

ORDINATEUR QUANTIQUE ET SÉCURITÉ INTERNET



Ordinateur quantique



Plan de la présentation

- Qu'est ce que la physique quantique ?
- Qu'est-ce qu'un ordinateur «traditionnel» ?
- Qu'est-ce qu'un ordinateur «quantique» ?
- Promesse de la supériorité d'un ordi quantique
- Une tentative d'explication de cette supériorité
- Internet et encodage (cryptologie)
- Comment briser l'encodage
- Désespoir
- Espoir

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

Caveat

- Le sujet peut devenir complexe et aride très rapidement.
- En fait , je ne comprends que quelques % de ce que je vais parler...
- (mais vous venez de passer un période électorale...vous êtes habitués maintenant aux discours où l'on ne comprend rien)
- Je promets d'essayer d'être clair et pas trop ennuyeux
- Il n'y a pas d'examen...
- Cela tombe dans la catégorie «enrichissement personnel»
- Corrigez moi si je dis des conneries...
- Mais tolérez si je suis presque correct

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

Les différentes sortes de «physiques»

■ **Physique classique** ...celle que l'on a apprise et oubliée..

■ La physique de Newton....celle qui nous sert dans 99 % des cas

■ **Physique relativiste:** celle d'Einstein...les grosses choses qui vont vite...

■ Vitesse de la lumière $E=mc^2$

■ C'est pas pour nous mais ...le GPS doit en tenir compte...

■ **Physique quantique:** cela se passe dans l'infiniment petit (niveau atomique et sub-atomique)

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

La physique quantique

- S'est développée au début des années 1900
- Surtout en Europe (de Broglie, Schrödinger, Planck, Bohr...)
- Elle ne nous concerne pas ...pas encore
- Des choses bien étranges se passent dans l'infiniment petit
- On parle de probabilité et non plus de certitude.
- Ce n'est plus 0 ou 1 mais «peut-être»

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique



Un ordinateur traditionnel

- Basé sur des 0 ou 1...le bit...
- Des opérations logiquesEt , Ou, Ou exclusif, Additionneur
- Machine séquentielle...ie: une opération à la suite de l'autre
- La puissance a explosé....loi de Moore....
- Tous les 18 mois, on double la puissance (mémoire, vitesse)
- Mais on arrive à la limiteen 2020
- Les derniers «chips» se butent aux phénomènes de l'infiniment petit

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique



Un ordinateur quantique

- C'est très expérimental...
- Cela coûte très cher...
- Ce n'est pas encore fiable...on est loin de la mise en marché
- Cela doit être refroidi (- 273 C ...sinon cela ne fonctionne pas...)
- Mais les grands de ce monde y mettent des millions \$ en recherche...

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

L'ordinateur quantique

- Basé sur le «bit quantique» ou «qubit»...
- On semble distinguer les ordi quantique par le nombre de qubits qu'ils peuvent «cascader»...Google a un ordi de 20 qubits.
- Un «qubit» : 0 ou 1 ou *quelque chose entre les 2*
- Pourquoi est-ce supérieur à « 0 ou 1 » ?
- Exemple boiteux , pauvre et simpliste



Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

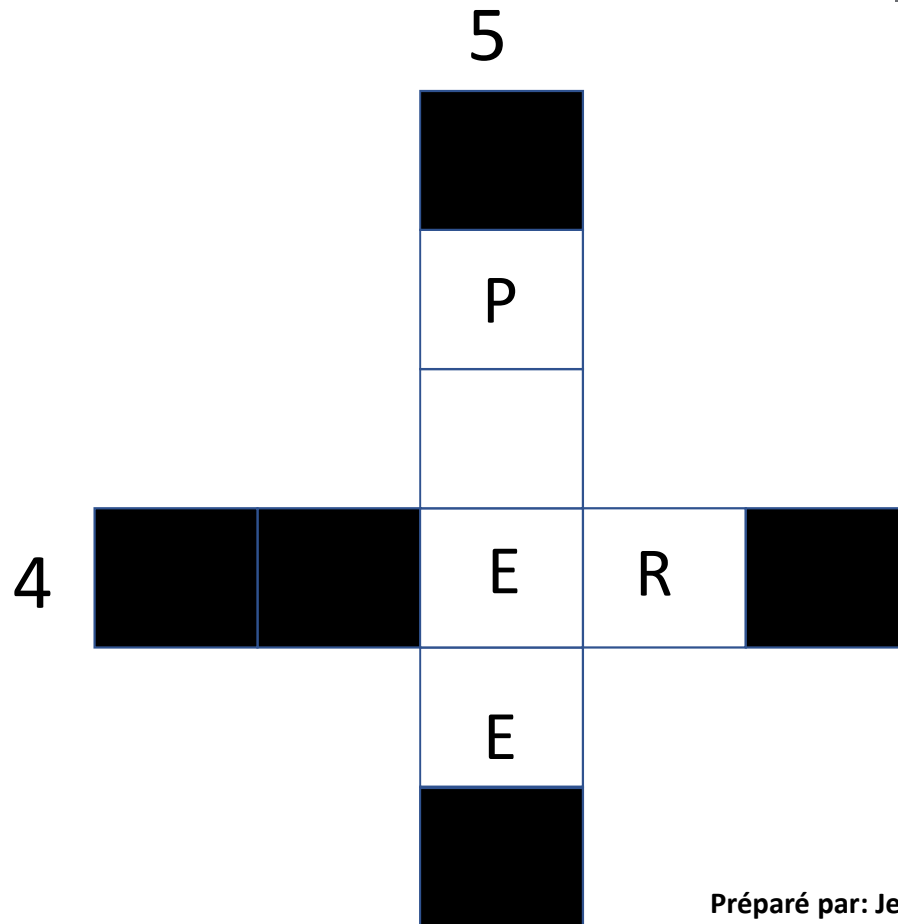
Prenons l'exemple d'un mots croisés

Ce que ferait un ordi traditionnel

Questions :

4 horizontal: Fin de verbe

5 vertical: Difficulté



Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

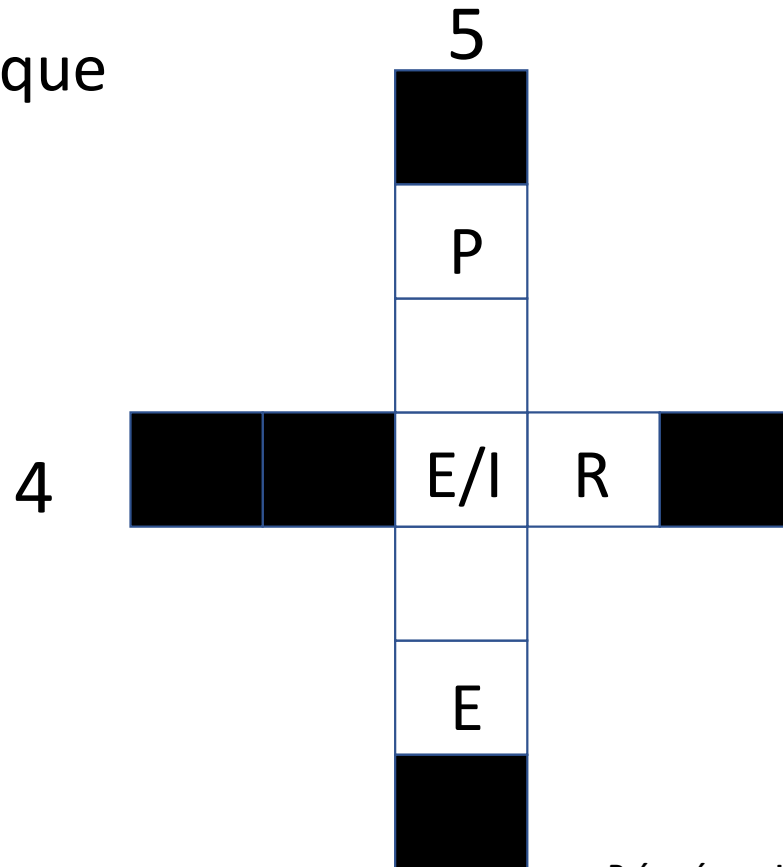


Ce que ferait un ordi quantique

Questions :

4 horizontal: Fin de verbe

5 vertical: Difficulté



Préparé par: Jean-Pierre Bonneau

A decorative graphic consisting of a grid of colored squares in blue, orange, and grey, arranged in a pattern that resembles a stylized arrow or a cluster of data points.

4

		P		
		E		
		E/I	R	
		N		
		E		

5

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

Autres avantages de l'ordi quantique

- Il peut travailler en «parallèle» et non seulement en «séquence»
- Ce n'est pas le «multi tâches» (qui n'est que la séquence à tour de rôle) mais vraiment faire plusieurs opérations en même temps
- La programmation en parallèle: un défi de programmation...
- Exemple du livre marqué dans une bibliothèque

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

Les premiers essais ...

- En Octobre 2019, Google annonce une percée
- L'équivalent de 10,000 ans de calculs en quelques heures.
- Pour l'instant ...curiosité de laboratoire
- Problème adressé....un problème «jouet» mais très complexe...
- C'est pas demain la veille.



Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

Pourquoi tant d'intérêt ?

- Plusieurs labo de recherche y consacrent des fortunes
- Les puissances nationales...(USA, Russie, Chine...Canada..)
- Plusieurs domaines de recherches demandent de grandes puissances de calculs...
- Ex. : météorologie, recherche en biologie,
- Mais surtout: le **décodage des codes secrets....**



Préparé par: Jean-Pierre Bonneau



Comment fonctionne l'encodage

- Un sujet aride et «platte»
- Mais combien nécessaire
- Toutes nos transactions bancaires... (<https://...>)
- Nos courriels contenant des infos personnelles.
- Documents personnels échangés sur le net

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

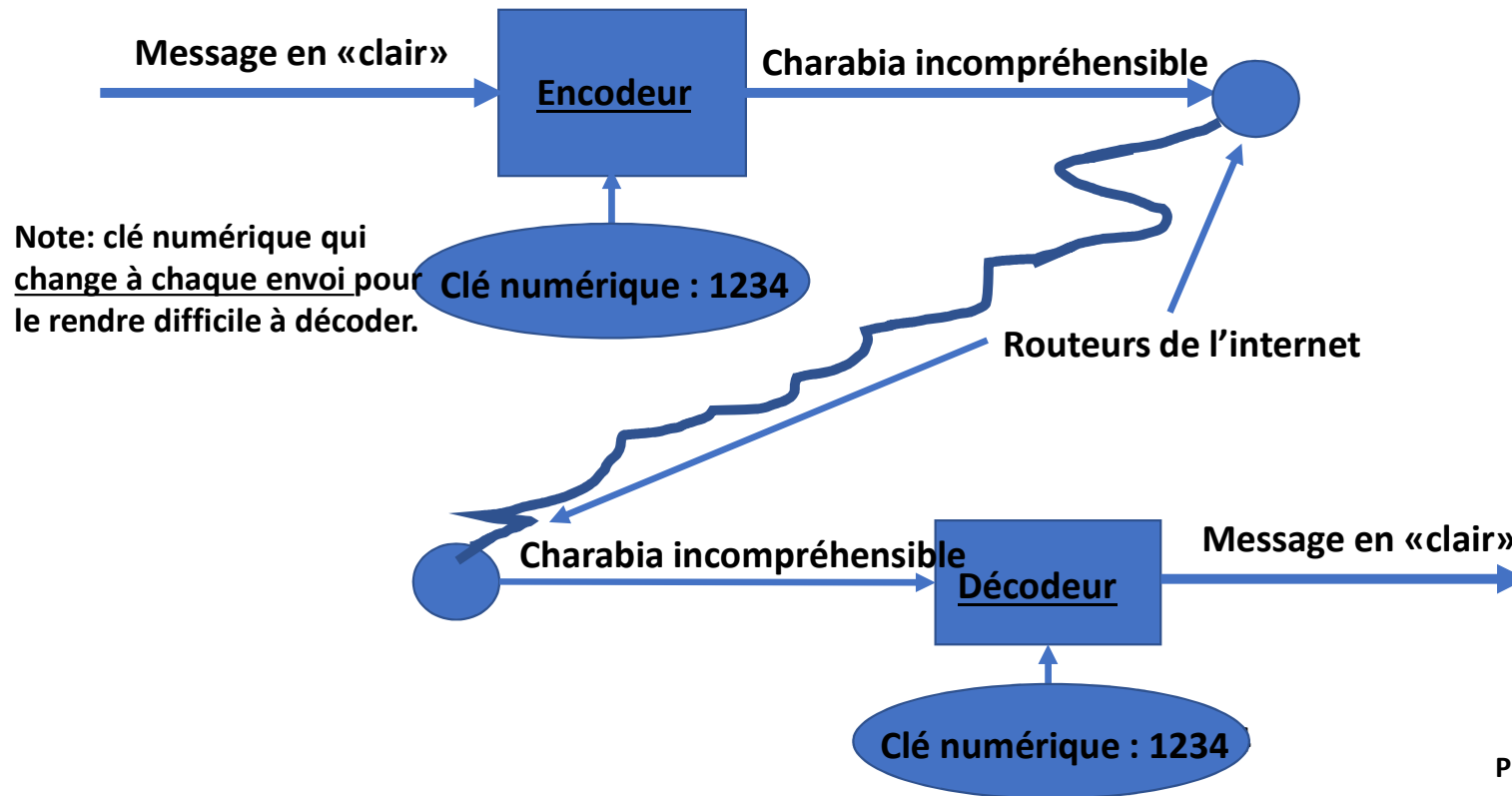
Ce que j'ai compris...

- Un processus qui transforme des données claires en «charabia » numérique
- Le «charabia» numérique est transmis sur le «net»
- Un processus inverse se fait à la réception...ie: décodage
- Une clé échangée entre TX et RX permet le codage et son décodage

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

Comment fonctionne l'encodage / décodage sur l'internet



Préparé par: Jean-Pierre Bonneau



La décomposition d'un nbre en ses nbres premiers

- Il est extrêmement difficile de décomposer un nombre (très grand) en ses nombres premiers
- Nombres qui sont très grands...ils sont écrits avec plus de 1000 chiffres..
- Il n'y a pas de façon facile de les décomposer ...«force brute»
- Un ordi tradi peut prendre des années
- ***Un ordi quantique pourrait le faire en quelques minutes...***

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique

Les agences de renseignements en «bavent»

- Toutes nos communications seraient décodables...
- La seule façon de se prémunir est de multiplier par des nombres premiers encore plus grands...mais il y a un prix...
- Le doute subsistera toujours....est ce que l'autre peut me décoder ?
- Bien pire: nos échanges actuels sont tous enregistrés...
- On ne peut pas les lire présentement...mais dans le futur
- Des organismes pourront les lire....rétroaction qui viendra nous hanter...

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique



Solution : l'encodage quantique

- Cela aussi c'est du matériel à laboratoire
- Je ne comprends pas comment cela fonctionne
- Mais utilise un principe de base des effets quantiques..
- Quand on mesure un phénomène quantique , on le perturbe...
- Alors il s'agit d'associer un «phénomène quantique» à un message...et
- Si quelqu'un a essayé de le lire ...on le saura à la réception
- Désolé c'est tout ce que j'ai compris

Préparé par: Jean-Pierre Bonneau

Ordinateur quantique



Si ce que je vous ai présenté aujourd'hui vous apparaît clair et net...j'ai dû me tromper en quelque part....

FIN

Préparé par: Jean-Pierre Bonneau