# Cryptologie et physique quantique : Espoirs et menaces

Matthieu Amiguet

2005 – 2006

haute école arc ingénierie
neuchâtel berne jura — saint-imier le locle porrentruy



## Objectifs 2

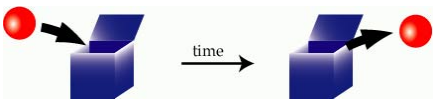
- Obtenir une compréhension de base des principes régissant le calcul quantique et la cryptographie quantique
- Comprendre les implications sur la cryptographie
- Savoir où on en est actuellement
- Approche informelle ! ! !



## Information classique 3

- L'élément de base est le *bit*, qui peut prendre deux valeurs :

- On peut stocker ces balles dans des boîtes, et les récupérer




- Conséquence : on peut copier l'information facilement.



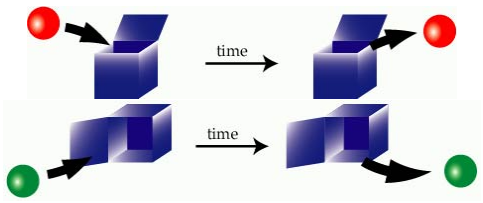
## Information quantique 4

- Et si les bits suivaient les lois de la mécanique quantique ?
- L'élément de base est le qubit, qui peut prendre deux valeurs :

- On ne peut stocker les quballes que dans des quboîtes, qui ont *deux portes* :

## Jusque là tout va bien... 5

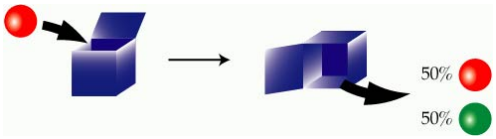
- Si on utilise qu'une seule porte, pas de surprise :






## Les joies de la physique quantique... 6

- Si on mélange les portes, c'est déjà plus surprenant :




- Pour les physiciens, la quballe est dans une "superposition d'états" :
  - Elle est *à la fois* rouge et verte !
- Par contre, après avoir ouvert la porte, la superposition est détruite : la quballe est *soit* rouge *soit* verte !

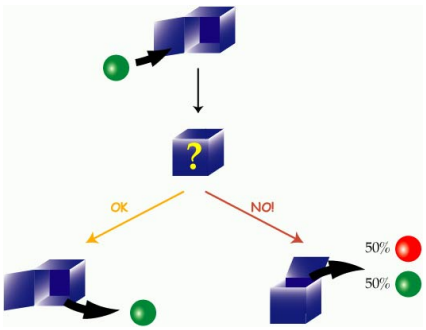


## Objections 7

- Les physiciens sont fous ?
  - Peut-être, mais les résultats de la théorie sont *excellents* !
- Les quballes n'existent pas ?
  - C'est vrai, mais il existe des objets qui se comportent de cette manière :
    - spin d'un électron
    - polarisation d'un photon
    - niveaux d'énergie d'un atome
    - ...



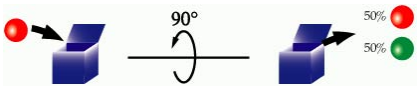
## L'information quantique ne peut pas être dupliquée ! 8



## La rotation



- Dans la réalité, on ne peut souvent accéder qu'à la porte du dessus de la boîte.
- On peut par contre faire une *rotation* qui génère une *superposition d'états* :

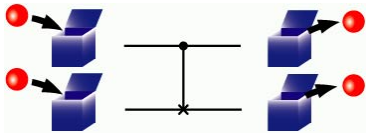




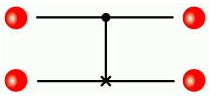

## Le "Non Contrôlé"



- Opération binaire : le C-NOT



- Comme on ne considère plus que la porte du haut, on peut oublier la boîte





## Le "Non Contrôlé" – table de vérité



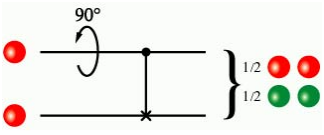
- Inverse la couleur de la seconde balle, mais seulement si la première est verte :

| Entrée | Sortie |
|---|---|
|  |  |
|  |  |
|  |  |
|  |  |

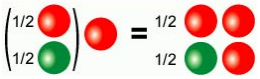


## Un circuit quantique

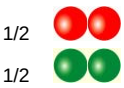





- Après la rotation :

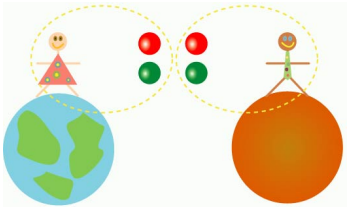



- À la sortie du circuit



## Enchevêtrement quantique 13

- Dans le cas précédent, on dit que les deux quballes sont *enchevêtrées* (ou *paire EPR*, pour Einstein, Podolsky et Rosen)
- L'observation d'*une* quballe détermine sa couleur, et donc celle de l'*autre* quballe
  - immédiatement
  - même à distance





## Non-clonage et cryptographie 14

**L'information quantique ne peut pas être dupliquée**

- Autrement dit, toute observation perturbe le système
- Autrement dit, sur une ligne de communication quantique, on ne peut pas observer une communication sans la perturber
- Peut-on utiliser ce phénomène pour transmettre des clés de manière sûre ?

- La réponse est oui !
- Discipline correspondante : "cryptographie quantique".



## Cryptographie quantique, mode d'emploi 15

- Alice génère une suite aléatoire de quballes rouges ou vertes et les met dans des boîtes, parfois par la porte du haut, parfois par la porte de côté
- Elle envoie les boîtes à Bob
- Bob ouvre les boîtes, parfois par la porte du haut, parfois par la porte de côté
- Après réception d'un nombre suffisant de quballes, Bob annonce publiquement la suite des portes qu'il a utilisé
- Alice annonce publiquement la liste des fois où elle a utilisé la même porte que Bob
- Bob et Alice ne retiennent que les valeurs correspondant à cette liste.



## Un exemple 16

| Portes d'Alice | 1 | 1 | 2 | 1 | 2 | 2 | 2 |
|---|---|---|---|---|---|---|---|
| Quballe envoyée |  |  |  |  |  |  |  |
| Porte de Bob | 1 | 2 | 1 | 1 | 2 | 2 | 1 |
| Mesures de Bob |  |  |  |  |  |  |  |
| Valeurs retenues |  | – | – |  |  |  | – |

## Et si la ligne est sur écoute ? 17

- Si Ève intercepte la communication, elle se trompera de porte dans 50% des cas (comme Bob, d'ailleurs)
- Dans ce cas, elle transmettra à Bob une valeur (aléatoire) *par la fausse porte*
- Bob obervera donc un résultat aléatoire, faux dans 50% de ces cas
- Donc Bob aura un résultat faussé dans 25% des cas en tout
- Alice et Bob comparent donc publiquement une partie de leurs résultats ; si l'erreur est bien inférieure à 25%, la communication n'a pas été observée.



## Et en pratique ? 18

- La méthode a été validée expérimentalement
  - sur quelques dizaines de km en lignes généralistes (fibres optiques)
  - sur une centaine de km en lignes dédiées
- Technologie disponible dans le commerce
  - Par exemple : `http://www.idquantique.com/products/vectis.htm`



## Vers un calculateur quantique ? 19

- En 1981, Richard Feynman relève l'énorme complexité à simuler par ordinateur les phénomènes quantiques
- Inversion de perspective : il évoque la possibilité d'utiliser les phénomènes quantiques pour effectuer des calculs complexes...
- À cause des superpositions d'états et de l'enchevêtrement, il faut $2^n$ bits "classiques" pour représenter l'état de $n$ qubits
- Pourrait-on exploiter cette complexité à des fins de calcul ?



## Algorithmes quantiques les plus célèbres 20

- Algorithme de factorisation (Shor, 1994) :
  - $O((\log N)^3)$ en temps
  - $O(\log N)$ en espace
- Algorithme de recherche par force brute (Grover, 1996)
  - $O(\sqrt{N})$ en temps
  - $O(\log N)$ en espace.

## Présentation 21

- Recherche dans une base de données non triée
  - Recherche exhaustive
  - $N$ possibilités à priori équivalentes (pas d'indice)
- Exemples d'applications
  - Recherche d'information (bases de données, internet, ...)
  - Cryptanalyse
- Algorithmes classiques : $O(\frac{N}{2})$ en moyenne
  - L'amélioration amenée par Grover n'est donc "que" quadratique
  - La plupart des algorithmes quantiques amènent une amélioration exponentielle...
  - ... mais Grover est un peu plus facile à comprendre !



## Grover : l'algorithme 22

- On initialise la mémoire (quantique) dans une superposition uniforme de tous les états
- On applique de manière répétée un opérateur qui augmente la probabilité d'observer une "bonne" réponse
- Après $\frac{\pi}{4}\sqrt{N}$ itérations, on observe la réponse !
- Probabilité d'erreur : $O(\frac{1}{N})$.



## Où en sommes-nous ? 23

- Le problème de l'implémentation d'un calculateur quantique n'est pas la matière première...
- Par contre, la réalisation se heurte à deux contraintes très fortes :
  - Le système doit être totalement isolé de l'extérieur (éviter les enchevêtrements...)
  - Toutes les opérations effectuées doivent être réversibles
- Algorithme de Shor : réalisé expérimentalement
  - par un groupe d'IBM
  - sur un calculateur quantique de... 7 qubits (spins des atomes d'une molécule développée pour l'occasion)
  - pour factoriser 15 en 3*5 (!).



## Le calculateur quantique d'IBM 24

- $10^{18}$ molécules dans un tube à essai ("wetware")
- Durée de vie de quelques minutes
- Pour aller plus loin, il faudra probablement passer à une structure solide.

## Perspectives 25

Quels apports possibles des phénomènes quantiques pour l'informatique ?

- Nous avons vu...
  - La transmission sécurisée de clés cryptographiques
  - La cryptanalyse
    - factorisation de grands nombres
    - recherche exhaustive de clés ou de messages
  - La recherche d'information
- Il y aurait aussi...
  - La génération de nombres aléatoires, cf. p. ex. `http://www.idquantique.com/products/quantis.htm`
  - La simulation numérique (notamment... en physique quantique !)
  - ...



## Pour aller plus loin... 26

- Alexandre Blais, "Introduction à l'informatique quantique"
  - `http://www.physique.usherbrooke.ca/~ablais/d-wave-web/intro_francais.html`
  - Cette présentation en est fortement inspirée ; source de la plupart des illustrations. Merci !
- Les différents articles de Wikipedia
  - Calculateur quantique
  - Quantum computer
  - Algorithme de Shor
  - Grover's algorithm
  - ...



## Pour aller plus loin... (suite) 27

- La page d'IBM sur son calculateur quantique : `http://domino.research.ibm.com/comm/pr.nsf/pages/news.20011219_quantum.html`
- Sciences et Avenir, Hors-série, "Le paradoxe du chat de Schrödinger", n°148, octobre-novembre 2006



## En guise de conclusion 28

**"Popular Mechanics", 1949**

"Computers in the future may weigh no more than 1.5 tons"