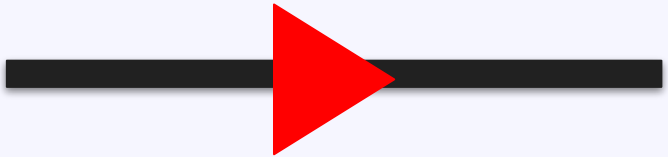
L'ORDINATEUR QUANTIQUE

Veille 14 Juin 2022 - Becode

El Khattouti Bilalle

Récupérer les données d’hier pour les déchiffrer demain ?

Un ordinateur classique



1

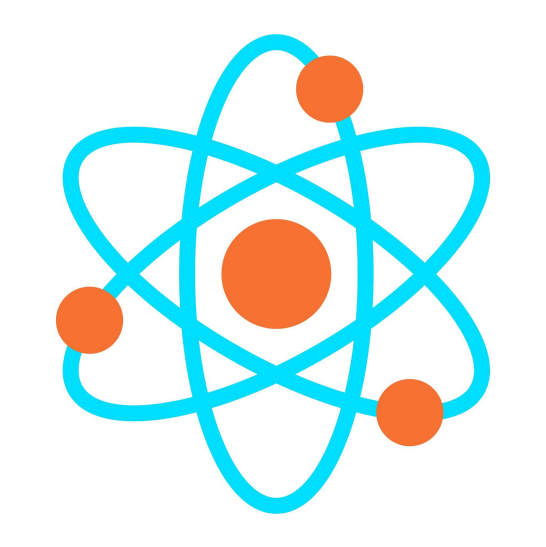
0

Un ordinateur classique

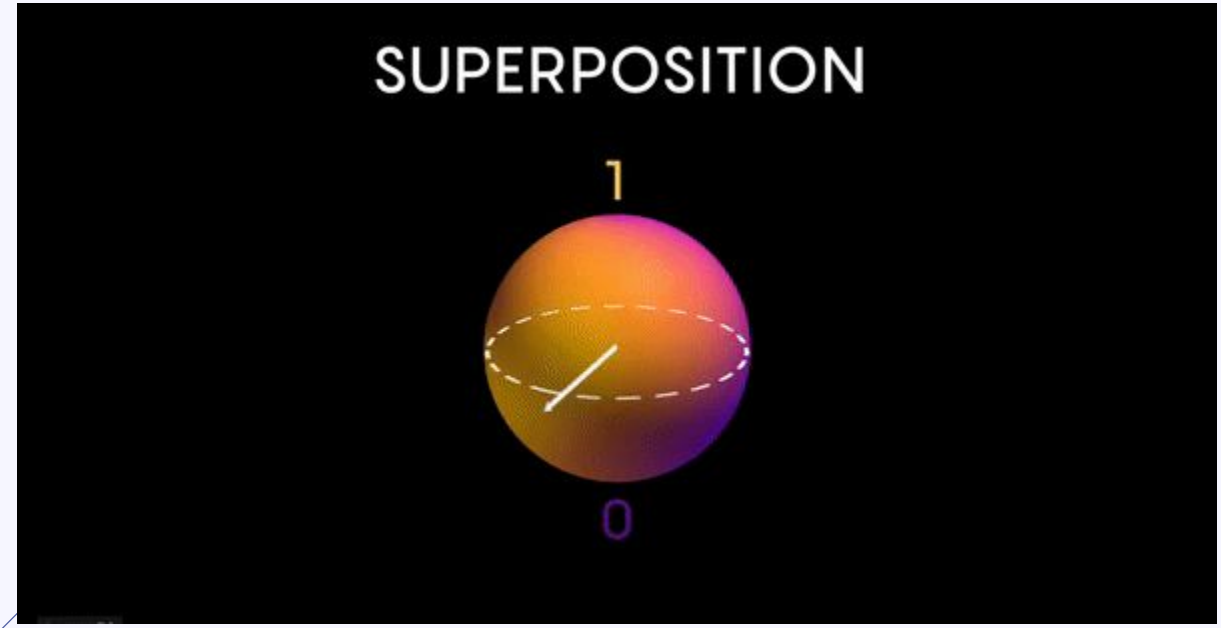
Ordinateur quantique… quantique ?

Référence à la ‘physique quantique’ né au début du XXe siècle

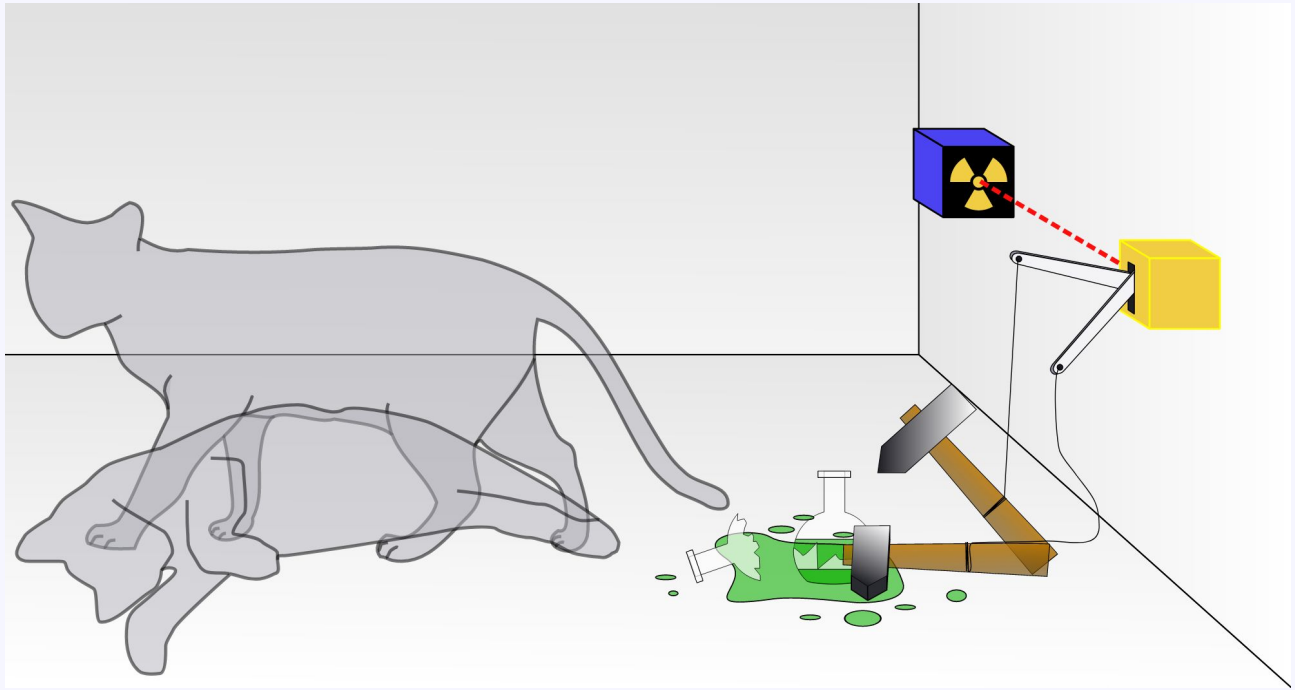
Un principe contre-intuitif : la **superposition des états**



Ordinateur quantique



Ordinateur quantique



Le chat de Schrödinger

Ordinateur quantique

bit

“Classique”

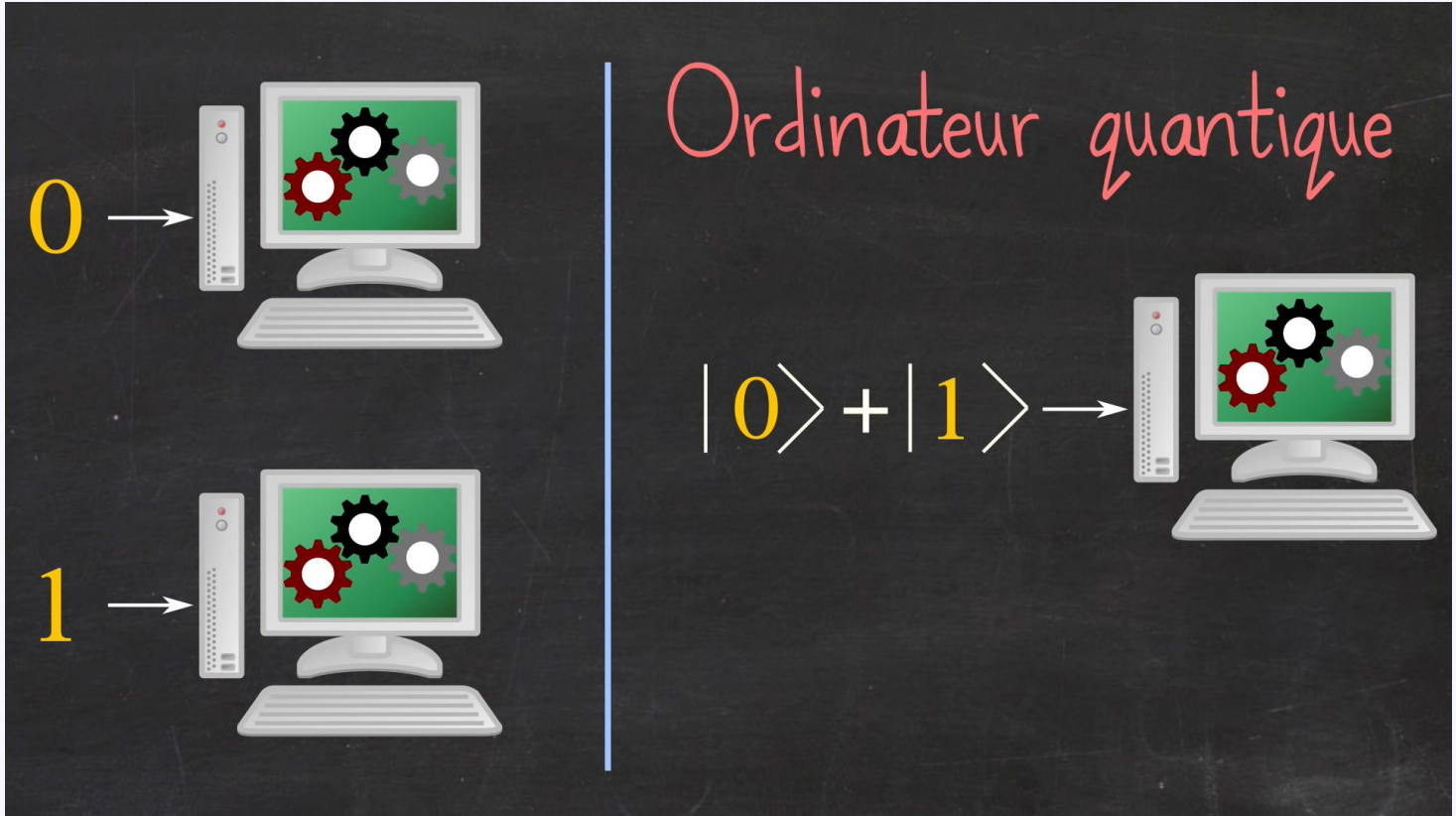
0 ou **1**

qubit

“Quantique”

0 **1**

Ordinateur quantique



Bit classique

Je cherche ce livre

1	1	1	1

16 étapes !

0	0	0	0
0	0	0	1
0	0	1	0
0	1	0	0
1	0	0	0
...			
1	1	1	1

Je cherche ce livre

1	1	1	1

qubit

0/1	0/1	0/1	0/1

Une seule étape !

Beaucoup de personnes sur le doss' !

Google

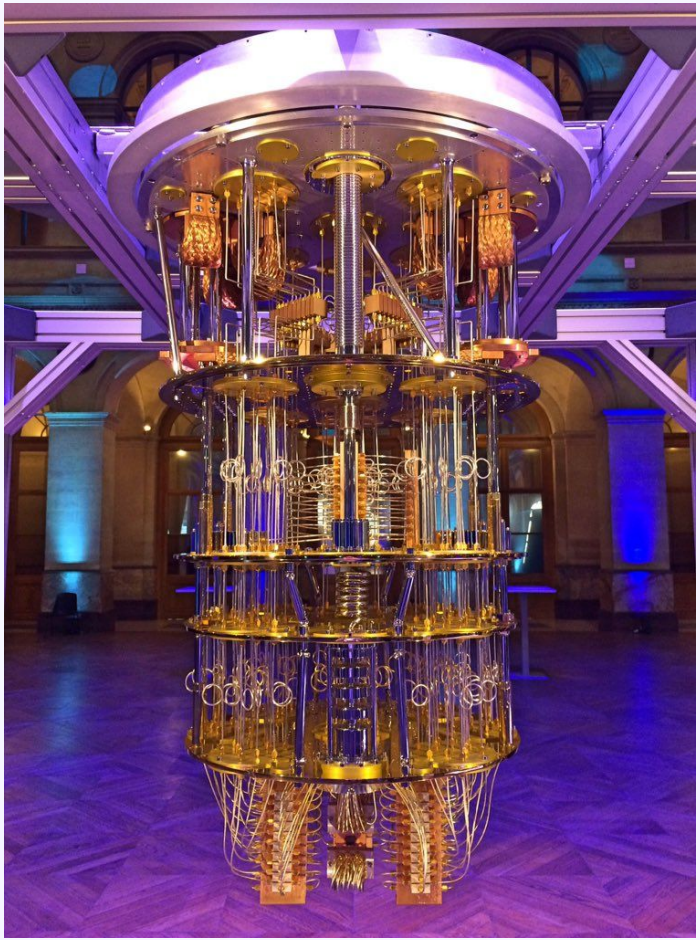
D-Wave
The Quantum Computing Company™

IBM

Microsoft

Ordinateur quantique

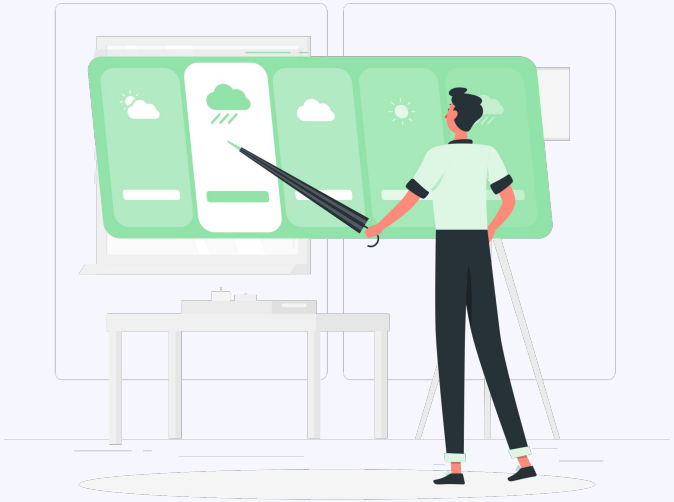
Sycamore, l’ordinateur quantique de Google



Pas le prochain ordinateur !

Chaque ordinateur a des rôles spécifiques

(Super)Ordinateur



Pas le prochain ordinateur !

Chaque ordinateur a des rôles spécifiques

Ordinateur quantique

Une aventure semée d'embûches

Des problèmes :

- Plus on essaye de rajouter des qubits moins c'est stable
- Il faut refroidir au zéro absolu (-273,15°)
- Les résultats ne sont stockables que quelques microsecondes... on cherche alors à développer de la 'qram' (qsouris, qclavier, ...^^) pour pouvoir les stocker quelques heures
- Le record de qubits est 127 (IBM)
- Les algorithmes sont en cours de recherche (Algorithme de Grover, ...)
- La suprématie quantique atteinte ?

Quantum cryptography

- Le chiffrement à base de clé public (symétrique et asymétrique) des années 70 peut être faible face aux ordinateurs quantiques

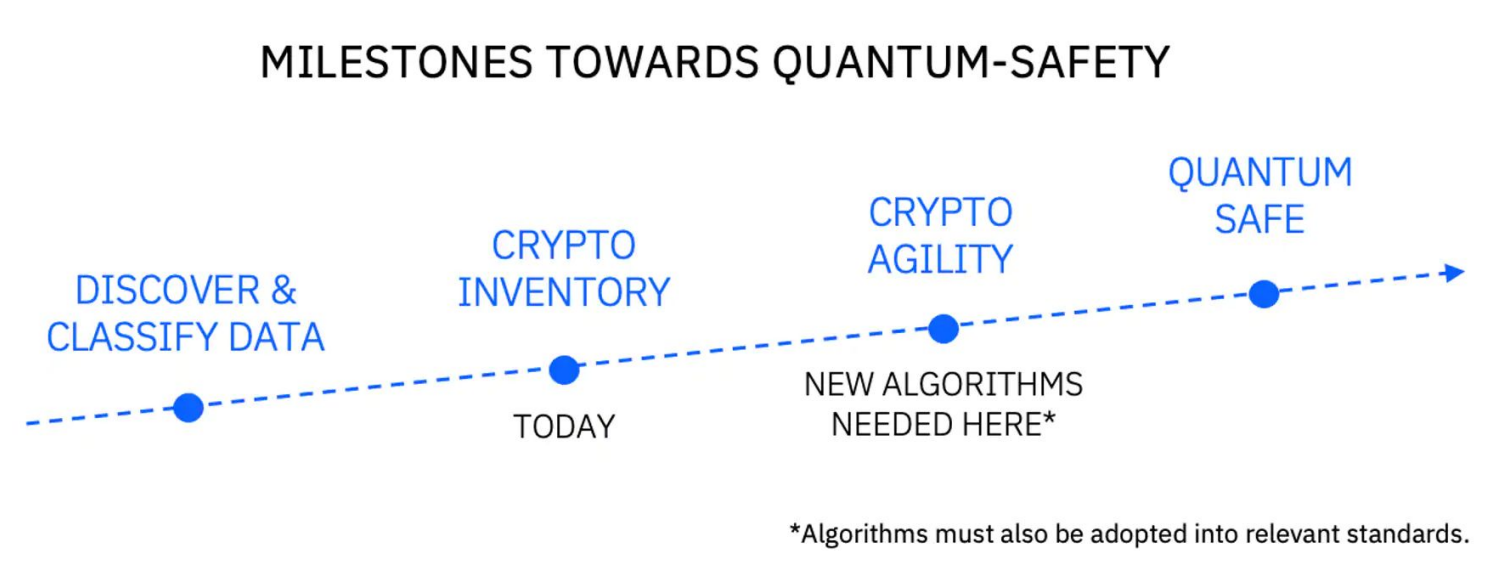
- Prouvé par le mathématicien Peter Shor

Symétrique : AES est “quantum-safe” mais pas le TDES

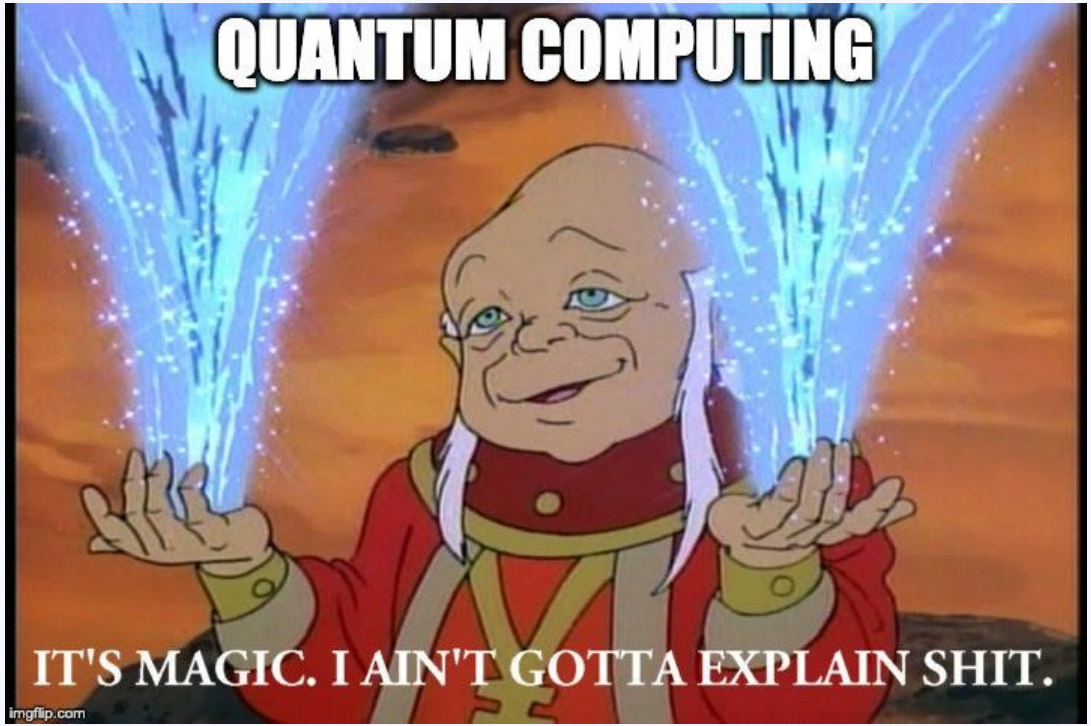
Asymétrique : RSA qui est très répandu n’est pas quantum-safe

On peut déchiffrer mais aussi chiffrer !

Quantum cryptography



Merci pour votre écoute !



Source 1/2

- https://www.forbes.com/sites/forbestechcouncil/2021/12/22/what-to-expect-from-quantum-computing-in-the-next-two-years/
- https://www.montanainstruments.com/blog/supercomputer-vs-quantum-computer
- https://www.darkreading.com/edge-articles/threat-actors-are-stealing-data-now-to-decrypt-when-quantum-computing-comes
- https://analyticsindiamag.com/quantum-computers-vs-supercomputers-how-do-they-differ/
- https://thequantuminsider.com/2022/06/10/whats-the-difference-between-a-supercomputer-a-quantum-computer/

Source 2/2

- https://quantumxc.com/blog/quantum-computing-impact-on-cybersecurity/
- https://www.defenseone.com/ideas/2022/04/china-may-have-just-taken-lead-quantum-computing-race/365707/
- https://www.zdnet.com/article/quantum-computers-could-crack-encryption-warns-white-house-as-it-details-action-plan/

- https://www.youtube.com/watch?v=2aCS5mEeiwg&t=1058s **(L'ORDINATEUR QUANTIQUE - Dossier #38 - L'Esprit Sorcier)**
- https://www.youtube.com/watch?v=bayTbt_8aNc&t=285s **(Les Ordinateurs Quantiques par ScienceEtonnante)**
- https://www.youtube.com/watch?v=44ya-DSF6fw **([Comment ça marche?] Le chat de Schrödinger par CEARecherche)**