La science quantique

Une vision singulière

XI) Qubits optiques B:

cryptographie quantique

Paradoxe EPR,

et téléportation quantique

P.A. Besse

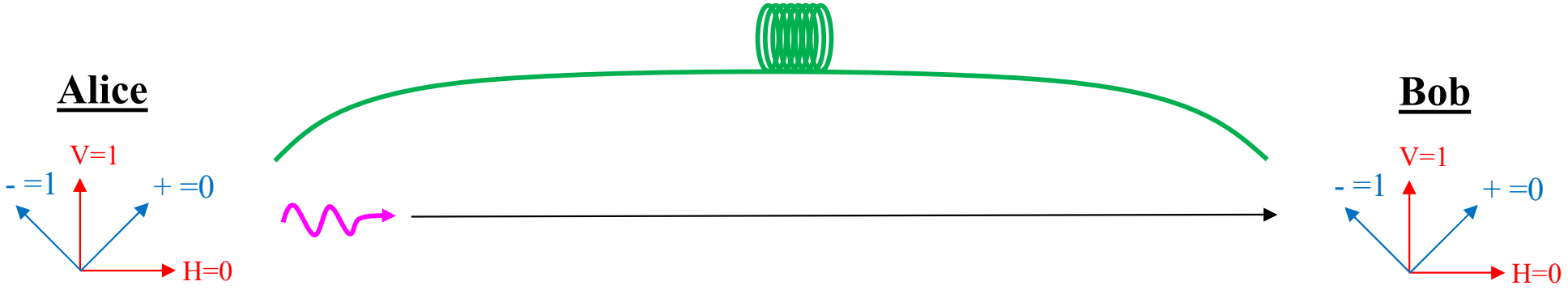
Cryptographie quantique

Protocole BB84

(Bennett and Brassard 1984)

Protocole BB84

(Bennett and Brassard 1984)



1) Alice choisit aléatoirement (avec un Quantum Random Number Generator, QRNG) la série de «1» ou de «0» qu'elle va émettre. (ex.: 100'000 bits)
2) Alice et Bob choisissent aléatoirement (QRNG) leurs bases d'émission et de mesure.
3) Alice envoie à Bob sa liste de bases d'émission
4) Bob sélectionne les cas où les bases correspondent (ex.: 50'000 bits env.)
5) Bob envoie à Alice un petit set de cas sélectionnés (ex.: 1000 bits) et Alice vérifie que les bits correspondent
6) Les bits restants (ex.: env 49'000) peuvent servir de clé

Protocole BB84
exemple avec 16 bits

1) Alice choisit aléatoirement la série de «1» ou de «0» qu'elle va émettre.

1)	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**1**	**0**
2A)																
2B)																
3-4)																
5)																
6)																

QRNG

Protocole BB84
exemple avec 16 bits

2) Alice et Bob choisissent aléatoirement leurs bases d'émission et de mesure.

1)	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**1**	**0**
2A)	**+-**	**HV**	**HV**	**HV**	**+-**	**HV**	**+-**	**+-**	**HV**	**HV**	**+-**	**+-**	**HV**	**+-**	**HV**	**+-**
																
2B)	**+-**	**+-**	**HV**	**+-**	**HV**	**HV**	**HV**	**+-**	**+-**	**+-**	**+-**	**HV**	**HV**	**+-**	**HV**	**HV**
3-4)																
5)																
6)																

QRNG

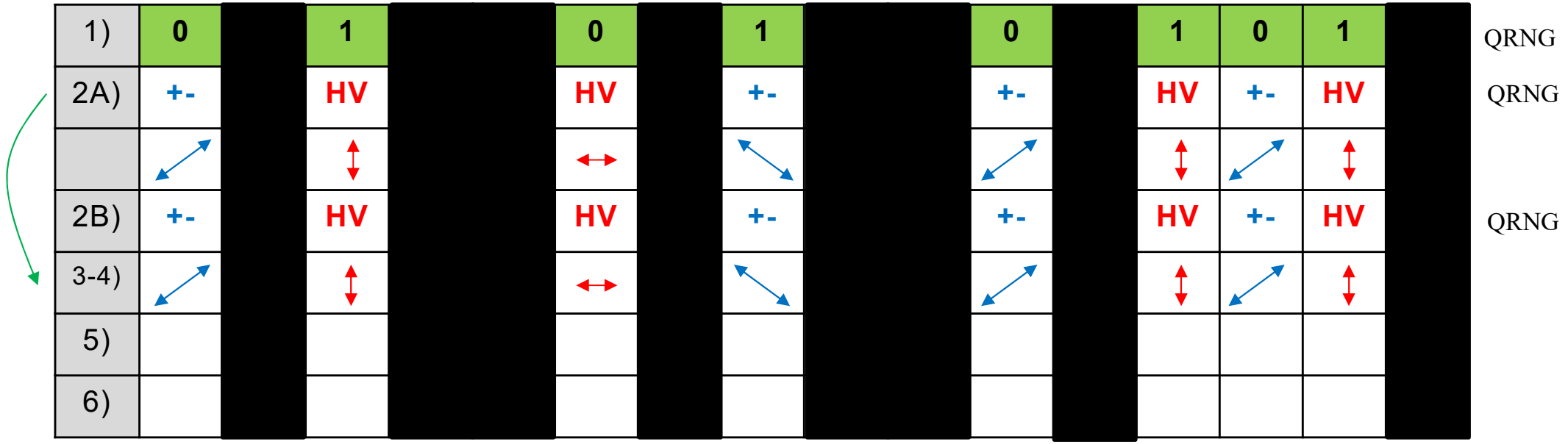
QRNG

QRNG

Protocole BB84
exemple avec 16 bits

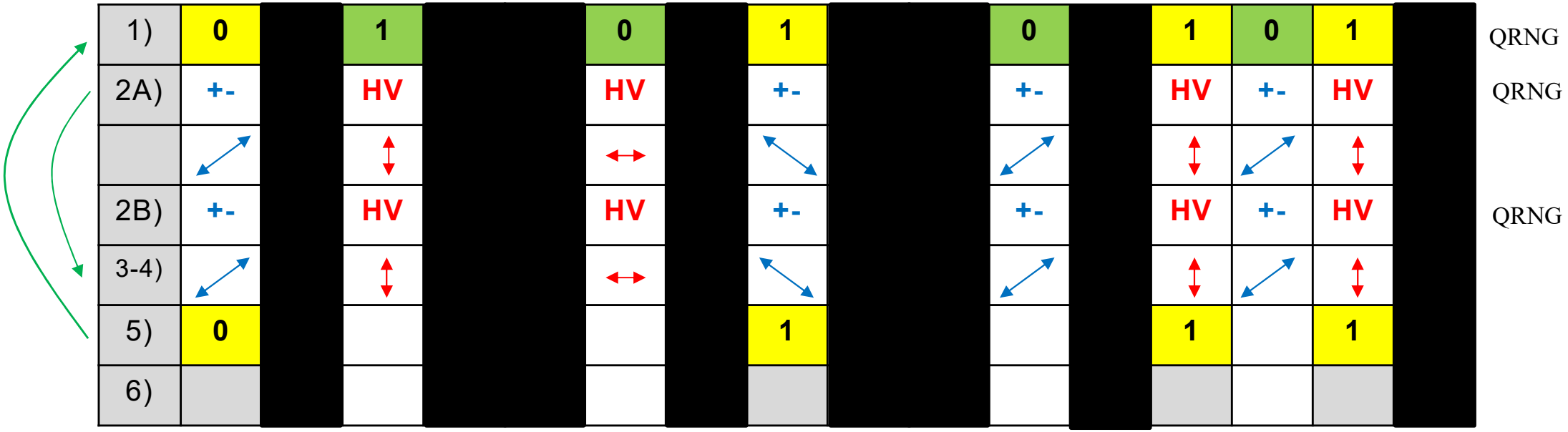
3) Alice envoie à Bob sa liste de bases d'émission

4) Bob sélectionne les cas où les bases correspondent



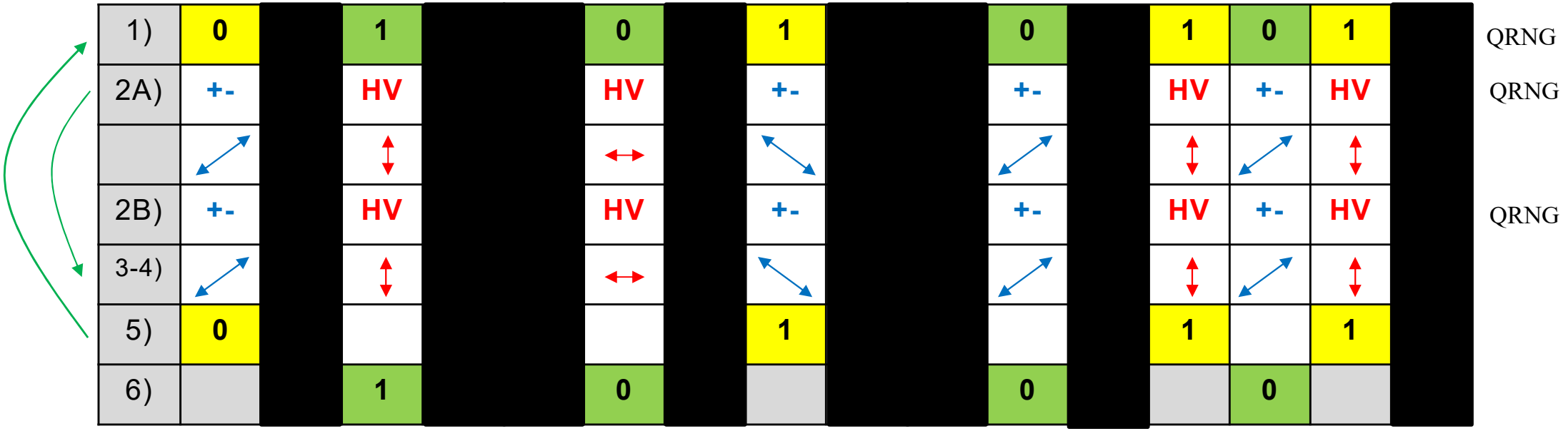
Protocole BB84
exemple avec 16 bits

5) Bob envoie à Alice un petit set de cas sélectionnés et Alice vérifie que les bits correspondent



Protocole BB84
exemple avec 16 bits

6) Les bits restants peuvent servir de clé



1 0 0 0

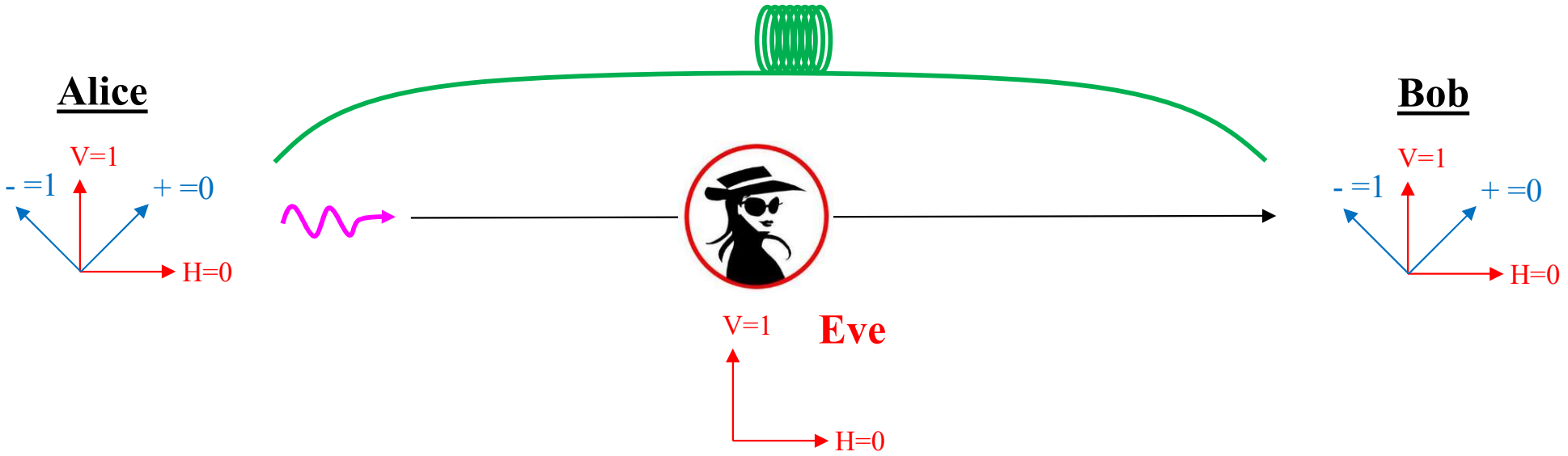
Clé partagée

Utilisation de la clé (exemple 4 bits)

Info à transmettre par Alice	1 1 0 1	
Clé Alice	1 0 0 0	
Signal transmis	0 1 0 1	**(info + clé) modulo 2**
	⇩	
Clé Bob	1 0 0 0	
Info décodée chez Bob	1 1 0 1	**(signal + clé) modulo 2**

Protocole BB84

(Bennett and Brassard 1984)



Eve mesure avec sa propre base et renvoie la même polarisation que celle obtenue dans sa base

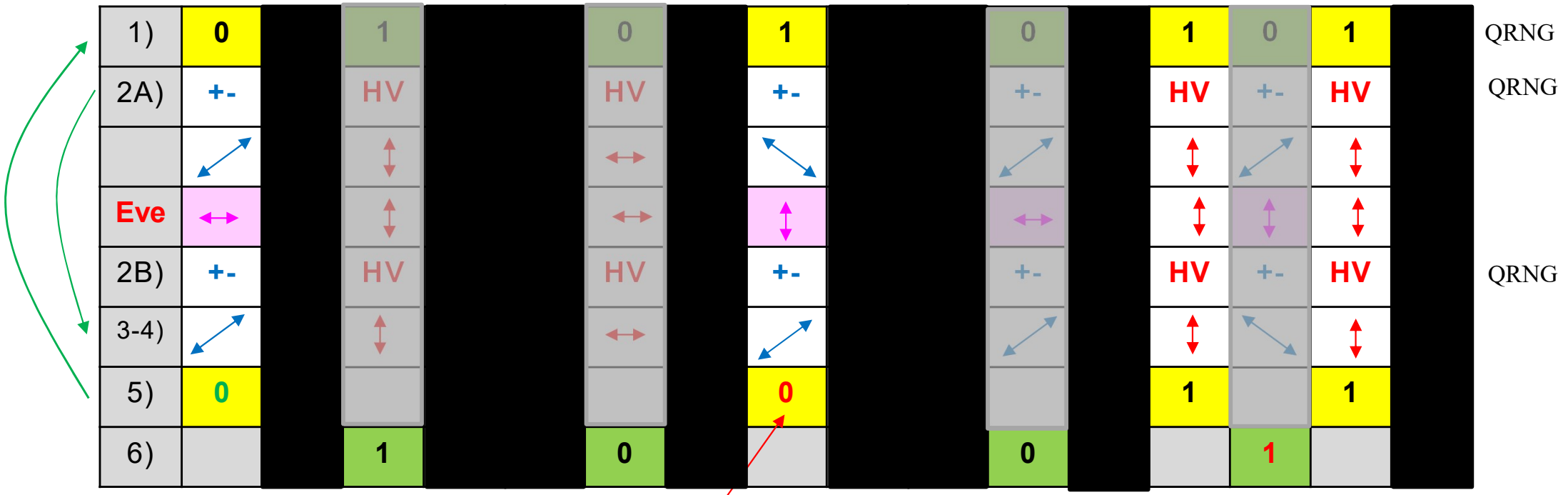
⇩

On ne considère que les cas où les bases sont identiques chez Alice et Bob

- Si la base d'Eve est la même que celles d'Alice et de Bob → aucune différence en étape 5)

- Si la base d'Eve est différente que celle d'Alice et de Bob → 50% de différence en étape 5)

Protocole BB84
exemple avec 16 bits



Erreur → **Eve écoute**

Dans ¼ des cas en moyenne

Fausse clé

Alice 1 0 0 0
Bob 1 0 0 1

Dans ¼ des cas en moyenne

Paire de

Qubits intriqués:

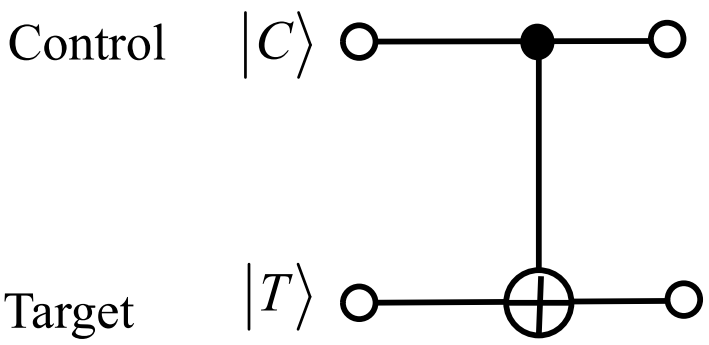
CNOT

Rappel: CNOT

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

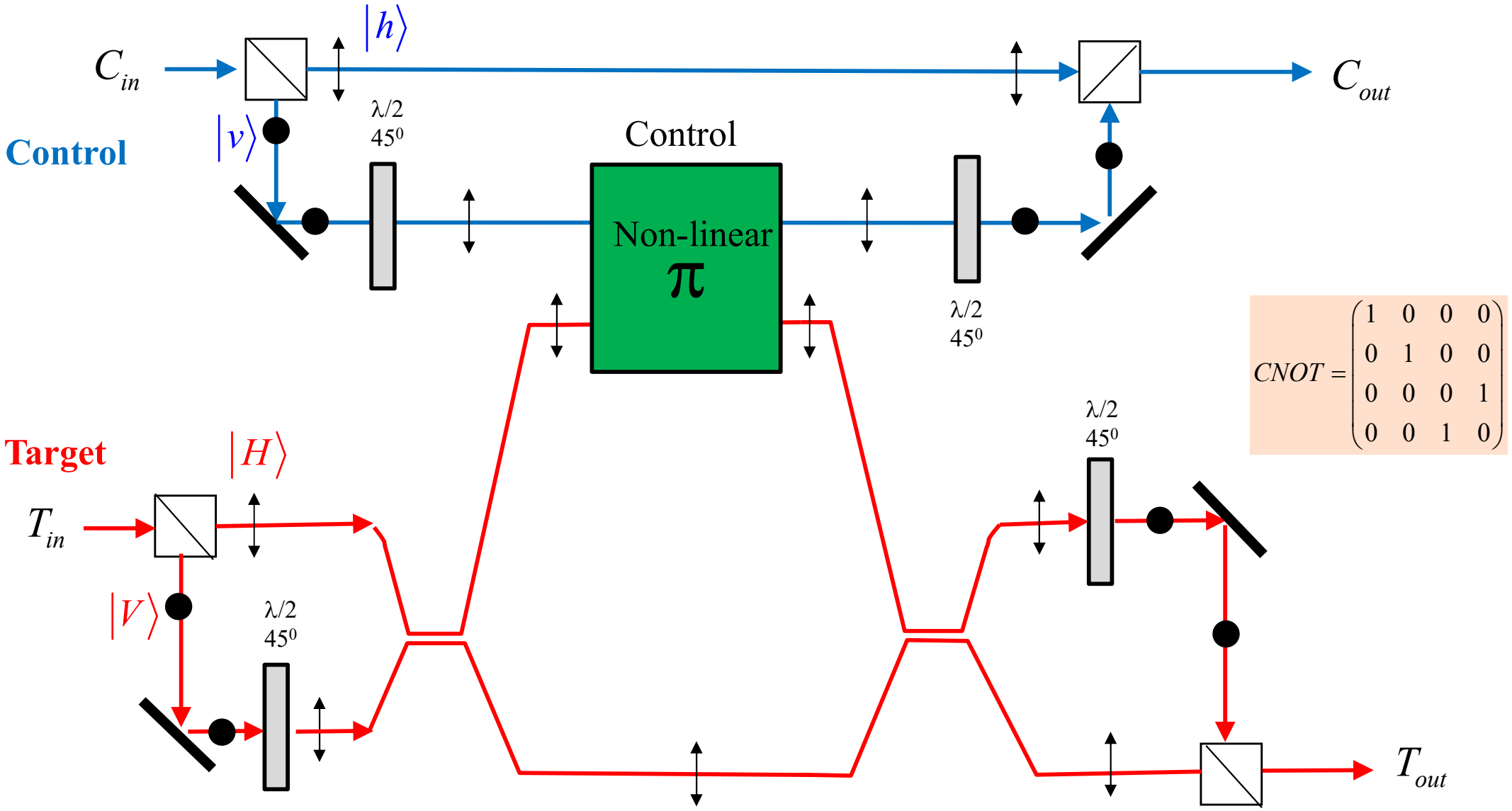
«control NOT» $|C\rangle \quad |T\rangle$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} Uu \\ Ud \\ Du \\ Dd \end{pmatrix} = \begin{pmatrix} Uu \\ Ud \\ Dd \\ Du \end{pmatrix}$$

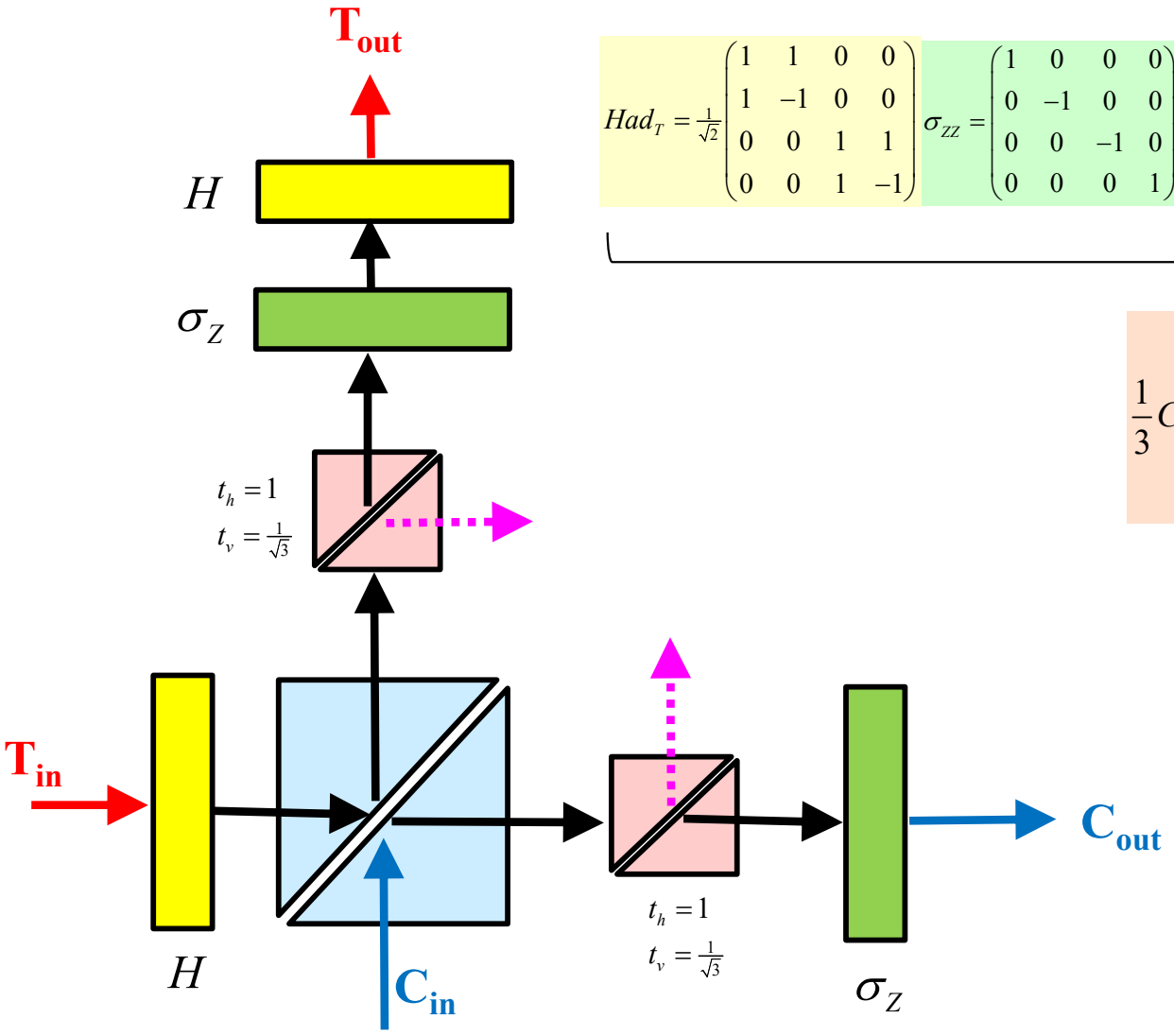


$$|C\rangle = |U\rangle \quad \Rightarrow \quad |T\rangle \text{ inchangé}$$
$$|C\rangle = |D\rangle \quad \Rightarrow \quad |u\rangle \leftrightarrow |d\rangle$$

CNOT avec un milieu non linéaire



CNOT avec un Polarization Dependent Beam Splitter (PDBS)



$$Had_T = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \quad \sigma_{ZZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad F = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \frac{1}{\sqrt{3}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{3}} & 0 \\ 0 & 0 & 0 & \frac{1}{3} \end{pmatrix} \quad PDBS = \begin{pmatrix} \frac{1}{3} & 0 & 0 & 0 \\ 0 & -\frac{1}{\sqrt{3}} & 0 & 0 \\ 0 & 0 & -\frac{1}{\sqrt{3}} & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad Had_T = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\frac{1}{3}CNOT = \frac{1}{3}\cdot\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Optical quantum computer

Chinese optical quantum computer Jiuzhang 2.0 can solve a problem 10^24 faster than a classical computer. CHAO-YANG LU/UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA

https://spectrum.ieee.org/quantum-computing-china

Paire de

Qubits intriqués:

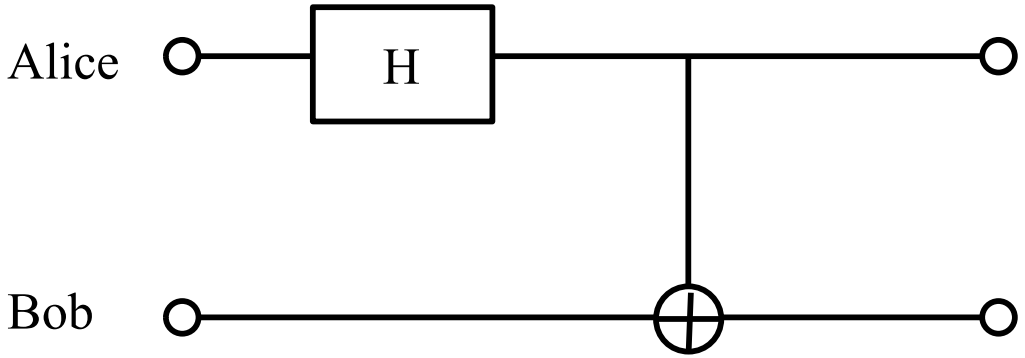
Génération des états de Bell

Génération des états de Bell

$\lambda/2 \qquad \alpha = 22.5^0$

$$H_A = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

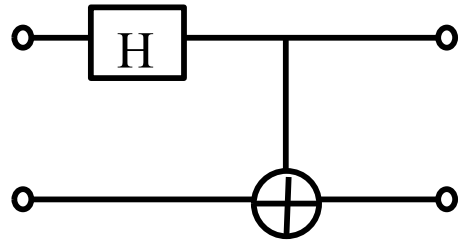
Hadamar $\quad \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$



CNOT $\quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

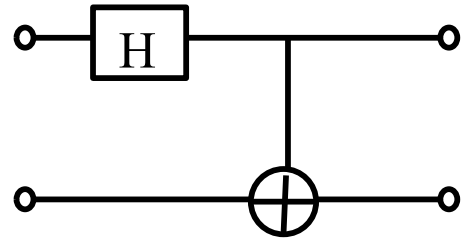
Génération des états de Bell

$$\left.\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right\} \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$$



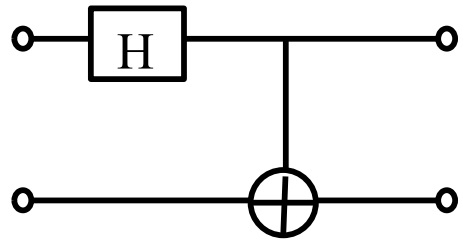
$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$$

$$\left.\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right\} \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$



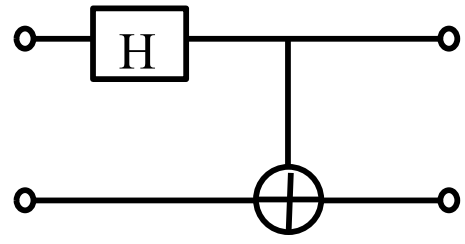
$$\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$$

$$\left.\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right\} \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$



$$\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$$

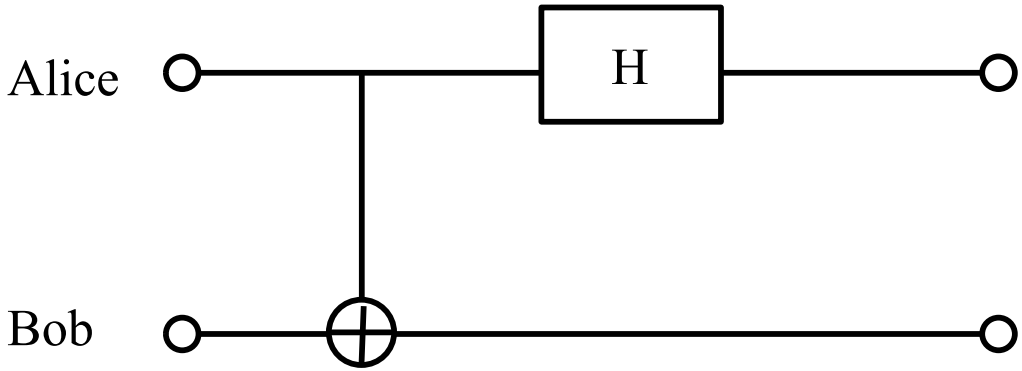
$$\left.\begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right\} \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$



$$\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$$

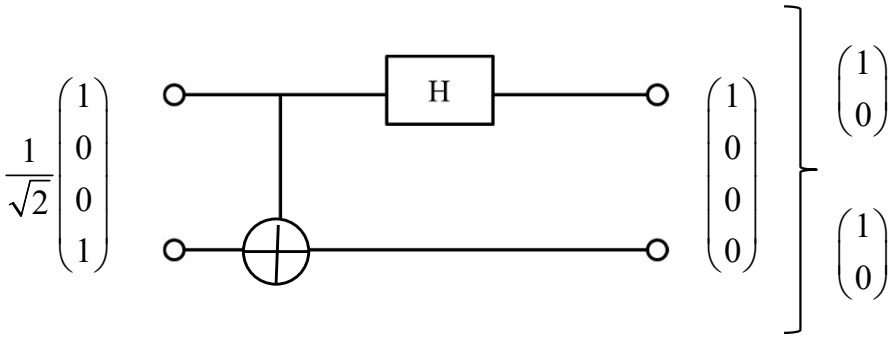
Décomposition des états de Bell

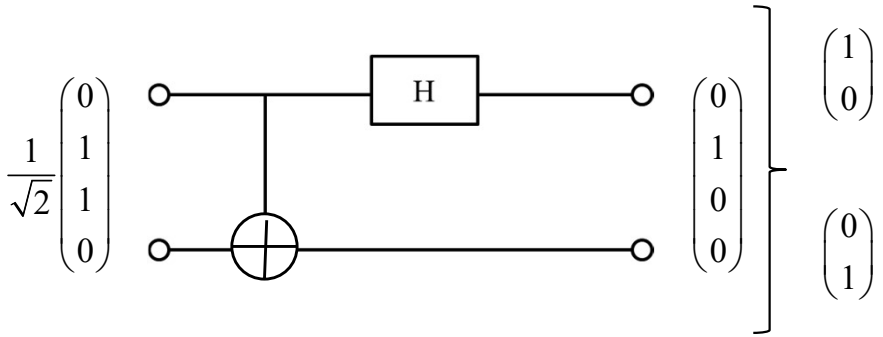
$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$ Hadamar

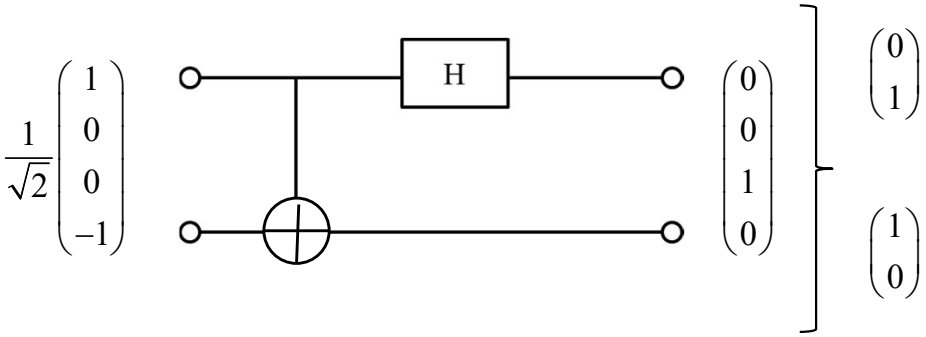


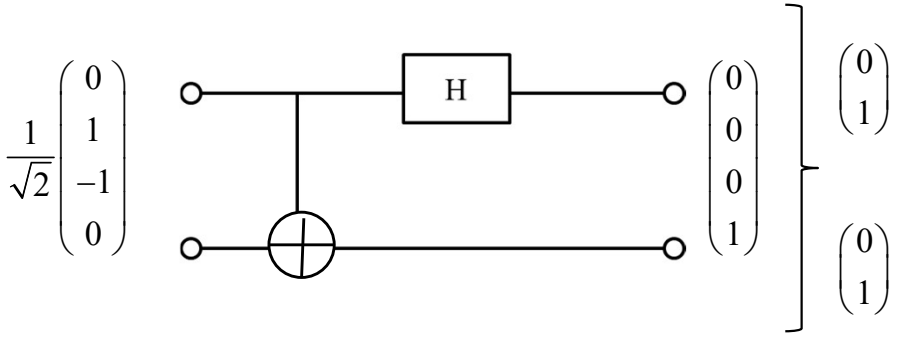
CNOT $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$

Décomposition des états de Bell



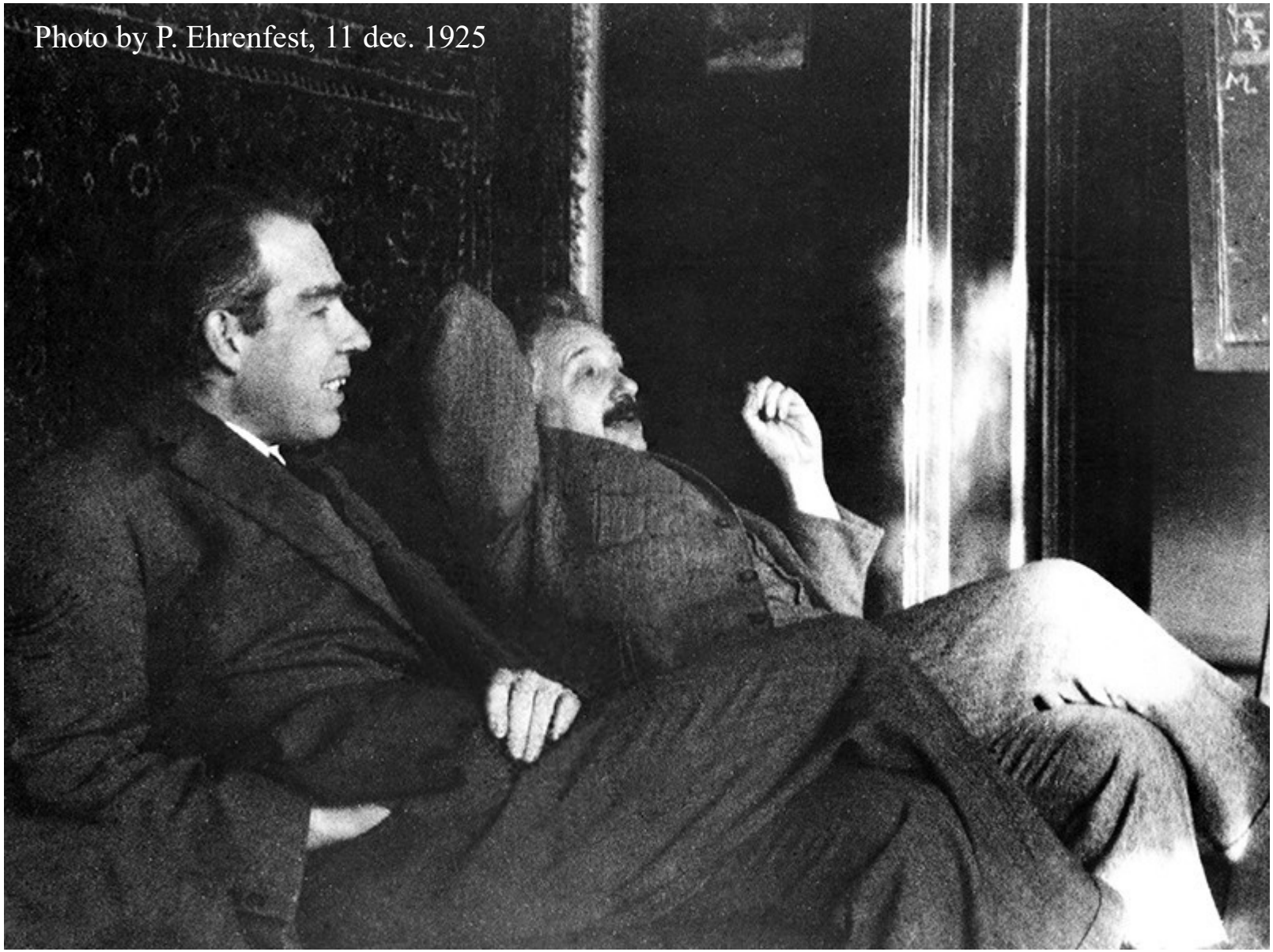




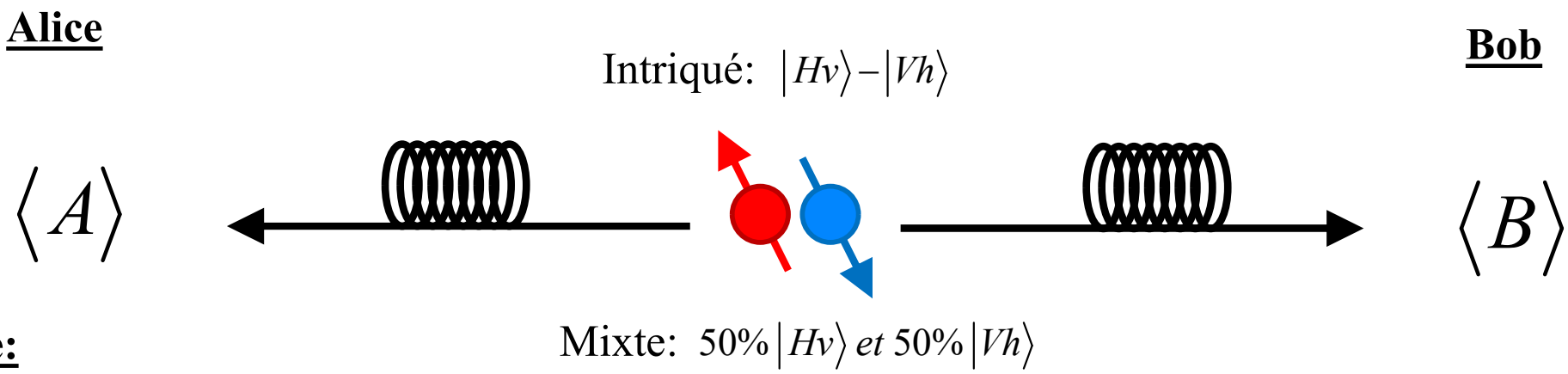


Paradoxe EPR et Inégalités de Bell

La dispute …



Paradoxe EPR
Einstein – Podolski – Rosen

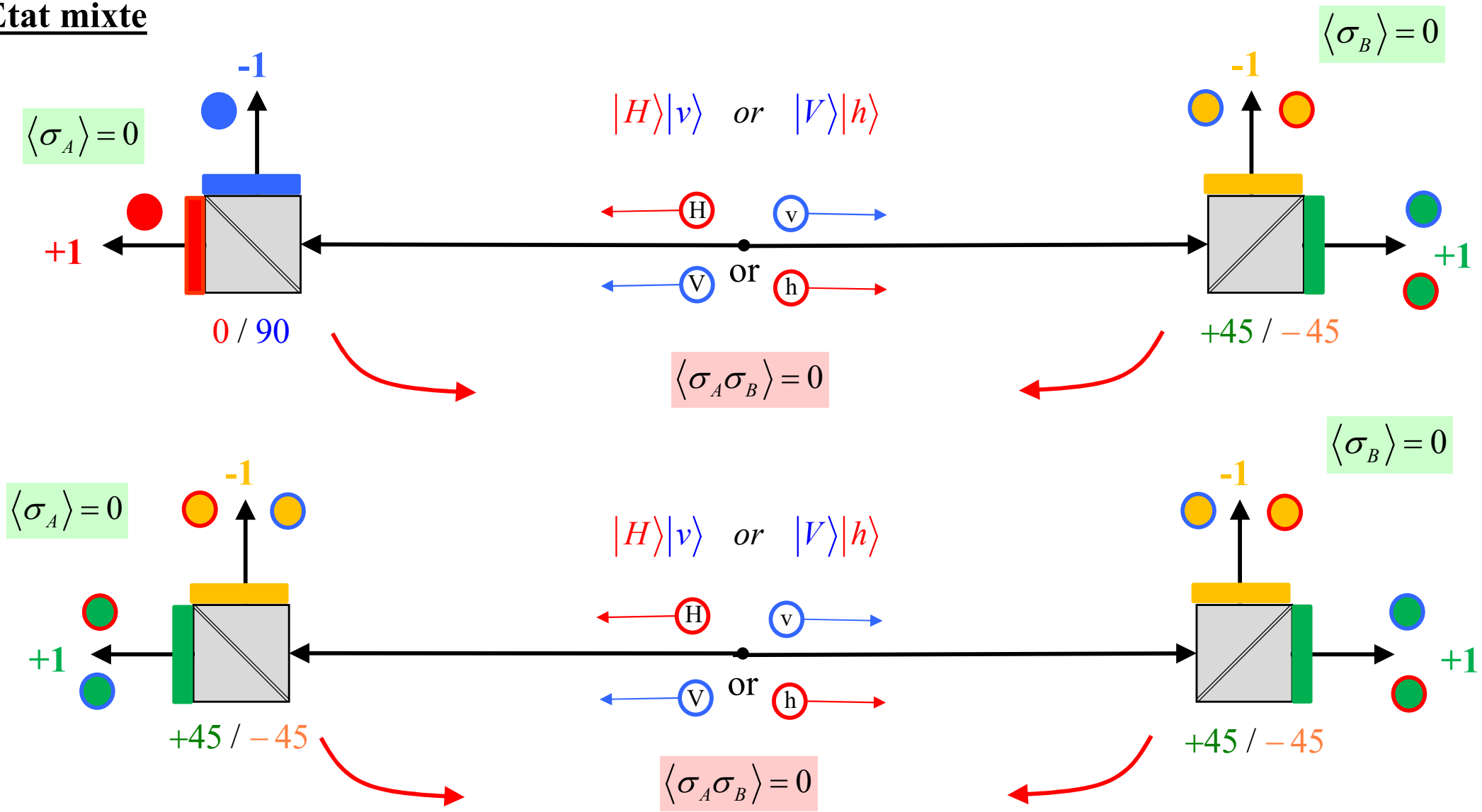


- Générer deux particules intimement liées
- Les séparer à une distance «infinie» tout en conservant le lien intime
- Alice mesure la propriété A et simultanément Bob mesure la propriété B avec une précision maximale.
- Calcul de A chez Bob et de B chez Alice en utilisant le lien intime

→ ?? Levée des incertitudes ??

Corrélations et paradoxe EPR

Etat mixte



Rappel: Mode intriqué exemple le «singulet»

$$\text{singulet} = +\frac{1}{\sqrt{2}}\left|H\right\rangle \otimes \left|v\right\rangle$$
$$-\frac{1}{\sqrt{2}}\left|V\right\rangle \otimes \left|h\right\rangle$$

Angle du polarisateur d'Alice

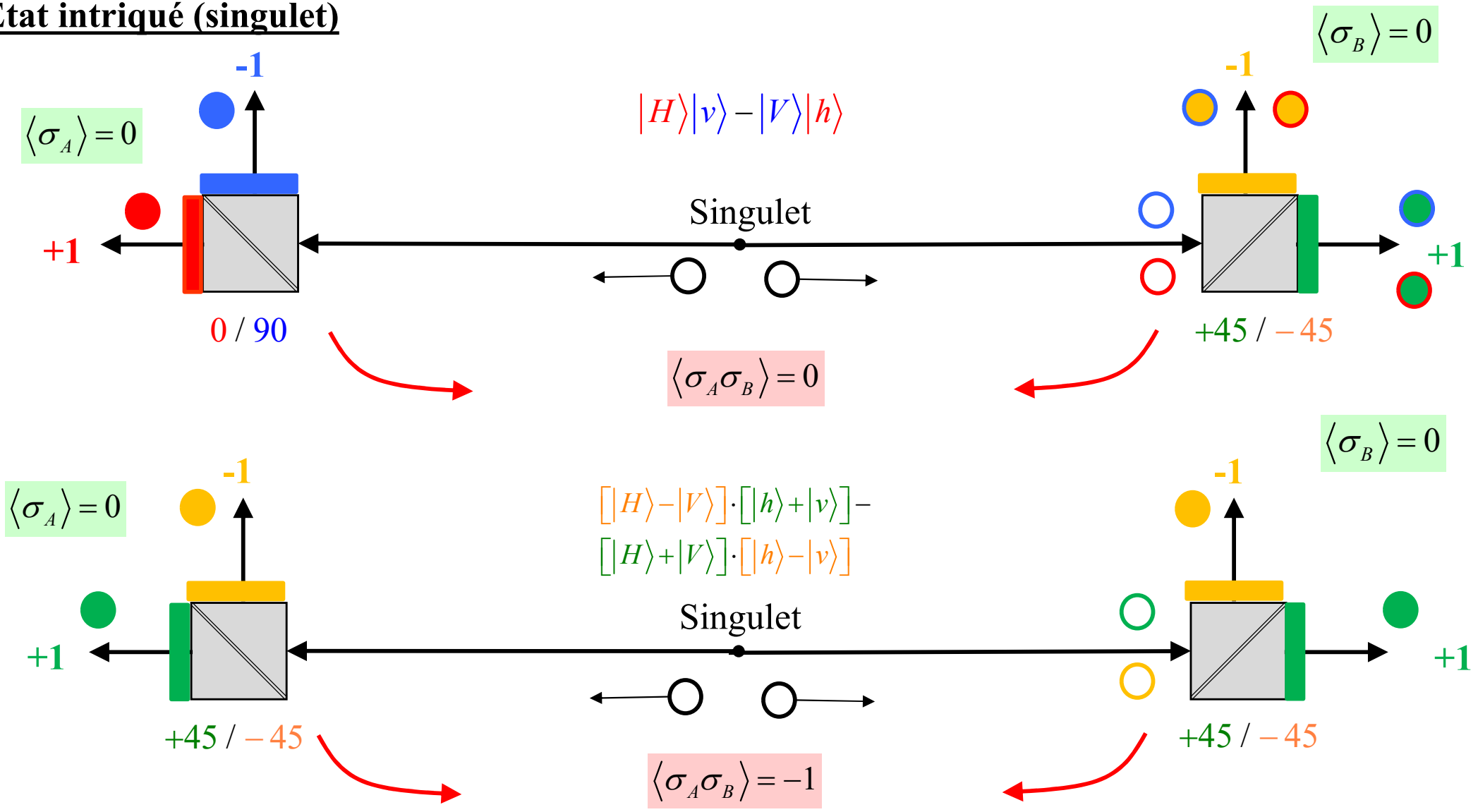
$\alpha = 0$

$$= \frac{1}{2}\cdot\left[\left|H\right\rangle - \left|V\right\rangle\right] \otimes \left[\left|h\right\rangle + \left|v\right\rangle\right]$$
$$-\frac{1}{2}\cdot\left[\left|H\right\rangle + \left|V\right\rangle\right] \otimes \left[\left|h\right\rangle - \left|v\right\rangle\right]$$

$\alpha = +45$

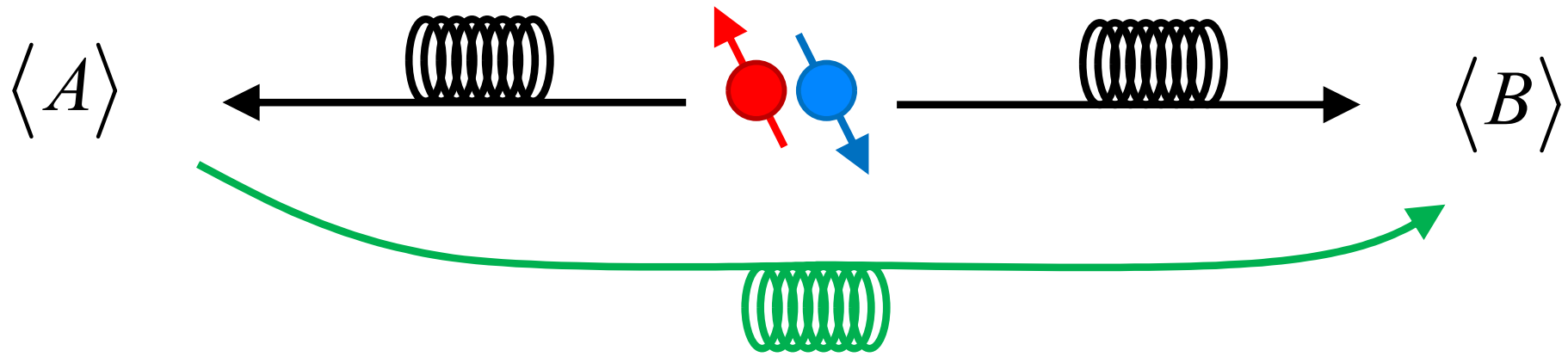
Corrélations et paradoxe EPR

Etat intriqué (singulet)



Inégalités de Bell:

Alice **Bob**



Corrélations

Alice mesure:

$$\sigma_1 \equiv \sigma_{\alpha=0}$$

$$\sigma_2 \equiv \sigma_{\alpha=45}$$

$$M_{11} \equiv \sigma_1 \otimes \tau_1$$

$$M_{21} \equiv \sigma_2 \otimes \tau_1$$

$$M_{22} \equiv \sigma_2 \otimes \tau_2$$

$$M_{12} \equiv \sigma_1 \otimes \tau_2$$

Bob mesure:

$$\tau_1 \equiv \sigma_\beta$$

$$\tau_2 \equiv \sigma_{\beta+45}$$

Inégalités de Bell:

$$\sigma_1 = \pm 1 \qquad \sigma_2 = \pm 1 \qquad \tau_1 = \pm 1 \qquad \tau_2 = \pm 1 \quad \Rightarrow \quad \begin{array}{r} |\sigma_1 + \sigma_2| = 2 \; et \; (\sigma_2 - \sigma_1) = 0 \\ ou \; |\sigma_2 - \sigma_1| = 2 \; et \; (\sigma_1 + \sigma_2) = 0 \end{array}$$

$$\sigma_1\tau_1 + \sigma_2\tau_1 + \sigma_2\tau_2 - \sigma_1\tau_2 = \tau_1(\sigma_1 + \sigma_2) + \tau_2(\sigma_2 - \sigma_1) \quad \in [-2, +2]$$

Si la mesure par Bob de τ1 et τ2 ne dépend pas de σ1 et σ2 mesurés chez Alice

$$S_{CHSH} \equiv \left| \langle M_{11} \rangle + \langle M_{21} \rangle + \langle M_{22} \rangle - \langle M_{12} \rangle \right| \leq 2$$

"Valeur de Clauser-Horne-Shimony-Holt"

Rappel:
Cas général avec l'état «singulet»

Alice et Bob font leurs mesures avec un polarisateur à angle α reesp. β.

Alice

$$\sigma_\alpha = \begin{pmatrix} \cos(2\alpha) & \sin(2\alpha) \\ \sin(2\alpha) & -\cos(2\alpha) \end{pmatrix}$$

Bob

$$\sigma_\beta = \begin{pmatrix} \cos(2\beta) & \sin(2\beta) \\ \sin(2\beta) & -\cos(2\beta) \end{pmatrix}$$

$$M_{\alpha\beta} = \begin{pmatrix} \cos(2\alpha)\begin{pmatrix} \cos(2\beta) & \sin(2\beta) \\ \sin(2\beta) & -\cos(2\beta) \end{pmatrix} & \sin(2\alpha)\begin{pmatrix} \cos(2\beta) & \sin(2\beta) \\ \sin(2\beta) & -\cos(2\beta) \end{pmatrix} \\ \sin(2\alpha)\begin{pmatrix} \cos(2\beta) & \sin(2\beta) \\ \sin(2\beta) & -\cos(2\beta) \end{pmatrix} & -\cos(2\alpha)\begin{pmatrix} \cos(2\beta) & \sin(2\beta) \\ \sin(2\beta) & -\cos(2\beta) \end{pmatrix} \end{pmatrix}$$

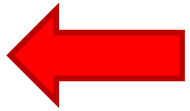
Etat «singulet»

$$|\psi_{\text{sing}}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

$$\langle M_A \rangle = 0 \qquad \langle M_B \rangle = 0$$

Corrélation

$$\langle M_{AB} \rangle = -\cos\big(2(\alpha - \beta)\big)$$



Comparaison

Alice:

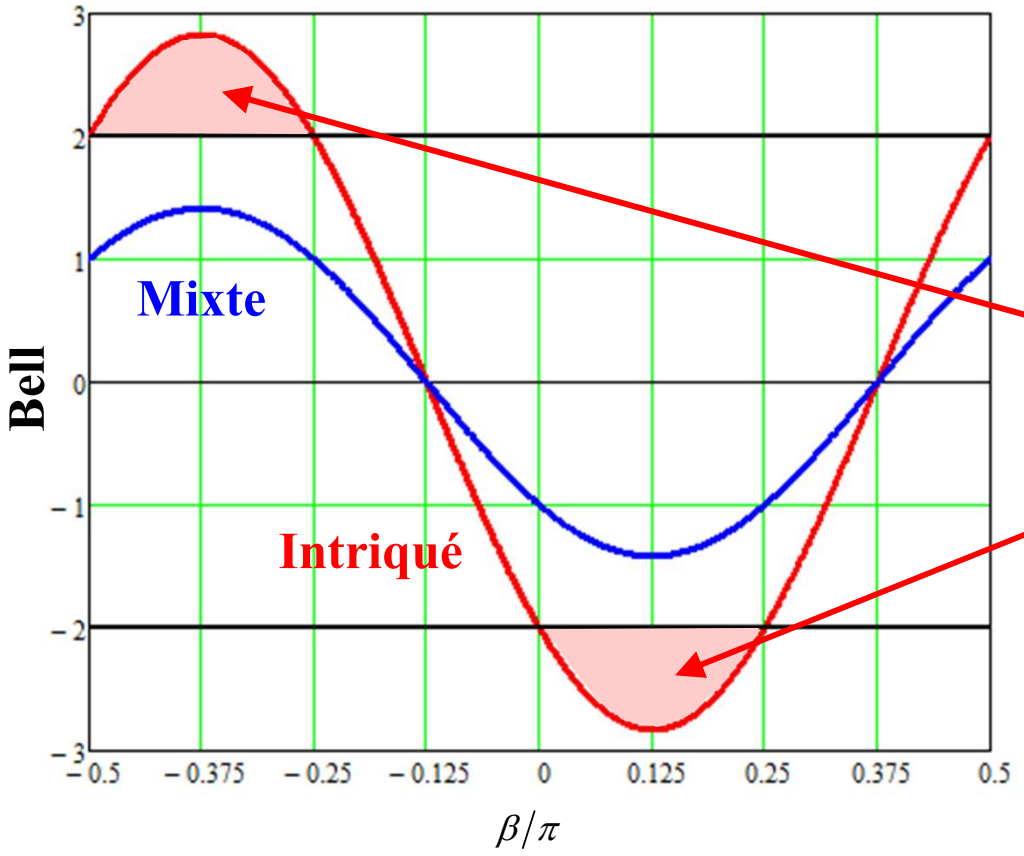
$$\alpha_1 = 0$$

$$\alpha_2 = 45^0$$

Bob:

$$\beta_1 = \beta$$

$$\beta_2 = \beta + 45^0$$



$$|\psi_{in}\rangle = \frac{1}{\sqrt{2}} \cdot \left(|Hv\rangle - (Vh) \right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}$$

Violation de l'inégalité de Bell

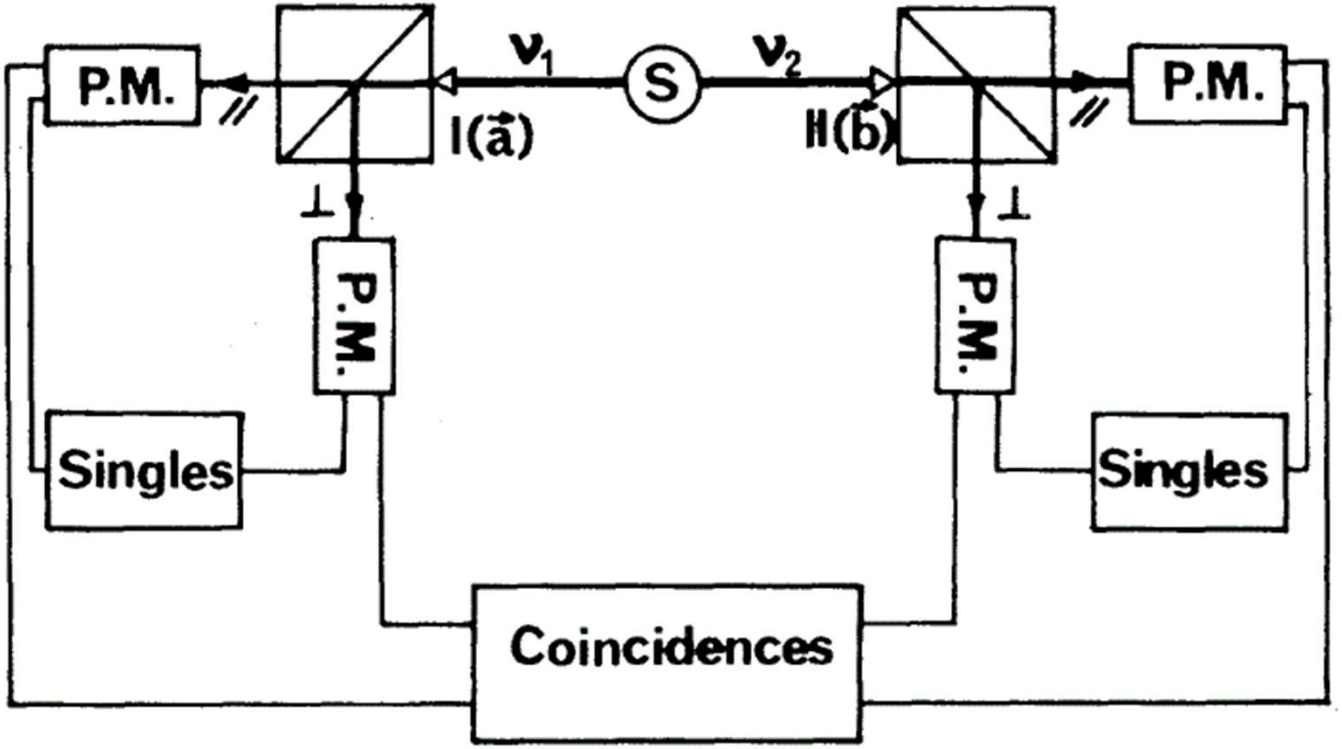
$$\langle M_{11} \rangle + \langle M_{21} \rangle + \langle M_{22} \rangle - \langle M_{12} \rangle = -2 \cdot \left(\cos(2\beta) + \sin(2\beta) \right) = -2\sqrt{2} \cdot \sin\left(2\beta + \frac{\pi}{4} \right)$$

Résultats expérimentaux: Expérience EPR

Alain Aspect, Orsay, 1982

!! Les inégalités de Bell sont violées !!

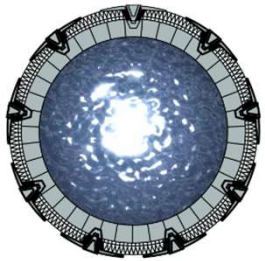
A. Aspect
Nobel Prize 2022



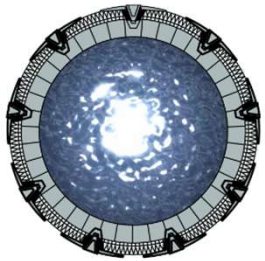
A. Aspect, et al. « Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bell's inequalities », *Physical Review Letters*, Vol. 49, nº 2, p. 91–94 (1982)

Téléportation quantique

Vision «stargate»



Vision «stargate»



Classical Teleportation

Object O

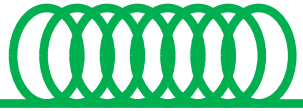
Alice **Bob**

Classical Teleportation

Object O

Canal normal

Recette



Object O

Ingrédients

Alice

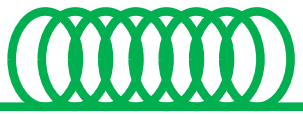
Bob

Quantum Measurements

Qbit A
(Superposition quantique de deux états)

Mesure 1
Projection
Mesure 2
!!! Erreur !!!
Mesure 3
….
→ Fausse recette

Canal normal



Qbit P
«Perturbé»

Alice

Bob

Téléportation quantique : exemple

Manipulation
(interaction sans
extraire des infos)

→ **Intrication = Interdépendance forte à distance et instantanée**

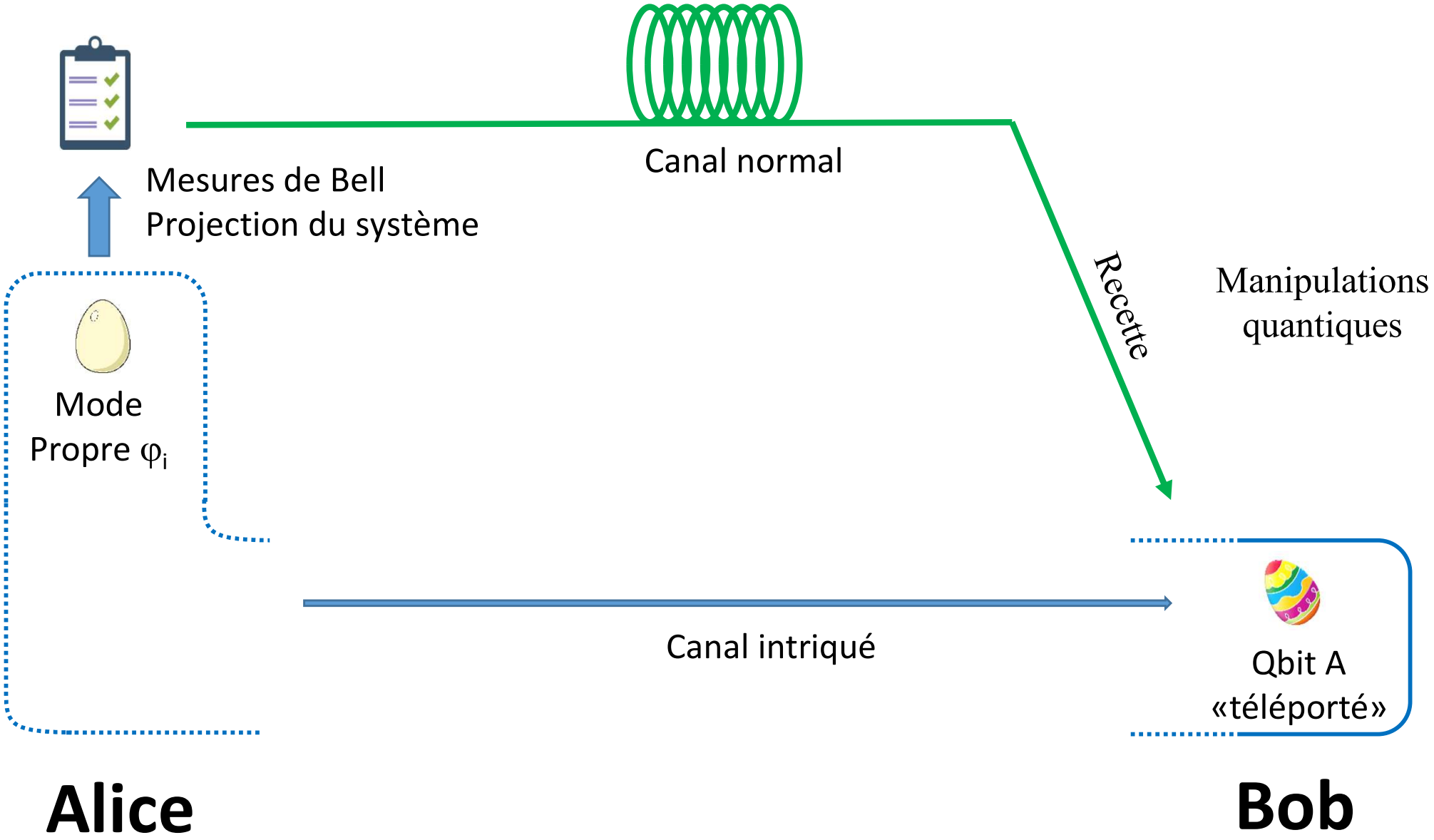
Qbit $\overline{A}$
intriqué

Qbit $\overline{Q}$
intriqué

Alice

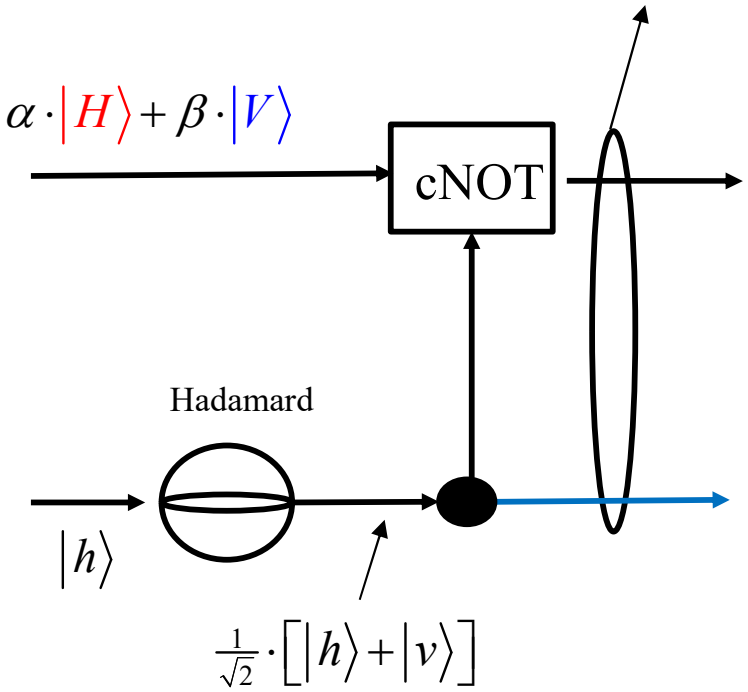
Bob

Téléportation quantique : exemple



Détails mathématiques

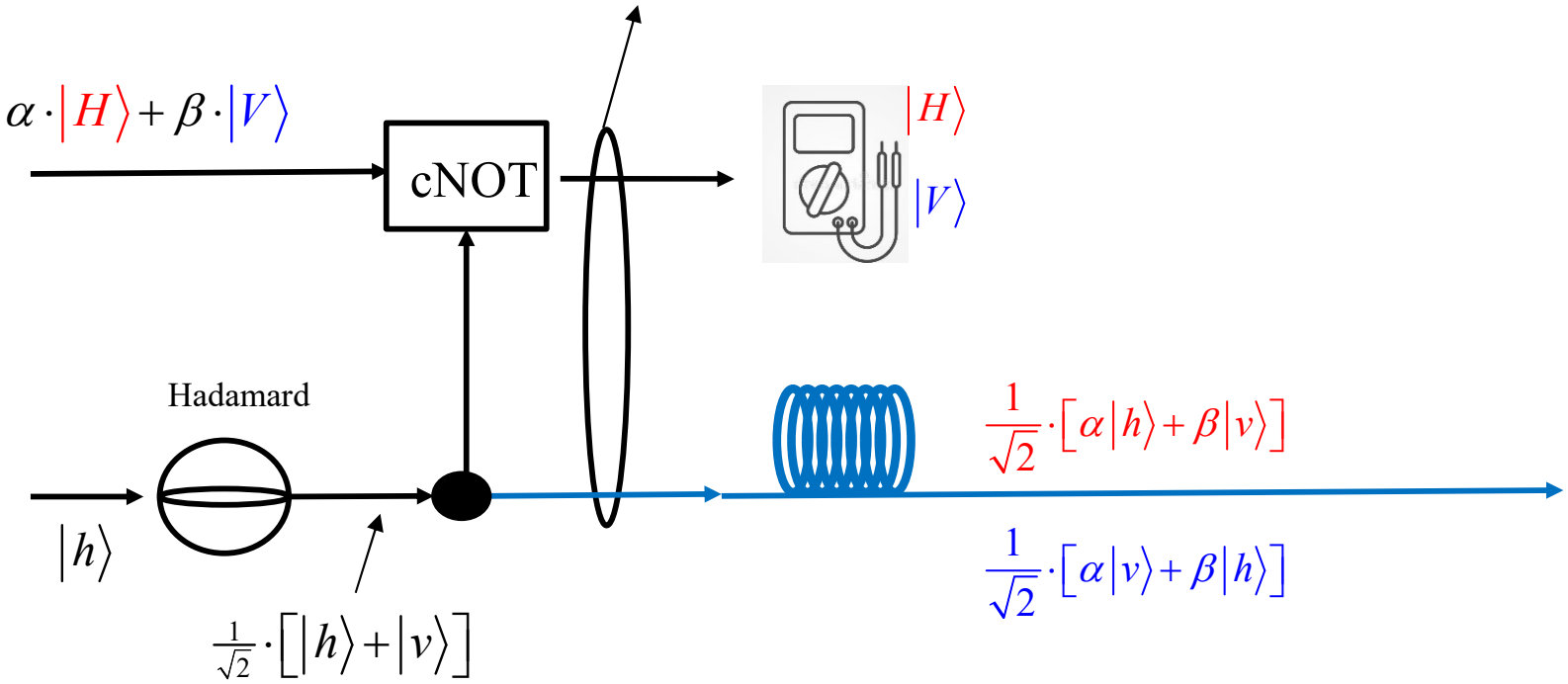
$$\frac{1}{\sqrt{2}}|h\rangle\cdot\left[\alpha|H\rangle+\beta|V\rangle\right] \quad +\frac{1}{\sqrt{2}}|v\rangle\cdot\left[\alpha|V\rangle+\beta|H\rangle\right]$$



Détails mathématiques

$$\frac{1}{\sqrt{2}}|h\rangle\cdot\left[\alpha|H\rangle+\beta|V\rangle\right] \quad +\frac{1}{\sqrt{2}}|v\rangle\cdot\left[\alpha|V\rangle+\beta|H\rangle\right]$$

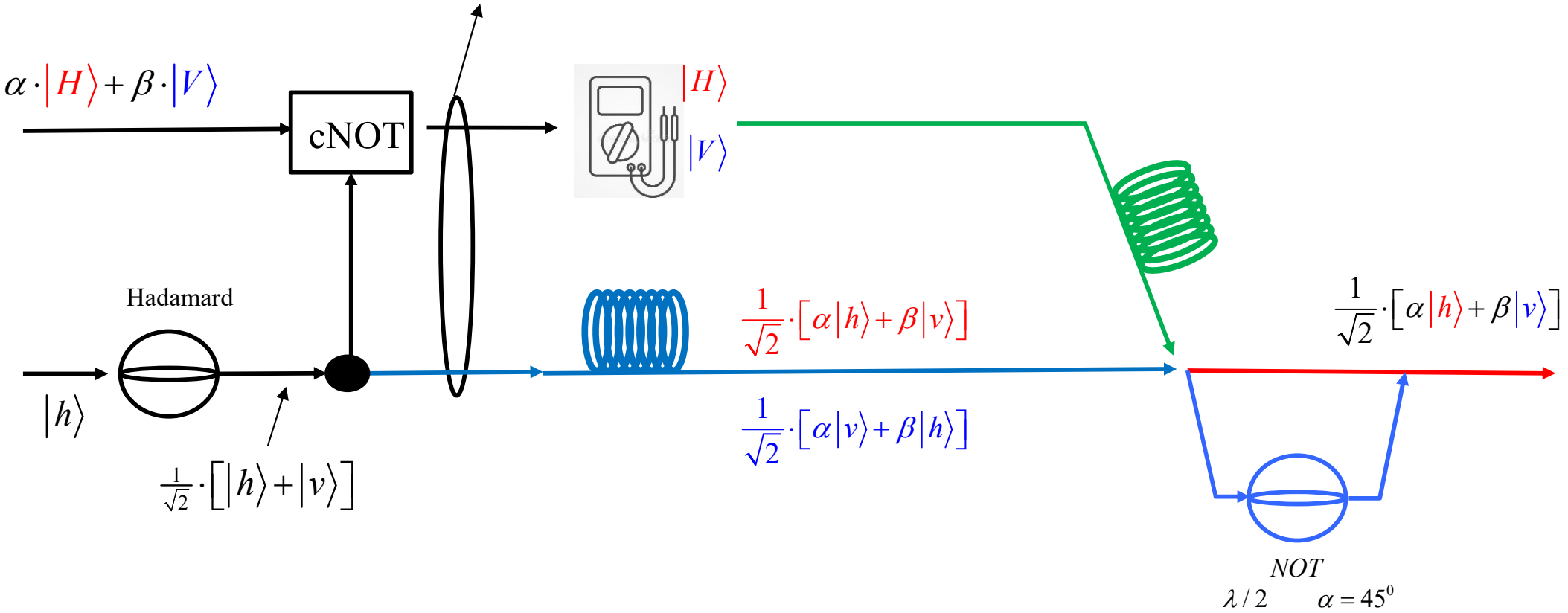
$$= \quad |H\rangle\cdot\frac{1}{\sqrt{2}}\cdot\left[\alpha|h\rangle+\beta|v\rangle\right] \quad +|V\rangle\cdot\frac{1}{\sqrt{2}}\cdot\left[\alpha|v\rangle+\beta|h\rangle\right]$$



Détails mathématiques

$$\frac{1}{\sqrt{2}}|h\rangle\cdot\left[\alpha|H\rangle+\beta|V\rangle\right] \quad +\frac{1}{\sqrt{2}}|v\rangle\cdot\left[\alpha|V\rangle+\beta|H\rangle\right]$$

$$= \quad |H\rangle\cdot\frac{1}{\sqrt{2}}\cdot\left[\alpha|h\rangle+\beta|v\rangle\right] \quad +|V\rangle\cdot\frac{1}{\sqrt{2}}\cdot\left[\alpha|v\rangle+\beta|h\rangle\right]$$



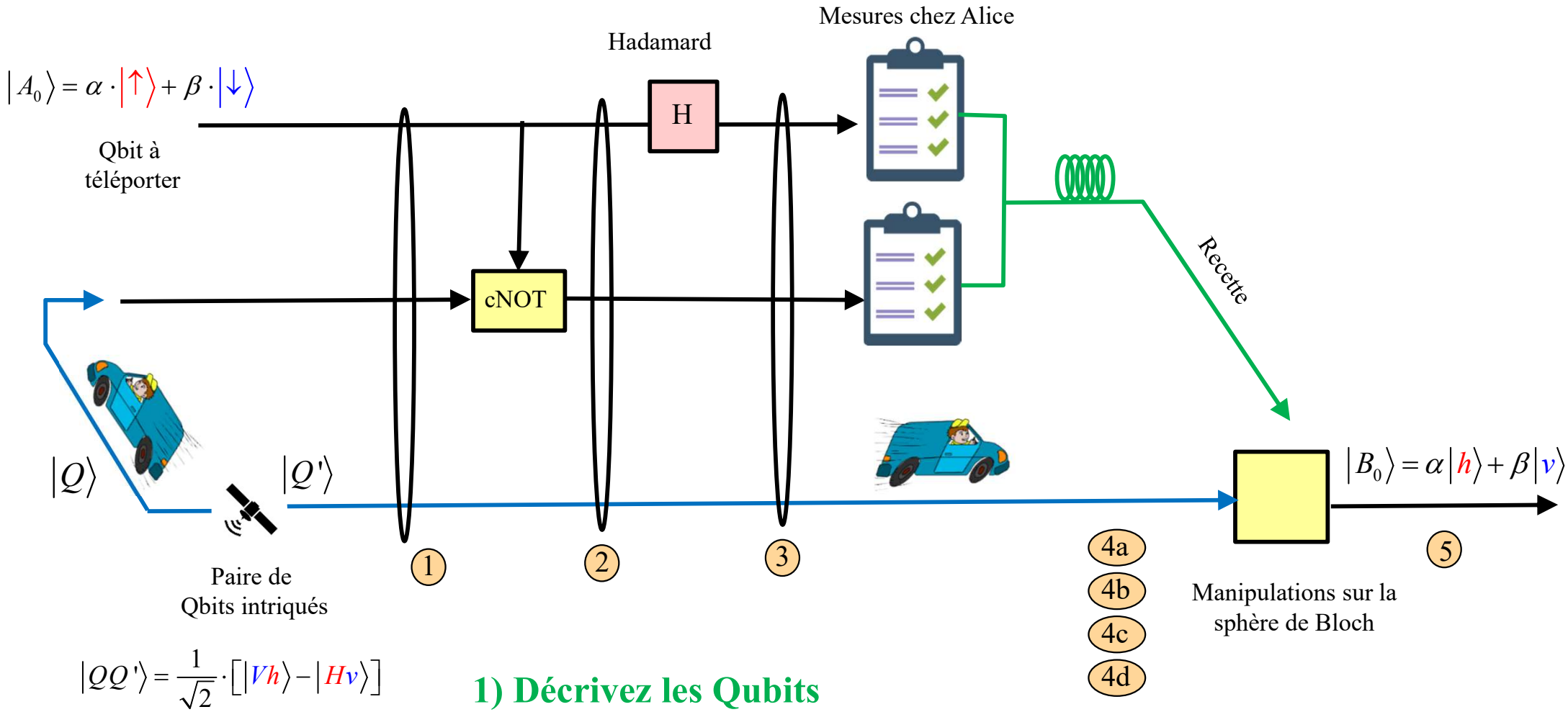
Dieu joue aux dés !

…

A nous d'en profiter !

- **Cryptographie** ✓
- **Téléportation** ✓
- **Clonage** ⊗
- **Quantum computing** ✓

Exercice 11.1:
Téléportation second schéma



1) Décrivez les Qubits aux différentes étapes: 1---5.

2) Déterminez les manipulations nécessaires pour retrouver chez Bob le Qubit de départ.