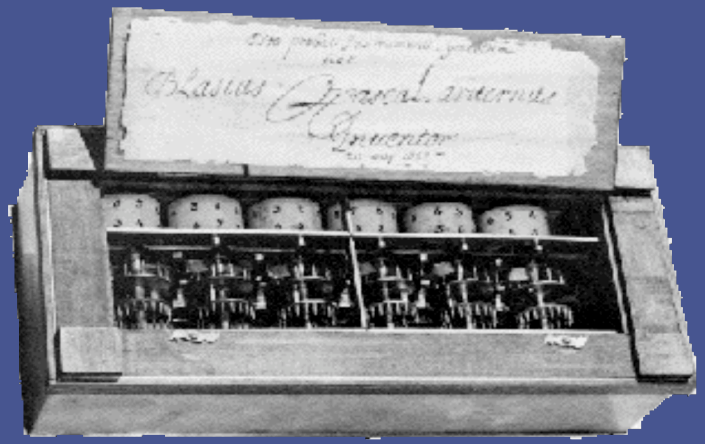
Informatique et physique à la recherche de l'ordinateur quantique

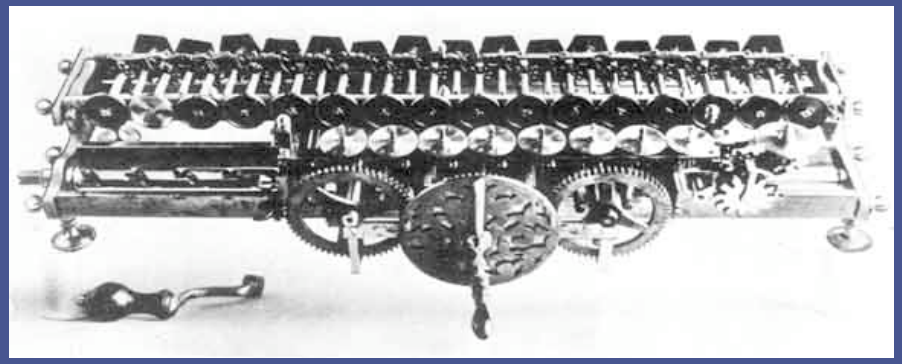
Philippe Jorrand
CNRS
Laboratoire d'Informatique de Grenoble

Philippe.Jorrand@imag.fr
http://capp.imag.fr/

L'information et son traitement peuvent *être* mécaniques



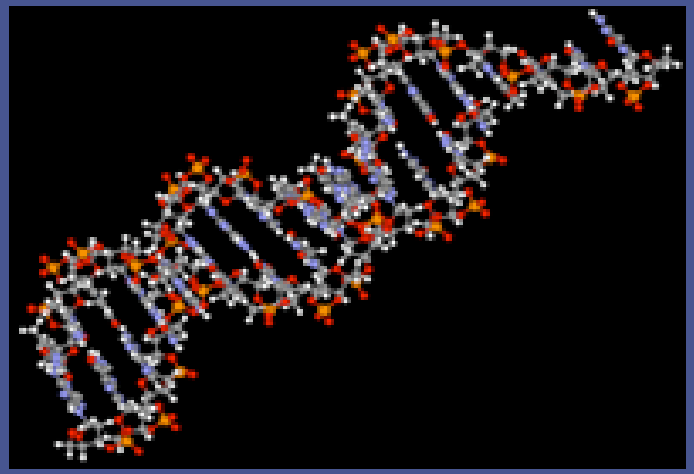
Pascal
1642

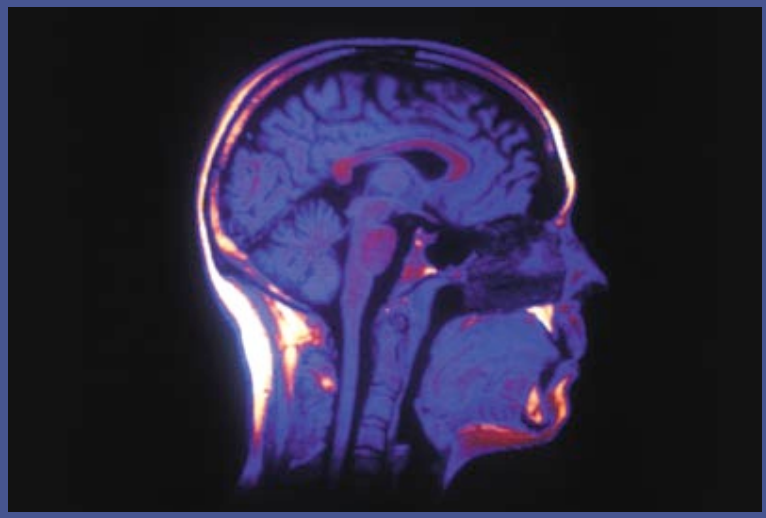


Leibniz
1673

L'information et son traitement peuvent *être* électro-chimico-bio-moléculaires

Depuis des millions d'années...



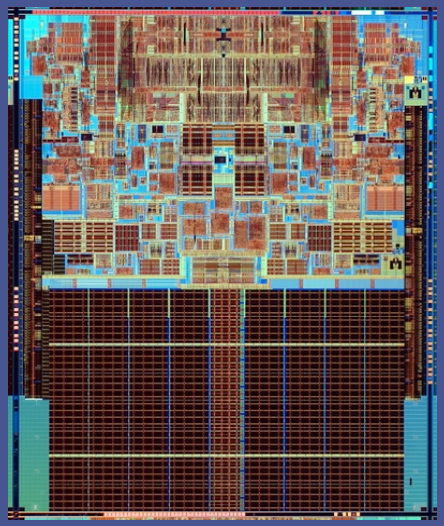


L'information et son traitement peuvent *être* électroniques

Depuis quelques dizaines d'années...

Intel
2006

65 nm
2.66 GHz
4 MB cache
64 bits

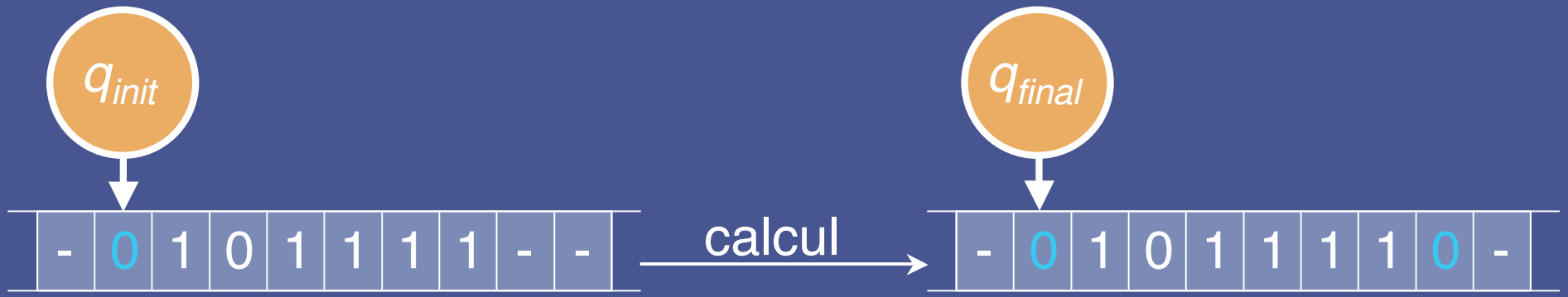


L'information *est* physique

- Il n'y a d'information qu'inscrite sous la forme d'états d'un système physique.
- Il n'y a de traitement et de communication de l'information que par transformation de l'état d'un système physique.
- *L'information et son traitement sont soumis aux lois de la physique, et à nulle autre loi.*
- Dans les ordinateurs du commerce, l'information et son traitement *sont* évidemment physiques.
- Plus fondamentalement, le fait que l'information *soit* physique détermine les principes de base des modèles les plus abstraits de ce qu'est un calcul, comme la machine de Turing.

Soumis aux lois de la physique...
... mais de quelle physique ?

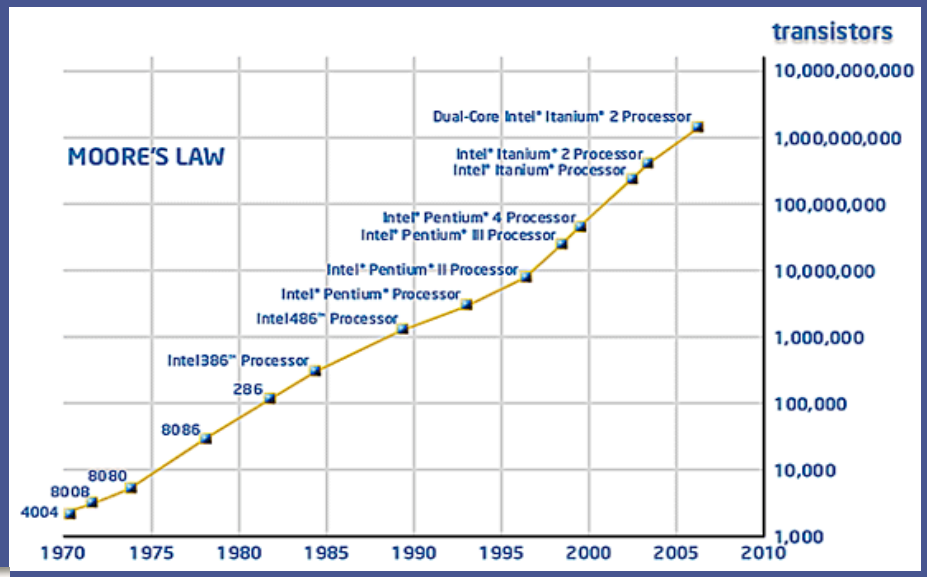
- La machine abstraite imaginée par Turing en 1936 est le modèle le plus général du traitement de l'information.



- "Lire le bit de gauche, le copier à droite, revenir à gauche, stop"
- Les lois de la physique classique permettent l'opération de copie.
- Les lois de la physique quantique interdisent l'opération de copie.
- Les lois du calcul définies par Turing sont elles-mêmes soumises aux lois de la physique classique, celle de Newton et de Maxwell.

Quelle quantité de matière pour l'information et son traitement ?

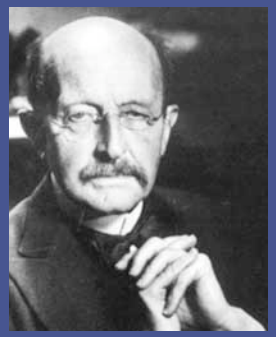
Moore, 1965



Dans quinze ou vingt ans,
quelques particules pour un bit.

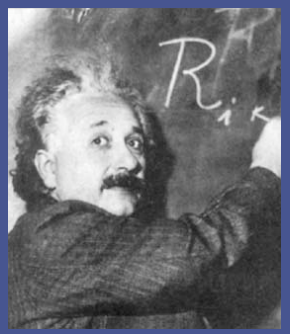
Rencontre de deux grands courants scientifiques du XX^{ème} siècle

Physique quantique, 1900



Max Planck

Albert Einstein

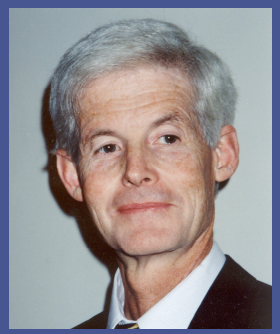


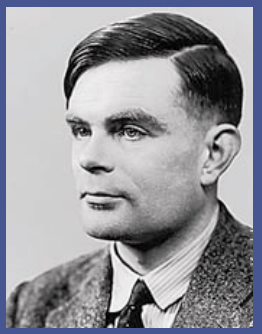
John Von Neumann

Sciences de l'information, 1936

Alan Turing

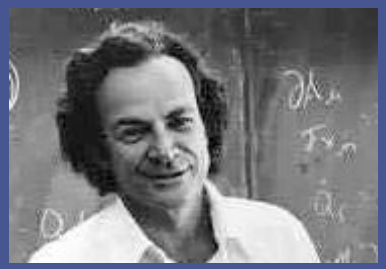
Stephen Cook





Information quantique, 1982

Richard Feynman



David Deutsch

Charles Bennett

Peter Shor

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 fournira la même information pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A peut être recopié sur un autre système physique B.

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

Physique quantique

A chaque instant, un système physique peut être dans un état parmi un ensemble d'états de base possibles. Mais il est en général dans plusieurs états de base à la fois.

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

L'observation d'un système physique dans l'état S modifie S de façon irréversible. Elle est probabiliste : elle pourra fournir des informations différentes pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A ne peut pas, en général, être recopié sur un autre système physique B.

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

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 fournira la même information pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A peut être recopié sur un autre système physique B.

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

Physique quantique

A chaque instant, un système physique peut être dans un état parmi un ensemble d'états de base possibles. Mais il est en général dans plusieurs états de base à la fois.

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

L'observation d'un système physique dans l'état S modifie S de façon irréversible. Elle est probabiliste : elle pourra fournir des informations différentes pour des systèmes identiques tous dans le même état S.

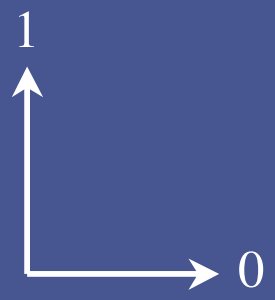
L'état d'un système physique A ne peut pas, en général, être recopié sur un autre système physique B.

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

Bit classique

A chaque instant, un bit classique peut être :

- soit dans l'état 0,
- soit dans l'état 1,
- et un seul de ces deux états à la fois :

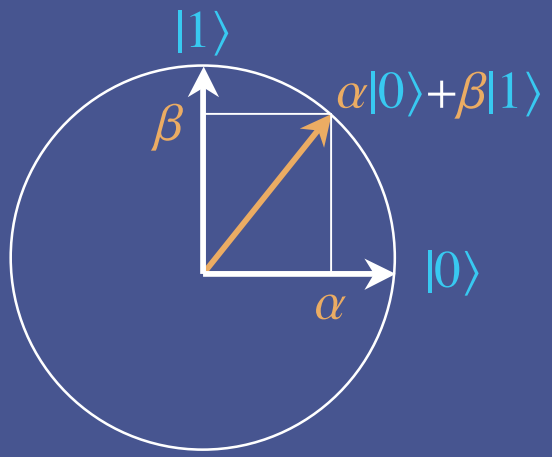


L'ensemble des états possibles pour un bit classique est $\{0,1\}$.

Bit quantique

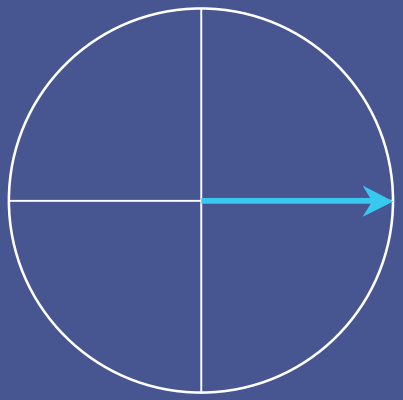
A chaque instant, un bit quantique (qubit) peut être :

- soit dans l'état de base $|0\rangle$,
- soit dans l'état de base $|1\rangle$,
- mais il est en général à la fois dans l'état $|0\rangle$ et dans l'état $|1\rangle$:

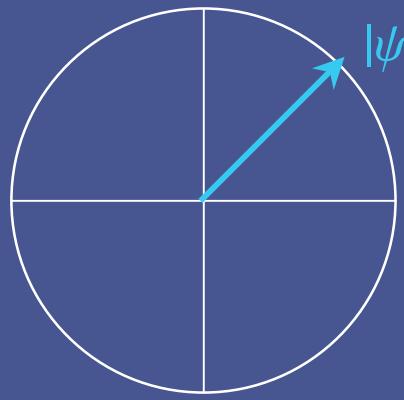


L'ensemble des états possibles pour un qubit sont les vecteurs $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, où $\alpha^2+\beta^2=1$ (c.à.d. les rayons du cercle unité dans l'espace à 2 dimensions).

Exemples d'états d'un qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$

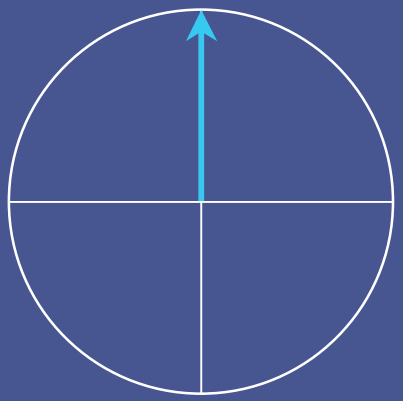


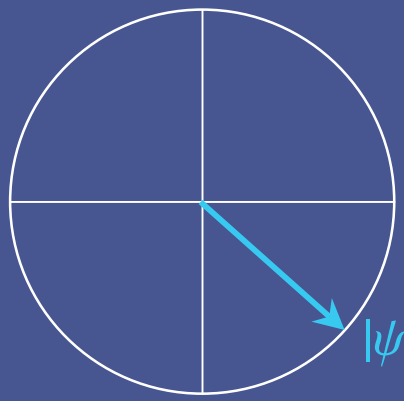
$|\psi\rangle = |0\rangle$



$|\psi\rangle = 1/\sqrt{2}\,|0\rangle + 1/\sqrt{2}\,|1\rangle$

$|\psi\rangle = |1\rangle$





$|\psi\rangle = 1/\sqrt{2}\,|0\rangle - 1/\sqrt{2}\,|1\rangle$

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 fournira la même information pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A peut être recopié sur un autre système physique B.

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

Physique quantique

A chaque instant, un système physique peut être dans un état parmi un ensemble d'états de base possibles. Mais il est en général dans plusieurs états de base à la fois.

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

L'observation d'un système physique dans l'état S modifie S de façon irréversible. Elle est probabiliste : elle pourra fournir des informations différentes pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A ne peut pas, en général, être recopié sur un autre système physique B.

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

Calculer = transformer l'état

Calculer avec un bit

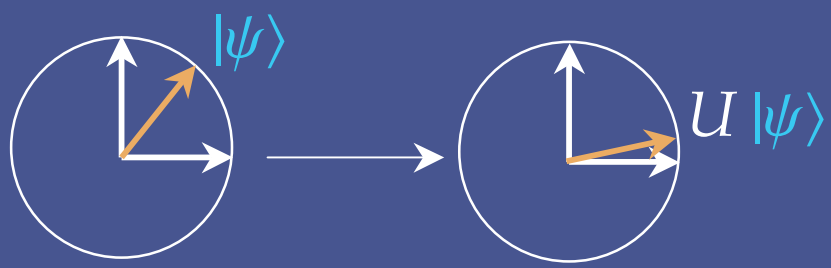
$$\{0,1\} \longrightarrow \{0,1\}$$

Avec plusieurs bits :

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

- fonctions booléennes arbitraires
- en général non réversibles

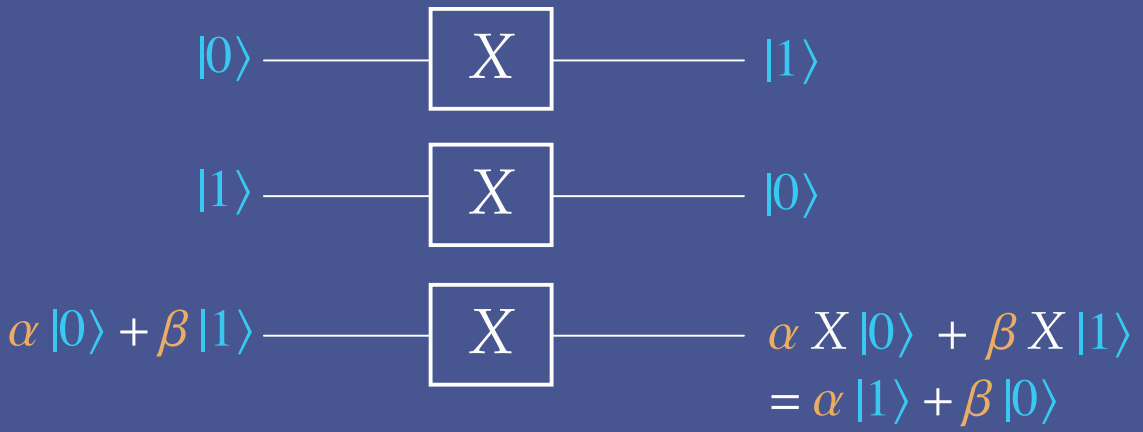
Calculer avec un qubit



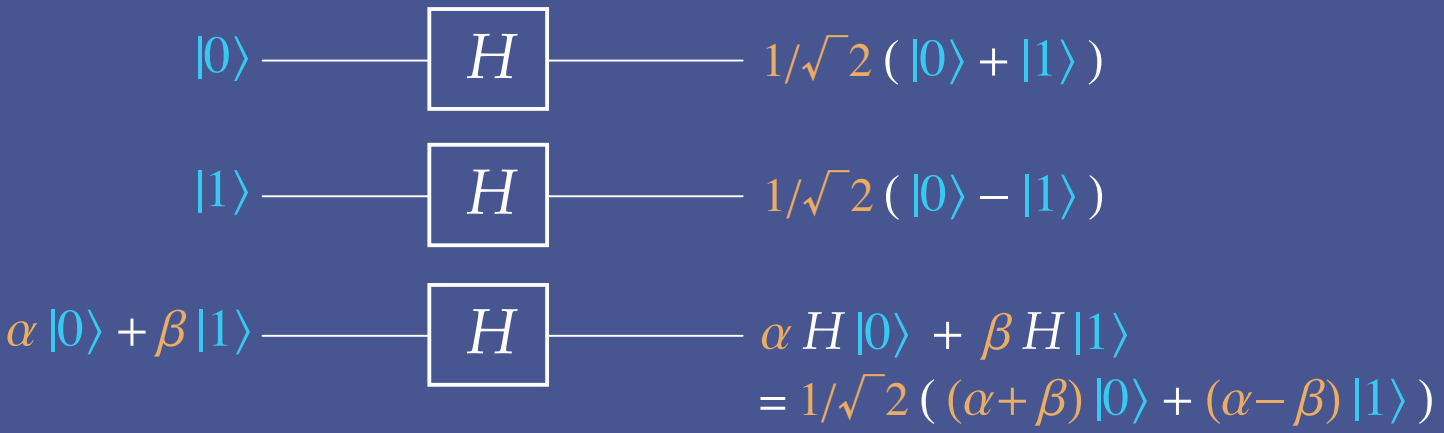
- U est un opérateur linéaire $\Longrightarrow$ déterministe
- U est unitaire $\Longrightarrow$ réversible

Exemples d'opérations sur un qubit

Opérateur X de Pauli :



Opérateur H de Hadamard :



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 fournira la même information pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A peut être recopié sur un autre système physique B.

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

Physique quantique

A chaque instant, un système physique peut être dans un état parmi un ensemble d'états de base possibles. Mais il est en général dans plusieurs états de base à la fois.

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

L'observation d'un système physique dans l'état S modifie S de façon irréversible. Elle est probabiliste : elle pourra fournir des informations différentes pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A ne peut pas, en général, être recopié sur un autre système physique B.

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

Obtenir un résultat = observer l'état

Lire un bit

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

Mesurer un qubit

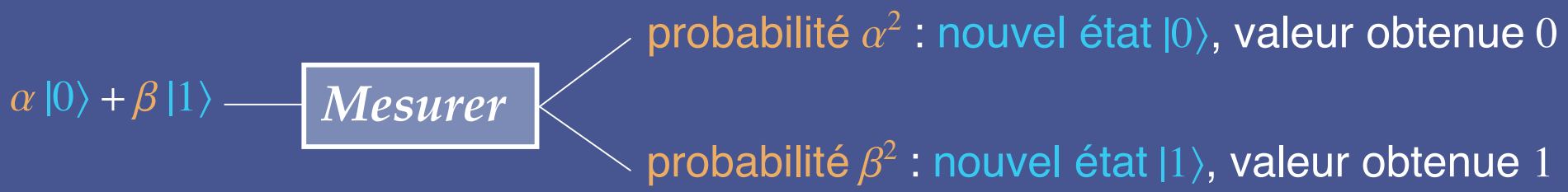
Mesurer un qubit qui est dans l'état $|0\rangle$ donne la valeur 0 et le qubit reste dans l'état $|0\rangle$. Idem pour $|1\rangle$.

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

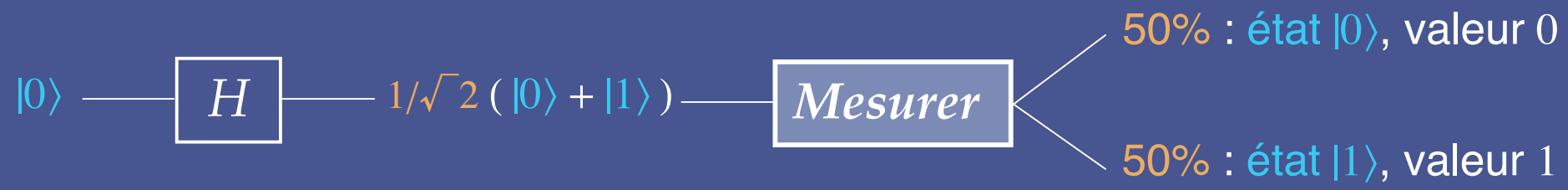
- soit la valeur 0, avec probabilité α^2, et l'état du qubit devient $|0\rangle$,
- soit la valeur 1, avec probabilité β^2, et l'état du qubit devient $|1\rangle$.

α et β : amplitudes de probabilité

Mesure d'un qubit, cas général :

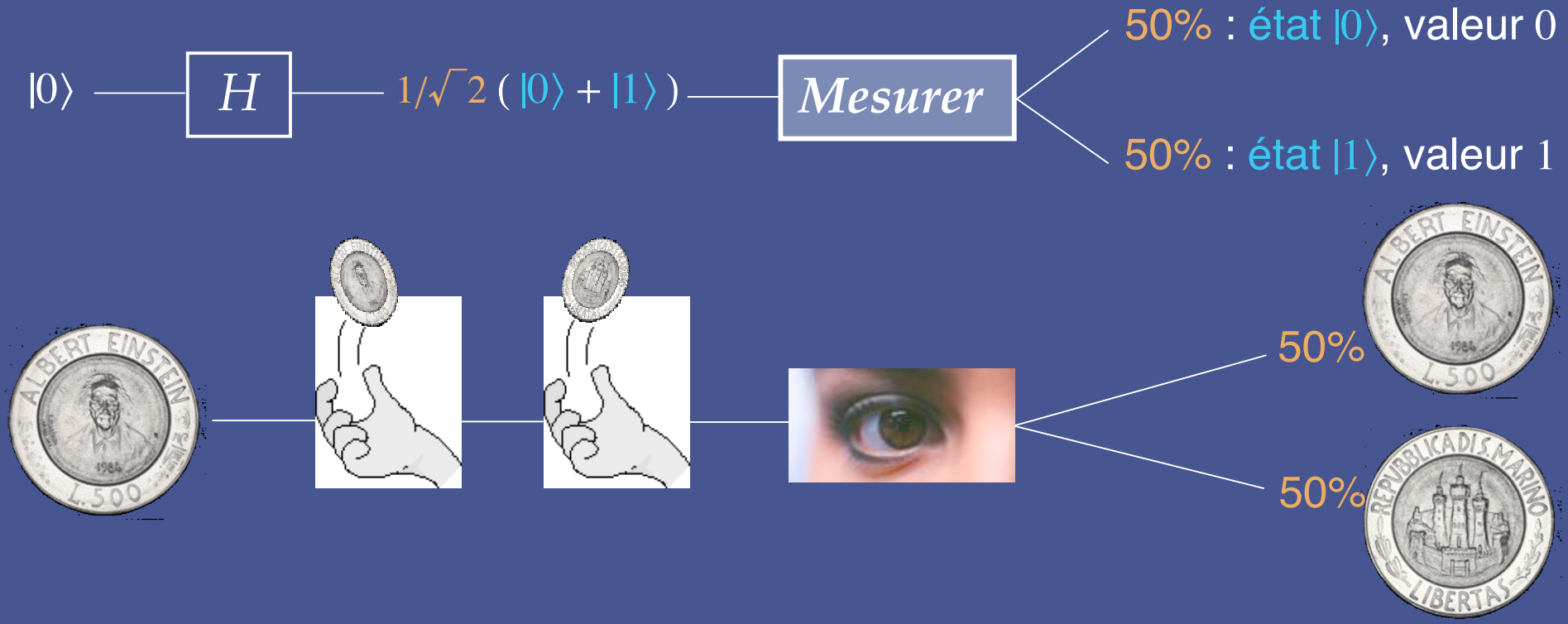


Exemple :



Pile ou face quantique, avec un "vrai" hasard produit par la nature.

Pile ou face ? Pas vraiment...



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 fournira la même information pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A peut être recopié sur un autre système physique B.

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

Physique quantique

A chaque instant, un système physique peut être dans un état parmi un ensemble d'états de base possibles. Mais il est en général dans plusieurs états de base à la fois.

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

L'observation d'un système physique dans l'état S modifie S de façon irréversible. Elle est probabiliste : elle pourra fournir des informations différentes pour des systèmes identiques tous dans le même état S.

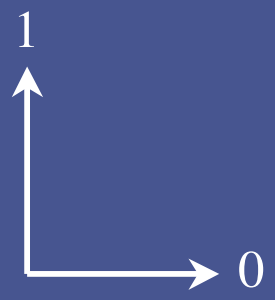
L'état d'un système physique A ne peut pas, en général, être recopié sur un autre système physique B.

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

Bit classique

A chaque instant, un bit classique peut être :

- soit dans l'état 0,
- soit dans l'état 1,
- et un seul de ces deux états à la fois :

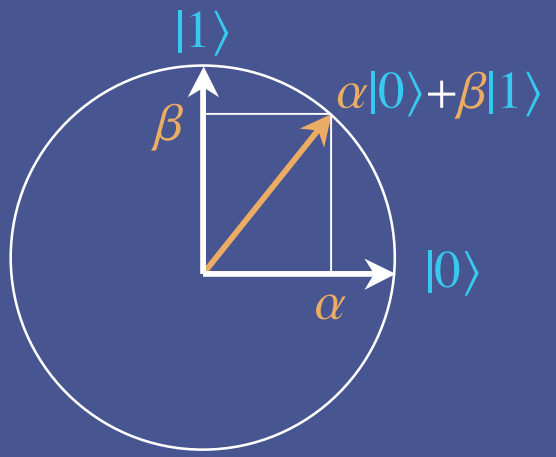


L'ensemble des états possibles pour un bit classique est $\{0,1\}$.

Bit quantique

A chaque instant, un bit quantique (qubit) peut être :

- soit dans l'état de base $|0\rangle$,
- soit dans l'état de base $|1\rangle$,
- mais il est en général à la fois dans l'état $|0\rangle$ et dans l'état $|1\rangle$:



L'ensemble des états possibles pour un qubit sont les vecteurs $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, où $\alpha^2+\beta^2=1$ (c.à.d. les rayons du cercle unité dans l'espace à 2 dimensions).

Système de 2 bits

A chaque instant, un système de 2 bits peut être :

- soit dans l'état $00 = 0$,
- soit dans l'état $01 = 1$,
- soit dans l'état $10 = 2$,
- soit dans l'état $11 = 3$,
- et un seul de ces quatre états à la fois.

L'ensemble des états possibles pour un système de 2 bits est $\{0,1,2,3\}$.

Système de 2 qubits

A chaque instant, un système de 2 qubits peut être :

- soit dans l'état de base $|00\rangle = |0\rangle$,
- soit dans l'état de base $|01\rangle = |1\rangle$,
- soit dans l'état de base $|10\rangle = |2\rangle$,
- soit dans l'état de base $|11\rangle = |3\rangle$,
- mais il est en général à la fois dans plusieurs de ces 4 états de base, voire tous à la fois.

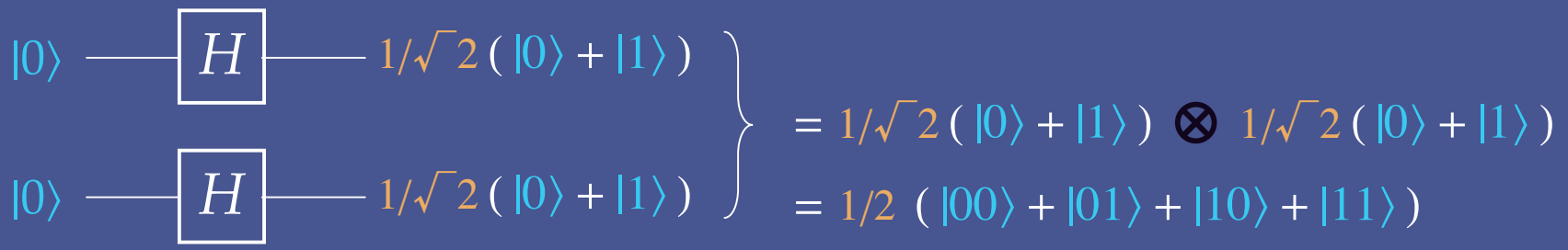
L'ensemble des états possibles pour un système de 2 qubits sont les vecteurs $|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$, où $\alpha^2+\beta^2+\gamma^2+\delta^2=1$ (c.à.d. les rayons de la sphère unité dans l'espace à 4 dimensions).

Système de 2 qubits : exemples d'états et d'opérations

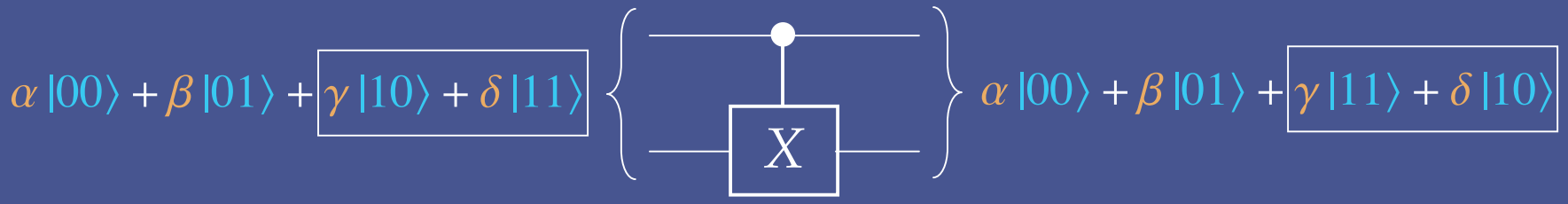
Forme générale de l'état :

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle \quad \text{où} \quad \alpha^2+\beta^2+\gamma^2+\delta^2=1$$

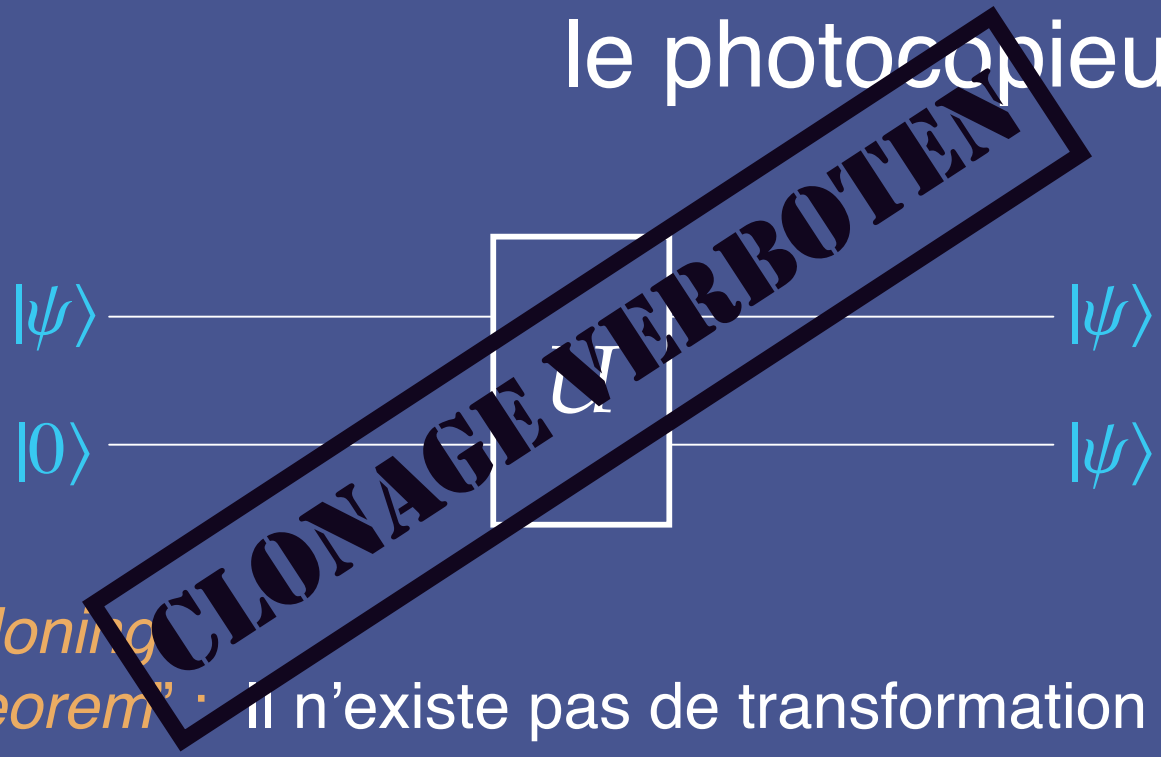
Opérateur de Hadamard sur 2 qubits :



"Controlled Not", opérateur CX:



Une machine impossible : le photocopieur quantique



"*No-cloning theorem*" : Il n'existe pas de transformation linéaire U telle que pour tout état $|\psi\rangle$, $U(\,|\psi\rangle|0\rangle\,) = |\psi\rangle|\psi\rangle$.

Preuve : conséquence directe de la linéarité de la mécanique quantique.

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 fournira la même information pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A peut être recopié sur un autre système physique B.

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

Physique quantique

A chaque instant, un système physique peut être dans un état parmi un ensemble d'états de base possibles. Mais il est en général dans plusieurs états de base à la fois.

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

L'observation d'un système physique dans l'état S modifie S de façon irréversible. Elle est probabiliste : elle pourra fournir des informations différentes pour des systèmes identiques tous dans le même état S.

L'état d'un système physique A ne peut pas, en général, être recopié sur un autre système physique B.

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

En général, $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ est intriqué

- Il existe a, b, c, d ($a = b = c = d = 1/\sqrt{2}$) tels que :

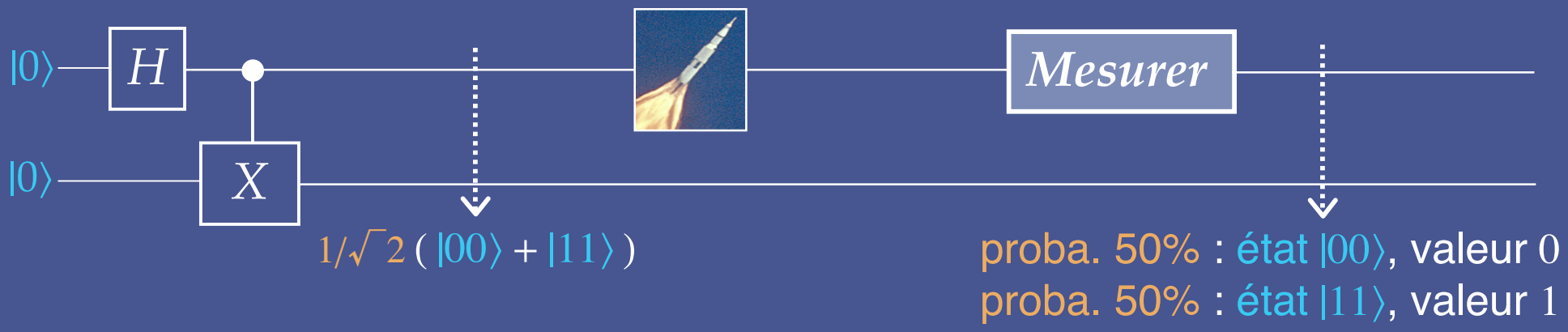
$$1/2\ (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

$$\Rightarrow\ 1/2\ (|00\rangle + |01\rangle + |10\rangle + |11\rangle) \text{ est un état séparable.}$$

- Il n'existe pas a, b, c, d tels que :

$$1/\sqrt{2}\ (|00\rangle + |11\rangle) = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle)$$

$$\Rightarrow\ 1/\sqrt{2}\ (|00\rangle + |11\rangle) \text{ est un état intriqué.}$$



[EPR] Einstein, Podolsky and Rosen, 1935

Can quantum mechanical description of physics reality be considered complete?

Il était une fois ...

… Alice et Bob qui, avant de se séparer, prirent chacun l'un des 2 qubits d'une «paire EPR» dans l'état $1/\sqrt{2}\,(|00\rangle+|11\rangle)$. Puis Bob partit vers une lointaine galaxie secrète.

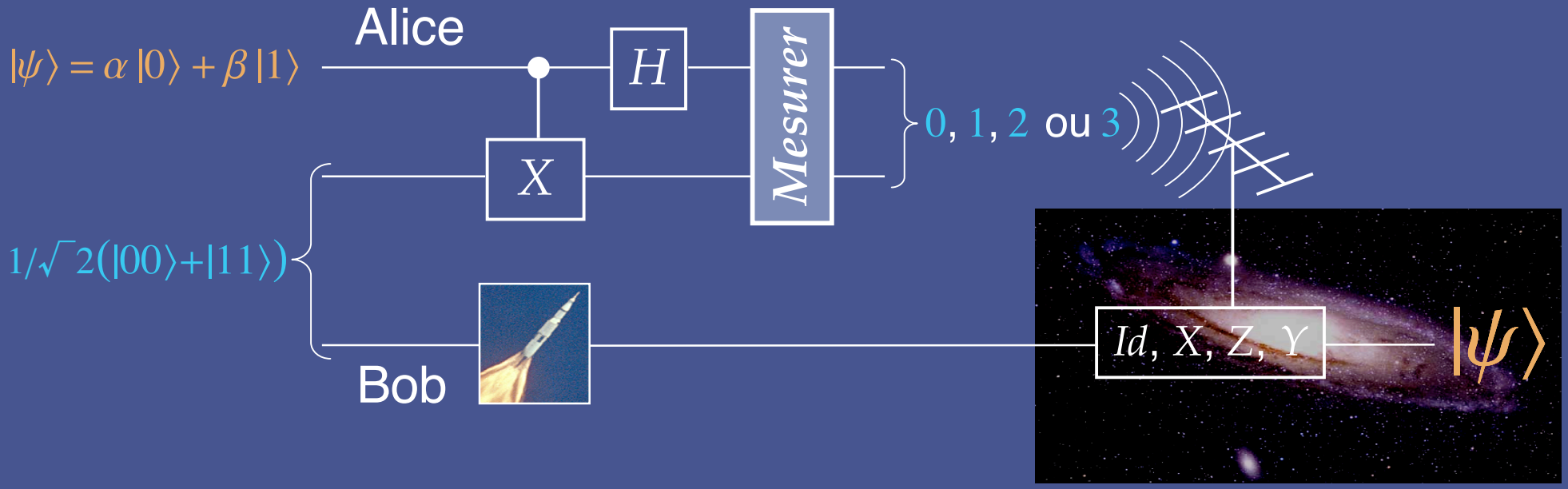
Plus tard ...

… 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.

Or, Alice ne pouvait ...

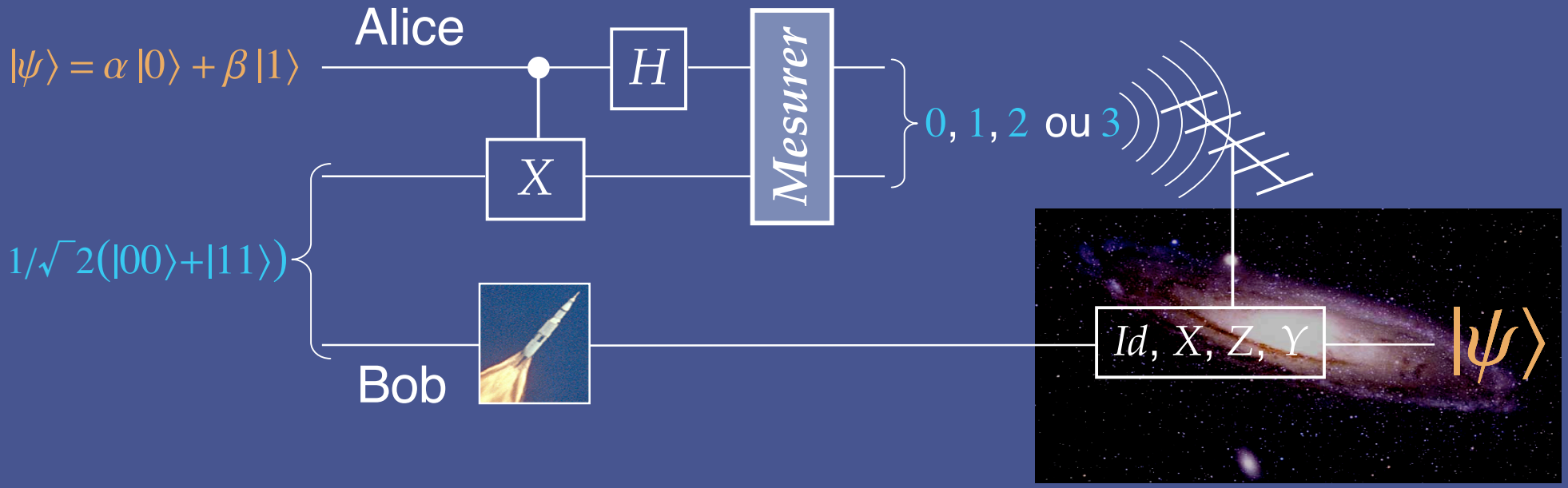
… ni porter ce qubit à Bob,
… ni cloner $|\psi\rangle$ pour en disperser des copies dans l'univers,
… ni connaître α et β pour diffuser leurs valeurs sur les ondes dans l'espace intergalactique.

La solution : Alice téléporte $|\psi\rangle$ à Bob



- Alice applique CX, ce qui a pour conséquence d'intriquer les 3 qubits, puis H.
- Alice mesure ses 2 qubits. Le 0, 1, 2 ou 3 qu'elle obtient lui donne une information sur l'état du qubit de Bob : c'est $\alpha|0\rangle+\beta|1\rangle$, $\alpha|1\rangle+\beta|0\rangle$, $\alpha|0\rangle-\beta|1\rangle$ ou $\alpha|1\rangle-\beta|0\rangle$
- Mais Bob, sur sa galaxie, n'a pas cette information. Alice diffuse le 0, 1, 2 ou 3 obtenu (2 bits classiques suffisent), et Bob obtient à son tour cette information.
- Bob sait lequel de ses 4 opérateurs il doit appliquer : $|\psi\rangle$ est sur la galaxie de Bob !

La solution : Alice téléporte $|\psi\rangle$ à Bob



Charles Bennett
IBM Research Yorktown
1993

Anton Zeilinger
Université de Vienne
1997

Système de 2 bits

A chaque instant, un système de 2 bits peut être :

- soit dans l'état $00 = 0$,
- soit dans l'état $01 = 1$,
- soit dans l'état $10 = 2$,
- soit dans l'état $11 = 3$,
- et un seul de ces quatre états à la fois.

L'ensemble des états possibles pour un système de 2 bits est $\{0,1,2,3\}$.

Système de 2 qubits

A chaque instant, un système de 2 qubits peut être :

- soit dans l'état de base $|00\rangle = |0\rangle$,
- soit dans l'état de base $|01\rangle = |1\rangle$,
- soit dans l'état de base $|10\rangle = |2\rangle$,
- soit dans l'état de base $|11\rangle = |3\rangle$,
- mais il est en général à la fois dans plusieurs de ces 4 états de base, voire tous à la fois.

L'ensemble des états possibles pour un système de 2 qubits sont les vecteurs $|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$, où $\alpha^2+\beta^2+\gamma^2+\delta^2=1$ (c.à.d. les rayons de la sphère unité dans l'espace à 4 dimensions).

Système de n bits

A chaque instant, un système de n bits peut être :

- soit dans l'état $0...000 = 0$,
- soit dans l'état $0...001 = 1$,
- soit dans l'état $0...010 = 2$,

...

- soit dans l'état $1...110 = 2^n - 2$,
- soit dans l'état $1...111 = 2^n - 1$,
- et un seul de ces 2^n états à la fois.

L'ensemble des états possibles pour un système de n bits est $\{0,1,2,...,2^n-1\}$.

Système de n qubits

A chaque instant, un système de n qubits peut être :

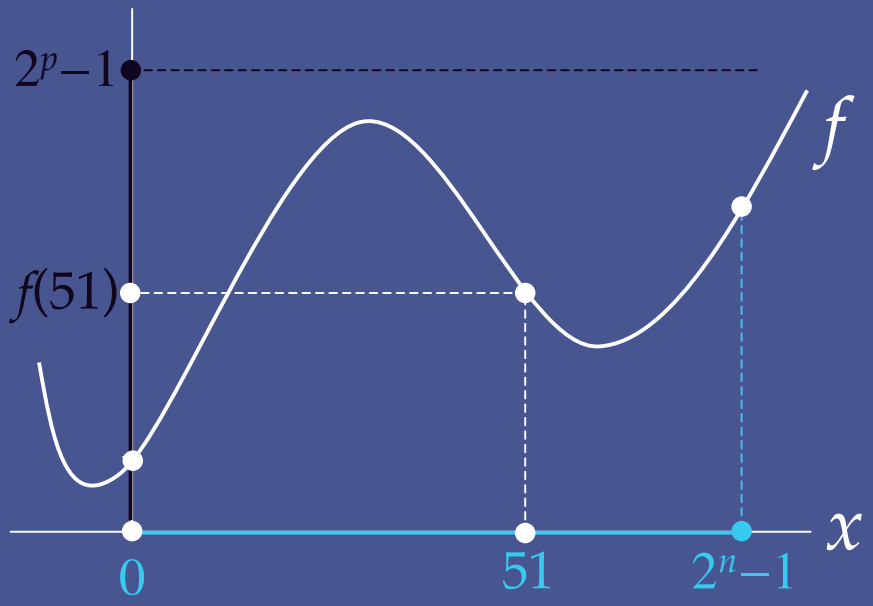
- soit dans l'état $|0...000\rangle = |0\rangle$,
- soit dans l'état $|0...001\rangle = |1\rangle$,
- soit dans l'état $|0...010\rangle = |2\rangle$,

...

- soit dans l'état $|1...110\rangle = |2^n-2\rangle$,
- soit dans l'état $|1...111\rangle = |2^n-1\rangle$,
- mais il est en général à la fois dans plusieurs de ces 2^n états de base, voire tous à la fois.

L'ensemble des états possibles pour un système de n qubits sont les vecteurs $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + ... + \alpha_{2^n-1}|2^n-1\rangle$, où $\alpha_0{}^2 + \alpha_1{}^2 + ... + \alpha_{2^n-1}{}^2 = 1$ (c.à.d. les rayons de la sphère unité dans l'espace à 2^n dimensions).

Calcul quantique : parallélisme massif

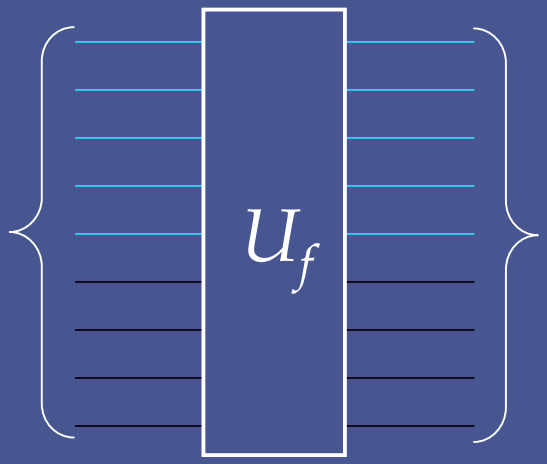


Exemple: calculer toutes les valeurs de $f(x)$, pour x entier variant de 0 à 2^n-1.

Avec le calcul classique:
2^n calculs de la fonction f pour produire les 2^n paires $[x, f(x)]$.

$n+p$ qubits dans l'état :

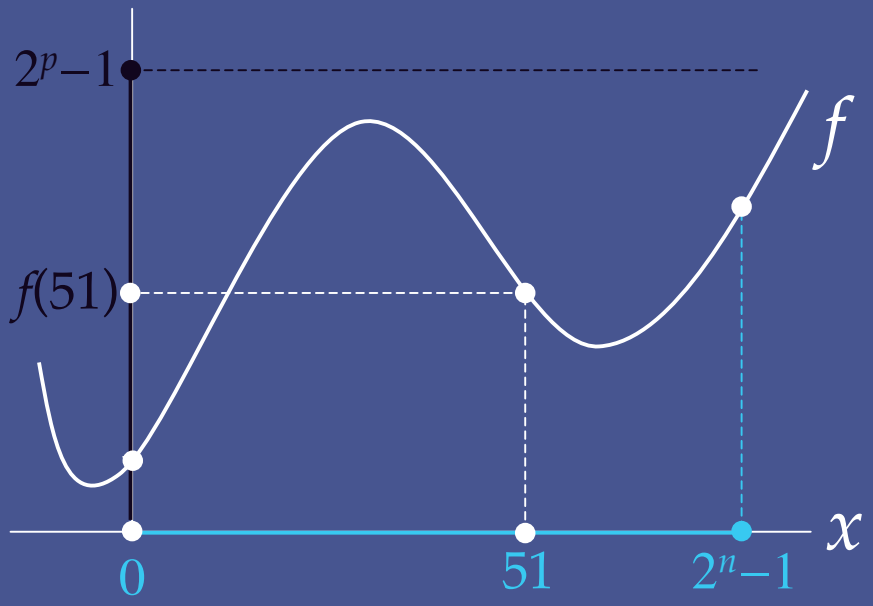
$|51\rangle|0\rangle$



Les mêmes $n+p$ qubits dans l'état :

$|51\rangle|f(51)\rangle$

Calcul quantique : parallélisme massif

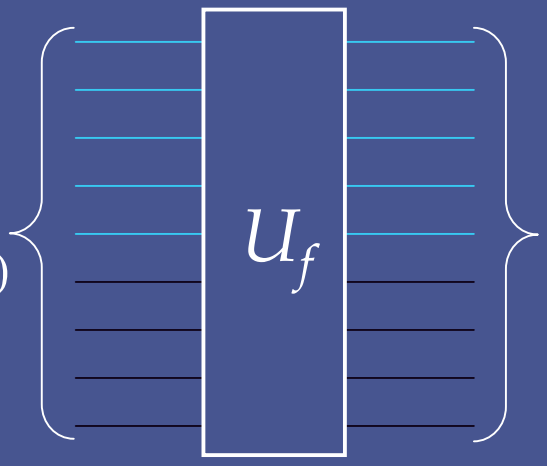


Exemple: calculer toutes les valeurs de $f(x)$, pour x entier variant de 0 à 2^n-1.

Avec le calcul classique:
2^n calculs de la fonction f pour produire les 2^n paires $[x, f(x)]$.

$n+p$ qubits dans l'état :

$$1/\sqrt{2^n}\,(\,|0\rangle|0\rangle + |1\rangle|0\rangle + \ldots + |51\rangle|0\rangle + \ldots + |2^n-1\rangle|0\rangle\,)$$



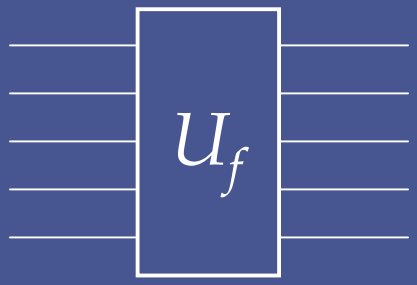
Les mêmes $n+p$ qubits dans l'état :

$$1/\sqrt{2^n}\,(\,|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle + \ldots + |51\rangle|f(51)\rangle + \ldots + |2^n-1\rangle|f(2^n-1)\rangle\,)$$

Avec le calcul quantique :
une seule application de U_f produit les 2^n paires $[x, f(x)]$.

Une machine quantique universelle

Doit permettre de réaliser U_f
pour toute fonction calculable f

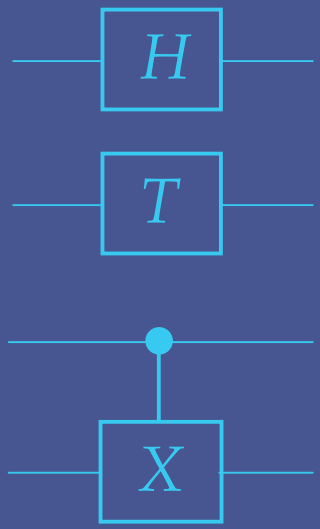


Un jeu de 3 instructions élémentaires est suffisant :

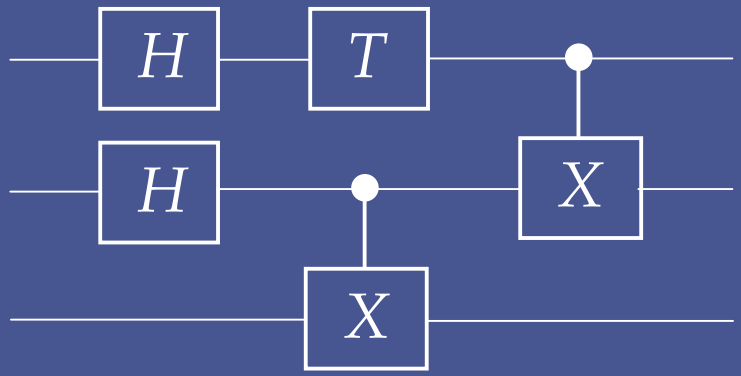
Hadamard :

Phase :

Controlled Not :

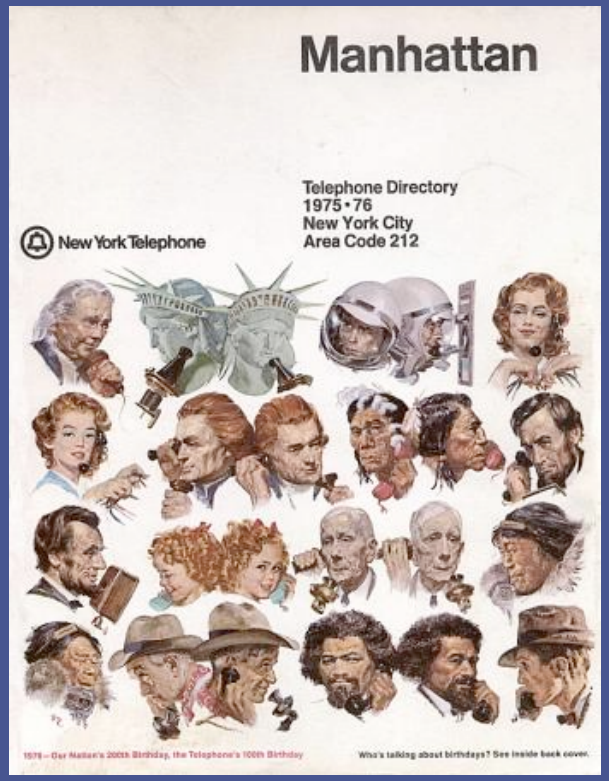


Exemple de circuit quantique :



$(CNot \otimes Id) \bullet (T \otimes CNot) \bullet (H \otimes H \otimes Id)$

Accélération quadratique pour la recherche d'information



- Annuaire téléphonique, avec 1 000 000 d'abonnés en ordre alphabétique de leurs noms :

  $NOM \quad xxxxxxx$

- Etant donné un numéro de téléphone $ddddddd$, trouver l'unique $NOM \quad xxxxxxx$ tel que:

  $xxxxxxx = ddddddd$

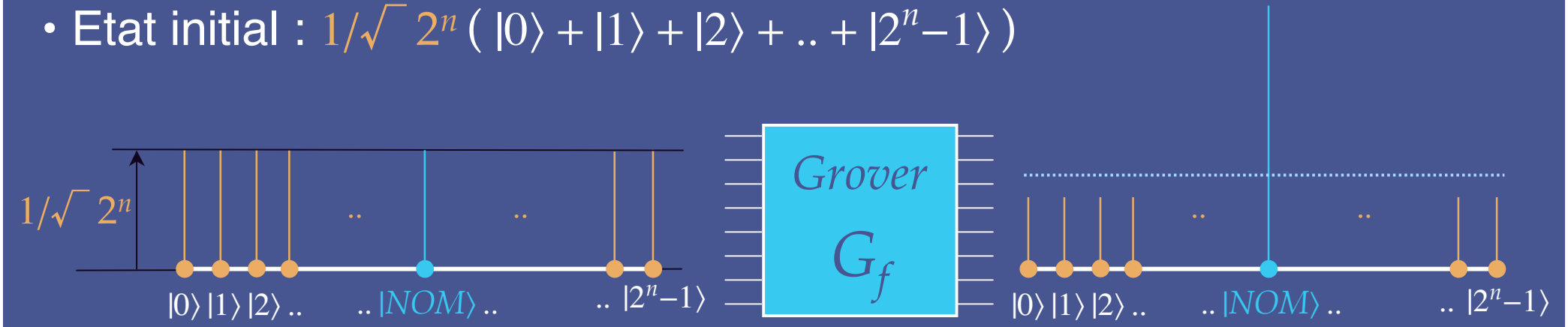
- Avec le calcul classique, jusqu'à 1 000 000 de requêtes à la fonction f, qui dit si oui ou non $xxxxxxx = ddddddd$?

- Avec le calcul quantique, 1 000 requêtes à l'opérateur U_f qui réalise f quantiquement.

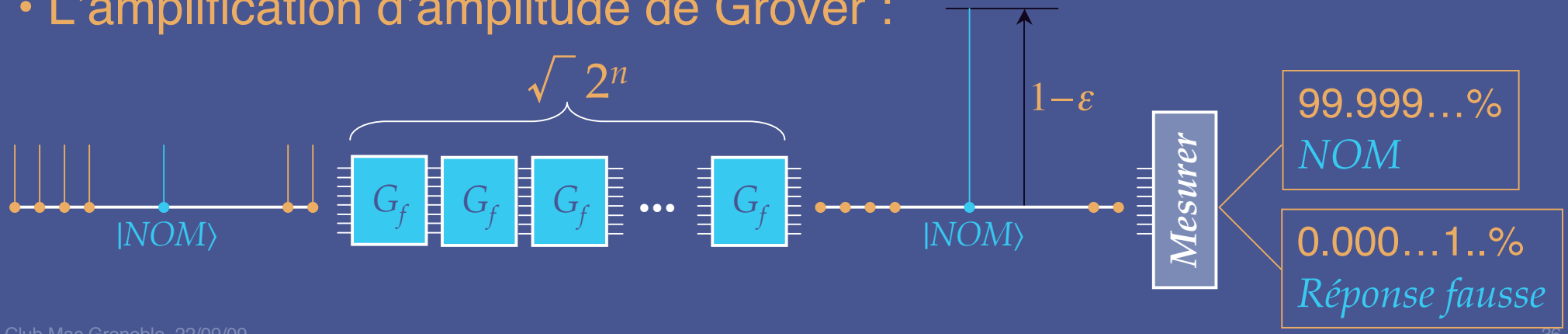
- Algorithme quantique de Grover (1996) : trouver un élément qui satisfait f dans une base non ordonnée de taille N se fait en $\sqrt{N}$ requêtes à f.

Recherche quantique de "*NOM ddddddd*"

- Requête classique: $f(nom) = 1$ ssi *ddddddd* est le numéro de *nom*.
- 2^n noms : n qubits pour coder les 2^n noms qui sont dans l'annuaire.
- Etat initial : $1/\sqrt{2^n}\,(\,|0\rangle + |1\rangle + |2\rangle + .. + |2^n-1\rangle\,)$



- L'amplification d'amplitude de Grover :



Accélération exponentielle pour d'autres problèmes

RSA-200 is factored!

May 10, 2005

RSA Laboratories congratulate the team of F. Bahr, M. Boehm, J. Franke, and T. Kleinjung, University of Bonn and CWI Amsterdam, for the successful factorization of RSA-200, another one of the numbers from the original RSA Factoring Challenge. At 663 bits, RSA-200 is the largest RSA Challenge Number factored to date.

The sieving effort is estimated to have taken the equivalent of 55 years on a single 2.2 GHz Opteron CPU. The matrix step reportedly took about 3 months on a cluster of 80 2.2 GHz Opterons. The sieving began in late 2003 and the matrix step was completed in May 2005.

RSA-200 = 79978339112213278708294676387226016210704467869542853756000992932612840010760934567105295536085661822351910951365788637105954482006576775098580576135790987349501441788631789462951872378692218239 83

Factor p = 353246193440277012127260497819846436867119740019762503649303468776121253679423200058547956528088349

Factor q = 792586995447833303334708584148005968773797585736429960734330341455767872818152135381409304740185467

- Le meilleur algorithme classique connu aujourd'hui pour factoriser un entier de p chiffres, exécute un nombre d'opératons qui croît exponentiellement avec p.

La sécurité du système de cryptage à clé publique le plus utilisé (RSA) est fondée sur cet obstacle algorithmique.

- Algorithme quantique de Shor (1994) : seulement p^3 opérations pour factoriser un entier de p chiffres.

Menace sérieuse pour RSA.

La factorisation est un cas particulier d'une classe de problèmes, qui bénéficient tous de cette accélération.

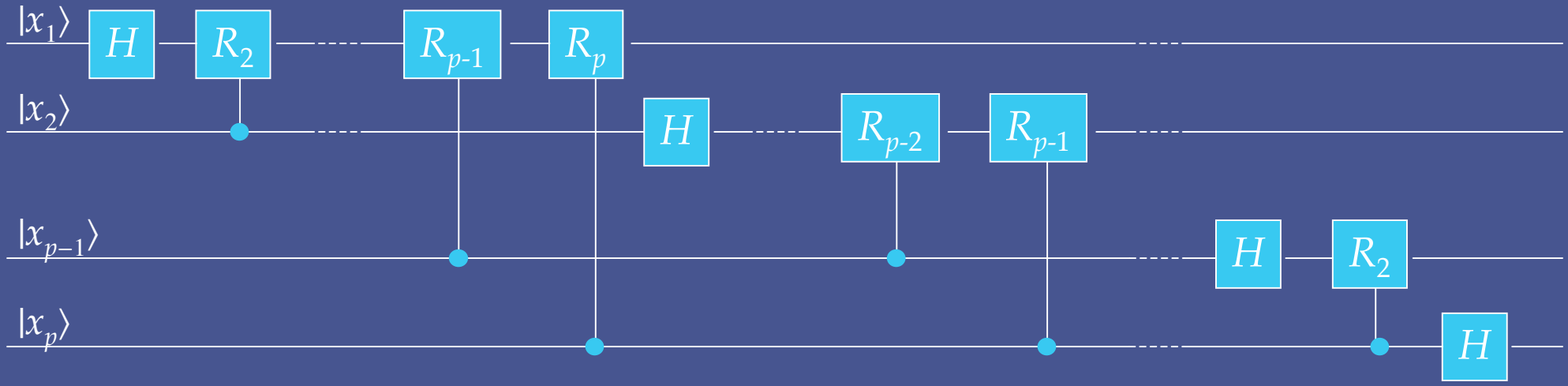
Algorithme de Shor pour factoriser un entier P

1. Choisir au hasard un entier a tel que $1<a<P$
2. Si $PGCD(a,P) = 1$, continuer. Sinon, pb résolu!
3. Trouver la période r de $f_a(k) = a^k \bmod P$.
4. Or, $a^r = 1 \bmod P$ (théorie des groupes). Donc :
   Si r est pair, alors $(a^{r/2}+1)(a^{r/2}-1) = 0 \bmod P$.
   Si r est aussi tel que $a^{r/2} \not\equiv \pm 1 \bmod P$, alors :
   $PGCD(a^{r/2}+1\ ,\ P)$ et/ou
   $PGCD(a^{r/2}-1\ ,\ P)$ sont des facteurs de P : pb résolu !
   Sinon, retourner au pas 1.

QFT: Quantum Fourier Transform

- Calcul classique de la Transformée de Fourier sur p bits :
  - 2^{2p} opérations avec *DFT* (*Discrete Fourier Transform*)
  - $p2^p$ opérations avec *FFT* (*Fast Fourier Transform*)

- Calcul quantique de la transformée de Fourier p qubits :
  - $p(p+1)/2$ opérations avec *QFT*, c.à.d. de l'ordre de p^2



- L'algorithme Shor effectue en moyenne p essais de *QFT* :
  - p^3 opérations pour factoriser un entier de p bits.

L'ordinateur quantique, défi à la physique quantique

- Un problème très difficile : trouver une incarnation physique du qubit, exploitable et assez stable pour effectuer des calculs utiles.

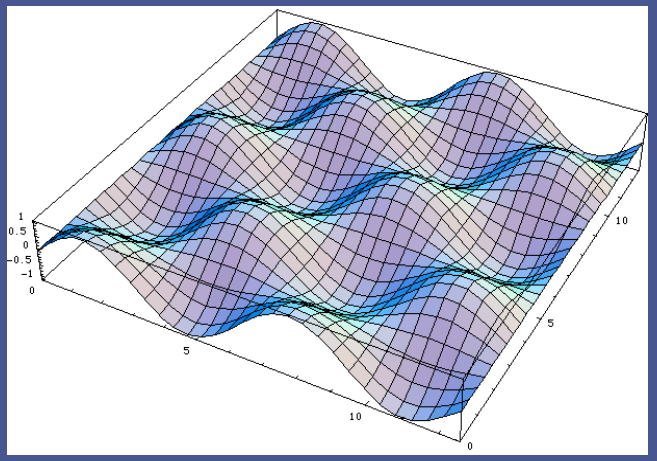
- Les 5 critères de David Di Vincenzo (IBM Research Yorktown) :

  1- Les qubits doivent être initialisables dans un état standard simple.
  2- Il faut pouvoir appliquer aux qubits un jeu universel d'opérateurs.
  3- Il faut pouvoir mesurer les qubits.
  4- La technologie choisie doit passer l'échelle.
  5- Le temps avant décohérence doit être >> au temps d'une opération.

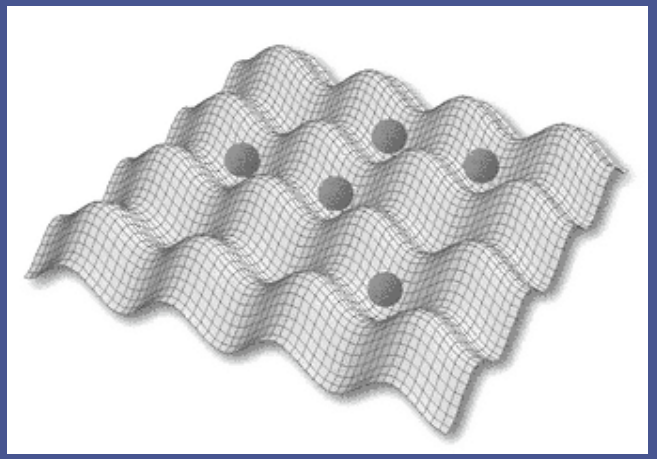
- Beaucoup de technologies candidates, pas encore d'élue.

Qubits = atomes dans un treillis optique

- Treillis optique : onde optique stationnaire créée par une paire de laser de même longueur d'onde, et qui se propagent dans des directions opposées.

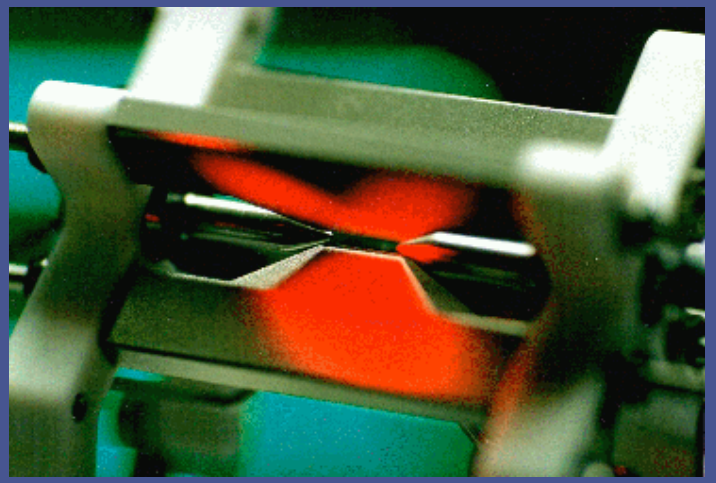


- Des atomes en interaction avec un treillis optique 3D (3 paires de lasers dans les 3 directions de l'espace) sont ralentis et refroidis (10^{-6} K), pour se stabiliser aux sites de potentiel minimum. Un atome = un qubit.

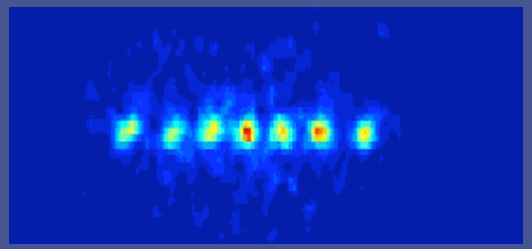


Qubits = ions piégés

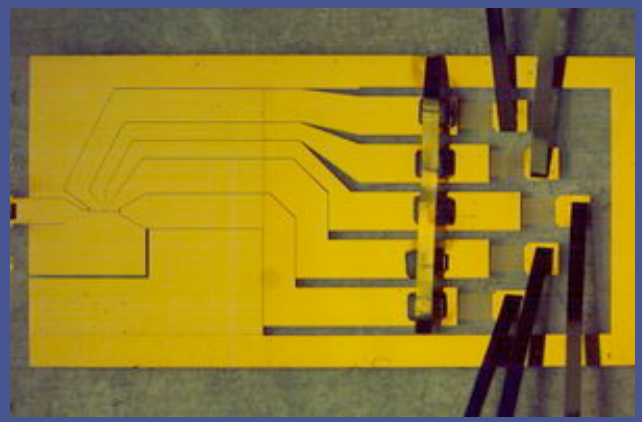
- Ion : particule atomique chargée, atome qui a gagné ou perdu un ou plusieurs électrons.
- Piège de Wolfgang Paul : ions injectés dans un champ électrique quadripolaire, et piègeage dynamique des ions par application d'un potentiel oscillant entre les électrodes.



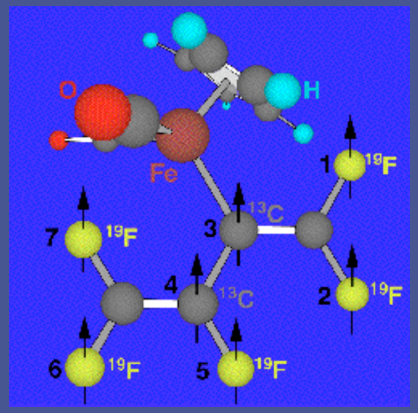
- Longue durée de stockage de plusieurs ions alignés.



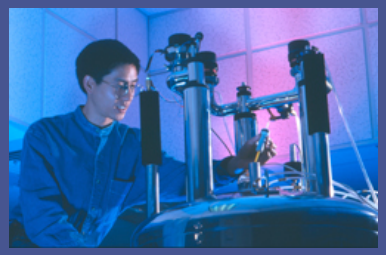
- Réalisation on chip en cours d'expérimentation.



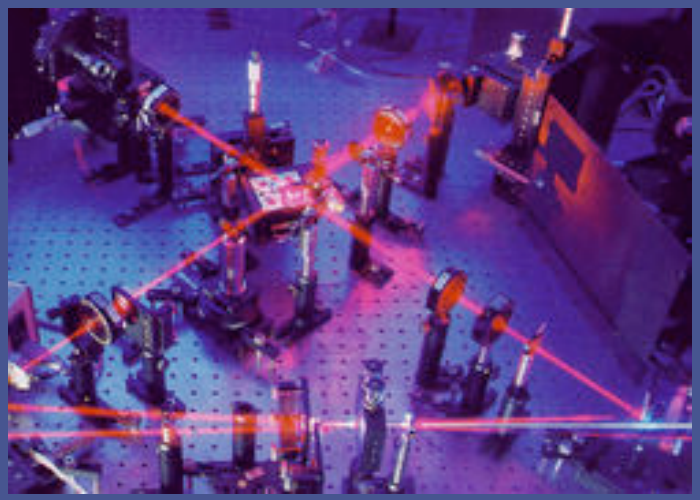
Autres technologies pour les qubits



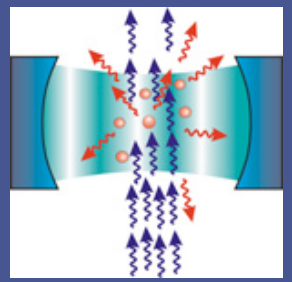
- Résonnance Magnétique Nucléaire (RMN) :
  1 qubit = 1 spin nucléaire dans une molécule.



1er ordinateur quantique, 1998-2002.
Isaac Chuang, IBM Almaden (puis Center for Bits and Atoms, MIT).



- Calcul quantique optique : 1 qubit = 1 photon,
  $|0\rangle$ = polarisation →, $|1\rangle$ = polarisation ↑
- Electrodynamique quantique en cavité :
  (interactions laser-matière) : 1 qubit
  = 1 atome couplé à 1 photon.

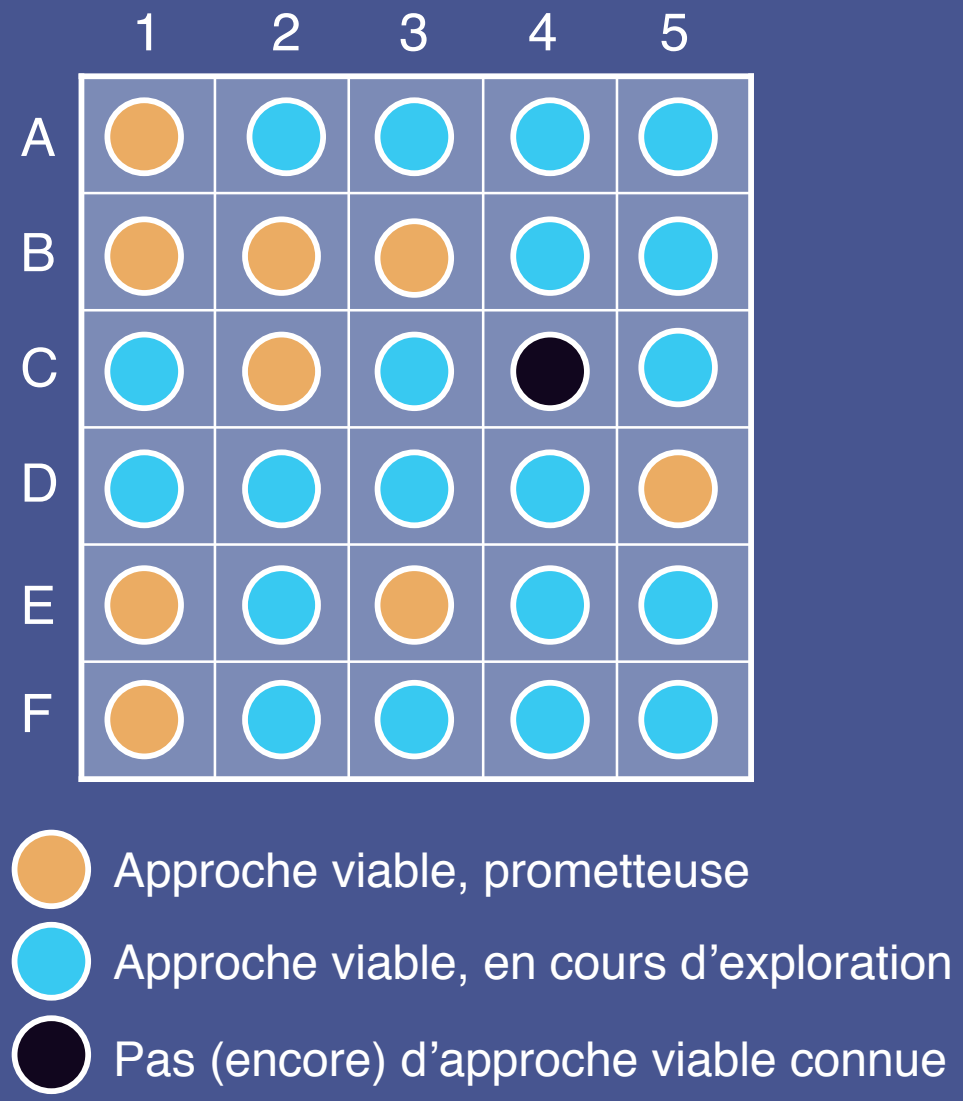


- Nanojonctions supraconductrices
  (jonctions Josephson).
- Etc.

L’ordinateur quantique : c’est possible

- Critères :
  1. Qubits initialisables
  2. Famille universelle d’opérateurs
  3. Qubits mesurables
  4. Technologie qui passe à l’échelle
  5. Temps de décohérence élevé

- Technologies :
  A. Atomes neutres, treillis optiques
  B. Ions piégés
  C. RMN
  D. Optique
  E. Electrodynamique quantique
  F. Nanojonctions supraconductrices



L'ordinateur quantique : c'est pour quand ?

- Objectifs raisonnables pour 2015 :
  - Maintien de cohérence et correction d'erreurs sur 10 qubits.
  - Exécution d'algorithmes quantiques sur 10 qubits.
  - Exécution d'algorithmes distribués sur 2 ou 3 ordinateurs à 10 qubits.
  - Etablissement et maintien d'états intriqués sur 10 qubits.
  - Simulations de systèmes quantiques infaisables classiquement (Feynman).
- Vers 2020 :
  - Réalisation de mémoires quantiques d'au moins une centaine de qubits.
  - Algorithmes sur 50 qubits exécutés de façon fiable, avec correction d'erreurs.
  - Percée scientifique, par simulation, dans un problème clé en sciences.
- Sources :

  US : *A Quantum Information Science and Technology Roadmap*, ARDA, 2004
  http://qist.lanl.gov

  EU : *Quantum Information Sciences and Technologies*, *ERA Pilot Roadmap*, 2007
  http://qist.ect.it/

Information et physique, aventure scientifique du XXI^{ème} siècle...

• "*Information is inevitably physical* !" Quête conjointe du chercheur en informatique et du chercheur en physique quantique : débusquer dans notre connaissance ultime du monde physique, ce qui peut être exploité comme étant de l'information, du calcul et de la communication.

Rolf Landauer 1961

Charles Bennett IBM

Elham Kashefi Edimbourg

Anton Zeilinger Vienne

Samson Abramsky Oxford

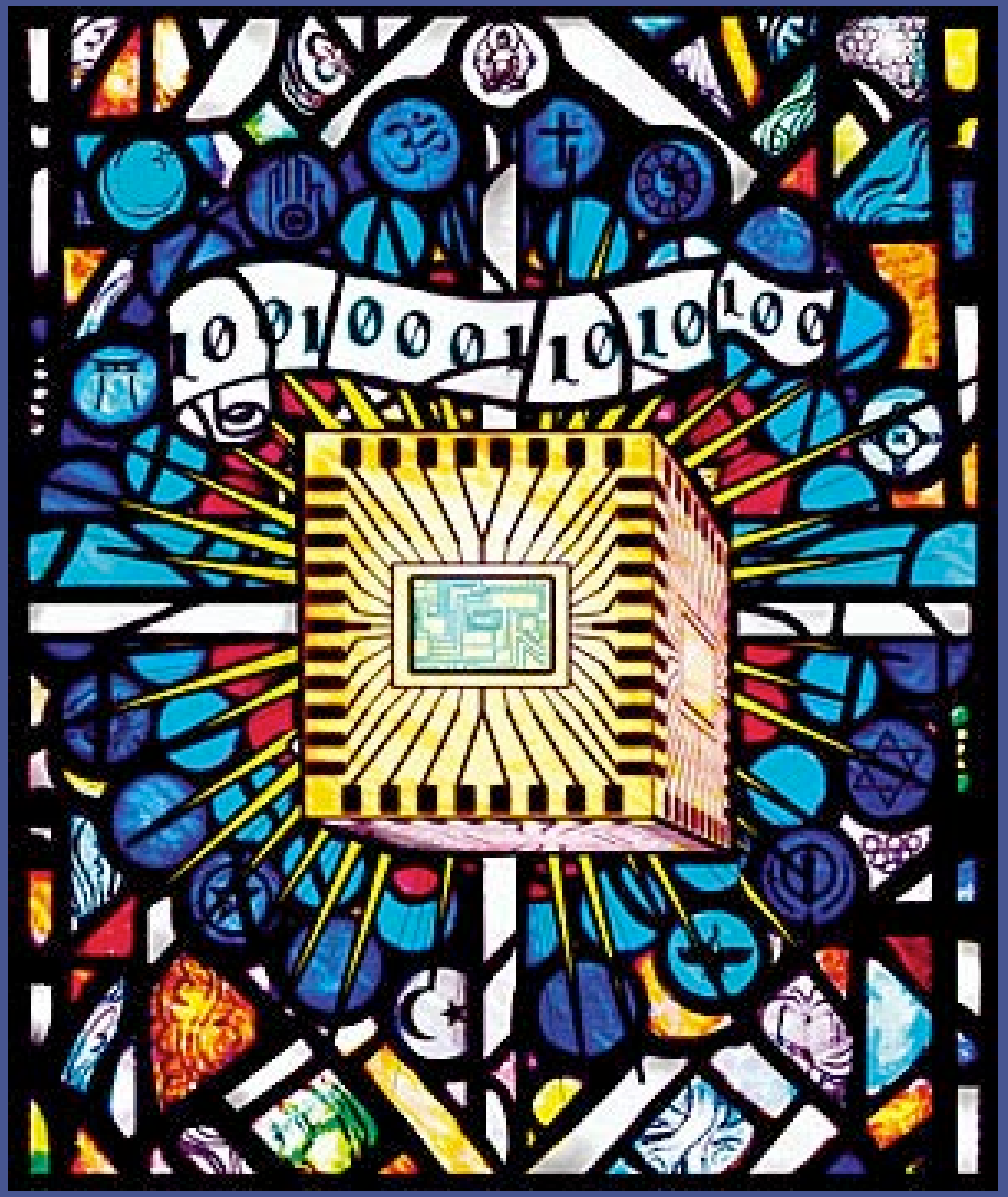
John A. Wheeler 1989

• "*It from bit*" : tout n'est qu'information. Un regard nouveau pour la physique quantique et la théorie de l'information : revisiter les phénomènes formalisés par la la mécanique quantique du XX^{ème} siècle, et les reformuler entièrement en termes d'information et de relations spatio-temporelles sur de l'information.

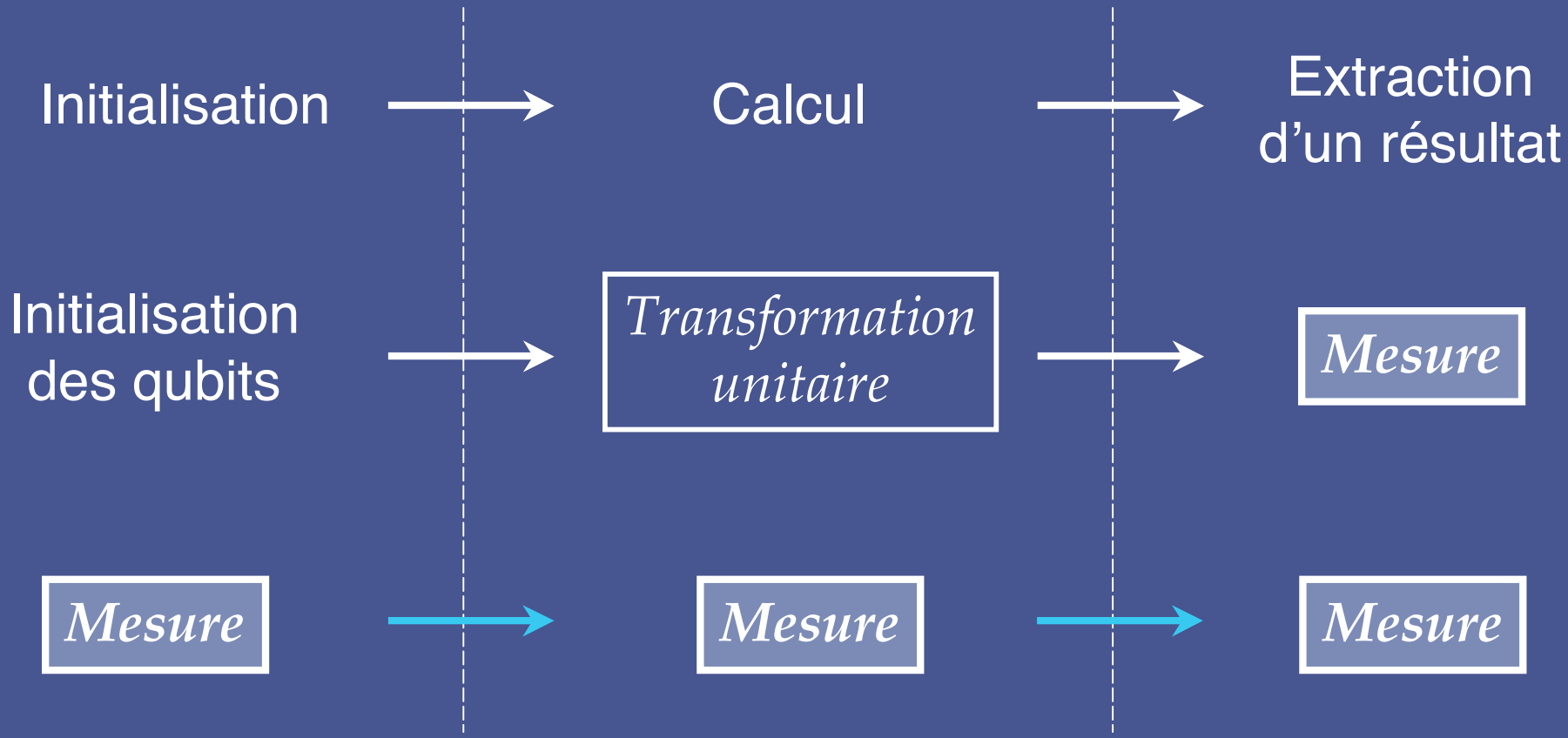
Où le physicien et l'informaticien rejoignent le philosophe : la source ultime de toute "réalité" ne serait-elle qu'information ?

In principio erat Verbum... Omnia per ipsum facta sunt, et sine ipso factum est nihil quod factum est.

Jn 1, 1,3



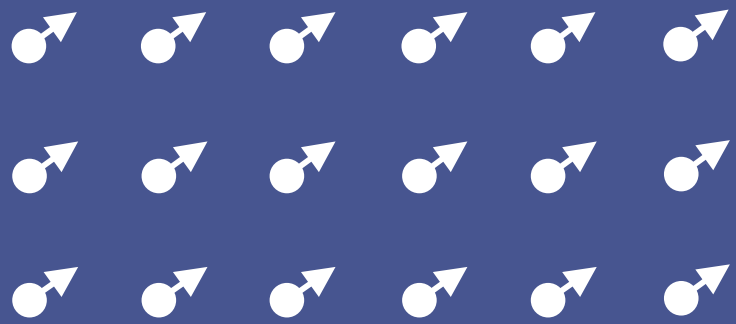
Autre modèle : le calcul quantique fondé sur la mesure



La mesure quantique est probabiliste

=> calcul quantique contrôlé classiquement

Le “*one-way quantum computer*”



- Une grille rectangulaire de qubits.

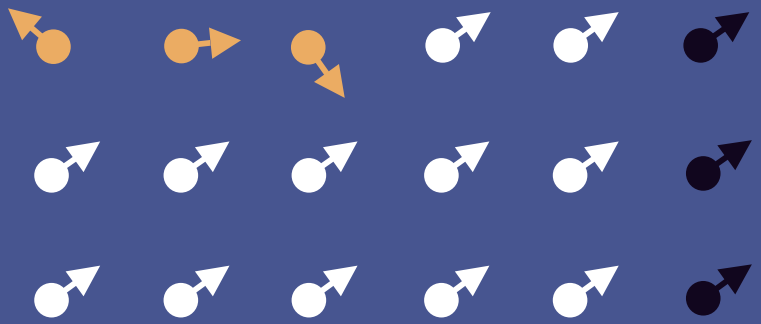
Le “*one-way quantum computer*”

- Une grille rectangulaire de qubits.
- Des qubits d’entrée

Le “*one-way quantum computer*”

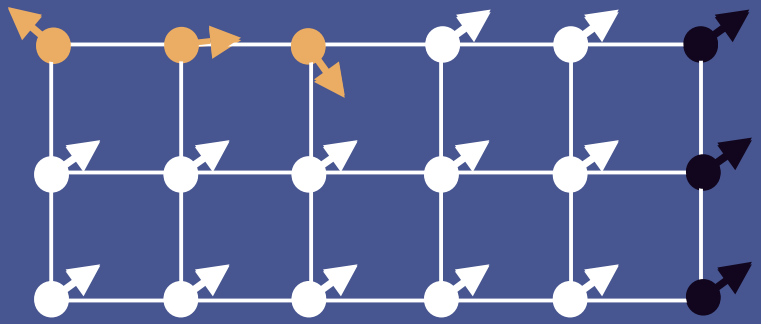
- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie

Le “*one-way quantum computer*”



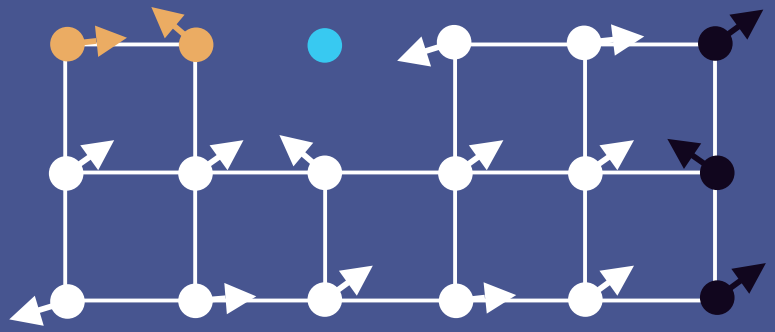
- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.

Le “*one-way quantum computer*”



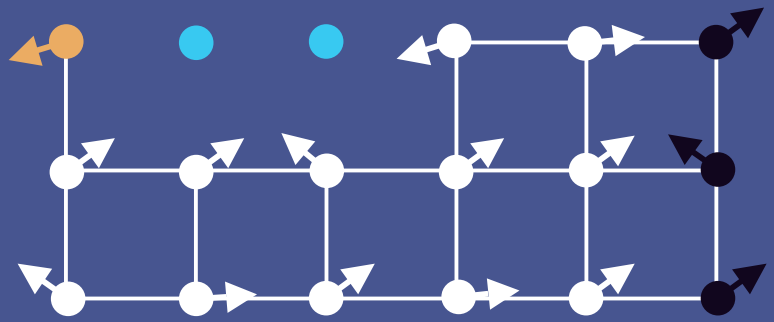
- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.

Le “*one-way quantum computer*”



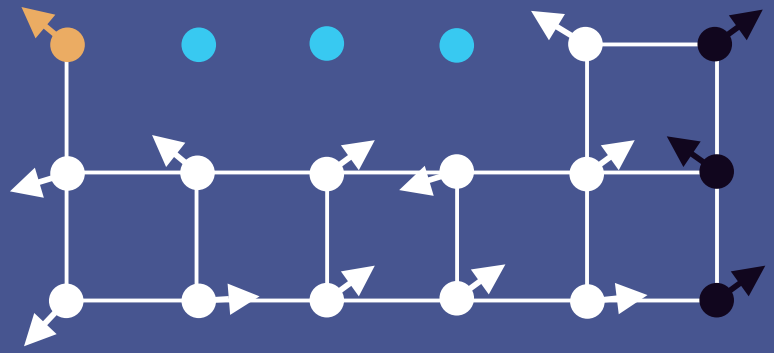
- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.
- Mesurer un qubit :
  - modifie l’état de tout le reste, à cause de l’état intriqué global,
  - sépare ce qubit du reste de l’état intriqué.

Le “*one-way quantum computer*”



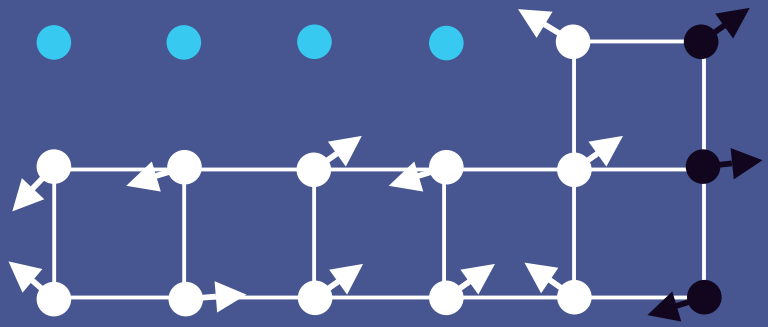
- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.
- Mesurer un qubit :
  - modifie l’état de tout le reste, à cause de l’état intriqué global,
  - sépare ce qubit du reste de l’état intriqué.

Le “*one-way quantum computer*”



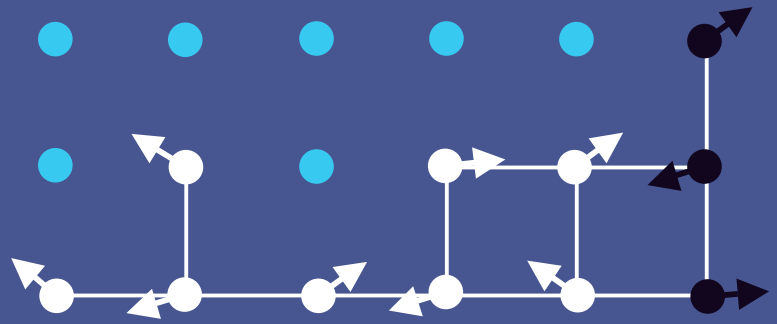
- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.
- Mesurer un qubit :
  - modifie l’état de tout le reste, à cause de l’état intriqué global,
  - sépare ce qubit du reste de l’état intriqué.
- Exécution = séquence de mesures, chaque fois d’un seul qubit.

Le “*one-way quantum computer*”



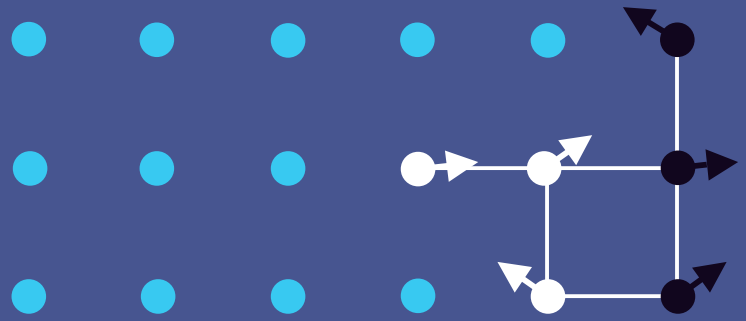
- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.
- Mesurer un qubit :
  - modifie l’état de tout le reste, à cause de l’état intriqué global,
  - sépare ce qubit du reste de l’état intriqué.
- Exécution = séquence de mesures, chaque fois d’un seul qubit.

Le “*one-way quantum computer*”



- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.
- Mesurer un qubit :
  - modifie l’état de tout le reste, à cause de l’état intriqué global,
  - sépare ce qubit du reste de l’état intriqué.
- Exécution = séquence de mesures, chaque fois d’un seul qubit.

Le “*one-way quantum computer*”

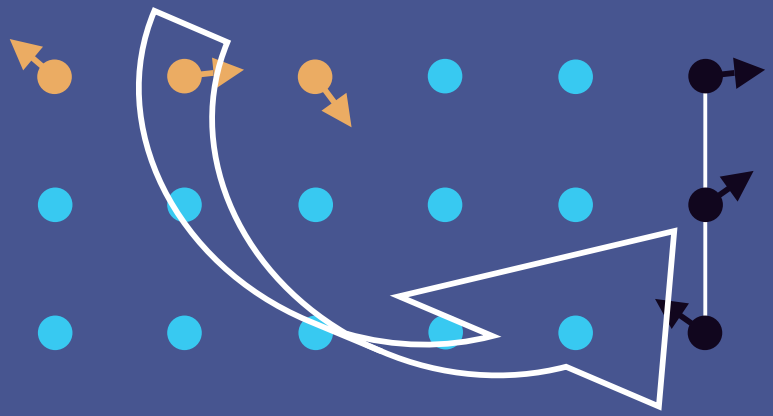


- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.
- Mesurer un qubit :
  - modifie l’état de tout le reste, à cause de l’état intriqué global,
  - sépare ce qubit du reste de l’état intriqué.
- Exécution = séquence de mesures, chaque fois d’un seul qubit.

Le “*one-way quantum computer*”

- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.
- Mesurer un qubit :
  - modifie l’état de tout le reste, à cause de l’état intriqué global,
  - sépare ce qubit du reste de l’état intriqué.
- Exécution = séquence de mesures, chaque fois d’un seul qubit.

Le “*one-way quantum computer*”



- Une grille rectangulaire de qubits.
- Des qubits d’entrée, des qubits de sortie, initialisation des qubits d’entrée.
- Le système constitué par l’ensemble des qubits est mis dans un état intriqué.
- Mesurer un qubit :
  - modifie l’état de tout le reste, à cause de l’état intriqué global,
  - sépare ce qubit du reste de l’état intriqué.
- Exécution = séquence de mesures, chaque fois d’un seul qubit.
- Un calcul a été effectué, au moyen d’une ressource inexistante classiquement : l’état intriqué initial, “détricoté” pas à pas à chaque étape du calcul.

Qu'est-ce qu'un calcul quantique ?

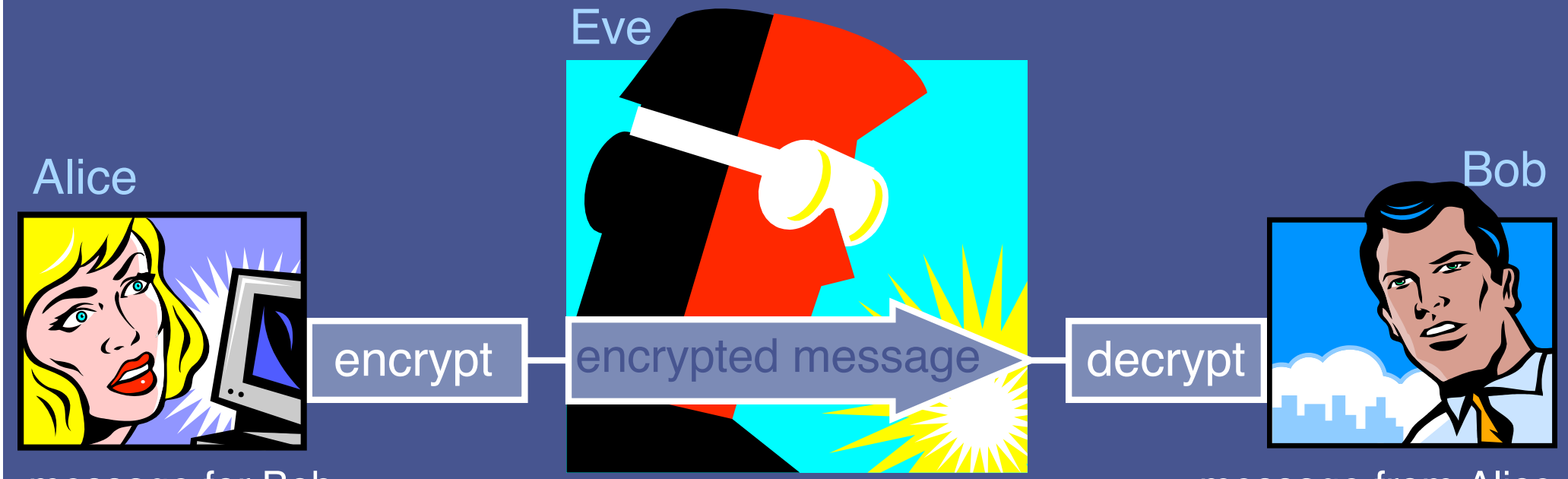
- David Deutsch (1985, Oxford) introduit un principe physique qui définit le calcul de façon abstraite : c'est la simulation d'un système physique fini par un autre système physique qui opère avec des ressources finies (temps et espace).
- Une Machine de Turing Quantique (MTQ), définie selon ce principe, rend compte du calcul quantique par transformations unitaires, et montre que :
  - Sur le plan de la calculabilité, quantique et classique sont équivalents,
  - Sur le plan de la complexité, il existe des MTQ qui ne peuvent pas être simulées en temps polynomial par des Machines de Turing Classiques.
- Une Machine de Turing Quantique contrôlée Classiquement (MTQC, PhJ, S. Perdrix, 2005, Grenoble), rend compte aussi du calcul quantique fondé sur la mesure et a permis de déterminer les ressources minimales pour un ordinateur quantique fondé sur la mesure : jeu d'instructions, nombre de qubits auxiliaires.
- Un modèle fondé sur la théorie des graphes (*graph states*) rend compte du *one-way quantum computer* (H. Briegel et M. Van Den Nest, 2001-2007, Innsbruck, S. Perdrix et M. Mhalla, 2006-2007, Grenoble, E. Kashefi, 2006-2007, Oxford), et permet d'optimiser les calculs par consommation d'intrication.

Physique quantique et informatique théorique

- Algorithmique quantique : amplification d'amplitude, QFT, marches quantiques, et sûrement d'autres techniques algorithmiques, à découvrir.
- Formes du calcul quantique : par opérateurs unitaires, par mesures quantiques, calcul quantique adiabatique, calcul quantique topologique, automates cellulaires quantiques, calcul quantique distribué, et sûrement d'autres façons, encore inconnues, de faire évoluer un système quantique sur des trajectoires interprétables comme des calculs.
- Théories et modèles abstraits : machines de Turing quantiques, lambda-calculs quantiques, langages de programmation quantiques, calcul quantique contrôlé classiquement/quantiquement, algèbres de processus quantiques, analyse de programmes et protocoles quantiques, et d'autres structures fondamentales, à découvrir, pour comprendre le calcul quantique.

Un territoire ouvert, interdisciplinaire, effervescent, à la pointe de la recherche de base

Cryptography



Classical cryptography:

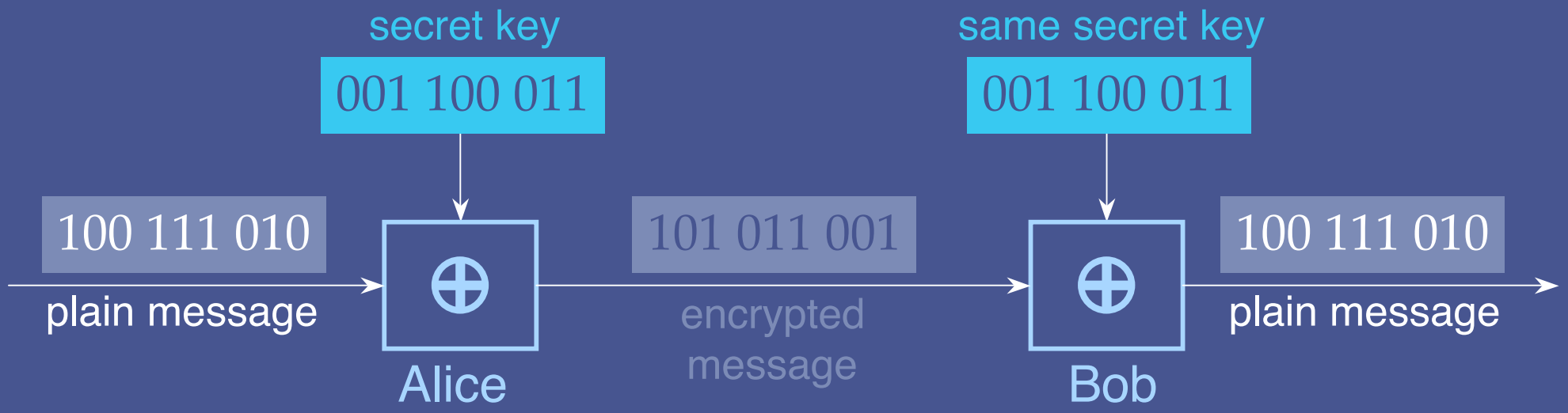
- Secret key cryptography: Alice encrypts with a key. Bob decrypts with the same key. This key must be known by Alice and Bob, and by no one else.
- Public key cryptography: Alice encrypts with Bob's public key, known by everyone. Bob decrypts with his private key, known by him only.

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 : 30000 ans 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)

One-time pad: the unbreakable secret key

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

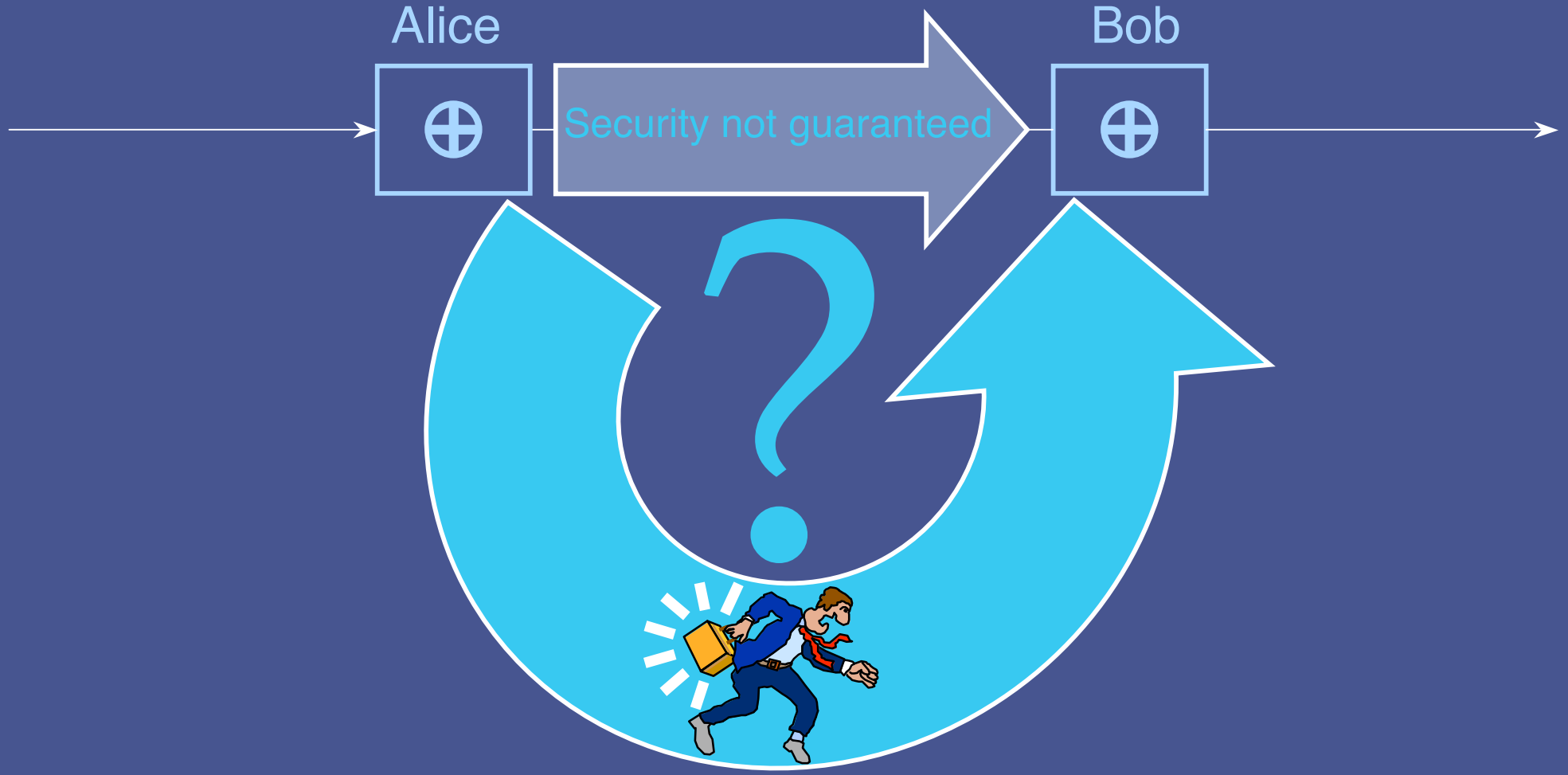


- Joseph Mauborgne, US Army, in the 20's:

  If the key is a random sequence, then the encrypted message is also a random sequence, i.e. contains no information for anyone ignoring the key.

- Two conditions:
  - The key must be secret
  - The key should not be used more than once

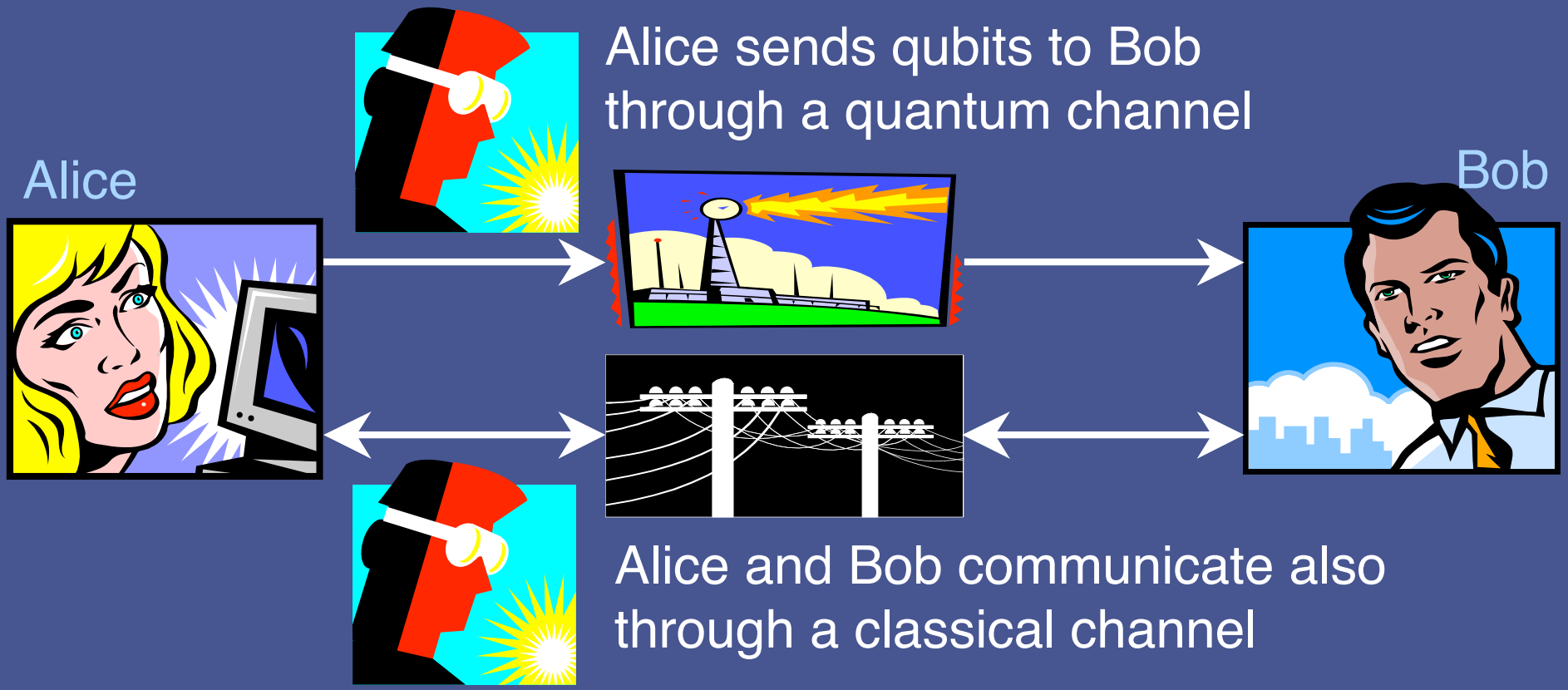
Problem: the key must be secret



Quantum cryptography: guarantee the secrecy of the key, without assuming anything about the security offered by the channels.

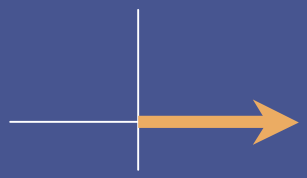
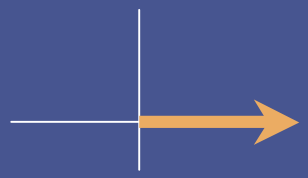
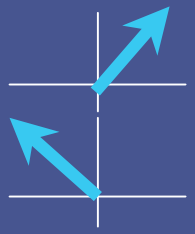
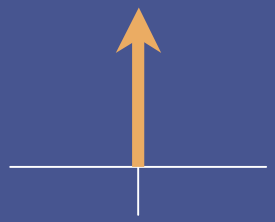
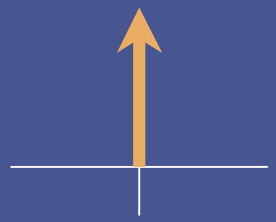
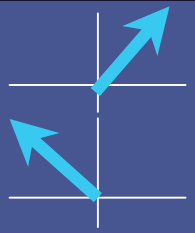
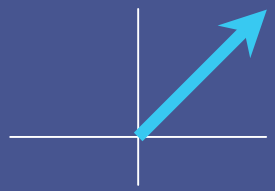
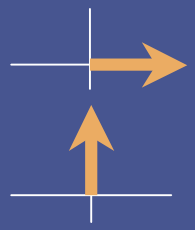
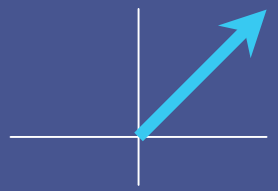
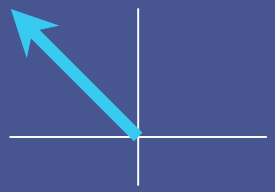
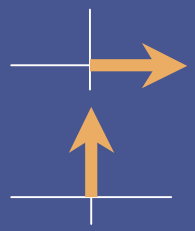
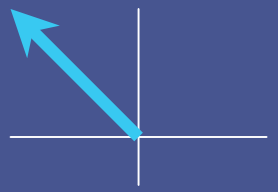
Quantum cryptography: the characters, the scenery

Eve, an eavesdroper, intercepts and measures the qubits on the quantum channel, and forwards them Bob



Eve also listens to the conversations of Alice and Bob

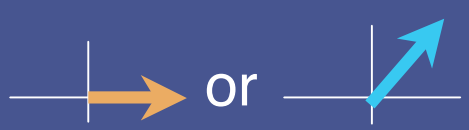
More about quantum measurement

State before measurement	Measurement in the standard basis: Prob.	State after	Value returned	… and in the diagonal basis: Prob.	State after	Value returned
	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

A quantum cryptography protocol (BB84)

1 On the quantum channel

- Alice builds a random sequence of $4n$ 0's and 1's, where n is the length of the key, and sends each bit to Bob, encoded at random by a qubit:



sent for 0

sent for 1

- Eve and Bob measure each qubit, at random in  or in 
- Both Alice and Bob now have sequences of $4n$ bits

2 On the classical channel

- For each bit, Alice and Bob compare the bases they have used. They discard those for which the bases were different, i.e. $2n$ bits.
- Alice and Bob compare n of the remaining bits, chosen at random, and discard them: without Eve, these bits should be pairwise identical.
- With Eve: probability of all remaining n bits pairwise identical = $(3/4)^n$

Quantum cryptography on the market

- Qubit = photon
- Commercial products, with transmission through optical fibers:

Geneva, Switzerland

New York, USA

Lannion, France

- Ongoing projects by British Telecom, Swiss Telecom, Thalès, IBM, Lucent, AT&T, NEC, Mitsubishi, etc.
- Recent open air experiment: 144 km, between two Canary islands
- Next step, decisive : ground-satelite key exchange