Traitement et communication de l'information quantique

- Moyen terme : cryptographie quantique
- Long terme : ordinateur quantique

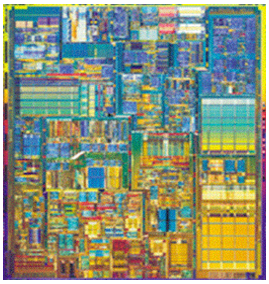
Philippe Jorrand
CNRS
Laboratoire Leibniz, Grenoble, France

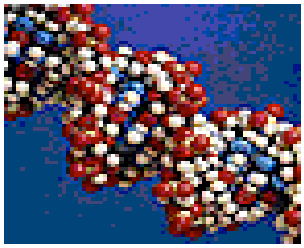
Philippe.Jorrand@imag.fr

L'information peut s'inscrire sur divers supports…

… mécanique,

… électronique,





… bio-moléculaire,

… quantique, …

Mais pas d'information sans état de la matière,
pas de calcul sans processus physique.
Les lois de la physique gouvernent ce qu'est le calcul.

Physique classique

A chaque instant, un système physique est dans un état, et un seul état à la fois, parmi un ensemble d'états possibles de ce système.

Les transformations de l'état d'un système physique ne sont pas, en général, réversibles.

L'observation d'un système physique dans l'état S ne modifie pas S. Elle est déterministe : elle retourne la même information pour des systèmes identiques observés dans le même état S.

L'état d'un système physique A peut être recopié sur un autre système physique B, si A et B ont les mêmes états possibles.

L'état d'un système physique composé de n sous-systèmes est toujours réductible à un n-uplet des états de ces sous-systèmes.

Physique quantique

A chaque instant, un système physique peut être dans l'un des états d'un ensemble d'états de base possibles. Mais son état est en général une superposition de plusieurs états de base.

Les transformations de l'état d'un système physique isolé, non observé, sont réversibles et déterministes.

L'observation d'un système physique dans l'état S transforme S de façon irréversible. Elle est probabiliste : elle peut retourner des informations différentes pour des systèmes identiques observés dans le même état S.

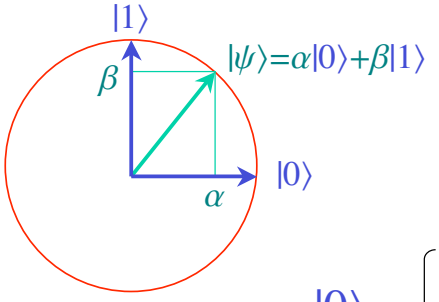
L'état d'un système physique A ne peut pas être recopié sur un autre système physique B, même si A et B ont les mêmes états possibles.

L'état d'un système physique composé de n sous-systèmes n'est pas, en général, reductible à un n-uplet des états de ces sous-systèmes.

L'état d'un qubit est un vecteur $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

L'état d'un qubit (*quantum bit*) est un vecteur dans un espace vectoriel à deux dimensions :

- soit le vecteur $|0\rangle$, soit le vecteur $|1\rangle$, qui forment une base,
- ou, plus généralement, un vecteur $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$, où α et β sont des nombres (complexes) tels que $|\alpha|^2+|\beta|^2=1$



$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \qquad |\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

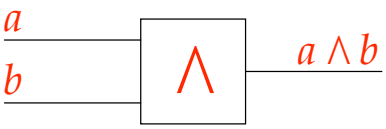
Calculer = transformer l'état

Avec des bits classiques

$\{0,1\} \longrightarrow \{0,1\}$

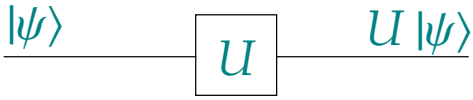
Plus généralement :

$\{0,1\}^n \longrightarrow \{0,1\}^m$



- fonctions booléennes arbitraires
- en général non réversibles

Avec des qubits

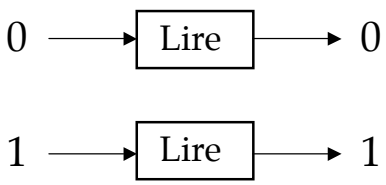


- U est un opérateur linéaire, représenté par une matrice 2×2
  $\Longrightarrow$ déterministe
- U unitaire $\Longrightarrow$ reversible

Obtenir un résultat = observer l'état

Avec des bits classiques

Lire un bit classique qui est dans l'état 0 donne la valeur 0 et le bit reste dans l'état 0.
Idem pour 1.



Avec des qubits

Mesurer un qubit qui est dans l'état $|0\rangle$ donne la valeur 0 et le qubit reste dans l'état $|0\rangle$.
Idem pour $|1\rangle$.

Mesurer un qubit qui est dans l'état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ donne :

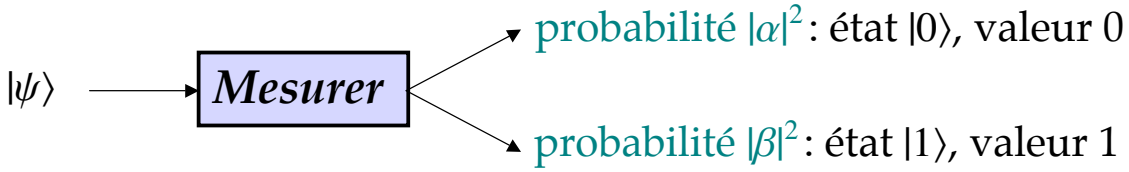
- soit la valeur 0, avec probabilité $|\alpha|^2$, et l'état du qubit devient $|0\rangle$,
- soit la valeur 1, avec probabilité $|\beta|^2$, et l'état du qubit devient $|1\rangle$.

α et β : « amplitudes de probabilité »

En bref : 2 sortes d'évolutions pour $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Calcul déterministe : évolution de l'état par application d'un opérateur unitaire à $|\psi\rangle$, c.à.d. en faisant le produit du vecteur $|\psi\rangle$ par U, matrice 2×2 unitaire.

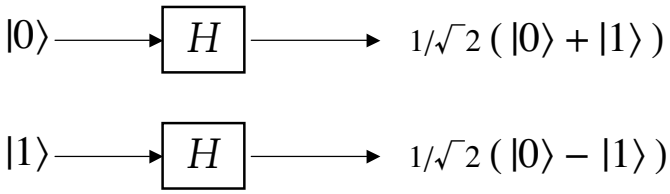
Mesure probabiliste : selon une probabilité qui dépend de $|\psi\rangle$, évolution de l'état par projection de $|\psi\rangle$ soit sur $|0\rangle$ soit sur sur $|1\rangle$ (puis renormalisation de la projection), et retour de la valeur classique 0 si la projection était sur $|0\rangle$, de la valeur 1 si la projection était sur $|1\rangle$.



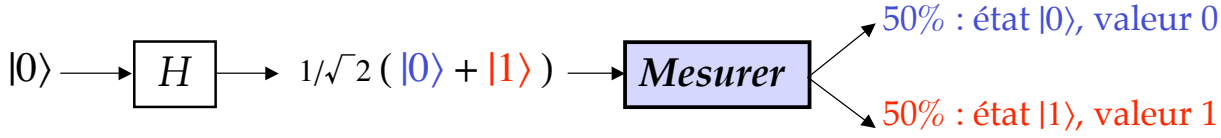
Exemples d'opérations sur un qubit

Opérateur unitaire :

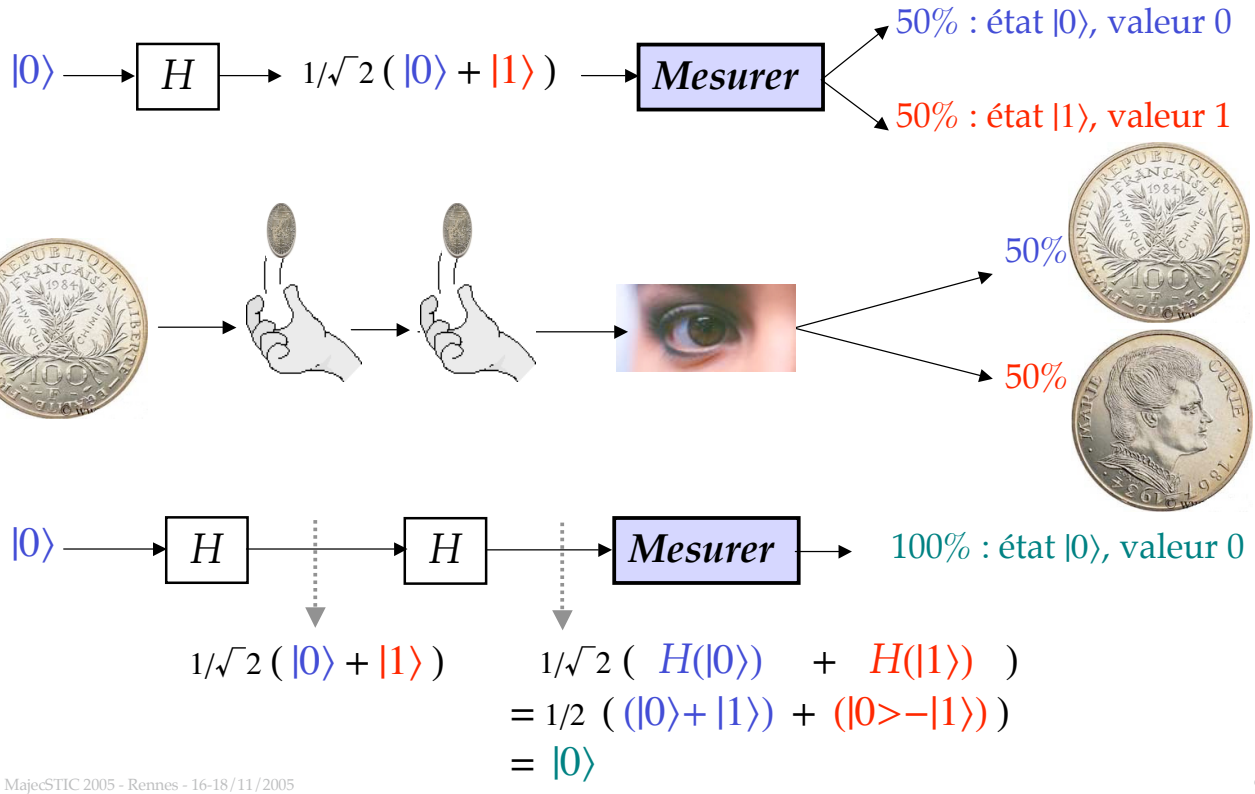
$$H = 1/\sqrt{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Mesure :



Etats quantiques : pas classiques du tout !



Cryptographie

La sécurité d'un canal de communication n'est jamais garantie à 100%

Cryptographie classique :

- Cryptographie à clé secrète : Alice crypte avec une clé. Bob décrypte avec la même clé. Cette clé est connue par Alice et Bob, et par personne d'autre.
- Cryptographie à clé publique : Alice crypte avec la clé publique de Bob, connue par tout le monde. Bob décrypte avec sa clé privée, connue de lui seul.

Cryptographie classique : quelques écueils

- Cryptographie à clé secrète
  - Le cryptage peut être absolument sûr, à condition que la clé soit secrète
  - Exige la sécurité absolue du canal par lequel la clé est distribuée
  - L'observation passive d'un canal est toujours possible
  - Recours à une sécurité non prouvée pour distribuer la clé
- Cryptographie à clé publique
  - Sécurité fondée sur des conjectures mathématiques non prouvées (comme la complexité exponentielle de la factorisation des entiers : beaucoup de fois l'age de l'univers pour factoriser un nombre de 300 chiffres)
  - Une preuve invalidant une telle conjecture détruirait rétroactivement la sécurité de tout message crypté de cette façon
  - L'algorithme quantique de Peter Shor factorise les entiers en temps polynomial (dès qu'un ordinateur quantique est disponible, quelques secondes suffisent pour factoriser un nombre de 300 chiffres)

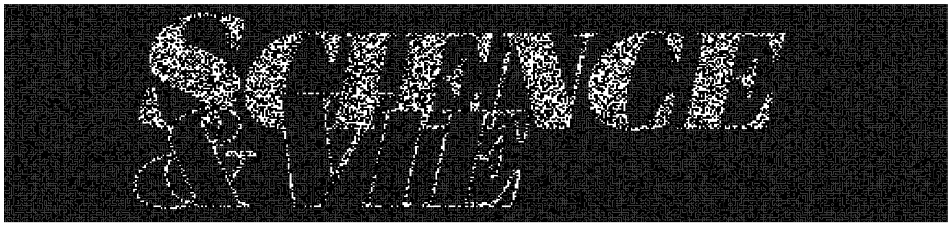
Le *one-time pad* : sécurité absolue et prouvée

- Gilbert Vernam, AT&T, 1917 : $(m \oplus k) \oplus k = m$

- Joseph Mauborgne, US Army, années 20 :
  Si la clé est une suite aléatoire, alors le message crypté est une suite aléatoire, sans information pour quiconque ignore la clé.
- Deux conditions :
  - La clé doit être secrète
  - La clé ne doit être utilisée qu'une seule fois

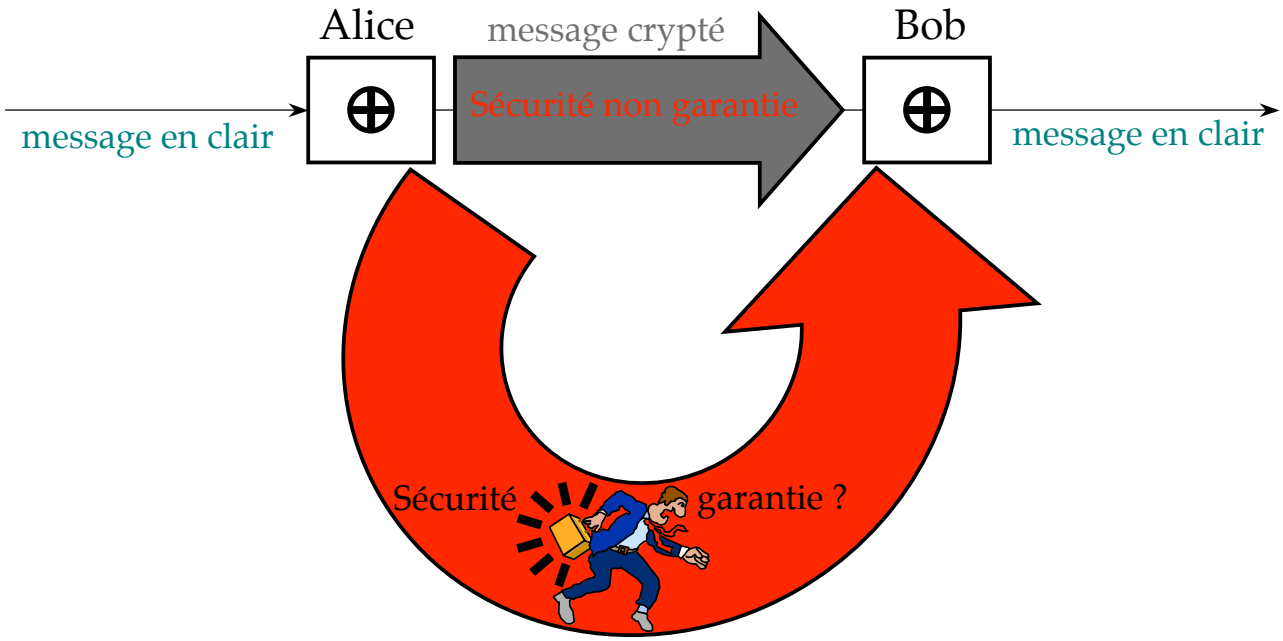
Le *one time pad* en action chez Bob

clé secrète



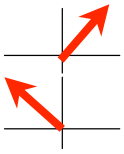
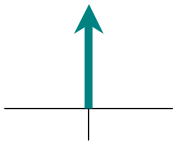
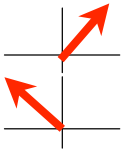
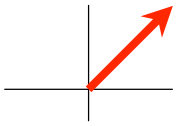
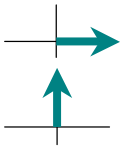
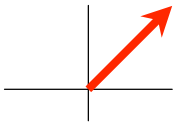
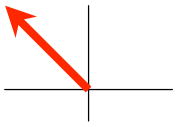
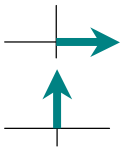
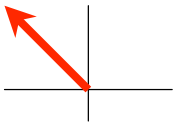
message crypté

Problème : la clé doit être secrète



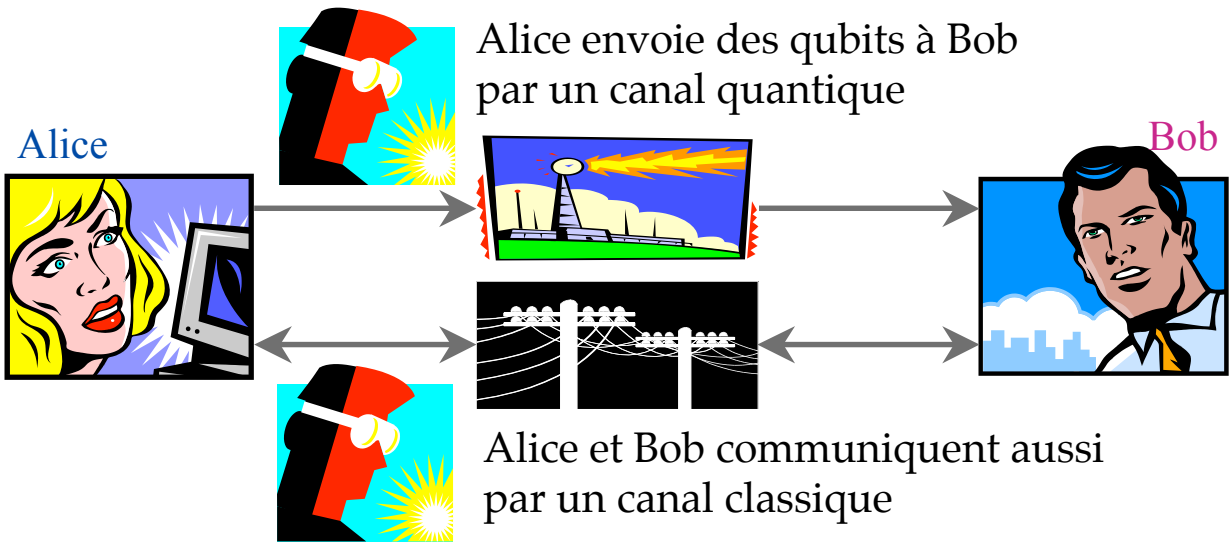
Cryptographie quantique : garantir le secret de la clé sans rien avoir à supposer de la sécurité offerte par les canaux utilisés.

Retour sur la mesure quantique

Etat avant mesure	Dans la base standard : Proba.	Etat après mesure	Valeur obtenue	Dans la base diagonale : Proba.	Etat après mesure	Valeur obtenue
	1		0	0.5 0.5		0 1
	1		1	0.5 0.5		0 1
	0.5 0.5		0 1	1		0
	0.5 0.5		0 1	1		1

Cryptographie quantique : les personnages, le décor

Eve, observateur indiscret, intercepte les qubits sur le canal quantique, les mesure et les fait suivre à Bob

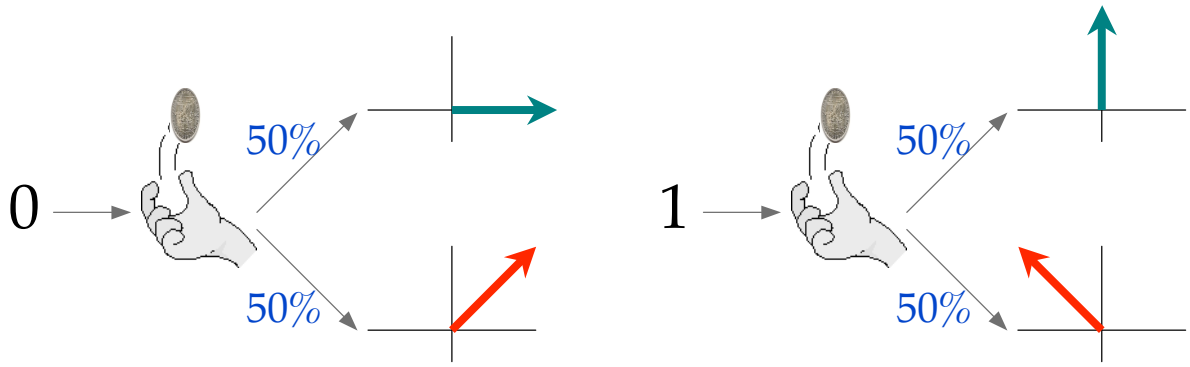


Eve écoute aussi les conversations d'Alice et Bob

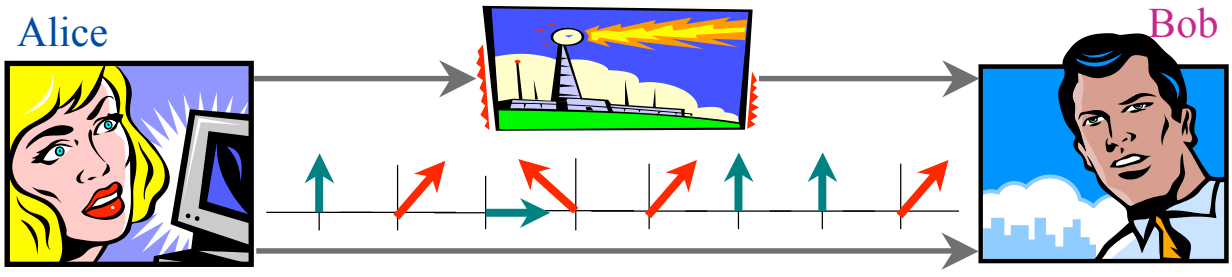
Protocole BB84 (Bennett - Brassard, 1984)

1ère étape : Alice envoie des qubits à Bob par le canal quantique

- Alice construit chez elle une suite aléatoire de 0 et de 1, quatre fois plus longue que la clé confidentielle dont Alice et Bob auront besoin plus tard.
- Alice envoie ces 0 et ces 1, un par un, à Bob, codés chaque fois par un qubit. Pour chaque 0 et chaque 1, elle choisit au hasard entre 2 codages possibles :

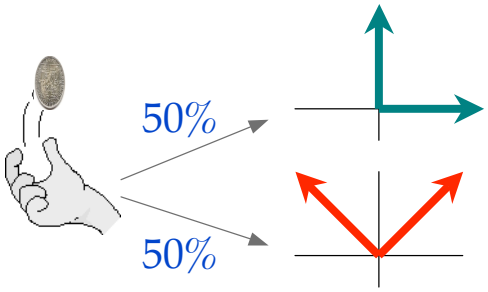


BB84 : suite de la 1ère étape



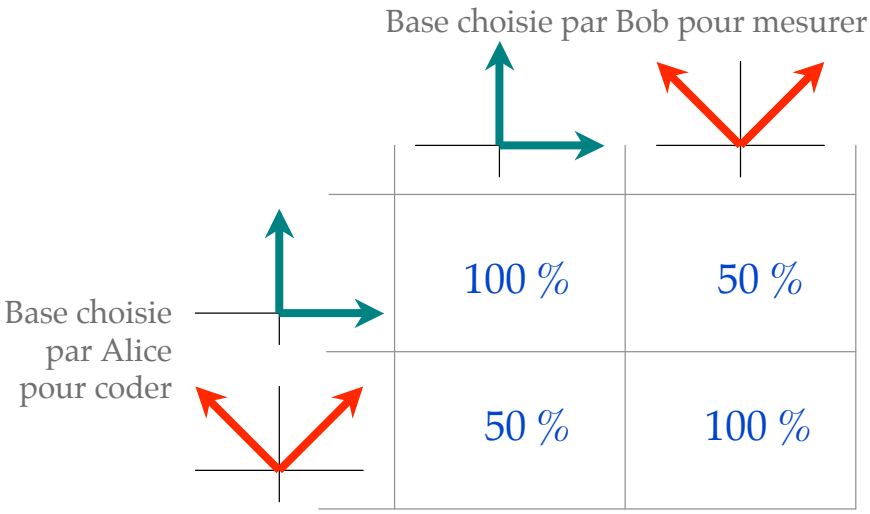
- Pour chaque qubit qu'il reçoit, Bob ne sait :
  - ni si Alice a codé un 0 ou un 1 avec ce qubit
  - ni dans quelle base, standard ou diagonale, Alice a codé ce 0 ou ce 1

- Pour chaque qubit reçu, Bob tire au hasard la base dans laquelle il va le mesurer :

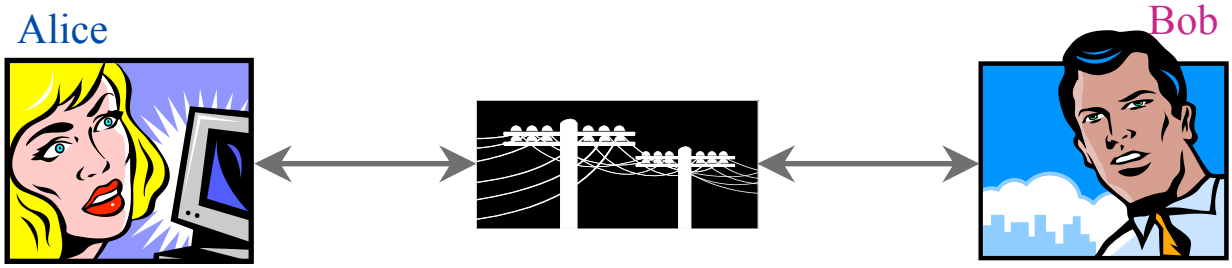


BB84 : résultats de la 1ère étape

- Pour chaque 0 et 1 de la suite aléatoire qu'Alice a chez elle, Bob obtient un 0 ou un 1. Bob construit ainsi chez lui une suite aléatoire de 0 et de 1.
- La probabilité d'avoir la même valeur, 0 ou 1, à la même position dans ces deux suites, dépend des bases choisies par Alice et Bob à cette position :



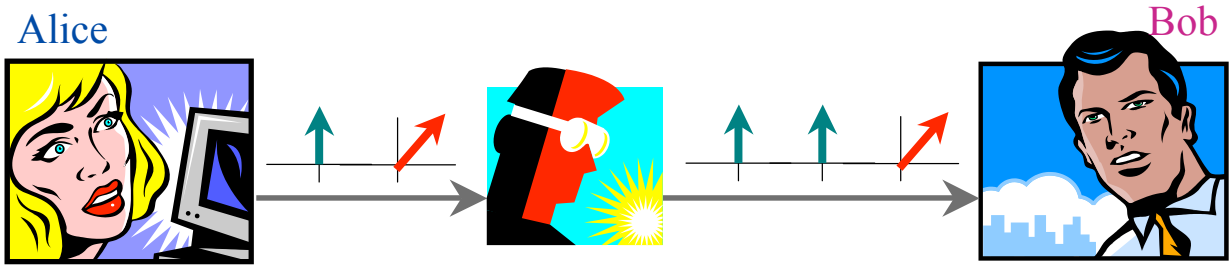
BB84 : 2ème étape, sur le canal classique



- Alice dit à Bob la suite des bases qu'elle a utilisées pour coder, sans révéler si c'était un 0 ou un 1 qu'elle avait codé.
- Bob dit à Alice la suite des bases qu'il a utilisées pour mesurer, sans révéler si c'est un 0 ou 1 qu'il a obtenu.
- Ils ne conservent, chacun de leur côté, que les 0 et les 1 des positions pour lesquelles ils ont utilisé les mêmes bases, soit approximativement la moitié des 0 et des 1 de la suite initiale d'Alice.

Ceci pourrait former une clé secrète ... sauf si ...

BB84 : les indiscrétions d'Eve



Pendant la 1ère étape, Eve a pu observer le canal quantique :

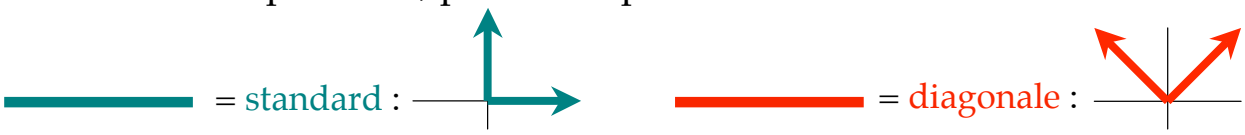
- Intercepter les qubits.
- Les mesurer dans une base qu'elle a dû, comme Bob, choisir au hasard.
- Renvoyer à Bob chaque qubit ainsi intercepté et mesuré, Bob croyant que ce qubit vient d'Alice.

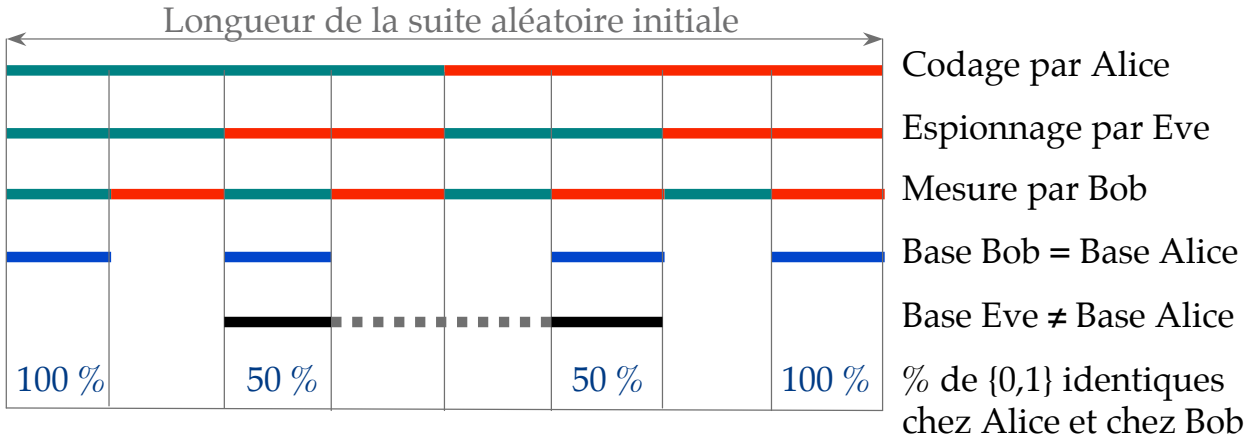
Conséquences :

- Chaque fois qu'Eve choisit la même base qu'Alice, le qubit reçu par Bob est identique à celui envoyé par Alice. Cette indiscrétion est indétectable.
- Mais si Eve ne choisit pas la même base qu'Alice, le qubit reçu par Bob est différent de celui envoyé par Alice. Cette indiscrétion laisse des traces.

BB84 : traces laissées par les indiscrétions d'Eve

- Bases utilisées par Alice, par Eve et par Bob :





- Si Eve a espionné, 25 % des {0,1} conservés par Alice et Bob à l'issue de la 2ème étape sont différents bien qu'ils aient utilisé des bases identiques.

BB84 : dernière étape, encore au téléphone

- Alice et Bob choisissent au hasard 50 % des positions de {0,1} qui avaient été retenues à l'issue de la 2ème étape.
- Ils comparent ces {0,1}, position par position, dans la suite d'Alice et dans la suite de Bob. Ils sacrifient ces positions, car Eve peut écouter.
- La probabilité qu'ils soient tous identiques malgré un espionnage décroit de façon exponentielle avec le nombre n de {0,1} comparés : $(3/4)^n$ (soit 3.10^{-13} pour n=100).
- Si le taux d'erreurs est de l'ordre du taux dû à une ligne normalement bruitée, le 1/4 restant est une clé confidentielle après correction d'erreurs (et amplification de confidentialité si nécessaire). Sinon, ils recommencent.

Cryptographie quantique : état de l'art

- La « cryptographie » quantique n'est pas de la cryptographie, car rien n'est crypté. En anglais : *Quantum Key Distribution* (QKD).
- Plusieurs protocoles :
  BB84 utilise 4 états pour coder les {0,1}
  B92 (Bennet) utilise 2 états non orthogonaux
  EPR (Ekert) utilise des mesures d'états intriqués (paires EPR)
  Et beaucoup de variantes. Ils exploitent tous les perturbations des états quantiques inévitablement provoquées les indiscrétions.
- Ces protocoles doivent être complétés par des procédures classiques de réconciliation (correction d'erreur) et d'amplification de confidentialité.
- Plusieurs formes d'attaques prises en compte, car Eve peut être plus subtile que « *j'intercepte tout, je mesure tout et je renvoie tout à Bob* ».
- Exploitation des propriétés de l'information quantique pour traiter d'autres problèmes : authentification, partage de secrets.

La cryptographie quantique sur le marché

- Expérimentée sur 50 à 100 kilomètres (qubit = photon) sur fibre optique, dans l'air. Performances encore modestes (100 kbps, NEC)
- id Quantique (Genève)

  Premier système commercial de distribution quantique de clés :

- MagiQ Technologies (New York et Boston)
- QIPC « EQUIS » project (Heriot-Watt University et Corning, UK)

  Intégration dans des PC standards
- Thalès, British Telecom, Swiss Telecom, IBM, Lucent, AT&T, NEC, etc.
- Réseaux de distribution envisagés par des institutions financières, échanges de clés terre-satellites en cours de conception (US, Europe)

Etat d'un registre de 2 qubits

L'état d'un seul qubit est un vecteur dans un espace à 2 dimensions :

- l'un des 2 états de base : $|0\rangle$ ou $|1\rangle$
- ou, plus généralement, une superposition d'états de base :

  $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, avec $|\alpha|^2 + |\beta|^2 = 1$

L'état d'un registre de 2 qubits est un vecteur dans un espace à 4 dimensions :

- l'un des 4 états de base : $|00\rangle$, $|01\rangle$, $|10\rangle$ ou $|11\rangle$
- ou, plus généralement, une superposition d'états de base :

  $|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, avec $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$

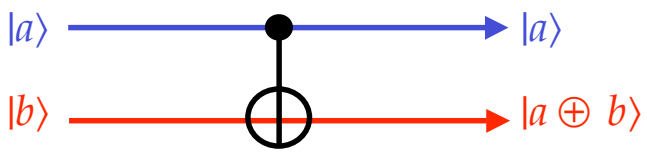
Exemples :

$|\psi\rangle = 1/2\ (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = 1/\sqrt{2}\,(\,|0\rangle + |1\rangle\,) \otimes 1/\sqrt{2}\,(\,|0\rangle + |1\rangle\,)$

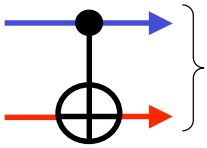
$|\varphi\rangle = 1/\sqrt{2}\ (|00\rangle + |11\rangle)$

Exemple d'opérateur sur 2 qubits : *Controlled Not*

CNot :

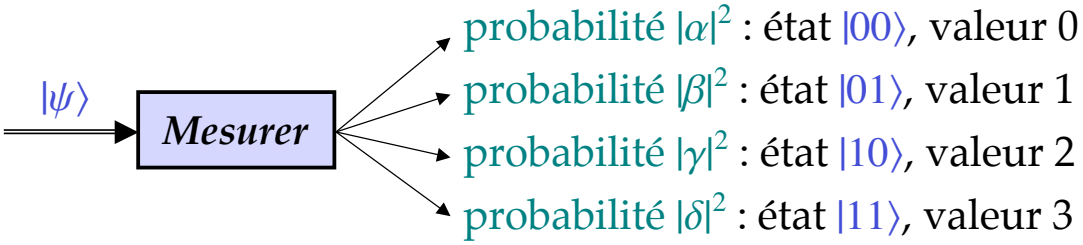


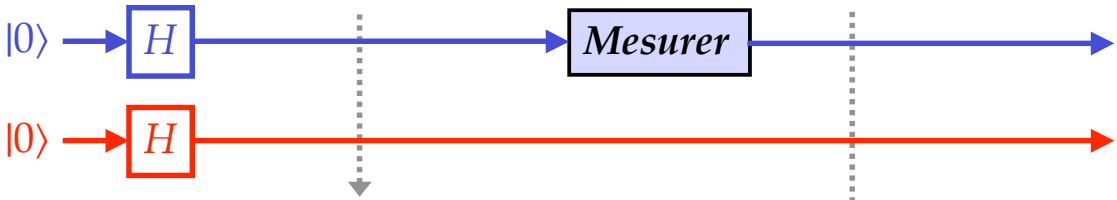
$CNot\ (|00\rangle) = |00\rangle$
$CNot\ (|01\rangle) = |01\rangle$
$CNot\ (|10\rangle) = |11\rangle$
$CNot\ (|11\rangle) = |10\rangle$

$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ {  } $\alpha|00\rangle + \beta|01\rangle + \gamma|11\rangle + \delta|10\rangle$

Mesurer un registre de 2 qubits

$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

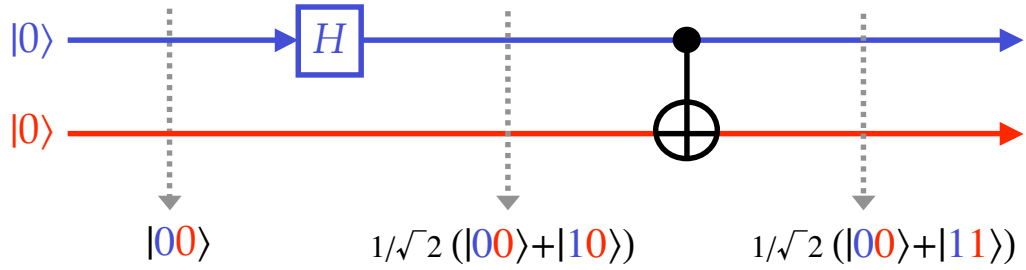




$1/\sqrt{2}\,(|0\rangle + |1\rangle) \otimes 1/\sqrt{2}\,(|0\rangle + |1\rangle)$
$= 1/2\ (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

proba. 50% : état $|0\rangle \otimes 1/\sqrt{2}\,(|0\rangle+|1\rangle) = 1/\sqrt{2}\,(|00\rangle+|01\rangle)$, valeur 0
proba. 50% : état $|1\rangle \otimes 1/\sqrt{2}\,(|0\rangle+|1\rangle) = 1/\sqrt{2}\,(|10\rangle+|11\rangle)$, valeur 1

En général, les états quantiques sont intriqués



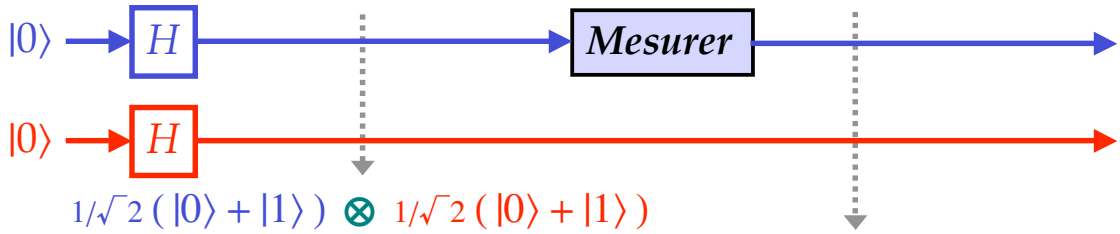
C'est une situation impossible dans le monde classique :
il n'existe pas $|\psi_1\rangle$, $|\psi_2\rangle$ tels que $1/\sqrt{2}\,(|00\rangle+|11\rangle) = |\psi_1\rangle \otimes |\psi_2\rangle$

Après exécution, les deux qubits sont dans un état intriqué.

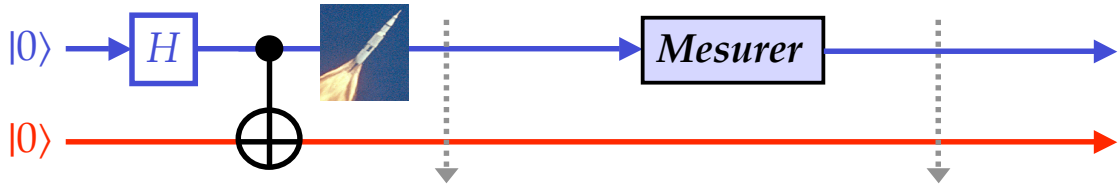
L'état $1/\sqrt{2}\,(|00\rangle+|11\rangle)$ est une "paire EPR" :

[Einstein, Podolsky, Rosen]
« *Can quantum mechanical description of physics reality be considered complete?* » *Physical Review*, 1935

Etats quantiques : encore plus loin du classique…



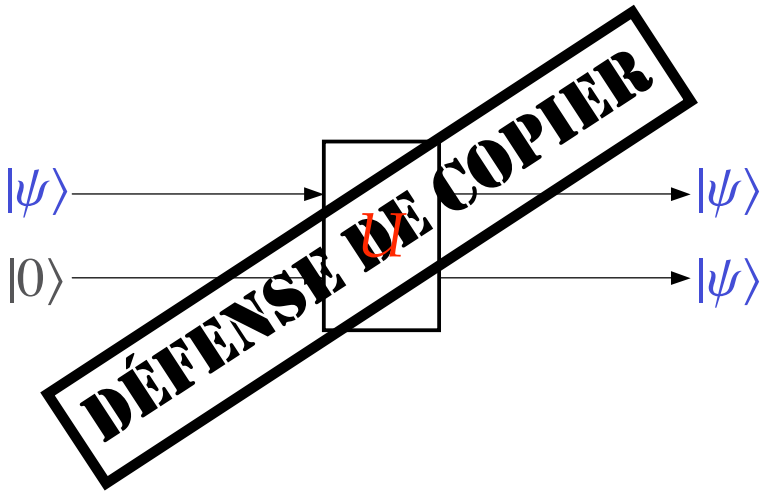
proba. 50% : état $|0\rangle \otimes 1/\sqrt{2}\,(|0\rangle+|1\rangle)$, valeur 0
proba. 50% : état $|1\rangle \otimes 1/\sqrt{2}\,(|0\rangle+|1\rangle)$, valeur 1



proba. 50% : état $|00\rangle$, valeur 0
proba. 50% : état $|11\rangle$, valeur 1

Einstein, 1935 : « … *spooky action at a distance* … »

… et toujours plus loin du classique : *no cloning* !



Théorème : Il n'existe pas de transformation unitaire U telle que pour tout état $|\psi\rangle$, $U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$.

Preuve : conséquence immédiate de la linéarité des opérateurs.

L'histoire d'Alice et Bob

Il était une fois ...

… Alice et Bob qui, avant de se séparer, prirent chacun un qubit d'une même paire EPR : $1/\sqrt{2}\,(|00\rangle+|11\rangle)$.
Puis Bob s'en alla, vers une galaxie secrète et lointaine.

C'est alors que, plus tard, ...

... un qubit dans un état inconnu, $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, arriva chez Alice, avec une mission pour Alice : transmettre $|\psi\rangle$ à Bob.

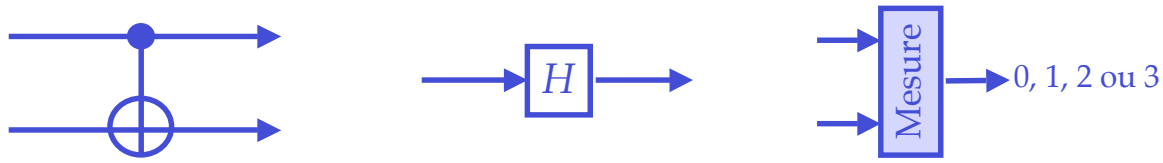
Mais Alice ne pouvait pas ...

... porter ce qubit à Bob,
... ni cloner $|\psi\rangle$ pour en disperser des copies dans l'univers,
... ni connaître α et β pour diffuser leurs valeurs sur les ondes dans l'espace intergalactique.

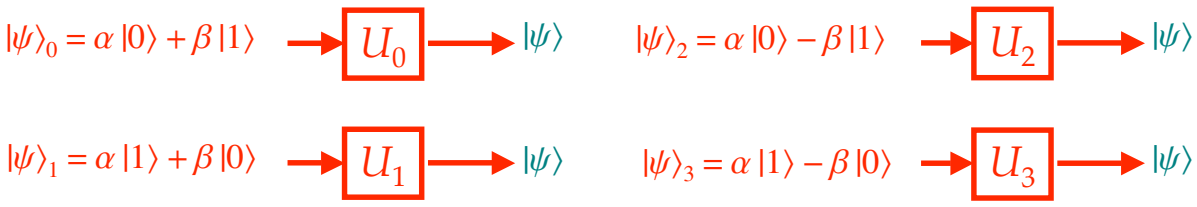
Alors Alice téléporta $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ à Bob

Ils avaient prévu tout ce qu'il fallait :

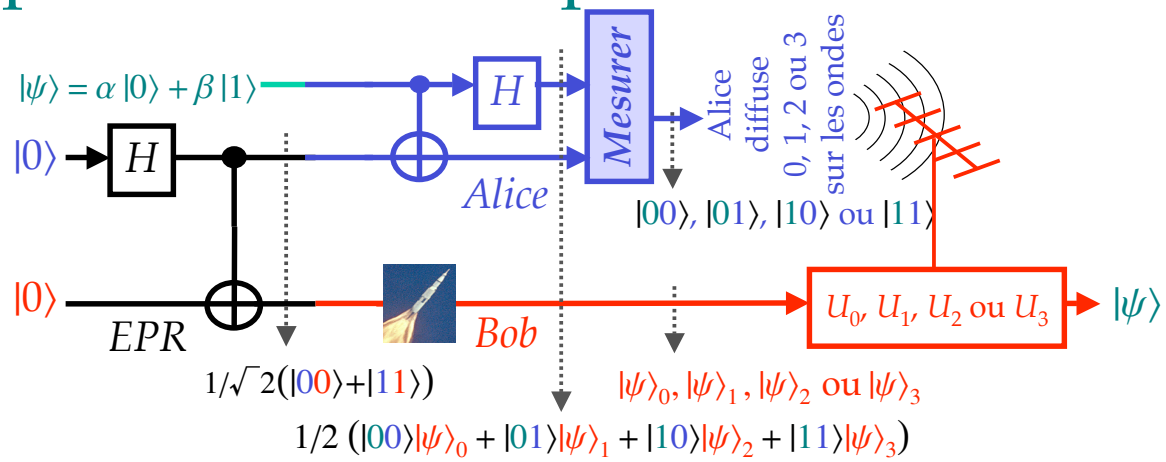
- Un « canal quantique », la paire EPR $1/\sqrt{2}\,(|00\rangle+|11\rangle)$, dont ils avaient soigneusement gardé chacun un qubit avant le départ de Bob.
- Alice a chez elle les opérateurs *Cnot* et *H*, et un appareil pour mesurer 2 qubits :



- Bob a emporté quatre opérateurs, U_0, U_1, U_2 et U_3, dans son vaisseau spatial :

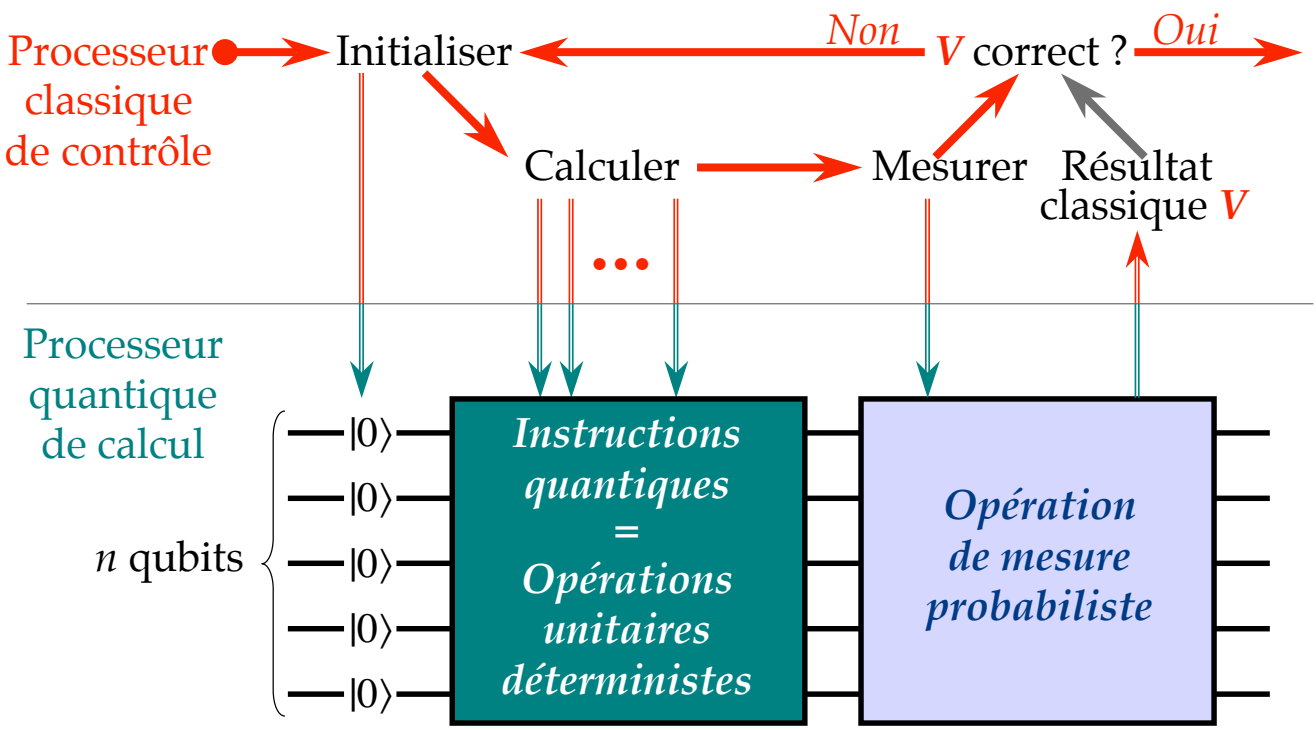


Le protocole de téléportation



- 3 processus : *EPR*, *Alice*, *Bob*. Les 2 qubits de *EPR* sont initialisés à $|0\rangle$
- Ces 2 qubits sont intriqués par *EPR*, puis ils sont pris, l'un par *Alice*, l'autre par *Bob*
- Un qubit dans un état inconnu $|\psi\rangle$ arrive chez *Alice*
- *Alice* effectue des opérations unitaires. Conséquence : les 3 qubits sont intriqués
- *Alice* mesure ses 2 qubits. Conséquence : l'état du qubit de *Bob* $\in \{|\psi\rangle_0,|\psi\rangle_1,|\psi\rangle_2,|\psi\rangle_3\}$
- Une valeur sur 2 bits classiques est envoyée par *Alice* et reçue, un jour, par *Bob*
- Au vu de ces 2 bits, *Bob* sait quel opérateur unitaire appliquer : $|\psi\rangle$ est chez *Bob*

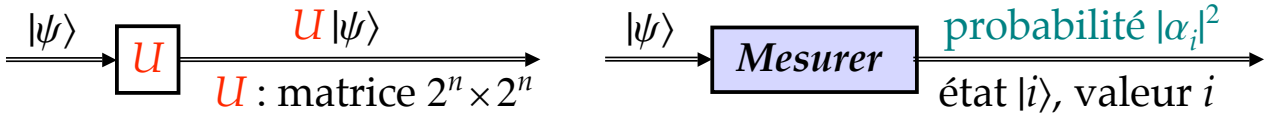
Calculer avec des ressources quantiques



Registre de n qubits : état et évolution

L'état d'un registre de n qubits est un vecteur dans un espace à 2^n dimensions :

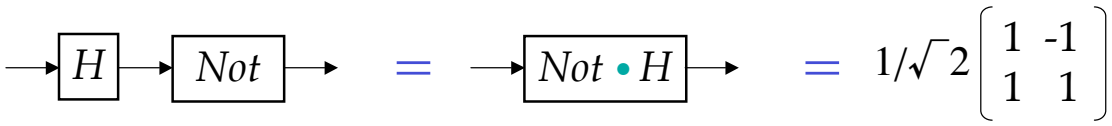
- l'un des 2^n états de base : $|00..00\rangle$ (c.à.d. $|0\rangle$)
  $|00..01\rangle$ (c.à.d. $|1\rangle$)
  $|00..10\rangle$ (c.à.d. $|2\rangle$)
  ...
  $|11..11\rangle$ (c.à.d. $|2^n-1\rangle$)
- ou, plus généralement, une superposition d'états de base :
  $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle + \ .. \ + \alpha_{2^n-1}|2^n-1\rangle$,
  avec $|\alpha_0|^2 + |\alpha_1|^2 + \ .. \ + |\alpha_{2^n-1}|^2 = 1$



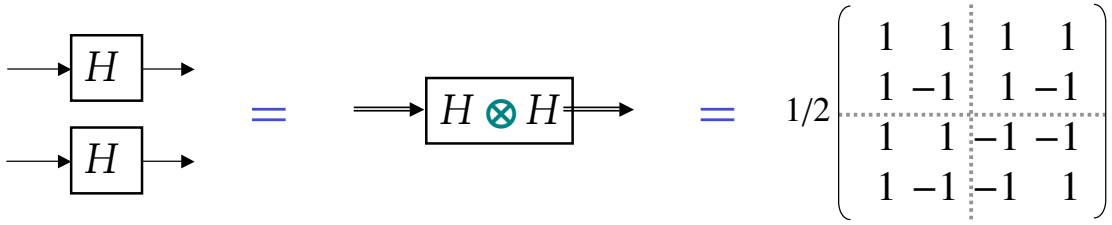
Famille universelle pour approcher tout U ($2^n \times 2^n$)

$$H = 1/\sqrt{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix} \qquad CNot = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- Composition temporelle d'opérateurs : produit matriciel



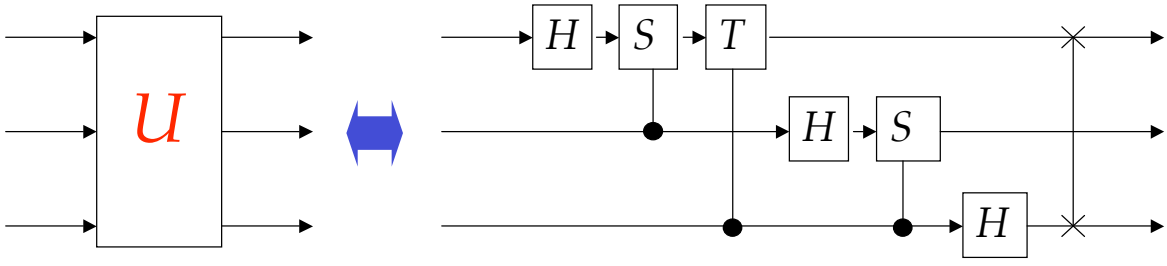
- Composition spatiale d'opérateurs : produit tensoriel



Calcul par transformation unitaire

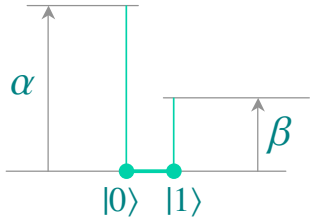
Théorème : Tout produit (matriciel, tensoriel) de transformations unitaires est une transformation unitaire.

Théorème : Toute transformation unitaire sur n qubits peut se décomposer en produit de transformations unitaires sur 1 qubit ou sur 2 qubits.

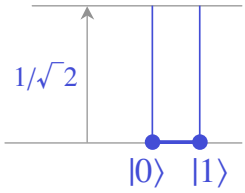


Représentation graphique d'amplitudes réelles

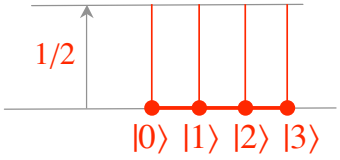
$\alpha\,|0\rangle + \beta\,|1\rangle$



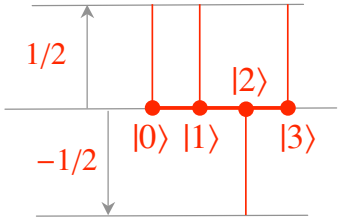
$1/\sqrt{2}\,(|0\rangle+|1\rangle)$



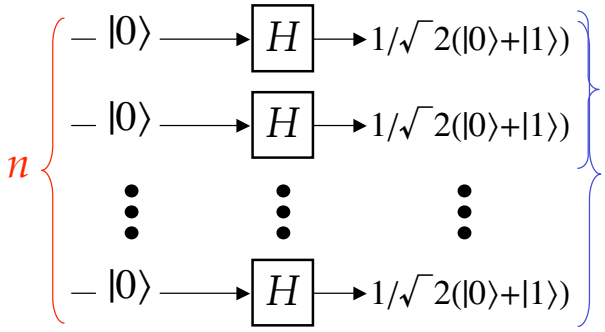
$1/2\,(\,|0\rangle + |1\rangle + |2\rangle + |3\rangle\,)$



$1/2\,(\,|0\rangle + |1\rangle - |2\rangle + |3\rangle\,)$



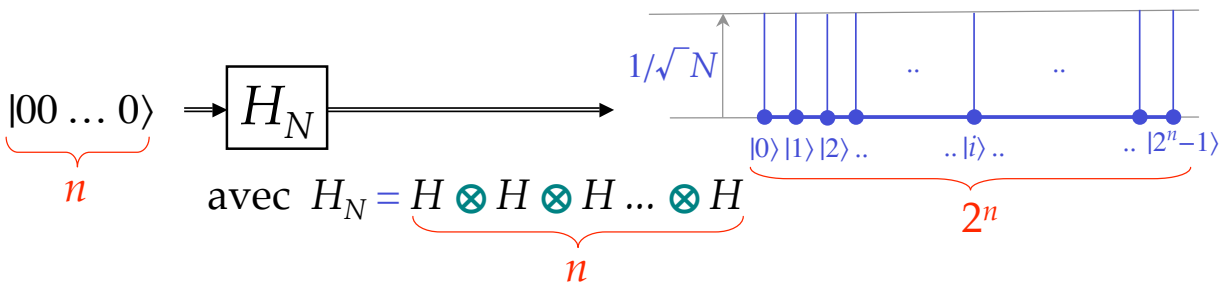
2^n valeurs superposées dans un registre de n qubits



$= 1/2\,(\,|0\rangle + |1\rangle + |2\rangle + |3\rangle\,)$

$= 1/\sqrt{N}\,(\,|0\rangle + |1\rangle + |2\rangle + \,..\, + |2^n-1\rangle\,)$

avec $N = 2^n$

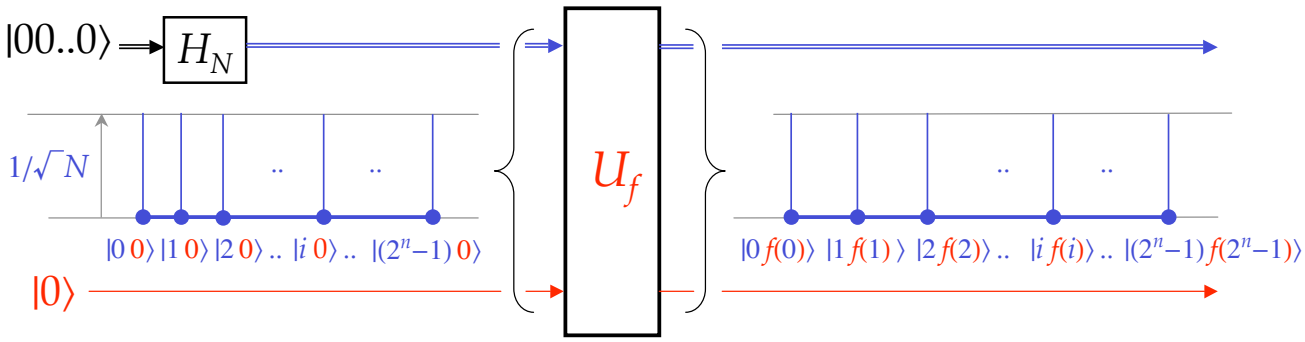


avec $H_N = \underbrace{H \otimes H \otimes H \ldots \otimes H}_{n}$

- n opérations pour calculer 2^n valeurs

Calculer une fonction : parallélisme quantique

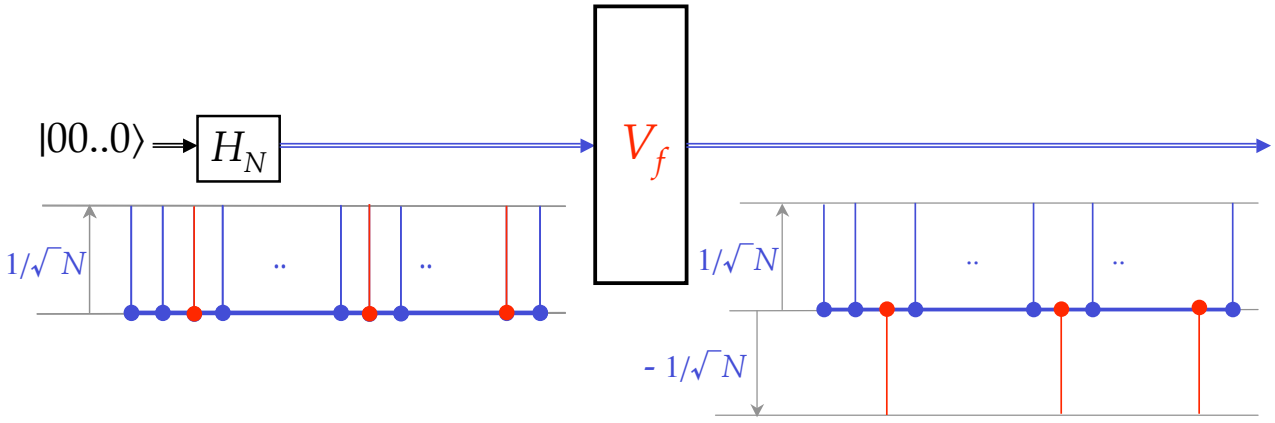
$f(a) \in \{0,1\}$ $a \in [0,2^n-1]$



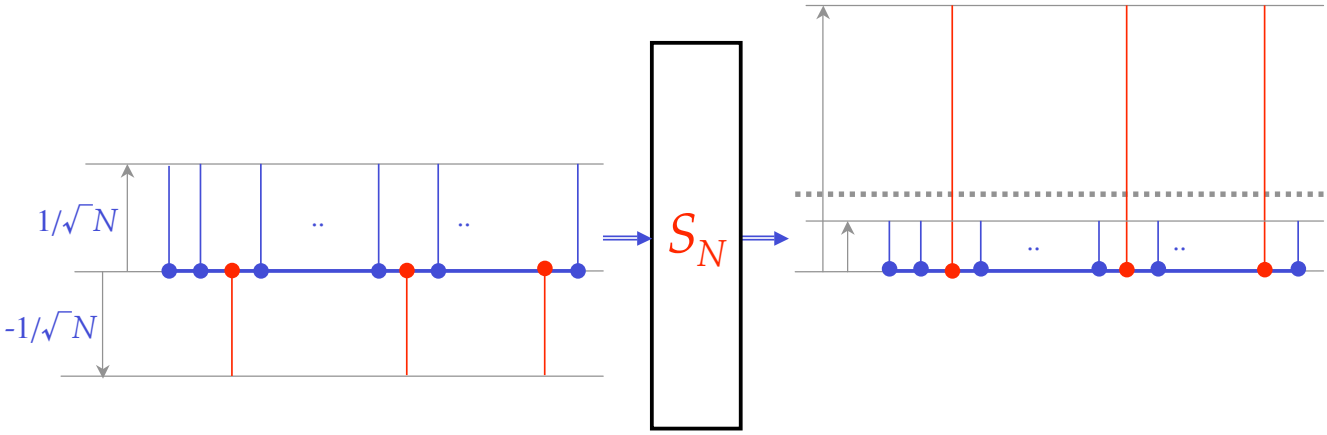
- 1 opération pour calculer toutes les valeurs de la fonction

Inverser les amplitudes des a tels que $f(a) = 1$

$f(a) \in \{0,1\}$ $a \in [0,2^n-1]$



Symétrie par rapport à la moyenne



Algorithme de Grover (1996) : accélération quadratique

- 1 000 000 de noms listés dans un annuaire, en ordre alphabétique :
  NOM nnn nn nn
- Etant donné un numéro xxx xx xx, trouver le NOM unique tel que :
  nnn nn nn = xxx xx xx
- Algorithmes classiques :
  jusqu'à 1 000 000 de requêtes « nnn nn nn = xxx xx xx ? »
- Algorithme quantique de Lov Grover (Lucent, USA) :
  exactement 1 000 requêtes « nnn nn nn = xxx xx xx ? »

Trouver l'élément qui, parmi $N=2^n$, satisfait f

$f(a) \in \{0,1\}$ $a \in [0,2^n-1]$

$f(a)=1$ pour un et un seul $a = a_0 \in [0,2^n-1]$

Aucune autre information disponible sur f

Problème : trouver ce a_0

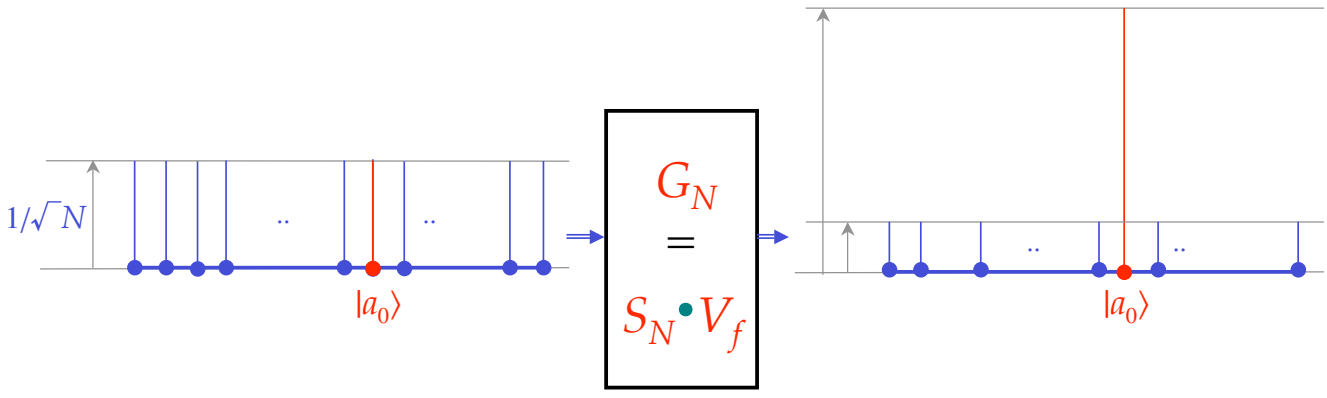
Calcul classique :
- au pire, N appels à f
- en moyenne, $N/2$ appels à f

Calcul quantique :
- exactement $\sqrt{N}$ appels à f,
- hors d'accès du calcul classique

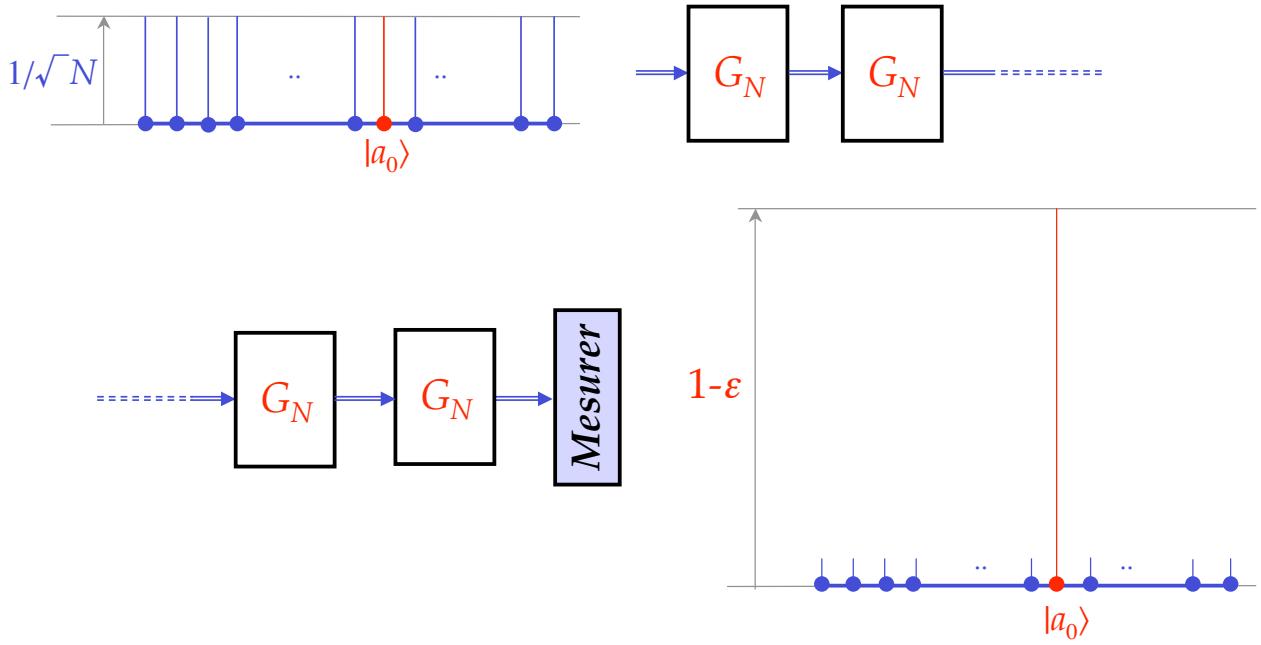
Amplification de l'amplitude de $|a_0\rangle$

$f(a) \in \{0,1\}$ $a \in [0,2^n-1]$

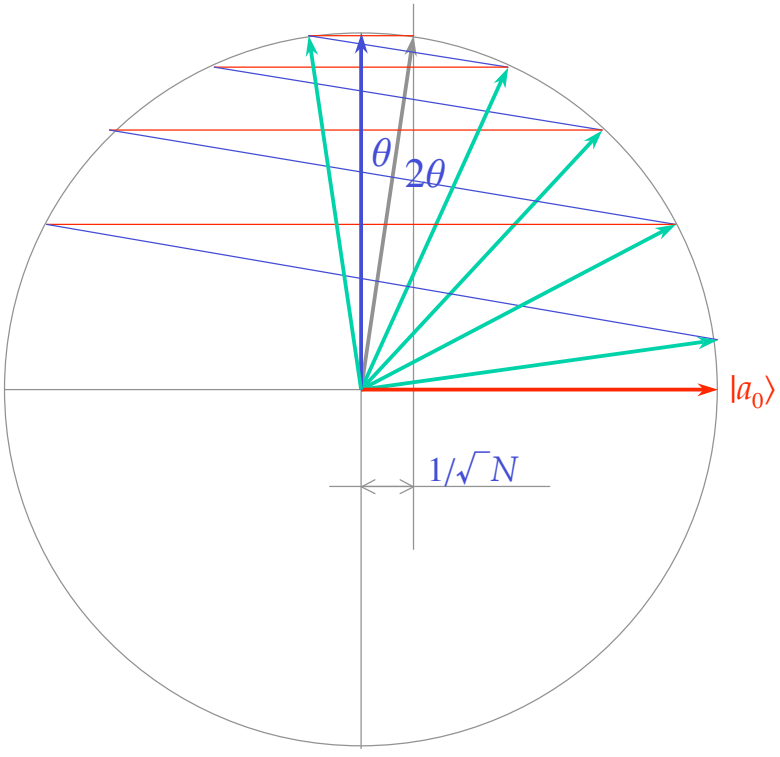
$f(a)=1$ pour un seul $a = a_0 \in [0,2^n-1]$



Recherche de a_0 : algorithme de Grover



Stop à $\sqrt{N}$ fois G_N ! Preuve géométrique



- But : arriver aussi près que possible de $|a_0\rangle$. Pour cela, il faut répéter k fois G_N, où :

$$\pi/2 - \theta \leqslant \theta + k\,2\theta \leqslant \pi/2 + \theta$$

- N est grand, donc θ est petit :

$$\theta \approx \sin\theta = 1/\sqrt{N}$$

- Donc : $k \approx \pi/4\,\sqrt{N}$
- Accélération quadratique

Algorithme de Shor (1994) : accélération exponentielle

Factorization of RSA-155

On August 22, 1999, a team of scientists from 6 different countries, led by CWI (Amsterdam), completed the factorization of the 155 digit (512 bit) RSA Challenge Number:

RSA-155=109417386415705274218097073220403576120 037329454492059909138421314763499842889347847179972578912673324976257528997818337970765372440271467435315933543338 97

The computation took 35.7 CPU-years on :

160	*175-400 MHz SGI and Sun workstations*
8	*250 MHz SGI Origin 2000 processors*
120	*450 MHz Pentium II PCs*
4	*500 MHz Digital/Compaq boxes*

The CPU-effort is estimated to be equivalent to 8000 MIPS years. The Total calendar time for factoring RSA-155 was 7.4 months, whereas RSA-140 took about 9 weeks «only».

The found factors are:
p=102639592829741105772054196573991675900716567 808038066803341933521790711307779, and
q=106603488380168454820927220360012878679207958 575989291522270608237193062808643

- Factorisation classique

Le nombre d'opérations nécessaires aux meilleurs algorithmes classiques est une fonction exponentielle de la taille (combien de chiffres pour l'écrire) du nombre à factoriser : de l'ordre de $e^{155/3}$ pour RSA-155.

- Factorisation quantique

Le nombre d'opérations nécessaires à l'algorithme quantique de Peter Shor (AT&T, USA) est une fonction polynomiale de la taille du nombre à factoriser : de l'ordre de 155^3 pour RSA-155.

Calcul quantique : quelques étapes majeures

- 1982, Richard Feynman (Caltech) - Calculer en se fondant sur la physique quantique serait exponentiellement plus efficace qu'en se fondant sur la physique classique.
- 1985, David Deutsch (Oxford) - Calcul quantique ou calcul classique, les fonctions calculables sont les mêmes. Mais il y a plus de fonctions "raisonnablement calculables".
- 1993, Charles Bennet (IBM Research) - Conception du principe théorique de la téléportation : l'état d'un système quantique a initialement localisé chez A peut être relocalisé chez B, sans que cet état ne soit connu, ni copié, ni déplacé de A à B.
- 1994, Peter Shor (AT&T) - Conception théorique d'un algorithme polynomial pour factoriser les entiers (le meilleur algorithme classique est exponentiel).
- 1996, Lov Grover (Lucent) - Conception théorique d'un algorithme qui n'a besoin que de $\sqrt{N}$ pas pour trouver un élément dans une base de données non ordonnée de taille N (en calcul classique, de l'ordre de N pas sont requis).
- 1997, Anton Zeilinger (Vienne) - Première téléportation expérimentale (de l'état d'un photon). Suivie depuis par beaucoup d'autres, avec d'autres particules.
- 1999, 2002, Isaac Chuang (IBM Research) - Première réalisation expérimentale d'un ordinateur quantique, fondé sur la RMN, avec 7 qubits. Premières exécutions expérimentales des algorithmes de Grover et de Shor.
- 2004, Christof Dürr, Peter Hoyer, Mehdi Mhalla - Accélération quadratique pour des problèmes classiques sur les graphes (connectivité, arbre couvrant de poids minimal, ...)

Hot topics en traitement de l'information quantique

- Algorithmes quantiques, théorie de la complexité algorithmique quantique
- Cryptographie quantique, partage de secrets, authentification, répéteurs quantiques
- Communication et calcul quantique distribué, théorie de la complexité de communication quantique
- Autres modèles de calcul quantique : calcul quantique fondé sur la mesure, calcul quantique adiabatique, calcul quantique topologique, automates cellulaires quantiques
- Machines quantiques abstraites, algèbres de processus quantiques, fondements logiques et mathématiques, principes architecturaux pour machines quantiques
- Compréhension et caractérisation des états intriqués
- Canaux de communication quantique, théorie de l'information quantique

… et mise en œuvre physique
de l'ordinateur quantique…

Vers l'ordinateur quantique

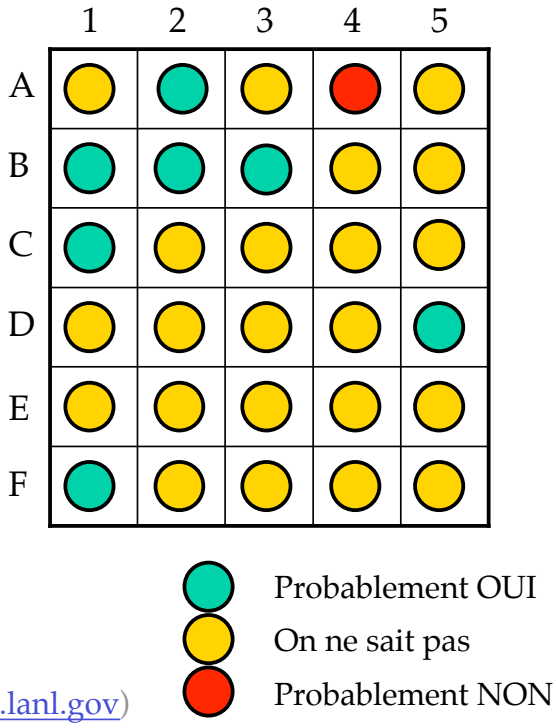
Critères de DiVicenzo (IBM Research) :

1. Qubits initialisables
2. Famille universelle d'opérateurs
3. Qubits mesurables
4. Passage à l'échelle
5. Temps de décoherence
   >> temps pour 1 opérateur

Six approches (parmi d'autres) :

A. Résonance magnétique nucléaire
B. Ions piégés
C. Atome neutres piégés
D. Optique
E. Spins l'électrons
F. Jonctions de Josephson

(Source: *A Quantum Information Science and Technology Roadmap*, ARDA, April 2004 - http://qist.lanl.gov)



Informatique théorique ET physique

"We need to find a synergy between abstract models of computation and proposed implementations. As physicists better understand the limitations of what we can implement, computer scientists can better devise models and algorithms to handle these limitations. Conversely, as computer scientists understand what resources are critical for quantum algorithms to work, physicists can better design implantations to address these issues."

(Source: *Report on the Theory of Quantum Computing*, NSF, January 2002)

Quelques références et liens utiles

• Quantum Computation and Quantum Information
M. A. Nielsen and I. L. Chuang - Cambridge University Press, 2000

• Quantum Computing
M. Hirvensalo - Springer, 2001

• An Introduction to Quantum Computing for Non-Physicists
E. Rieffel and W. Polak - http://arxiv.org/abs.quant-ph/9809016
Aussi dans ACM Computing Surveys, Vol. 32 , No. 3, Sept. 2000, pp. 300 - 335

• Quantum physics archive at Los Alamos - http://arxiv.org/archive/quant-ph
Plusieurs preprints par jour sur le traitement et la communication de l'information quantique, depuis la physique expérimentale jusqu'à l'informatique théorique.