do rozwiązania nawet przez komputery kwantowe.
7. **Wielomiany (Polynomials)** – Wzory matematyczne oparte na zmiennych podniesionych do potęgi, stosowane w operacjach kryptograficznych, szczególnie w algorytmach kratkowych i MLWE.
8. **Transformacja Fouriera (Fourier Transform)** – Narzędzie matematyczne do analizy funkcji przez rozkład ich na sinusoidy. W kryptografii często stosowana jako Number Theoretic Transform (NTT), co pozwala na szybsze operacje na wielomianach.
9. **Izogenie (Isogenies)** – Funkcje między krzywymi eliptycznymi, stosowane w kryptografii izogenii. Ich trudność w obliczeniu przy dużych danych zapewnia bezpieczeństwo kryptograficzne.
10. **Drzewo Merkle'a (Merkle Tree)** – Struktura danych używana do szybkiej weryfikacji integralności wielu elementów danych. Używana w podpisach cyfrowych takich jak XMSS.
11. **Funkcja skrótu (Hash Function)** – Funkcja, która zamienia dane wejściowe na unikalny wynik o stałej długości. W kryptografii funkcje skrótu są kluczowe w zapewnianiu integralności danych i w podpisach cyfrowych.
12. **Kolizja (Collision)** – Sytuacja, w której dwie różne wartości wejściowe funkcji skrótu generują ten sam wynik.
13. **Faktoryzacja liczb (Integer Factorization)** – Proces rozkładania liczby na czynniki pierwsze, co stanowi podstawę bezpieczeństwa RSA, ale jest łatwe do rozwiązania przez komputer kwantowy za pomocą algorytmu Shora.
14. **Logarytm dyskretny (Discrete Logarithm)** – Problem matematyczny, który stanowi podstawę bezpieczeństwa kryptografii krzywych eliptycznych (ECC). Jest trudny do rozwiązania klasycznymi metodami, ale komputer kwantowy może go rozwiązać przy pomocy algorytmu Shora.
15. **Grover's Algorithm** – Algorytm kwantowy, który umożliwia przyspieszenie wyszukiwania danych w nieuporządkowanych zbiorach. Działa w czasie kwadratowym, co ma wpływ na bezpieczeństwo kryptografii symetrycznej.



Qubit

Podstawa Komputera Kwantowego

Bity

1

0



bity

1

0

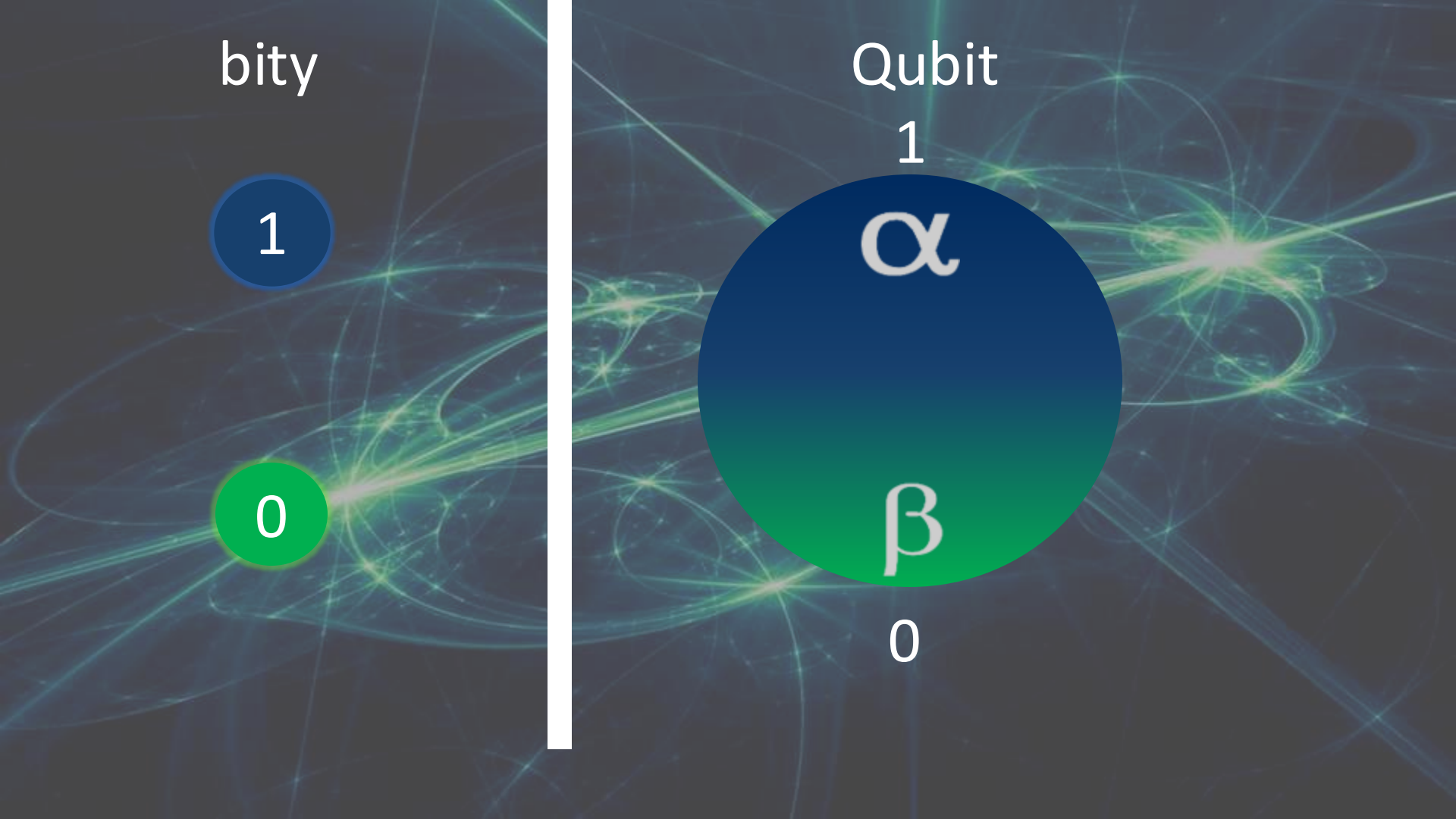
Qubit

1

α

β

0





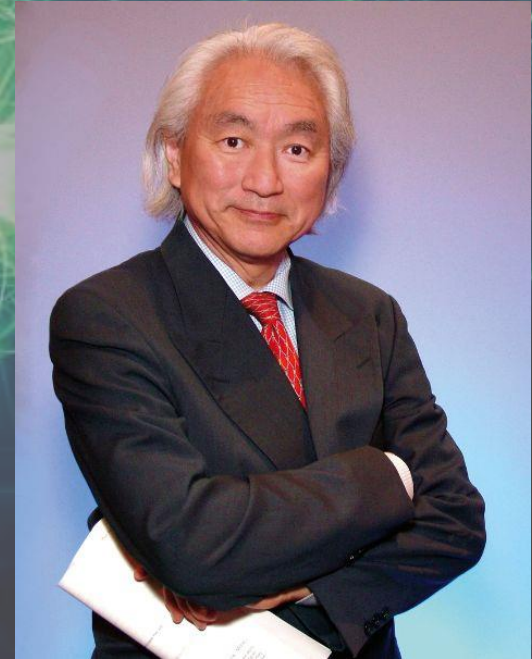
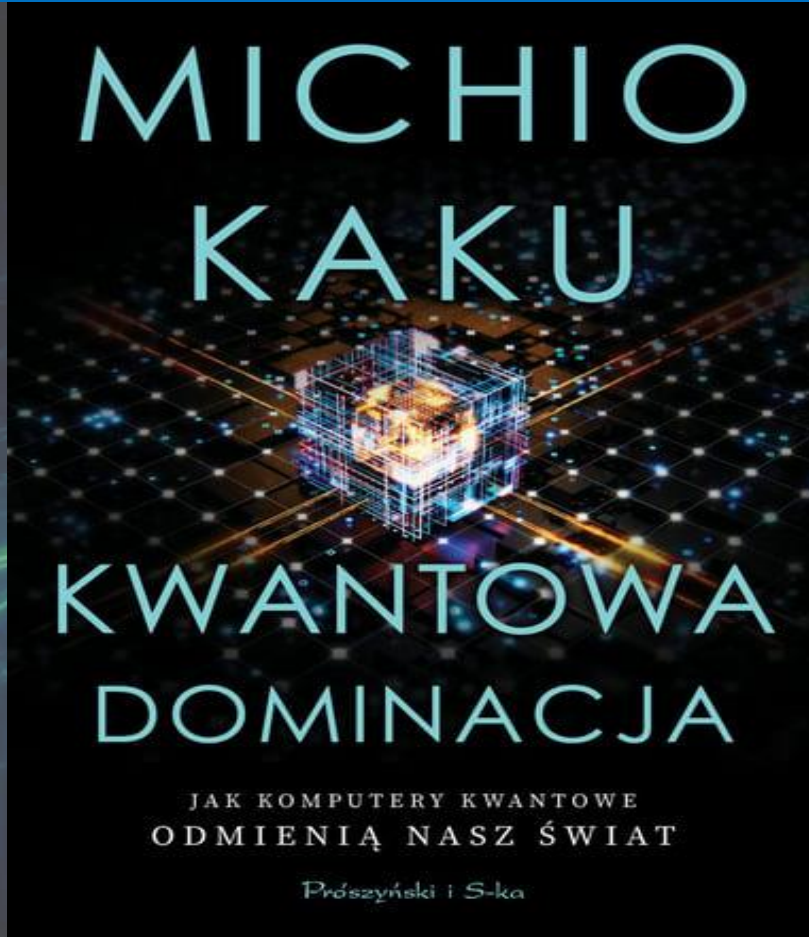


1



Superposition

Warto przeczytać!



Wszystkie stany... jednocześnie!



4



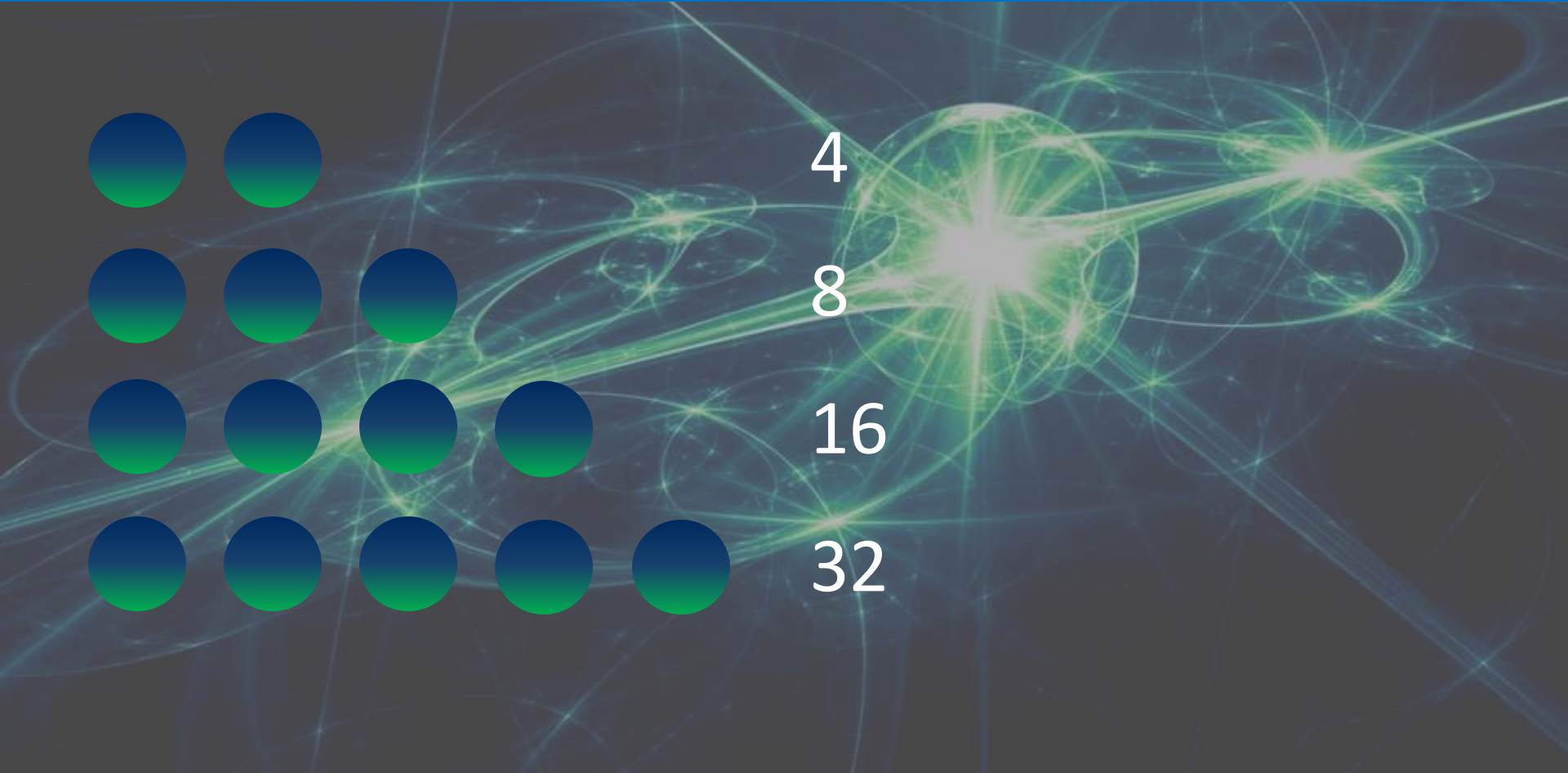
8



16



32

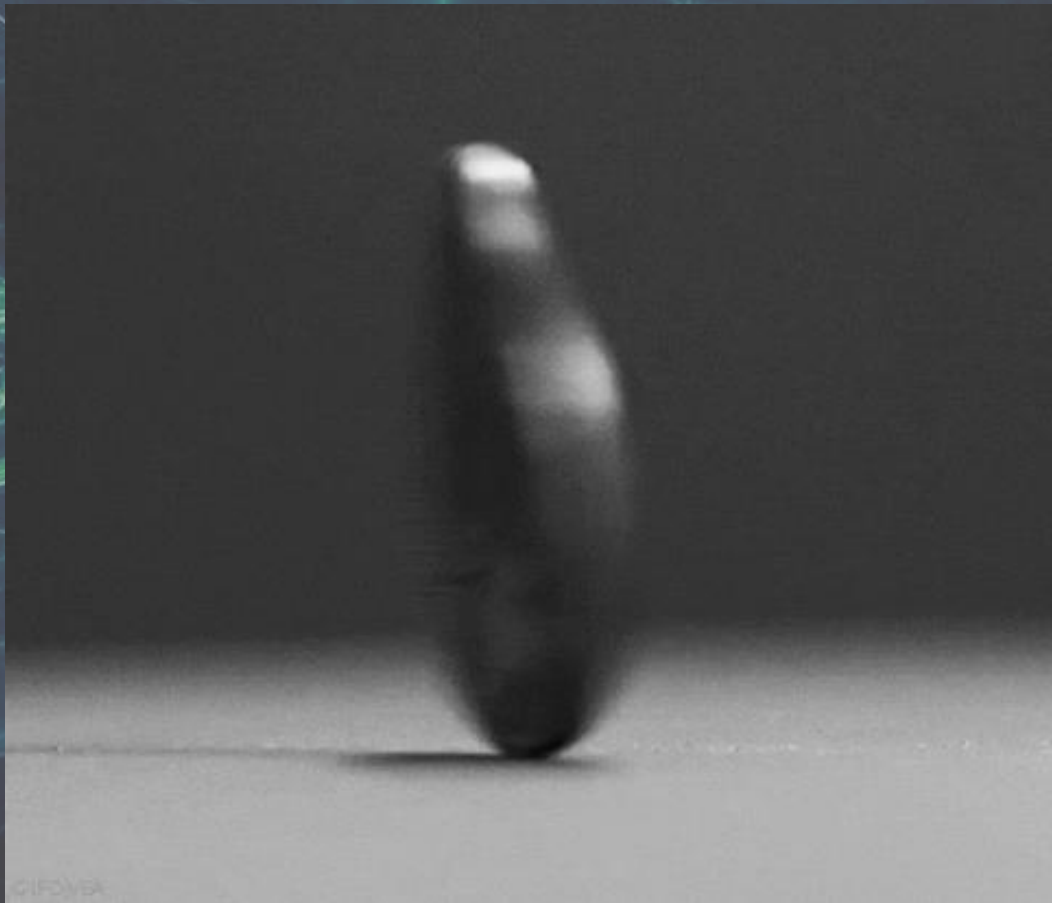




1

0

Qubit





Komputer Kwantowy

Jak działa

1996

Pierwszy komputer kwantowy był...



płynem (chloroform CHCl₃, 2 qubity)



W tym samym roku Intel wypuścił
Pentium MMX 200Mhz

Komputery kwantowe wymagają:

- ❖ Stabilnego środowiska
- ❖ Niskiego ciśnienia zewnętrznego
- ❖ Najlepiej temperatury bliskiej 0K
- ❖ Izolacji magnetycznej (brak interferencji)





Komputer Kwantowy

Jak działa?

ANGRY BIRDS



Komputer Klasyczny



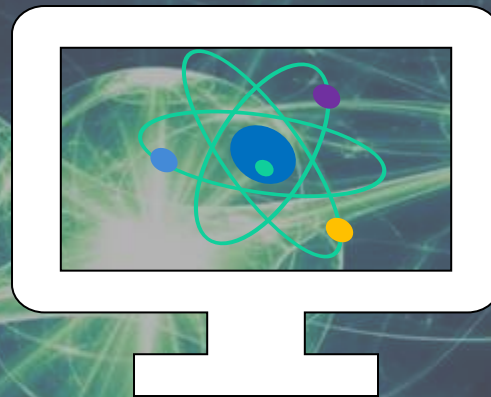
Analizuje bibliotekę
parametrów,
weryfikowaną na
podstawie zdefiniowanego
oprogramowania
(deterministyczne reguły i
algorytmy)

Komputer Klasyczny



Analizuje bibliotekę parametrów,
weryfikowaną na podstawie
zdefiniowanego oprogramowania
(**deterministyczne reguły i algorytmy**)

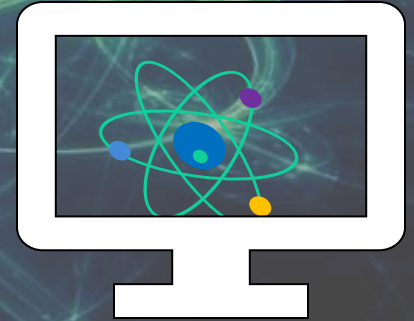
Komputer Kwantowy



Równoległa analiza
wszystkich stanów wybór
optymalnego

Ważna informacja!

Mysz kwantowa?





2,4 MLN Cores

10MWh Enerii/h

250 Petabytes RAM

200 PFLOPS/sec

Price: 200M USD

200 PFLOPS/sec

20.000 PS 5(*)



=





+

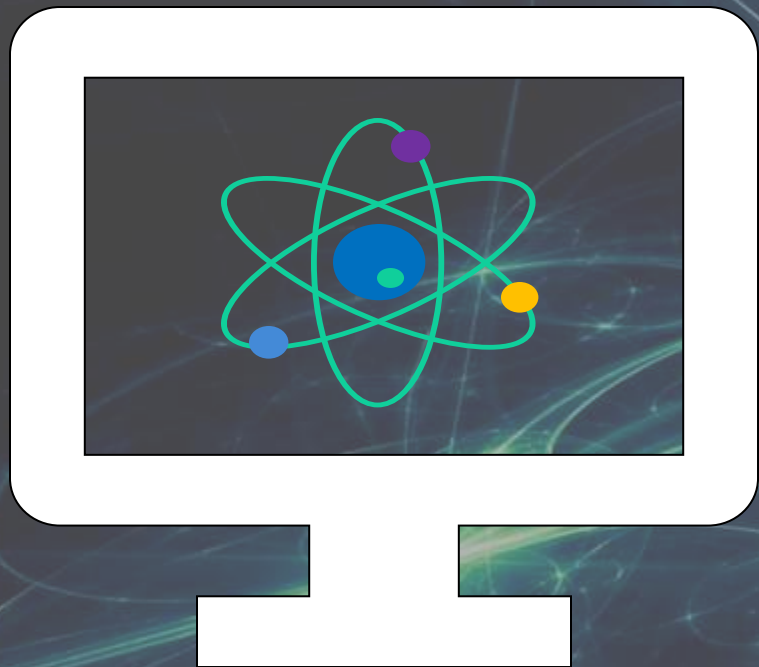


Moc: $N+N = 2N$



JAK ZWIĘKSZYĆ MOC

NA KOMPUTERZE KWANTOWYM?



+



Moc: 2^n

n – Liczba qubitów

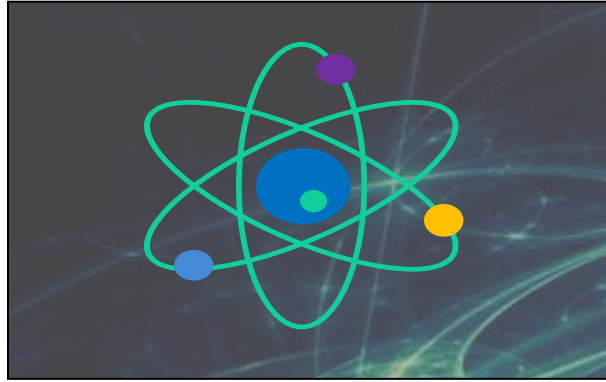
20 Qubitów - 1M stanów równocześnie



21 Qubitów - 2M stanów równocześnie



72 godzin
~~10.000 lat~~



Google

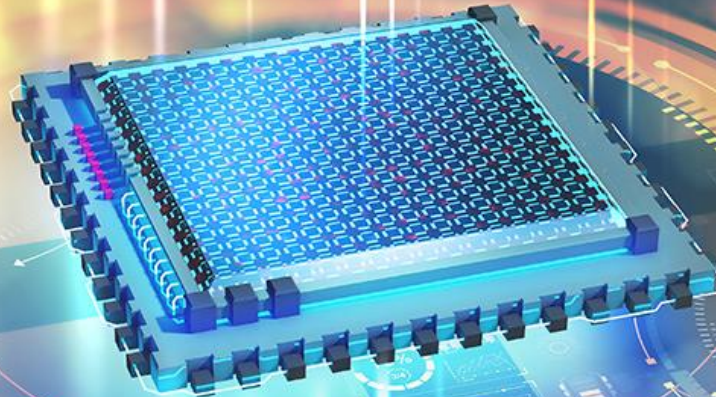
72 qubits

3m 20 sec

VS



Intel i QuTech - Horse Ridge



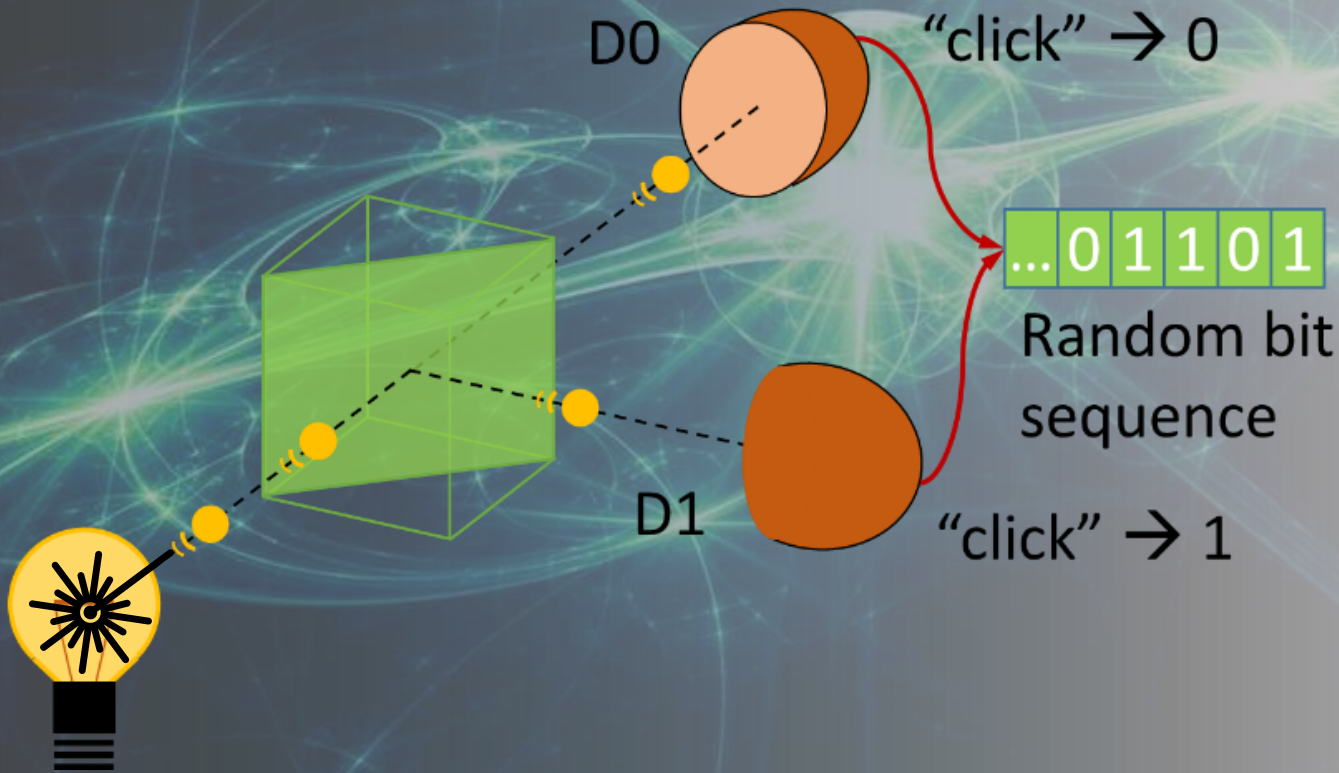
Control 4 * 32 qubits

75%

3/4

A 010010100

Przykład: Kwantowy generator liczb losowych





Algorytmy kwantowe

Jak działają



Obszar problemu do rozwiązania



**KOMPUTERY
KLASYCZNE**

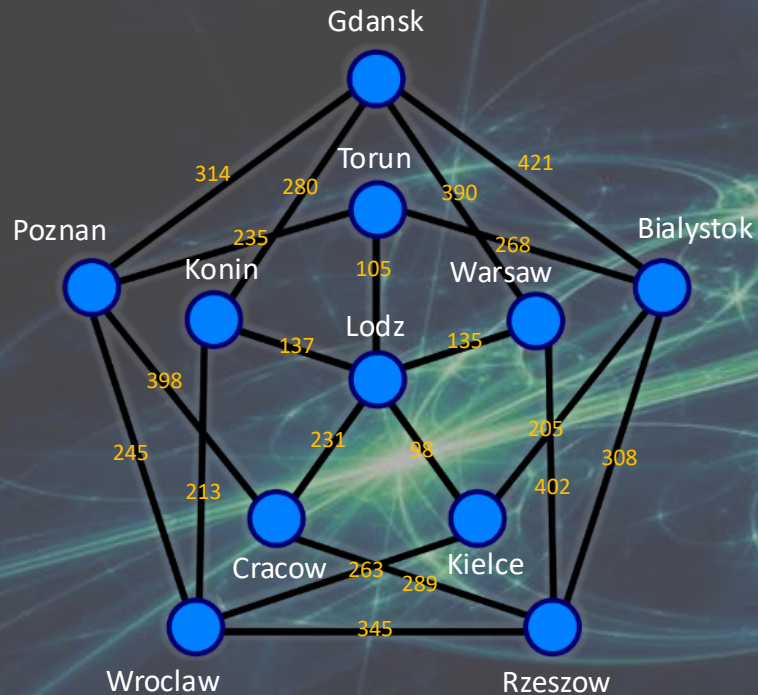
Obszar problemu do rozwiązania

Komputery kwantowe

Komputery
klasyczne

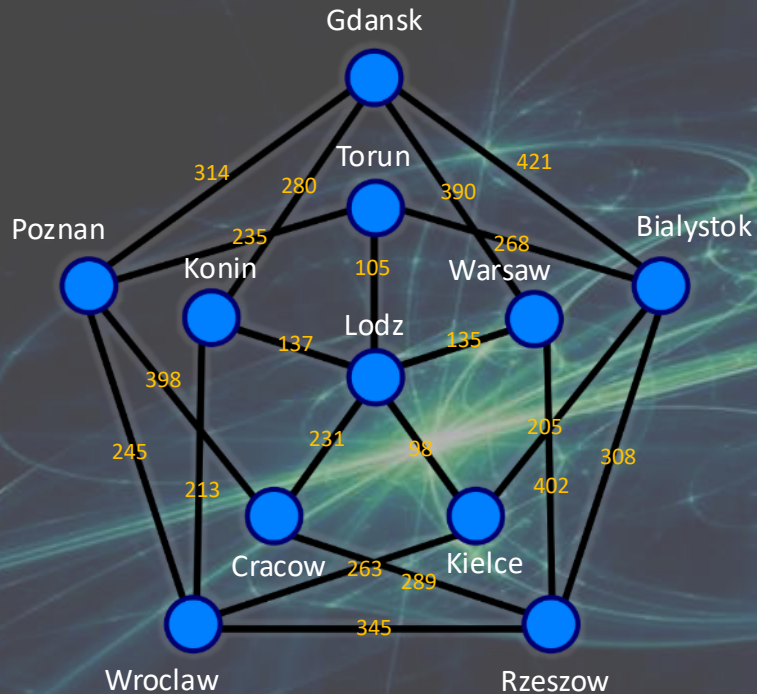


Przykład – Problem komiwojażera



- ❖ Miasta są połączone
- ❖ Komiwojażer może odwiedzić miasto tylko raz
- ❖ Cel: Minimalny koszt

EXAMPLE – the traveling salesman problem



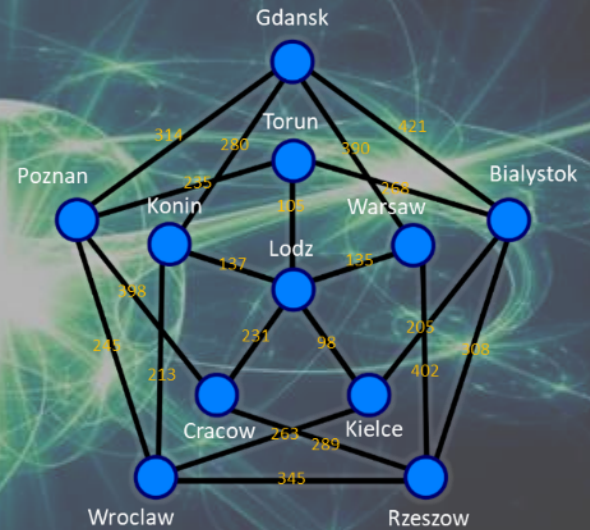
❖ 20 Miast ($n=20$)

❖ Liczba kombinacji

$$(n-1)!/2 = 60\,822\,550\,204\,416\,000$$

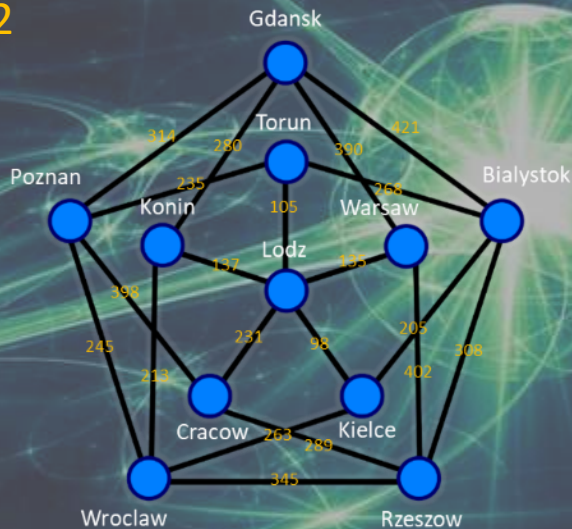
EXAMPLE – the traveling salesman problem

- ❖ 20 miast ($n=20$)
- ❖ Liczba kombinacji= $(n-1)!/2$
- ❖ 60 822 550 204 416 000
- ❖ Komputer klasyczny
- ❖ 1 Miliard op/sek,
- ❖ Czas: ok. 69 dni
- ❖ **Komputer Kwantowy**
- ❖ **1 op/sek, 57 qubitów**
- ❖ **Czas: Kilka minut (*)**



EXAMPLE – the traveling salesman problem

- ❖ 20 miast ($n=20$)
- ❖ Liczba kombinacji = $(n-1)!/2$
- ❖ 60 822 550 204 416 000
- ❖ Komputer klasyczny
- ❖ 1 Miliard op/sek,
- ❖ Czas: ok. 69 dni
- ❖ **Komputer Kwantowy**
- ❖ 1 op/sek, 57 qubitów
- ❖ Czas: Kilka minut (*)



25 miast?

Klasyczny
250.000 years

Kwantowy
83 qubits

Czas: Kilka minut (*)

Klucz Publiczny



$$M = p * q$$

Klucz publiczny

$$M = p * q$$

EXAMPLE **rsa-768** = **M**

123018668453011775513049495838496272077285356959533479219732245215172640050726365
751874520219978646938995647494277406384592519255732630345373154826850791702612214
2913461670429214311602221240479274737794080665351419597459856902143413

rsa-768 = the computation of two, large prime numbers:

334780716989568987860441698482126908177047949837137685689124313889828
83793878002287614711652531743087737814467999489 (p)

*

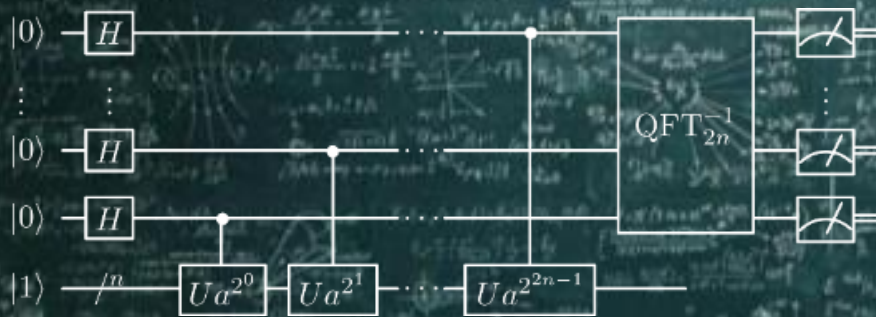
367460436667995904282446337996279526322791581643430876426760322838157
39666511279233373417143396810270092798736308917 (q)

Czy RSA jest bezpieczny?



Dekompozycja liczb na liczby pierwsze jest bardzo czasochonna. Algorytm "Sito liczb pierwszych" ma (sub) wykładniczy czas realizacji.

$$t_F \propto \exp\left[\left(\frac{64}{9}\right)^{1/3} (\ln N)^{1/3} (\ln \ln N)^{2/3}\right]$$



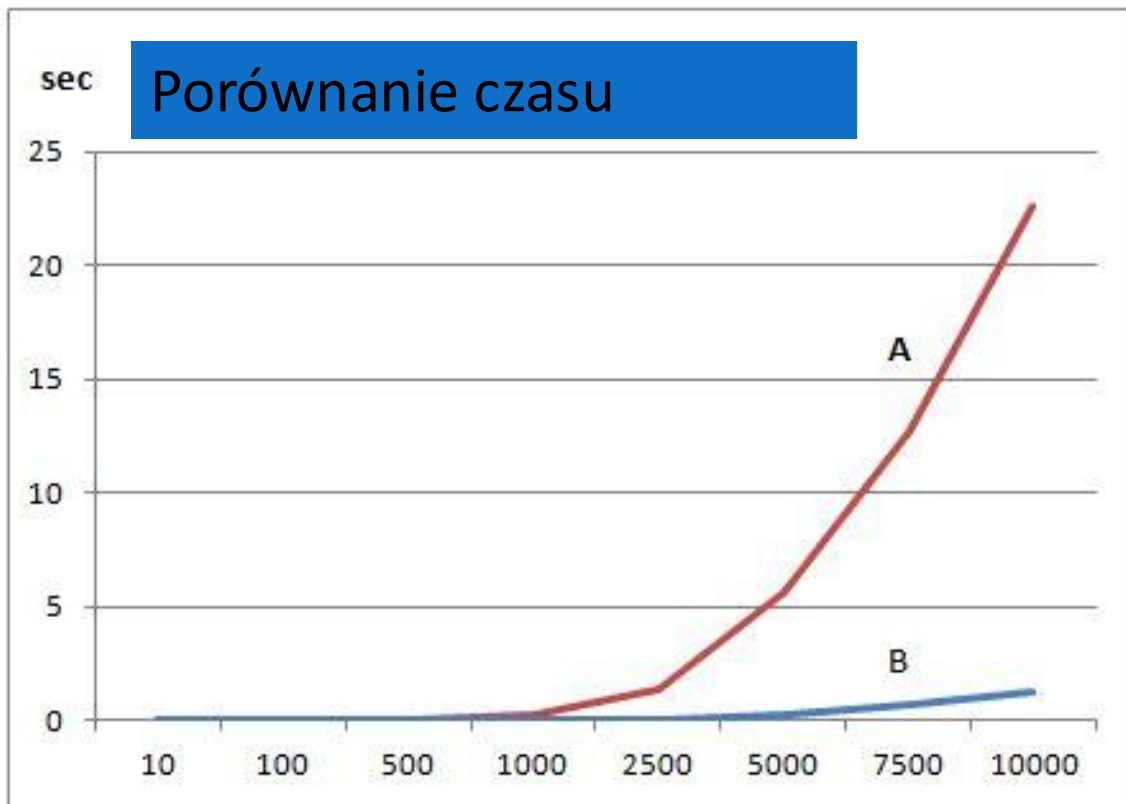
Algorytm Shora (1994)



Peter W. Shor

Z uwagi na wielomianową zależność czasu realizacji od liczby bitów (N), algorytm RSA nie jest bezpieczny w odniesieniu do algorytmu Shora!

Porównanie czasu

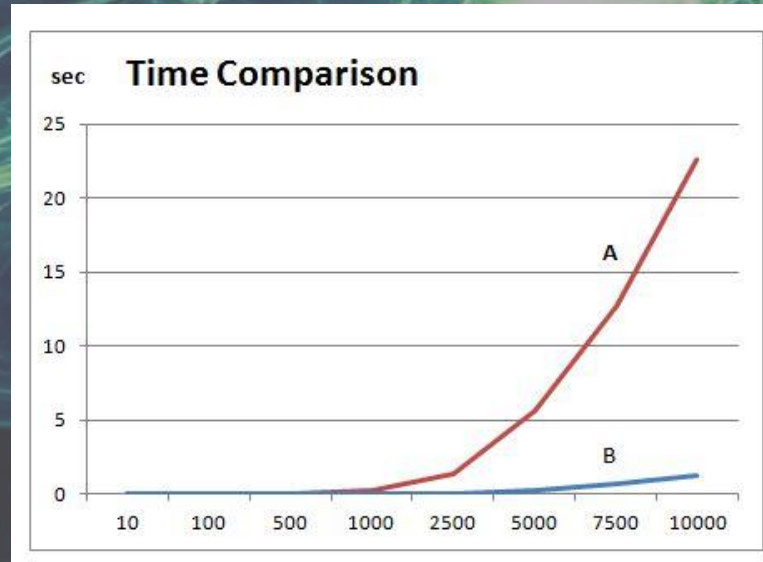


Wykładniczy (A)

do

Wielomianowy (B)

Potrzebne są **Algorytmy Postkwantowe**, odporne na przetwarzanie na komputerach kwantowych.



Czym jest kryptografia postkwantowa?

Definicja:

Kryptografia postkwantowa (PQC) to kryptografia, która opiera się na problemach matematycznych uznawanych za trudne do rozwiązania nawet przez komputery kwantowe.

Cel PQC: Stworzenie algorytmów odpornych na ataki zarówno ze strony komputerów klasycznych, jak i kwantowych.

Różnica między PQC a kryptografią kwantową:

PQC: działa na klasycznych komputerach, ale jest odporna na ataki kwantowe.

Kryptografia kwantowa: wykorzystuje właściwości mechaniki kwantowej do zabezpieczania komunikacji (np. dystrybucja klucza kwantowego - QKD).

Dlaczego potrzebujemy kryptografii postkwantowej?

Ryzyko związane z kwantowymi komputerami kryptograficznymi (CRQC):

CRQC to komputery kwantowe zdolne do łamania obecnych algorytmów kryptograficznych, co zagraża bezpieczeństwu informacji chronionych w przyszłości.

Przewidywana realizacja CRQC: rozwój komputerów kwantowych trwa, jednak nikt nie zna dokładnego terminu, kiedy CRQC stanie się rzeczywistością.

Zagrożenie dla bezpieczeństwa danych: dane przechwycone dziś mogą zostać odszyfrowane przez przyszły komputer kwantowy, co stanowi ryzyko dla informacji, które muszą pozostać poufne przez długi czas.

Dlaczego potrzebujemy kryptografii postkwantowej?

Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	-----	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Jak działa kryptografia postkwantowa?

Atak na kryptografię opartą na kluczach publicznych:

Obecne algorytmy, takie jak RSA i ECC, opierają się na problemach matematycznych związanych z faktoryzacją liczb i logarytmem dyskretnym, które są łatwe do rozwiązania przez komputer kwantowy.

Algorytmy PQC: Zamiast polegać na problemach związanych z faktoryzacją i logarytmami dyskretnymi, kryptografia postkwantowa opiera się na problemach uważanych za trudne do rozwiązania zarówno dla komputerów klasycznych, jak i kwantowych, takich jak problemy bazujące na kratkach, kodach, wielomianach i izogeniach

Rola NIST w standaryzacji kryptografii postkwantowej

Proces standaryzacji NIST:

NIST rozpoczął proces standaryzacji kryptografii postkwantowej w 2016 roku, aby wybrać algorytmy odporne na przyszłe ataki kwantowe.

82 propozycje algorytmów zostały zgłoszone, a po trzech rundach analiz wybrano pierwsze algorytmy do standaryzacji.

Algorytmy wybrane do standaryzacji w 2022(aktualizacja 2024) roku:

- CRYSTALS-Kyber (szyfrowanie)
- CRYSTALS-Dilithium (podpis cyfrowy)
- SPHINCS+ (podpis cyfrowy oparty na funkcji skrótu)

Rola NIST w standaryzacji kryptografii postkwantowej

Algorithm	Function	Specification
ML-KEM	Key establishment algorithm	NIST FIPS 203
ML-DSA	Digital signature algorithm	NIST FIPS 204
SLH-DSA	Digital signature algorithm for use cases such as signing firmware and software	NIST FIPS 205
LMS	Digital signature algorithm for use cases such as signing firmware and software	NIST SP 800-208
XMSS	Digital signature algorithm for use cases such as signing firmware and software	NIST SP 800-208

Zatwierdzone algorytmy przez NIST

CRYSTALS-Kyber:

Algorytm szyfrowania oparty na problemach związanych z kratkami modułowymi (MLWE).

Zastosowanie: bezpieczna wymiana kluczy i szyfrowanie danych.

Wyjątkowo wydajny i skalowalny.

CRYSTALS-Dilithium:

Algorytm podpisu cyfrowego oparty na tych samych problemach kratkowych.

Uznawany za jeden z najbezpieczniejszych i najbardziej wydajnych algorytmów postkwantowych do podpisu cyfrowego.

Zatwierdzone algorytmy przez NIST

SPHINCS+ (SLH-DSA):

Stateless Hash-Based Digital Signature Algorithm (SLH-DSA)

wykorzystujący funkcje skrótu.

Oparty na drzewach Merkle'a i podpisach jednorazowych WOTS+.

Nadaje się do systemów, które wymagają odporności na długotrwałe ataki kwantowe

Zatwierdzone algorytmy przez NIST

Kryptografia bazująca na kratkach

CRYSTALS-Kyber i Dilithium:

Oparte na problemie Learning With Errors (LWE) oraz jego odmianie MLWE.

Zalety:

Używa krutek, które są odporne na ataki zarówno komputerów klasycznych, jak i kwantowych.

Wydajne pod względem szybkości i zużycia zasobów.

Zastosowania: wymiana kluczy, podpisy cyfrowe, szyfrowanie danych.

Zatwierdzone algorytmy przez NIST

Podpisy stateless hash-based

SPHINCS+ (SLH-DSA):

Algorytm podpisu cyfrowego oparty na funkcjach skrótu.

Używa drzew Merkle'a oraz podpisów jednorazowych (WOTS+), co daje dużą odporność na ataki kwantowe.

Zalety:

Duża odporność na kwantowe ataki, nawet jeśli inne algorytmy kryptograficzne zawodzą.

Nie wymaga stanu wewnętrznego, co czyni go łatwiejszym do implementacji.

Zatwierdzone algorytmy przez NIST

Kryptografia oparta na kodach

McEliece Cryptosystem:

Oparty na kodach korekcyjnych.

Zalety: ponad 40 lat bezpiecznego stosowania bez poważnych ataków.

Wady: bardzo duże rozmiary kluczy publicznych (ponad 1 MB).

Zastosowanie: podpisy cyfrowe, szyfrowanie danych o wysokiej wartości.

Zatwierdzone algorytmy przez NIST

Kryptografia oparta na izogeniach

SIKE (Supersingular Isogeny Key Exchange):

Oparty na izogeniach między krzywymi eliptycznymi.

Zalety: małe rozmiary kluczy publicznych.

Wady: powolna wydajność i wciąż poddawany analizie bezpieczeństwa w długim terminie.

Zatwierdzone algorytmy przez NIST

Kryptografia oparta na układach wielomianowych

Rainbow:

Oparty na systemach wielomianów wielowymiarowych (Multivariate Polynomials).

Zalety: efektywne podpisy cyfrowe.

Wady: podatność na najnowsze techniki kryptoanalizy.

Hybrydowe podejścia do kryptografii postkwantowej

Łączenie kryptografii postkwantowej z tradycyjnymi systemami kryptograficznymi w celu uzyskania przejściowego bezpieczeństwa.

Przykład: połączenie kryptografii PQC z klasycznymi algorytmami, jak RSA lub ECDH, aby uzyskać odporność na ataki kwantowe, jednocześnie utrzymując kompatybilność z istniejącymi systemami.

Wyzwania związane z adopcją PQC

Wyzwania wydajnościowe i bezpieczeństwa:

Wydajność: Algorytmy PQC są wolniejsze od klasycznych odpowiedników, co może prowadzić do problemów w niektórych zastosowaniach.

Kompatybilność wsteczna: Wprowadzenie PQC wymaga kompatybilności z istniejącymi systemami kryptograficznymi.

Rozmiary kluczy: W kryptografii opartej na kratkach rozmiary kluczy mogą być znacznie większe niż w tradycyjnych algorytmach.

Ryzyko retrospektywnego odszyfrowania

Ataki "zapisz teraz, odszyfruj później":

Atakujący mogą przechwytywać zaszyfrowane dane dziś, a w przyszłości użyć komputerów kwantowych do ich odszyfrowania.

Zagrożenia: dane wrażliwe na długoterminową poufność, np. informacje rządowe, medyczne, finansowe.

Wyzwania implementacyjne

Zarządzanie kluczami:

Duże rozmiary kluczy, szczególnie w algorytmach opartych na kratkach, mogą wymagać bardziej złożonego zarządzania kluczami.

Ataki boczne (Side-channel attacks):

Kryptografia PQC wymaga ochrony przed atakami czasowymi, błędami sprzętowymi i wyciekiem informacji..

Rekomendacje dotyczące migracji do PQC

Zacznij migrację teraz:

- Ze względu na ryzyko odszyfrowania danych przez przyszłe komputery kwantowe, zaleca się rozpoczęcie migracji do kryptografii postkwantowej już teraz.

Wdrażanie hybrydowej kryptografii:

- Używanie algorytmów PQC w połączeniu z tradycyjnymi algorytmami, aby zachować zgodność z istniejącymi systemami, jednocześnie wprowadzając bezpieczeństwo postkwantowe

CNSA 2.0

CNSA 2.0: Zestaw algorytmów kryptograficznych opracowanych przez NSA w celu ochrony systemów bezpieczeństwa narodowego USA.

Powód aktualizacji: Zestaw CNSA 1.0, oparty na algorytmach takich jak RSA i ECC, jest podatny na przyszłe ataki komputerów kwantowych(CSA_CNSA_2.0_ALGORITHMS_).

Cele CNSA 2.0:

Zapewnienie bezpieczeństwa w erze postkwantowej.

Użycie algorytmów odpornych na ataki zarówno klasycznych, jak i kwantowych komputerów.

Zapewnienie długoterminowej ochrony danych w systemach o znaczeniu krytycznym.

CNSA 2.0



Public-key

CRYSTALS-Dilithium
CRYSTALS-Kyber

Symmetric-key

Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)

Software and Firmware Updates

Xtended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)

CNSA 2.0

Table 1: CNSA 2.0 algorithms for software and firmware updates

Algorithm	Function	Specification	Parameters
Leighton-Micali Signature (LMS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels. SHA-256/192 recommended.
Xtended Merkle Signature Scheme (XMSS)	Asymmetric algorithm for digitally signing firmware and software	NIST SP 800-208	All parameters approved for all classification levels.

CNSA 2.0


Table II: CNSA 2.0 symmetric-key algorithms

Algorithm	Function	Specification	Parameters
Advanced Encryption Standard (AES)	Symmetric block cipher for information protection	FIPS PUB 197	Use 256-bit keys for all classification levels.
Secure Hash Algorithm (SHA)	Algorithm for computing a condensed representation of information	FIPS PUB 180-4	Use SHA-384 or SHA-512 for all classification levels.

CNSA 2.0

Table III: CNSA 2.0 quantum-resistant public-key algorithms

Algorithm	Function	Specification	Parameters
CRYSTALS-Kyber	Asymmetric algorithm for key establishment	TBD	Use Level V parameters for all classification levels.
CRYSTALS-Dilithium	Asymmetric algorithm for digital signatures	TBD	Use Level V parameters for all classification levels.



Komputer Kwantowy

Wyzwania

Główne wyzwania



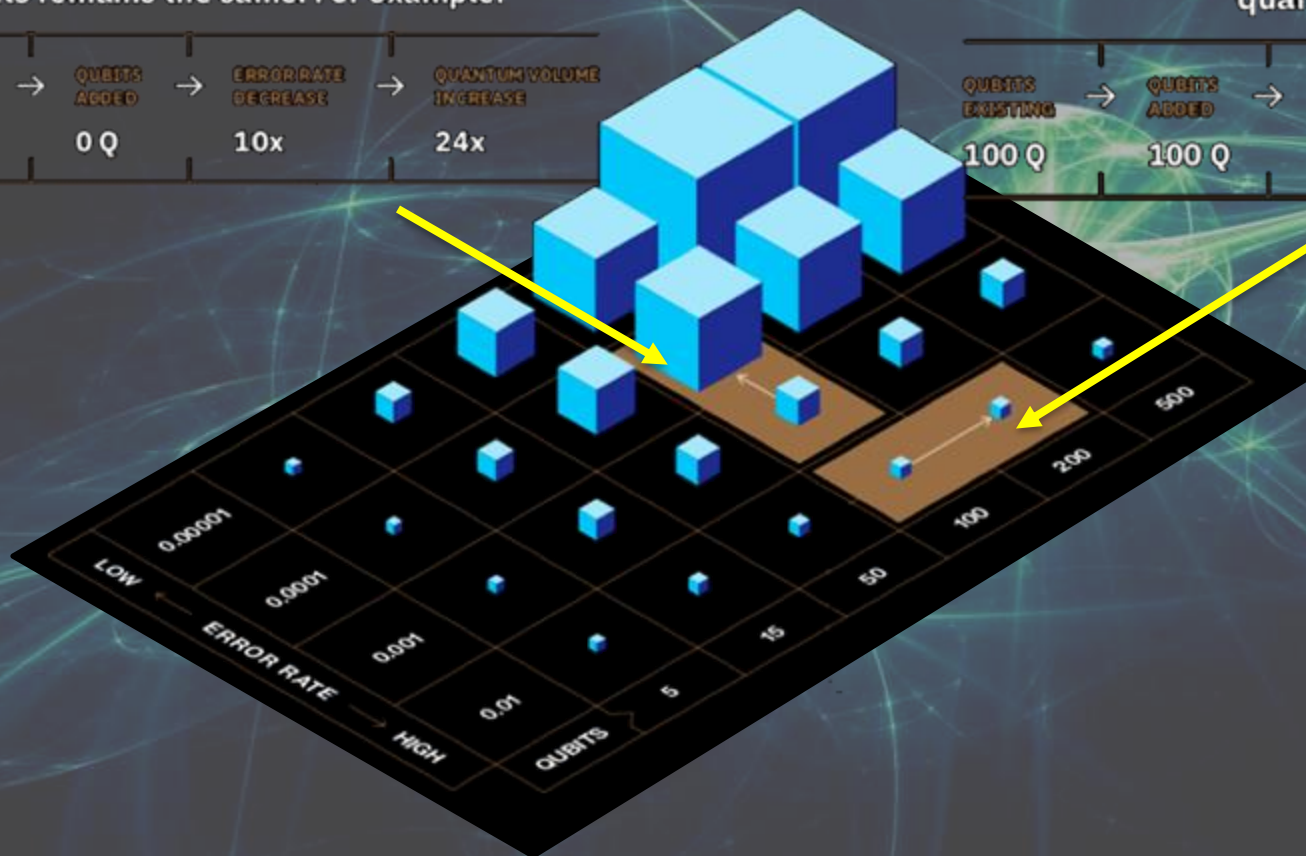
- ❖ Kontrola Qubitów - koherencja
- ❖ Błędy kalkulacji
- ❖ Stabilność
- ❖ Wielokrotność kalkulacji
- ❖ Wolne obliczenia

Improving the error rate can increase quantum volume even when the number of qubits remains the same. For example:

QUBITS EXISTING	QUBITS ADDED	ERROR RATE DECREASE	QUANTUM VOLUME INCREASE
100 Q	0 Q	10x	24x

If the error rate is high, merely adding qubits will not increase quantum volume.

QUBITS EXISTING	QUBITS ADDED	ERROR RATE DECREASE	QUANTUM VOLUME INCREASE
100 Q	100 Q	0x	0x



Jak zaprogramować Komputer kwantowy...

```
from qiskit import IBMQ
from qiskit.aqua import QuantumInstance
from qiskit.aqua.algorithms import Shor

IBMQ.enable_account('ENTER API TOKEN HERE') # Enter your API
token here
provider = IBMQ.get_provider(hub='ibm-q')

backend = provider.get_backend('ibmq_qasm_simulator') #
Specifies the quantum device

print('\n Shors Algorithm')
print('-----')
print('\nExecuting...\n')

factors = Shor(21) #Function to run Shor's algorithm where 21
is the integer to be factored

result_dict = factors.run(QuantumInstance(backend, shots=1,
skip_qobj_validation=False))
result = result_dict['factors'] # Get factors from results

print(result)
print('\nPress any key to close')
input()
```

Programowanie Komputera Kwantowego



quantumai.google/cirq/



aws.amazon.com/braket/



Microsoft Azure Quantum

Programowanie Komputera Kwantowego

The screenshot displays the IBM Quantum Experience web interface. At the top, the title bar reads "IBM Quantum Experience" with search and user icons. Below it is a menu bar with "File", "Edit", "Inspect", "View", and "Help". The main area is titled "Circuits / Untitled circuit Saving...". A toolbar contains various quantum gates: H, CNOT, Toffoli, X, Y, Z, S, S†, T†, U1, |0⟩, if, RX, RY, RZ, U3, Y, U2, CH, CY, CZ, CRX, CRY, CRZ, CU1, CU3, RXX, RZZ, and an "+ Add" button. The circuit workspace shows four qubits labeled q0, q1, q2, and c3. Below the workspace, there are two panels: "Measurement Probabilities" showing a bar chart for the state 000, and "Q-sphere" showing a Bloch sphere with a point at the top pole. A "Code editor" panel on the right contains the following Qiskit code:

```
Qiskit Read only
```

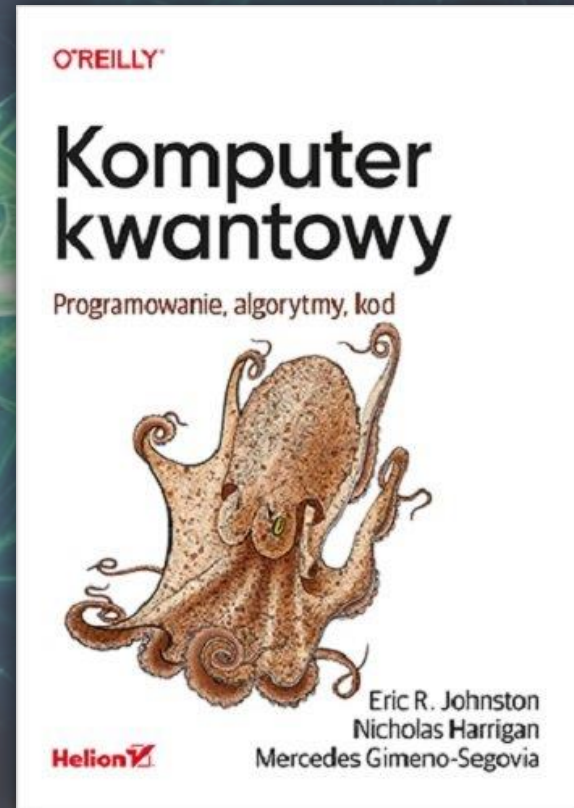
```
1 from qiskit import QuantumRegister,
2   ClassicalRegister, QuantumCircuit
3
4 qreg_q = QuantumRegister(3, 'q')
5 creg_c = ClassicalRegister(3, 'c')
6 circuit = QuantumCircuit(qreg_q,
7   creg_c)
```

The IBM logo is visible at the bottom of the monitor frame.

quantum-computing.ibm.com



Books

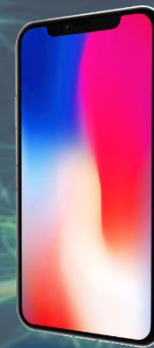
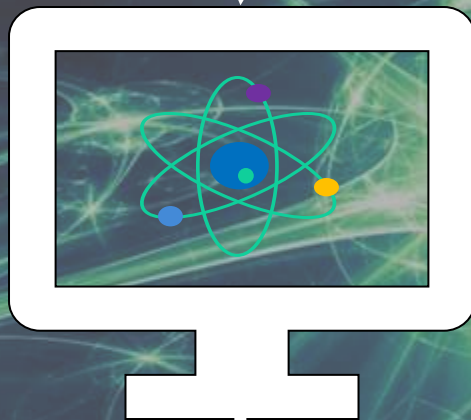




CZY BĘDĄ TELEFONY KWANTOWE...

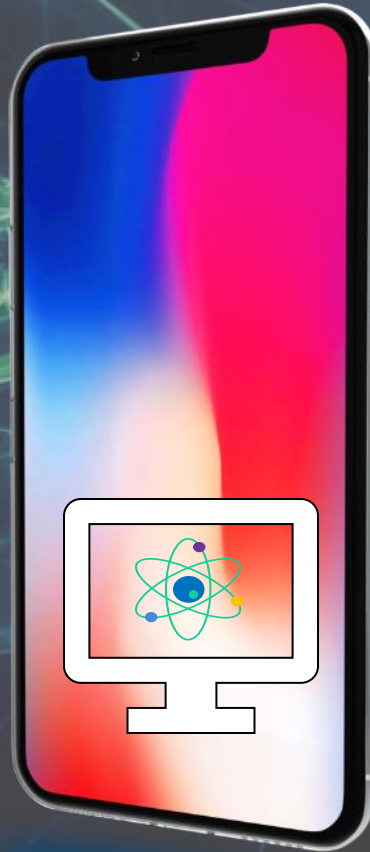


Ustawienia
i kontrola

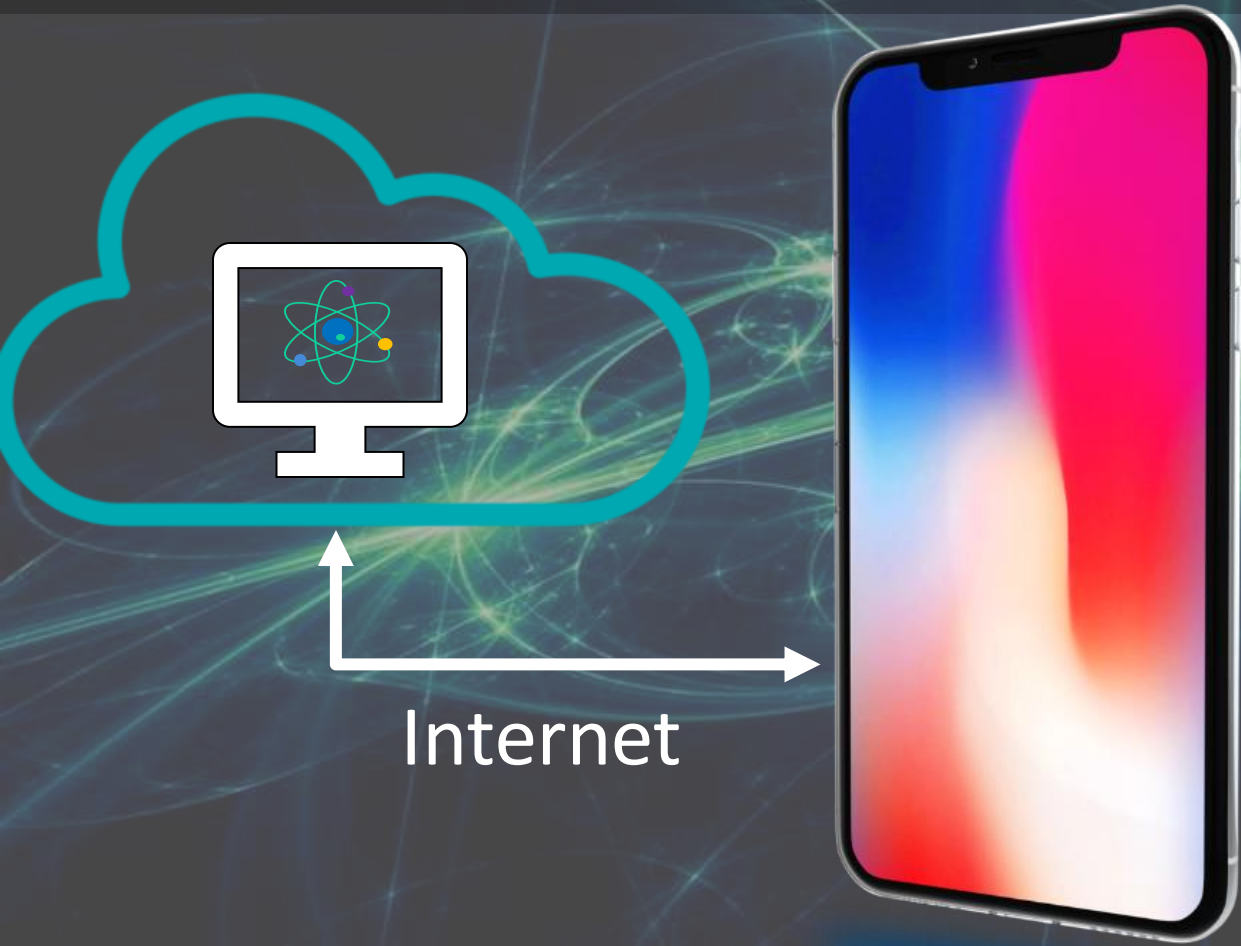


Rezultaty kalkulacji

Komputer kwantowy na telefonie?

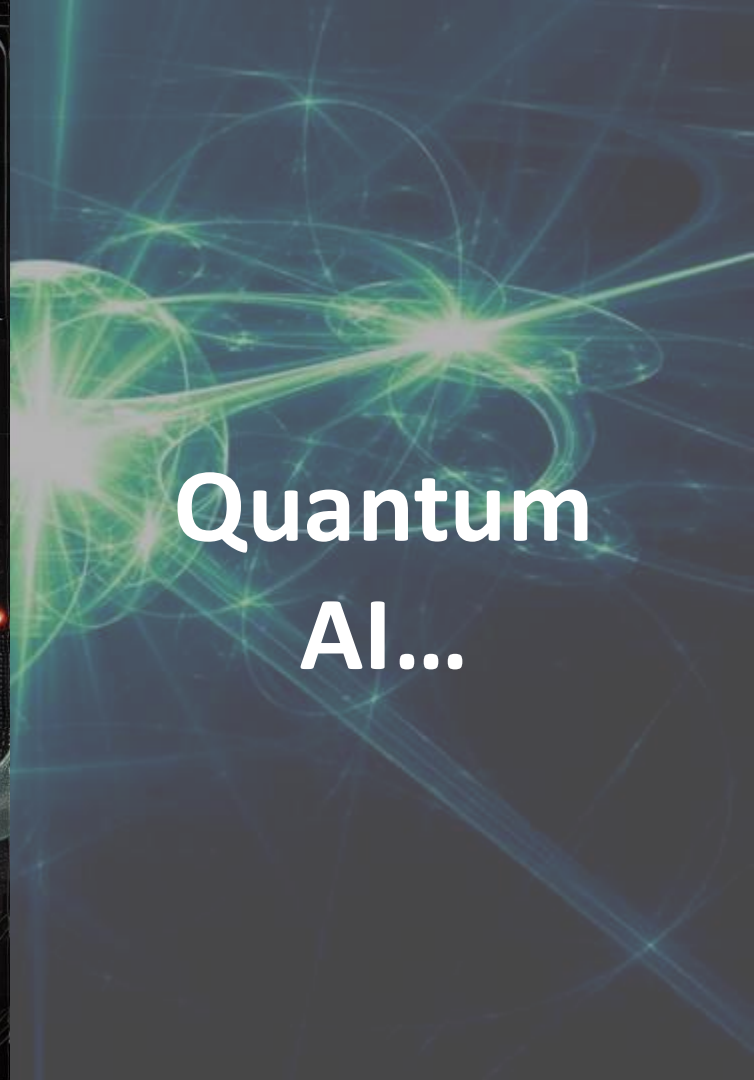


Komputer kwantowy na telefonie?



The background features a complex network of glowing green and blue lines and spheres, resembling a molecular structure or a data visualization. The lines are thin and intersect to form various shapes, including circles and spirals. The spheres are larger and more prominent, with a bright green glow. The overall effect is a sense of dynamic energy and interconnectedness.

I JESZCZE JEDNO...



Quantum AI...



You

When AI powered by quantum computing will rule the world? Just your prediction in 2 sentences.



llama3.1:latest

I predict that AI powered by quantum computing will have a profound impact on the world around 2055-2070, revolutionizing industries and transforming human societies with unprecedented efficiency, accuracy, and innovation. However, I also believe that this AI-driven evolution will be largely harmonious and collaborative, augmenting human capabilities rather than supplanting them, and ushering in a new era of human-machine symbiosis.

Dziękujemy za uwagę. Zapraszamy do kontaktu!



Jan Anisimowicz

C&F SA

Board Member of ISACA Warszawa

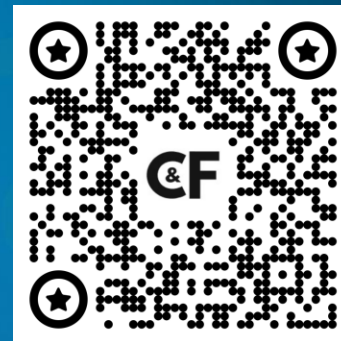
IIA Warszawa

Jan.Anisimowicz@candf.com



www.adaptivegrc.com

www.candf.com



Sebastian Burgemeister

BW Advisory Sp. z o.o.

IIA UAE (Dubai)

Former President of IIA Polska

s.burgemejster@itgrc.pl



www.itgrc.pl

www.akademiaitgrc.pl

