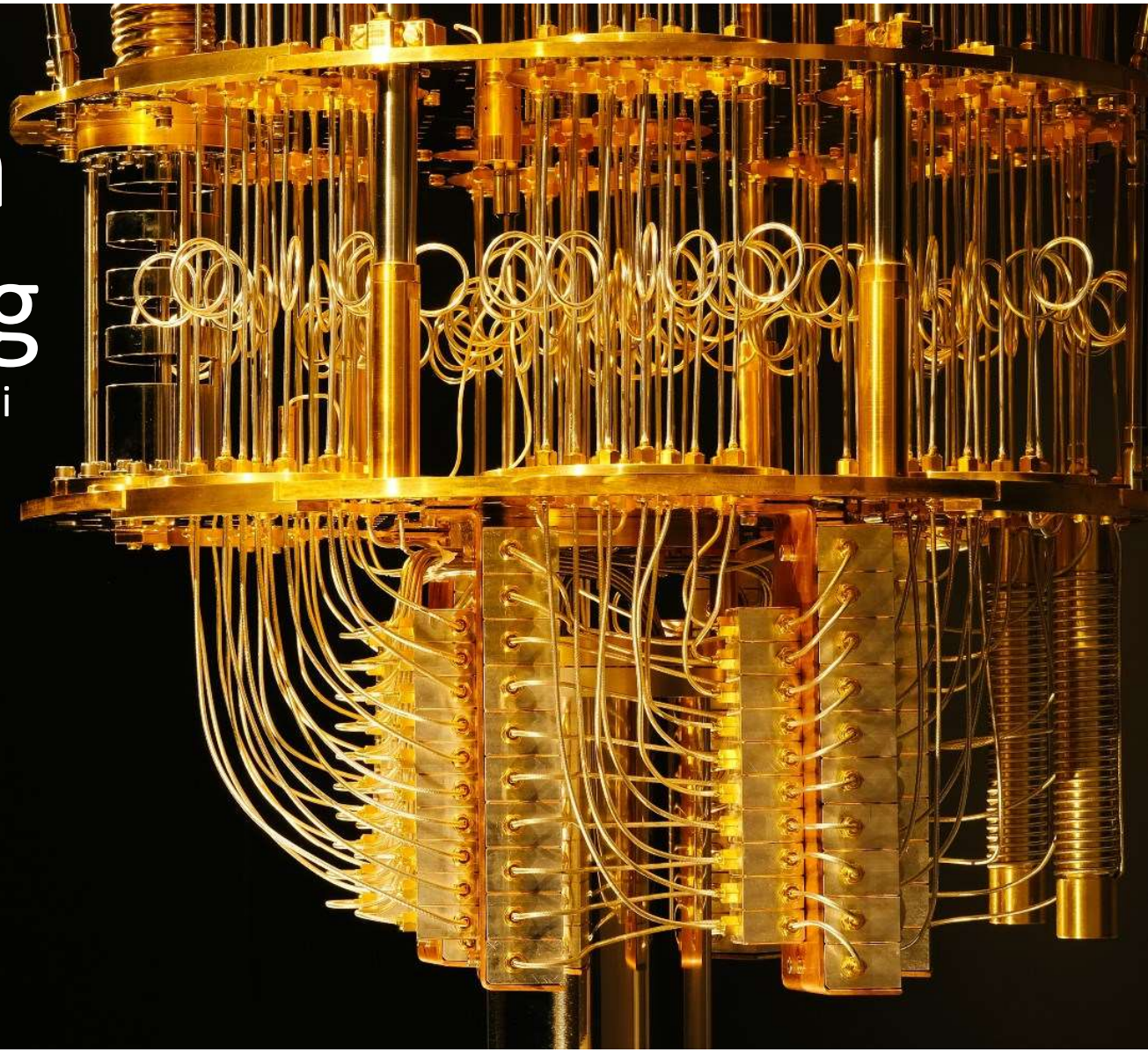
Quantum computing

Elemente de arhitectură și criptografie post-cuantică



Pandelea Dariand-Florian W.

Dragomir Mircea-Constantin

Photo source: IBM

Notiuni Introductive

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \equiv \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix}.$$

$$\begin{bmatrix}a\\b\end{bmatrix} \otimes \begin{bmatrix}c\\d\end{bmatrix} = \begin{bmatrix}ac\\ad\\bc\\bd\end{bmatrix}$$

- Qubiti
- Produs Tensor
- Notatie Dirac $|\Phi^+\rangle$
- Porti Cuantice
- Criteriile lui DiVicenzo:
  - Un sistem fizic scalabil cu qubiti bine-caracterizati
  - Abilitatea de a initializa qubitii intr-o stare de baza
  - Timpuri de decoerenta relevante lungi
  - Un set universal de porti
  - Abilitatea specifica de a masura qubitii
  - Bonus: Abilitatea de a interconverti qubitii zburatori si cei stationari + de a transmite qubiti zburatori intre locatii specificate

$$I = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$$

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$$

$$R_x(\theta) = \begin{bmatrix}\cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2})\\-i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{bmatrix}$$

$$R_y(\theta) = \begin{bmatrix}\cos(\frac{\theta}{2}) & -\sin(\frac{\theta}{2})\\\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{bmatrix}$$

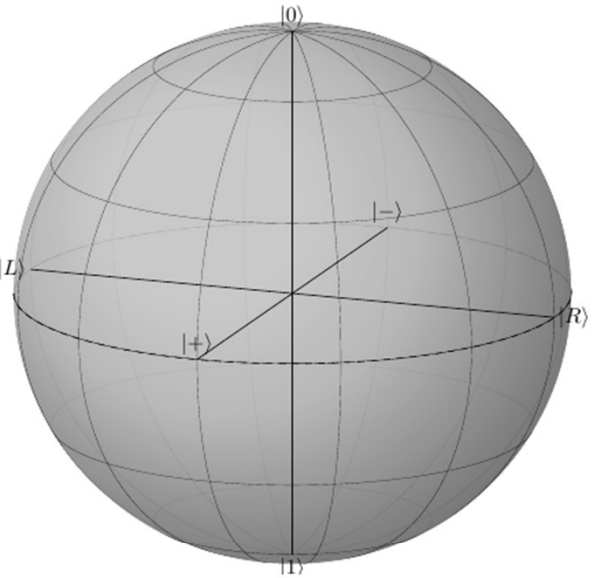
$$R_z(\theta) = \begin{bmatrix}\exp(-i\frac{\theta}{2}) & 0\\0 & \exp(-i\frac{\theta}{2})\end{bmatrix}$$

$$X = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$$

$$Y = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$$

$$Z = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$$

$$P(\varphi) = \begin{bmatrix}1 & 0\\0 & e^{i\varphi}\end{bmatrix}$$



$$CNOT = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}$$

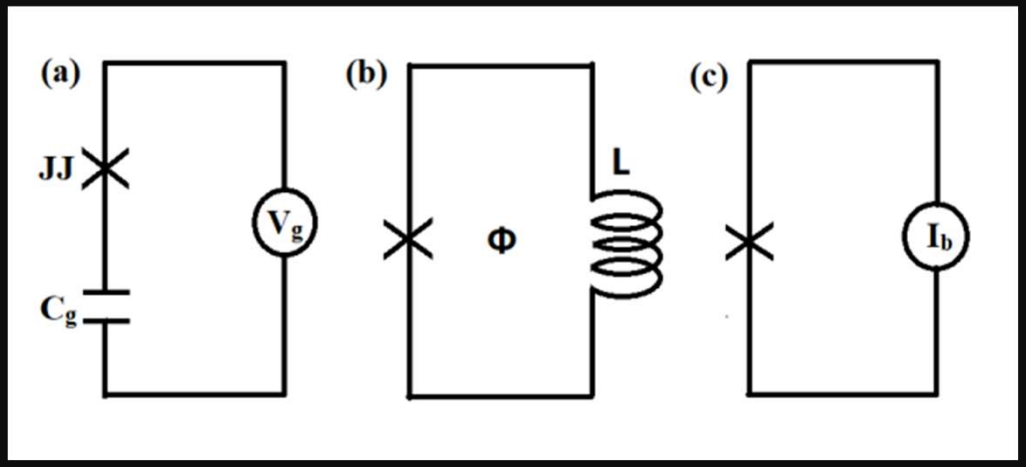
QUANTUM COMPUTING FOR COMPUTER SCIENTISTS
Noson S. Yanofsky
Brooklyn College, City University of New York
and
Mirco A. Mannucci

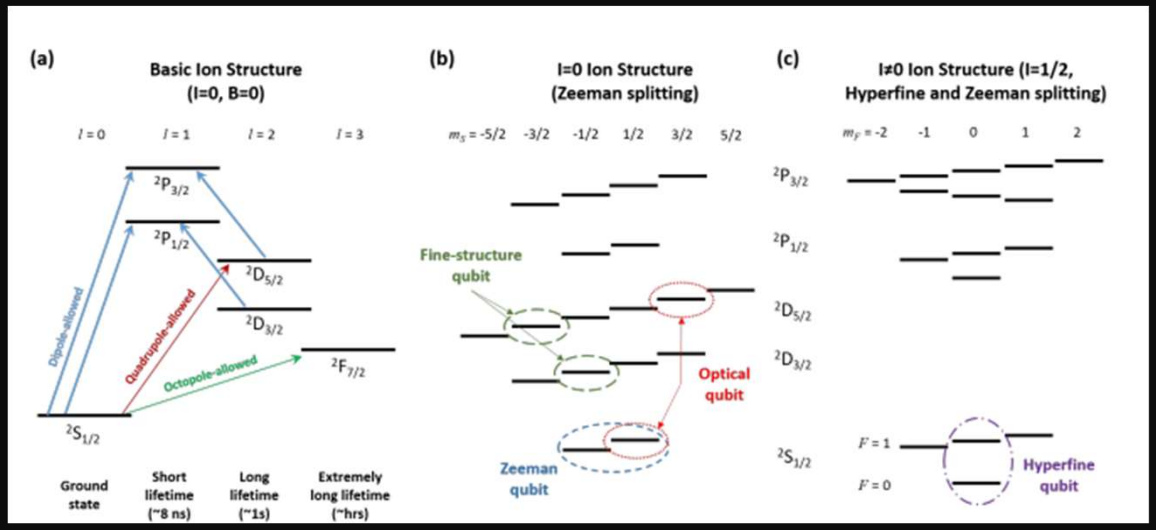
Procesori

- Supraconductori
  - Qubiti de incarcatura
  - Qubiti de faza
  - Qubiti de flux
- Ioni Captati
  - Qubiti Zeeman
  - Qubiti Hiperfini
  - Qubiti Optici
  - Qubiti de Structura Fina

https://arxiv.org/pdf/2006.10433

https://arxiv.org/pdf/1904.04178

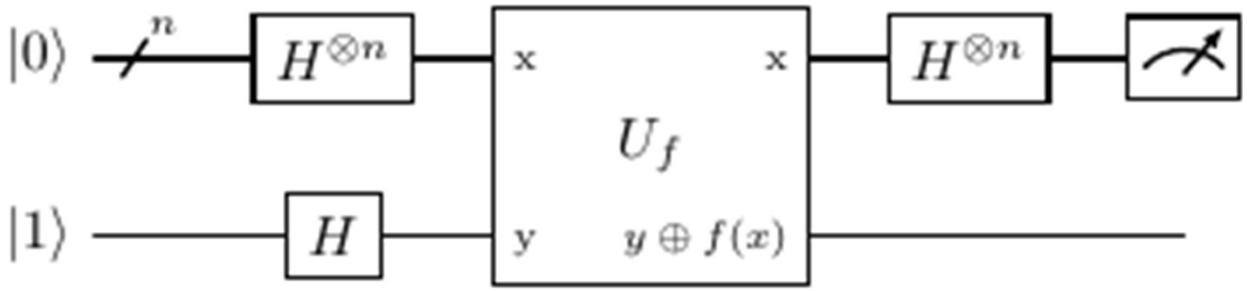




Algoritmi

https://doi.org/10.1098/rspa.1992.0167

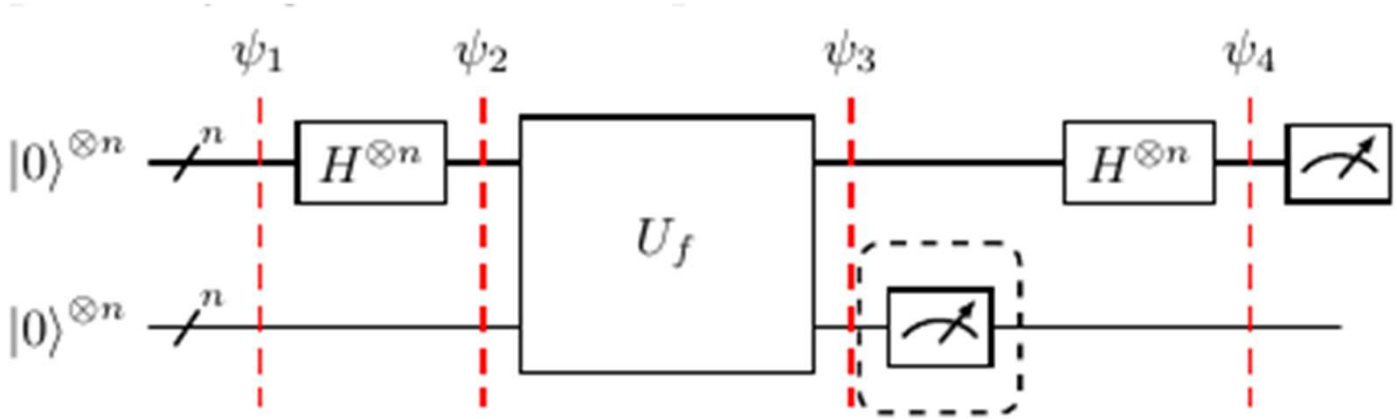
- Deutsch-Josza



$$|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|^2$$

Algoritmul lui Simon

https://doi.org/10.1137/S0097539796298637



- $(\psi_1)\ \ |0\rangle^{\otimes n}\,|0\rangle^{\otimes n}$
- $(\psi_2)\ \ \frac{1}{\sqrt{2^n}}\sum_x |x\rangle\,|0\rangle^{\otimes n}$
- $(\psi_3)\ \ \frac{1}{2^n}\sum_x |x\rangle\,|f(x)\rangle$
- $(\psi_4)\ \ \frac{1}{2^n}\sum_{x,y}(-1)^{x\cdot y}\,|y\rangle\,|f(x)\rangle$

Rezultatul final al Algoritmului

$$\frac{1}{2^n} \sum_{y, f(a)} (-1)^{ay} (1 + (-1)^{sy}) \, |y\rangle \, |f(a)\rangle$$

Despre criptografie

- Criptografia este domeniul care studiază protejarea și securizarea tuturor informaților transmise online, de la date medicale până la secrete de stat.
- Criptarea este procesul de codificare al unui mesaj.
- Fundația criptografiei curente este formată din algoritmi bazați pe anumite probleme matematice, de o complexitate proporțională cu dimensiunea numerelor utilizate, precum problema logaritmilor discreți.
- În prezent calculatoarele nu sunt suficient de puternice pentru a sparge acești algoritmi, dar viitoarele calculatoare cuantice vor putea în materie de „zile” sau chiar „câteva ore”.
- Din acest motiv a apărut criptografia post-cuantică, cu scopul de a folosi alte tehnici matematice rezistente la atacuri cuantice (ex. latici, hashing etc)

- În anul 2015, Institutul Național de Standarde și Tehnologie din SUA, NIST, a demarat un proiect pentru a dezvolta și standardiza noi algoritmi criptografici rezistenți cuantic.
- În vara anului trecut, 2024, a publicat primele 3 standarde de criptare post-cuantică: ML-KEM, bazat pe CRYSTALS-Kyber, ML-DSA, bazat pe CRYSTALS-Dilithium și SLH-DSA, bazat pe Sphincs+. Urmează și un al patrula algoritm, bazat pe FALCON.

Type	Initial Name	Specification Name	FIPS Name
KEM	CRYSTALS-Kyber	ML-KEM	FIPS 203
Signature	CRYSTALS-Dilithium	SLH-DSA	FIPS 204
Signature	Sphincs+	SLH-DSA	FIPS 205
Signature	FALCON	FN-DSA	FIPS 206

ML-KEM

- ML-KEM, bazat pe fostul algoritm Crystals-Kyber, este un criptosistem cu cheie publică, rezistent la atacurile cuantice grație unei variante a problemei “learning with errors” combinate cu polinoame ciclotomice.
- Acest algoritm, spre deosebire de alți algoritmi post-cuantici, exploatează proprietățile laticelor pentru o viteză sporită și o dimensiune redusă a cheii de criptare.

NUME	SIGURANȚA	Encapsulation key	Decapsulation key	Criptotext	Shared secret key
ML-KEM-512	De bază	800 octeți	1632 octeți	768 octeți	32 octeți
ML-KEM-786	Medie	1184 octeți	2400 octeți	1088 octeți	32 octeți
ML-KEM-1024	Crescută	1568 octeți	3168 octeți	1568 octeți	32 octeți

Funcționare

- Cheie privată = vector de polinoame, s.
- Cheie publică = matrice de polinoame + vector de polinoame (A, t), $t = A \times s + e$, unde e=vector de erori.
- m_i este convertit într-o reprezentare polinomială, cu coeficienții binari, notat m_b (ex:$11 = 1x^3 + 0x^2 + 1x^1 + 1x^0$). În continuare suferă o modificare, fiind înmulțit cu cel mai aproape întreg de $\frac{q}{2}$ (q=modulul prestabilit, prim, pentru calcule). Mesajul obținut, m, este criptat cu (A, t), obținându-se: $u = A^T \times r + e_1$ și $v = t^T \times r + e_2 + m$, unde r=vector de polinom oarecare, iar e_1 și e_2 sunt doi vectori dintr-un singur polinom menit introducerii de erori. Se obține (u, v).
- Criptotextul obținut se decriptează pe baza cheii s. $m_n = v - s^T \times u$. Coeficienții săi vor fi mai aproape ori de 0 sau $q \rightarrow$ coeficientul binar inițial era 0, ori mai aproape de $\frac{q}{2}$ rotunjit $\rightarrow$ coeficientul binar inițial era 1. Se fac substituțiile și se obține m_i.

Despre comunicarea cuantică

- Comunicarea cuantică: transmiterea informației în mod securizat, păstrându-și integritatea, între sisteme cuantice distanțate fizic.
- Depinde de 3 principii: superpoziția, inseparabilitatea cuantică și teleportarea cuantică.
- Siguranța comunicării cuantice este determinată de colapsul stării cuantice în urma oricărei forme de interferență.
- De asemenea, au o particularitate interesantă: stările nu pot fi copiate, măsurarea unui singur qubit conduce la colapsul stării și produce un rezultat insuficient în reproducerea ei.

- Inseparabilitatea cuantică, „Acțiune fantomă la distanță”: legătura dintre două particule, separate una de alta, în așa fel încât orice modificare suferită de o particulă, va produce modificării instantanee, corelate, stării celeilalte particule.
- Teleportare cuantică: o pereche de particule inseparabile cuantic sunt distribuite între un emițător și un receptor. Informația este codificată într-un qubit. Emițătorul măsoară starea Bell a celor doi qubiți pe care îi posedă, iar colapsul provocat modifică și starea qubitului receptorului. Emițătorul trebuie să transmită, printr-un canal clasic, rezultatul măsurării sale, pentru ca receptorul să poată aplica anumite operații cuantice să recupereze starea inițială exactă a informației transmise.
- Din cauza dependenței de mijloacele clasice de comunicare, teleportarea cuantică nu poate depăși viteza luminii.

Distribuția cheilor cuantice, BBM92

- Între două persoane se împart qubiții unei cantități semnificative de perechi inseparabile cuantic, apoi se stabilesc două baze, Z (în general rectilinie) și X (în general diagonală). Se mai stabilește și o corelație între rezultatul cuantic și valorile binare „0” si „1”.
- Amândoi încep să-și măsoare qubiți într-o bază aleasa la întâmplare dintre cele două, păstrând un istoric al bazei folosite și al rezultatului măsurătorii, în final obținând două șiruri de biți, adică două chei brute.
- Printr-un canal clasic, se transmite lista bazelor folosite, astfel încât să se poată identifica cazurile în care au folosit amândoi aceeași bază, (de obicei, aproximativ jumătate din perechile generate).

- Orice intervenție străină va provoca neconcordanțe între cele două chei brute, deoarece vor fi valori diferite, dar „obținute” prin utilizarea aceleași baze, lucru care e imposibil.
- Deși asemenea erori pot apărea natural, o pondere mărită de erori semnalează o prezență nefastă, astfel încât tot procesul trebuie abandonat. Verificarea acestor discrepanțe se execută pe o secțiune „de sacrificiu” din cheia brută, trimisă printr-un canal public celeilalte persoane.
- Dacă rata de erori este neglijabilă, se mai execută niște algoritmi de corectare a erorilor, urmați obligatoriu de un algoritm de amplificare a securității. La final se obține o cheie de criptare puternică din punctul de vedere al siguranței.

Vă mulțumim pentru atenție!

Photo source: Lawrence Berkeley National Laboratory