Introduction à la cryptographie quantique et au calcul quantique

Pierre Rouchon

Centre Automatique et Systèmes
Mines ParisTech
pierre.rouchon@mines-paristech.fr

Décembre 2012

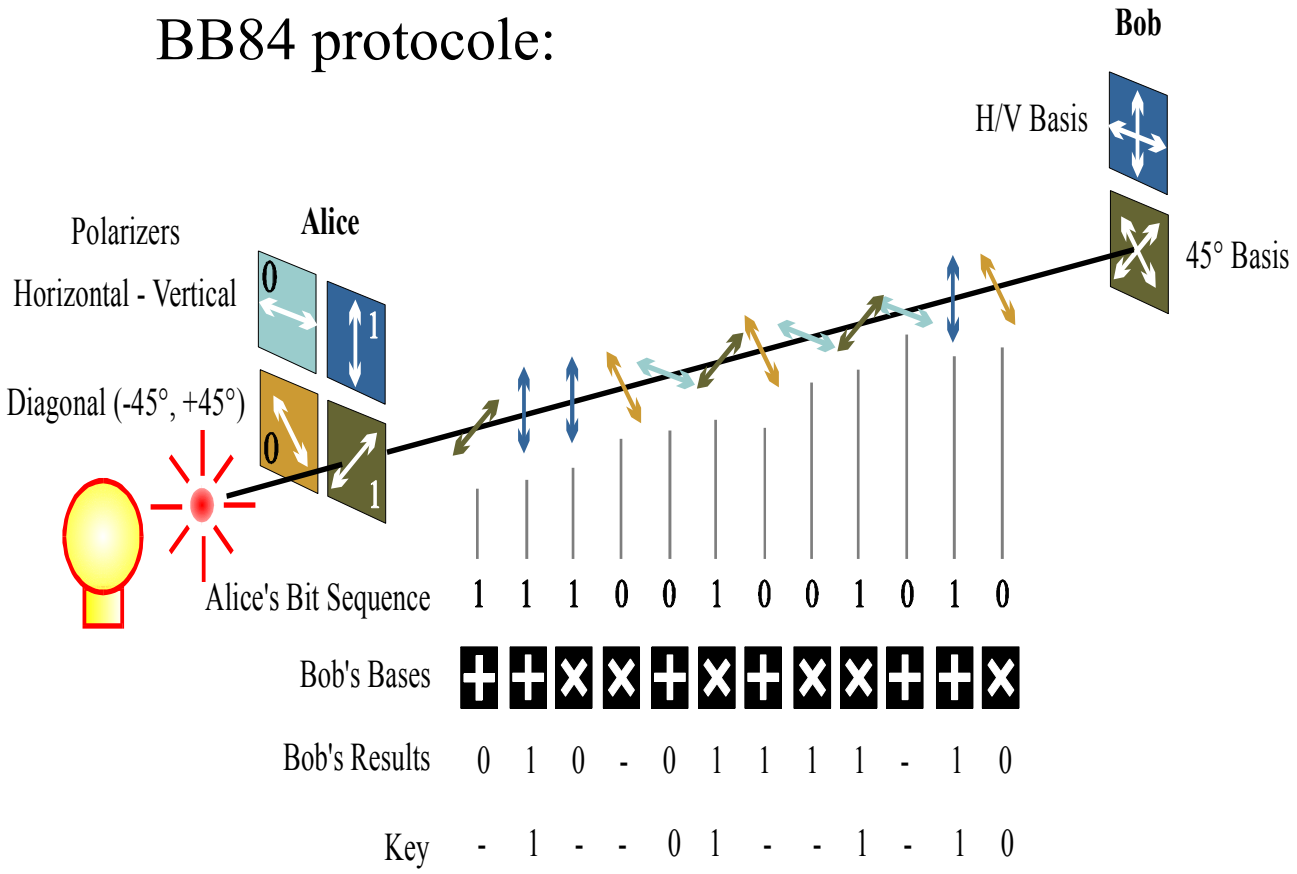
Quelques références

- Le cours de Mécanique Quantique de C. Cohen-Tannoudji B. Diu et F. Laloë. Hermann, Paris, Volumes I& II, 1977.
- Cours en ligne de Serge Haroche au Collège de France : `http://www.cqed.org/college/college.html`
- Exploring the quantum : atoms, cavities and photons. S. Haroche and J-M Raimond. Oxford University Press (2006).
- Cours de Peskill au Caltech intitulé Quantum computation : `www.theory.caltech.edu/people/preskill/ph229/#lecture`
- Quantum computation and quantum information. M.A. Nielsen and I.Chuang, Cambridge Univ.Press. (2000)
- Le site web d'une entreprise : `http://www.idquantique.com`

Plan

1. BB84
   - Le protocole de distribution de clés de chiffrement
   - Sureté du protocole : impossibilité du clonage
2. Intrication
   - Inégalité de Bell pour un 2-qubit
   - Distribution de clés secrètes par partage d'états intriqués
   - Protocole de téléportation
3. Calculs et algorithmes quantiques
   - Portes et circuits logiques classiques
   - Portes et circuits logiques quantiques
   - Algorithme de Deutsch-Josza
   - Algorithme de recherche de Grover

Une idée due à Bennet et Brassard en 1984 (BB84)



GAP Optique
Geneva University

- Alice envoie à Bob des photons polarisés linéairement (i.e. les qubits $|\psi\rangle = a_0 |0\rangle + a_1 |1\rangle$) aléatoirement selon les 4 directions suivantes :
  - polarisation horizontale $|0\rangle$ et verticale $|1\rangle$.
  - polarisation à +45, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ et -45, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$
- Lorsque Bob reçoit un photon d'Alice, il choisit aléatoirement de le mesurer selon deux types de polariseurs :
  - Polariseur H/V : $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$
  - Polariseur à 45 : $X = |1\rangle\langle 0| + |0\rangle\langle 1|$
- Alice communique à Bob (canal classique public) pour chaque photon le type de polarisation (H/V ou +45/-45) mais pas la polarisation exacte.
- Bob communique à Alice (canal classique public) pour chaque photon mesuré le type de polariseur choisi (Z ou X) mais pas le résultat de sa mesure.

BB84 (fin)

- Les photons pour lesquels Alice et Bob ont utilisé des polarisations compatibles : (H/V,Z) et (+45/-45, X) sont partagés en deux groupes :
  1. le premier groupe forme la clé secrète qui sera utilisée dans un système classique de chiffrement.
  2. pour le second groupe, Bob envoie à Alice sur le canal classique et public les résultats de ses mesures.
- La sécurité vient du fait que si l'espion Oscar écoute la ligne, i.e., capte certains photons envoyés par Alice, il les perturbe inévitablement et alors Alice s'en rend compte sur les photons du second groupe (certaines mesures de Bob ne coincident pas avec les siennes). Intuitivement le nombre de photons envoyés par Alice doit être grand pour laisser une chance quasi-nulle à Oscar d'espionner sans être repéré.
- Impossibilité du clonage par Oscar d'un photon venant d'Alice.

Sureté du protocole : impossibilité du clonage d'un qubit

- Pour copier le qubit $|\psi\rangle \in \mathbb{C}^2$, dans le qubit clone d'état initial $|b\rangle \in \mathbb{C}^2$, on utilise un appareil de fonction d'onde initiale $|f_b\rangle$ qui vit dans un espace de Hilbert $\mathcal{H}$.
- La fonction d'onde $|\Xi\rangle$ du système composite (qubit initial, qubit clone, appareil) vit dans le produit tensoriel $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathcal{H}$. Sa valeur à l'instant initial $t = 0$, début du clonage, est donc

$$|\Xi\rangle_{t=0} = |\psi\rangle \otimes |b\rangle \otimes |f_b\rangle \,.$$

- Le clonage met un temps $T > 0$. Entre $t = 0$ et $t = T$, $|\Xi\rangle$ évolue selon Schrödinger : $\imath\hbar \frac{d}{dt} |\Xi\rangle = H(t) |\Xi\rangle$ où $H(t)$ est l'hamiltonien, un opérateur linéaire auto-adjoint $H^\dagger = H$. La transformation (propagateur) $U_T : |\Xi\rangle_0 \mapsto |\Xi\rangle_T = U_T |\Xi\rangle_0$ est linéaire, et préserve le produit hermitien (transformation unitaire).

Impossibilité du clonage d'un qubit (fin)

Si U_T permet le clonage de n'importe quel qubit $|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle$, cela implique en particulier que U_T vérifie :

$$|0\rangle \otimes |0\rangle \otimes \left|f_{|0\rangle}\right\rangle = U_T \left(|0\rangle \otimes |b\rangle \otimes |f_b\rangle\right)$$

$$\left|\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right\rangle \otimes \left|\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right\rangle \otimes \left|f_{\frac{|0\rangle+|1\rangle}{\sqrt{2}}}\right\rangle = \ldots$$

$$\ldots U_T \left(\left|\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right\rangle \otimes |b\rangle \otimes |f_b\rangle\right)$$

Ce qui est impossible car U_T préserve le produit hermitien :

$$\langle \Xi | \Lambda \rangle > \langle \Xi | U_T^\dagger U_T | \Lambda \rangle$$

avec $|\Xi\rangle = |0\rangle \otimes |b\rangle \otimes |f_b\rangle$ et $|\Lambda\rangle = \left|\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right\rangle \otimes |b\rangle \otimes |f_b\rangle$.

Intrication d'un 2-qubit : mesure de $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ sur le 1er qubit

- Etat décrivant l'intrication d'une paire de qubits :

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

qui ne peut pas s'écrire comme le produit tensoriel de deux qubit :

$$\forall a_0, a_1, b_0, b_1 \in \mathbb{C}, |\psi\rangle \neq (a_0 |0\rangle + a_1 |1\rangle) \otimes (b_0 |0\rangle + b_1 |1\rangle).$$

- Le premier qubit va vers Alice et le second qubit va vers Bob.
- Les mesures de Bob et Alice ont lieu en même temps (causalement indépendantes).
- Si Alice mesure Z sur son qubit et trouve -1 alors Bob qui mesure Z sur le sien trouvera nécessairement 1, bien que Alice et Bob fassent leur mesure en même temps. Non localité de la fonction d'onde $|\psi\rangle$.

Intrication d'un 2-qubit : mesure de $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ sur le 1er qubit

- Avec $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ et $|-\rangle = \frac{-|0\rangle+|1\rangle}{\sqrt{2}}$ on a

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{|+-\rangle - |-+\rangle}{\sqrt{2}}$$

- Le premier qubit va vers Alice et le second qubit va vers Bob.
- Les mesures de Bob et Alice ont lieu en même temps (causalement indépendantes).
- Si Alice mesure $X = |+\rangle\langle +| - |-\rangle\langle -|$ sur son qubit et trouve -1 alors Bob qui mesure X sur le sien trouvera nécessairement 1, bien que Alice et Bob fasse leur mesure en même temps. Non localité de la fonction d'onde $|\psi\rangle$.

Impossibilité d'interpréter $\frac{|01\rangle-|10\rangle}{\sqrt{2}}$ comme une **distribution statistique classique** de $|01\rangle$ avec la probabilité classique de $1/2$ et de $|10\rangle$ avec aussi une probabilité de $1/2$: preuve expérimentale via la violation des inégalités de Bell.

Inégalité de Bell

- Alice et Bob disposent d'un grand nombre N de paires de qubits intriqués du type $|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$.
- Pour chaque paire Alice mesure aléatoirement sur son qubit soit $Q = Z \otimes I_d$ soit $R = X \otimes I_d$; Bob mesure aussi sur la même paire aléatoirement (et indépendamment d'Alice) soit $S = I_d \otimes \left(\frac{-Z-X}{\sqrt{2}}\right)$ soit $T = I_d \otimes \left(\frac{Z-X}{\sqrt{2}}\right)$.
- A la fin des expériences Alice et Bob mettent en commun leur résultats et calculent ainsi la valeur moyenne de

$$QS + RS + RT - QT = \\ - \frac{(Z+X) \otimes (Z+X)}{\sqrt{2}} - \frac{(Z-X) \otimes (Z-X)}{\sqrt{2}}$$

et ils trouvent environ $2\sqrt{2}$.

Inégalité de Bell (fin)

- Raisonnement classique : comme $QS+RS+RT-QT=(Q+R)S+(R-Q)T$ on voit que chaque mesure ne peut donner que ± 2 car chaque mesure de Q, R, S et T donne ± 1.
- On suppose qu'avant chaque mesure le système à la probabilité $\pi(p,r,s,t)$ que la mesure de Q donne $p=\pm 1$, celle de R donne $r=\pm 1$, celle de S donne $s=\pm 1$ et celle de T donne $t=\pm 1$
- Donc la valeur moyenne $E(QS+RS+RT-QT)$ vérifie l'inégalité de Bell :

$$E(QS+RS+RT-QT)=\sum_{q,r,s,t=\pm 1}\pi(q,r,s,t)(qs+rs+rt-qt)\leq 2$$

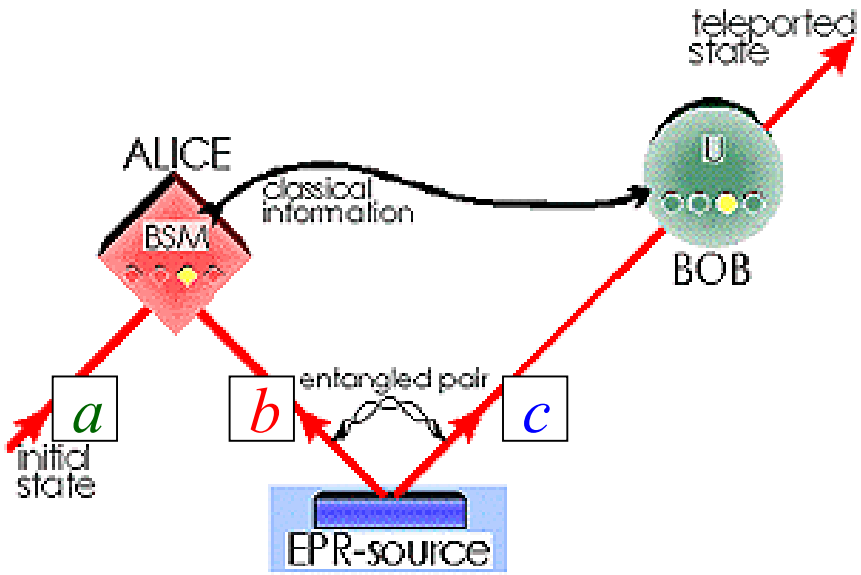
- Or Alice et Bob (Alain Aspect dans les années 1980) trouvent un résultat proche de $2\sqrt{2}>2$. Donc le raisonnement classique ci-dessus n'est pas valable : **les valeurs de Q, R, S et T ne sont pas définies** même de façon probabiliste, **avant d'être mesurées**, comme c'est implicitement le cas avec la théorie des variables cachées locales et le raisonnement probabiliste ci-dessus.

Clés secrètes par partage d'états intriqués

Protocole imaginé par Ekert en 1991 ayant la même utilité que BB84.

- Alice prépare un grand nombre N de 2-qubits intriqués $|\psi\rangle_k = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Pour chaque 2-qubit, Alice garde le premier qubit et envoie le second à Bob.
- Alice et Bob se ramènent à la fin du protocole BB84. Indépendamment l'un de l'autre, Alice et Bob décident de mesurer leur qubit no k selon u_k pour Alice et v_k pour Bob ($u_k, v_k \in \{X, Z\}$).
- Après avoir fait chacun N mesures, ils échangent publiquement les u_k et v_k.
- Ils se retrouvent alors exactement dans la même situation qu'en fin de BB84 après l'échange des u_k et v_k. Ils procèdent alors comme pour BB84 pour se convaincre que les N qubits étaient au départ bien intriqués.

Téléportation quantique combinant intrication et transport d 'information classique (Bennet et al, 1993):*



Alice et Bob partagent une paire EPR (b-c). Alice reçoit une particule quantique a dans un état inconnu (qu 'elle ne peut d 'ailleurs déterminer) et la couple à son partenaire EPR (b). Elle effectue une mesure collective sur l 'ensemble a - b ainsi formé. Cette mesure a un effet immédiat sur la particule c de Bob (en raison de l'intrication b-c). L'état final de c dépend de l 'état initial de a et du résultat de la mesure d 'Alice. Elle communique classiquement ce résultat à Bob qui peut alors, par une transformation unitaire sur c, reconstituer l 'état initial de a.

6

1

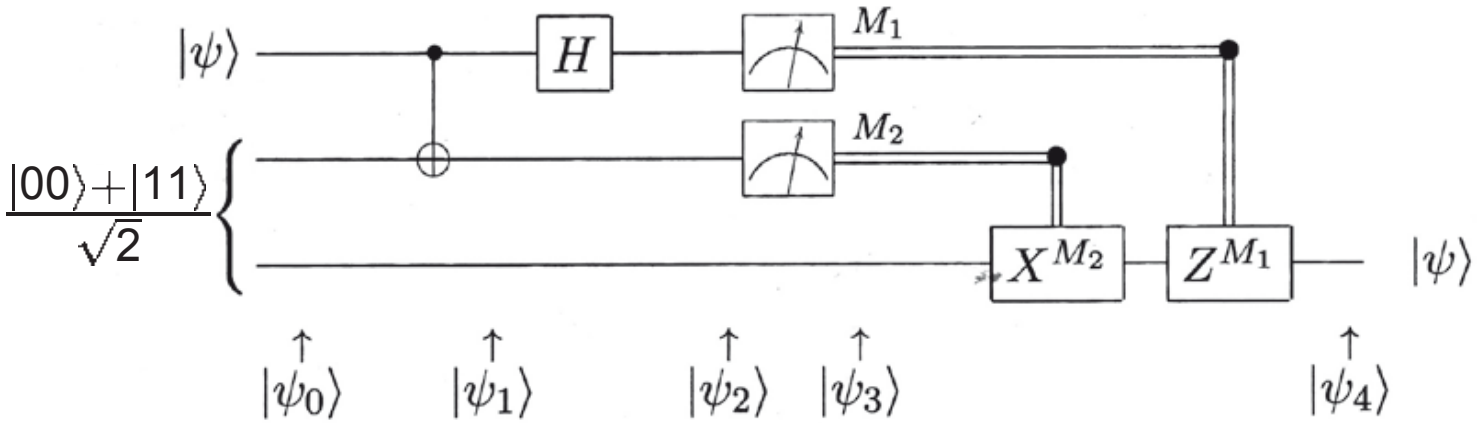
(*) Phys.Rev.Lett. 70, 1895 (1993).

[1] Source : cours 2001/2002 de Serge Haroche, Collège de France

Téléportation de $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Alice

Bob



$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|00\rangle + |11\rangle\right)\right]$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|10\rangle + |01\rangle\right)\right]$$

$$|\psi_2\rangle = \frac{1}{2}\left[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\right]$$

$$|\psi_2\rangle = \frac{1}{2}\left[|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) + \ldots\right.$$
$$\left.\ldots|10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)\right]$$

Téléportation de $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (fin)

$$|\psi_2\rangle = \frac{1}{2}\left[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + \ldots\right.$$
$$\left.\ldots|10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right]$$

Mesure d'Alice :
$$\begin{cases} m_1 & m_2 & \\ 0 & 0 & \mapsto |\psi_3\rangle = \alpha|0\rangle + \beta|1\rangle \\ 0 & 1 & \mapsto |\psi_3\rangle = \alpha|1\rangle + \beta|0\rangle \\ 1 & 0 & \mapsto |\psi_3\rangle = \alpha|0\rangle - \beta|1\rangle \\ 1 & 1 & \mapsto |\psi_3\rangle = \alpha|1\rangle - \beta|0\rangle \end{cases}$$

Alice communique à Bob, via un canal de transmission classique, les valeurs de m_1 et m_2. Bob retrouve alors $|\psi\rangle$ sur son qubit $(\alpha|0\rangle + \beta|1\rangle)$ en appliquant les portes $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ et $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$ si nécessaire à $|\psi_3\rangle$:

$$\alpha|0\rangle + \beta|1\rangle = Z^{m_1} X^{m_2} |\psi_3\rangle .$$

Trois portes logiques classiques universelles AND, XOR et NOT

Fonction booléenne : f de $\{0,1\}^n$ vers $\{0,1\}^m$; réalisation de f par un circuit classique par assemblage de quelques portes logiques dites universelles où $n, m \leq 2$ comme les trois portes logiques universelles, AND, XOR et NOT :

- AND : $\{0,1\}^2 \ni (x_1, x_2) = x \mapsto f(x) = \begin{cases} 1, & \text{si } x_1 = x_2 = 1\,; \\ 0, & \text{sinon.} \end{cases}$
- XOR : $\{0,1\}^2 \ni (x_1, x_2) = x \mapsto f(x) = \begin{cases} 1, & \text{si } x_1 \neq x_2\,; \\ 0, & \text{sinon.} \end{cases}$
- NOT : $\{0,1\} \ni x \mapsto f(x) = \begin{cases} 1, & \text{si } x = 0\,; \\ 0, & \text{sinon.} \end{cases}$

- Le calcul de $f_n(x) : \{0,1\}^n \mapsto \{0,1\}$ est considéré comme facile (resp. difficile) si le nombre c_n de portes universelles du circuit qui réalise f_n croit de façon polynômiale (resp. exponentielle) avec n.
- $f_n(x) : \{0,1\}^n \mapsto \{0,1\}$ code un problème de décision où n est le nombre de bit nécessaire pour le stockage des données x : $f_n(x) = 1$ caractérise les instance positive. Si le problème est dans **P** , alors le calcul de f_n est facile.
- Exemple : $x = (r, s)$ entiers positifs r et s d'au plus $n/2$ bits chacun : r et s ont-ils un diviseur non trivial ?

$$f_n(r,s) = \begin{cases} 0, & \text{si } r \wedge s = 1\,; \\ 1, & \text{sinon.} \end{cases}$$

Comme le calcul du pgcd est polynômiale (algorithme fondé sur la division euclidienne) celui de f_n est facile.

Unités de calcul quantique :

- qubit évoluant dans des superpositions de $|0\rangle$ et $|1\rangle$
- n-qubit dans l'espace de Hilbert $\mathcal{H}_n = \mathbb{C}^{2^n}$ de dimension $N = 2^n$. Base canonique $|x\rangle$ indexée par $x = \sum_{k=0}^{n-1} x_k 2^k$, chaque $x_k \in \{0, 1\}$:

$$|x\rangle = |x_0\rangle \otimes |x_1\rangle \otimes \ldots \otimes |x_k\rangle \otimes \ldots \otimes |x_{n-1}\rangle = |x_0, x_1, \ldots, x_k, \ldots, x_{n-1}\rangle .$$

- état général d'un n-qubit :

$$|\psi\rangle = \sum_{x=0}^{N-1} \psi_x |x\rangle = \sum_{x_0,\ldots,x_{n-1}\in\{0,1\}} \psi_{x_0\ldots x_{n-1}} |x_0, \ldots, x_{n-1}\rangle$$

où chaque $\psi_x \in \mathbb{C}$ et $\sum_{x=0}^{N-1} |\psi_x|^2 = 1$.

Une porte logique quantique à n qubits : une transformation unitaire U de $\mathcal{H}_n = \mathbb{C}^{2^n}$ dans lui-même.
Circuit quantique : dispositif idéal qui réalise une transformation unitaire associée à son évolution selon l'équation différentielle de Schrödinger.

Portes quantiques universelles : portes à un seul qubit et la porte CNOT

Réalisation d'une transformation unitaire arbitraire avec un nombre fini de portes quantiques CNOT à deux qubits et de portes quantiques à un seul qubit :

- CNOT : transformation unitaire sur $\mathcal{H}_2$ ($\oplus$ est l'addition modulo 2) :

$$U_{\text{CNOT}} |x_0, x_1\rangle = |x_0, x_0 \oplus x_1\rangle$$

- La porte à un seul qubit : décomposition de toute transformation unitaire U_1 de $\mathcal{H}_1 = \mathbb{C}^2$:

$$U_1 = e^{\imath\theta} e^{-\imath\alpha Z/2} e^{-\imath\beta X/2} e^{-\imath\gamma Z/2}$$

avec quatre angles θ, α, β et γ arbitraire X, Y et Z les trois matrices de Pauli :

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad Y = \imath\,|1\rangle\langle 0| - \imath\,|0\rangle\langle 1|, \quad Z = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

La porte de Hadamard $H = (X + Z)/\sqrt{2}$ est très utilisée :

$$H = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\langle 0| + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\langle 1| = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|\right).$$

Porte quantique associée à une fonction booléenne classique

- Fonction booléenne (classique) $\{0,1\}^n \ni x \mapsto f_n(x) \in \{0,1\}$
- Porte logique quantique U_{f_n} sur $\mathcal{H}_n \otimes \mathcal{H}_1$ de base canonique $|x\rangle \otimes |q\rangle$ où $(x,q) \in \{0,1\}^n \times \{0,1\}$:

$$U_{f_n}\big(\,|x\rangle \otimes |q\rangle\,\big) = |x\rangle \otimes |q \oplus f_n(x)\rangle$$

- Si f_n est facile à calculer (circuit classique avec nombre polynômiale en n de `AND`, `XOR` et `NOT`), alors U_{f_n} est aussi facile à calculer (circuit quantique avec un nombre polynômiale en n de portes quantiques à un seul qubit et de portes `CNOT`).
- Preuve : la transformation du circuit classique irréversible en un circuit classique réversible.

”Parallélisation” propre au calcul quantique

$$\{0,1\}^n \ni x \mapsto f_n(x) \in \{0,1\}, \quad U_{f_n}\big(\,|x\rangle \otimes |q\rangle\,\big) = |x\rangle \otimes |q \oplus f_n(x)\rangle$$

- Calcul de $f_n(x)$ avec U_{f_n} : mesurer le dernier qubit de $U_{f_n}\,|x\rangle \otimes |0\rangle$
- Parallélisation du calcul de f_n :

$$U_{f_n}\left(\frac{1}{\sqrt{N}}\left(\sum_x |x\rangle\right) \otimes |0\rangle\right) = \frac{1}{\sqrt{N}}\left(\sum_x |x\rangle \otimes |f_n(x)\rangle\right).$$

  Exploitation possible en rajoutant des transformations unitaires simples avant la mesure.
- On dispose d’algorithmes quantiques rapides pour factoriser un grand nombre (Peter Shor 1994) et aussi pour calculer le logarithme discret. Ces deux algorithmes trop longs à décrire dans le cadre du cours reposent sur la transformée de Fourier quantique (généralisation directe de la FFT).

Le problème résolu par l'algorithme de Deutsch-Josza

- Les données : une fonction booléenne $f : \{0,1\}^n \ni x \mapsto f(x) \in \{0,1\}$ qui est soit balancée soit constante.
- La question : la fonction est-elle constante ?
- Sans autre information structurelle sur f, la réponse à la question nécessite de calculer $f(x)$ pour au moins la moitié des x possibles.
- l'algorithme de Deutsch-Josza permet de répondre avec un seul appel à la porte quantique associée U_f.

L'avantage n'est décisif que pour une réponse sûr. Pour f polynômiale, la certification des instances positives (et aussi négatives) est dans **RP** : avec r évaluations de f sur des x tirés au hasard, on se persuade de la réponse avec une probabilité d'erreur $\leq 1/2^r$.

Algorithme de Deutsch-Josza

$$X = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad H = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\langle 0| + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\langle 1|$$

1. On part de $|\Psi\rangle_0 = |0,\ldots,0\rangle \otimes |0\rangle \in \mathcal{H}_n \otimes \mathcal{H}_1$.
2. $H^{\otimes n}$ sur les n premiers qubits et HX sur le dernier :
   $|\Psi\rangle_1 = \left(\frac{\sum_x |x\rangle}{\sqrt{N}}\right) \otimes \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$.
3. $|\Psi\rangle_2 = U_f |\Psi\rangle_1 = |f\rangle \otimes \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$, état séparable avec
   $$|f\rangle = \frac{1}{\sqrt{N}} \sum_x (-1)^{f(x)} |x\rangle \in \mathcal{H}_n.$$
   f balancée : $|f\rangle$ est orthogonal à $\sum_x |x\rangle$
   f constante : $|f\rangle$ est colinéaire à $\sum_x |x\rangle$
4. Comme $H^{\otimes n}\left(\frac{1}{\sqrt{N}}\sum_x |x\rangle\right) = |0\rangle$ on a :
   f balancée donne $H^{\otimes n}|f\rangle$ orthogonal à $|0\rangle$
   f constante donne $H^{\otimes n}|f\rangle$ colinéaire à $|0\rangle$.
5. Mesure de chacun des n qubits de $H^{\otimes n}|f\rangle$: si les n mesures donnent toutes $|0\rangle$ alors f constante ; sinon f est balancée.

Algorithme de recherche de Grover

Recherche non structurée généralisant celle du nom d'une personne dans un annuaire à partir de son numéro de téléphone :

- Données : $f : \{0,1\}^n \ni x \mapsto f(x) \in \{0,1\}$, nulle sauf pour un seul $\bar{x}$ inconnu pour lequel $f(\bar{x}) = 1$.
- Problème : trouver la solution de $f(x) = 1$.
- Sans autre information structurelle sur f : un algorithme classique nécessite dans le pire des cas $O(N)$ appels à la fonction f pour trouver $\bar{x}$.
- L'algorithme de Glover, valable pour tout f, donne la solution avec $O(\sqrt{N})$ appels à la porte quantique U_f associée à f.

Le départ identique Deutsch-Josza : $\mathcal{H}_n \ni |0\rangle \mapsto |f\rangle = O_f H^{\otimes n} |0\rangle$ où la transformation unitaire O_f est définie par

$$\forall |\psi\rangle \in \mathcal{H}_n, \quad U_f \left(|\psi\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \right) = \left(O_f |\psi\rangle \right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right).$$

Sur la base canonique de $\mathcal{H}_n$: $\forall x \in \{0,1\}^n, \quad O_f |x\rangle = (-1)^{f(x)} |x\rangle$.

Algorithme de recherche de Grover (suite)

- Avec O_f ($O_f |x\rangle = (-1)^{f(x)} |x\rangle$) on construit la transformation unitaire :

$$G_f = H^{\otimes n}(2|0\rangle\langle 0| - \mathbb{I}_n)H^{\otimes n}O_f.$$

- Elle est itérée $m = E\left(\frac{\pi}{4}\sqrt{N}\right)$ fois pour calculer

$$|f_m\rangle = (G_f)^m \left(\frac{1}{\sqrt{N}}\sum_x |x\rangle\right) = (G_f)^m H^{\otimes n}|0\rangle .$$

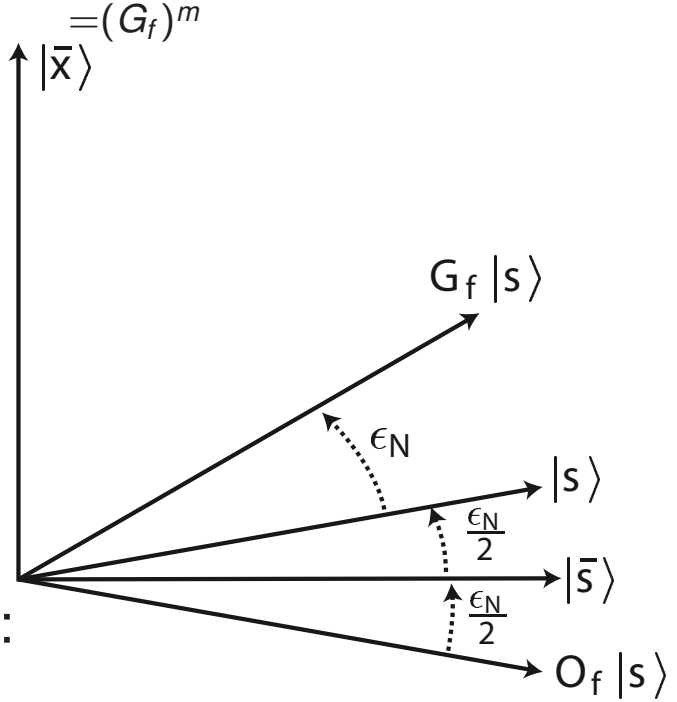
- Les mesures des n qubits formant $|f_m\rangle$ donnent avec une probabilité très proche de 1, les n bits codant $\bar{x}$.
- Il est alors facile de vérifier que cette mesure donne bien la solution par un seul appel à f.
- Efficacité du grand principe Shadok à la base de la classe **RP**

”Plus ça rate, plus ça a des chances de marcher.”

Algorithme de recherche de Grover : si $m = E\left(\frac{\pi}{4}\sqrt{N}\right)$ on a $|f_m\rangle \approx |\bar{x}\rangle$:

$$|s\rangle = H^{\otimes n}|0\rangle = \frac{1}{\sqrt{N}}\sum_x |x\rangle, \quad |f_m\rangle = \underbrace{\left(H^{\otimes n}\left(2|0\rangle\langle 0| - \mathbb{I}_n\right)H^{\otimes n}O_f\right)^m}_{=(G_f)^m}|s\rangle$$

1. $H^{\otimes n}(2|0\rangle\langle 0| - \mathbb{I}_n)H^{\otimes n} = 2|s\rangle\langle s| - \mathbb{I}_n$ est la symétrie orthogonale par rapport à $|s\rangle$.
2. $O_f|s\rangle = |s\rangle - \frac{2}{\sqrt{N}}|\bar{x}\rangle$, $O_f|\bar{x}\rangle = -|\bar{x}\rangle$.
3. $G_f|s\rangle = \left(1 - \frac{4}{N}\right)|s\rangle + \frac{2}{\sqrt{N}}|\bar{x}\rangle$.
4. $G_f|\bar{x}\rangle = |\bar{x}\rangle - \frac{2}{\sqrt{N}}|s\rangle$.
5. Plan $(|s\rangle, |\bar{x}\rangle)$ invariant par G_f de base orthonormée $|\bar{x}\rangle$, $|\bar{s}\rangle = (\sum_{x\neq\bar{x}}|x\rangle)/\sqrt{N-1}$: $|s\rangle = \sqrt{(N-1)/N}\,|\bar{s}\rangle + \sqrt{1/N}\,|\bar{x}\rangle$.



La restriction de G_f au plan $(|\bar{s}\rangle, |\bar{x}\rangle)$: rotation d'angle ϵ_N avec $\cos\left(\frac{\epsilon_N}{2}\right) = \sqrt{\frac{N-1}{N}}$, $\sin\left(\frac{\epsilon_N}{2}\right) = \sqrt{\frac{1}{N}}$. Comme $|s\rangle = \cos\left(\frac{\epsilon_N}{2}\right)|\bar{s}\rangle + \sin\left(\frac{\epsilon_N}{2}\right)|\bar{x}\rangle$:

$$|f_m\rangle = (G_f)^m|s\rangle = \cos\left(\frac{2m+1}{2}\epsilon_N\right)|\bar{s}\rangle + \sin\left(\frac{2m+1}{2}\epsilon_N\right)|\bar{x}\rangle \quad \text{avec } \frac{2m+1}{2}\epsilon_N \approx \frac{\pi}{2}$$