COLLÈGE DE FRANCE
1530

Algorithmes quantiques

Information quantique, premières utilisations calculatoires

07-04-2021

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

Présentation de la séance

- Présentation et fonctionnement de l'ensemble des cours et séminaires

- Cours 1 : Information quantique, premières utilisations

  Superposition, mesure, transformation, non-clonage, distribution quantique de clés, téléportation

- Séminaire 1 : Réseaux de communication quantique

  avec Eleni Diamanti, CNRS, Paris

Présentation et fonctionnement

8 Cours - 8 séminaires

7 avril - 9 juin 2021

- Cours : accessible à tous

  Questions à

  frederic.magniez@college-de-france.fr

  Réponses au début du cours suivant

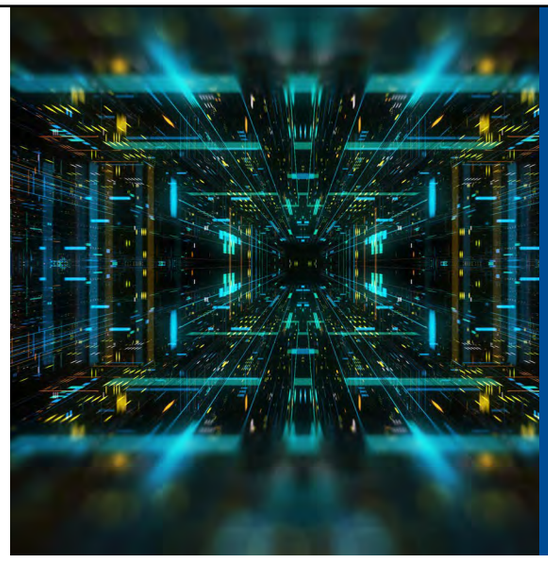
- Séminaires en prolongement de chaque cours

  Questions à l'orateur par email

  Réponses par email

- Enregistrement : Les mercredis 10h-12h30

- Diffusion : Dès le vendredi/samedi



COLLÈGE DE FRANCE
1530

CHAIRE INFORMATIQUE ET SCIENCES NUMÉRIQUES
Année académique 2020-2021

Frédéric MAGNIEZ

Algorithmes quantiques

Cours les mercredis de 10h à 11h30,
suivis des séminaires de 11h30 à 12h30
Salle 5

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*
05 mai 2021	**Cours :** Circuits quantiques, premiers algorithmes : portes universelles, algorithmes de Deutsch-Jozsa et Bernstein-Vazirani, supériorité des algorithmes quantiques **Séminaire :** Langages graphiques pour programmer et raisonner en informatique quantique Simon PERDRIX, *CNRS, Nancy*
12 mai 2021	**Cours :** Transformée de Fourier quantique I : réalisation, estimation de phase, algorithmes de Simon et de Shor (recherche de période et factorisation) et généralisations récentes **Séminaire :** Le problème du sous-groupe caché, Miklos SANTHA, *CNRS, Paris et CQT, Singapour*
19 mai 2021	**Cours :** Optimisation quantique : algorithme de Grover, estimateurs quantiques, chaînes de Markov quantiques, heuristiques quantiques **Séminaire :** A Unified Framework for Quantum Walk Search, Stacey JEFFERY, *CWI, Amsterdam*
26 mai 2021	**Cours :** Transformée de Fourier quantique II : résolution ultra-rapide de systèmes linéaires et applications en technique d'apprentissage automatique **Séminaire :** Quantum Machine Learning, Iordanis KERENIDIS, *CNRS, Paris*
02 juin 2021	**Cours :** Limites et impact du calcul quantique : complexité en requêtes, simulation classique, déquantization d'algorithmes quantiques **Séminaire :** Suprématie quantique : où en sommes-nous aujourd'hui ? André CHAILLOUX, *Inria, Paris*
09 juin 2021	**Cours :** Derniers développements pour l'internet et intelligence artificielle quantique : apprentissage, optimisation, calcul délégué et sécurisé, calcul distribué **Séminaire :** Quantum Computing as a Service: Secure and Verifiable Multi-Tenant Quantum Data Centre Elham KASHEFI, *CNRS, Paris et University of Edinburgh*

Chaire crée avec le soutien de

Inria

11, place Marcelin-Berthelot, 75005 Paris
www.college-de-france.fr

Thomas Römer
Administrateur du Collège de France

Partie 1 - 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*

Partie 2 - Les bases algorithmiques

- Concepts du calcul et principales méthodes algorithmiques
- Mise en évidence de propriétés algébriques (déchiffrement)
- Optimisation et applications algorithmiques

05 mai 2021

Cours : Circuits quantiques, premiers algorithmes : portes universelles, algorithmes de Deutsch-Jozsa et Bernstein-Vazirani, supériorité des algorithmes quantiques

Séminaire : Langages graphiques pour programmer et raisonner en informatique quantique
Simon PERDRIX, *CNRS*, *Nancy*

12 mai 2021

Cours : Transformée de Fourier quantique I : réalisation, estimation de phase, algorithmes de Simon et de Shor (recherche de période et factorisation) et généralisations récentes

Séminaire : Le problème du sous-groupe caché, Miklos SANTHA, *CNRS*, *Paris et CQT*, *Singapour*

19 mai 2021

Cours : Optimisation quantique : algorithme de Grover, estimateurs quantiques, chaînes de Markov quantiques, heuristiques quantiques

Séminaire : A Unified Framework for Quantum Walk Search, Stacey JEFFERY, *CWI*, *Amsterdam*

Partie 3 - Algorithmique avancée

- Apprentissage automatique
- Limites du calcul quantique
- Usage décentralisé de type Internet.

26 mai 2021

Cours : Transformée de Fourier quantique II : résolution ultra-rapide de systèmes linéaires et applications en technique d'apprentissage automatique

Séminaire : Quantum Machine Learning, Iordanis KERENIDIS, *CNRS*, *Paris*

02 juin 2021

Cours : Limites et impact du calcul quantique : complexité en requêtes, simulation classique, déquantization d'algorithmes quantiques

Séminaire : Suprématie quantique : où en sommes-nous aujourd'hui ?
André CHAILLOUX, *Inria*, *Paris*

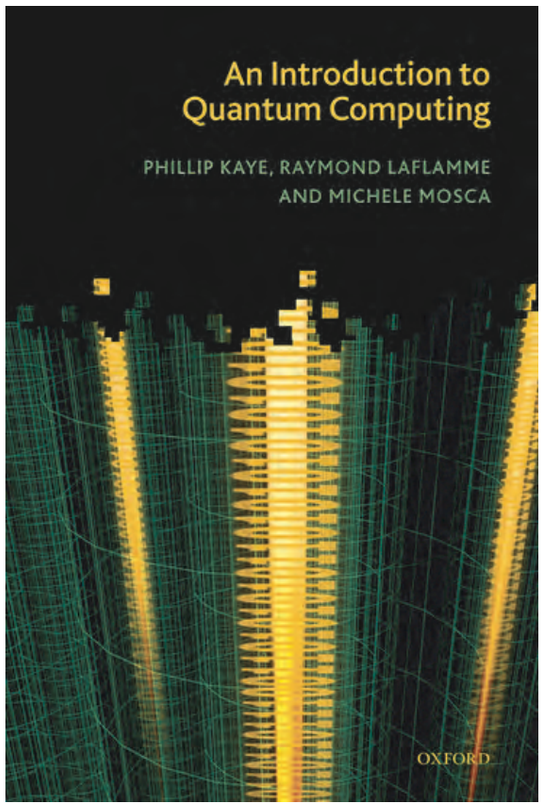
09 juin 2021

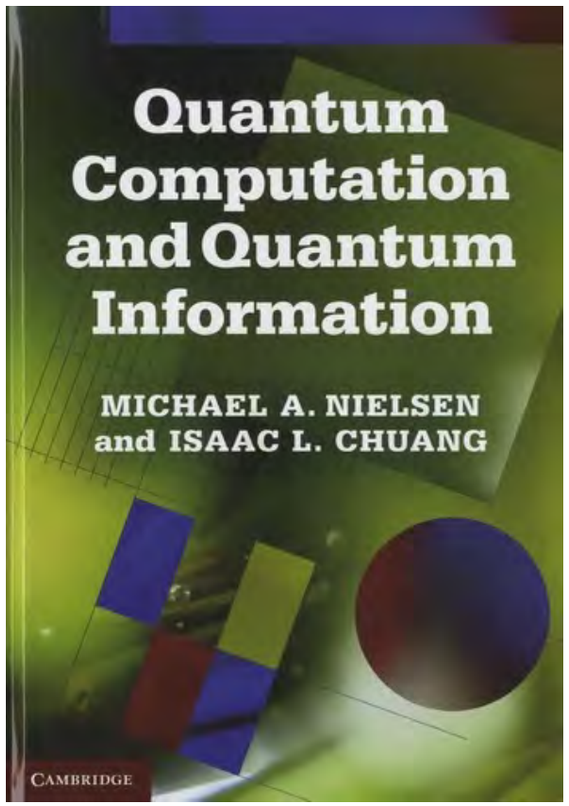
Cours : Derniers développements pour l'internet et intelligence artificielle quantique : apprentissage, optimisation, calcul délégué et sécurisé, calcul distribué

Séminaire : Quantum Computing as a Service:
Secure and Verifiable Multi-Tenant Quantum Data Centre
Elham KASHEFI, *CNRS*, *Paris et University of Edinburgh*

Livres de référence (mais anciens)

- *An Introduction to Quantum Computing*. Kaye, Laflamme, Mosca. Oxford University Press.
- *Quantum Computation and Quantum Information*. Nielsen, Chuang. Cambridge: Cambridge University Press.





Algorithmes

- Notes de cours

  Ronald de Wolf : https://homepages.cwi.nl/~rdewolf/qcnotes.pdf
  Andrew Childs : https://www.cs.umd.edu/~amchilds/qa/qa.pdf

- Quantum algorithm zoo

  https://quantumalgorithmzoo.org

Programmation

- Qiskit

  https://qiskit.org

- Beaucoup d'autres possibilités

  https://en.wikipedia.org/wiki/Quantum_programming

Méthode quantique

- "Survey" de Andrew Drucker et Ronald de Wolf

  http://theoryofcomputing.org/articles/gs002/gs002.pdf

Algorithmes quantiques

Cours 1 - 6/04/2021

Information quantique,
premières utilisations calculatoires :
superposition, mesure, transformation, non-clonage,
distribution quantique de clés, téléportation

Ecole de Copenhague (Bohr, Heisenberg, …) 1920-30

- Parler des propriétés physiques d'un système indépendamment de mesure n'a pas de sens

  L'état d'une particule quantique n'est fixé qu'après une mesure

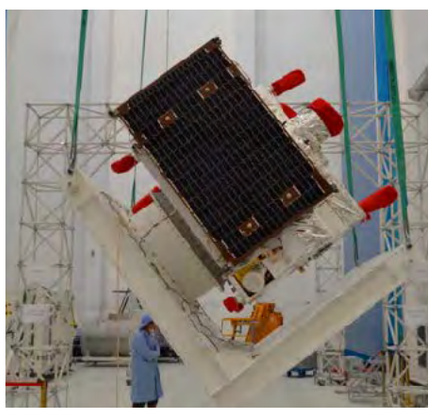
Utilisation en informatique quantique

- Protocole quantique de chiffrement [Bennett, Brassard'84]

  Sécurité basée sur les lois de la physique quantique…

  et utilisable en pratique !

Prototype 1984

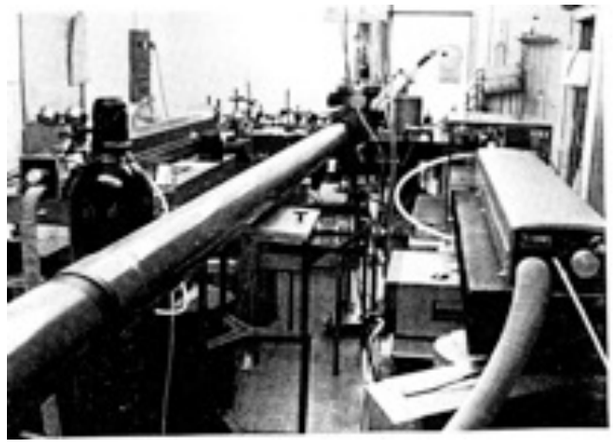


Satellite chinois dédié aux communications quantiques 2016

Paradoxe d'Einstein, Podolsky, Rosen 1935

- Des particules très éloignées restent-elles liées !?

- Aspect, Grangier, Roger, Dalibard'80-82 : Oui !


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

Utilisation en informatique (pour ce cours)

- Téléportation quantique : [Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters'93]
  - 1 photon [Popescu et al : Rome'97][Zeilinger et al : Innsbruck'97]
  - 1 photon, 6 km [Gisin et al : Genève'02]
  - 1 atome [Blatt et al : Innsbruck'04]
  - Par satellite (1400km) [Pan et al : Tibet'17]


Expérience de téléportation, Australie'02.

Filtre polarisant : expérience

Un filtre

- Peu importe l'orientation : l'intensité de lumière est identique

Filtre polarisant : expérience

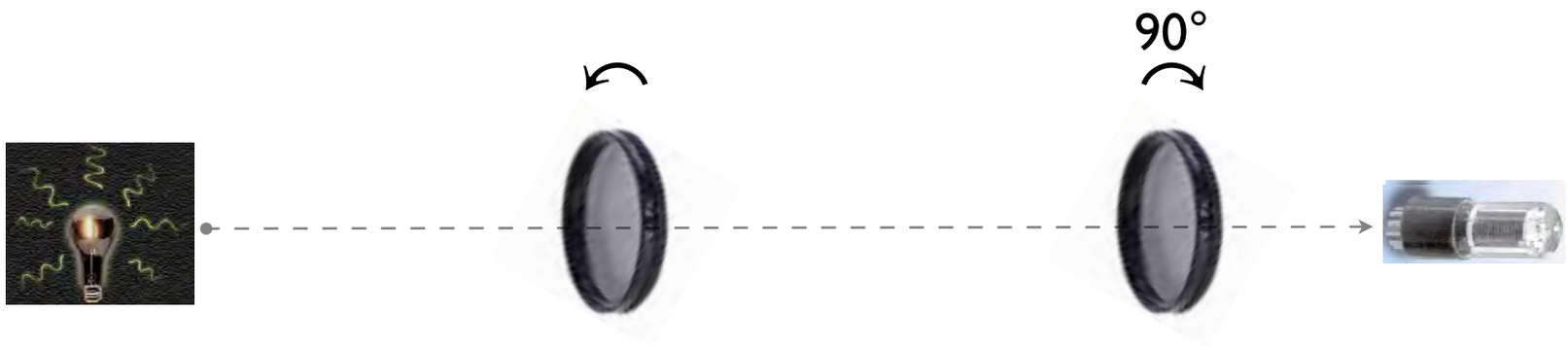
Un filtre

- Peu importe l'orientation : l'intensité de lumière est identique

Deux filtres identiques

- Sur un écart : l'intensité est identique
- Sur un autre décalé de 90° : l'intensité est nulle

Filtre polarisant : expérience



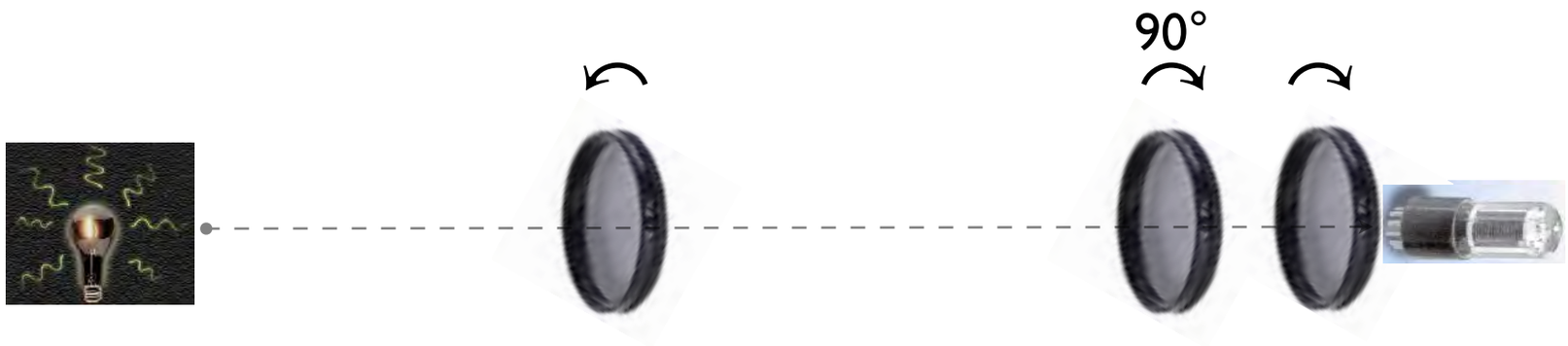
Un filtre

- Peu importe l'orientation : l'intensité de lumière est identique

Deux filtres identiques

- Sur un écart : l'intensité est identique
- Sur un autre décalé de 90° : l'intensité est nulle

Filtre polarisant : expérience



Un filtre

- Peu importe l'orientation : l'intensité de lumière est identique

Deux filtres identiques

- Sur un écart : l'intensité est identique
- Sur un autre décalé de 90° : l'intensité est nulle

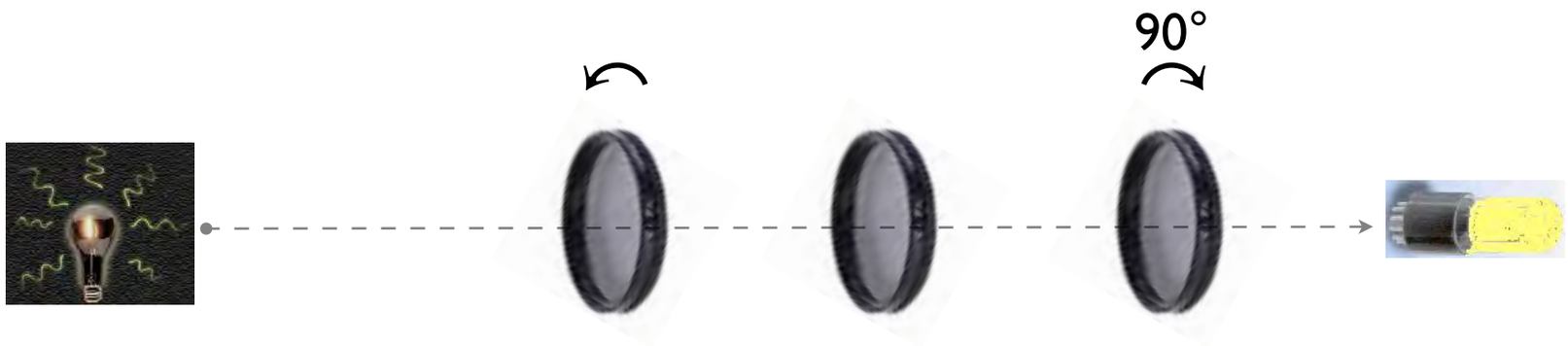
Trois filtres identiques

- Si le filtre est en dernier, l'intensité reste nulle (peu importe la rotation)
- S'il est en 2e

    Sur un écart : la lumière réapparaît jusqu'à 25% d'intensité

    Sur un autre décalé de 45° : l'intensité est à nouveau nulle

Filtre polarisant : expérience



Un filtre

- Peu importe l'orientation : l'intensité de lumière est identique

Deux filtres identiques

- Sur un écart : l'intensité est identique
- Sur un autre décalé de 90° : l'intensité est nulle

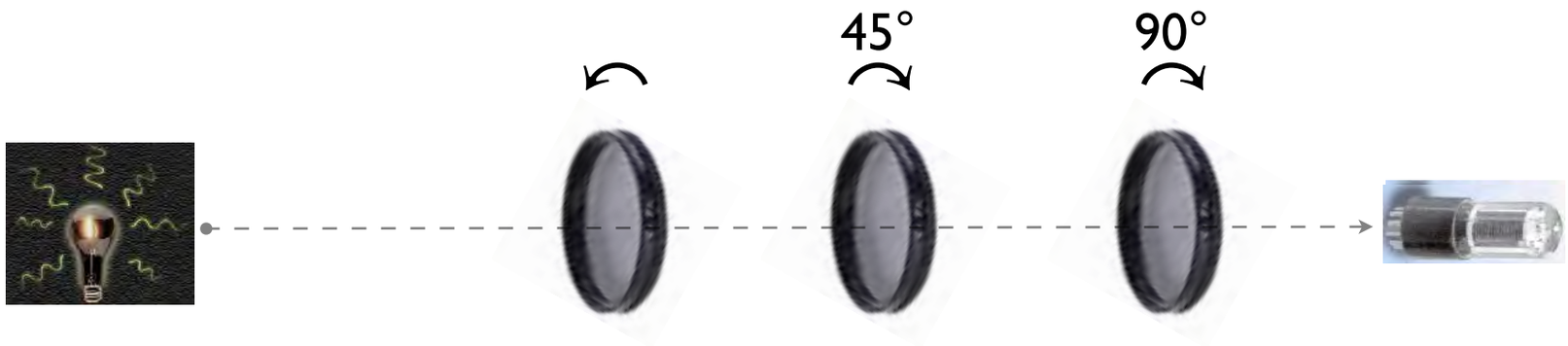
Trois filtres identiques

- Si le filtre est en dernier, l'intensité reste nulle (peu importe la rotation)
- S'il est en 2e

    Sur un écart : la lumière réapparaît jusqu'à 25% d'intensité

    Sur un autre décalé de 45° : l'intensité est à nouveau nulle

Filtre polarisant : expérience



Un filtre

- Peu importe l'orientation : l'intensité de lumière est identique

Deux filtres identiques

- Sur un écart : l'intensité est identique
- Sur un autre décalé de 90° : l'intensité est nulle

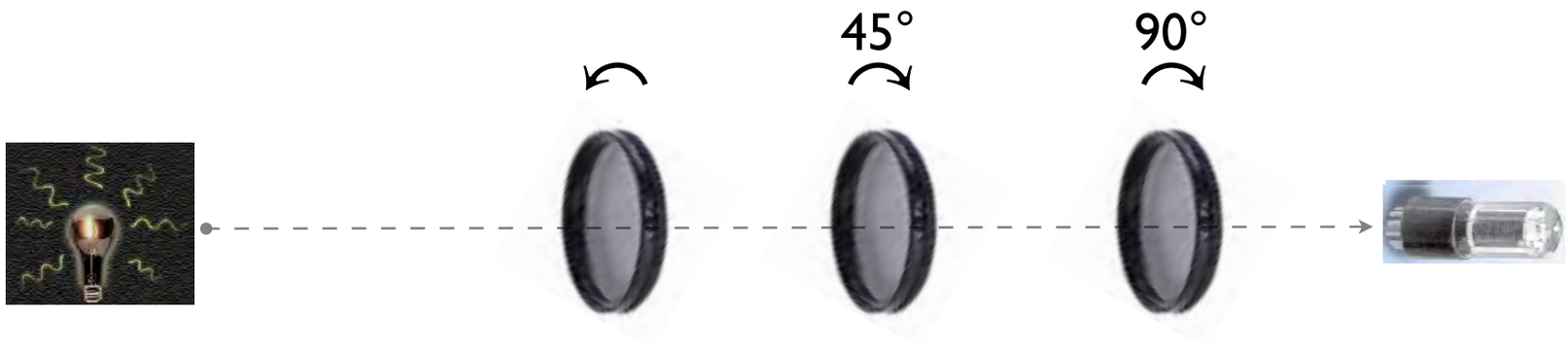
Trois filtres identiques

- Si le filtre est en dernier, l'intensité reste nulle (peu importe la rotation)
- S'il est en 2e

  Sur un écart : la lumière réapparaît jusqu'à 25% d'intensité

  Sur un autre décalé de 45° : l'intensité est à nouveau nulle

Filtre polarisant : expérience



Un filtre

- Peu importe l'orientation : l'intensité de lumière est identique

Deux filtres identiques

- Sur un écart : l'intensité est identique
- Sur un autre décalé de 90° : l'intensité est nulle

Trois filtres identiques

- Si le filtre est en dernier, l'intensité reste nulle (peu importe la rotation)
- S'il est en 2e

  Sur un écart : la lumière réapparaît jusqu'à 25% d'intensité

  Sur un autre décalé de 45° : l'intensité est à nouveau nulle

Conclusion

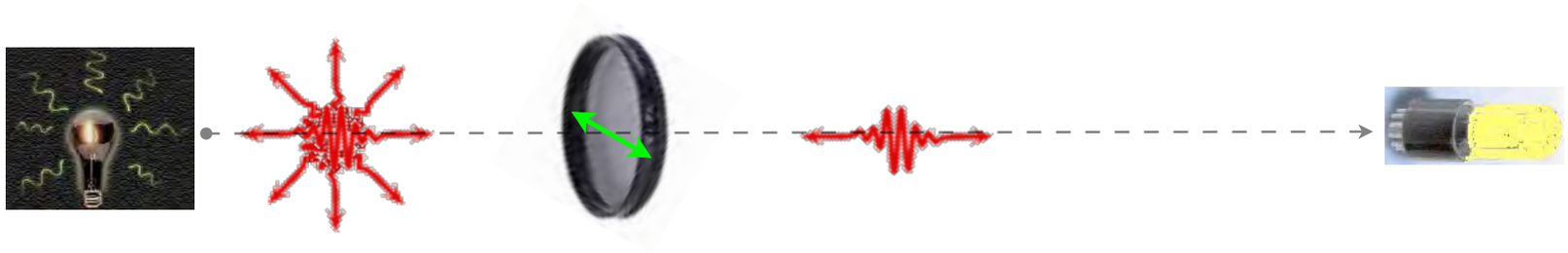
L'ordre des filtres est important

Filtre polarisant : explication

Caractéristiques de la lumière et des photons

- direction, longueur d'onde, polarisation

Filtre polarisant : explication



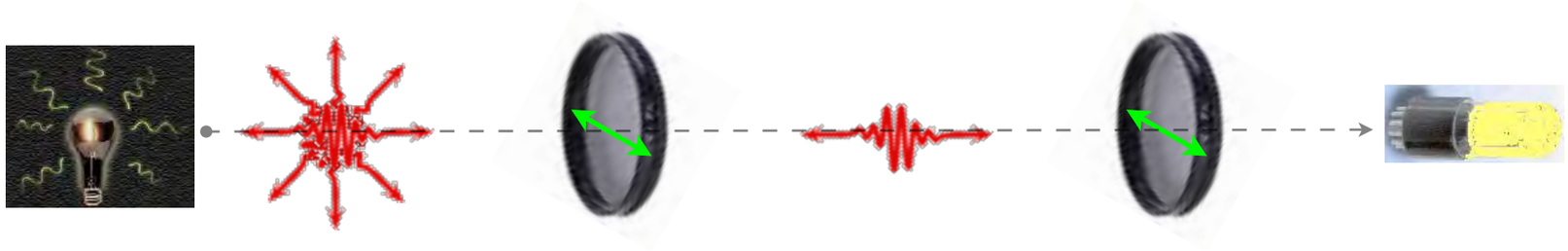
Caractéristiques de la lumière et des photons

- direction, longueur d'onde, polarisation

Sortie d'un filtre polarisant

- Lumière polarisée selon la direction du filtre.
- Lumière parallèle au filtre passe.
- Lumière orthogonale au filtre ne passe pas.

Filtre polarisant : explication



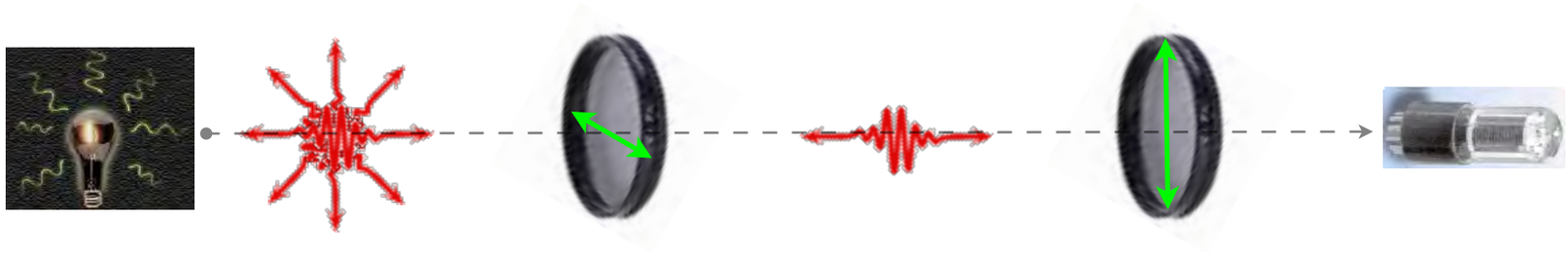
Caractéristiques de la lumière et des photons

- direction, longueur d'onde, polarisation

Sortie d'un filtre polarisant

- Lumière polarisée selon la direction du filtre.
- Lumière parallèle au filtre passe.
- Lumière orthogonale au filtre ne passe pas.

Filtre polarisant : explication



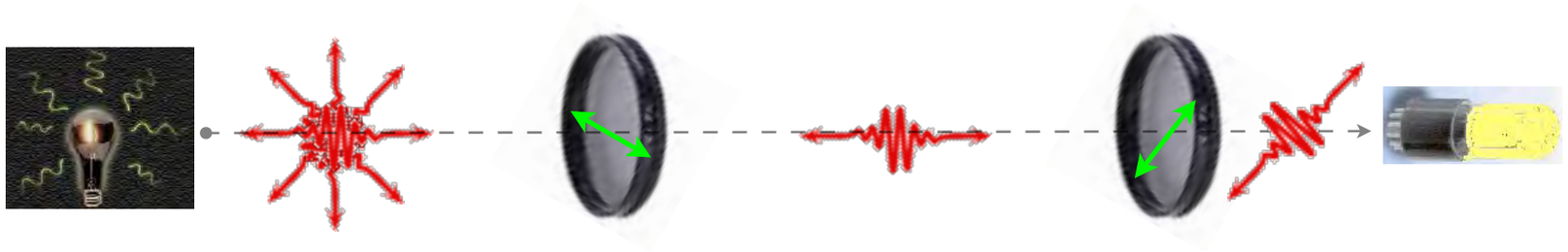
Caractéristiques de la lumière et des photons

- direction, longueur d'onde, polarisation

Sortie d'un filtre polarisant

- Lumière polarisée selon la direction du filtre.
- Lumière parallèle au filtre passe.
- Lumière orthogonale au filtre ne passe pas.

Filtre polarisant : explication



50 %

Caractéristiques de la lumière et des photons

- direction, longueur d'onde, polarisation

Sortie d'un filtre polarisant

- Lumière polarisée selon la direction du filtre.
- Lumière parallèle au filtre passe.
- Lumière orthogonale au filtre ne passe pas.

Polarisation 45°

- La lumière passe mais diminuée de 50%

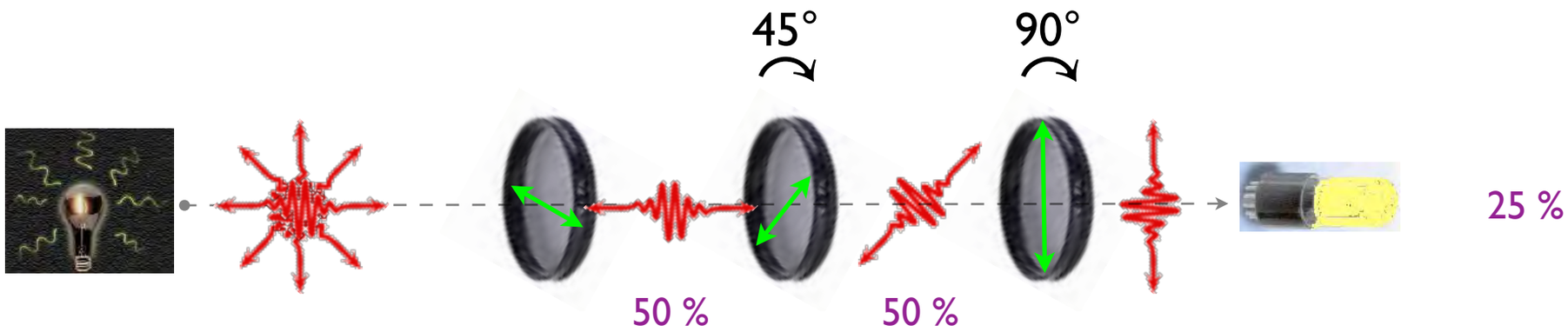
  Un photon sur deux est passé

  et se retrouve donc polarisé à 45°

  Le filtre modifie la polarisation

Filtre polarisant : retour sur l'expérience



Premier filtre

- La lumière est polarisée, par exemple horizontalement

Deuxième filtre

- La lumière est polarisée à 45°, mais perd 50% de son intensité

  Un photon sur deux est passé

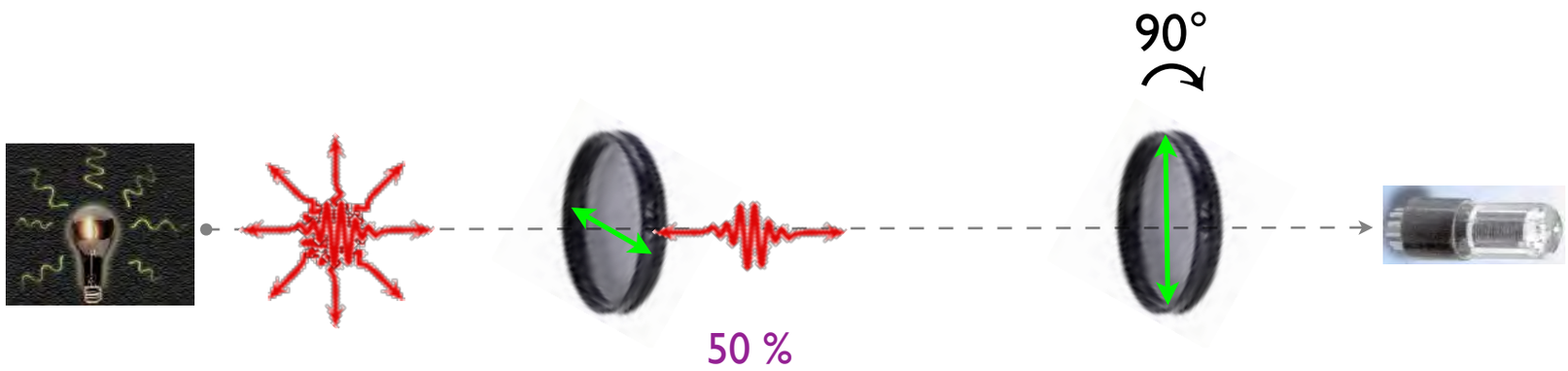
Troisième filtre

- La lumière est polarisée à 90°, mais perd encore 50% de son intensité

  Encore un photon sur deux est passé

  soit au total 25%

Filtre polarisant : retour sur l'expérience



Premier filtre

- La lumière est polarisée, par exemple horizontalement

Deuxième filtre

- La lumière est polarisée à 45°, mais perd 50% de son intensité

  Un photon sur deux est passé

Troisième filtre

- La lumière est polarisée à 90°, mais perd encore 50% de son intensité

  Encore un photon sur deux est passé

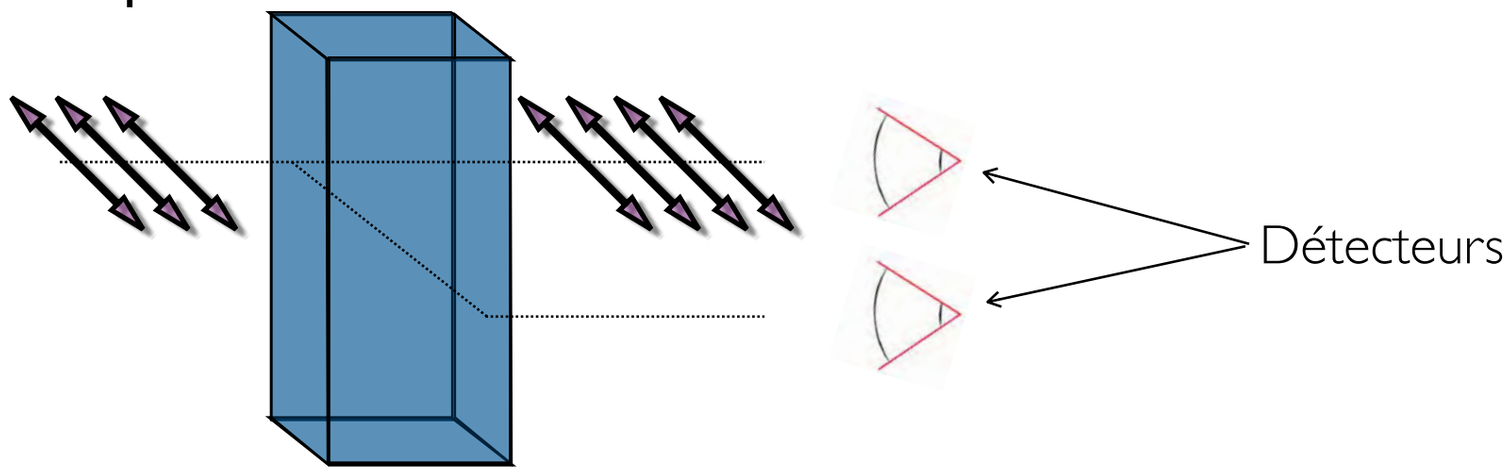
  soit au total 25%

Suppression 2e filtre

- La polarisation est orthogonale au dernier filtre, donc pas d'intensité

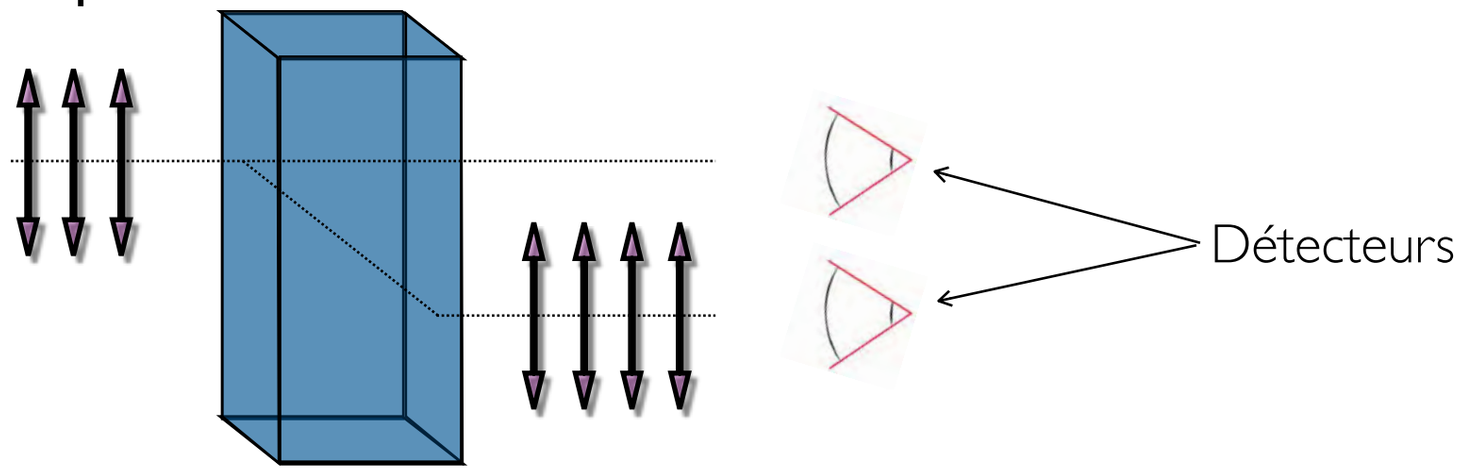
Cristal biréfringent (exemple : Calcite)

- Cristal sépare les polarisation horizontales et verticales



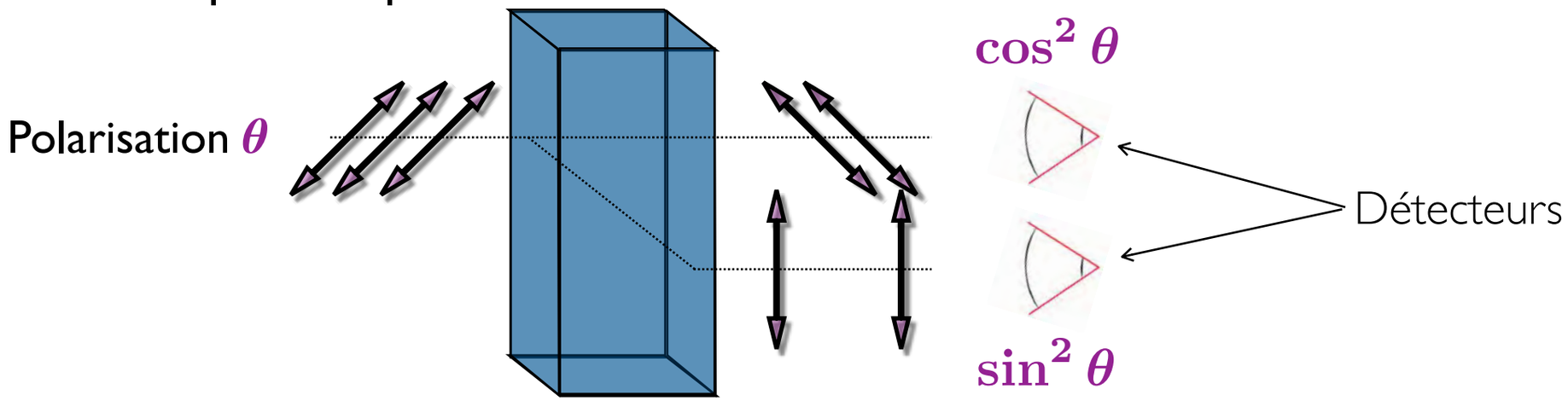
Cristal biréfringent (exemple : Calcite)

- Cristal sépare les polarisation horizontales et verticales



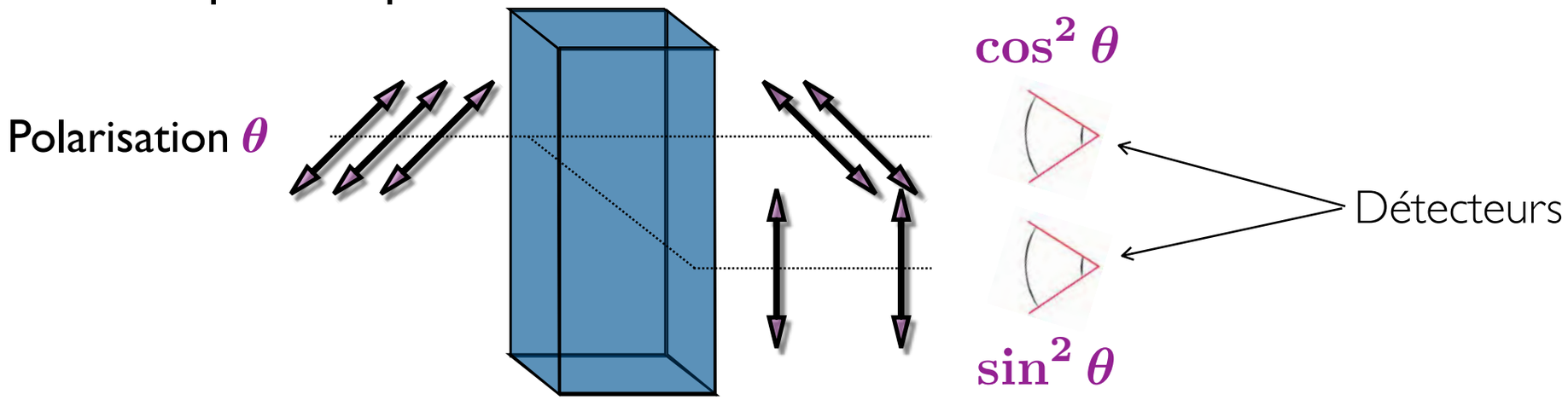
Cristal biréfringent (exemple : Calcite)

- Cristal sépare les polarisation horizontales et verticales



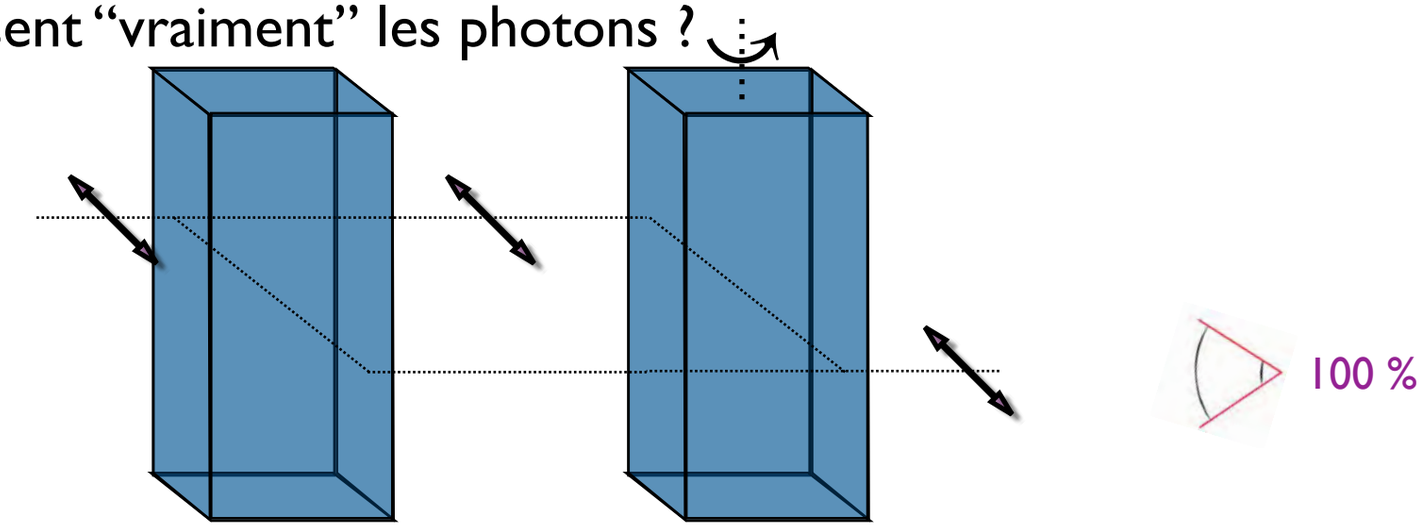
Cristal biréfringent (exemple : Calcite)

- Cristal sépare les polarisation horizontales et verticales



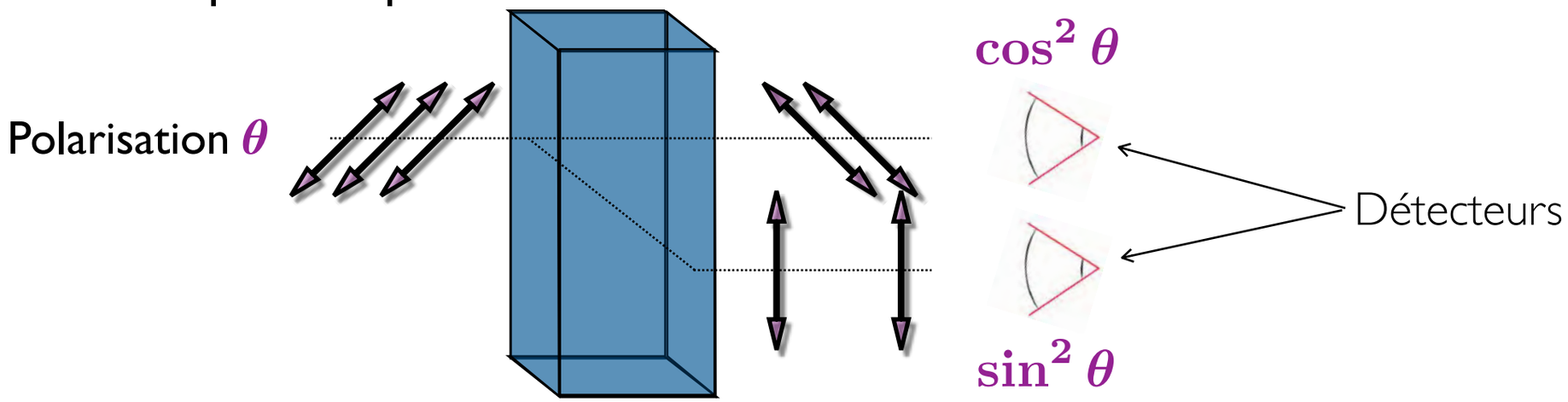
Deux cristaux en cascade (interféromètre)

- Par où passent "vraiment" les photons ?



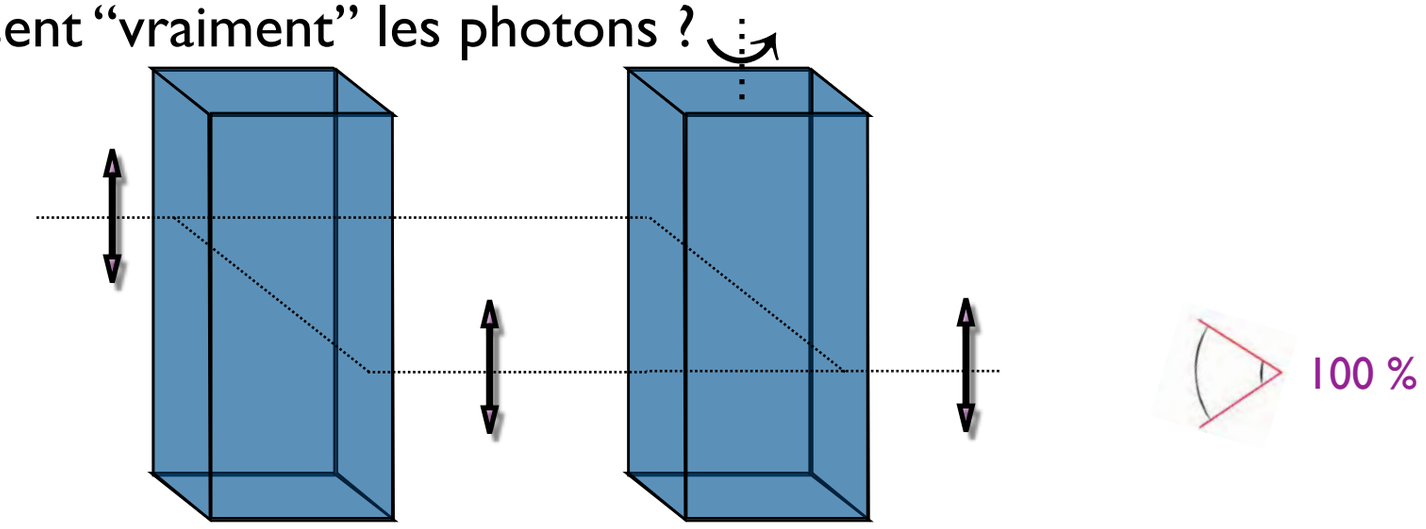
Cristal biréfringent (exemple : Calcite)

- Cristal sépare les polarisation horizontales et verticales



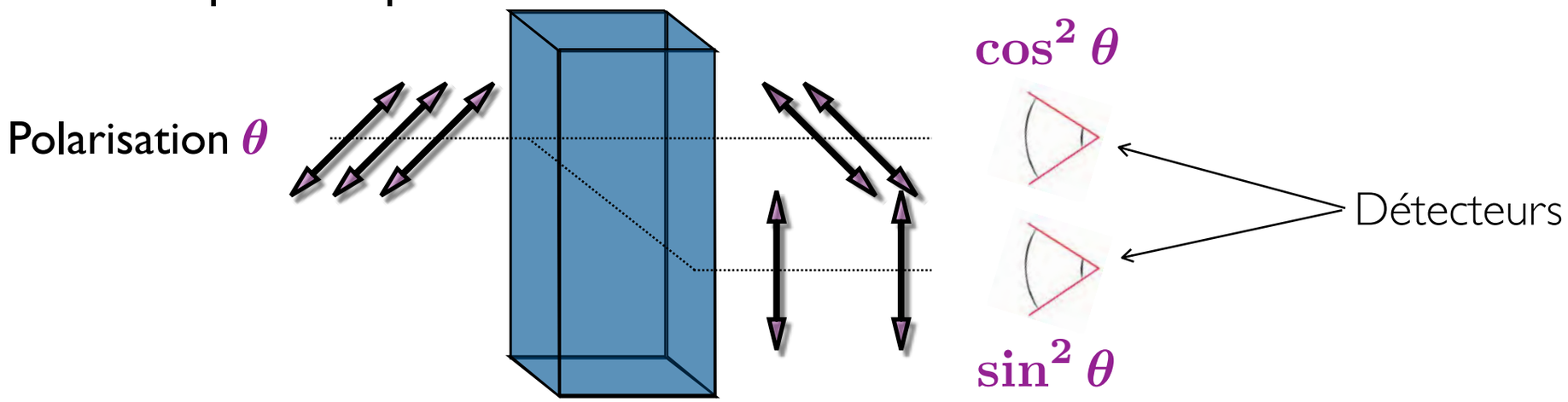
Deux cristaux en cascade (interféromètre)

- Par où passent "vraiment" les photons ?



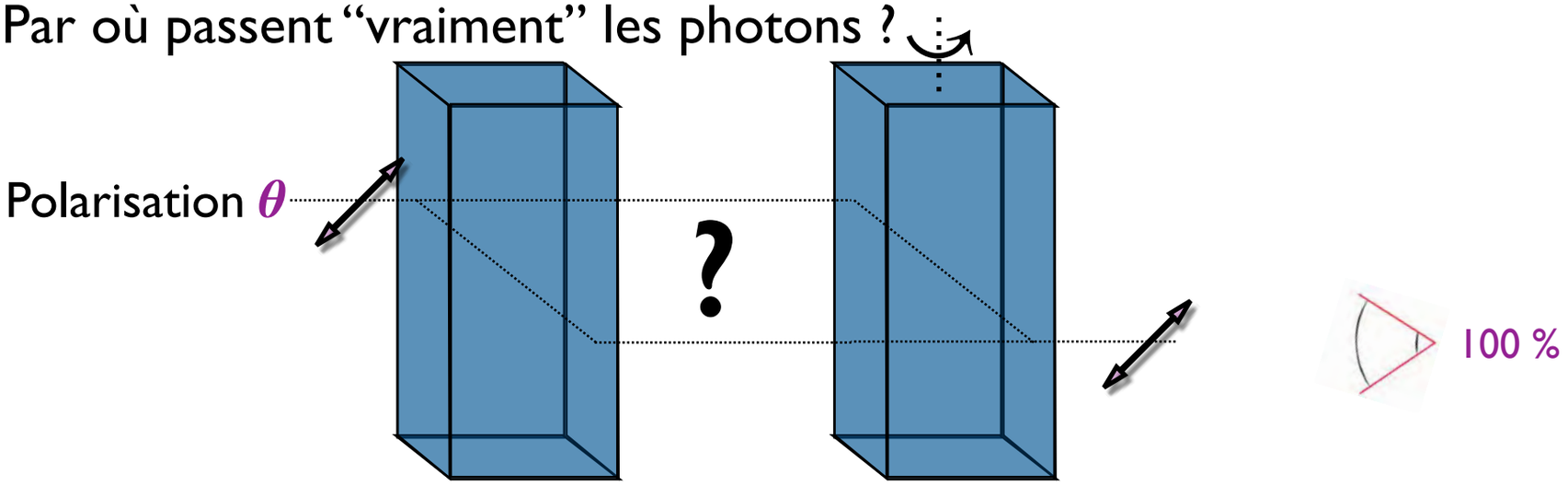
Cristal biréfringent (exemple : Calcite)

- Cristal sépare les polarisation horizontales et verticales



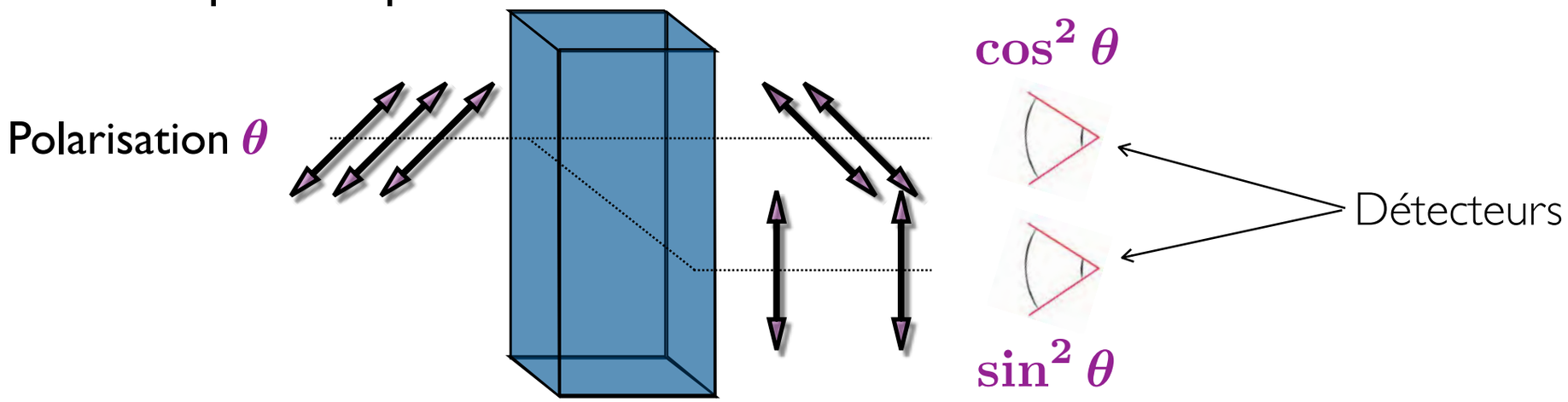
Deux cristaux en cascade (interféromètre)

- Par où passent "vraiment" les photons ?



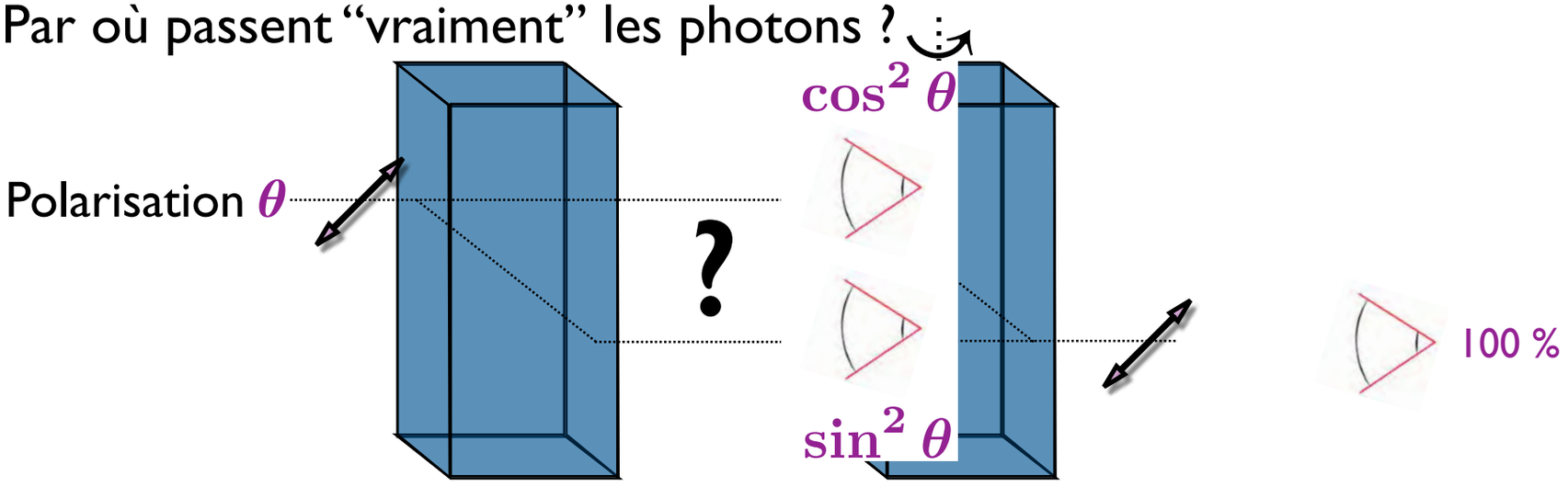
Cristal biréfringent (exemple : Calcite)

- Cristal sépare les polarisation horizontales et verticales



Deux cristaux en cascade (interféromètre)

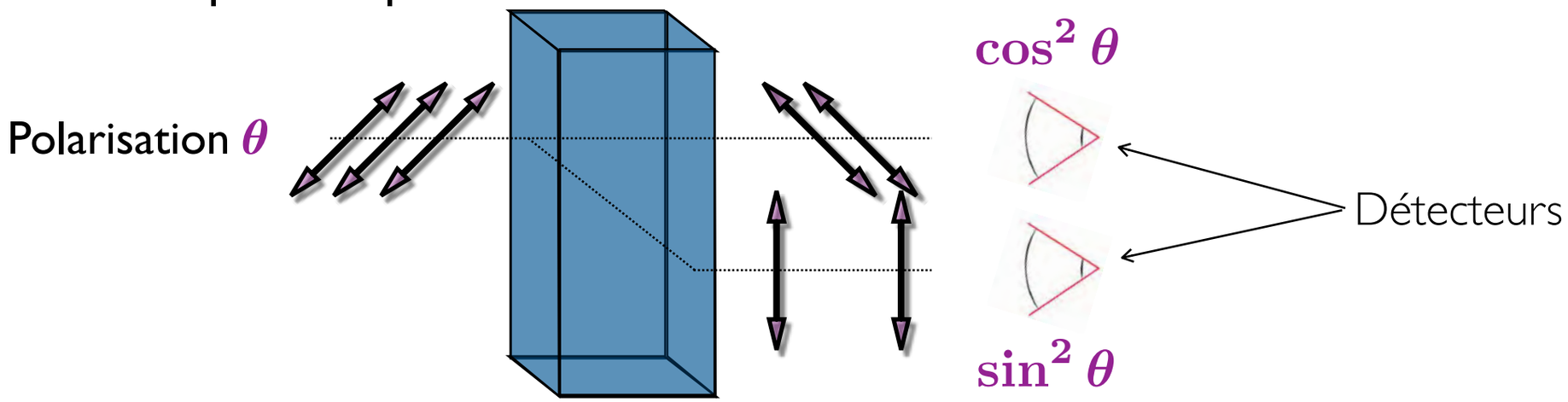
- Par où passent "vraiment" les photons ?



- Observons entre les cristaux : Parfois en haut et parfois en bas

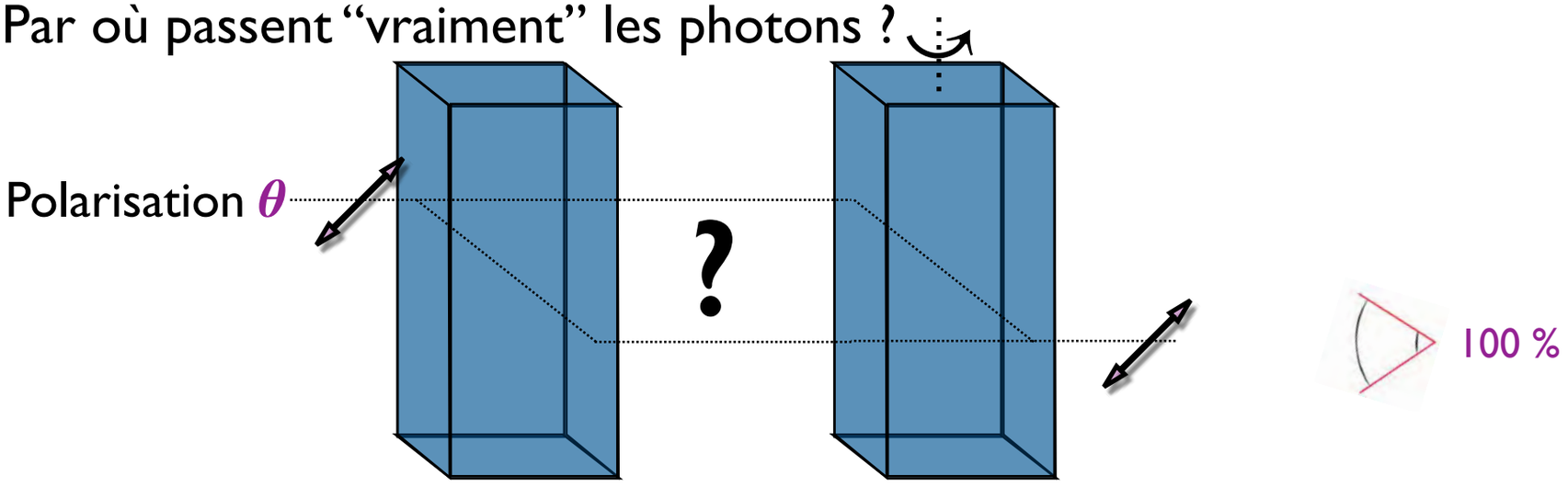
Cristal biréfringent (exemple : Calcite)

- Cristal sépare les polarisation horizontales et verticales



Deux cristaux en cascade (interféromètre)

- Par où passent "vraiment" les photons ?



- Observons entre les cristaux : Parfois en haut et parfois en bas
- Mais sans observation entre, le photon ressort toujours avec la polarisation initiale. Ce choix n'est donc pas fait !

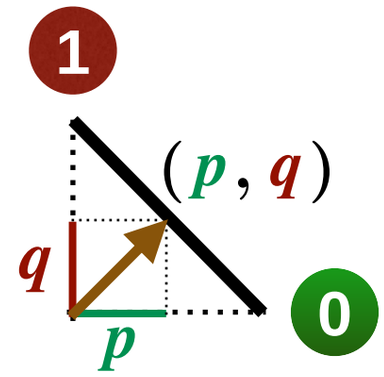
Principe de superposition

Bit classique

- Binary digit (Bit) : 0 ou 1
- Bit probabiliste

  (p, q) :"0" avec probabilité p ou "1" avec probabilité q

Description classique



$$p + q = 1$$

Bit quantique (qubit)

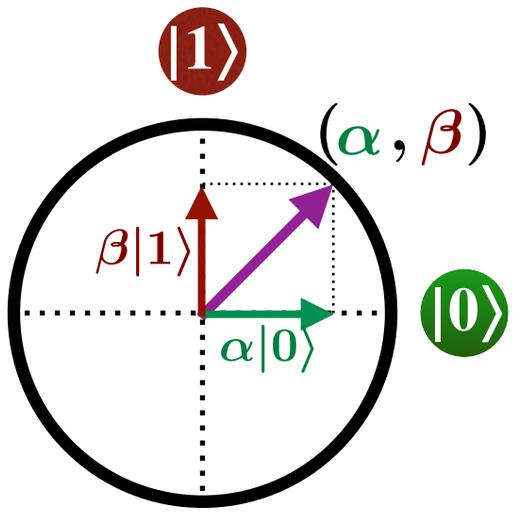
- Réalité quantique en amont de l'observation

  (α, β) : "0" avec amplitude α, "1" avec amplitude β

$$(\alpha, \beta) = \alpha|0\rangle + \beta|1\rangle$$

SUPERPOSITION

Description quantique



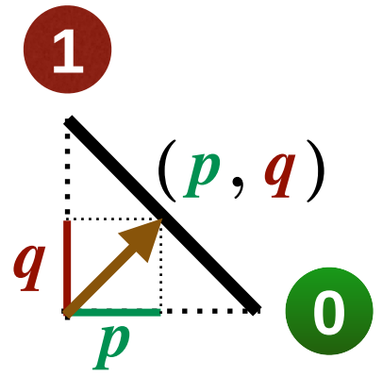
$$|\alpha|^2 + |\beta|^2 = 1$$

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

OBSERVATION ou MESURE

$$p = \alpha^2$$
$$q = \beta^2$$

Description classique



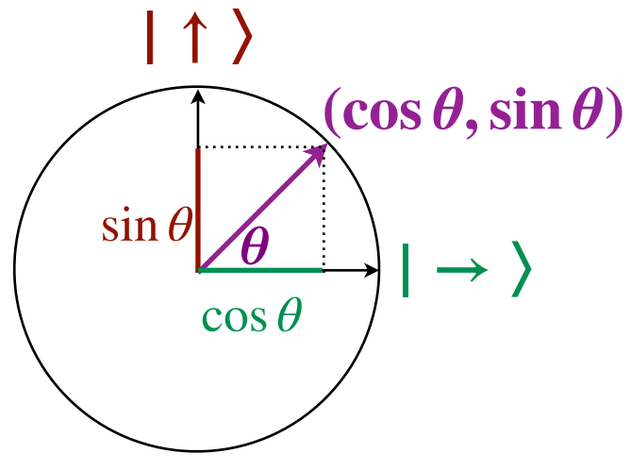
$$p + q = 1$$

Réalisation d'un qubit avec la polarisation

Etat quantique

- Polarisation: vecteur à 2 dimensions

$$(\cos\theta, \sin\theta) = \cos\theta|\rightarrow\rangle + \sin\theta|\uparrow\rangle$$



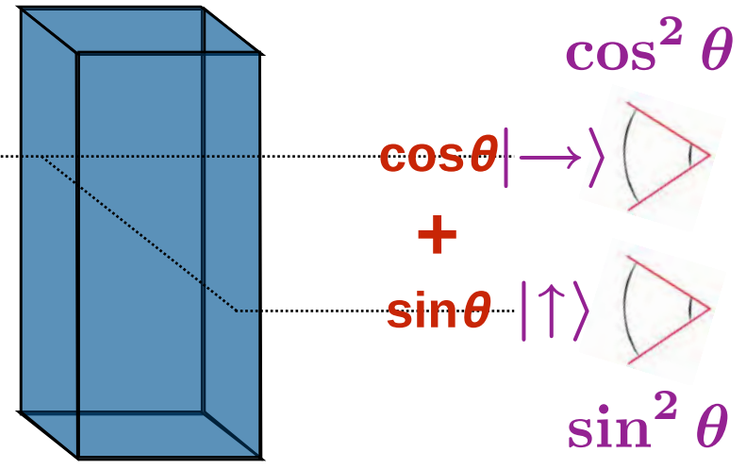
Mesure

- Calcite crystal

  sépare les polarisation horizontales et verticales

  mais aucun filtre n'est fait (≠ filtre polarisant)

- Détecteur de photon force le choix (probabiliste)



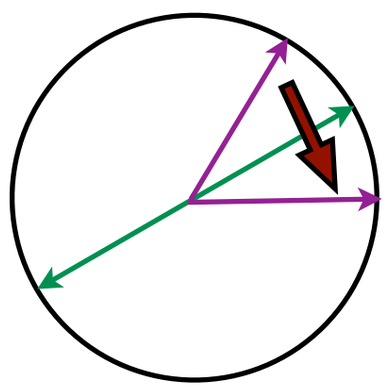
Une mesure modifie l'état

Transformation de la polarisation

- Lame demi-onde

  Symétrie orthogonale par rapport à son axe

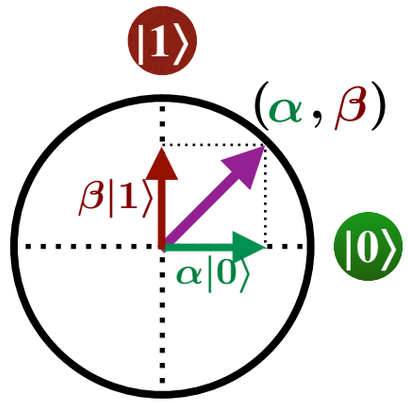
- Toutes les rotations sont donc possibles !



Etat

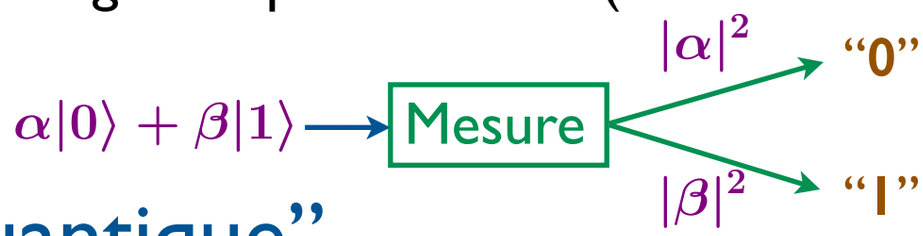
- Vecteur à 2 coordonnées complexes de longueur 1 (unitaire)

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha|0\rangle + \beta|1\rangle, \quad |\alpha|^2 + |\beta|^2 = 1$$



Mesure

- Projection orthogonale probabiliste (une autre base est possible)



Evolution "quantique"

- Modifie les amplitudes (α,β) en préservant $|\alpha|^2+|\beta|^2=1$
- Linéaire : Si $|0\rangle \mapsto |\psi_0\rangle, |1\rangle \mapsto |\psi_1\rangle$ alors $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha|\psi_0\rangle + \beta|\psi_1\rangle$
- Uniquement symétries et rotations (éventuellement complexes) : REVERSIBLE !
- Notation matricielle (non nécessaire à ce stade)

Matrice unitaire 2x2 : $G = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$ telle que $G^* = \begin{pmatrix}\overline{a} & \overline{c}\\ \overline{b} & \overline{d}\end{pmatrix} = G^{-1}$

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

$$|\psi'\rangle = G|\psi\rangle \dashrightarrow \boxed{G^*} \dashrightarrow |\psi\rangle$$

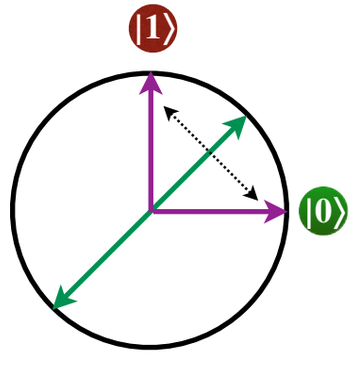
Transformations "classiques" réversibles

- Identité : "rien"

$$\mathbf{Id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \quad \begin{matrix} |0\rangle & |1\rangle \end{matrix}$$

- Négation : symétrie à 45%

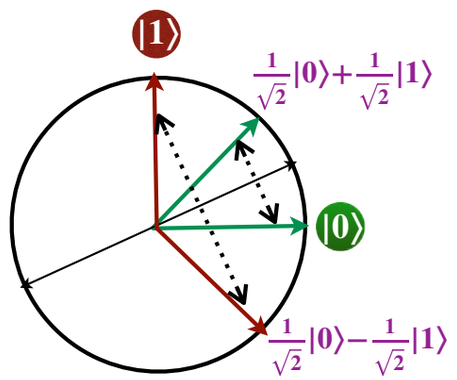
$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \quad \begin{matrix} |0\rangle & |1\rangle \end{matrix}$$



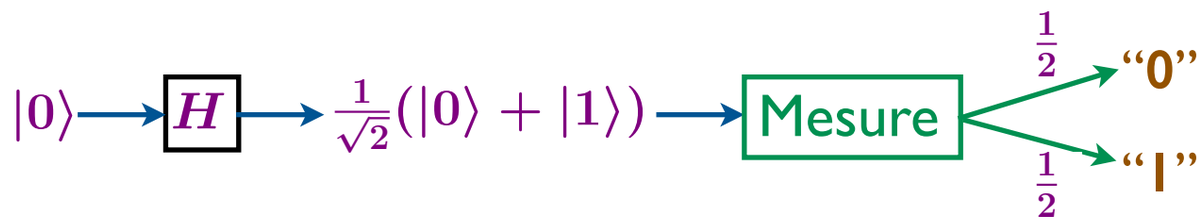
Porte de Hadamard

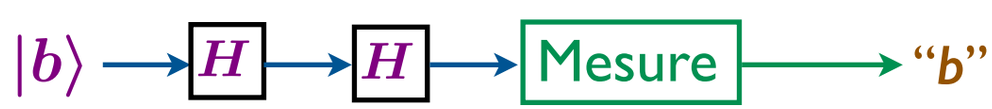
- Definition: Symétrie à 22,5°:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \quad \begin{matrix} |0\rangle & |1\rangle \end{matrix}$$

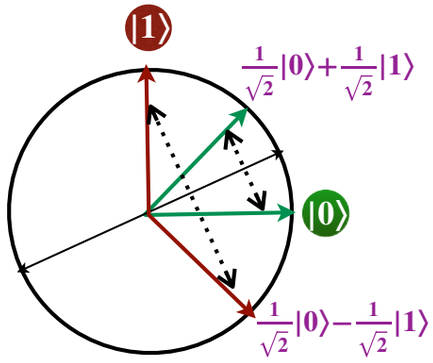


- Propriété: générateur aléatoire quantique

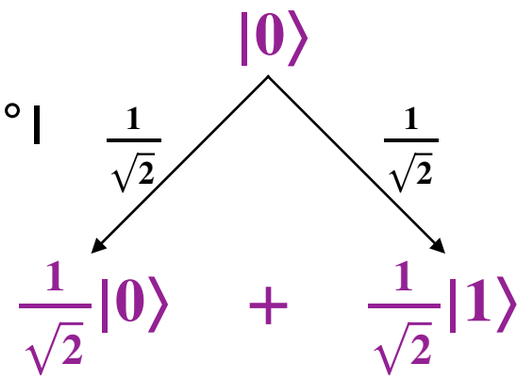




Dispositif simple de type Interféromètre

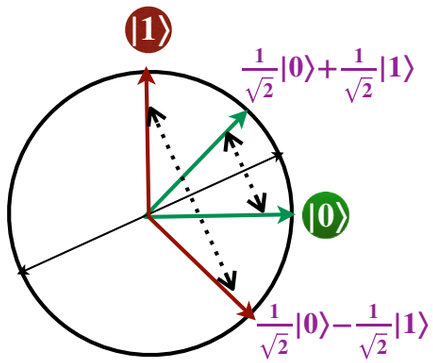


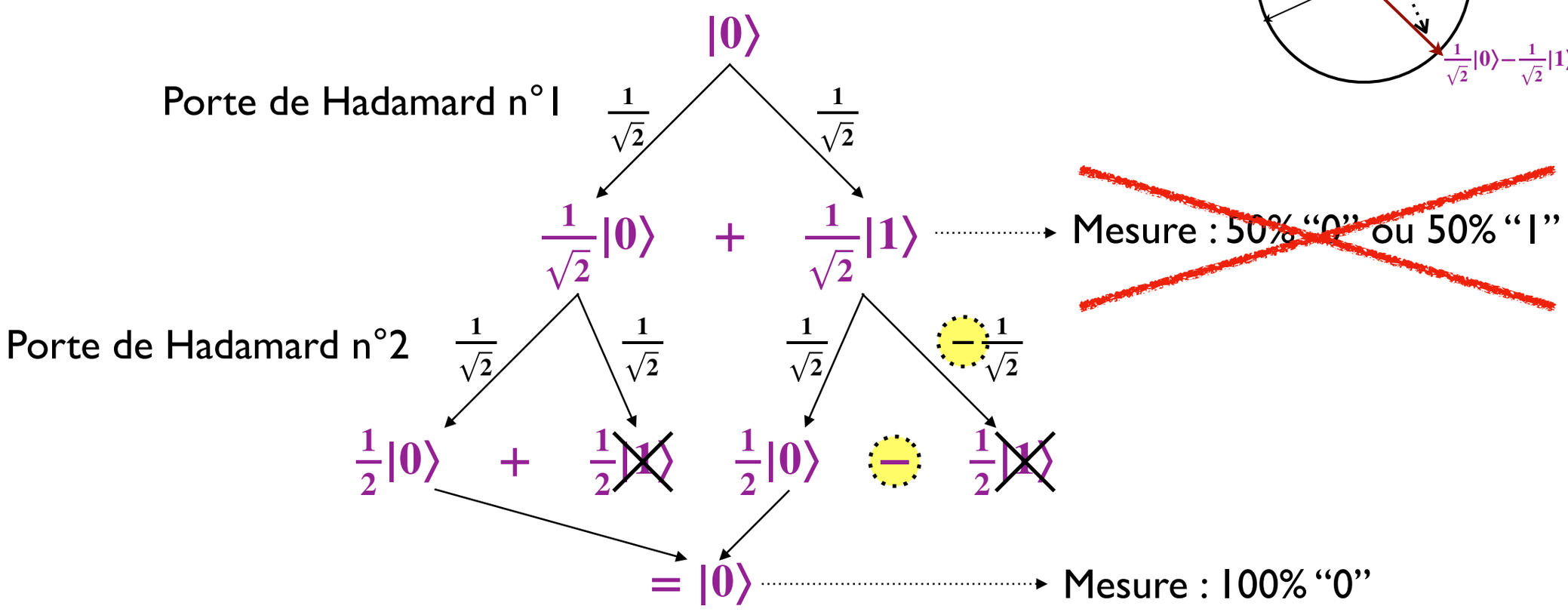
Porte de Hadamard n°1



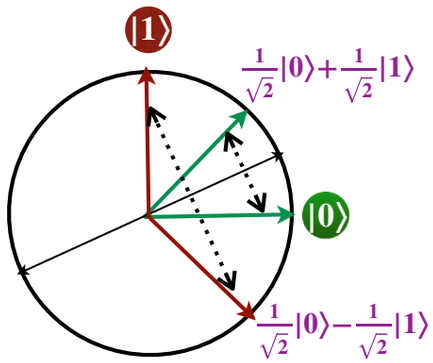
Mesure : 50% "0" ou 50% "1"

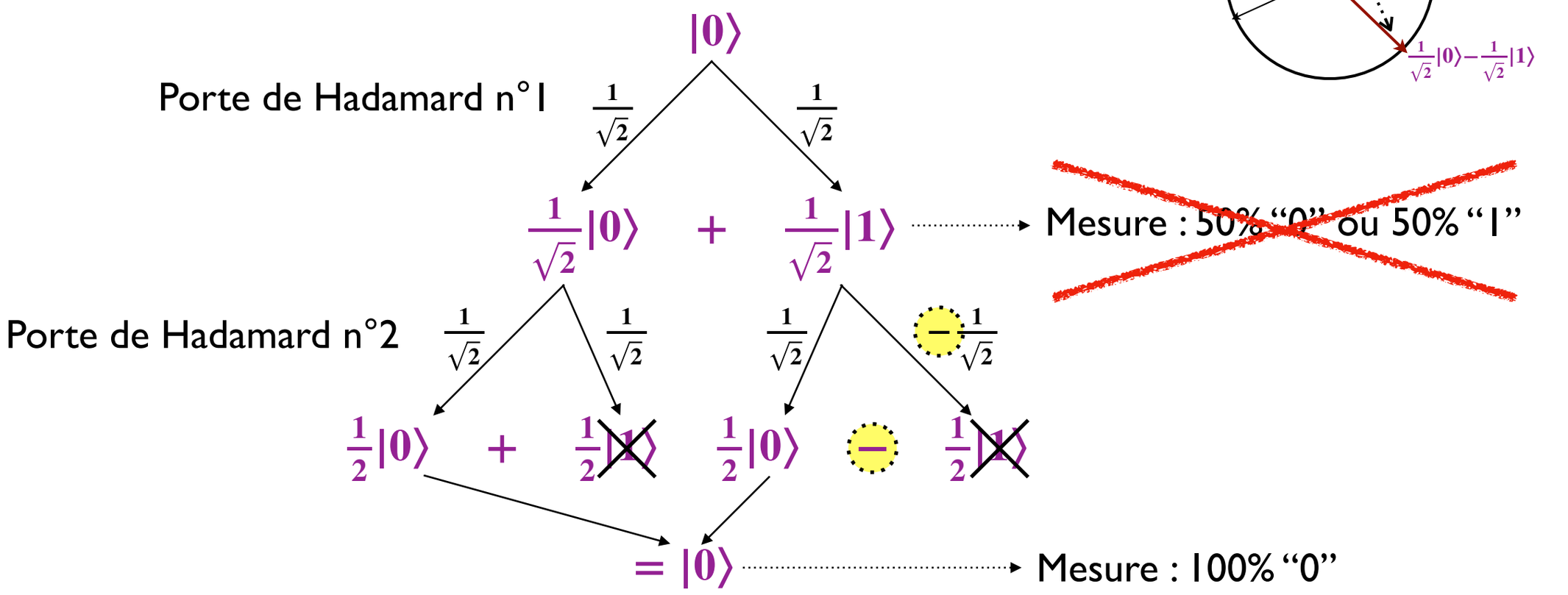
Dispositif simple de type Interféromètre





Dispositif simple de type Interféromètre

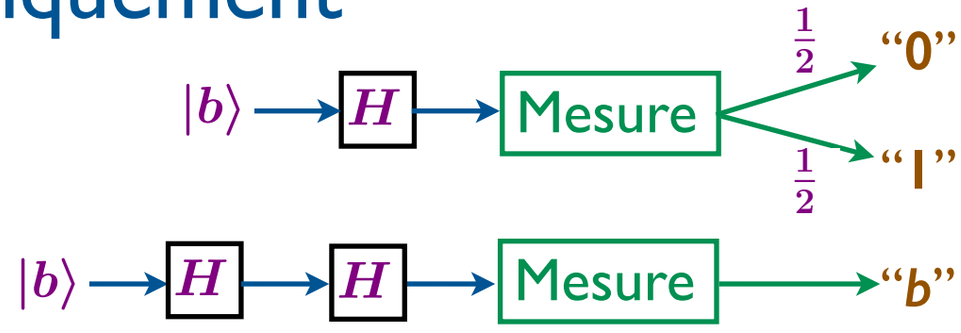




Comportement impossible classiquement

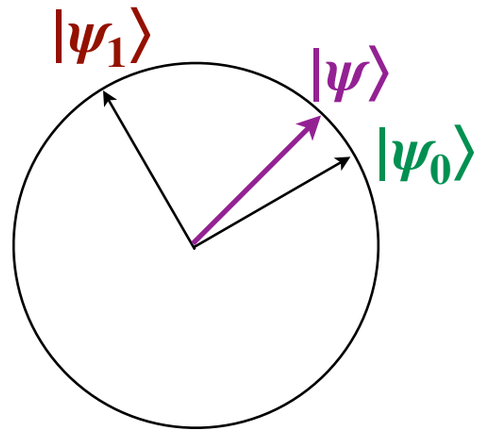
- Sans variable cachée
- Semaine prochaine

  Inégalités de Bell

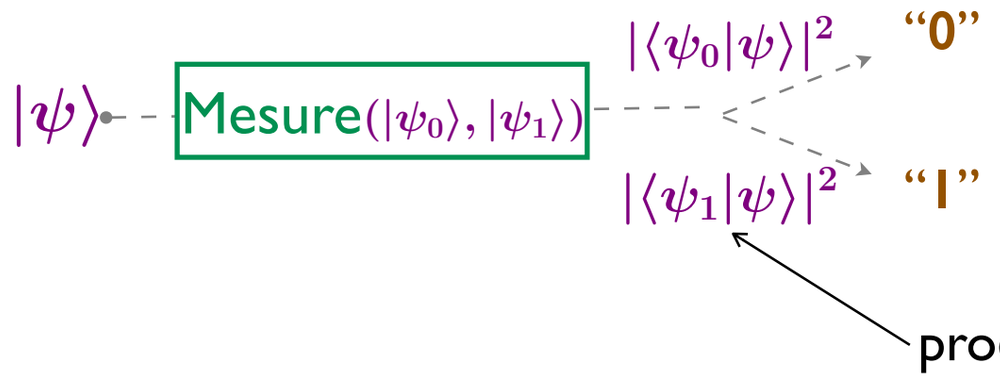


Nouvelle base orthogonale

$$|\psi_0\rangle \perp |\psi_1\rangle$$



Mesure souhaitée



Porte changement de base

$$M = \begin{pmatrix} \langle 0|\psi_0\rangle & \langle 0|\psi_1\rangle \\ \langle 1|\psi_0\rangle & \langle 1|\psi_1\rangle \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

Réalisation

En optique : tourner le filtre ou le cristal

Chiffrement à l'aide d'une clé privée (secret partagé)

One-time pad

Message :	0	1	1	0	0	1	0	1	1	1	0
Clé privée :	1	1	0	1	0	0	1	0	1	0	0
XOR bit à bit :	1	0	1	1	0	1	1	1	0	1	0

Washington-Moscow hotline (1963)

- Théorème : Sécurité parfaite si chaque bit de clé est utilisé une seule fois !
- Pour une sécurité parfaite, la clé doit être aussi longue que le message...

Solutions utilisées en pratique

- Permettent d'utiliser plusieurs fois une même et plus petite clé

  Exemple : Advanced Encryption Standard (AES)

- Sécurité combinatoire : pas de preuve de sécurité mais semble résister aux tentatives de déchiffrement, y compris quantiques

  En pratique, très sûr si la clé n'est pas trop utilisée...

- Utilisation courante : la clé privée est générée à l'aide d'un protocole à clé publique, dont RSA et Diffie-Hellman qui ne résisteraient pas aux attaques quantiques…

Objectif

- Initialement : aucune information secrète entre Alice et Bob
- A la fin : une clé secrète connue uniquement d'Alice et de Bob

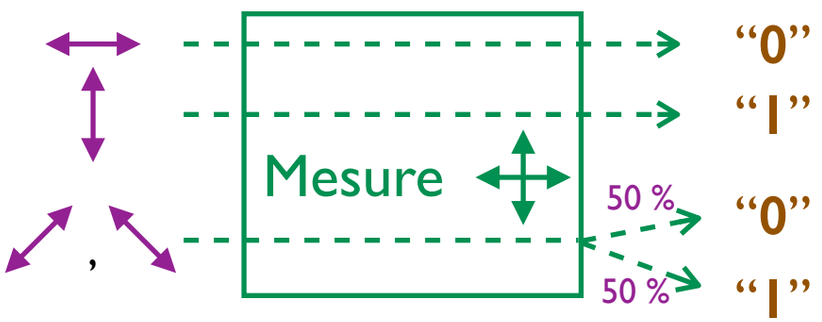
Solutions classiques

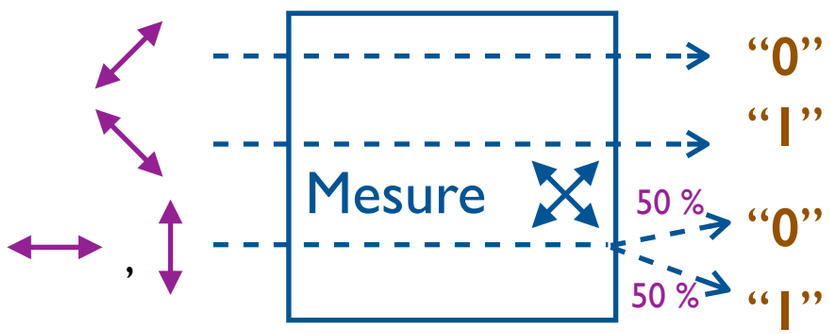
- Sécurité combinatoire, car toute l'information est sur le canal
- Cependant il est possible (outils probabilistes) de :

  Amplifier/Réconcilier le secret d'une clé avec erreur et fuite, en en réduisant la taille

  Identifier un message avec une clé secrète

Incertidude liée à la mesure





Impossibilité de cloner

- Impossible de dupliquer un état inconnu
- Preuve utilisant la linéarité des transformations

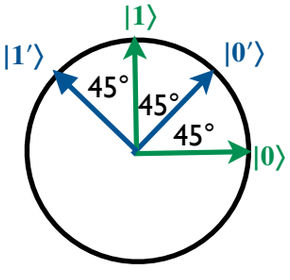
Le protocole BB84 [Bennett-Brassard 84]

Protocole : partie quantique

Clé : 0 1 1 0 0 1 0 1 1 1 0

Base :

Qubit



Base :

Clé : 1 1 0 0 1 1 0 1 0 1 0

Protocole : partie classique

- Filtre : Alice et Bob révèlent publiquement la séquences de bases utilisées

  A&B ne conservent que les bits avec même choix (proba. 1/2)

  Si aucune observation de la communication → A&B ont la même clé !
- Sécurité : A&B vérifient que leurs clés ont peu d'erreurs (<11%) en en échangeant une partie aléatoire publiquement
- Réconciliation : A&B utilisent des techniques de codes correcteurs classiques pour corriger les erreurs sur les autres bits
- Amplification : A&B réduisent les fuites potentielles vers un espion en utilisant une fonction de hachage qui réduit la taille de la clé
- Au final : la clé est identique, mais réduite, et la perte d'information très petite

Authentification

- Ligne authentifiée : Génération de clé sans secret initial
- Ligne non-authentifiée : Petite clé secrète ⇒ grande clé secrète

Utilisation I

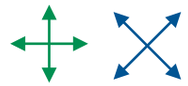
- Avec la clé obtenue, encoder un texte de même longueur en utilisant le codage “one-time pad”
- Une fois utilisée, la clé est jetée...

Utilisation II

- Utiliser la clé secrète dans des applications cryptographiques qui utilisent une clé petite, éventuellement plusieurs fois (exemple : AES)
- Attention : la sécurité n’est plus inconditionnelle

Exercice 1 : Analyse d'une attaque (sur un photon)

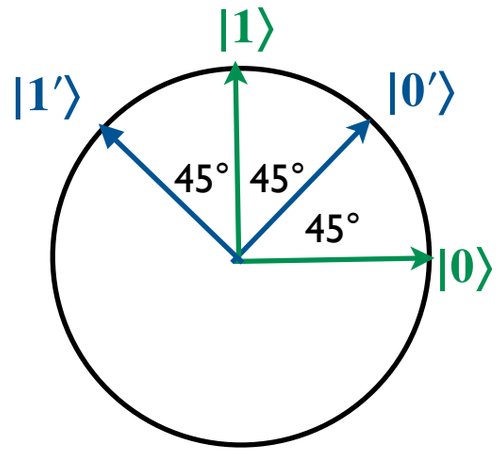
Stratégie 1

- Eve observe chaque qubit dans une des bases 
- Eve renvoie le qubit encodé dans la même base

Question 2

- Quel est le taux d'erreur généré ?

Considérons un bit conservé après filtrage.
Avec probabilité 1/2 Eve fait le bon choix, et ne génère aucune erreur.



Avec probabilité 1/2, Eve fait le mauvais choix.
Son bit et celui de Bob sont aléatoires et indépendants,
donc Bob lit une valeur différente d'Alice avec probabilité 1/2.

Il y a donc un taux d'erreur d'1/4 = 25%.

- Quelle portion de clé secrète d'Alice est apprise ?

Considérons un bit conservé après filtrage.
Avec probabilité 1/2 Eve fait le bon choix, et apprend le bon bit.

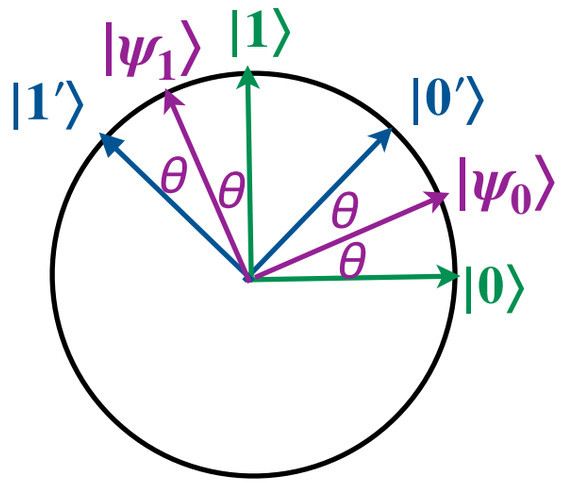
Avec probabilité 1/2, Eve fait le mauvais choix.
Son bit est aléatoire, et donc correspond à celui d'Alice avec probabilité 1/2.

Chaque bit de clé d'Alice est donc appris avec probabilité 1/2+1/4= 75%.

Exercice 1 : Analyse d'une attaque (sur un photon)

Stratégie 1

- Eve observe chaque qubit dans la base tournée de θ =22,5°
- Eve renvoie $|\psi_b\rangle$ observé quand elle observe b



Question 2

- Quel est le taux d'erreurs générées ?

Considérons un bit conservé après filtrage.

Il y a 2 façon de faire une erreur.
Eve lit l'opposé du bit d'Alice (proba. $\sin^2\theta$), et Bob lit la même valeur qu'Eve (proba. $\cos^2\theta$).
Eve lit le même bit que celui d'Alice (proba. $\cos^2\theta$), et Bob lit la valeur opposée d'Eve (proba. $\sin^2\theta$).

Soit au final $2\sin^2\theta\cos^2\theta = 25\%$ (comme précédemment).

- Quelle portion de clé secrète d'Alice est apprise ?

Considérons un bit conservé après filtrage.

La probabilité qu'Eve lise le même bit que celui choisi par Alice est proba. $\cos^2\theta$.

Chaque bit de clé d'Alice est donc appris avec probabilité $\cos^2\theta \approx 85{,}4\%$ (au lieu de 75%).

Etat *n*-qubit

- $|\psi\rangle \in \mathbb{C}^{\{0,1\}^n}$ tel que $\||\psi\rangle\| = 1$

$$|\psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \qquad \text{avec} \sum_{x\in\{0,1\}^n} |\alpha_x|^2 = 1$$

- Exemples

  Etat séparé : $(|00\rangle + |01\rangle)/\sqrt{2} = |0\rangle(|0\rangle + |1\rangle)/\sqrt{2}$

  Etat enchevêtré (EPR) : $(|00\rangle + |11\rangle)/\sqrt{2} \neq |\psi_0\rangle|\psi_1\rangle$

Mesure

- Projection orthogonale probabiliste

$$\sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \dashrightarrow \boxed{\text{Mesure}} \xrightarrow{|\alpha_x|^2} \text{“}x\text{”}$$

Evolution

- Transformation unitaire $G \in \mathcal{U}(2^n)$ $\quad (G \in \mathbb{C}^{2^n\times 2^n}$ s.t. $G^*G = \mathrm{Id})$

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

Théorème

- Il n'existe pas d'opération unitaire qui réalise

$$G(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

Preuve par l'absurde : clonage d'un qubit

- Hypothèses

$$G(|0\rangle|0\rangle) = |0\rangle|0\rangle$$

$$G(|1\rangle|0\rangle) = |1\rangle|1\rangle$$

$$G\left(\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle\right) = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \left(\frac{|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle}{2}\right)$$

- Linéarité de G

$$G\left(\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)|0\rangle\right) = \left(\frac{G(|0\rangle|0\rangle) + G(|1\rangle|0\rangle)}{\sqrt{2}}\right) = \left(\frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}\right)$$

- Contradiction !

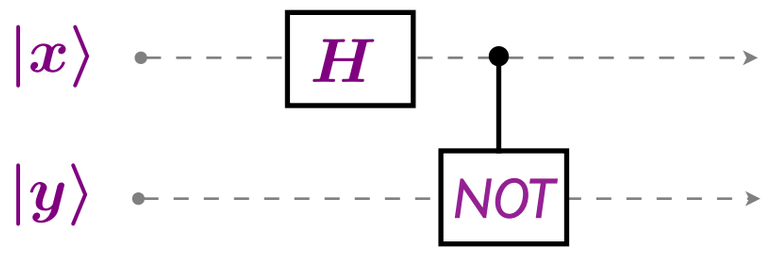
Définition

- c-$NOT|0b\rangle = |0b\rangle$
- c-$NOT|1b\rangle = |1\rangle|(1-b)\rangle$
- c-$NOT|ab\rangle = |a\rangle|a \oplus b\rangle$

$$\text{c-}NOT = \begin{array}{c} \begin{matrix} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix} \end{array}$$

Représentation

Résultat



$|\beta_{xy}\rangle$

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Preuve : cas *xy*=11

- Etat initial

$$|11\rangle = |1\rangle|1\rangle$$

- Hadamard sur le 1er qubit

$$(H|1\rangle)|1\rangle = \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)|1\rangle = \frac{|01\rangle - |11\rangle}{\sqrt{2}}$$

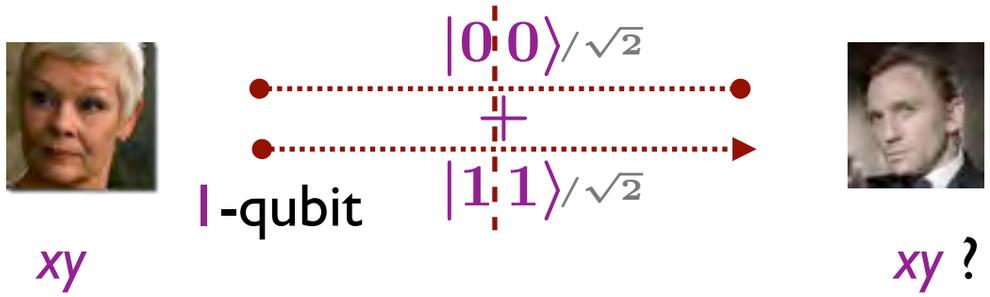
- Control-Not

$$\text{c-}NOT\left(\frac{|01\rangle - |11\rangle}{\sqrt{2}}\right) = \frac{\left(\text{c-}NOT(|01\rangle) - \text{c-}NOT(|11\rangle)\right)}{\sqrt{2}} = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

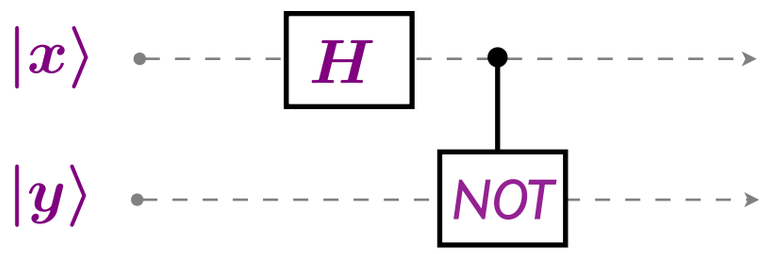
[Bennett, Wiesner' 1992]

Objectif

- Alice & Bob partage un état EPR : $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Alice veut envoyer deux bits *xy* à Bob
- Mais Alice ne peut envoyer qu'un qubit à Bob



Changement de base de Bell



$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$
$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Protocole

- Alice applique *NOT* sur son qubit si *y*=1 ; et *FLIP* si *x*=1
- Alice envoie son qubit à Bob
- Bob fait un changement de base de Bell inverse et observes xy

$$FLIP = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{matrix} |0\rangle \\ |1\rangle \end{matrix} \quad \begin{matrix} |0\rangle & |1\rangle \end{matrix}$$

Mesure du premier qubit

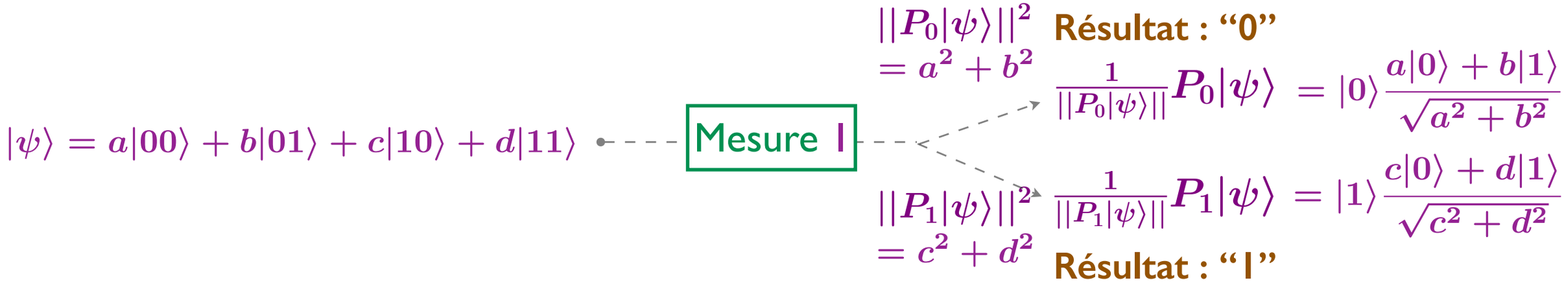
- Projecteur $P_0 = |00\rangle\langle 00| + |01\rangle\langle 01| = |0\rangle\langle 0| \otimes \mathbf{I_2}$

$P_1 = |10\rangle\langle 10| + |11\rangle\langle 11| = |1\rangle\langle 1| \otimes \mathbf{I_2}$

$P_0 \overset{\perp}{\oplus} P_1 = Id$

projecteur orthogonal

- Mesure du premier qubit → projection du deuxième



Interprétation

- Mesure partielle projette sur le sous-espace compatible avec l'opération

  Probabilité = carré de la norme de la projection

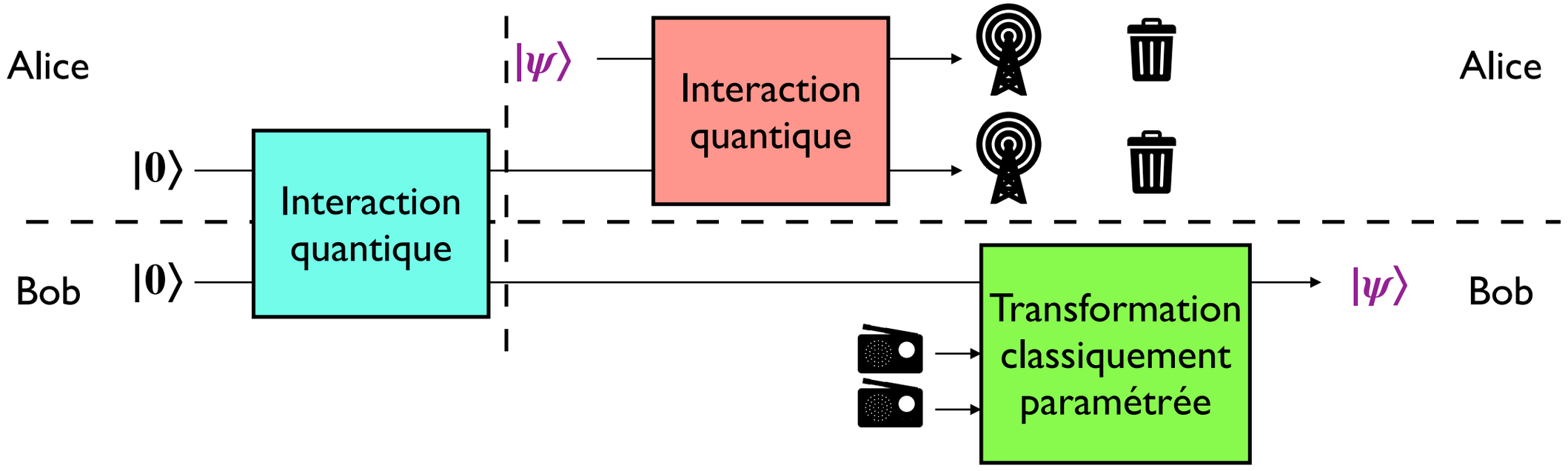
  Sortie = re-normalisation de la projection

[Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters'93]

Problème

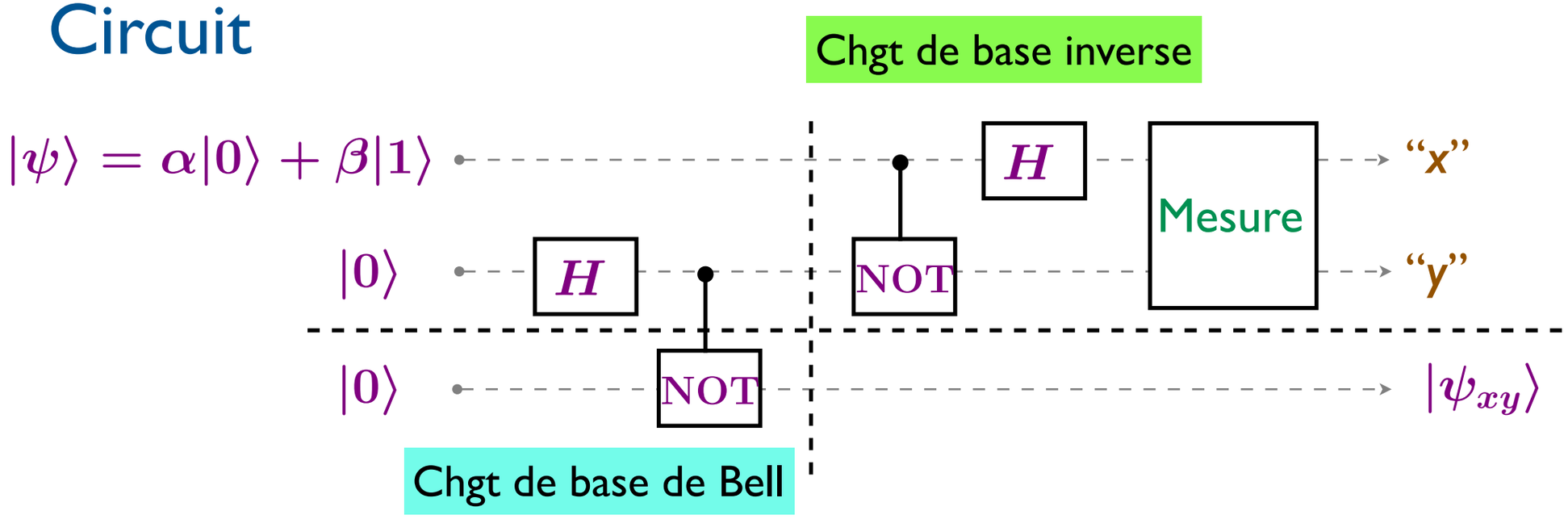
- Alice veut transmettre un qubit $|\psi\rangle$ à Bob
- Bob: position éloignée et inconnue d'Alice
- Broadcast classique possible : classique à sens unique Alice → Bob

Réalisation



- La communication classique ne révèle rien sur l'état $|\psi\rangle$!

Circuit



Analyse

- Etat final $\frac{1}{2}\sum_{x,y}|xy\rangle|\psi_{xy}\rangle$ avec $|\psi_{xy}\rangle = (\mathbf{NOT})^y(\mathbf{FLIP})^x|\psi\rangle$

Preuve : $|\psi\rangle|0\rangle|0\rangle \mapsto \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|0\rangle|0\rangle + |1\rangle|1\rangle)$

$$= \frac{1}{2}|\beta_{00}\rangle(\alpha|0\rangle + \beta|1\rangle)$$
$$+ \frac{1}{2}|\beta_{01}\rangle(\alpha|1\rangle + \beta|0\rangle)$$
$$+ \frac{1}{2}|\beta_{10}\rangle(\alpha|0\rangle - \beta|1\rangle)$$
$$+ \frac{1}{2}|\beta_{11}\rangle(\alpha|1\rangle - \beta|0\rangle)$$

- En mesurant *x,y*, le 3e qubit est projeté sur $|\psi_{xy}\rangle$
- En apprenant *x,y*, Bob peut corriger $|\psi_{xy}\rangle$ en $|\psi\rangle$

Remarque

- Le circuit de téléportation

est en faire une porte Identité, et donc quantique

Application

- Etant donné un système à *n*-qubit

  Que se passe-t-il si chaque qubit est téléporté ?

- Il s'agit toujours d'une opération unitaire (i.e. quantique)
- Sur les états séparés, par exemple les états classiques

  $|x\rangle = |x_1, x_2, \ldots, x_n\rangle$,

  chaque bit est bien transmis
- Par linéarité de l'opération…

  toute superposition est aussi transmise !

Difficulté ?

- En pratique, il faut que toute l'opération reste unitaire

Initiatives pédagogiques

- Quantum game : https://quantumgame.io/
- Initiatives pédagogiques européennes :

  https://qworld.lu.lv

  https://www.quantum-quest.nl

  https://algassert.com/quirk

Protocole quantique de distribution de clé

- *A largely self-contained and complete security proof for quantum key distribution.* Tomamichel, Leverrier

  https://arxiv.org/abs/1506.08458

- Un Mooc avec Vidick et Wehner

  https://ocw.tudelft.nl/courses/quantum-cryptography/

Séminaire du cours !

- Réseaux de communication quantique

  avec Eleni Diamanti, CNRS, Paris