Kwanty, qubity i inni

PLAN

1. Kwant, Qubit, mechanika kwantowa
2. Komputery kwantowe
3. Algorytmy kwantowe
4. Kryptografia kwantowa
5. Kryptografia postkwantowa

Definicja

Kwant – najmniejsza porcja, jaką może mieć lub o jaką może zmienić się dana wielkość fizyczna w pojedynczym zdarzeniu.

Definicja

https://youtu.be/QpLdw1IC-Q0

Qubit - Definicja

Bit – 0 lub 1

Qubit - może istnieć w superpozycji stanów 0 i 1 jednocześnie (trochę zerem trochę jedynką**).**

Qubity - mogą być splątane (ang. entanglement), co oznacza, że stan jednego qubitu staje się skorelowany ze stanem innego qubitu, nawet jeśli są one fizycznie oddzielone.

Rejestr kwantowy

00000000
00000001
00000010
…
11111111

Rejestr tradycyjny
przechodzi przez wszystkie stany (2^n) sekwencyjnie (wraz z taktem zegarowym)

Rejestr kwantowy
Ma te wszystkie stany NARAZ.

Komputer kwantowy 64 qubitowy będzie 2^64 (18 trylionów) razy szybszy od komputera 64-bitowego!!!

Komputery kwantowe

- z wykorzystaniem qubitów **nadprzewodzących**:

Qubity są reprezentowane przez stany kwantowe strumienia w pętli nadprzewodzącej.

IBM Q; Google's Sycamore.

- z wykorzystaniem qubitów jonowych:

Qubity są reprezentowane przez stany kwantowe jonów w **pułapkach jonowych**.

IonQ

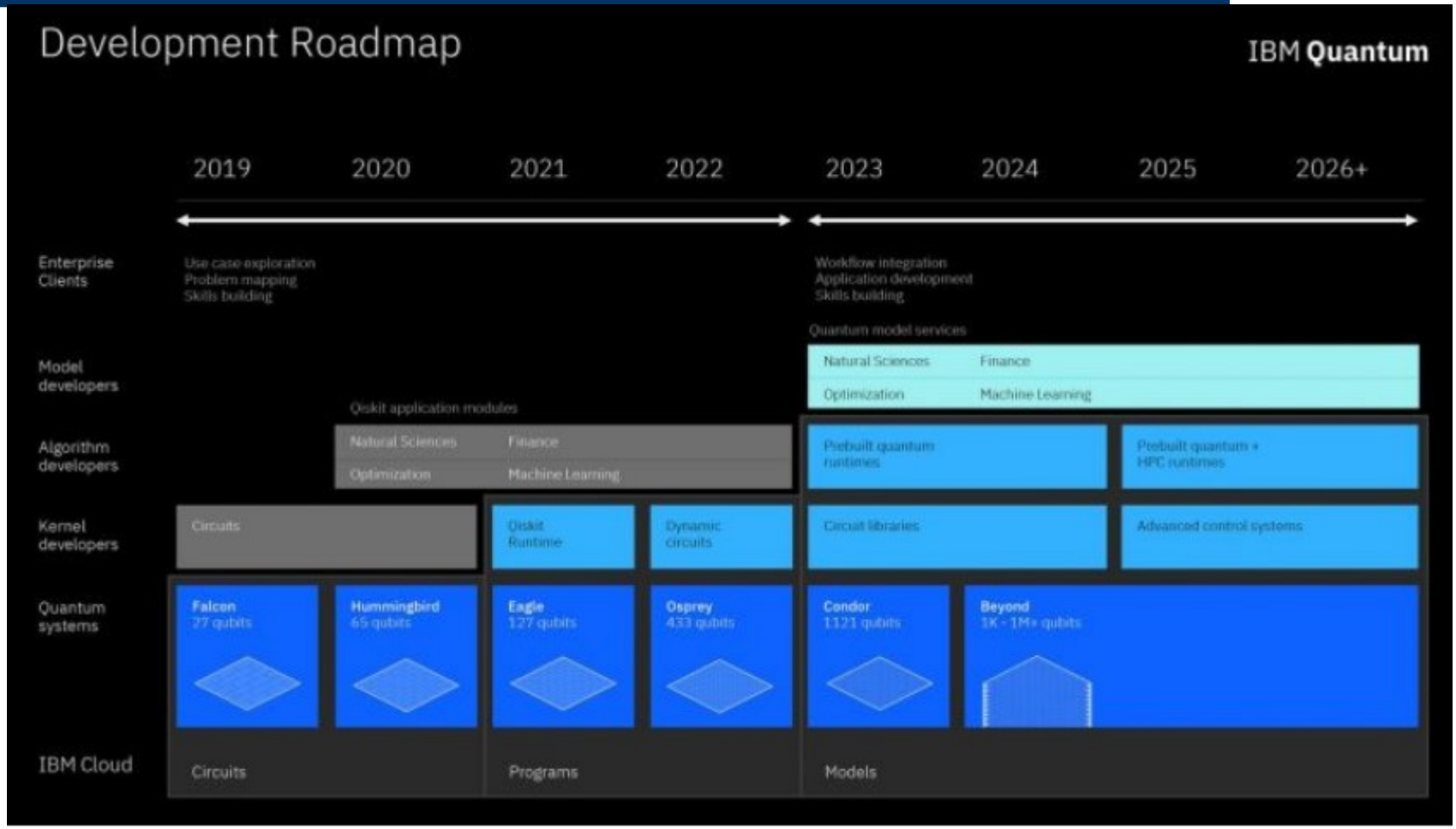
- z wykorzystaniem qubitów półprzewodnikowych:

Qubity są reprezentowane przez stany kwantowe ładunku lub **spinu elektronów w półprzewodnikach**.

Intel

Istnieją komputery nie kwantowe ale wykorzystujące zjawiska kwantowe.

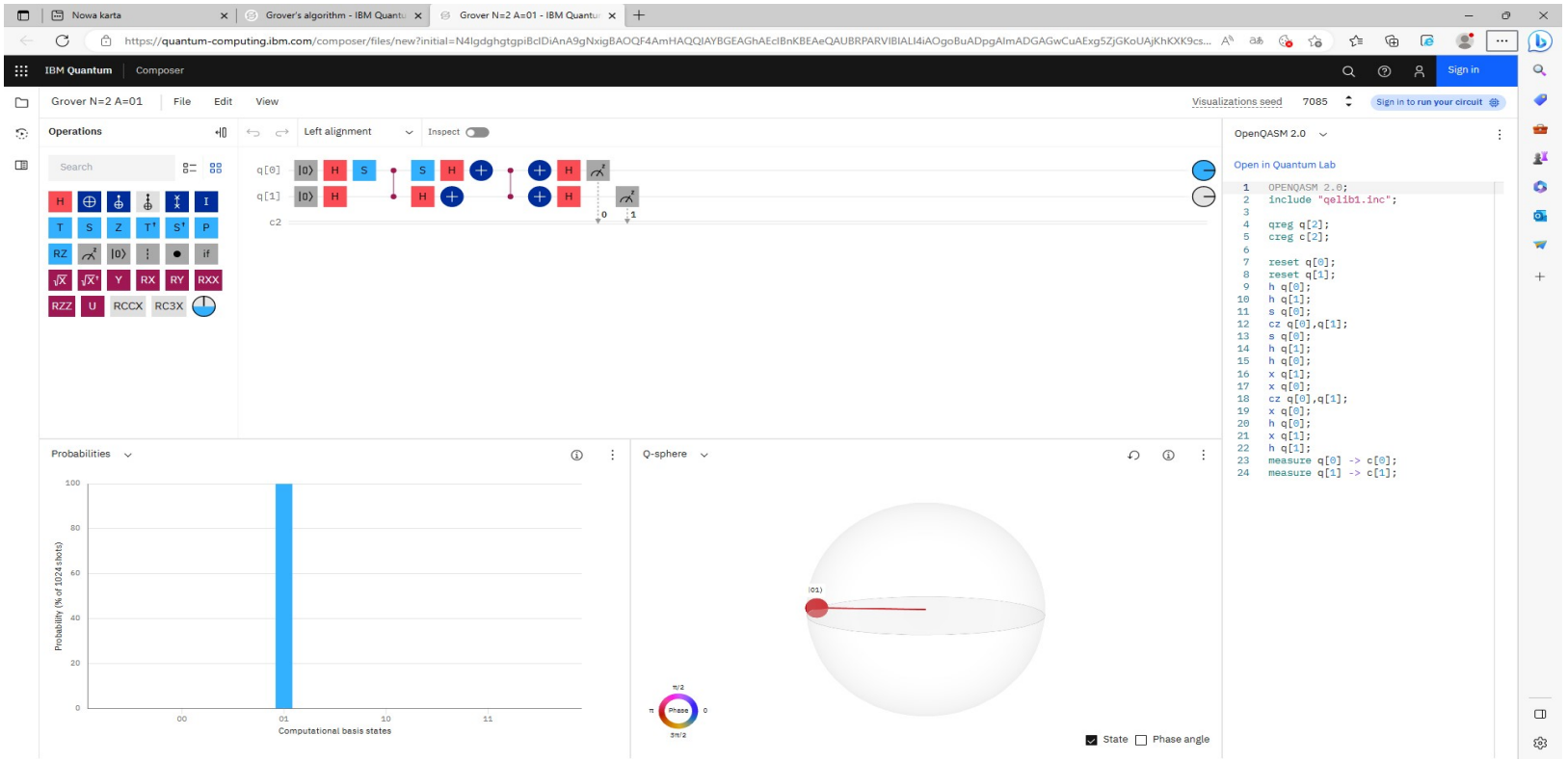
Komputery kwantowe



Komputery kwantowe

https://quantum-computing.ibm.com/composer/files/new

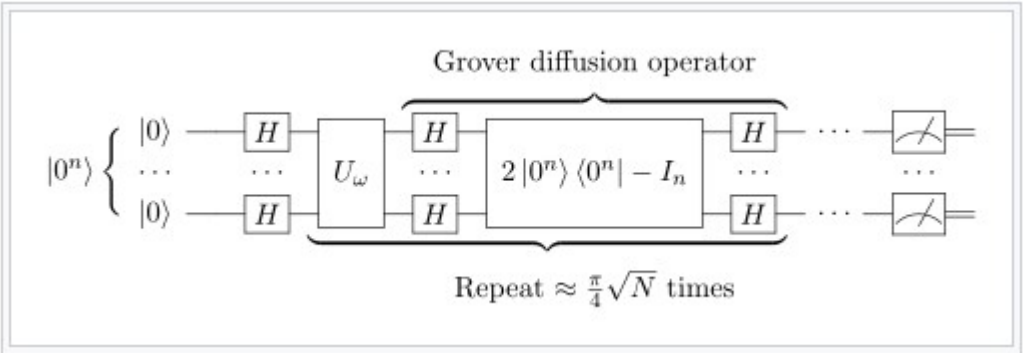
Komputery kwantowe



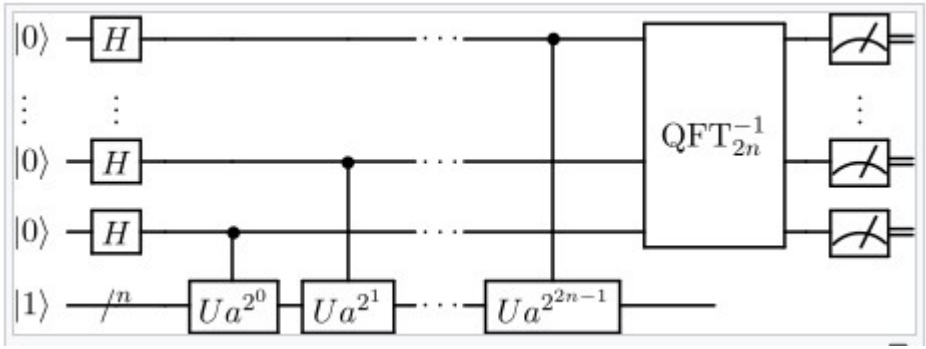
Komputery kwantowe

Algorytmy kwantowe

- **Grovera – przeszukiwania**

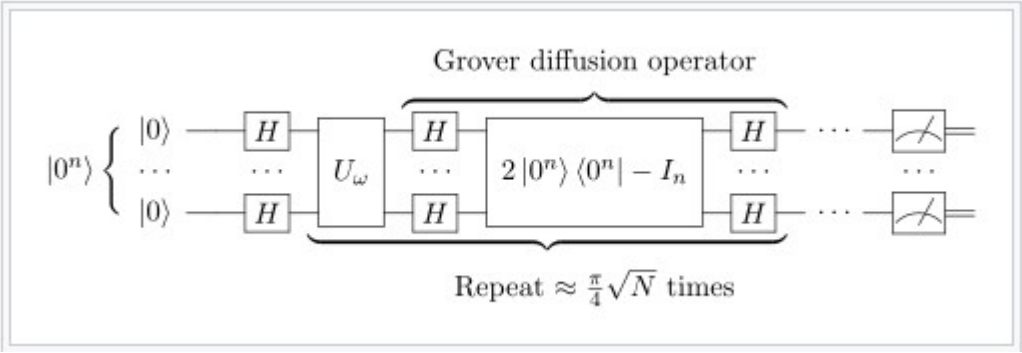


- **Shora – znajdowania liczb pierwszych**



Algorytmy kwantowe

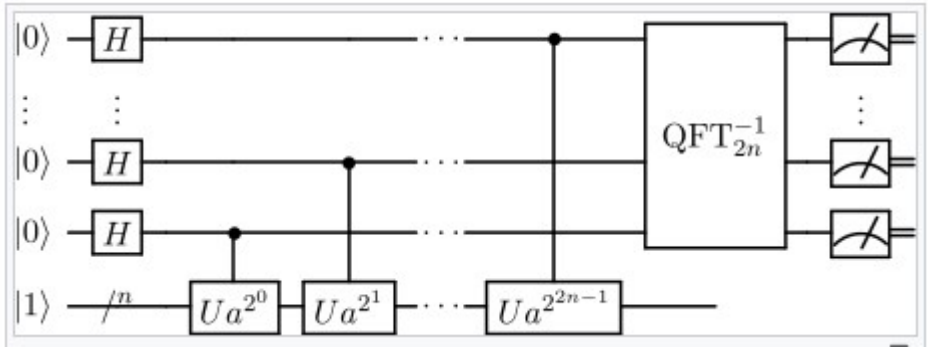
- **Grovera – przeszukiwania**



p(n) : 1/n -> 1/√n klucz: 128 -> 64

Algorytmy kwantowe

- **Shora – znajdowania liczb pierwszych**



$C_{11}H_5F_5O_2Fe$

IBM 2001r - 7 - qubitowa implementacja algorytmu Shora

Kryptografia kwantowa

Kryptografia kwantowa odnosi się głównie do protokołów i technik używanych do bezpiecznej **wymiany klucza** kwantowego między nadawcą a odbiorcą. Proces ten polega na wykorzystaniu zasad mechaniki kwantowej do stworzenia klucza, który jest bezpieczny przed przechwyceniem przez potencjalnego atakującego.

Kryptografia kwantowa

Kryptografia kwantowa >

Kwantowa dystrybucja klucza

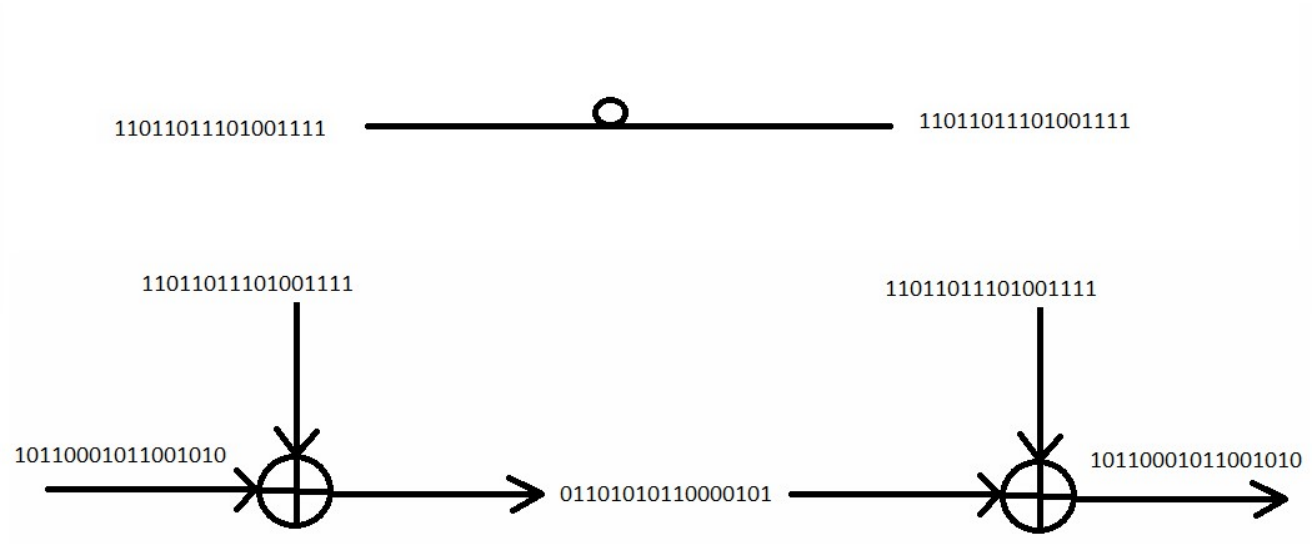
Kryptografia kwantowa

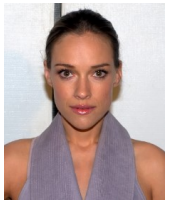
Protokół BB84: Charles H. Bennett i Gilles Brassard (1984) – polaryzacja

Protokół E91: Artur Ekert (1991)

- splątanie

Kryptografia kwantowa





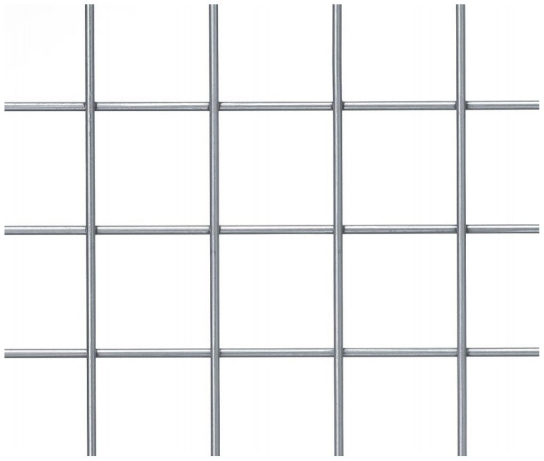
Kryptografia postkwantowa

Algorytm Grovera – osłabia algorytmy symetryczne, funkcje skrótu

Algorytm Shora – znacząco osłabia algorytm asymetryczny RSA, problem logarytmu dyskretnego (też dla krzywych eliptycznych)

Kryptografia postkwantowa

Dlatego niezbędne było poszukiwanie algorytmów odpornych na algorytmy kwantowe.



Kryptografia postkwantowa

Keccak?
SHA-3?

NTRUEncrypt* – algorytm szyfrowania
NTRUESign* – podpis cyfrowy

* opatentowane

Kryptografia postkwantowa

NIST (ang. National Institute of Standards and Technology) prowadzi konkurs na postkwantowe algorytmy asymetryczne od 2017 roku, a obecnie trwa czwarta runda tego konkursu. Trzecia runda zakończyła się w 2022 roku i po niej ogłoszono pierwsze kryptosystemy rekomendowane jako standardy postkwantowe:

- Crystals-Dilithium,
- Falcon,
- SPHINCS+,
- Crystals-Kyber (uzgadnianie klucza, np. dla witryn).

[https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions]

Extra materiały i slajdy

https://csrc.nist.gov/Projects/Cryptographic-Standards-and-Guidelines

https://slideplayer.pl/slide/816981/

https://docplayer.pl/60856541-W5-komputer-kwantowy.html