COLLÈGE DE FRANCE
1530

Algorithmes quantiques

Cryptographie et communication quantiques

14-04-2021

Frédéric Magniez

Professeur invité sur la chaire Informatique et sciences numériques

En partenariat avec Inria

Année académique 2020-2021

frederic.magniez@college-de-france.fr

Partie I - Bases indispensables

- Premiers paradoxes quantiques
- Fondements de la cryptographie et de la communication quantiques

07 avril 2021 — **Cours :** Information quantique, premières utilisations calculatoires : superposition, mesure, transformation, non-clonage, distribution quantique de clés

Séminaire : Réseaux de communication quantique, Eleni DIAMANTI, *CNRS, Paris*

14 avril 2021 — **Cours :** Cryptographie et communication quantiques : inégalités de Bell, tirage à pile ou face, mise en gage, certification

Séminaire : Certifier la génération de nombres aléatoires avec le quantique Thomas VIDICK, *California Institute of Technology*

Paradoxe d'Einstein, Podolsky, Rosen 1935

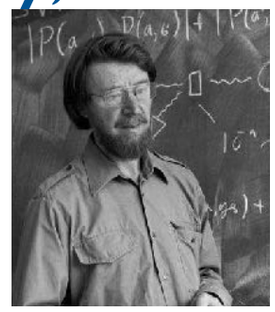

A. Einstein B. Podolsky N. Rosen

- Des particules très éloignées restent-elles liées !?

  L'observation d'une particule semble influencer l'autre instantanément

  Exemple de la paire EPR : $(|00\rangle + |11\rangle)/\sqrt{2}$

Inégalités de Bell 1964, puis Clauser, Horne, Shimony, Holt


John Bell

- Une proposition d'expérience pour départager entre

  Localité et variables cachées

  Non localité de la physique quantique

- Expérience réalisée de façon suffisamment rigoureuse pour convaincre

  Aspect, Grangier, Roger, Dalibard'80-82 (Orsay)

- Expériences sans aucune hypothèse en 2015

  Photons, distance 58m, Vienne

  Photons, distance 185m, Boulder

  Spins, distance 1,3km, Delft


Matériel de l'expérience d'Aspect à Orsay'82

Utilisation en informatique (pour ce cours)

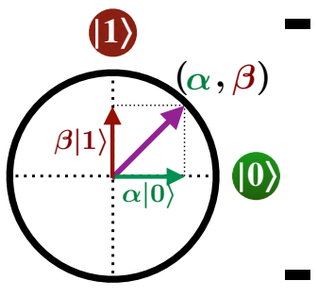
- Jeux quantiques, protocoles cryptographiques avancés
- Certification

Superposition quantique : Recap et généralisation 1/2

1-qubit

- 2 valeurs classiques : b=0, 1
- Superposition sur {0,1}

  Vecteur à 2 coordonnées α, β complexes $|\alpha|^2 + |\beta|^2 = 1$



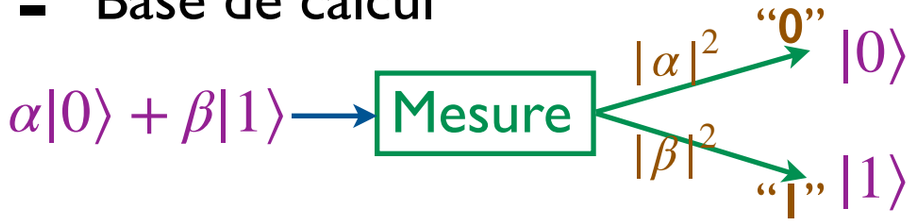
- Notation Dirac

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

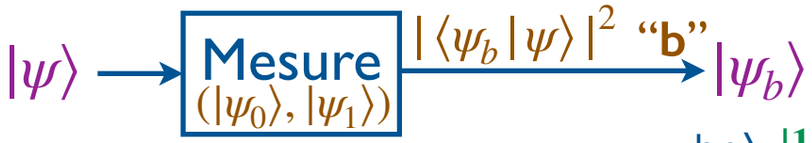
$$\alpha = \langle 0|\psi\rangle, \quad \beta = \langle 1|\psi\rangle$$

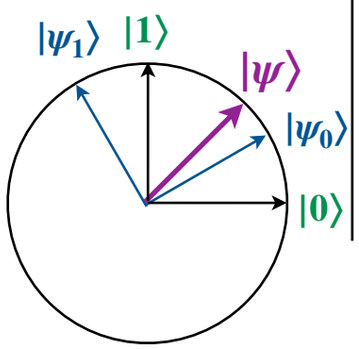
Mesures

- Base de calcul



- Base $|\psi_0\rangle \perp |\psi_1\rangle$





Cas général

- S : ensemble d'états classiques

  S={0,1}, S={0,1}^{n}, S={1,…,N}

- Superposition sur S

  Vecteur à |S| coordonnées complexes $(\alpha_x)_{x\in S}$

- Notation Dirac

$$|\psi\rangle = \sum_{x\in S} \alpha_x |x\rangle, \quad \alpha_x = \langle x|\psi\rangle$$

Mesures

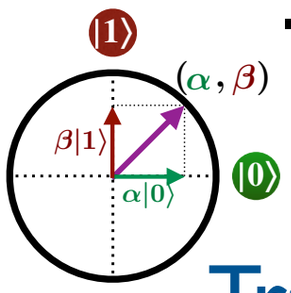
- Base de calcul

- Base orthonormée $(|\psi_x\rangle)_{x\in S}$

Superposition quantique : Recap et généralisation 2/2

1-qubit

- 2 valeurs classiques : b=0, 1
- Superposition sur {0,1}



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
$$\alpha = \langle 0|\psi\rangle, \quad \beta = \langle 1|\psi\rangle$$

Transformations unitaires

- Rotations et symétries G

$$|b\rangle \dashrightarrow \boxed{G} \dashrightarrow |\psi_b\rangle$$
$$\alpha|0\rangle + \beta|1\rangle \dashrightarrow \boxed{G} \dashrightarrow \alpha|\psi_0\rangle + \beta|\psi_1\rangle$$

avec $|\psi_0\rangle \perp |\psi_1\rangle$ base

- Notation matricielle

$$G = \left(|\psi_0\rangle, |\psi_1\rangle\right) = \begin{pmatrix} \langle 0|\psi_0\rangle & \langle 0|\psi_1\rangle \\ \langle 1|\psi_0\rangle & \langle 1|\psi_1\rangle \end{pmatrix}$$

Cas général

- S : ensemble d'états classiques
- Superposition sur S

$$|\psi\rangle = \sum_{x\in S} \alpha_x |x\rangle, \quad \alpha_x = \langle x|\psi\rangle$$

Transformations unitaires

- Rotations et symétries G

$$|x\rangle \dashrightarrow \boxed{G} \dashrightarrow |\psi_x\rangle$$
$$\sum_{x\in S} \alpha_x |x\rangle \dashrightarrow \boxed{G} \dashrightarrow \sum_{x\in S} \alpha_x |\psi_x\rangle$$

avec $(|\psi_x\rangle)_{x\in S}$ base orthonormée

- Notation matricielle

$$G = \left(|\psi_x\rangle\right)_{x\in S} = \left(\langle x|\psi_y\rangle\right)_{x,y\in S}$$

$$|\psi\rangle \dashrightarrow \boxed{G} \dashrightarrow G|\psi\rangle$$

- G unitaire : $G^* = ({}^t\overline{G}) = G^{-1}$

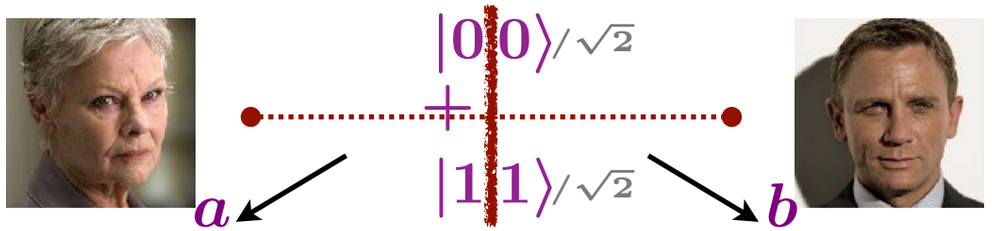
Corrélations quantiques

Etat enchevêtré / intriqué

Scenario

- Alice & Bob partagent un état EPR : $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

  Alice détient le 1er qubit, et Bob le second



- Alice & Bob observent leur qubit et obtiennent respectivement *a,b*

Remarques

- *a*=*b* avec probabilité 1
- *a* (resp. *b*) sont des bits aléatoires non biaisés

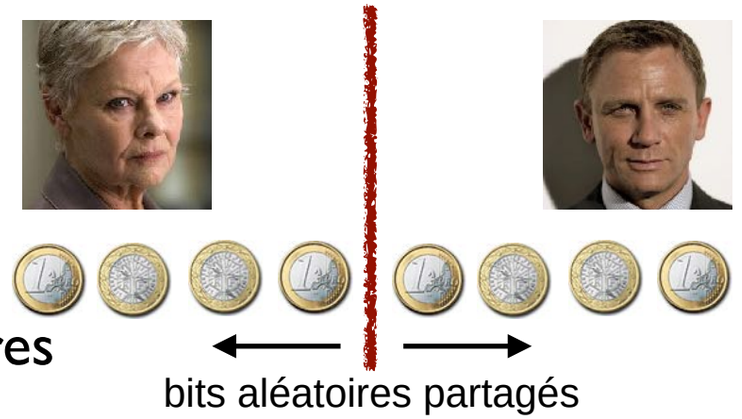
Analogue classique ?

- Aléa partagé (ou variable cachée en physique) :

  Alice & Bob ont accès aux mêmes bits aléatoires

  → Probabilités dépendantes :

  00 with prob. 1/2 and 11 with prob. 1/2

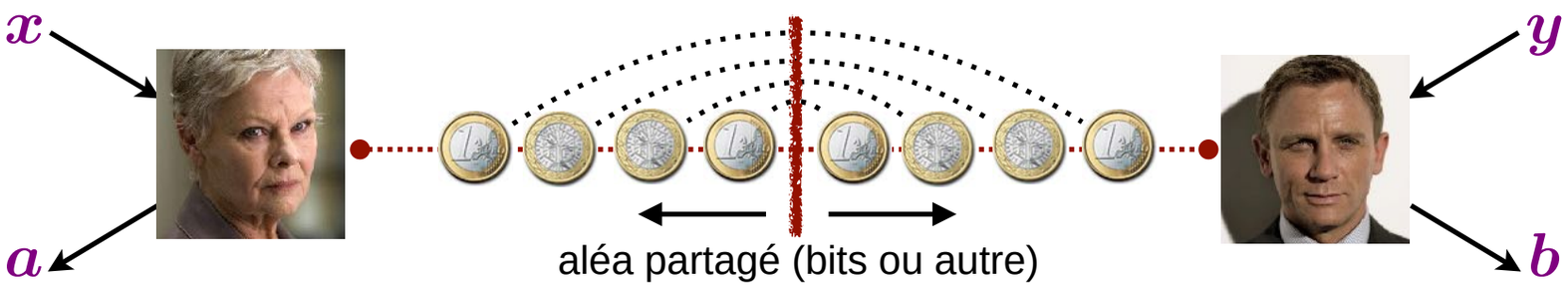


- Peut-on simuler l'enchevêtrement quantique avec de l'aléa partagé ?

Inégalité CHSH

Jeu

- Alice et Bob partage des bits aléatoires, mais ne communiquent pas
- Alice reçoit un bit x, et Bob y, tous deux aléatoires non biaisés
- Alice renvoie un bit a, et Bob b



- Objectif : Satisfaire $a \oplus b = x \wedge y$

  (ou encore : a=b quand xy≠11, et a≠b quand xy=11)
- Probabilité de gain à maximiser :

$$p = \Pr_{x,y}(a \oplus b = x \wedge y)$$

⊕	0	1
0	0	1
1	1	0

∧	0	1
0	0	0
1	0	1

Inégalité CHSH [Clauser, Horne, Shimony, Holt'69]

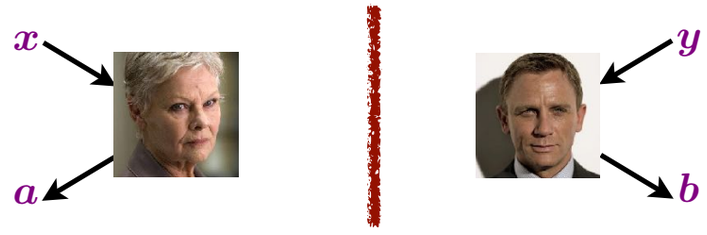
- Toute stratégie quantique locale avec aléa partagé (ie variable cachée)

  est limitée par $p \leq 3/4$

Analyse 1/3 : cas déterministe

Modélisation

- Réponse d'Alice à la question x : a(x)
- Réponse de Bob à la question y : b(y)



Gain si a⊕b=x∧y
- a=b quand xy≠11
- a≠b quand xy=11

Solution avec p=3/4

- a(0)=a(1)=b(1)=b(0)=0
- Pour xy≠11 : gain
- Pour xy=11 : perte
- Au total p=3/4

Il n'est pas possible de toujours gagner

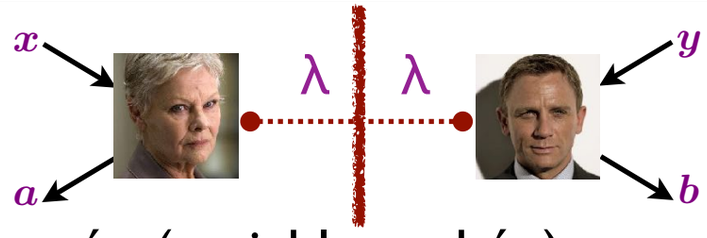
- Par l'absurde

  Lorsque xy≠11 : b(1)=a(0)=b(0)=a(1)

  Lorsque xy=11 : b(1)≠a(1)

Donc la probabilité de gain est au plus p≤3/4

Analyse 2/3 : cas probabiliste



Modélisation

- Supposons l'accès à une variable probabiliste λ partagée (variable cachée)
- Les réponses sont maintenant dépendantes de λ

  Réponse d'Alice à la question x : a(x, λ)

  Réponse de Bob à la question y : b(y, λ)

Gain si $a \oplus b = x \wedge y$
- a=b quand xy≠11
- a≠b quand xy=11

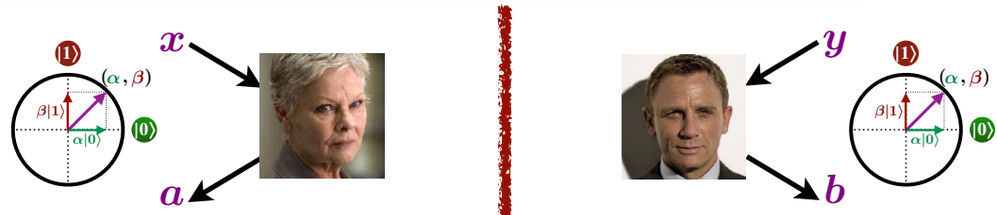
Analyse

- Soit p_λ la probabilité de gain à λ fixée
- La probabilité de gain total est donc la moyenne

  p = Moyenne(p_λ) lorsque λ varie selon sa loi de probabilité
- Donc $p \leq \text{Max}(p_\lambda)$
- Mais lorsque λ est fixée, la stratégie est déterministe

  et donc $p_\lambda \leq 3/4$
- Conclusion $p \leq 3/4$

Analyse 3/3 : cas quantique local

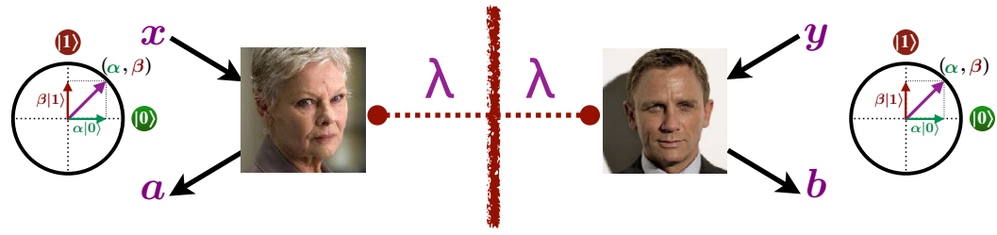


Modélisation

- Alice et Bob utilisent des ressources quantiques mais non partagées
- Les réponses sont maintenant des réponses probabilistes (indépendantes)

  Réponse d'Alice à la question x : A(x)

  Réponse de Bob à la question y : B(y)



Simulation

- Il n'y a plus rien de quantique !
- Soit λ la variable aléatoire formée de 4 registres et distribuée

  selon [A(0),A(1),B(0),B(1)]
- Alice et Bob peuvent simuler une réponse "quantique locale" avec λ

Extension

- Le cas quantique local avec aléa partagé ne change rien

  il reste un cas particulier du cas déterministe avec aléa partagé !

Théorème final

- La meilleure stratégie quantique avec aléa partagée ne peut faire mieux que la meilleure stratégie déterministe, et donc $p \leq 3/4$.

Inégalité CHSH, cas quantique

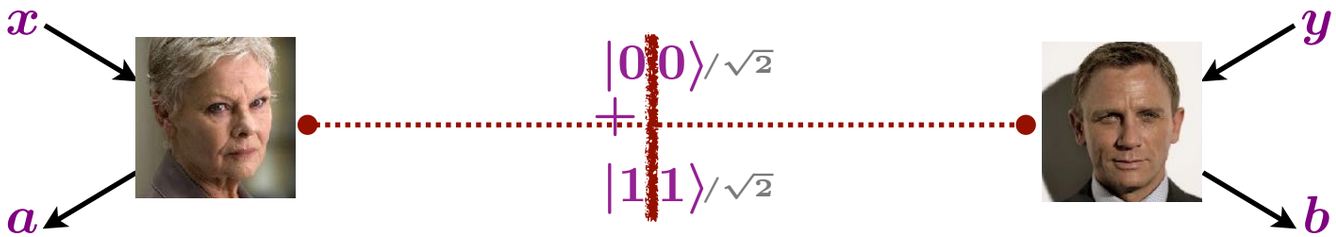
Gain si $a \oplus b = x \wedge y$
- a=b quand xy≠11
- a≠b quand xy=11

Rappel

- Objectif : maximiser la probabilité p de gagner

Stratégie quantique optimale

- Alice et Bob partagent un état EPR



- Bob effectue une rotation d'angle π/8
- Si x=1, Alice effectue une rotation d'angle π/4
- Si y=1, Bob effectue une rotation d'angle -π/4
- Alice et Bob observent leur qubit respectif et renvoient leur résultat

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

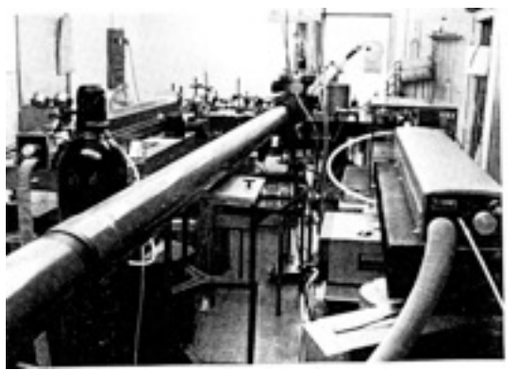
y\x	0	1
0	$\|\beta_{0,\frac{\pi}{8}}\rangle$	$\|\beta_{\frac{\pi}{4},\frac{\pi}{8}}\rangle$
1	$\|\beta_{0,-\frac{\pi}{8}}\rangle$	$\|\beta_{\frac{\pi}{4},-\frac{\pi}{8}}\rangle$

Théorème

- Cette stratégie réalise $p = \cos^2(\frac{\pi}{8}) \approx 0{,}854$
- De plus, aucune stratégie ne peut faire mieux [Tsirelson'80]

Réalisation

[Aspect-Grangier-Roger-Dalibard: Orsay'80-82]



Registres multiples 1/3 : produit tensoriel

Vision multi-registre

- A,B : ensembles d'états classiques
- S=AxB={(x,y): x∈A,y∈B} ensemble des états combinés
- Superposition sur AxB

  Vecteur $(\gamma_{x,y})_{x\in A,y\in B}$

- Notation Dirac

$$|\psi\rangle = \sum_{x\in A,y\in B} \gamma_{x,y}|x,y\rangle$$

Vision équivalente !

Vision produit tensoriel

- Superposition sur A

  Vecteur $(\alpha_x)_{x\in A}$

$$|\psi_1\rangle_A = \sum_{x\in A} \alpha_x|x\rangle_A$$

- Superposition sur B

  Vecteur $(\beta_y)_{y\in B}$

$$|\psi_2\rangle_B = \sum_{y\in B} \beta_y|y\rangle_B$$

- Superposition produit sur AxB

$$|\psi_1\rangle_A \otimes |\psi_2\rangle_B = \sum_{x\in A,y\in B} \alpha_x\beta_y|x\rangle_A \otimes |y\rangle_B$$

- Superposition générale

$$|\psi\rangle_{AB} = \sum_{x\in A,y\in B} \gamma_{x,y}|x\rangle_A \otimes |y\rangle_B$$

Si non produit, alors enchevêtrée (ou intriquée)

Transformations unitaires

- A,B : ensembles d'états classiques
- G_A une transformation unitaire sur les superpositions de A
- G_B une transformation unitaire sur les superpositions de B
- $G_A \otimes G_B$ est défini sur les états séparés

$$(G_A \otimes G_B)\left(|\psi_1\rangle_A \otimes |\psi_2\rangle_B\right) = G_A\left(|\psi_1\rangle_A\right) \otimes G_B\left(|\psi_2\rangle_B\right)$$

et étendu par linéarité

$$(G_A \otimes G_B)\left(\sum_{xy} \gamma_{xy}|x,y\rangle_{AB}\right) = \sum_{xy} \gamma_{xy} G_A\left(|x\rangle_A\right) \otimes G_B\left(|y\rangle_B\right)$$

Remarques

- Faire une opération G_A sur A, revient à faire l'opération $G_A \otimes Id_B$ sur AxB
- Les transformations G_A sur A commutent avec les opérations G_B sur B

Mesures partielles (sur le 1er registre)

- A,B : ensembles d'états classiques
- Méthode 1 : se ramener à une décomposition sur la base de A

$$\sum_{x\in A} \alpha_x |x\rangle_A |\psi_x\rangle_B \rightarrow \boxed{\text{Mesure A}} \xrightarrow{|\alpha_x|^2 \text{ “x”}} |x\rangle_A |\psi_x\rangle_B$$

- Méthode 2 : se ramener aux projecteurs associés à la mesure

$|x\rangle\langle x|$ est un projecteur orthogonal sur $|x\rangle$

$(|x\rangle\langle x|)|y\rangle = |x\rangle(\langle x|y\rangle) = |x\rangle$ si y=x et $\vec{0}$ sinon

Soit $P_x = |x\rangle\langle x|_A \otimes \mathrm{Id}_B$ alors

$$|\psi\rangle \rightarrow \boxed{\text{Mesure A}} \xrightarrow{\|P_x|\psi\rangle\|^2 \text{ “x”}} P_x|\psi\rangle / \|P_x|\psi\rangle\|$$

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

Remarques

- Les mesures sur A et B commutent
- Mesurer sur A puis B, est identique à mesurer sur AxB

Exercice 1

- Montrer qu'effectuer une transformation unitaire U sur le premier qubit de $|\beta_{00}\rangle$ est équivalent à effectuer la transformation ${}^tU$ sur le deuxième qubit.

  Posons $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

  Alors $U \otimes I|\beta_{00}\rangle = (a|0\rangle + c|1\rangle) \otimes |0\rangle/\sqrt{2} + (b|0\rangle + d|1\rangle) \otimes |1\rangle/\sqrt{2}$.

  Développons et factorisons :

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

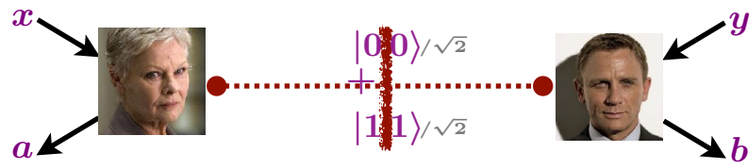
  Nous avons donc $U \otimes I|\beta_{00}\rangle = I \otimes {}^tU|\beta_{00}\rangle$, avec ${}^tU = \begin{pmatrix} a & \boldsymbol{c} \\ \boldsymbol{b} & d \end{pmatrix}$.

Exercice 2

- La probabilité d'observer 0 ou 1 sur le premier qubit de $|\beta_{00}\rangle$ est 1/2. Quand est-il dans une autre base ?

  Changer de base, revient à appliquer d'abord une transformation unitaire puis faire une mesure dans la base de calcul.
  Mais cette transformation unitaire peut être déportée sur le 2e qubit d'après l'exercice précédent.
  Donc ce changement de base n'affecte pas le résultat de la mesure !

Inégalité CHSH, cas quantique : analyse



Stratégie quantique

- Alice et Bob partagent un état EPR
- Bob effectue une rotation d'angle π/8
- Si x=1, Alice effectue une rotation d'angle π/4
- Si y=1, Bob effectue une rotation d'angle -π/4
- Alice et Bob observent leur qubit respectif et renvoient leur résultat

Gain si a⊕b=x∧y
- a=b quand xy≠11
- a≠b quand xy=11

Analyse

- Les 4 états possibles sont :

y\x	0	1
0	$\|\beta_{0,\frac{\pi}{8}}\rangle$	$\|\beta_{\frac{\pi}{4},\frac{\pi}{8}}\rangle$
1	$\|\beta_{0,-\frac{\pi}{8}}\rangle$	$\beta_{\frac{\pi}{4},-\frac{\pi}{8}}\rangle$

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

- En utilisant que la transposée d'une rotation est son inverse, et la propriété $U \otimes I|\psi\rangle = I \otimes {}^tU|\psi\rangle$ de l'état EPR, ce tableau se simplifie en

y\x	0	1
0	$\|\beta_{0,\frac{\pi}{8}}\rangle$	$\|\beta_{\frac{\pi}{8},0}\rangle$
1	$\|\beta_{\frac{\pi}{8},0}\rangle$	$\|\beta_{\frac{\pi}{2},\frac{\pi}{8}}\rangle$

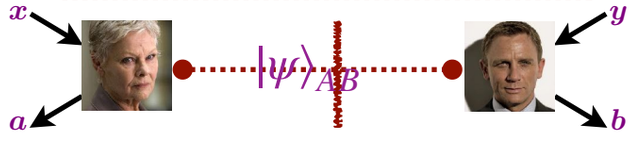
- Il n'y a donc qu'un seul cas

  Si Alice mesure 0 alors le qubit de Bob est réduit à $\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle$. Il observera donc 0 avec probabilité $\cos^2(\frac{\pi}{8})$.

- Conclusion : $p = \cos^2(\pi/8)$

Rigidité du "jeu CHSH"

Gain si $a \oplus b = x \wedge y$
- a=b quand xy≠11
- a≠b quand xy=11



Théorème

Preuve en fin de cours

- Toute stratégie quantique est limitée

  par $p \leq \cos^2(\frac{\pi}{8}) \approx 0{,}854$ [Tsirelson'80]

- Il y a unicité de la stratégie permettant d'obtenir

  $p = \cos^2(\pi/8)$ à une isométrie près… [Mayers, Yao'98,'04]

  (avec quelques hypothèses de plus mais supprimées depuis)

Remarques

- Ce théorème est robuste aux erreurs [Magniez, Mayers, Mosca, Ollivier'06]…[McKague, Yang, Scarani'12]

  Si $p \approx \cos^2(\pi/8)$ alors la stratégie est proche de la stratégie optimale

- Enormément d'applications dont

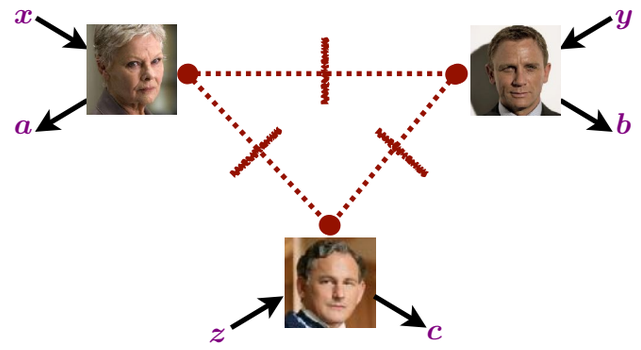
  Device-independent quantum cryptography

  Quantum self-testing

  Certifiable randomness → Séminaire de Thomas Vidick !

  Delegated quantum computation…

Paradoxe GHZ



Jeu

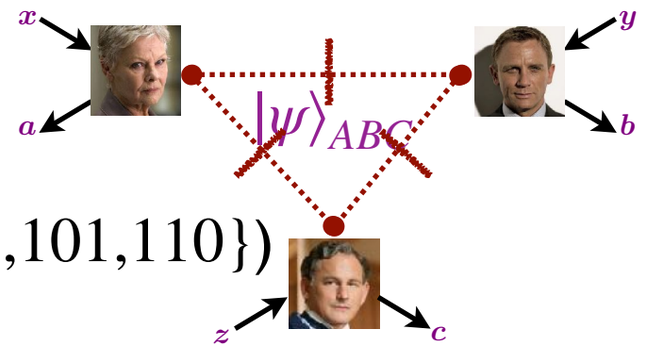
- Alice, Bob et Charlie partagent une information initiale
  mais ne communiquent pas
- Alice, Bob et Charlie reçoivent un bit aléatoire : x, y, z
- Contrainte : $x \oplus y \oplus z = 0$ (ou encore $xyz \in \{000,011,101,110\}$)
- Alice, Bob et Charlie renvoient un bit : a, b, c
- Objectif : Satisfaire $a \oplus b \oplus c = x \vee y \vee z$
  (ou encore : abc a un nombre pair de 1 quand $xyz = 000$, et un nombre impair de 1 sinon)

Classiquement

- La probabilité de succès maximale est 3/4

Quantiquement

- Il existe un protocole qui gagne le jeu avec probabilité 1



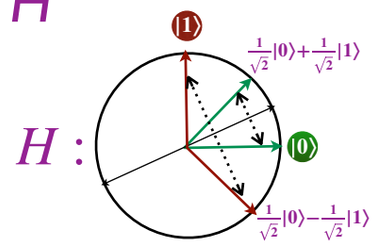
Jeu

- Contrainte : $x \oplus y \oplus z = 0$ (ou encore $xyz \in \{000,011,101,110\}$)
- Objectif : Satisfaire $a \oplus b \oplus c = x \vee y \vee z$

Stratégie quantique

- Alice, Bob et Charlie partagent $|\psi\rangle_{ABC} = (|000\rangle - |011\rangle - |101\rangle - |110\rangle)/2$
- Pour Alice/Bob/Charlie : Si le bit reçu est 1 alors appliquer la porte H

  Puis observer et renvoyer le résultat



Analyse : Probabilité 1 de succès dans tous les cas

- Cas xyz=000 : 000, 011, 101 et 110 ont tous un nombre pair de 1
- Cas xyz=011 : $|0\rangle(|00\rangle - |11\rangle)/2 - |1\rangle(|01\rangle + |10\rangle)/2$

  Mais

  $H \otimes H(|00\rangle - |11\rangle) = (|0\rangle + |1\rangle)^{\otimes^2}/2 + (|0\rangle - |1\rangle)^{\otimes^2}/2 = |01\rangle + |10\rangle$

  Donc l'état final est

  $|0\rangle(|01\rangle + |10\rangle)/2 - |1\rangle(|00\rangle - |11\rangle)/2$

  001, 010, 100 et 111 ont tous un nombre impair de 1
- Cas xyz=101,110 symétriques de 011

Motivation

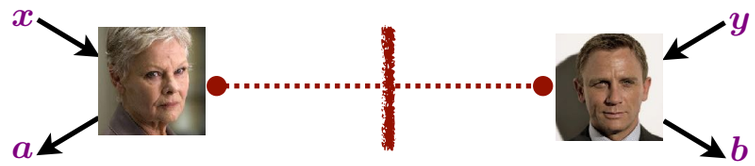
- Expliquer la physique quantique à partir de 2 principes

  Possibilité de non-localité

  Pas de communication sans interaction (non-signaling)

Jeu CHSH

- Localité et variables cachées : $p \leq 3/4$
- Corrélations quantiques : $p \leq \cos^2(\pi/8)$



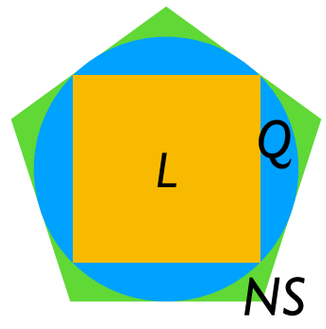
Gain si a⊕b=x∧y
- a=b quand xy≠11
- a≠b quand xy=11

Corrélations non-communicantes

- Nouvelle borne : $p \leq 1$ [Popescu, Rohrlich'94]

  Si xy≠11, alors ab=00 ou ab=11 avec proba. 1/2

  Si xy=11, alors ab=01 ou ab=10 avec proba. 1/2



- Pas de signification "physique" mais

  Les corrélations ne communiquent pas !

  Peu importe la valeur de y (resp. x), le bit a (resp. b) est non biaisé

- Une théorie de l'information riche [Barrett, Linden, Massar, Pironio, Popescu, Roberts'05]

Cryptographie quantique

Problème

- Alice et Bob sont distants
- Ils veulent tirer à pile ou face de façon équitable

  mais ils ne se font pas confiance

Applications

- *Mental Poker* [Shamir, Rivest, Adleman'79]
- *Coin flipping by telephone a protocol for solving impossible problems* [Blum'81]
- *How to generate and exchange secrets* [Yao'86]
- Une nouvelle cryptographie distribuée sans confiance mutuelle [Goldreich, Micali, Wigderson'87]

  Secure multipartite computation / Secure function evaluation
- A l'aide de primitives plus évoluées

  Mise en gage / Transfert équivoque / …

  Mais commençons par une primitive a priori simple…

Problème

- Alice et Bob sont distants
- Ils veulent tirer à pile ou face de façon équitable

  mais ils ne se font pas confiance

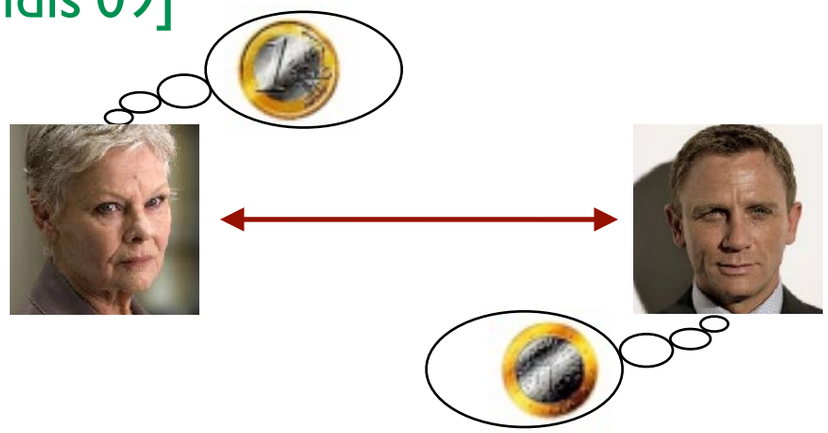
Classiquement

- Solutions basées sur la difficulté supposée de problèmes combinatoires
- Aucune alternative n'est possible

Quantiquement

- Il existe un protocole avec un biais d'au plus 0,25 [Ambainis'01]
- Aucun protocole ne peut garantir un biais meilleur que 0,207 [Kiatev'02]

  Il existe un tel protocole [Chailloux, Kerenidis'09]



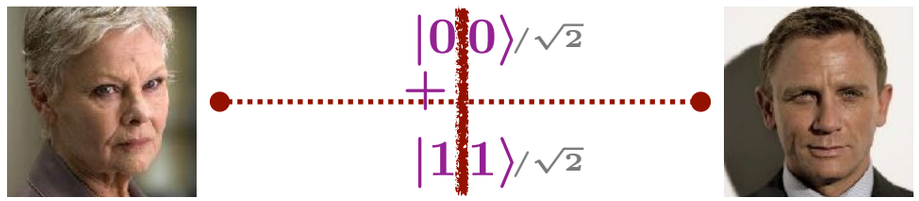
Version faible : élection

- Alice veut face
- Bob veut pile
- Il existe un protocole avec un biais arbitrairement petit [Mochon'07]…

Idée principale

- Si Alice & Bob partageait un état EPR

  Il suffirait qu'ils observent leur qubit respectif



  Alice & Bob auraient chacun a et b

  avec a=b et aléatoire sans biais

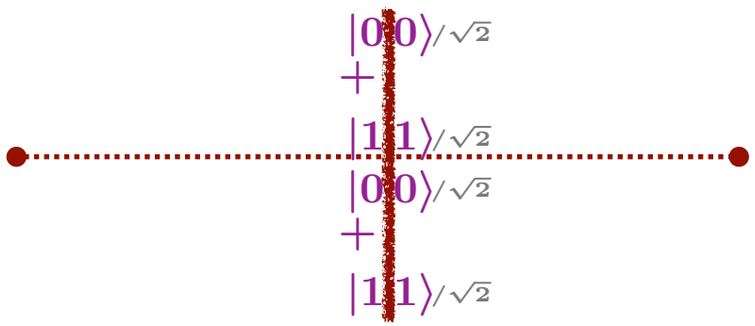
Problèmes

- Qui crée l'état EPR ?
- Si c'est Alice, Bob doit vérifier qu'il s'agit bien d'un état EPR

  Si par exemple l'état est $|00\rangle$ alors a=b=0 avec probabilité 1
- Pour vérifier l'état EPR, Bob a donc besoin du 2e qubit

  mais il peut alors tricher à son tour lorsqu'il le renvoie à Alice

Pile ou face avec 2 états EPR (protocole de Høyer-Salvail)



Protocole

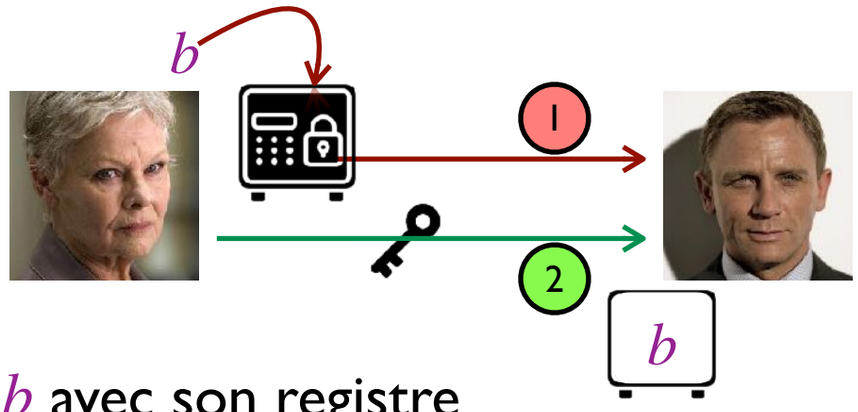
- Initialisation
  - Alice prépare 2 états EPR
  - Alice envoie le 2e qubit de chaque état
- Sélection
  - Bob choisit une des paires pour le pile ou face, et l'annonce à Alice
  - Alice & Bob observent leur qubit pour avoir le résultat du pile ou face
- Vérification : l'autre paire est utilisée pour vérifier l'honnêteté d'Alice
  - Alice envoie à Bob le qubit manquant de la paire
  - Bob fait une mesure de Bell
    - Si le résultat identifie comme étant correct, Bob accepte
    - Sinon, Bob déclare qu'Alice a triché

Théorème

- Si les deux participants sont honnêtes le résultat est aléatoire sans biais
- Si un des participants est malhonnête, le biais maximal est 1/4
- Attaques : Bob mesure les 2 qubits, et choisit celui qui donne 0 (si possible)

  Alice prépare et utilise $\frac{|00\rangle|\text{EPR state}\rangle}{\sqrt{3}} + \frac{|\text{EPR state}\rangle|00\rangle}{\sqrt{3}}$

Primitive [Brassard, Chaum, Crépeau'88]



1. Phase 1 : Mettre en gage

   Alice veut mettre en gage un bit b

   Contrainte : Bob ne peut rien apprendre de b avec son registre

2. Phase 2 : Révéler

   Alice révèle b et Bob vérifie que la mise en gage correspond

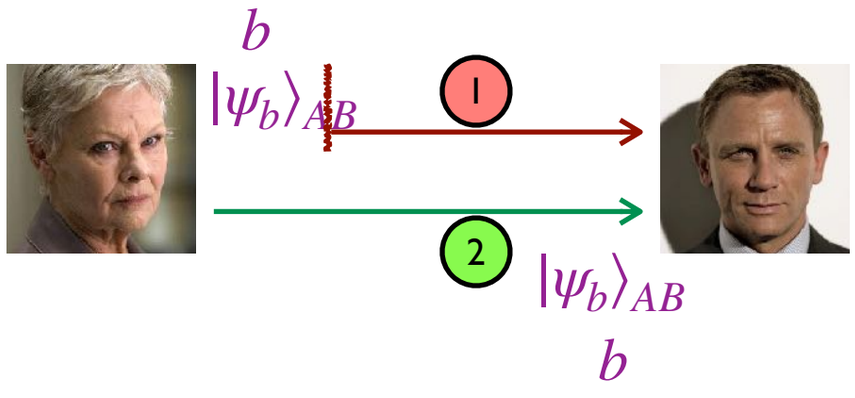
   Contrainte : Alice ne peut changer de mise en gage

Remarques

- Primitive fondamentale pour des tâches cryptographiques *modernes*, dont les preuves sans divulgation (zero-knowledge proofs)
- Solutions classiques basées sur la difficulté supposée de problèmes combinatoires
- Existe-t-il une alternative quantique ?

Mise en gage quantique : formalisation simplifiée

Primitive



1. Phase 1 : Mettre en gage d'un bit b

   Alice prépare un état $|\psi_b\rangle_{AB}$ a 2 registres

   et envoie un des registres à Bob

   Contrainte 1 : Bob ne peut rien apprendre de b avec son registre

2. Phase 2 : Révéler

   Alice envoie b et son registre à Bob

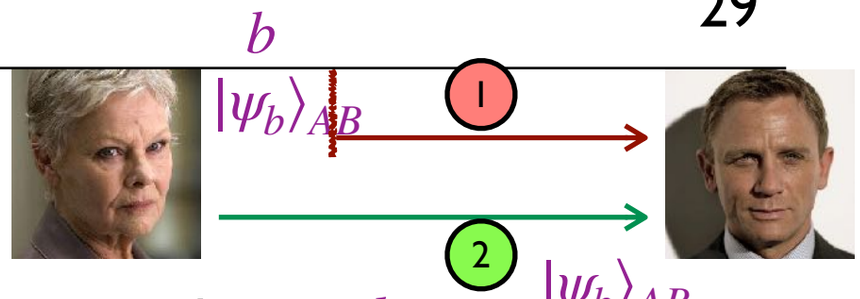
   Bob vérifie que la mise en gage correspond

   Contrainte 2 : Alice ne peut changer de mise en gage

Conséquence des contraintes

- 1 : Une mesure de Bob sur $|\psi_b\rangle_{AB}$ ne doit rien apprendre sur b
- 2 : Pas d'incertitude sur la valeur de b : $|\psi_0\rangle_{AB} \perp |\psi_1\rangle_{AB}$

Mise en gage : tentative



Contraintes

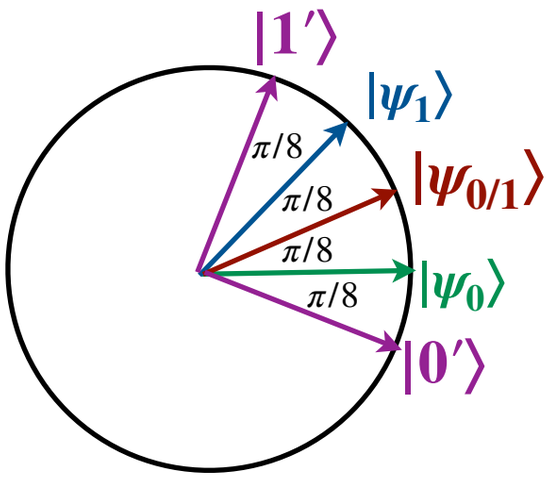
- Une mesure sur de Bob sur $|\psi_b\rangle_{AB}$ ne doit rien apprendre sur b
- Pas d'incertitude sur la valeur de b : $|\psi_0\rangle_{AB} \perp |\psi_1\rangle_{AB}$

Essai 1

- $|\psi_0\rangle_{AB} = (|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$ et $|\psi_1\rangle_{AB} = (|00\rangle_{AB} - |11\rangle_{AB})/\sqrt{2}$
- Mais Alice peut passer de l'un à l'autre !

Essai 2

- Sans registre A : $|\psi_0\rangle_B = |0\rangle$ et $|\psi_1\rangle_B = (|0\rangle + |1\rangle)/\sqrt{2}$
- Bob peut deviner b avec probabilité $\cos^2(\pi/8) = 0{,}854$
- Alice peut aussi tricher avec probabilité $\cos^2(\pi/8) = 0{,}854$



Théorème

- Il est impossible de réaliser une mise en gage quantique inconditionnellement sure [Mayers'97, Lo, Chau'97]
- Il existe une mise en gage quantique qui garantit une tricherie d'au plus 0,739, cette valeur est de plus optimale [Chailloux, Kerenidis'11]

Jeu CHSH

Optimalité de la stratégie quantique

$$p \leq \cos^2(\frac{\pi}{8}) \approx 0{,}854$$

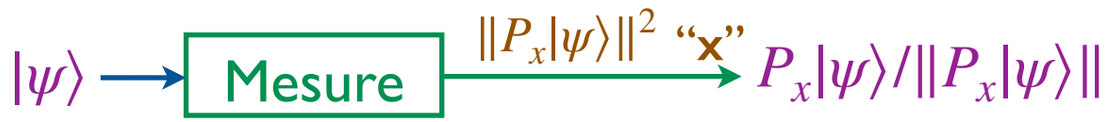
Context

- Superposition sur un ensemble S

$$|\psi\rangle = \sum_{x \in S} \alpha_x |x\rangle, \quad \alpha_x = \langle x \,|\, \psi \rangle$$

Mesures totales revisitées

- Projecteurs associés à la mesure $P_x = |x\rangle\langle x|$



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

Mesures partielles à k sorties

- $P_1, P_2, \ldots, P_k$ décomposant orthogonalement l'espace des superpositions

$$P_1 + P_2 + \ldots + P_k = \mathrm{Id} \qquad P_i P_i = P_i, \qquad P_i P_j = 0 \quad \text{if } i \neq j$$

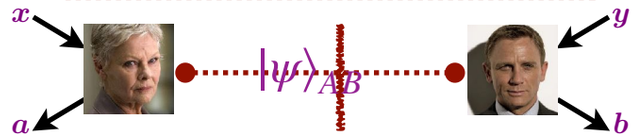
$\|P_i|\psi\rangle\|^2 = \langle\psi|P_i|\psi\rangle$

- Exemple : S= $\{0,1\}^n$, k=2

  P_0 = projection orthogonale sur les superpositions tq 1er bit = 0

  P_1 = projection orthogonale sur les superpositions tq 1er bit = 1

Gain si $a \oplus b = x \wedge y$
- a=b quand xy≠11
- a≠b quand xy=11



Cas général

- Alice et Bob partagent un état quelconque $|\psi\rangle_{AB}$
- Alice / Bob fait une mesure (P_0^x, P_1^x) / (Q_0^y, Q_1^y)
- Posons : $P^x = P_0^x - P_1^x$. Puisque $P_0^x + P_1^x = \mathrm{Id}$, nous avons

$$P_0^x = (\mathrm{Id} + P^x)/2 \text{ et } P_1^x = (\mathrm{Id} - P^x)/2$$

(et de même avec $Q^y = Q_0^y - Q_1^y$)

- La distribution des résultats est donc

$$p(a,b\,|\,x,y) = \langle\psi|P_a^x \otimes Q_b^y|\psi\rangle = \langle\psi|(\mathrm{Id} + (-1)^a P^x) \otimes (\mathrm{Id} + (-1)^b Q^y)|\psi\rangle/4$$

- La probabilité p de gain est

$$\begin{aligned} 4p = {} & p(0,0\,|\,0,0) + p(1,1\,|\,0,0) + p(0,0\,|\,0,1) + p(1,1\,|\,0,1) \\ & + p(0,0\,|\,1,0) + p(1,1\,|\,1,0) + p(0,1\,|\,1,1) + p(1,0\,|\,1,1) \end{aligned}$$

- Observons que $p(0,0\,|\,x,y) + p(1,1\,|\,x,y) = \big(1 + \langle\psi|P^x \otimes Q^y|\psi\rangle\big)/2$

et $p(0,1\,|\,x,y) + p(1,0\,|\,x,y) = \big(1 - \langle\psi|P^x \otimes Q^y|\psi\rangle\big)/2$

- Conclusion

$$p = \frac{1}{2} + \frac{\langle\psi|P^0 \otimes Q^0 + P^0 \otimes Q^1 + P^1 \otimes Q^0 - P^1 \otimes Q^1|\psi\rangle}{8}$$

Fin de l'analyse

- Conclusion

$$p = \frac{1}{2} + \frac{\langle\psi| P^0 \otimes Q^0 + P^0 \otimes Q^1 + P^1 \otimes Q^0 - P^1 \otimes Q^1 |\psi\rangle}{8}$$

Calcul

- Observons

$(P^x)^2 = (P_0^x - P_1^x)^2 = (P_0^x)^2 - P_0^x P_1^x - P_1^x P_0^x + (P_1^x)^2 = P_0^x + P_1^y = \mathrm{Id}$

- Donc $\left(P^0 \otimes Q^0 + P^0 \otimes Q^1 + P^1 \otimes Q^0 - P^1 \otimes Q^1\right)^2$

$= \left(P^0 \otimes (Q^0 + Q^1) + P^1 \otimes (Q^0 - Q^1)\right)^2$

$= \mathrm{Id} \otimes (Q^0 + Q^1)^2 + \mathrm{Id} \otimes (Q^0 - Q^1)^2 + P^0P^1 \otimes (Q^0 + Q^1)(Q^0 - Q^1) + P^1P^0 \otimes (Q^0 - Q^1)(Q^0 + Q^1)$

$= 4\mathrm{Id} + (P^0P^1 - P^1P^0) \otimes (Q^1Q^0 - Q^0Q^1)$ dont la norme est donc au plus 8

Enfin…

$$p \leq \frac{1}{2} + \frac{\sqrt{8}}{8} = \cos^2(\pi/8)$$

Corrélations quantiques et plus

- Notes de cours de Richard Cleve

  http://cleve.iqc.uwaterloo.ca/resources/Qic890LectureNotes2019Apr22(V22).pdf

Cryptographie quantique au delà de QKD

- Thèse d'André Chailloux

  https://who.paris.inria.fr/Andre.Chailloux/pdfs/thesis.pdf

Séminaire du cours !

- Certifier la génération de nombres aléatoires avec le quantique

  avec Thomas Vidick, California Institute of Technology