Informatique quantique IFT6155

Matrices de densité et chiffrement de données quantiques

Matrice de densité

Définition: On appelle *mélange* S, une distribution d'états quantiques $|\Psi_i\rangle$ (de même dimension) avec probabilité α_i ($\sum_i \alpha_i = 1$)

$$S = \{(\alpha_1, |\Psi_1\rangle), (\alpha_2, |\Psi_2\rangle), \cdots, (\alpha_n, |\Psi_n\rangle)\}$$

Définition: La matrice ρ_s associée au mélange S et définie par

$$\rho_s = \alpha_1 |\psi_1\rangle \langle\psi_1| + \alpha_2 |\psi_2\rangle \langle\psi_2| + \cdots + \alpha_n |\psi_n\rangle \langle\psi_n|$$

est appelée *matrice de densité* du mélange S.

Si les états de S sont de n qubits alors ρ_s est une matrice 2^n par 2^n.

Définition: Une matrice M est *hermitienne* si $M^\dagger M = M M^\dagger$.

Théorème: Toute matrice de densité ρ_s est hermitienne.

$$\begin{aligned}
\rho_s^\dagger &= (\alpha_1 |\psi_1\rangle \langle\psi_1| + \alpha_2 |\psi_2\rangle \langle\psi_2| + \cdots + \alpha_n |\psi_n\rangle \langle\psi_n|)^\dagger \\
&= (\alpha_1 (|\psi_1\rangle \langle\psi_1|)^\dagger + \alpha_2 (|\psi_2\rangle \langle\psi_2|)^\dagger + \cdots + \alpha_n (|\psi_n\rangle \langle\psi_n|)^\dagger \\
&= \alpha_1 |\psi_1\rangle \langle\psi_1| + \alpha_2 |\psi_2\rangle \langle\psi_2| + \cdots + \alpha_n |\psi_n\rangle \langle\psi_n| \\
&= \rho_s
\end{aligned}$$

Matrice de densité

La probabilité d'observer $|x\rangle$ si nous avons l'état $|\psi\rangle$ est donnée par

$$|\langle x|\psi\rangle|^2 = \langle x|\psi\rangle \langle\psi|x\rangle$$

La probabilité d'observer $|x\rangle$ si on mesure un registre dans un mélange S est donnée par

$$\begin{aligned} P(|x\rangle) &= \alpha_1 |\langle x|\Psi_1\rangle|^2 + \alpha_2 |\langle x|\Psi_2\rangle|^2 + \cdots + \alpha_n |\langle x|\Psi_n\rangle|^2 \\ &= \alpha_1 \langle x|\Psi_1\rangle \langle\Psi_1|x\rangle + \alpha_2 \langle x|\Psi_2\rangle \langle\Psi_2|x\rangle + \cdots + \alpha_n \langle x|\Psi_n\rangle \langle\Psi_n|x\rangle \\ &= \langle x| (\alpha_1 |\Psi_1\rangle \langle\Psi_1| + \alpha_2 |\Psi_2\rangle \langle\Psi_2| + \cdots + \alpha_n |\Psi_n\rangle \langle\Psi_n|)|x\rangle \\ &= \langle x| \rho_s |x\rangle \end{aligned}$$

Clairement, $\langle x| \rho_s |x\rangle$ est l'élément en x ième position sur la diagonale de ρ_s.

Matrice de densité

Si on applique U sur un registre dans l'état S on obtient S':

$$S = \{(\alpha_1, |\Psi_1\rangle), (\alpha_2, |\Psi_2\rangle), \cdots, (\alpha_n, |\Psi_n\rangle)\}$$

$$S\text{`} = \{(\alpha_1, U|\Psi_1\rangle), (\alpha_2, U|\Psi_2\rangle), \cdots, (\alpha_n, U|\Psi_n\rangle)\}$$

Clairement,

$$\begin{aligned} U\rho_s U^\dagger &= U(\alpha_1 |\psi_1\rangle \langle\psi_1| + \alpha_2 |\psi_2\rangle \langle\psi_2| + \cdots + \alpha_n |\psi_n\rangle \langle\psi_n|)U^\dagger \\ &= \alpha_1 U |\psi_1\rangle \langle\psi_1| U^\dagger + \alpha_2 U |\psi_2\rangle \langle\psi_2| U^\dagger + \cdots + \alpha_n U |\psi_n\rangle \langle\psi_n| U^\dagger \\ &= \alpha_1 (U|\psi_1\rangle)(\langle\psi_1| U^\dagger) + \alpha_2 (U|\psi_2\rangle)(\langle\psi_2| U^\dagger) + \cdots + \alpha_n (U|\psi_n\rangle)(\langle\psi_n| U^\dagger) \\ &= \rho_{s'} \end{aligned}$$

On peut donc associer à tout ensemble d'états S une matrice ρ_s appelée matrice de densité telle que $P(|x\rangle) = \langle x| \rho_s |x\rangle$ et $U\rho_s U^\dagger$ est la matrice de densité de l'ensemble S après l'application de U.

Pour un registre de k qubits, la matrice de densité est une matrice de dimension 2^k et ne dépend pas du nombre d'états dans S.

États distinguables

Théorème:
Si $\rho_1 = \rho_2$ alors il est impossible de distinguer ρ_1 de ρ_2.

Preuve:
Soit ρ_1 la matrice de densité de S_1 et ρ_2 la matrice de densité de S_2. Pour distinguer S_1 de S_2 on peut effectuer une opération unitaire suivie d'une mesure. La probabilité d'observer $|x\rangle$ pour l'ensemble S_1 est donnée par

$$\langle x| U\rho_1 U^\dagger |x\rangle = \langle x| U\rho_2 U^\dagger |x\rangle$$

et cette quantité est exactement égale à la probabilité d'observer $|x\rangle$ si l'on applique U sur S_2.

États distinguables

Exemple:
$S_1 = \{(1/2), |0\rangle), (1/2, |1\rangle)\}$ et $S_2 = \{(1/2, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)), (1/2, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))\}$

$$
\begin{aligned}
\rho_0 &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}I \\
\rho_1 &= \frac{1}{2}(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle))(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle))^\dagger + \frac{1}{2}(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle))^\dagger \\
&= \frac{1}{4}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|) + \frac{1}{4}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|) \\
&= \frac{1}{4}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1| + |0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) \\
&= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}I
\end{aligned}
$$

Donc ρ_1 et ρ_2 sont indistinguables!

Paire d'états

Théorème: Si ρ_A et ρ_B sont deux états indépendants alors la matrice de densité de l'état conjoint est donnée par $\rho_A \otimes \rho_B$.

preuve:
Soit $S_A = \{(p_1, |\psi_1\rangle), \ldots, (p_k, |\psi_k\rangle)\}$ un ensemble pour l'état ρ_A et $S_B = \{(q_1, |\phi_1\rangle), \ldots, (p_l, |\phi_k\rangle)\}$ un ensemble pour l'état ρ_A . Nous avons que

$$S_{AB} = \{(p_1 q_1, |\psi_1\rangle|\phi_1\rangle), \ldots, (p_1 q_l, |\psi_1\rangle|\phi_l\rangle), \ldots, (p_k q_l, |\psi_k\rangle|\phi_l\rangle)\}$$

est l'ensemble de la réunion des deux systèmes et donc

$$\begin{aligned}
\rho_{AB} &= \sum_{ij} p_i q_j |\psi_i\rangle|\phi_j\rangle \langle\psi_i| \langle\phi_j| \\
&= \sum_{ij} p_i q_j |\psi_i\rangle \langle\psi_i| \otimes |\phi_j\rangle \langle\phi_j| \\
&= \left(\sum_i p_i |\psi_i\rangle \langle\psi_i|\right) \otimes \left(\sum_j q_j |\psi_i\rangle \langle\psi_i|\right) \\
&= \rho_A \otimes \rho_B
\end{aligned}$$

États complètement mélangés

Si l'on choisit avec probabilités égales $|0\rangle$ ou $|1\rangle$ on obtient l'état $\rho = \frac{1}{2} I_2$.

Si on regroupe n tels états on obtient

$$\rho_n = \rho \otimes \rho \otimes \cdots \otimes \rho = \frac{1}{2} I_2 \otimes \cdots \otimes \frac{1}{2} I_2 = \frac{1}{2^n} I_{2^n}$$

Si on mesure ce registre, on obtient $|x\rangle$ uniformément distribué parmi tous les états de base.

$$\langle x| \frac{1}{2^n} I_{2^n} |x\rangle = \frac{1}{2^n} \langle x|x\rangle = \frac{1}{2^n}$$

Cet état est aussi invariant sous les transformations unitaires.

$$U \frac{1}{2^n} I_{2^n} U^\dagger = \frac{1}{2^n} U U^\dagger = \frac{1}{2^n} I_{2^n}$$

Mélange de mélanges

Lemme:
Si nous avons ρ_1 avec probabilité p et rho_2 avec probabilité $1-p$, alors l'état peut être décrit par la matrice de densité

$$\rho = p\rho_1 + (1-p)\rho_2$$

Preuve:
Si

$$S_1 = \{(\alpha_1, |\psi_1\rangle), \ldots, (\alpha_k, |\psi_k\rangle)\}$$

et

$$S_2 = \{(\beta_1, |\phi_1\rangle), \ldots, (\beta_l, |\phi_l\rangle)\}$$

alors

$$S = \{(p\alpha_1, |\psi_1\rangle), \ldots, (p\alpha_k, |\psi_k\rangle), ((1-p)\beta_1, |\phi_1\rangle), \ldots, ((1-p)\beta_l, |\phi_l\rangle)\}$$

et donc la matrice de densité de S est bel et bien donnée par

$$\rho = p\rho_1 + (1-p)\rho_2$$

Trace

Définition:
La *trace* d'une matrice ρ est la somme des éléments sur la diagonale. Si ρ est une matrice de dimension 2^k alors

$$Tr(\rho) = \sum_{i=0}^{2^k-1} \langle i|\, \rho |i\rangle = \sum_{i=0}^{2^k-1} \langle \psi_i|\, \rho |\psi_i\rangle$$

pour une base orthonormale $|\psi_i\rangle$ quelconque.

Théorème: Si ρ est une matrice de densité alors

$$Tr(\rho) = Tr(U\rho U^\dagger) = 1$$

La trace d'une matrice de densité ρ est donc la somme sur tous les $|x\rangle$ des probabilités d'observer $|x\rangle$ lors d'une mesure.

Théorème spectral

Théorème
Toutes les valeurs propres d'un opérateur hermitien M (matrice de densité) sont réelles.

Preuve:
Soit λ une valeur propre de M associée à $|\psi\rangle$.

$$\langle\psi|\, M|\psi\rangle = \langle\psi|\, \lambda|\psi\rangle = \lambda\, \langle\psi|\psi\rangle = \lambda$$

mais nous avons aussi

$$\langle\psi|\, M|\psi\rangle = \langle\psi|\, M^\dagger|\psi\rangle = (\langle\psi|\, M|\psi\rangle)^\dagger = (\langle\psi|\, \lambda|\psi\rangle)^\dagger = (\lambda\, \langle\psi|\psi\rangle)^\dagger = \lambda^*$$

alors comme $\lambda = \lambda^*$ alors λ est réel.

Définition:
Une matrice M est dite *normale* si $MM^\dagger = M^\dagger M$.

Clairement, les matrices unitaires sont normales ($UU^\dagger = U^\dagger U = I$) et les matrices hermitiennes (matrices de densité) sont normales ($M = M^\dagger$).

Théorème:
Si M est normale alors il existe une opération unitaire U tel que $UMU^\dagger = D$ où D est une matrice diagonale.

Matrice de densité

Définition:
Une matrice de densité est une matrice hermitienne de trace 1.

Théorème:
À tout mélange S on peut associer une matrice de densité et à toute matrice de densité ρ on peut associer un ensemble S.

Preuve:
Nous avons déjà vu qu'à tout ensemble S on peut associer une matrice hermitienne de trace 1.

Soit ρ une matrice hermitienne de trace 1. Il existe U tel que

$$U\rho U^\dagger = D = \sum_i \lambda_i |i\rangle \langle i|$$

. On remarque premièrement que les λ_i sont les valeurs propres de ρ. Nous avons donc

$$\rho = U^\dagger(\sum_i \lambda_i |i\rangle \langle i|)U = \sum_i \lambda_i U^\dagger |i\rangle \langle i| U = \sum_i \lambda_i |\psi_i\rangle \langle \psi_i|$$

et donc

$$S = \{(\lambda_1, |\psi_1\rangle), \ldots, (\lambda_n, |\psi_n\rangle)\}$$

est un ensemble ayant comme matrice de densité ρ.

Exemples

50% $|0\rangle$ et 50% $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$\begin{aligned}
\rho_1 &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|) \\
&= \frac{2}{4}|0\rangle\langle 0| + \frac{1}{4}(|0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) \\
&= \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix}
\end{aligned}$$

50% $|0\rangle$ et 50% $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

$$\begin{aligned}
\rho_2 &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}(\langle 0| - \langle 1|) \\
&= \frac{2}{4}|0\rangle\langle 0| + \frac{1}{4}(|1\rangle\langle 1| - |1\rangle\langle 0| - |0\rangle\langle 1|) \\
&= \begin{pmatrix} 3/4 & -1/4 \\ -1/4 & 1/4 \end{pmatrix}
\end{aligned}$$

Ces états sont-ils distinguables?
Pas directement.

Exemple

$$\rho_1 = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix} \qquad \rho_2 = \begin{pmatrix} 3/4 & -1/4 \\ -1/4 & 1/4 \end{pmatrix}$$

Clairement, si on applique H sur chacun des états on obtient des états distinguables puisque

$$H\rho_1 H^\dagger = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix} \qquad H\rho_2 H^\dagger = \begin{pmatrix} 1/4 & 1/4 \\ 1/4 & 3/4 \end{pmatrix}$$

Si on mesure ρ_1 on obtient $|0\rangle$ avec probabilité 3/4.

Si on mesure ρ_2 on obtient $|0\rangle$ avec probabilité 1/4.

Théorème:
Deux états sont distinguables si et seulement si leurs matrices de densité sont différentes.

Trace partielle

Définition: Soit ρ_{AB} vivant dans un espace $\mathcal{H}_A \otimes \mathcal{H}_B$ et $\{|0\rangle, |1\rangle, \ldots, |k-1\rangle\}$ la base normale de $\mathcal{H}_A$. alors la matrice de densité décrivant l'état de la partie du système vivant dans $\mathcal{H}_B$ est donnée par

$$\rho_B = Tr_A(\rho_{AB}) = \sum_i \langle i| \rho_{AB} |i\rangle = \sum_i \langle \psi_i| \rho_{AB} |\psi_i\rangle$$

pour une base orthonormale $|\psi_i\rangle$ de l'espace $\mathcal{H}_A$ quelconque.

Vérifions que ces définitions sont consistantes.

Si $\rho_{AB} = \rho_A \otimes \rho_B$ alors

$$\begin{aligned} Tr_A(\rho_A \otimes \rho_B) &= \sum_i \langle i| \rho_A \otimes \rho_B |i\rangle \\ &= \sum_i \langle i| \rho_A |i\rangle \otimes \rho_B \\ &= Tr(\rho_A) \otimes \rho_B \\ &= \rho_B \end{aligned}$$

Trace partielle

Soit ρ_{AB} vivant dans un espace $\mathcal{H}_A \otimes \mathcal{H}_B$. La probabilité d'observer $|j\rangle$ si on observe le deuxième registre est la somme sur tous les i d'observer $|i\rangle|j\rangle$

$$\begin{aligned} P(|j\rangle) &= \langle j| Tr_A(\rho_{AB})|j\rangle \\ &= \langle j| (\sum_i \langle i| \rho_{AB}|i\rangle)|j\rangle \\ &= \sum_i \langle j| \langle i| \rho_{AB}|i\rangle|j\rangle \\ &= P(|j\rangle) \end{aligned}$$

Trace partielle

Système conjoint.

Fait:

$$(U \otimes V)(\rho_A \otimes \rho_B)(U \otimes V)^\dagger = (U\rho_A U^\dagger) \otimes (V\rho_B V^\dagger)$$

Appliquer une transformation unitaire sur un système ne change pas la matrice de densité d'un autre système. Autrement, on pourrait communiquer plus vite que la lumière.

Fait

$$\begin{aligned} Tr_A(\rho_{AB}) &= \sum_i \langle i| \rho_{AB} |i\rangle \\ &= \sum_i (\langle \psi_i| U) \rho_{AB} (U^\dagger |i\rangle) \\ &= \sum_i \langle \psi_i| (U \otimes I) \rho_{AB} (U \otimes I)^\dagger) |i\rangle \\ &= Tr_A((U \otimes I) \rho_{AB} (U \otimes I)^\dagger) \end{aligned}$$

Trace partielle

$$
\begin{aligned}
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
\rho_{AB} &= \left|\Psi^+\right\rangle\left\langle\Psi^+\right| \\
&= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\ \frac{1}{\sqrt{2}}(\langle 00| + \langle 11|) \\
&= \frac{1}{2}(|00\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11| + |11\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|)
\end{aligned}
$$

$$
\begin{aligned}
\mathrm{Tr}_A(\rho_{AB}) &= \frac{1}{2}\mathrm{Tr}_A\left(|00\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11| + |11\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|\right) \\
&= \frac{1}{2}\langle 0|_A\left(|00\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11| + |11\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|\right)|0\rangle_A \\
&+ \frac{1}{2}\langle 1|_A\left(|00\rangle_{AB}\langle 00| + |00\rangle_{AB}\langle 11| + |11\rangle_{AB}\langle 00| + |11\rangle_{AB}\langle 11|\right)|1\rangle_A \\
&= \frac{1}{2}|0\rangle_B\langle 0| + \frac{1}{2}|1\rangle_B\langle 1| \\
&= \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} \\
&= \frac{1}{2}I
\end{aligned}
$$

Pour ρ_{AB} n'importe quel état de Bell

$$
\mathrm{Tr}_A(\rho_{AB}) = \mathrm{Tr}_B(\rho_{AB}) = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}
$$

Matrice de densité

Une matrice ρ est appelé matrice de densité si et seulement si:

$$\rho = \rho^\dagger \qquad Tr(\rho) = 1$$

La matrice de densité d'un état pur $|\psi\rangle$ est $|\psi\rangle \langle\psi|$.

Si une source produit l'état ρ_1 avec probabilité p et ρ_2 avec probabilité $1-p$ alors la matrice de densité de l'état obtenu est $p\rho_1 + (1-p)\rho_2$.

Toute matrice de densité représente une distribution d'états purs.

Si ρ_{AB} est un état bipartite et que l'on laisse de côté la partie A ce qui reste est dans l'état

$$Tr_A(\rho_{AB}) = \sum \langle i|_A \, \rho_{AB} |i\rangle_A$$

La matrice de densité d'un système quantique dépend de notre connaissance du système.

Entropie

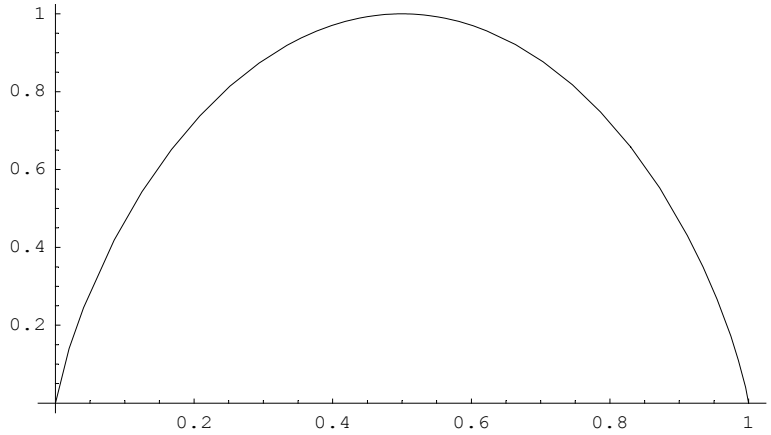
Soit X une variable aléatoire prenant la valeur $i \in \{1, \ldots, n\}$ avec probabilité p_i .

$$H(X) := \sum_{i=1}^{n} -p_i \log p_i$$

$$0 \leq H(X) \leq \log n$$

$H(X) = 0$ ssi $\exists i, p_i = 1$
$H(X) = \log n$ ssi $\forall i, p_i = 1/n$

Entropie



L'entropie $H(\{p, 1-p\})$ en fonction de p.

Entropie

Théorème:
Une source de k symboles ayant une distribution P peut être asymptotiquement encodée avec $H(P)$ bits en moyenne.

Exemple:
$k = 2$, $P(0) = 7/8$ et $P(1) = 1/8$.
$H(P) = 0.5436$.

Prenons le codage *prefix-free* suivant:
$C(000) = 0$
$C(001) = 100$
$C(010) = 101$
$C(011) = 11100$
$C(100) = 110$
$C(101) = 11101$
$C(110) = 11110$
$C(111) = 11111$

$P(000) = 0.67$, $P(001) = P(010) = P(100) = 0.96$, $P(110) = P(101) = P(011) = 0.014$ et $P(111) = 0.002$
En moyenne le message aura donc 1.75 bits de long pour 3 bit et donc 0.58 bit par symbole, ce qui est déjà proche de $H(P) = 0.5436$. En codant plus de symboles on peut s'approcher aussi proche que l'on veut de la borne.

Entropie

Soit X et Y deux variables aléatoires avec distribution conjointe $p_{(x,y)}$ où $1 \leq x \leq n$ et $1 \leq y \leq m$. Notez que $p_{(x|y)} = p_{(x,y)}/p_y$.

$$H(X,Y) := \sum_{x,y} -p_{(x,y)} \log p_{(x,y)}$$

$$H(X|Y) := \sum_{x,y} -p_{(x,y)} \log p_{(x|y)}$$

$$H(X,Y) = H(X) + H(Y|X)$$

$$H(Y|X) = H(X,Y) - H(X)$$

$$H(X,Y|Z) = H(X|Z) + H(Y|X,Z)$$

Théorème: [Shannon49]
Pour la transmission d'un message privé de n bits il est nécessaire et suffisant de partager une clef privée et aléatoire de n bits.

Preuve (suffisant):
M =message, C =cryptogramme, K =clef
Encryption de Vernam: *one-time pad*.

$$\begin{array}{rcccccc} M & = & 0 & 0 & 1 & 0 & 1 & 1 \\ K & = & 1 & 0 & 0 & 1 & 1 & 0 \\ \hline M \oplus K = C & = & 1 & 0 & 1 & 1 & 0 & 1 \\ \hline C \oplus K = M & = & 0 & 0 & 1 & 0 & 1 & 1 \end{array}$$

Connaissant seulement C, tout message possible M' est consistant avec l'utilisation de la clef $K' = M' \oplus C$. Comme $H(K) = n$ tous les messages sont équiprobables.

Théorème: [Shannon49]
Pour la transmission d'un message privé de n bits, il est nécessaire et suffisant de partager une clef privée et aléatoire de n bits.

Preuve (suffisant):
Soient M, C, K des variables aléatoires
(M =message, C =cryptogramme, K =clef)
et H l'entropie de Shannon.

$$H(K) = n \quad \rightarrow H(C|M) = n \quad \rightarrow H(C) = n$$

$$\begin{aligned} H(M|C) &= H(M,C) - H(C) \\ &= H(M,C) - n \\ &= H(C|M) + H(M) - n \\ &= n + H(M) - n \\ &= H(M) \end{aligned}$$

Theorème: [Shannon49]
Pour la transmission d'un message privé de n bits, il est nécessaire et suffisant de partager une clef privée et aléatoire de n bits.

Preuve (nécessaire):
Soit M, C, K des variables aléatoires
(M =message, C =cryptogramme, K =clef)
et H l'entropie de Shannon.

$$H(M|C,K) = 0 \qquad H(M|C) = H(M)$$

$$H(M,K|C) =$$

$$H(K|C) + H(M|K,C) = H(M|C) + H(K|M,C)$$

$$H(K|C) = H(M) + H(K|M,C)$$

$$H(K) \geq H(M)$$

Résultat principal

Théorème [AMTW00]:

Pour la transmission privée (non interactive) de n qubits, il est nécessaire et suffisant de partager une clef secrète et aléatoire de $2n$ bits.

Canal quantique privé (PQC)

Un système $[\mathcal{S} \subseteq \mathcal{H}_{2^n}, \mathcal{E} = \{(p_i, U_i) | 0 \leq i < N\}$,
$\rho_a \in \mathcal{H}_{2^m}, \rho_0 \in \mathcal{H}_{2^{m+n}}]$ forme un PQC ssi

$\forall\ |\psi\rangle \in \mathcal{S}$,

$$\mathcal{E}(|\psi\rangle \langle\psi| \otimes \rho_a) = \sum_{i=0}^{N-1} p_i U_i (|\psi\rangle \langle\psi| \otimes \rho_a) U_i^\dagger = \rho_0$$

La clef privée:

$k \in_R \{i | 0 \leq i < N\}$ avec distribution $\{p_i\}$.

Encodage:

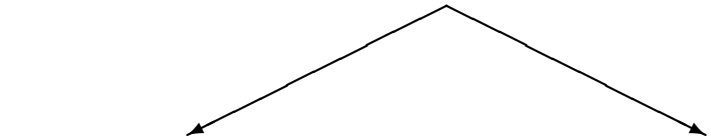
$$E(\rho, k) = U_k(\rho \otimes \rho_a) U_k^\dagger = \rho'$$

Décodage:

$$D(\rho', k) = \mathsf{Tr}_E(U_k^\dagger \rho' U_k) = \rho$$

PQC

$k \in_R \{0, \ldots, N-1\}$
avec distribution $\{p_i\}$



Alice

Bob

ρ

$\rho' \leftarrow U_k(\rho \otimes \rho_a)U_k^\dagger$

ρ'

$\rho \;=\; Tr_E(U_k^\dagger \rho' U_k)$

Eve

$\rho_0 \;=\; \sum_{i=0}^{N-1} p_i U_i(\rho \otimes \rho_a)U_i^\dagger$

PQC: Exemple 1

$$\mathcal{S} = \{|0\rangle, |1\rangle\} \qquad \rho_a = 1$$

$$\mathcal{E} = \{(1/2, I), (1/2, \sigma_x)\}$$

$$\rho_0 = \frac{1}{2} I \qquad H(\{p_i\}) = 1$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \sigma_x^\dagger$$

Clairement ce système forme un **PQC** puisque

$$\begin{aligned}
\mathcal{E}(|0\rangle\langle 0|) &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}\sigma_x|0\rangle\langle 0|\sigma_x \\
&= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| \\
&= \frac{1}{2} I = \rho_0 \\
&= \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|0\rangle\langle 0| \\
&= \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}\sigma_x|1\rangle\langle 1|\sigma_x \\
&= \mathcal{E}(|1\rangle\langle 1|)
\end{aligned}$$

PQC: Exemple 2

$$\mathcal{S} = \{|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\} \qquad \rho_a = 1$$

$$\mathcal{E} = \{(1/2, I), (1/2, W)\}$$

$$\rho_0 = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix} \qquad H(\{p_i\}) = 1$$

$$W = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = W^\dagger$$

$$W|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$W^2 = I$$

Clairement ce système forme un **PQC** puisque

$$\mathcal{E}(|0\rangle\langle 0|) = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}W|0\rangle\langle 0|W = \begin{pmatrix} 3/4 & 1/4 \\ 1/4 & 1/4 \end{pmatrix} = \rho_0$$

$$\mathcal{E}(W|0\rangle\langle 0|W) = \frac{1}{2}W|0\rangle\langle 0|W + \frac{1}{2}W^2|0\rangle\langle 0|W^2 = \rho_0$$

PQC: Exemple 3

$$\mathcal{S} = \mathcal{H}_2 \qquad \rho_a = 1$$

$$\mathcal{E} = \{(1/4, I), (1/4, \sigma_x), (1/4, \sigma_y), (1/4, \sigma_z)\}$$

$$\rho_0 = \frac{1}{2} I \qquad H(\{p_i\}) = 2$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z^\dagger$$

Clairement ce système forme un **PQC** puisque

$$\begin{aligned}
\rho &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
\sigma_x \rho \sigma_x &= \begin{pmatrix} d & c \\ b & a \end{pmatrix} \\
\sigma_y \rho \sigma_y &= \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \\
\sigma_y \rho \sigma_y &= \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
\mathcal{E}(\rho) &= \frac{1}{4} I \ \rho \ I + \frac{1}{4} \sigma_x \ \rho \ \sigma_x + \frac{1}{4} \sigma_y \ \rho \ \sigma_y + \frac{1}{4} \sigma_z \ \rho \ \sigma_z \\
&= \frac{1}{2} I
\end{aligned}$$

Lemme 1:
Si $\frac{1}{2^n} I \in \mathcal{S}$ et $\rho_a = 1$ alors $\rho_0 = \frac{1}{2^n} I$.

Preuve:

$$\rho_0 = \mathcal{E}(\frac{1}{2^n} I) = \sum_{i=0}^{N-1} p_i U_i \left(\frac{1}{2^n} I \right) U_i^\dagger = \frac{1}{2^n} I$$

Lemme 2:
Si $\forall\ |\psi\rangle \in \mathcal{H}_{2^n},\ \mathcal{E}(|\psi\rangle\langle\psi| \otimes \rho_a) = \rho_0$ alors
$\mathcal{E}(|x\rangle\langle y| \otimes \rho_a) = 0$ quand $x \neq y$.

Preuve:

$$
\begin{aligned}
1)\ \rho_0 &= \mathcal{E}(\frac{1}{2}(|x\rangle\langle x| + |y\rangle\langle y|) \\
&= \frac{1}{2}(\mathcal{E}(|x\rangle\langle x|) + \mathcal{E}(|y\rangle\langle y|)) \\
2)\ \rho_0 &= \mathcal{E}(\frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)\ \frac{1}{\sqrt{2}}(\langle x| + \langle y|)) \\
&= \frac{1}{2}(\mathcal{E}(|x\rangle\langle x|) + \mathcal{E}(|x\rangle\langle y|) + \mathcal{E}(|y\rangle\langle x|) + \mathcal{E}(|y\rangle\langle y|)) \\
3)\ \rho_0 &= \mathcal{E}(\frac{1}{\sqrt{2}}(|x\rangle + i|y\rangle)\ \frac{1}{\sqrt{2}}(\langle x| - i\langle y|)) \\
&= \frac{1}{2}(\mathcal{E}(|x\rangle\langle x|) + \mathcal{E}(|y\rangle\langle y|) - i\mathcal{E}(|x\rangle\langle y|) + i\mathcal{E}(|y\rangle\langle x|))
\end{aligned}
$$

1) et 2) $\Rightarrow\ \mathcal{E}(|x\rangle\langle y|) + \mathcal{E}(|y\rangle\langle x|) = 0$
1) et 3) $\Rightarrow\ \mathcal{E}(|x\rangle\langle y|) - \mathcal{E}(|y\rangle\langle x|) = 0$
alors $\mathcal{E}(|x\rangle\langle y|) = \mathcal{E}(|y\rangle\langle x|) = 0$.

Théorème [concaténation]
Si $[\mathcal{H}_{2^n}, \mathcal{E}, \rho_a, \rho_0]$ et $[\mathcal{H}_{2^m}, \mathcal{E}', \rho'_a, \rho'_0]$ sont des **PQC** alors $[\mathcal{H}_{2^{n+m}}, \mathcal{E} \otimes \mathcal{E}', \rho_a \otimes \rho'_a, \rho_0 \otimes \rho'_0]$ est un **PQC**.

Preuve:

$$
\begin{aligned}
&(\mathcal{E} \otimes \mathcal{E}')(|\psi\rangle \langle\psi|) \\
&= (\mathcal{E} \otimes \mathcal{E}') \left(\sum_{x,y} \alpha_{x,y} |x\rangle|y\rangle \right) \left(\sum_{x',y'} \alpha^*_{x',y'} \langle x'| \langle y'| \right) \\
&= (\mathcal{E} \otimes \mathcal{E}') \left(\sum_{x,y,x',y'} \alpha_{x,y} \ \alpha^*_{x',y'} \, |x\rangle \langle x'| \otimes |y\rangle \langle y'| \right) \\
&= \sum_{x,y,x',y'} \alpha_{x,y} \ \alpha^*_{x',y'} \ \mathcal{E}(|x\rangle \langle x'|) \otimes \mathcal{E}'(|y\rangle \langle y'|) \\
&\overset{*}{=} \sum_{x,y} \alpha_{x,y} \ \alpha^*_{x,y} \ \mathcal{E}(|x\rangle \langle x|) \otimes \mathcal{E}'(|y\rangle \langle y|) \\
&= \sum_{x,y} |\alpha_{x,y}|^2 \ \rho_0 \otimes \rho'_0 \\
&= \rho_0 \otimes \rho'_0
\end{aligned}
$$

Théorème [AMTW00, suffisant]:
Pour transmettre un message de n qubits de façon privée, il est suffisant de partager une clef privée aléatoire de $2n$ bits.

Preuve: Par le théorème [concaténation], l'encodage d'un registre de n qubits peut se faire en encodant chaque qubit en utilisant n fois le **PQC** de l'exemple 4, ce qui nécessite n clefs de 2 bits.

Entropie de von Neumann

Définition:
Soit ρ un état quantique et U une transformation unitaire quelconque, on note $p_{U,x} = \langle x| U\rho U^\dagger |x\rangle$ la probabilité d'observer $|x\rangle$ si on mesure ρ après avoir appliqué la transformation unitaire U. Alors on a que l'entropie de von Neumann de ρ est

$$S(\rho) = min_U H(p_{U,0}, p_{U,1}, \ldots, p_{U,n-1})$$

Théorème:
Soit $\rho = \sum_{i=1}^{N} p_i \, |\phi_i\rangle \langle\phi_i|$ avec $|\phi_i\rangle$ une base orthonormale. L'*entropie de von Neumann* de ρ est

$$S(\rho) = H(p_1, \ldots, p_N) = -\sum_{i=1}^{N} p_i \log p_i,$$

où H est l'entropie de Shannon.

Entropie de von Neumann

Théorème [entropie de von Neumann]

1. $S(|\phi\rangle\langle\phi|) = 0$ pour tout état pur $|\phi\rangle$.
2. $S(\rho_1 \otimes \rho_2) = S(\rho_1) + S(\rho_2)$.
3. $S(U\rho U^\dagger) = S(\rho)$.
4. $S(\sum_i \lambda_i \rho_i) \geq \sum_i \lambda_i S(\rho_i)$, $\lambda_i \geq 0$ et $\sum_i \lambda_i = 1$.
5. Si $\rho = \sum_{i=1}^N p_i \, |\phi_i\rangle\langle\phi_i|$ avec $|\phi_i\rangle$ quelconque, alors $S(\rho) \leq H(p_1, \ldots, p_N)$.
6. $S\left(\frac{1}{2^n} I\right) = n$.

Théorème [canal classique]
Si $[\mathcal{S} = \{|i\rangle \mid 0 \leq i < 2^k\}, \mathcal{E} = \{(p_i, U_i)\}, \rho_a, \rho_0]$ est un **PQC** alors $H(\{p_i\}) \geq k$.

Preuve:

$$\begin{aligned}
S(\rho_0) &= S(\mathcal{E}(|0\rangle\langle 0|) \\
&= S\left(\sum_{i=0}^{N-1} p_i U_i |0\rangle\langle 0| U_i^\dagger\right) \\
&= S\left(\sum_{i=0}^{N-1} p_i |\psi_i\rangle\langle\psi_i|\right) \\
&\leq H(\{p_i\}) \\
S(\rho_0) &= S(\mathcal{E}(\frac{1}{2^k} I)) \\
&= S(\frac{1}{2^k} I) \\
&= k
\end{aligned}$$

Théorème [AMTW00, nécessaire]:
Si $[\mathcal{S} = \mathcal{H}_{2^n}, \mathcal{E} = \{(p_i, U_i)\}, \rho_a, \rho_0]$ est un **PQC** alors $H(\{p_i\}) \geq 2n$.

Preuve:
$[\mathcal{S}' = \{|x\rangle | 0 \leq x < 2^{2n}\}, \mathcal{E}', \rho_a, \left(\frac{1}{2^n} I\right) \otimes \rho_0]$
est un **PQC** où

$$\mathcal{E}' = \{(p_i, (I_{2^n} \otimes U_i)U) | 0 \leq i < N\}$$

$$U|x\rangle = (\sigma_{x_1} \otimes \cdots \otimes \sigma_{x_n} \otimes I_{2^n}) \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n - 1} |i\rangle |i\rangle$$

et $\{0, \ldots, 2^{2n} - 1\} \equiv \{I, x, y, z\}^n$.

Par le théorème précédent on conclut que

$$H(\{p_i\}) \geq 2n.$$

L'état initial:

$$\frac{1}{\sqrt{2}}(|00\rangle_{AB}+|11\rangle_{AB})\frac{1}{\sqrt{2}}(|00\rangle_{CD}+|11\rangle_{CD})\frac{1}{\sqrt{2}}(|00\rangle_{EF}+|11\rangle_{EF})$$

Alice applique:

$$|x\rangle \longrightarrow \begin{array}{cccccc} A & C & E & B & D & F \\ \sigma_{x_1} & \sigma_{x_2} & \sigma_{x_3} & I & I & I \\ & & I & & & U_k \end{array}$$

alors du point de vue d'Ève:

$$\frac{1}{2^3} I_{2^3} \otimes \rho_0$$

$\mathcal{E}'(|x\rangle\langle x|)$

$$
\begin{aligned}
&= \sum_{i=1}^{N} p_i (I_{2^n} \otimes U_i) \left[(\overline{\sigma_x} \otimes I_{2^n}) \left(\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} |y\rangle|y\rangle \right) \left(\frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} \langle z| \langle z| \right) (\overline{\sigma_x} \otimes I_{2^n})^\dagger \right] (I_{2^n} \otimes U_i)^\dagger \\
&= (\overline{\sigma_x} \otimes I_{2^n}) \left[\frac{1}{2^n} \sum_{i=1}^{N} p_i (I_{2^n} \otimes U_i) \left(\sum_{y,z \in \{0,2^n-1\}} |y\rangle\langle z| \otimes |y\rangle\langle z| \right) (I_{2^n} \otimes U_i)^\dagger \right] (\overline{\sigma_x} \otimes I_{2^n})^\dagger \\
&= (\overline{\sigma_x} \otimes I_{2^n}) \left[\frac{1}{2^n} \sum_{y,z \in \{0,2^n-1\}} |y\rangle\langle z| \otimes \left(\sum_{i=1}^{N} p_i U_i |y\rangle\langle z| U_i^\dagger \right) \right] (\overline{\sigma_x} \otimes I_{2^n})^\dagger \\
&= (\overline{\sigma_x} \otimes I_{2^n}) \left[\frac{1}{2^n} \sum_{y,z \in \{0,2^n-1\}} |y\rangle\langle z| \otimes \mathcal{E}(|y\rangle\langle z|) \right] (\overline{\sigma_x} \otimes I_{2^n})^\dagger \\
&\overset{*}{=} (\overline{\sigma_x} \otimes I_{2^n}) \left[\frac{1}{2^n} \sum_{y=0}^{2^n-1} |y\rangle\langle y| \otimes \mathcal{E}(|y\rangle\langle y|) \right] (\overline{\sigma_x} \otimes I_{2^n})^\dagger \\
&= (\overline{\sigma_x} \otimes I_{2^n}) \left[\tilde{I}_{2^n} \otimes \rho_0 \right] (\overline{\sigma_x} \otimes I_{2^n})^\dagger \\
&= \tilde{I}_{2^n} \otimes \rho_0 .
\end{aligned}
$$

Différents types de canaux secrets

Message	Clef	Cryptogramme	
C	Q	Q	Codage dense
Q	C	Q	PQC
Q	Q	C	Téléportation

Téléportation

Dans la téléportation, Alice et Bob partagent l'état

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

et donc le qubit de Bob est dans l'état $\frac{1}{2}I$.

Alice possède un état $|\psi\rangle$.

Une fois l'état mesuré par Alice mais avant la transmission classique nous avons vue que si Alice obtient
00 alors Bob possède maintenant $|\psi\rangle$
01 alors Bob possède maintenant $N|\psi\rangle$
10 alors Bob possède maintenant $Z|\psi\rangle$
11 alors Bob possède maintenant $ZN|\psi\rangle$

chacun de ces résultats est obtenu avec la même probabilité et donc Bob possède le mélange

$$S = \{(1/4, |\psi\rangle), (1/4, N|\psi\rangle), (1/4, Z|\psi\rangle), (1/4, ZN|\psi\rangle)\}$$

qui est représenté par la matrice de densité $\rho = \frac{1}{2}I$ et donc évidemment la mesure d'Alice n'a pas réellement changé l'état de Bob, du moins avant qu'il n'apprenne les deux bits classiques de Alice.

Conclusion

Théorème: [Shannon49]
Pour la transmission d'un message privé de n bits il est nécessaire et suffisant de partager une clef privée et aléatoire de n bits.

Théorème: [AMTW00]
Pour la transmission privée (non interactive) de n qubits il est nécessaire et suffisant de partager une clef secrète et aléatoire de $2n$ bits.