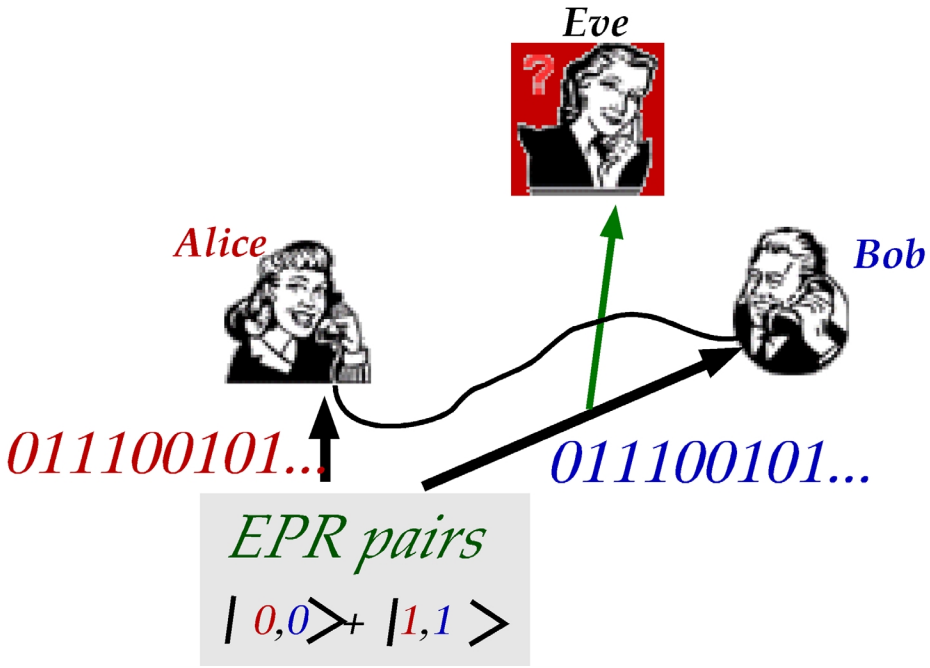
Distribution de clé cryptographique basée sur l' intrication (Ekert)*

L'intrication peut servir à la transmission d 'information si on la combine avec une ligne de communication classique. La cryptographie quantique en fournit un premier exemple



***Alice** et **Bob** partagent un ensemble de paires de qubits dans un état de Bell. Ils effectuent sur ces qubits des mesures locales d'observables qui ne commutent pas, choisies aléatoirement et indépendamment l 'une de l 'autre (par exemple σ_z et σ_x). Ils comparent ensuite (ligne publique) leur choix de base et ne gardent que les résultats pour lesquels leurs choix coïncident. Ils disposent alors d'une clé secrète identique pour coder (**Alice**) et décoder (**Bob**) des messages transmis publiquement.Si Eve intercepte les qubits et les mesure avant de les renvoyer à **Bob**, elle perturbe <u>nécessairement</u> leurs corrélations, ce dont **Bob** et **Alice** peuvent se rendre compte par des tests sur des échantillons de leurs clés qu'ils comparent publiquement avant de les jeter.*

(*) A. Ekert Phys.Rev.Lett. 67, 661 (1991).

Sécurité de principe du protocole

Alice et Bob partagent (canal quantique) des paires préparées dans l'état de Bell $|\varphi^+\rangle$. Ils mesurent aléatoirement chacun σ_x ou σ_z. Dans la moitié des cas, ils mesurent la même observable et leurs résultats doivent alors être identiques (l'état $|\varphi^+\rangle$ ayant une parité et une phase +1). Ils annoncent après coup publiquement leur choix, ce qui leur permet de trier les cas où ils ont fait le même et d'établir chacun, basé sur ce choix commun, une suite aléatoire de 0 et de 1. Ils vérifient enfin publiquement, sur un sous-ensemble de cette suite, qu' ils éliminent ensuite, qu'ils ont bien des résultats identiques. Ils s' assurent ainsi que les paires mesurées sont bien, quoiqu' il aît pu arriver sur le canal quantique, de parité et de phase +1.

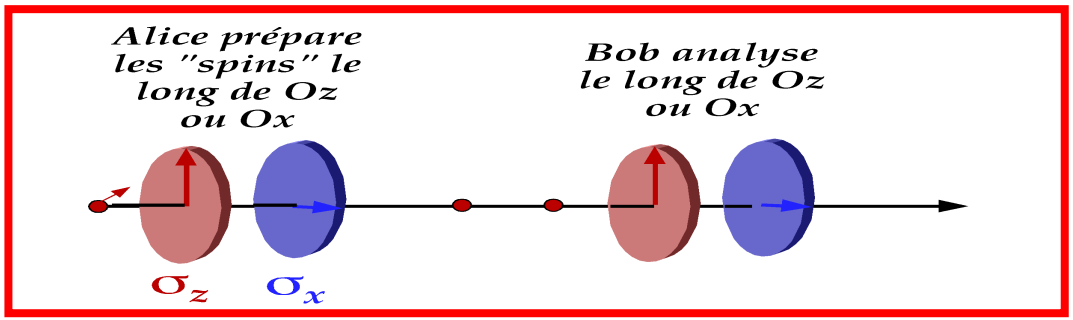
Que peut faire Eve? Elle peut chercher à coupler chaque bit de la clé qu'Alice envoie à Bob à un appareil de mesure (par exemple un ensemble de qubits «espions» E) avant de le réinjecter dans le canal de communication (il faut que Bob ne s' aperçoive de rien!). Son espoir est d'acquérir ainsi de l 'information sur l'état de la clé. Elle attend que A et B annoncent leur choix de base et s' intéresse alors aux qubits espions correspondants. Toute manipulation d'Eve correspond nécessairement à une transformation unitaire de la forme:

$$|\Psi\rangle^{ABE} = |\varphi^+\rangle_{AB} \otimes |E_0\rangle \rightarrow |\varphi^+\rangle_{AB} \otimes |E_1\rangle + |\varphi^-\rangle_{AB} \otimes |E_2\rangle + |\psi^+\rangle_{AB} \otimes |E_3\rangle + |\psi^-\rangle_{AB} \otimes |E_4\rangle$$

La procédure de vérification de A et B ne valide la clé que si le développement de $|\Psi\rangle^{ABE}$ se limite au premier terme ($|\Psi\rangle^{ABE} \rightarrow |\varphi^+\rangle_{AB} \otimes |E_1\rangle$). Eve ne peut donc s'intriquer avec (A-B) et ne peut acquérir aucune information à l'insu d' Alice et Bob.

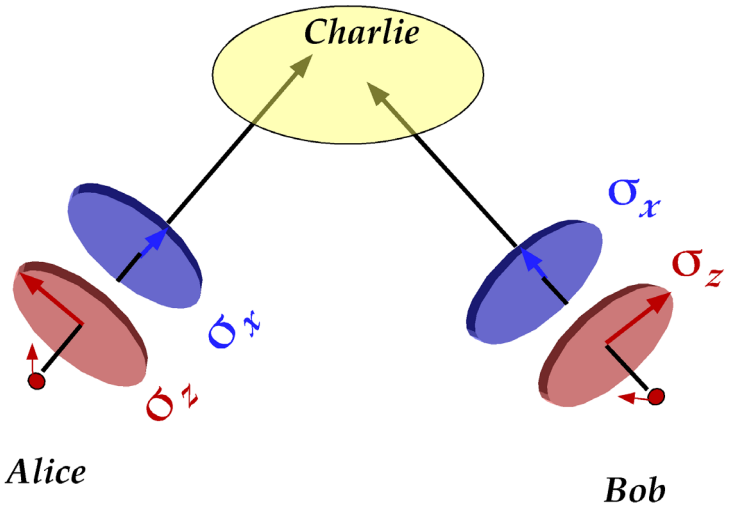
Variante (équivalente): partage de clé basé sur un échange de particules uniques (Bennet -Brassard 1984)

Le protocole précédent nécessite la préparation de paires de type EPR, dont l 'une doit être transmise à distance sur un canal quantique. On peut, sans altérer le principe fondamental de la méthode, s'affranchir de l 'utilisation explicite de paires EPR. La préparation d'une paire par Alice suivie de la mesure sur une des particule de σ_x ou σ_z (choisi aléatoirement) et de l 'envoi de l'autre à Bob est strictement équivalent à l'envoi aléatoire par Alice à Bob de l 'un des 4 états $|+1/2\rangle_z$, $|-1/2\rangle_z$, $|+1/2\rangle_x$, $|-1/2\rangle_x$. La suite de la procédure est identique: Bob choisit à son tour de mesurer la particule suivant Ox ou Oz, Alice et Bob annoncent publiquement leur choix de base et constituent leur clé. La vérification sur un sous-ensemble leur permet comme dans la procédure précédente de s'assurer de l 'absence d 'espionnage.



Toute opération de préparation par Alice d'un qubit dans un état propre de σ_x ou σ_z nécessite le couplage à un appareil avec lequel le qubit s'intrique en général. La version BB84 de cryptographie quantique est donc, implicitement, une expérience de type EPR. La différence avec la version EPR explicite est qu'Alice commence par faire sa mesure et que la clé est donc déterminée dès l'instant initial. Dans la version EPR, Alice et Bob peuvent garder leurs paires sans les lire jusqu'au moment où ils en ont besoin, ce qui limite les risques d 'espionnage trivial (vol de la clé stockée par Alice).

Partage de clé par procédure EPR renversée dans le temps



Alice et Bob préparent aléatoirement des spins le long de Oz et Ox et les envoient à Charlie qui fait une mesure des observables qui commutent $\sigma_z^A \sigma_z^B$ ***et*** $\sigma_x^A \sigma_x^B$ ***et obtient un des quatre résultats correspondant à la parité et à la phase de chaque paire. Charlie annonce publiquement son résultat. Puis, Alice et Bob annoncent également leur choix de base et ne gardent que ceux qui coïncident (50% des cas). L' annonce publique de Charlie leur apprend si chaque bit conservé est le même que celui de leur partenaire, ou son opposé (ils utilisent l 'information sur la parité si la base commune est Oz, celui sur la phase si la base est Ox). Ils établissent ainsi une clé.***

Charlie est essentiel pour permettre à Bob et Alice de comparer leurs bits. Il n 'a lui même aucune information sur chacun des bits de Bob ou d 'Alice. Il ne connaît que leur corrélations. S' il cherche à acquérir une information sur les bits, il va jouer le rôle d 'Eve et Alice et Bob s 'en rendront compte par des comparaisons sur des échantillons de leurs clés. Schéma établissant un standard cryptographique utilisable par plusieurs abonnés, deux d'entre eux pouvant interroger Charlie lorsqu'ils ont besoin d'une clé.

Un élément essentiel du « secret quantique »: utiliser des qubits dans des états non-orthogonaux.

Dans les différents schémas de partage de clé cryptographique, il est essentiel que A et B utilisent de façon aléatoire des bases non-orthogonales (états propres de σ_z ou σ_x, photons polarisés à 45°...). S'ils n'utilisent qu'une base orthonormée, ils peuvent échanger des bits (par exemple $|+1/2\rangle_z$ ou $|-1/2\rangle_z$), mais Eve peut alors effectuer des mesures non perturbantes (on peut toujours détecter des états propres orthogonaux associés à des valeurs propres différentes d' une observable, sans intrication avec l'appareil de mesure). C 'est l'utilisation d'états non-orthogonaux qui rend l'acquisition furtive d 'information par Eve impossible.

Variante de l' argument développé plus haut, directement applicable à la version BB84:

Supposons qu' Eve cherche à distinguer sans les modifier deux états $|\varphi\rangle$ et $|\psi\rangle$ d 'un qubit avec $\langle\varphi|\psi\rangle \neq 0$. Il lui faut donc coupler $|\varphi\rangle$ et $|\psi\rangle$ par une transformation unitaire U à un système d'espionnage initialement dans un état $|E_0\rangle$ suivant les relations:

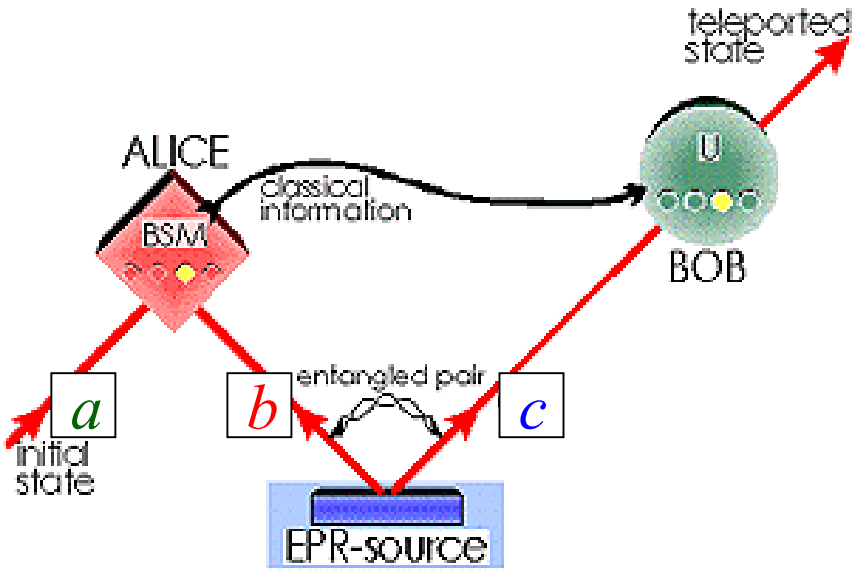
$$|\varphi\rangle|E_0\rangle \rightarrow |\varphi\rangle|E_\varphi\rangle; \qquad |\psi\rangle|E_0\rangle \rightarrow |\psi\rangle|E_\psi\rangle.$$

Comme la transformation est unitaire, on a $\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle\langle E_\varphi|E_\psi\rangle$ et, puisque $\langle\varphi|\psi\rangle \neq 0$:

$|E_\varphi\rangle = |E_\psi\rangle$ (on suppose les états $|\varphi\rangle, |\psi\rangle, |E_0\rangle, |E_\varphi\rangle$ et $|E_\psi\rangle$ normés).

Eve n 'a donc aucun moyen de distinguer sans les perturber deux états non-orthogonaux. Implicitement, ceci entraîne l' impossibilité de cloner un état: si Eve pouvait copier les qubits, elle pourrait réaliser à partir de chaque bit un ensemble grâce auquel elle pourrait déterminer statistiquement les états $|\varphi\rangle$ et $|\psi\rangle$ et donc les distinguer sans en perturber une copie qu 'elle pourrait renvoyer à Bob.

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**.*

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

Procédure de téléportation

1. **Alice** et **Bob** partagent une paire de particules (**b**-**c**) dans un état de Bell (par exemple $|\varphi^+\rangle$):

$$|\varphi^+\rangle_{b,c} = (1/\sqrt{2})(|0,0\rangle_{b,c} + |1,1\rangle_{b,c})$$

2. **Alice** reçoit un qubit (**a**) dans un état inconnu et se propose de le transmettre à **Bob**:

$$|\Psi\rangle_a = \alpha\,|0\rangle_a + \beta\,|1\rangle_a$$

3. **Alice** couple le qubit (**a**) à son partenaire EPR et effectue une mesure de l'état de Bell **a** - **b** correspondant (à l'aide d'un circuit quantique analogue à celui décrit à la fin de la leçon 5):

$$|\Psi\rangle_a |\varphi^+\rangle_{b,c} = (1/\sqrt{2})\,[\alpha\,|0\rangle_a + \beta\,|1\rangle_a]\;[|0,0\rangle_{b,c} + |1,1\rangle_{b,c}] =$$

$$(1/2)\,|\varphi^+\rangle_{a,b}\,[\alpha\,|0\rangle_c + \beta\,|1\rangle_c] \rightarrow 1$$

$$+\,(1/2)\,|\varphi^-\rangle_{a,b}\,[\alpha\,|0\rangle_c - \beta\,|1\rangle_c] \rightarrow \sigma_z$$

$$+\,(1/2)\,|\psi^+\rangle_{a,b}\,[\alpha\,|1\rangle_c + \beta\,|0\rangle_c] \rightarrow \sigma_x$$

$$+\,(1/2)\,|\psi^-\rangle_{a,b}\,[\alpha\,|1\rangle_c - \beta\,|0\rangle_c] \rightarrow \sigma_z\sigma_x = i\,\sigma_y$$

Transformation appliquée par Bob

4. **Alice** communique classiquement le résultat de sa mesure à **Bob** (2 bits) qui, en appliquant à (**c**), en fonction de ce résultat, l'**une de quatre transformations** (1, σ_z, σ_x, $\sigma_z\sigma_x = i\,\sigma_y$) reconstitue l'état <u>toujours inconnu</u> $|\Psi\rangle$ sur la particule (**c**).

Les propriétés de la téléportation

1. Ni Alice ni Bob ne connaissent $|\Psi>_a$. Il n 'y a aucune façon de déterminer les amplitudes α et β si le qubit (a) est unique. Aucun moyen de communiquer le qubit par un procédé de fax classique (lecture par Alice, puis transmission à Bob).

2. Alors que α et β correspondent en principe à une infinité de bits classiques, Alice ne doit communiquer à Bob que 2 bits (la parité et la phase de l 'état de Bell a-b).

3. Contrairement à un fax classique, l'état initial est détruit par la mesure d 'Alice. Sinon, la procédure équivaudrait à un clonage du qubit (a), ce qui est impossible. Un tel clonage permettrait, par itération, d 'obtenir à partir d 'une particule unique une infinité de copies sur lesquelles des mesures donneraient statistiquement avec une précision arbitrairement grande les valeurs de α et β, en contradiction avec 1.

4. La téléportation ne viole pas le principe de causalité. Même si les corrélations EPR sont «instantanées» (en fait ne dépendent pas de l'ordre dans lequel Alice et Bob effectuent leurs manipulations), la transmission d' information requiert un canal classique (Alice doit transmettre à Bob le résultat aléatoire de sa mesure). Cette information classique ne peut se propager plus vite que la lumière.

Une autre utilisation des états de Bell: le codage dense

Un qubit isolé ne peut transporter qu' un bit classique: si Alice et Bob conviennent d 'une direction de quantification (par exemple 0z), Alice choisit de préparer l 'état $|+1/2\rangle_z$ ou $|-1/2\rangle_z$ et envoie le qubit à Bob qui l'analyse. De cette façon, le canal quantique est équivalent à un canal de communication classique. On peut montrer qu' un seul qubit ne peut transporter plus d' information. Nous avons vu cependant que la possibilité d' utiliser des bits dans des états non orthogonaux (utilisation de bits polarisés selon Oz et Ox par exemple) apporte à la communication un élément nouveau non-classique: le secret de principe absolu qui est une conséquence de l' impossibilité de cloner des qubits.

L' utilisation de bits non-orthogonaux, combinée avec le partage d 'états de Bell entre Alice et Bob leur permet aussi d'échanger deux bits classiques en ne se transmettant qu' une particule: supposons que A et B se partagent une paire dans l'état $|\varphi^+\rangle$. Nous avons vu (leçon 5) que par une opération locale sur son qubit (action de 1, σ_x, σ_y ou σ_z), Alice peut transformer $|\varphi^+\rangle$ en l'un des quatre états de Bell, en choisissant à volonté la valeur de deux bits (parité et phase). Si elle envoie ensuite son partenaire EPR à Bob, celui-ci peut à l 'aide d 'un circuit quantique simple déterminer l 'état de Bell choisi par Alice et obtenir ainsi deux bits pour un seul qubit transmis. Si Eve intercepte le bit, elle n' obtient qu' une particule dont la matrice densité est l' unité, sans aucune information.

En fait, A et B ont dû échanger deux bits. Mais le premier échange (établissement de la paire EPR) a eu lieu avant qu 'ils aient besoin de communiquer et n'a transmis aucune information utile. Une fois cette ressource établie, A et B peuvent se transmettre deux bits par particule échangée.

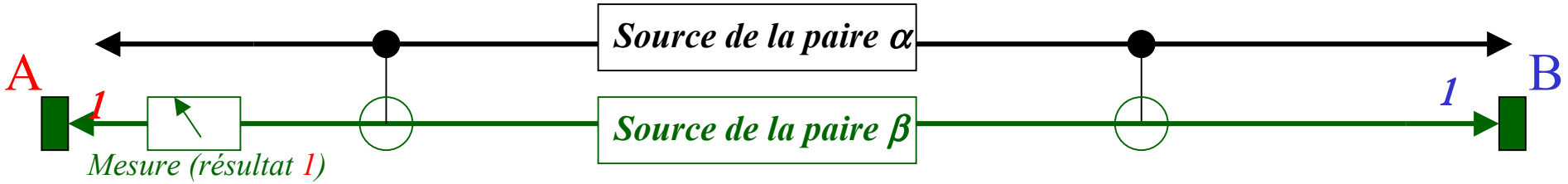
Retour sur la distillation de l' intrication

Revenons à la question abordée à la leçon précédente: comment Alice et Bob peuvent-ils distiller par des opérations locales des paires dans un état de Bell à partir de n paires ayant une intrication partielle d < 1?

Commençons par considérer le cas simple du partage de 2 paires dans l'état :

$$|\Psi\rangle_{AB} = \sqrt{(1-\lambda)}\ |0_A 0_B\rangle + \sqrt{\lambda}\,|1_A 1_B\rangle$$

$$d = -\lambda\ \log(\lambda)\ -(1-\lambda)\ \log(1-\lambda)$$



Portes C-NOT locales en A et B. Les qubits α sont sources, β cibles. Le qubit β de A est mesuré (résultat 1), puis la paire β jetée: la paire α aboutit dans un état d'intrication maximale:

$$|\Psi\rangle_{\alpha,\beta} = (1-\lambda)|0_\alpha 0_\beta\rangle + \sqrt{\lambda}\sqrt{(1-\lambda)}\,[|0_\alpha 1_\beta\rangle + |1_\alpha 0_\beta\rangle] + \lambda|1_\alpha 1_\beta\rangle$$

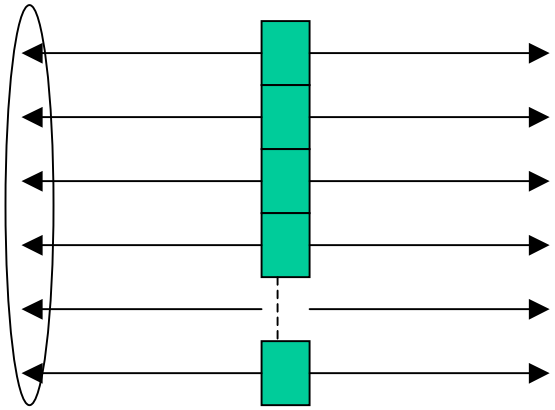
$$\xrightarrow{\text{Portes}} (1-\lambda)|0_\alpha 0_\beta\rangle + \sqrt{\lambda}\sqrt{(1-\lambda)}\,[|0_\alpha 1_\beta\rangle + |1_\alpha \underline{1}_\beta\rangle] + \lambda|1_\alpha \underline{0}_\beta\rangle$$

$$\xrightarrow{\text{Mesure } \sigma_z(A\beta)} (1/\sqrt{2})\,[|0_\alpha\rangle + |1_\alpha\rangle]\ |\underline{1}_\beta\rangle \quad \text{(probabilité de réussite: } 2\lambda(1-\lambda)\text{)}$$

L'opération revient à mesurer localement $\sigma_z^{A\alpha} + \sigma_z^{A\beta}$ (et ipso facto $\sigma_z^{B\alpha} + \sigma_z^{B\beta}$) en gardant l'état correspondant à une somme des qubits A (et B) = 1. En cas de réussite, l'intrication globale peut augmenter (si d < 0.5), mais en moyenne , elle diminue toujours (le qubit A, β peut être aussi trouvé dans l 'état 0 avec la probabilité 1–2λ(1–λ), la paire α étant alors projetée dans un état partiellement intriqué).

Généralisation à un grand nombre de paires:

A et B partagent un grand nombre n de paires d 'intrication d < 1: A (ou B) mesure localement la somme de ses qubits. Automatiquement, le système est projeté dans un état intriqué qui peut, par des transformations unitaires locales de A et B et le rejet d'un certain nombre de bits, se réduire à un ensemble de paires d 'intrication maximale (états de Bell).



$$|\Psi>_{\{n\}} = [\sqrt{(1-\lambda)}\ |{}^{A}0\,{}^{B}0> + \sqrt{\lambda}\ |{}^{A}1\,{}^{B}1>]^{\{n\}} =$$

$$\Sigma_{p=0,\,n}\ \lambda^{p/2}(1-\lambda)^{(n-p)/2}\ [\,|11>_1|11>_2 \ldots |11>_p|00>_{p+1}\ldots\ \ldots|00>_n\ +\ \text{permutations}]$$

Superposition de $\binom{n}{p} = \frac{n!}{p!\,n-p!}$ ***états orthonormés avec p bits 1 en A et B***

Une mesure locale de $\sum_{i=1}^{n}\sigma_z^{A,i}$ ***projette*** $|\Psi>_{\{n\}}$ ***sur l 'une de ces superpositions d'états:***

$$|\Psi>_{\{n\}} \rightarrow |\Psi>_{mesure} = \binom{n}{p}^{-1/2}\ [\,|11>_1|11>_2 \ldots |11>_p|00>_{p+1}\ldots\ \ldots|00>_n\ +\ \text{permutations}\ ]$$

avec la probabilité $\pi(p) = \binom{n}{p}\lambda^p(1-\lambda)^{(n-p)}$ ***, maximum pour*** $p \sim n\lambda$ ***(loi binomiale).***

Distillation asymptotiquement optimale de paires de qubits

L 'état $|\Psi>_{mesure} = \binom{n}{p}^{-1/2}$ [$|1\,1>_1 |1\,1>_2 \ldots |1\,1>_p |0\,0>_{p+1} \ldots \ldots |0\,0>_n$ + permutations]

est préparé avec une probabilité non négligeable <u>si et si seulement $p \sim n\lambda$</u> (fluctuation $\pm\sqrt{n\lambda(1-\lambda)}$).

$|\Psi>_{mesure}$ est dans l'immense majorité des cas (loi des grands nombres) une superposition à poids égaux de $N \approx \frac{n!}{(n\lambda)![n(1-\lambda)]!}$ états, chacun étant un produit tensoriel d'états de base de A et de B orthogonaux.
Il s'agit d'une décomposition de Schmidt, correspondant à une entropie maximale pour A et B:

$$S(\rho_A) = S(\rho_B) = \log_2(N) \sim -n\,[\log_2 \lambda + (1-\lambda)\log_2(1-\lambda)]$$

Les N états orthogonaux de A(B) sont des produits corrélés de n qubits orthogonaux de la forme $|0,1,1,0\ldots>$.
Si $N = 2^k$, des transfo. unitaires locales identiques de A et B peuvent changer ces N états en états de base du sous espace des k premiers qubits, avec, en produit tensoriel, l'état $|0,0,0\ldots>$ des n–k derniers qubits. On a $k \sim nd$ où d est le degré d'intrication des paires initiales. L'état obtenu se factorise alors de façon évidente:

$$|\Psi>_{final} = (2^{-k/2})\ [\,|0,0>+|1,1>\,]_1 \otimes \ldots [\,|0,0>+|1,1>\,]_k \otimes |0,0>_{k+1} \otimes \ldots |0,0>_n$$

$k \sim nd$ paires indépendantes dans l'état de Bell $|\varphi^+>$ — 2(n–k) qubits séparés (à jeter)

Si N n 'est pas proche de 2^k, on recommence la mesure de $\Sigma_{i=1,n}(\sigma_{z,i}^A)$ avec d'autres échantillons de n paires, en obtenant après chaque opération, des états intriqués A-B dont les nombres de Schmidt, tous voisins de 2^{nd}, se multiplient au cours du processus. On continue jusqu'à ce que, pour q échantillons, ce nombre approche par excès une puissance 2^k avec $k \sim \Sigma_i \log(N_i) \sim q\,n\,d$. A ou B effectue alors la mesure d 'une observable locale qui admet <u>exactement 2^k états propres dégénérés</u> communs avec ceux de la décomposition de Schmidt trouvée. Cette mesure projette (probabilité aussi proche de 1 que l'on veut), les $N_1 N_2 \ldots N_q$ états de Schmidt sur ces 2^k états. A et B peuvent alors transformer unitairement ces états en une base des k premiers qubits (en jetant les (n-k) qubits en excès de A et B). On <u>distille ainsi localement</u> (avec une probabilité $\to 1$ quand $q\,n \to \infty$) ~ q n d paires de Bell à partir de q n paires de $d < 1$. La procédure est <u>optimale</u> (on ne peut faire mieux par des opérations locales).
Toutes ces opérations peuvent s'effectuer en combinant des portes locales à 1 et 2 qubits (voir leçon 7).