Protocole E91

Ibrahim Chegrane
ibrahim.Chegrane@USherbrooke.ca

26 Février 2026

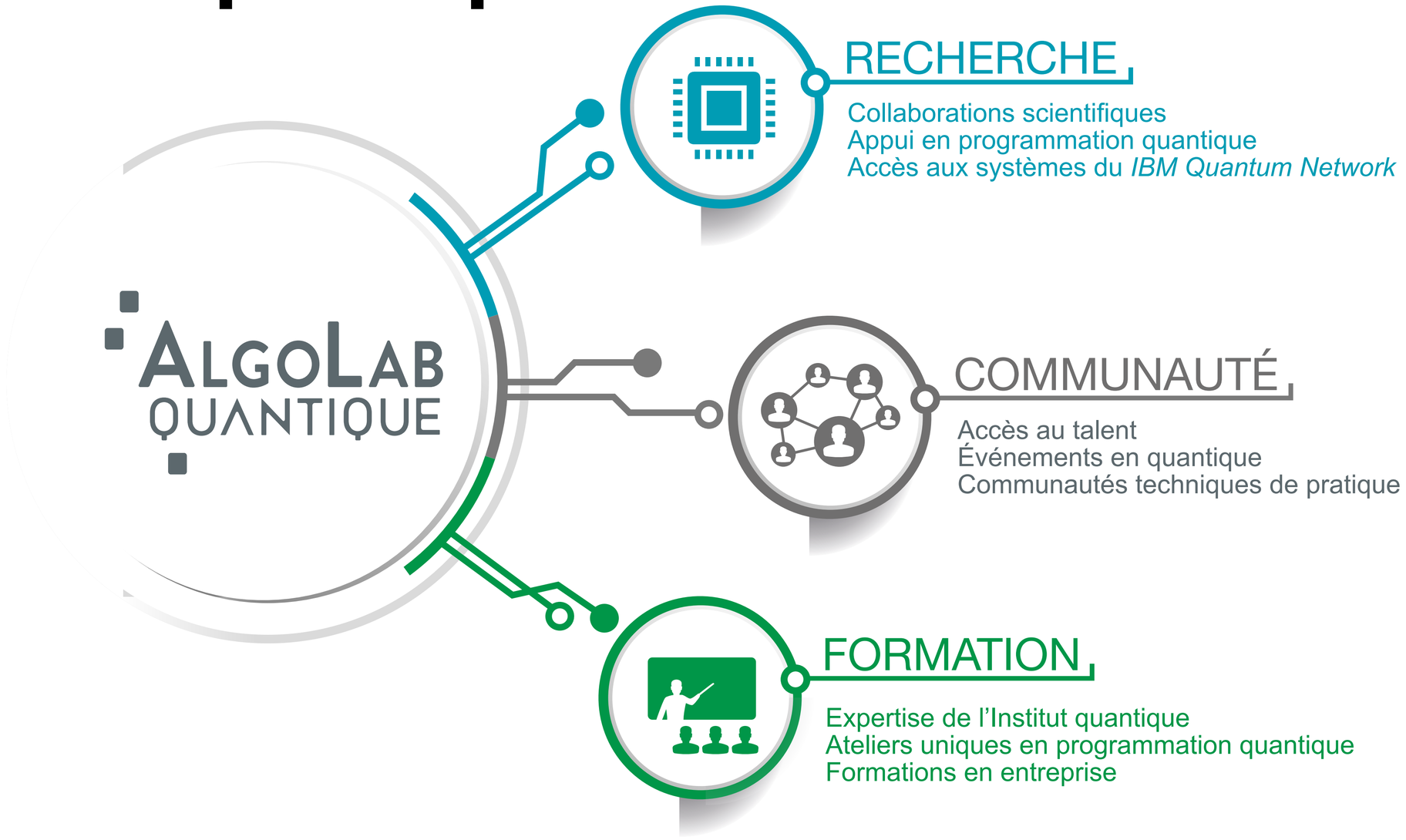
UNIVERSITÉ DE SHERBROOKE

Qui sommes-nous?

INSTITUT QUANTIQUE

Université de Sherbrooke

AlgoLab quantique

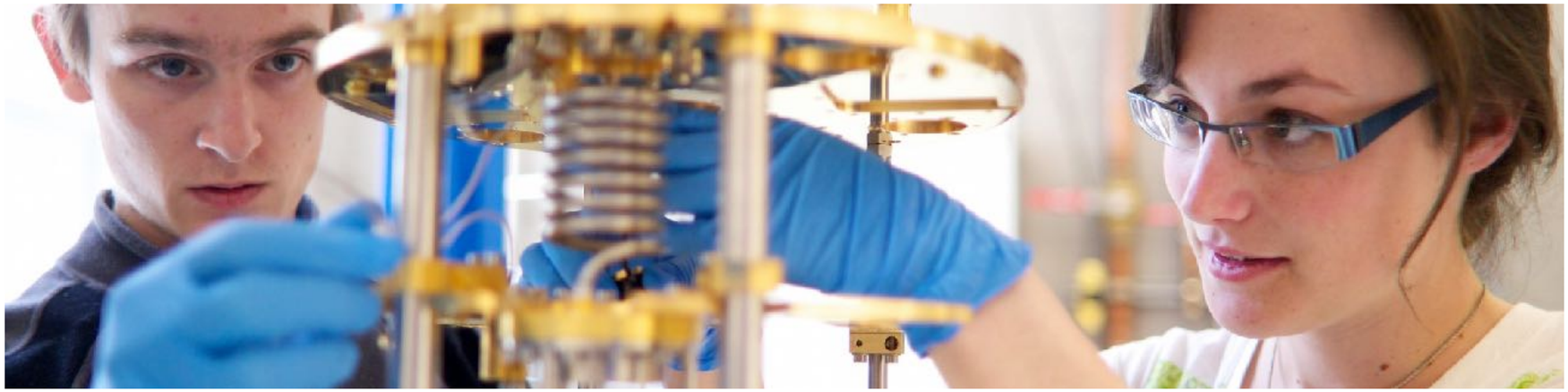


Nous contacter : AlgoLabquantique@usherbrooke.ca

INSTITUT QUANTIQUE
UNIVERSITÉ DE SHERBROOKE

Institut quantique

Nous plaçons les 250 étudiantes et étudiants au centre de la recherche dans un environnement ouvert et collaboratif pour accélérer le passage de la science aux technologies quantiques.



Nos 32 membres du corps professoral proviennent de 4 facultés et 7 départements

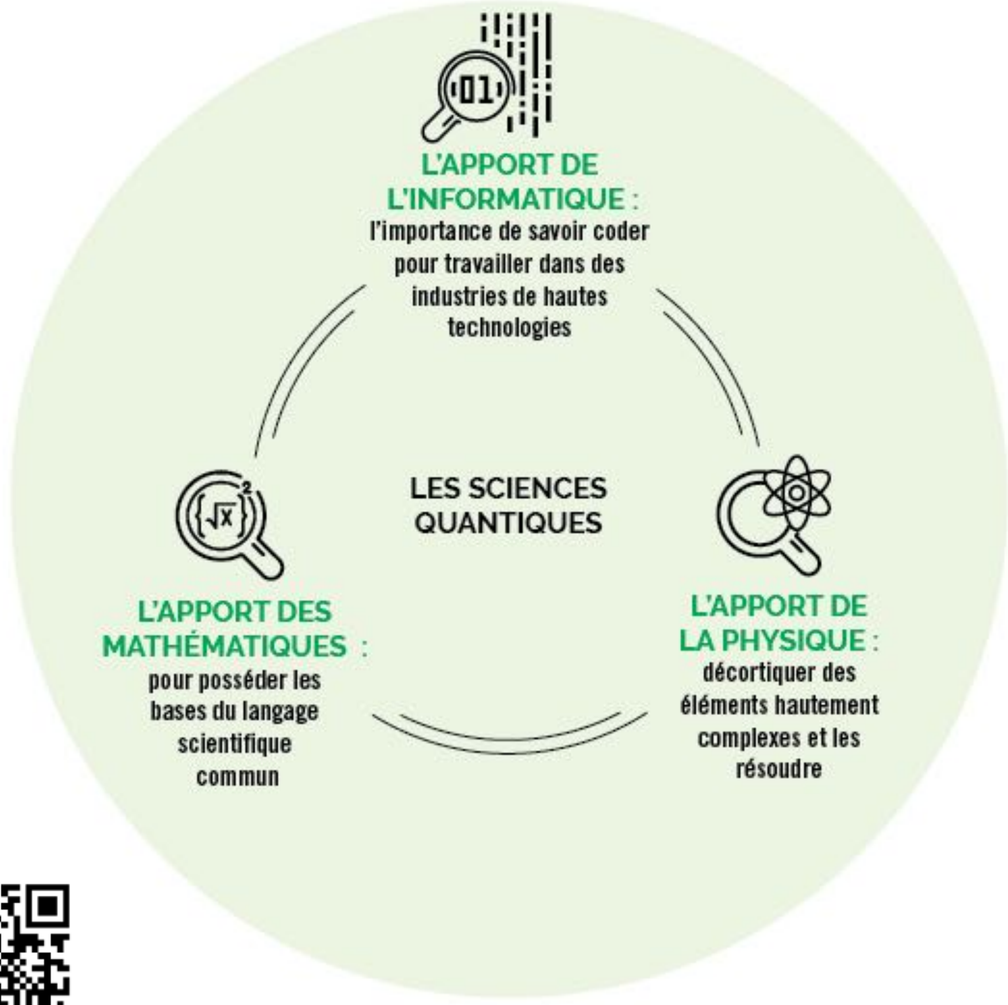
80M$ investis en 10 ans et un nouveau bâtiment depuis 2021

Premier baccalauréat en sciences quantiques au Québec

Nouvelle cohorte à l'automne 2026

Formation professionnalisante

- Programme interdisciplinaire
- Parcours coop
- Projets intégrateurs



Pour en savoir plus

UdS Université de Sherbrooke

Institut quantique

Environnement de R&D coopératif
pour l'académique et l'industrie

Plateformes technos quantiques

FabLab quantique

AlgoLab quantique

Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- [x] Présentation
- [ ] Cryptographie
- [ ] Le qubit
- [ ] Le photon: messager d’information quantique
- [ ] Intrication et inégalité CHSH
- [ ] Protocole E91
- [ ] Atelier pratique

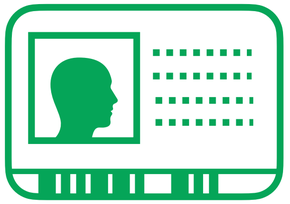
Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Cryptographie

Confidentialité

Authenticité



Intégrité

Cryptographie

Confidentialité

Authenticité

Intégrité

Cryptographie

Confidentialité

But: Assurer que le message soit inaccessible à un espion!

Cryptographie

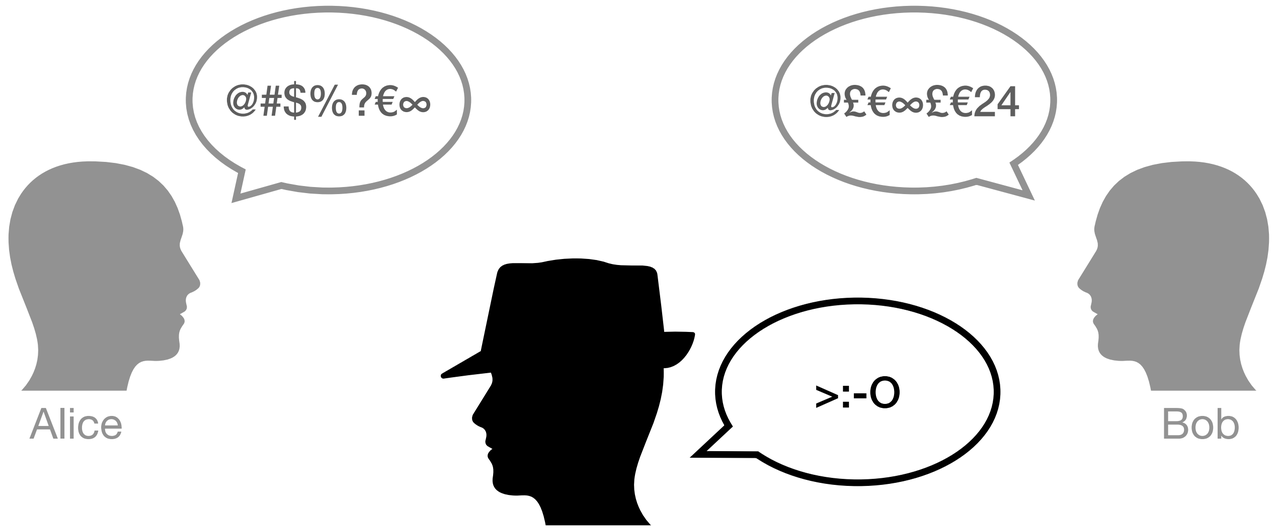
Confidentialité

But: Assurer que le message soit inaccessible à un espion!

Cryptographie

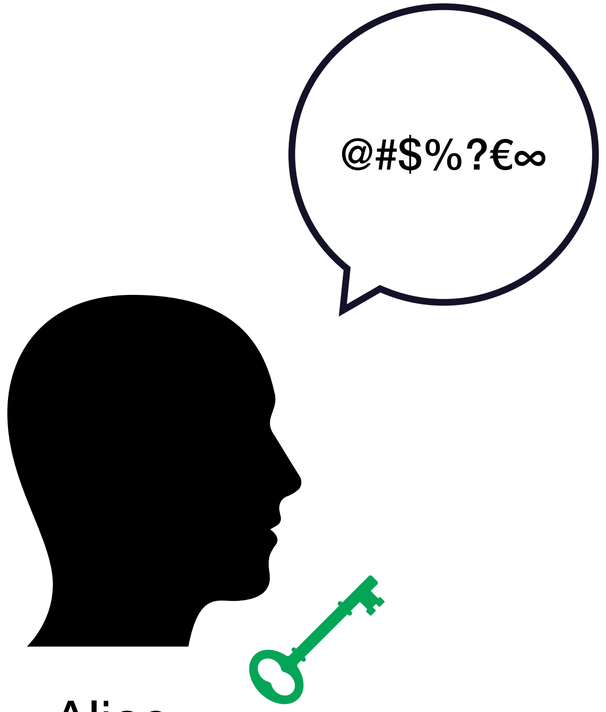
Confidentialité

But: Assurer que le message soit inaccessible à un espion!

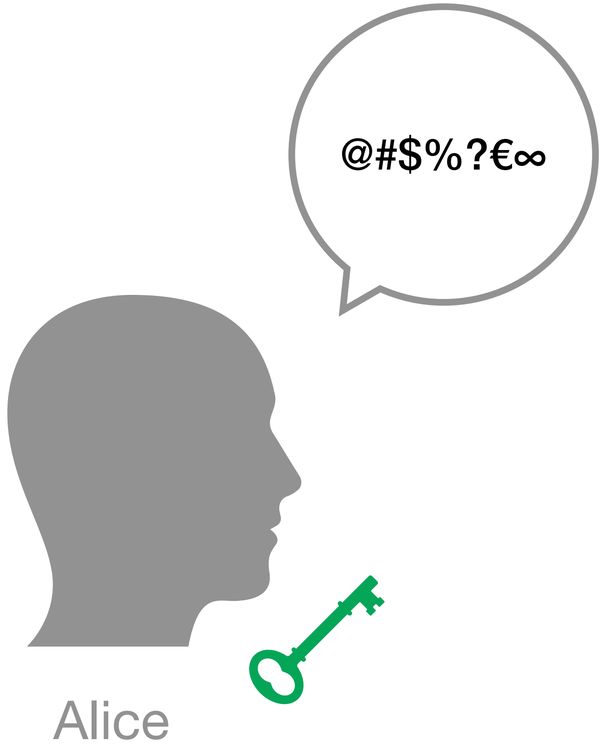


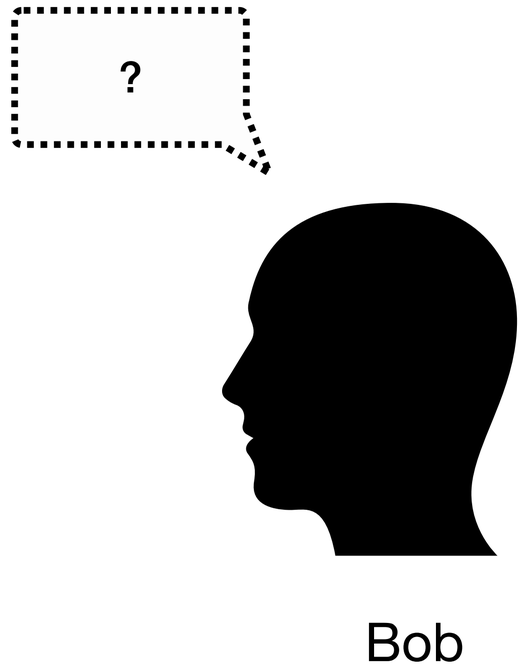
Clé symétrique

Clé symétrique

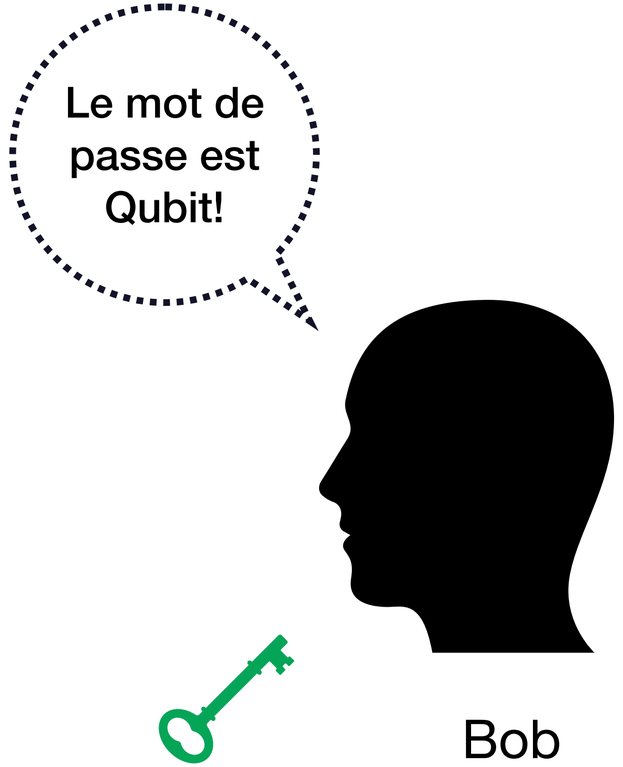


Clé symétrique





Clé symétrique



Clé symétrique

Caractéristiques

- une seule clé (privée) pour chiffrer et déchiffrer

Clé symétrique

Caractéristiques

- une seule clé (privée) pour chiffrer et déchiffrer

Avantages

- rapide et nécessite peu de ressource de calcul

Clé symétrique

Caractéristiques

- une seule clé (privée) pour chiffrer et déchiffrer

Avantages

- rapide et nécessite peu de ressource de calcul

Inconvénients

- distribution de la clé

Clé symétrique

Caractéristiques

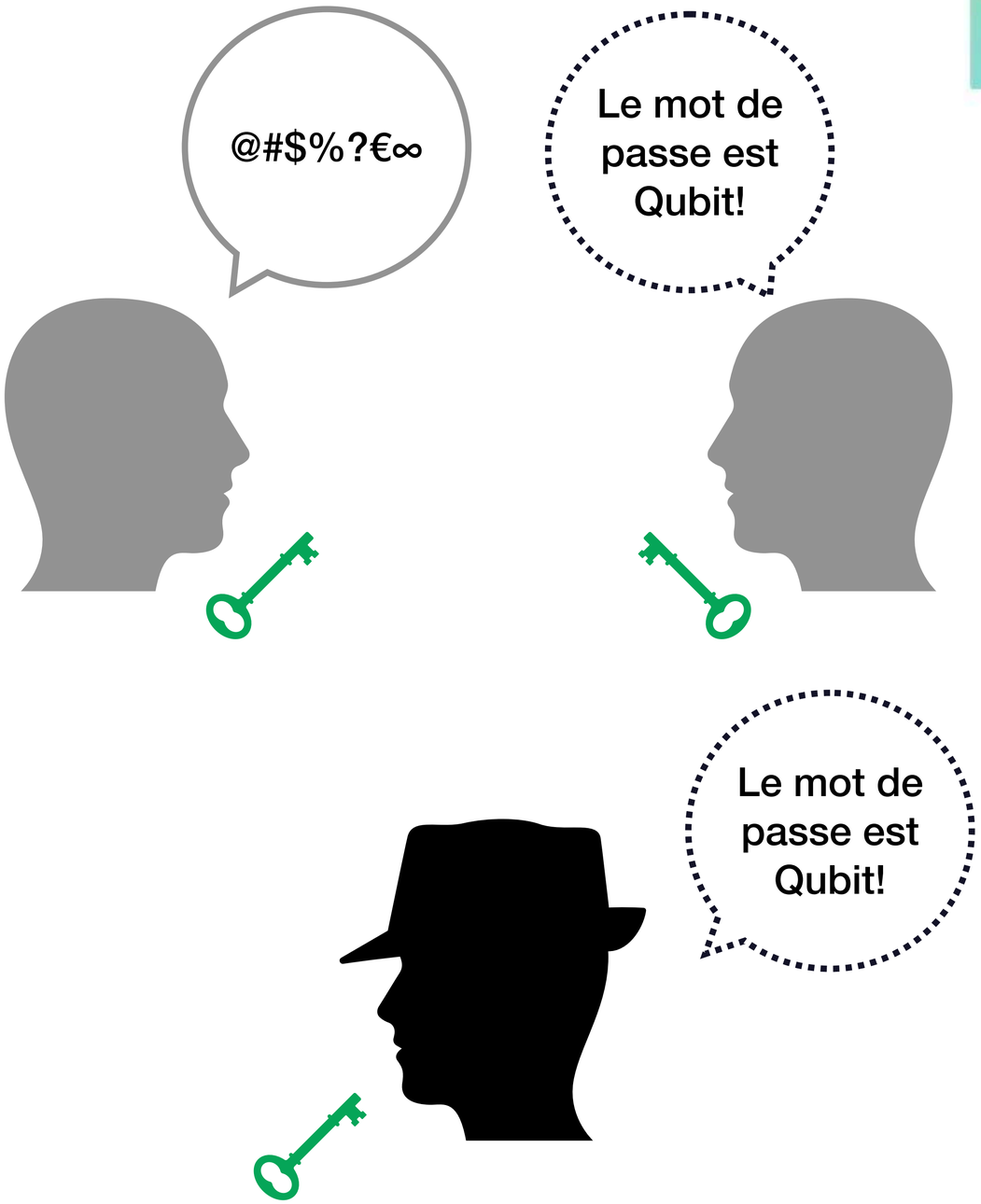
- une seule clé (privée) pour chiffrer et déchiffrer

Avantages

- rapide et nécessite peu de ressource de calcul

Inconvénients

- distribution de la clé



Clé asymétrique

Caractéristiques

- une clé publique pour chiffrer et
  une clé privée pour déchiffrer

Clé asymétrique

Caractéristiques

- une clé publique pour chiffrer et une clé privée pour déchiffrer

Avantages

- distribution de la clé publique

Clé asymétrique

Caractéristiques

- une clé publique pour chiffrer et une clé privée pour déchiffrer

Avantages

- distribution de la clé publique

Inconvénients

- lent et coûteux en ressources de calcul

Motivation

Cryptographie quantique

Motivation

Cryptographie quantique

Déchiffrer des messages

- Protocole de chiffrement asymétrique (p.e. RSA avec algorithme de Shor)
- Protocole de chiffrement symétrique (p.e. AES avec algorithme de Grover)

Motivation
Cryptographie quantique

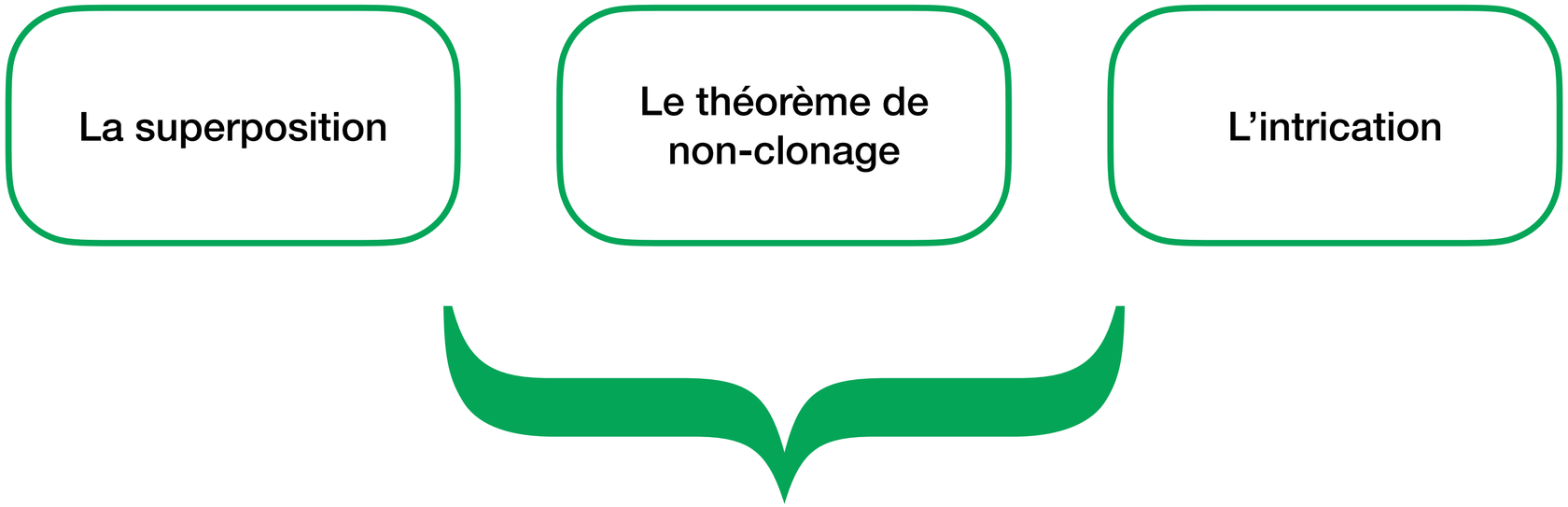
Déchiffrer des messages

- Protocole de chiffrement asymétrique (p.e. RSA avec algorithme de Shor)
- Protocole de chiffrement symétrique (p.e. AES avec algorithme de Grover)

Cryptographie quantique

Cryptographie quantique

Méthodes de cryptographie exploitant les propriétés de la mécanique quantique telles que



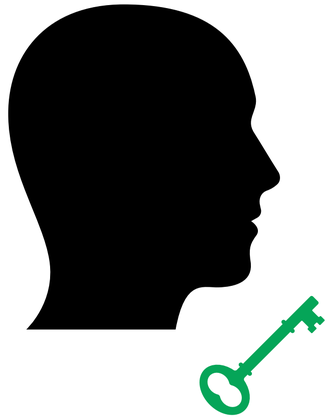
Distribution de clé quantique (QKD)

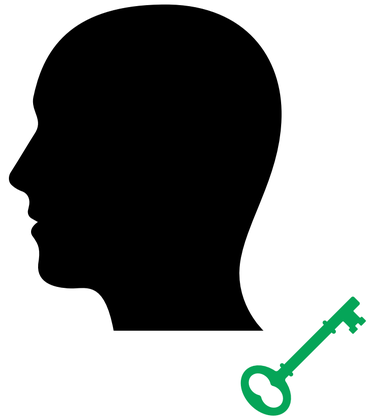
Distribution de clé quantique (QKD)

Déployer une clé symétrique chez Alice et chez Bob en utilisant les propriétés de la mécanique quantique

Sécurité théorique parfaite

Détection d’espion





Protocole E91

APS Journals All Journals Physics Magazine

Physical Review Letters

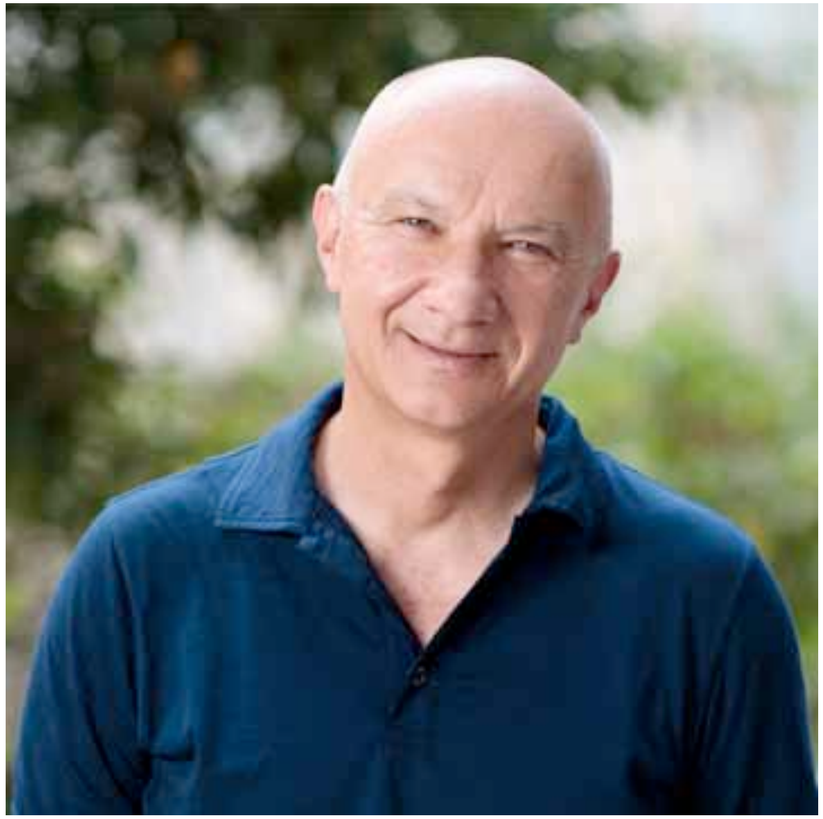
Quantum cryptography based on Bell's theorem

Artur K. Ekert

Show more

Phys. Rev. Lett. **67**, 661 – **Published 5 August, 1991**

DOI: https://doi.org/10.1103/PhysRevLett.67.661



Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- [x] Présentation
- [x] Cryptographie
- [ ] Le qubit
- [ ] Le photon: messager d’information quantique
- [ ] Intrication et inégalité CHSH
- [ ] Protocole E91
- [] Atelier pratique

Plan

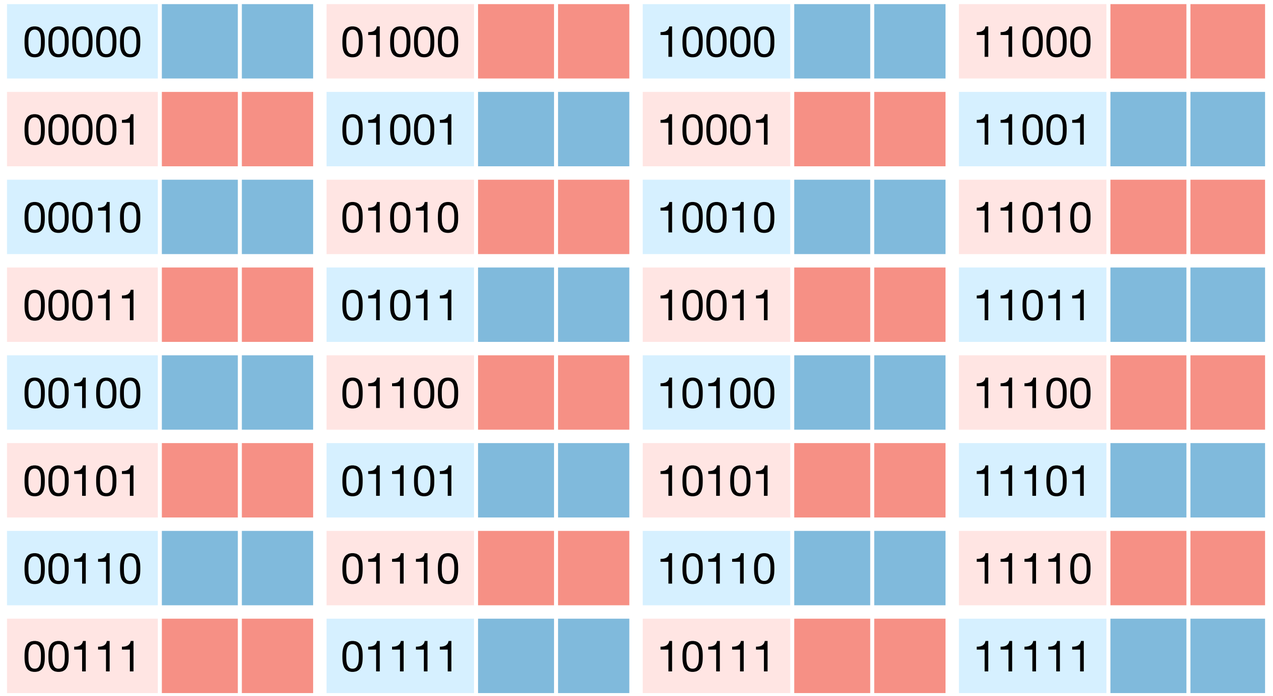
- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Le bit
Information classique

- Le bit = unité d’information

  0 ou 1

- L’information peut alors être encodée sous la forme de chaines de bits.



Le bit

Information classique

- Le bit = unité d'information

  0 ou 1

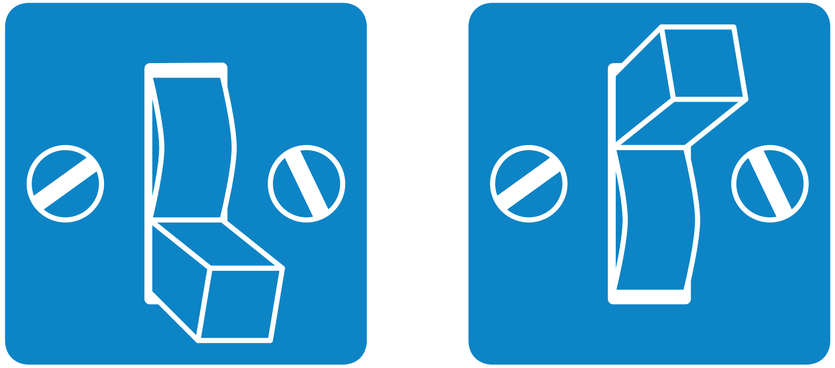
- L'information peut alors être encodée sous la forme de chaines de bits.
- Avec 5 bits il est possible d'encoder :
  - Les nombres de 0 à 31
  - L'alphabet

00000	0	a	01000	8	i	10000	16	q	11000	24	y
00001	1	b	01001	9	j	10001	17	r	11001	25	z
00010	2	c	01010	10	k	10010	18	s	11010	26	
00011	3	d	01011	11	l	10011	19	t	11011	27	
00100	4	e	01100	12	m	10100	20	u	11100	28	
00101	5	f	01101	13	n	10101	21	v	11101	29	
00110	6	g	01110	14	o	10110	22	w	11110	30	
00111	7	h	01111	15	p	10111	23	x	11111	31	

Représentation physique

Information classique

Bit



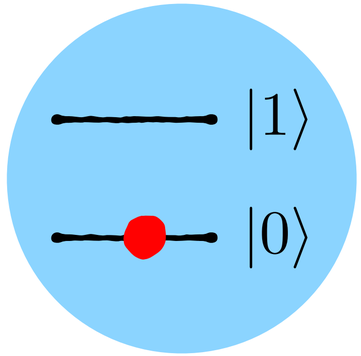
0 1

L’information quantique

Le qubit

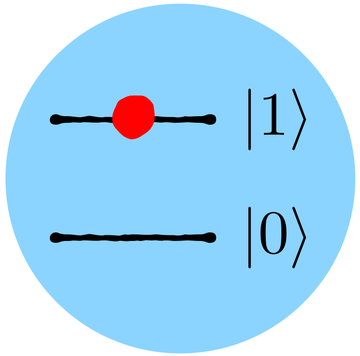
- Le qubit = bit quantique
- Prend un ensemble de valeurs

0



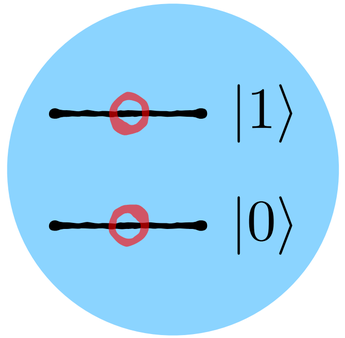
ou

1



ou

"0 et 1"

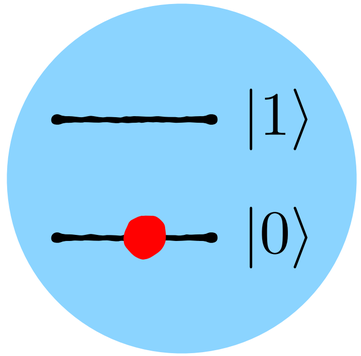


L’information quantique

Le qubit

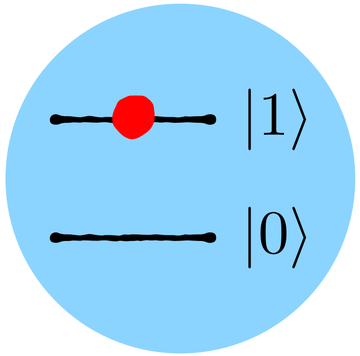
- Le qubit = bit quantique
- Prend un ensemble de valeurs

0



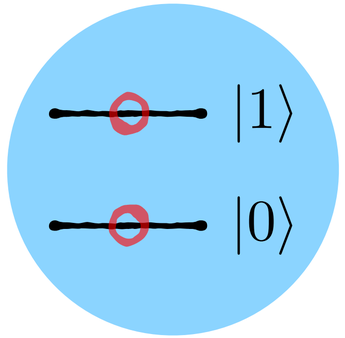
ou

1



ou

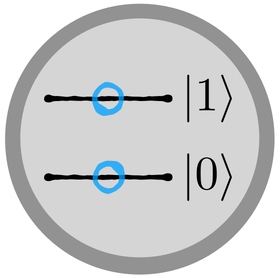
"0 et 1"



État de superposition

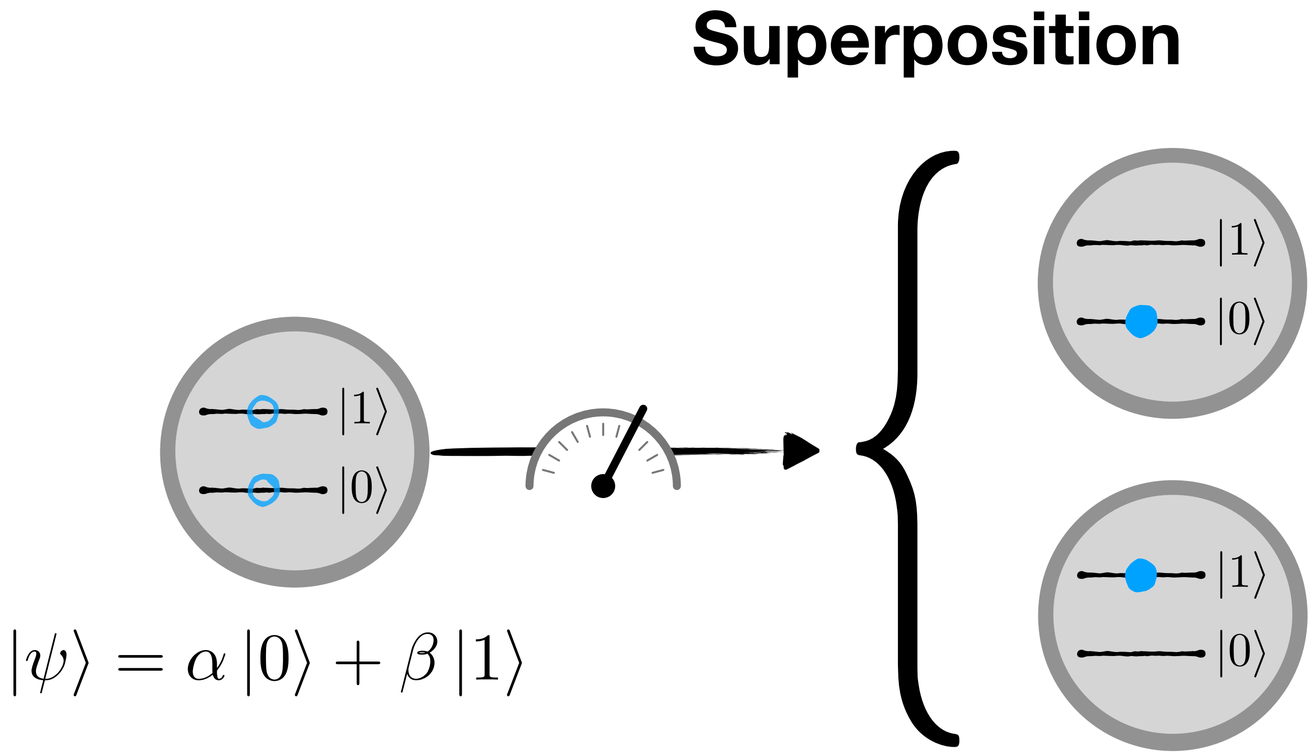
Notation de Dirac

Superposition

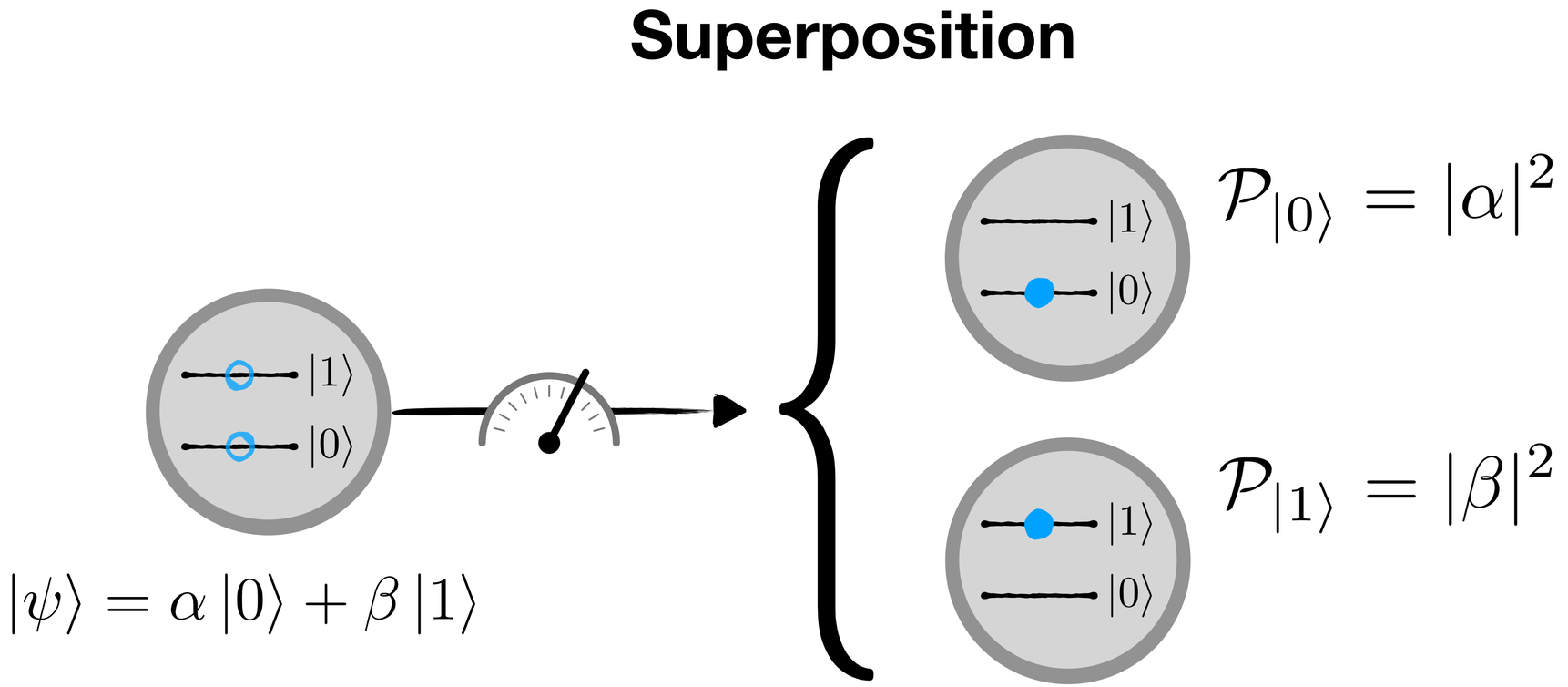


$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$

Notation de Dirac

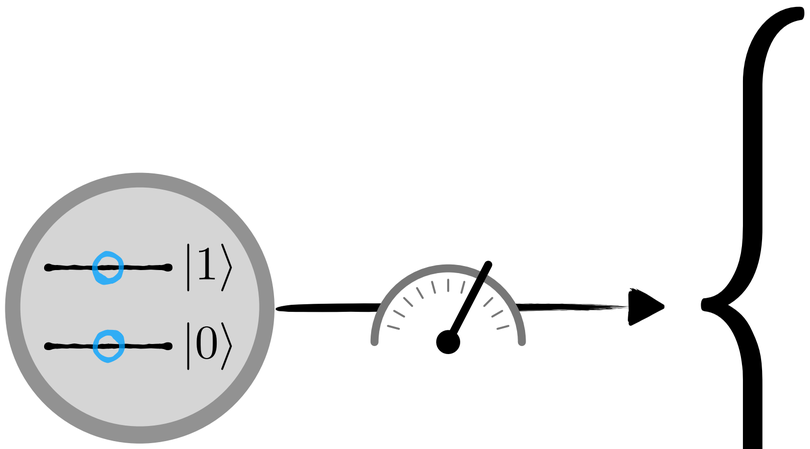


Notation de Dirac

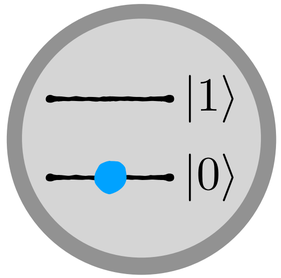


Notation de Dirac

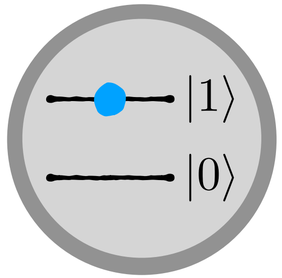
Superposition



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



$$\mathcal{P}_{|0\rangle} = |\alpha|^2$$

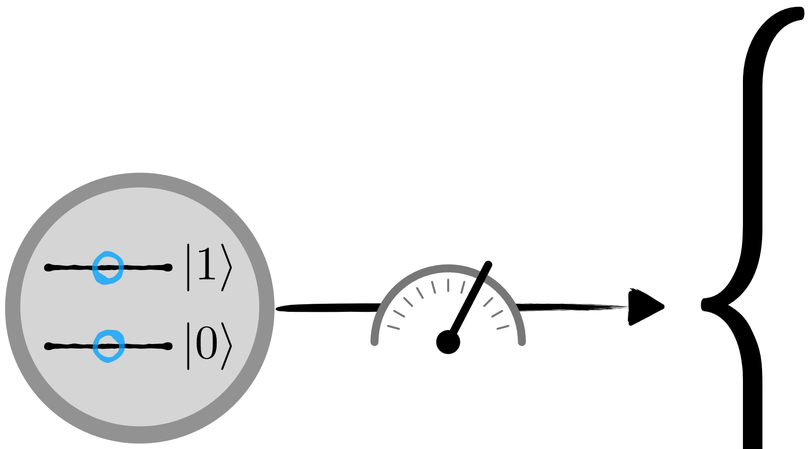


$$\mathcal{P}_{|1\rangle} = |\beta|^2$$

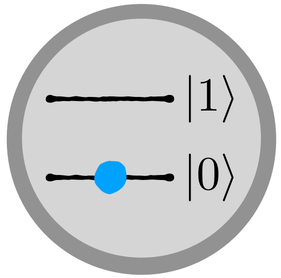
$$|\alpha|^2 + |\beta|^2 = 1$$

Notation de Dirac

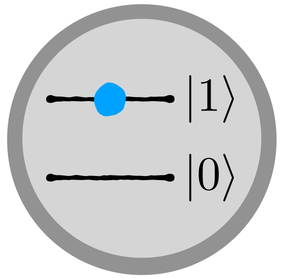
Superposition



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



$$\mathcal{P}_{|0\rangle} = |\alpha|^2$$



$$\mathcal{P}_{|1\rangle} = |\beta|^2$$

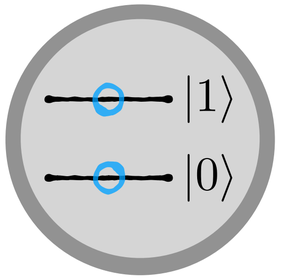
$$|\alpha|^2 + |\beta|^2 = 1$$

Exemples :

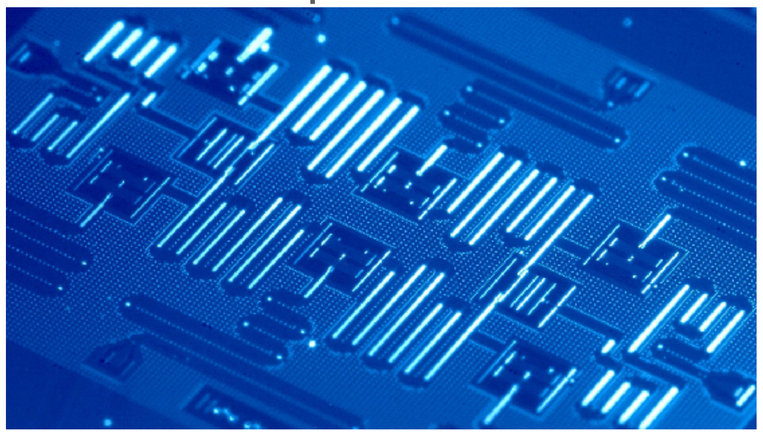
$$|\psi\rangle = 1|0\rangle + 0|1\rangle \qquad |\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \qquad |\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{-1}{\sqrt{2}}|1\rangle$$

Représentation physique
Information quantique

Qubit

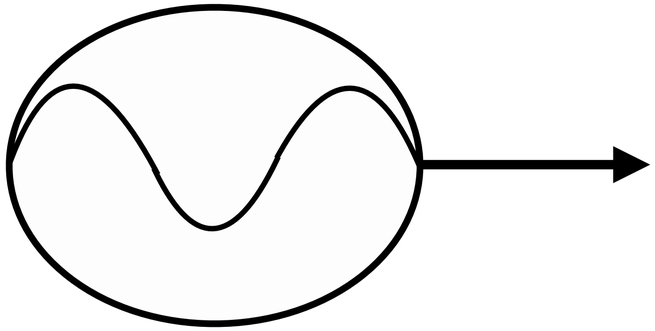


Qubits supraconducteurs



IBM

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



Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

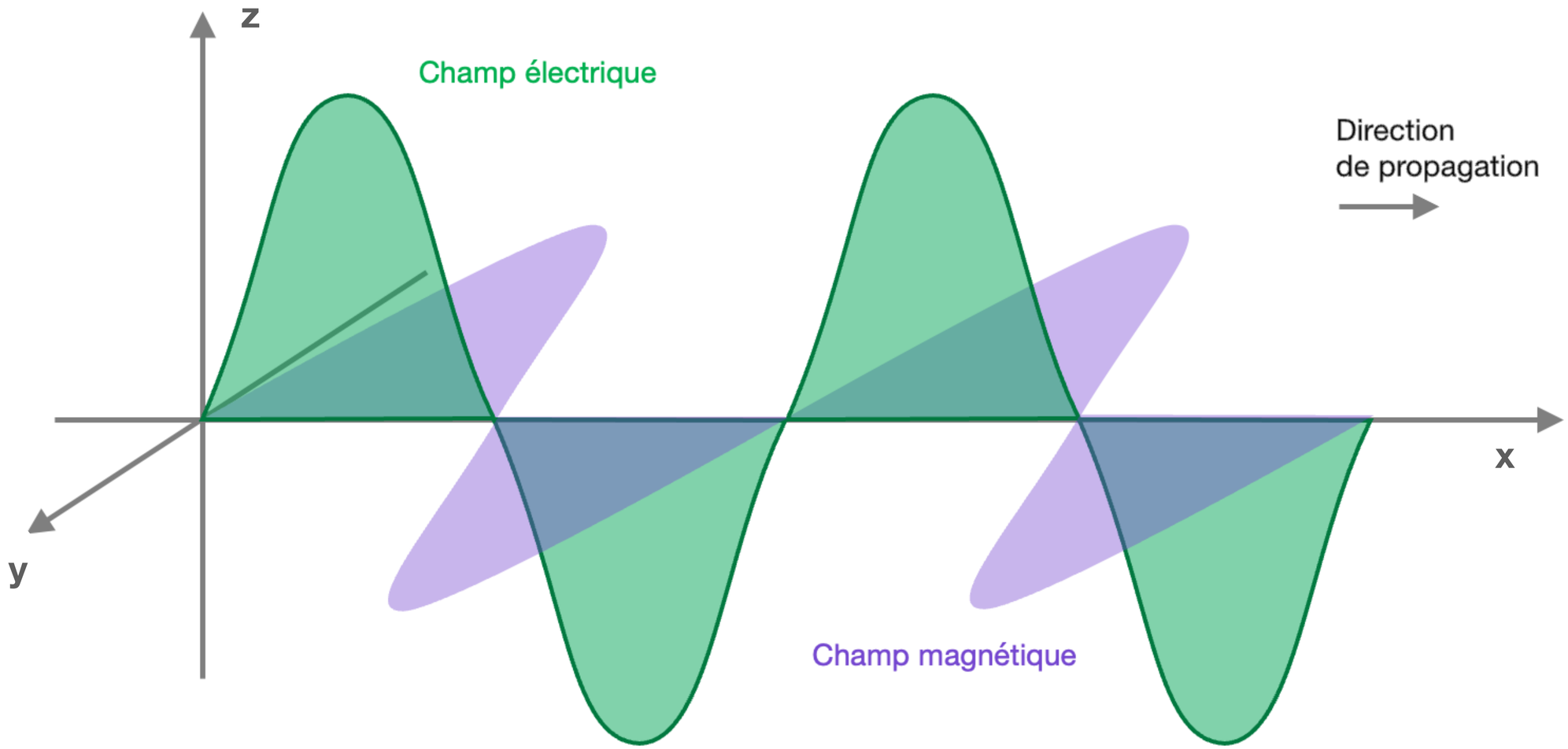
Plan

- [x] Présentation
- [x] Cryptographie
- [x] Le qubit
- [ ] Le photon: messager d’information quantique
- [ ] Intrication et inégalité CHSH
- [ ] Protocole E91
- [ ] Atelier pratique

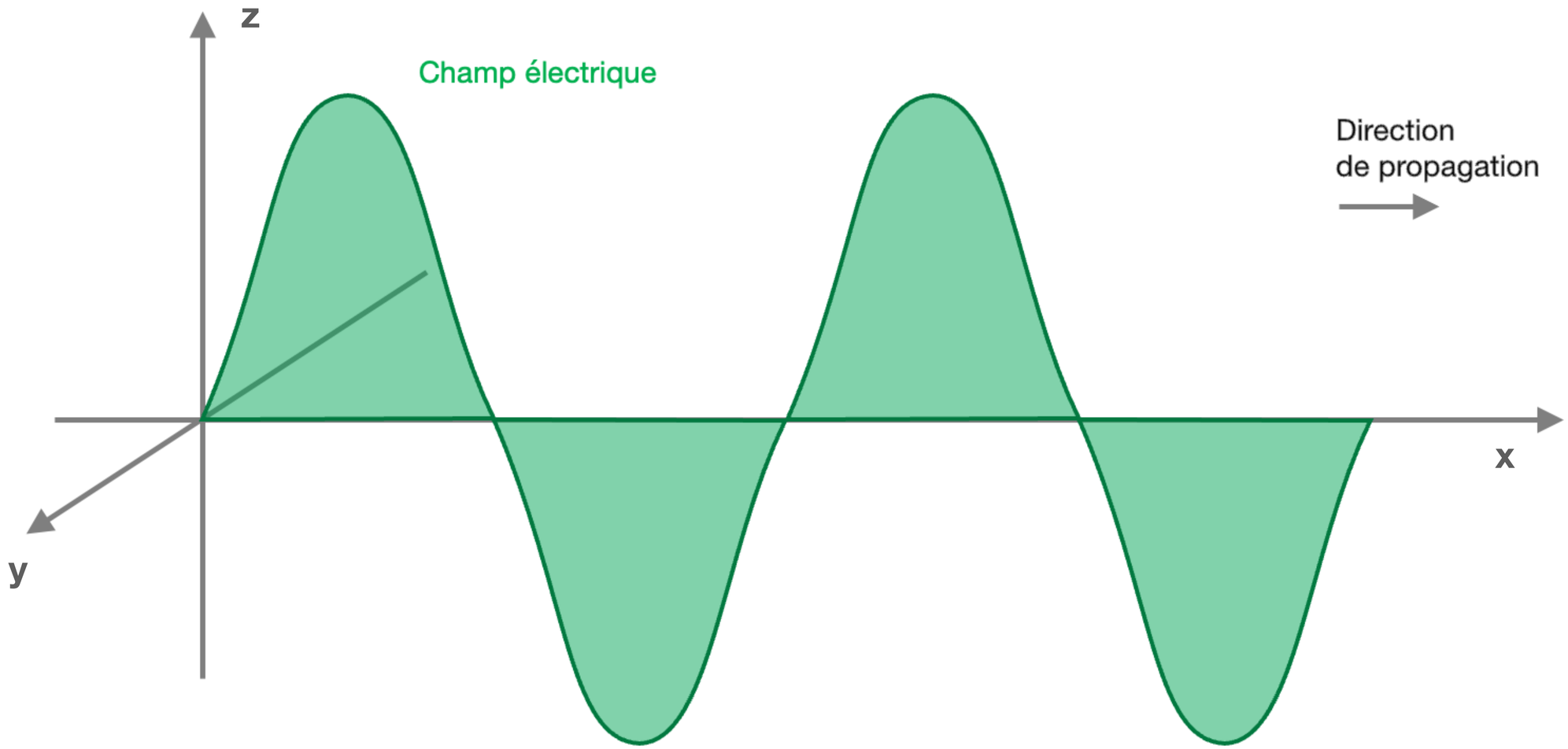
Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

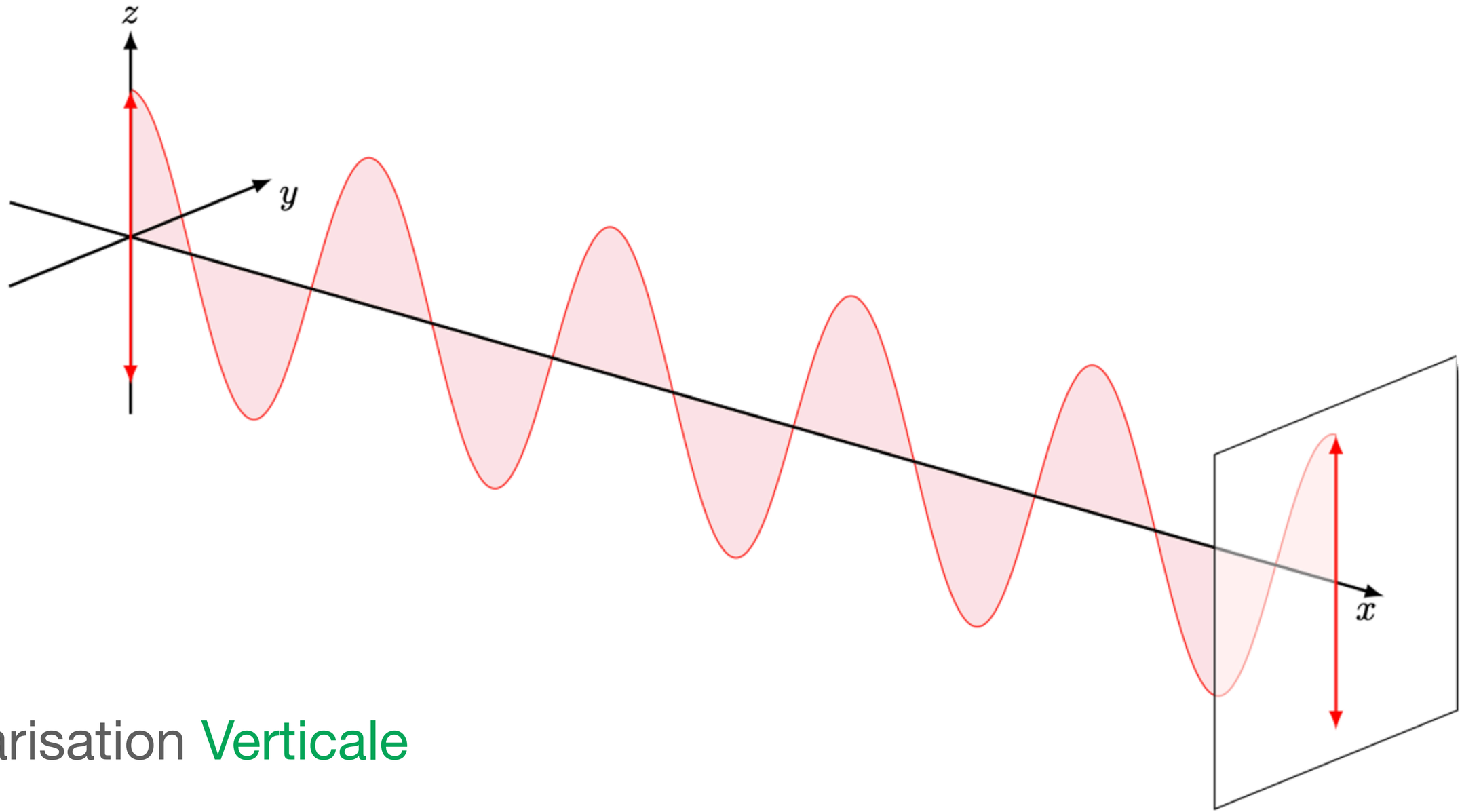
La lumière


z
Champ électrique
Direction
de propagation
x
y
Champ magnétique

La polarisation: propriété quantique

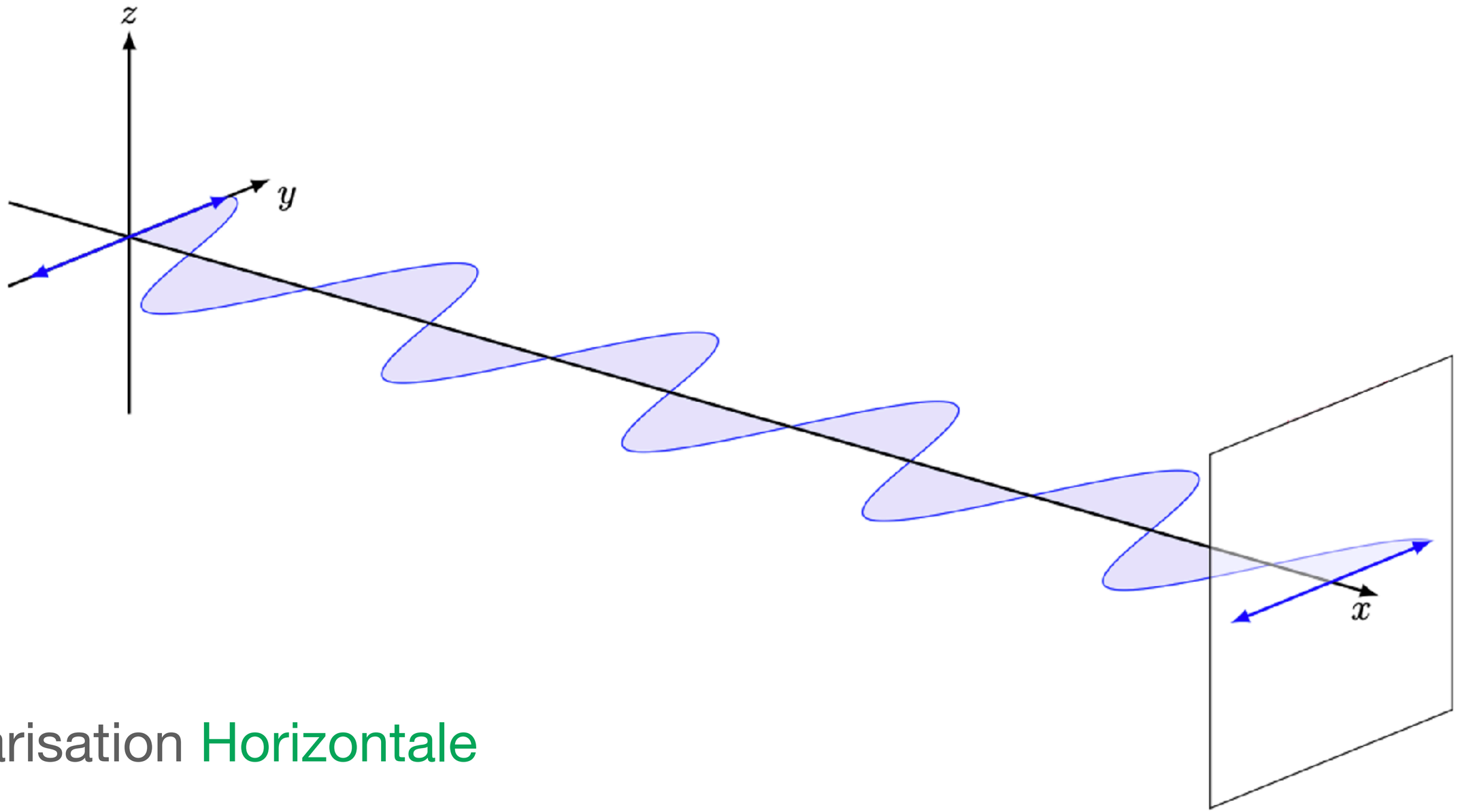


La polarisation: propriété quantique



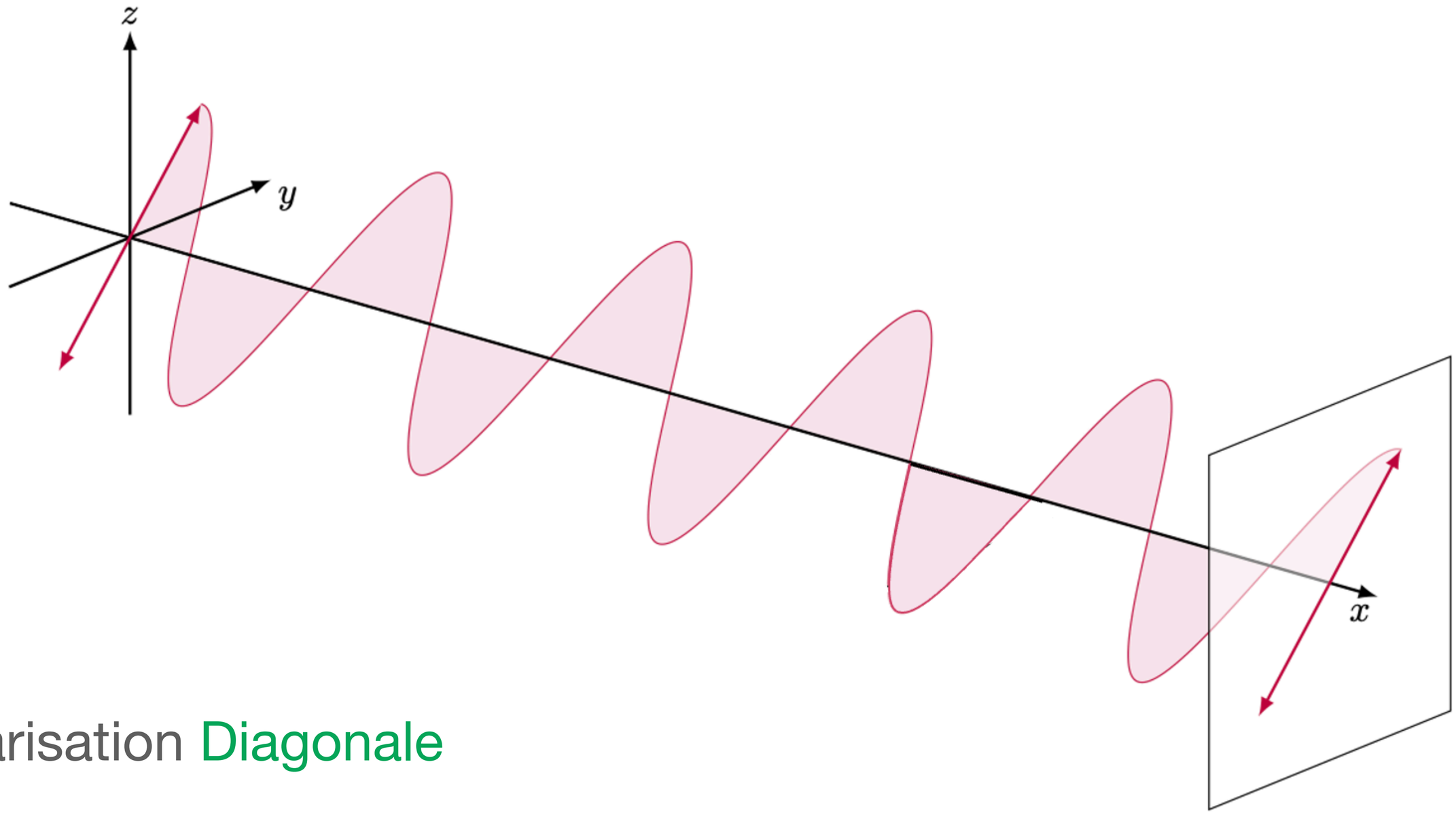
Polarisation Verticale

La polarisation: propriété quantique



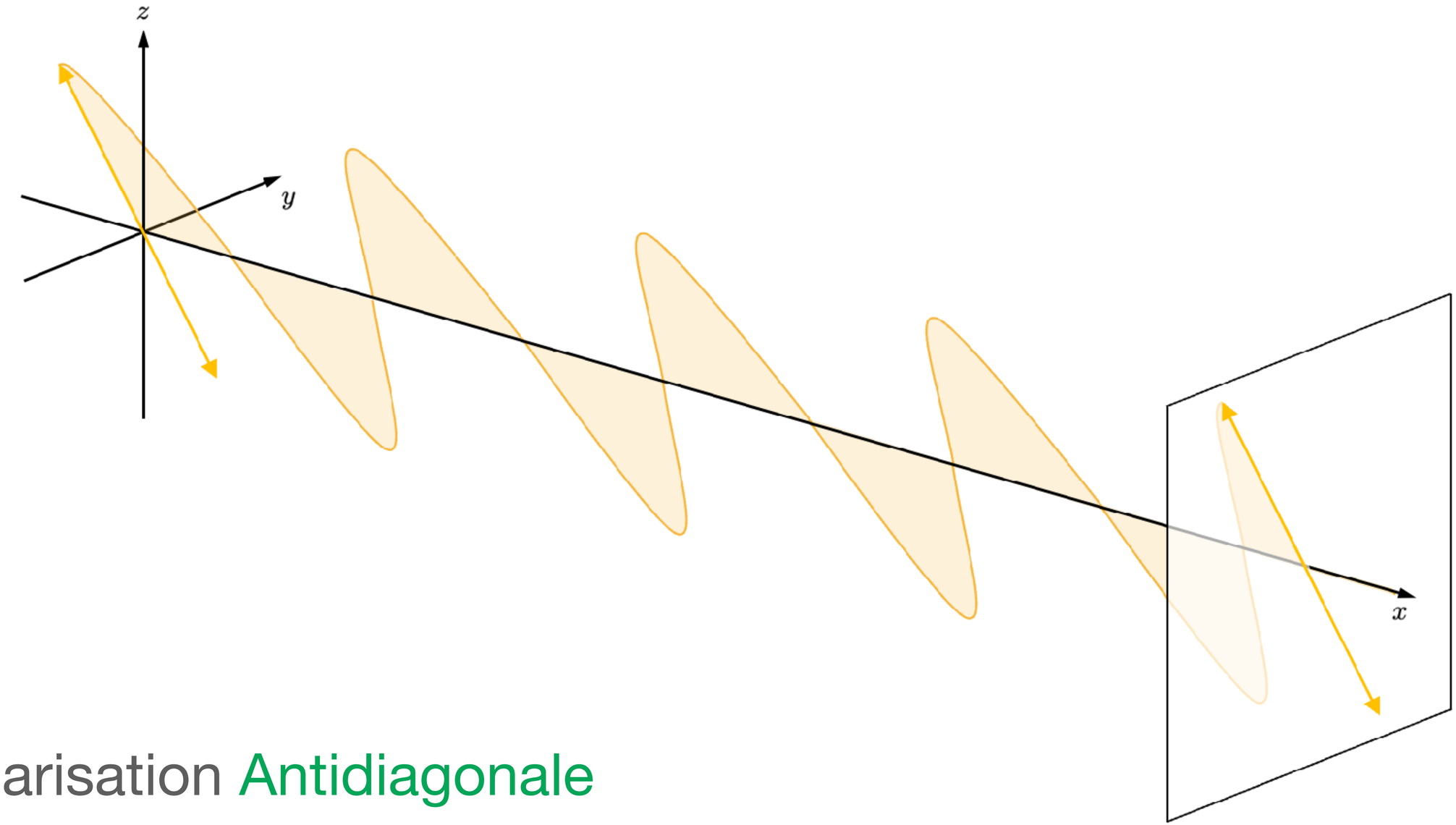
Polarisation Horizontale

La polarisation: propriété quantique



Polarisation Diagonale

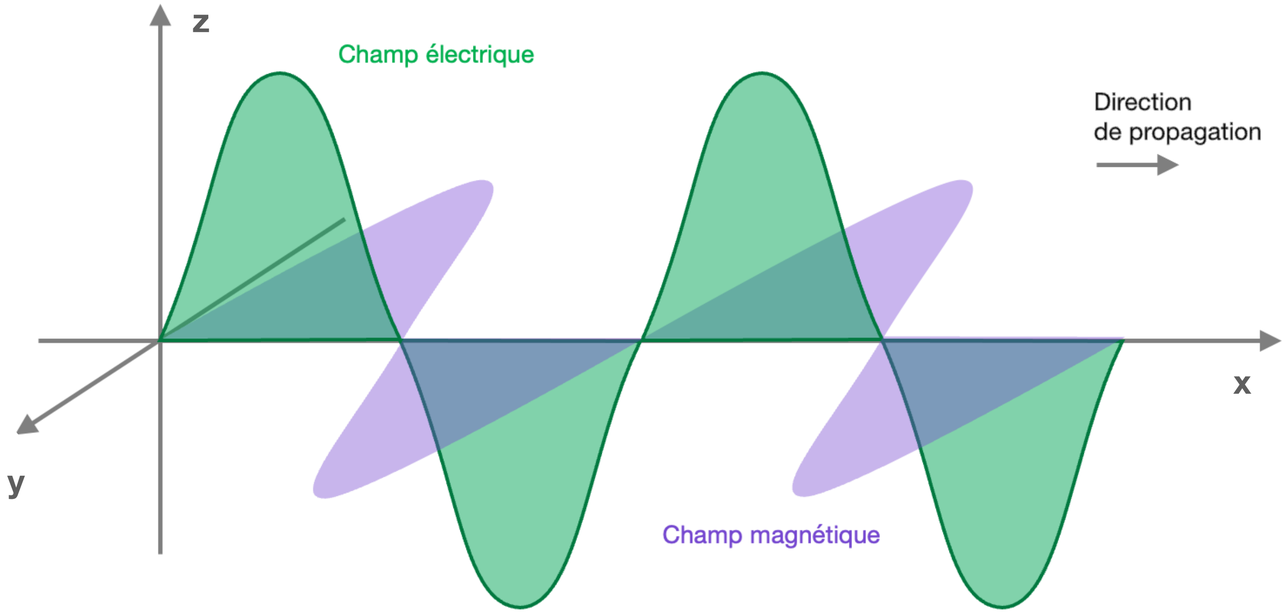
La polarisation: propriété quantique



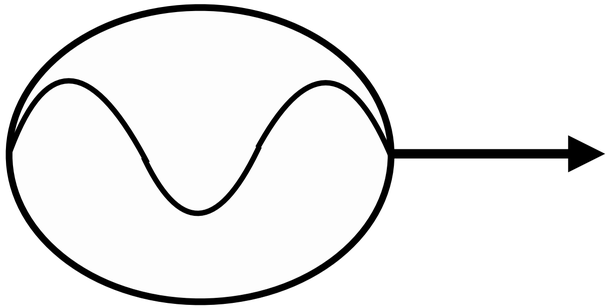
Polarisation Antidiagonale

Dualité onde-particule de la lumière

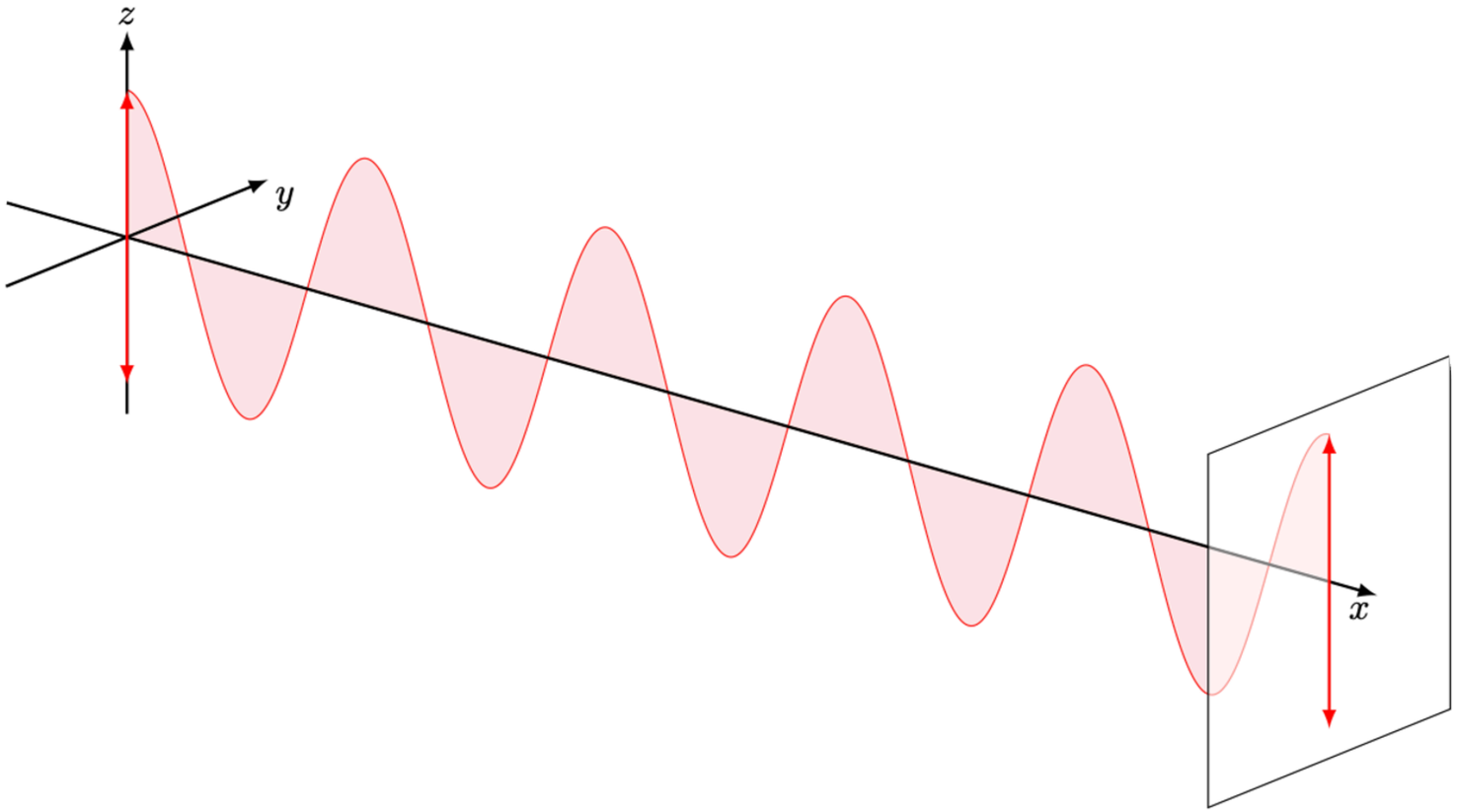
Onde électro-magnétique

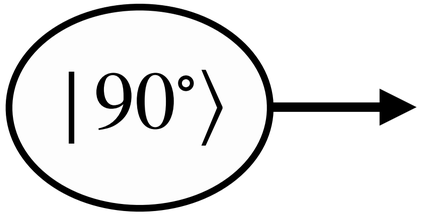


Le photon

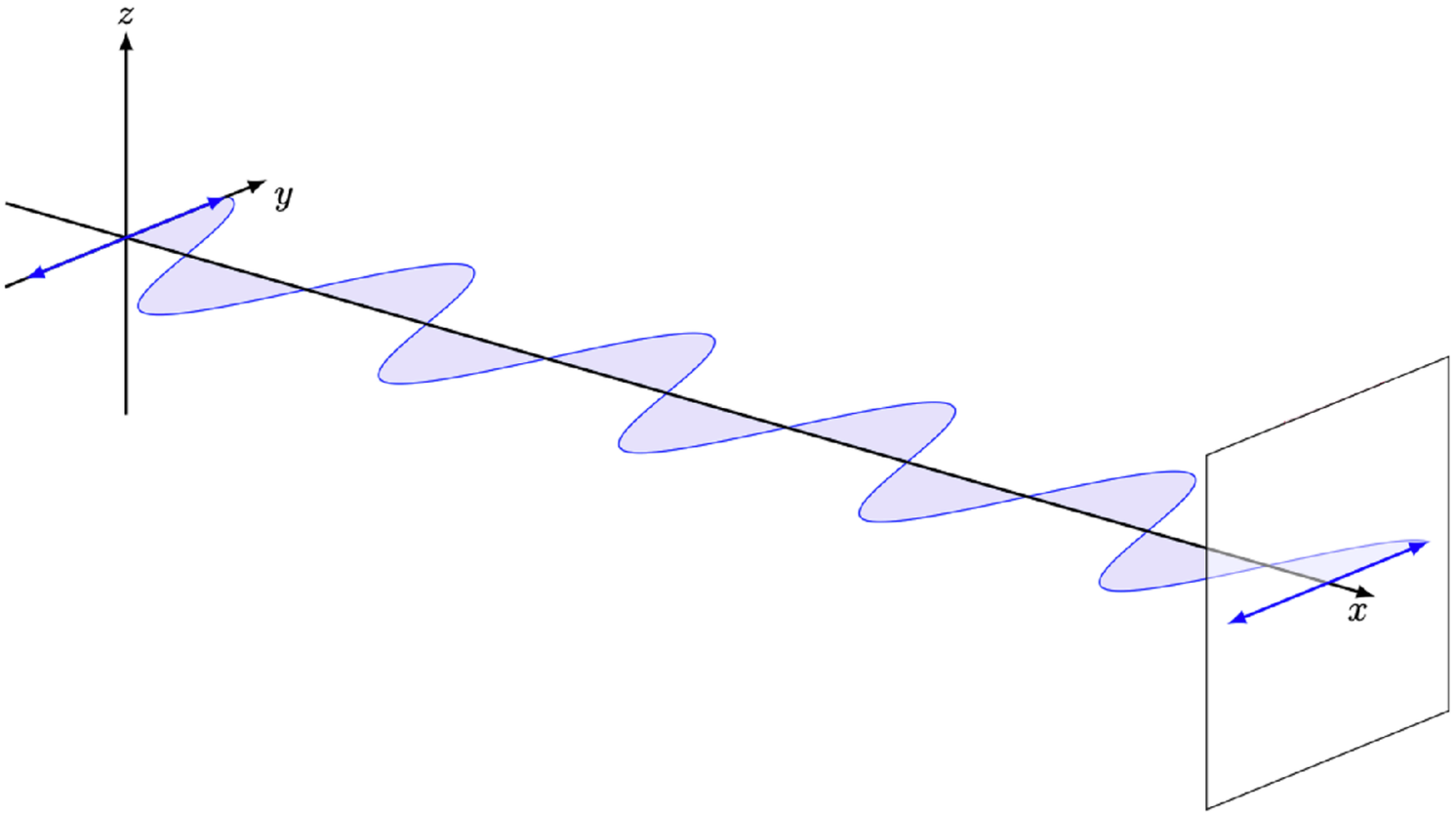


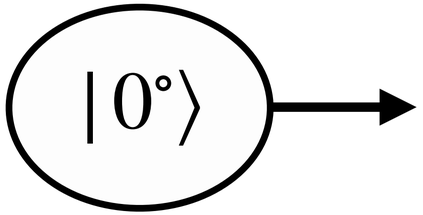
Polarisation Verticale



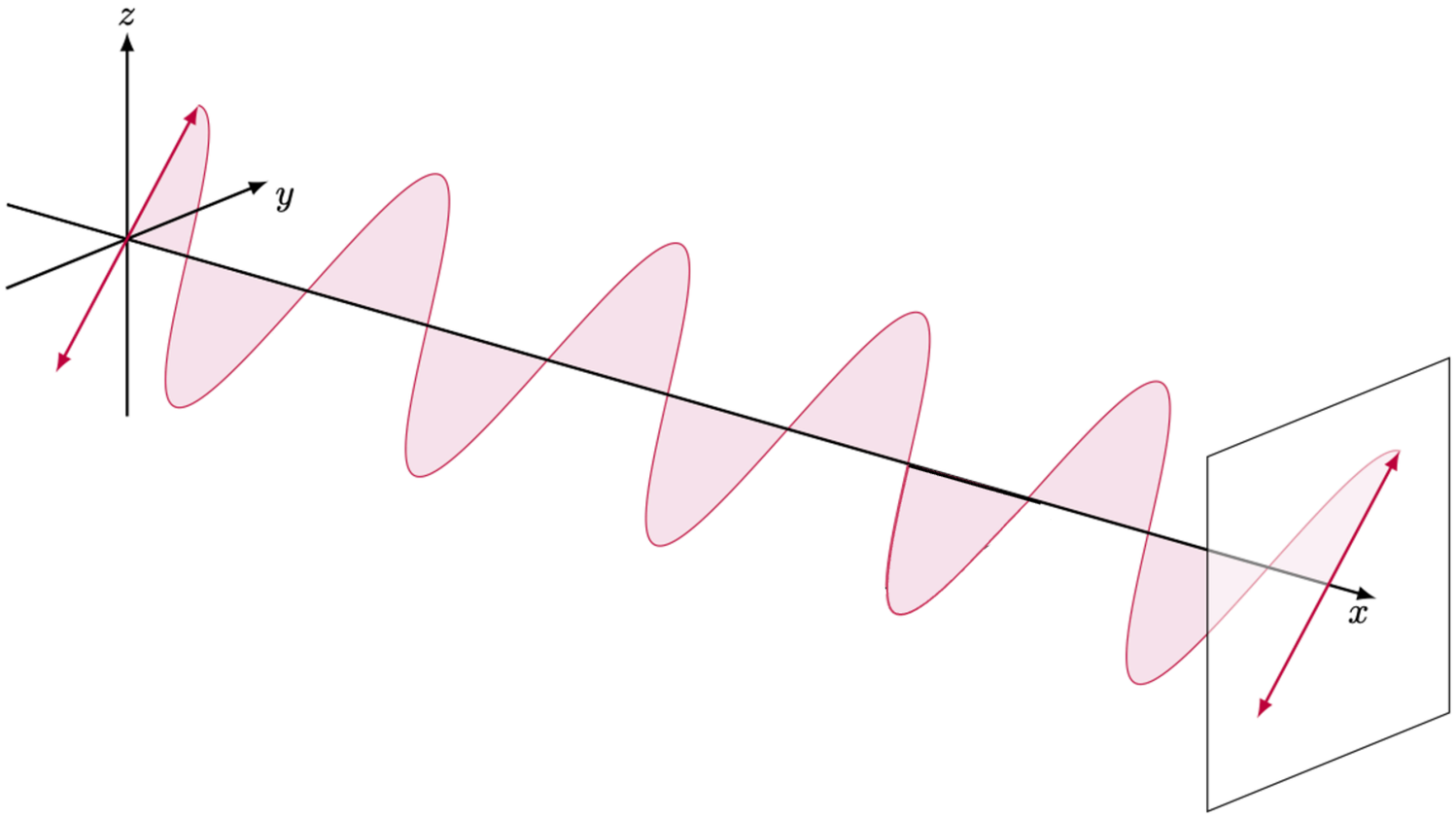


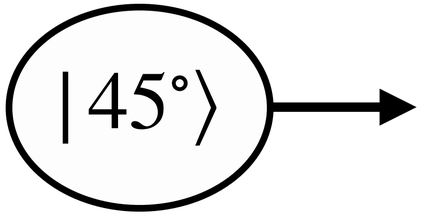
Polarisation Horizontale



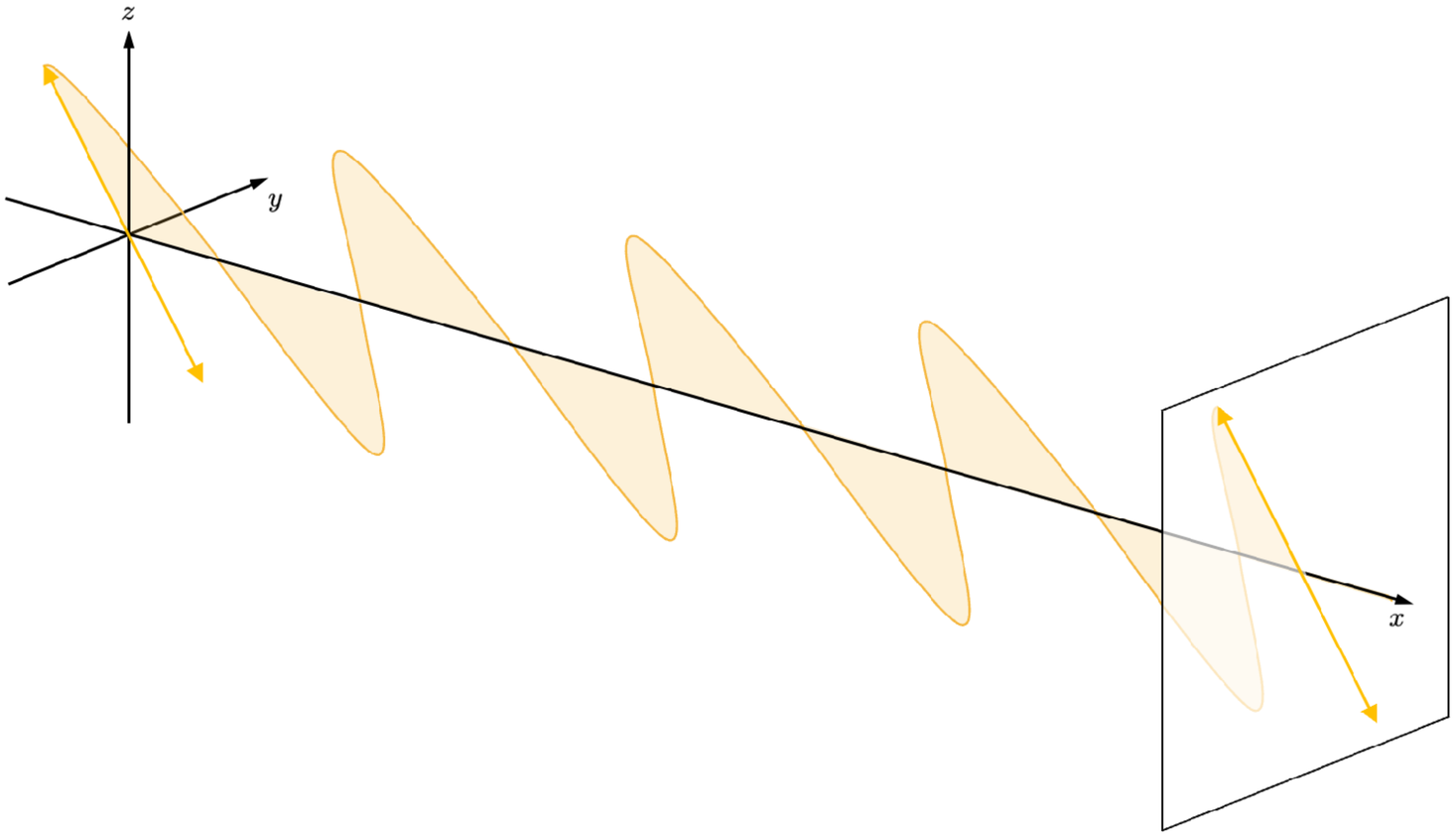


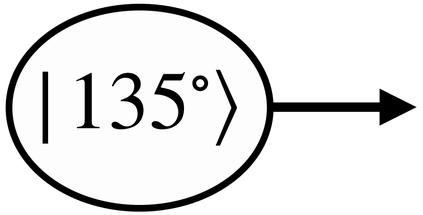
Polarisation Diagonale





Polarisation Antidiagonale

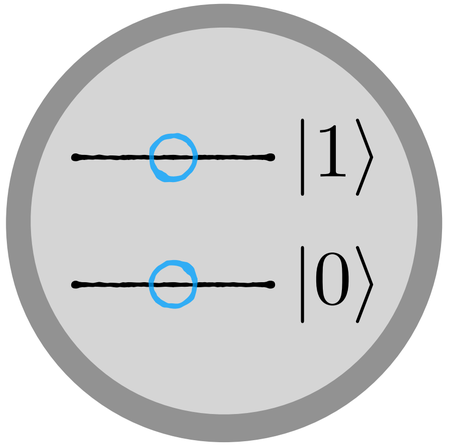




États de base

États de base

$|0\rangle$ et $|1\rangle$



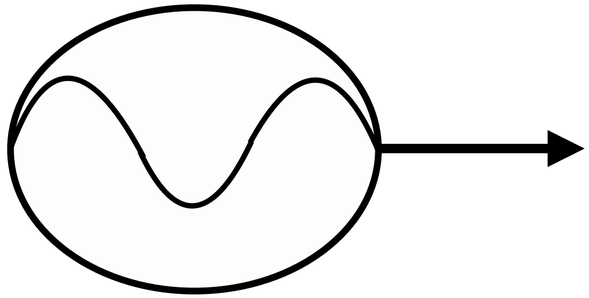
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

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

États de base

États de base

$|0\rangle$ et $|1\rangle$



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

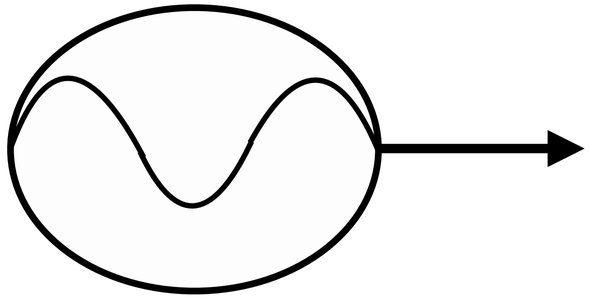
$$|\alpha|^2 + |\beta|^2 = 1$$

États de base

États de base

$|0\rangle$ et $|1\rangle$

$|90°\rangle$ et $|0°\rangle$



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

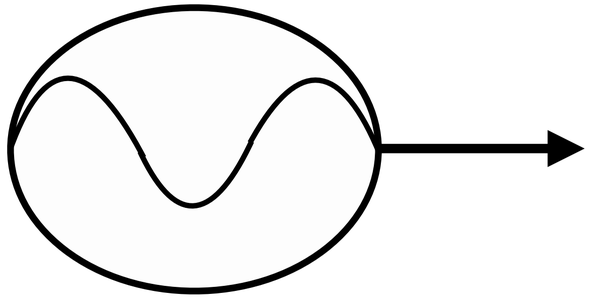
$$|\alpha|^2 + |\beta|^2 = 1$$

États de base

États de base

$|0\rangle$ et $|1\rangle$

$|90°\rangle$ et $|0°\rangle$



$$|\psi\rangle = \alpha|90°\rangle + \beta|0°\rangle$$

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

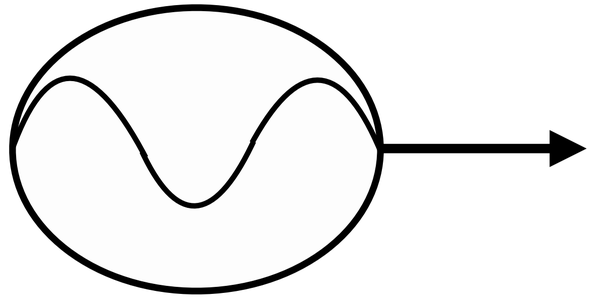
États de base

États de base

$|0\rangle$ et $|1\rangle$

$|90°\rangle$ et $|0°\rangle$

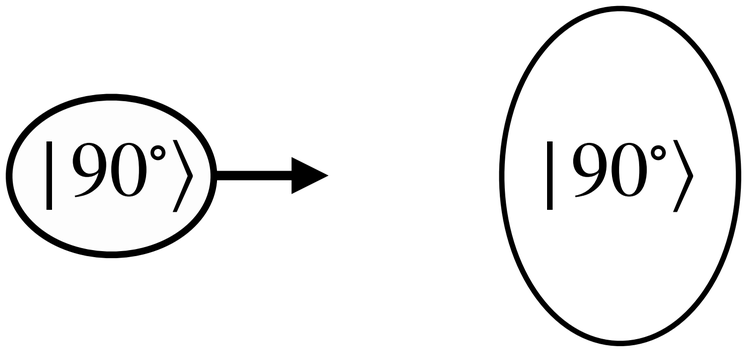
$|45°\rangle$ et $|135°\rangle$

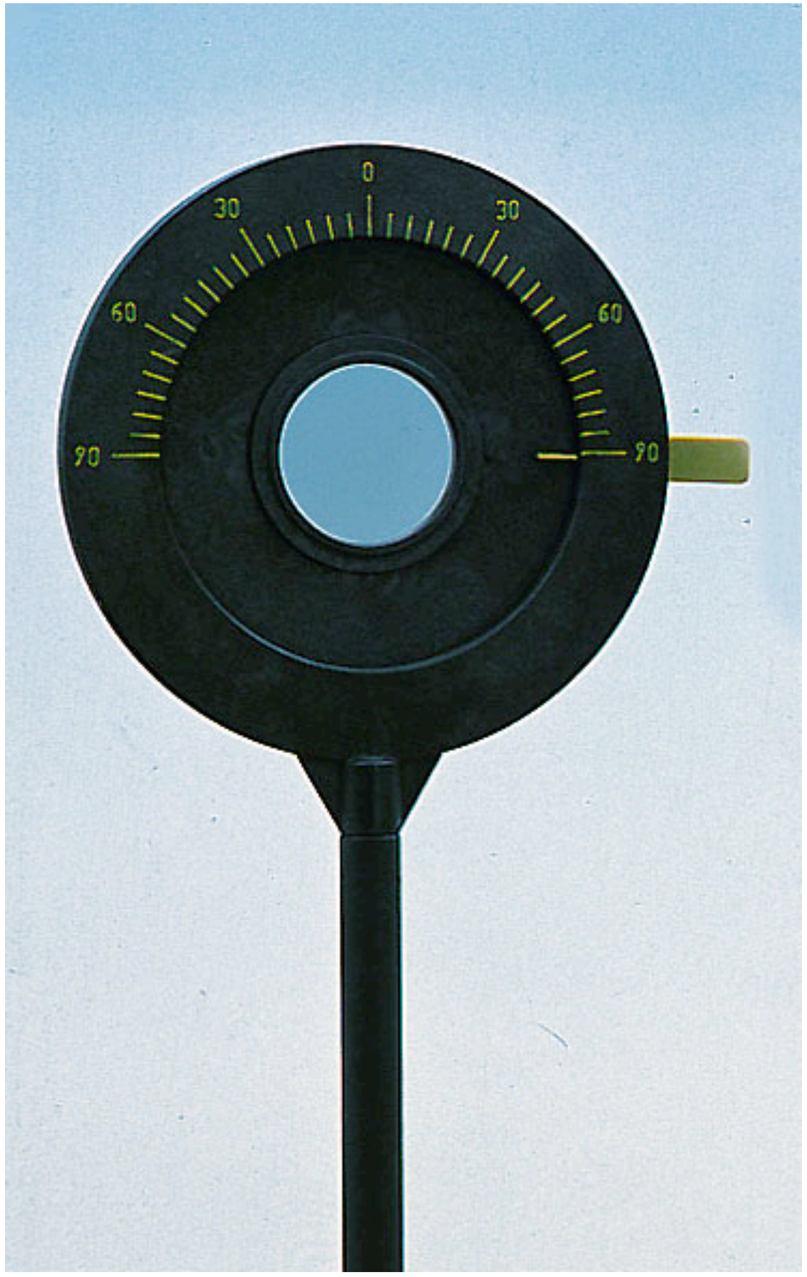


$$|\psi\rangle = \alpha|45°\rangle + \beta|135°\rangle$$

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

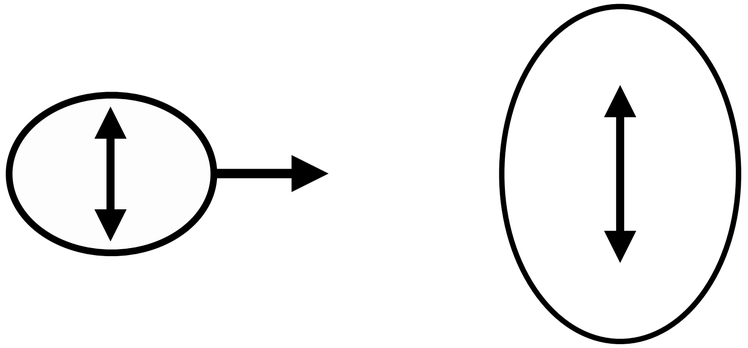
Le polariseur

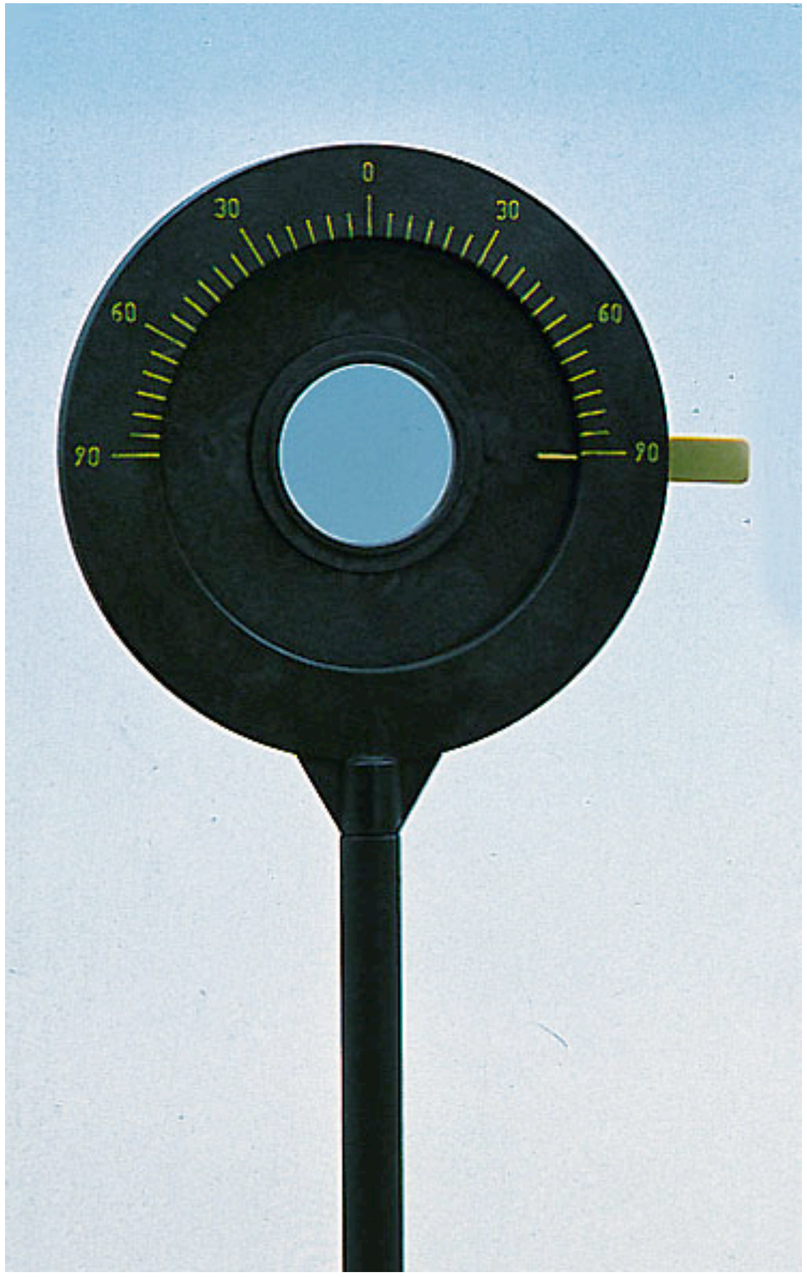




https://www.leybold-shop.fr/

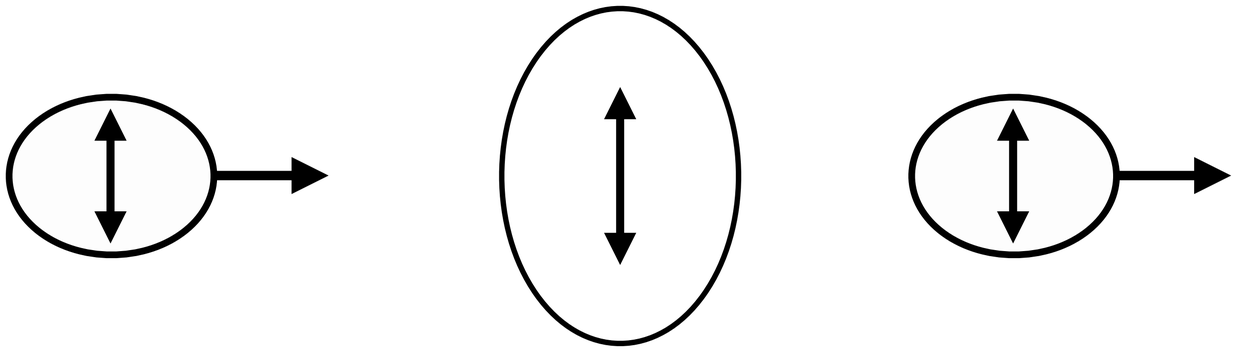
Le polariseur

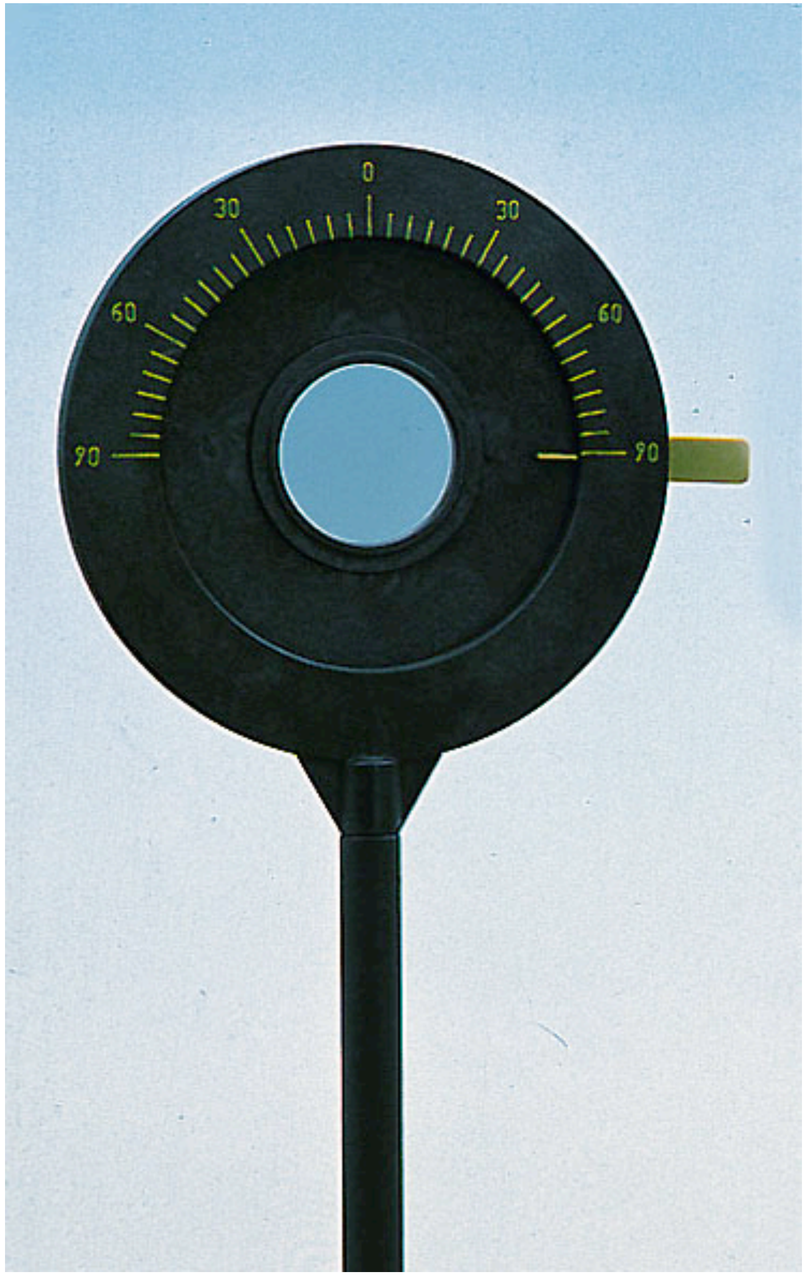




https://www.leybold-shop.fr/

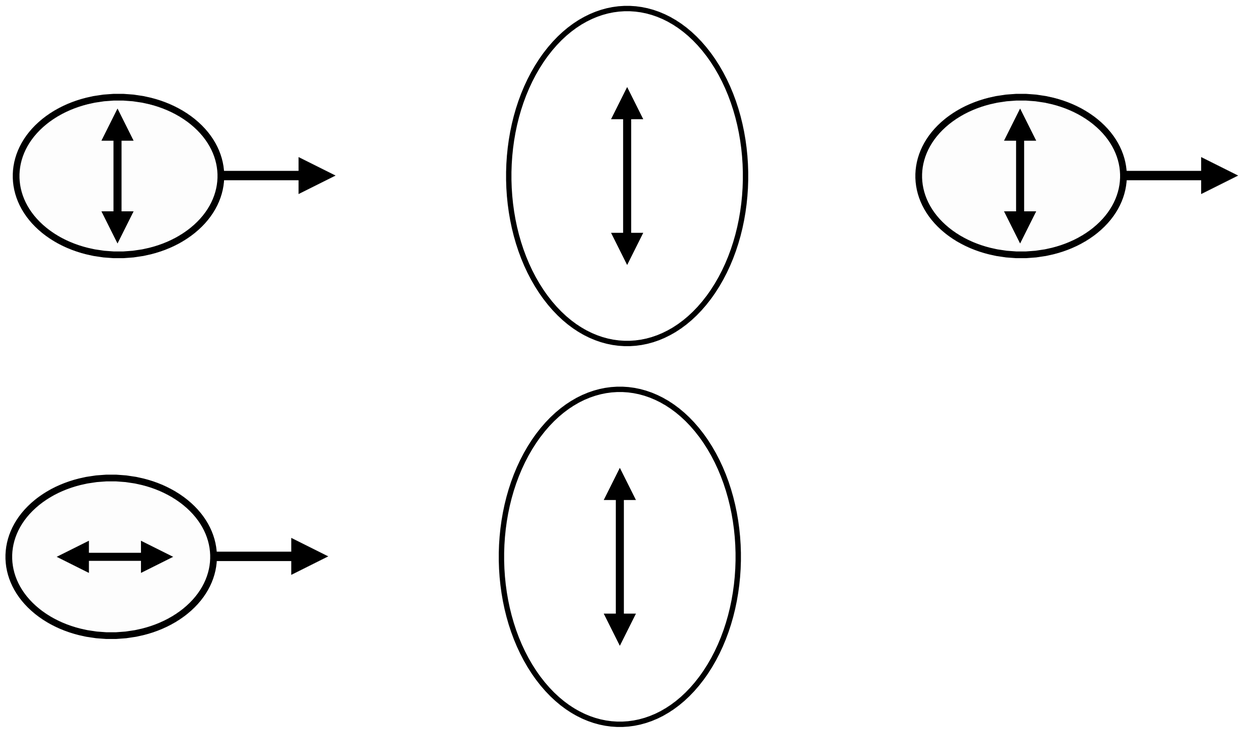
Le polariseur

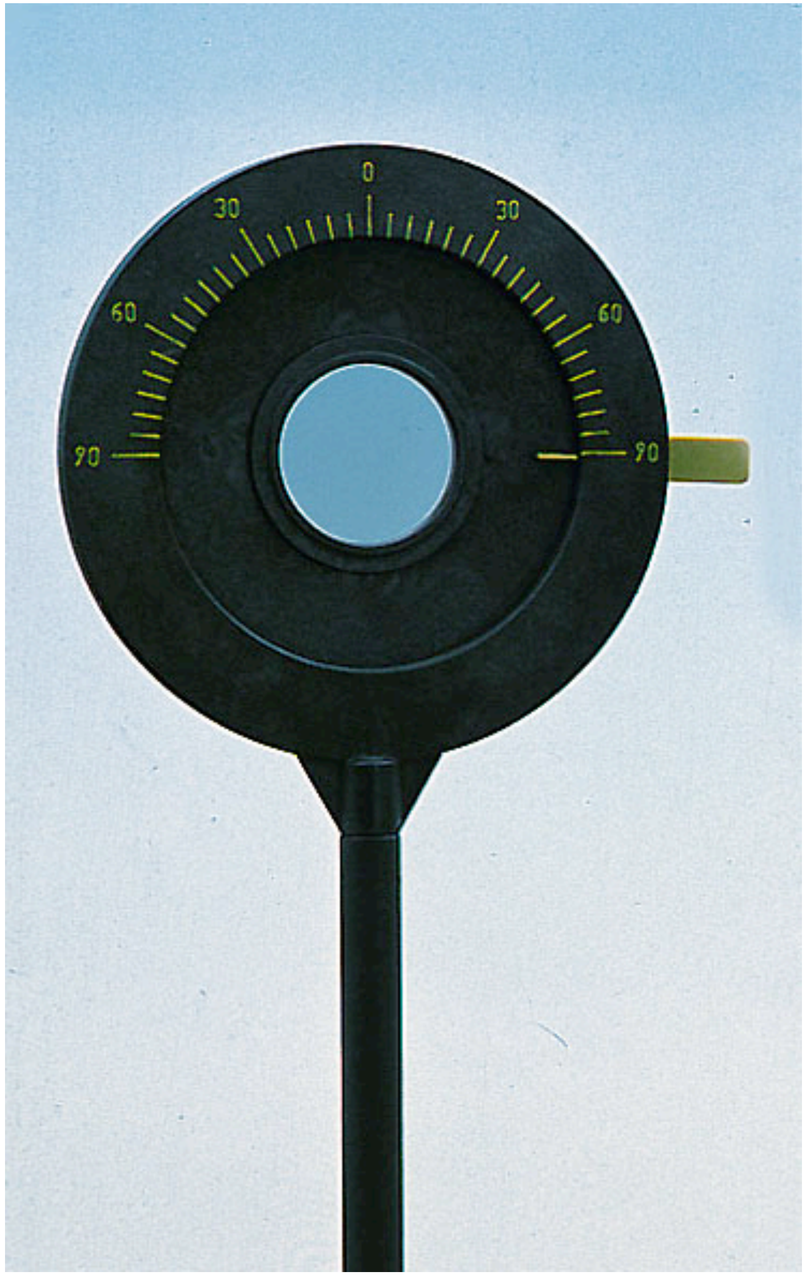




https://www.leybold-shop.fr/

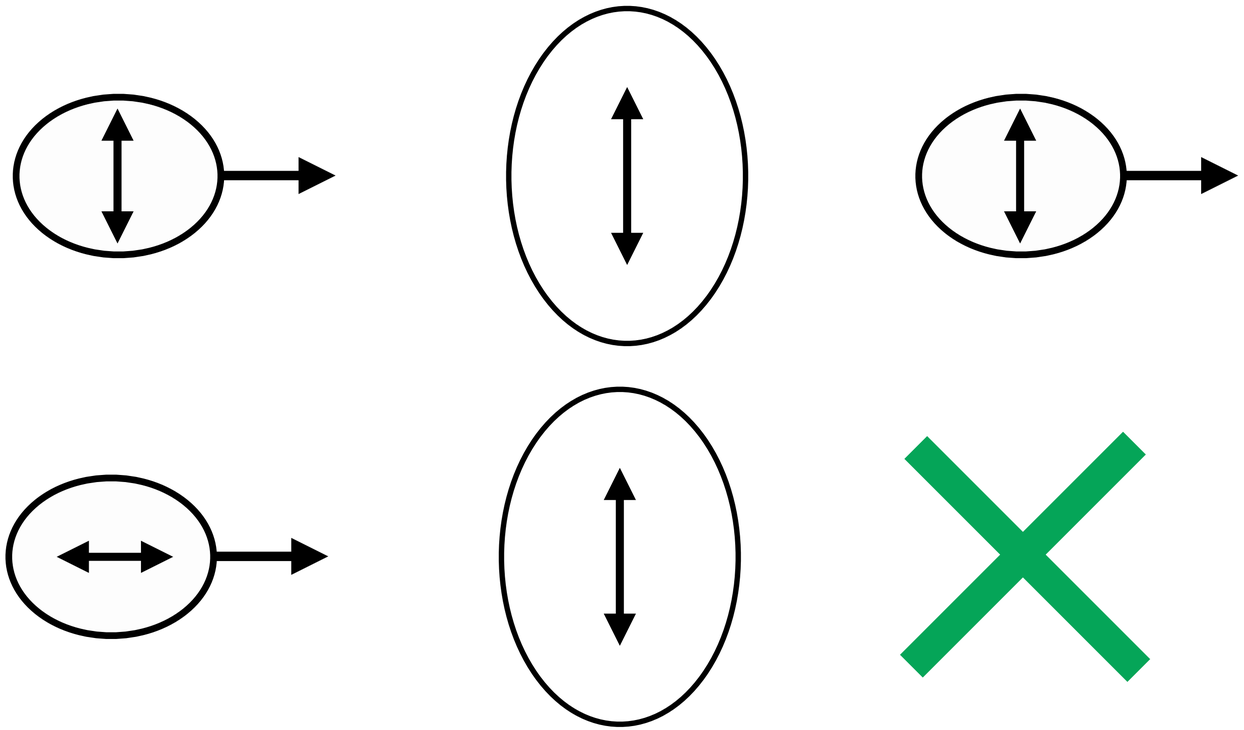
Le polariseur

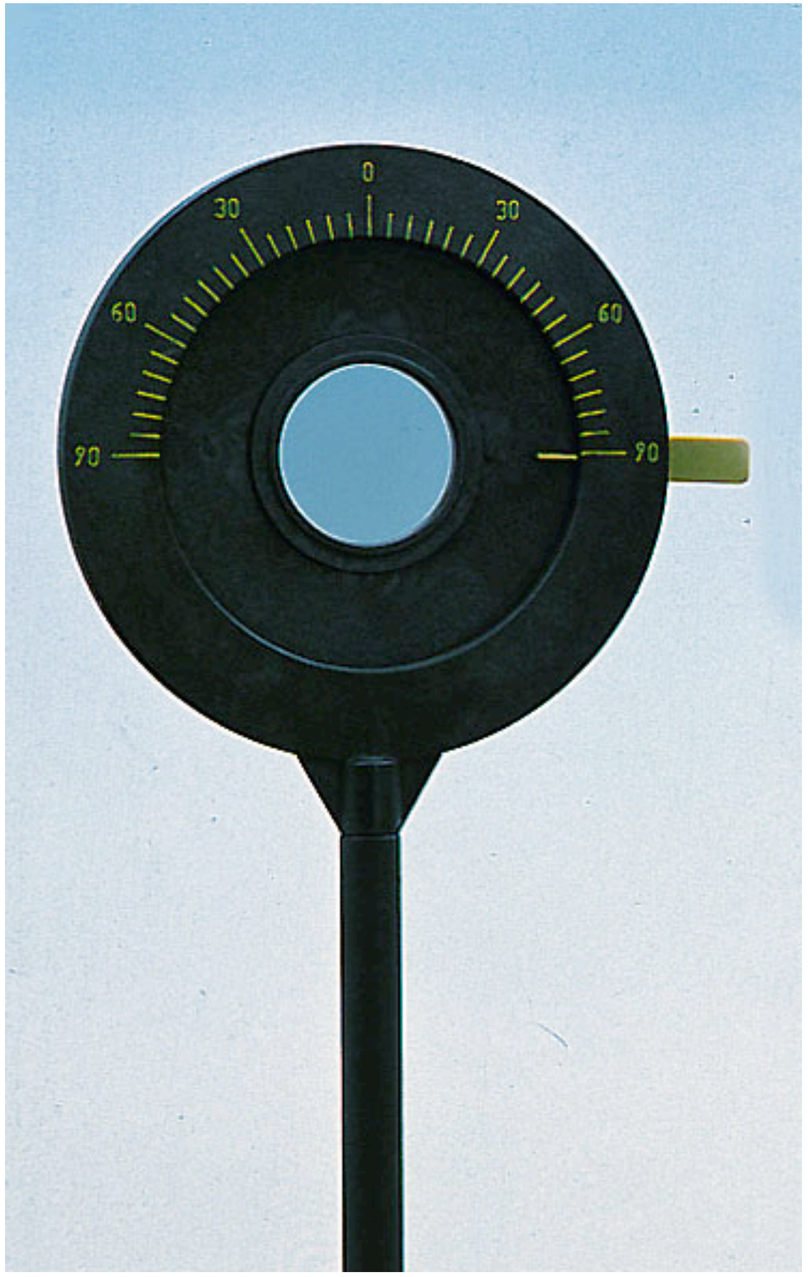




https://www.leybold-shop.fr/

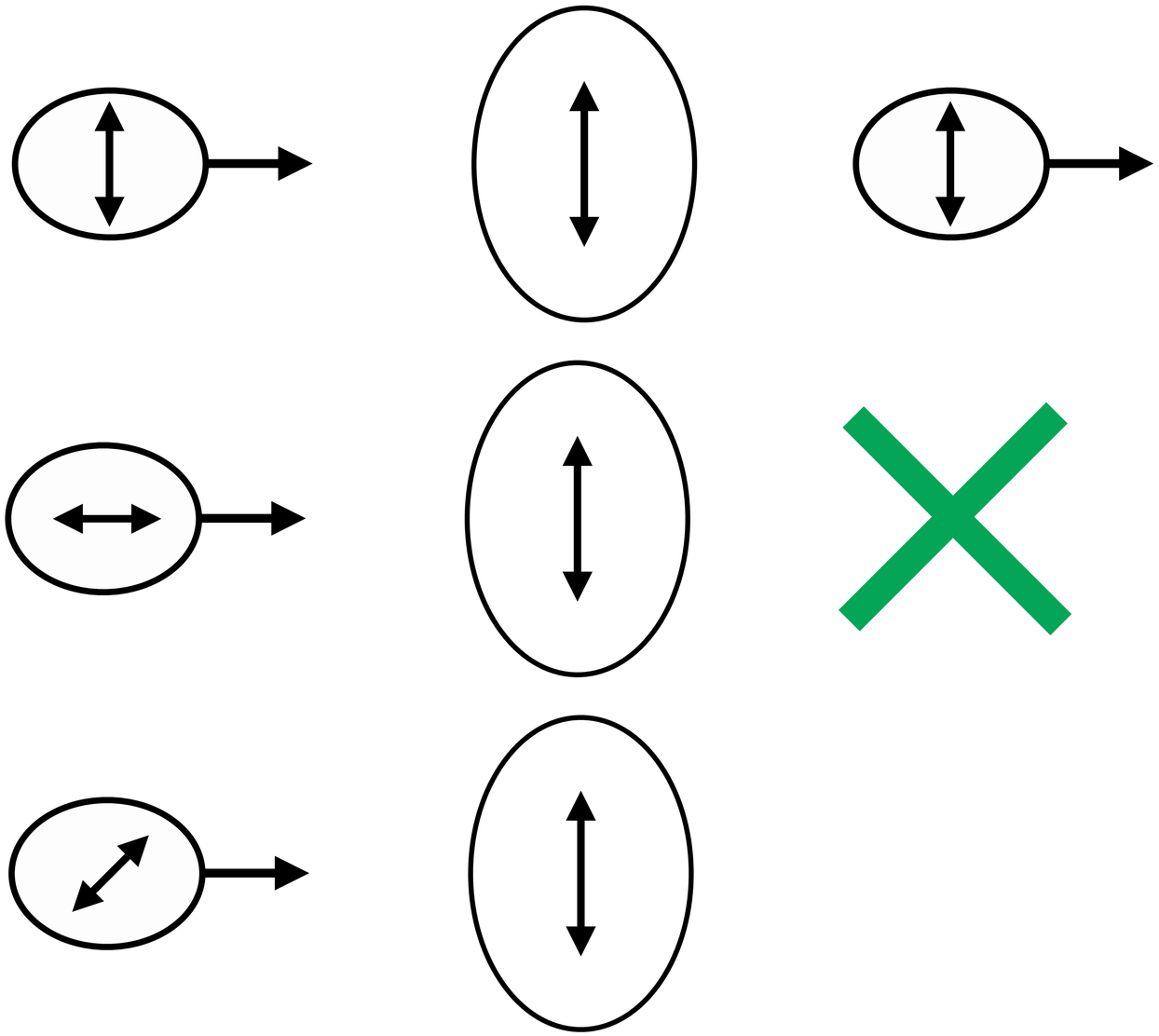
Le polariseur

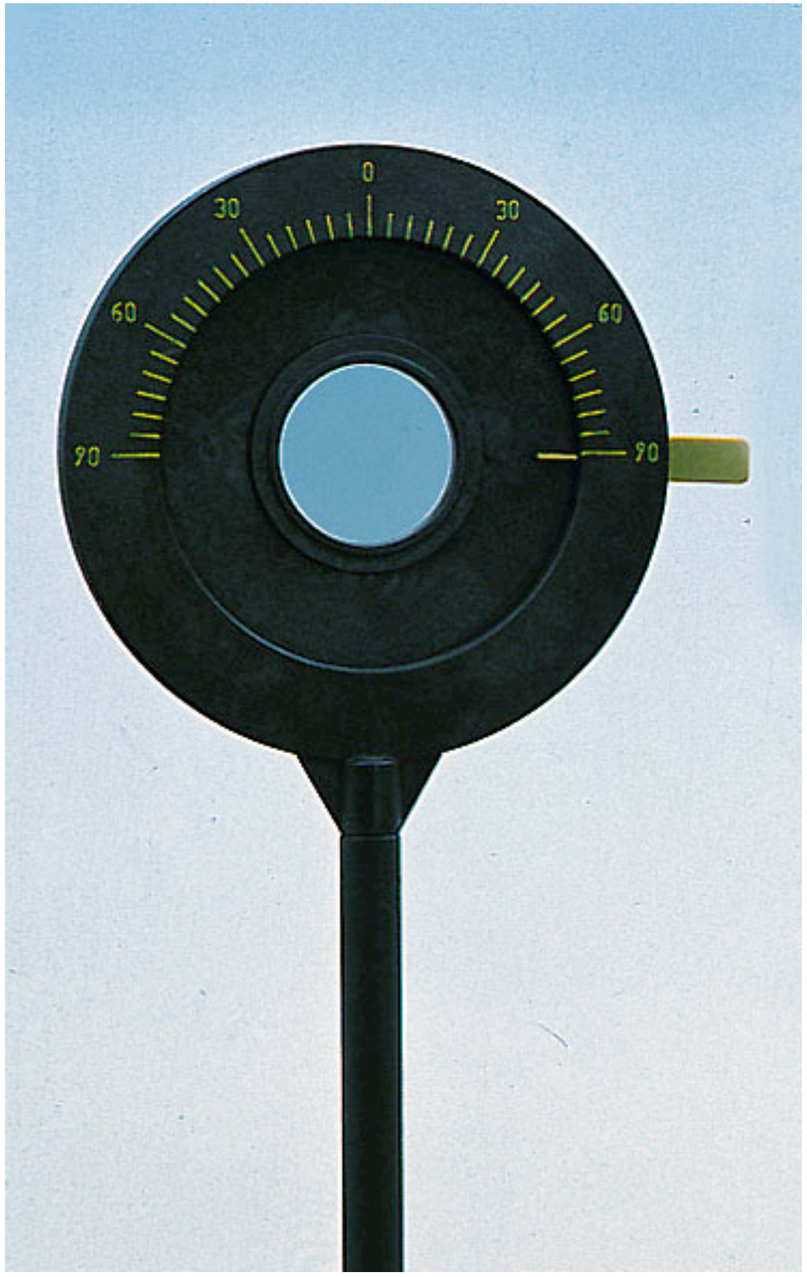




https://www.leybold-shop.fr/

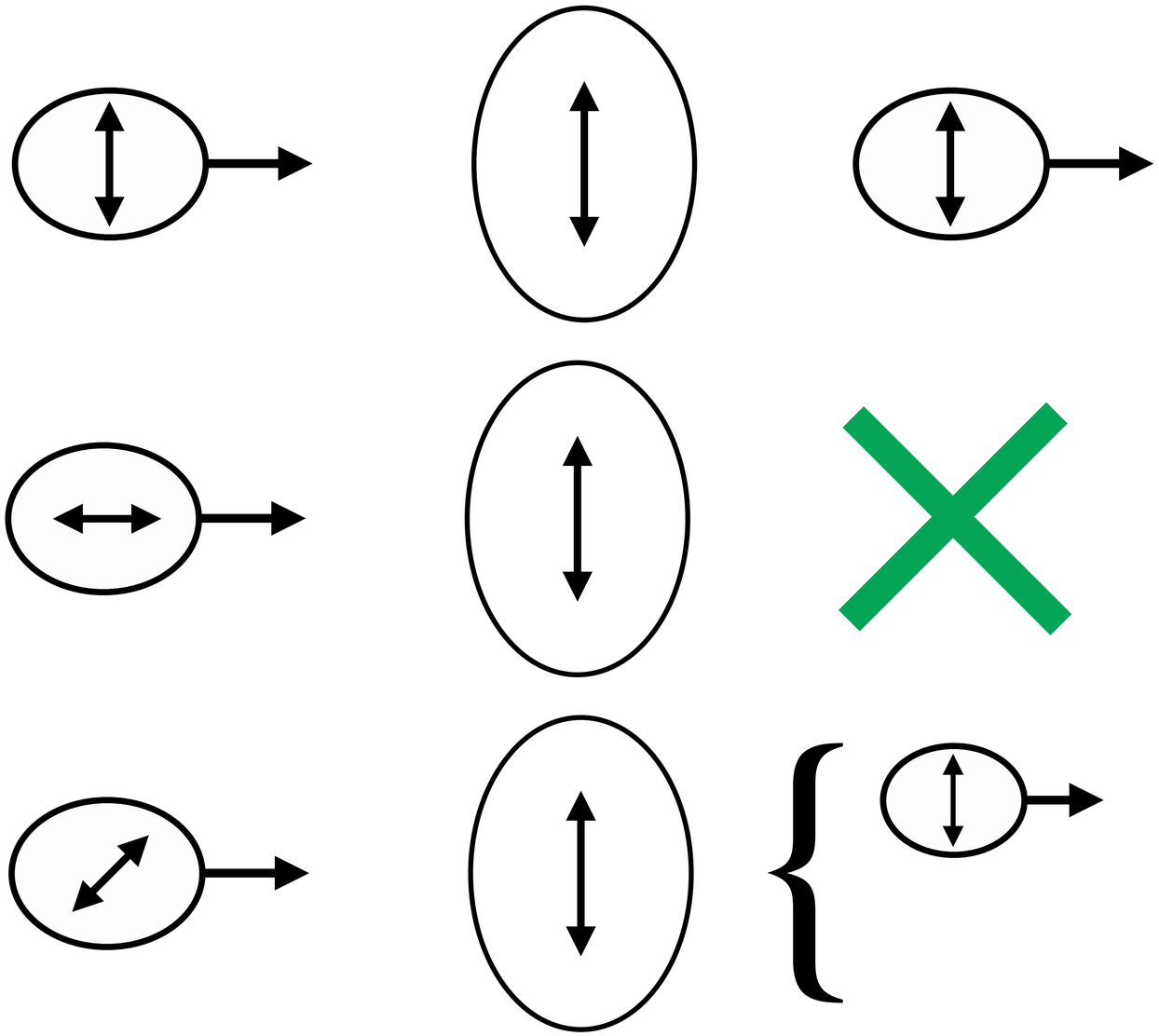
Le polariseur

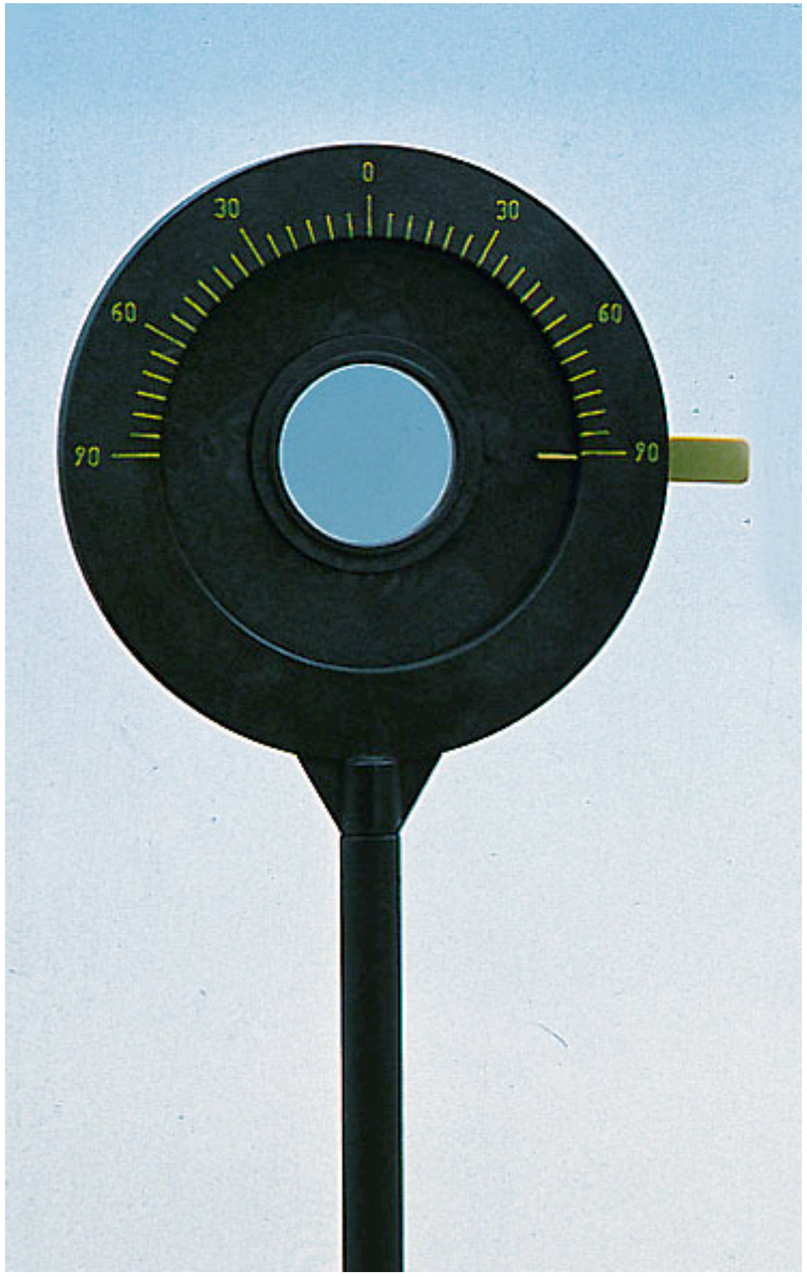




https://www.leybold-shop.fr/

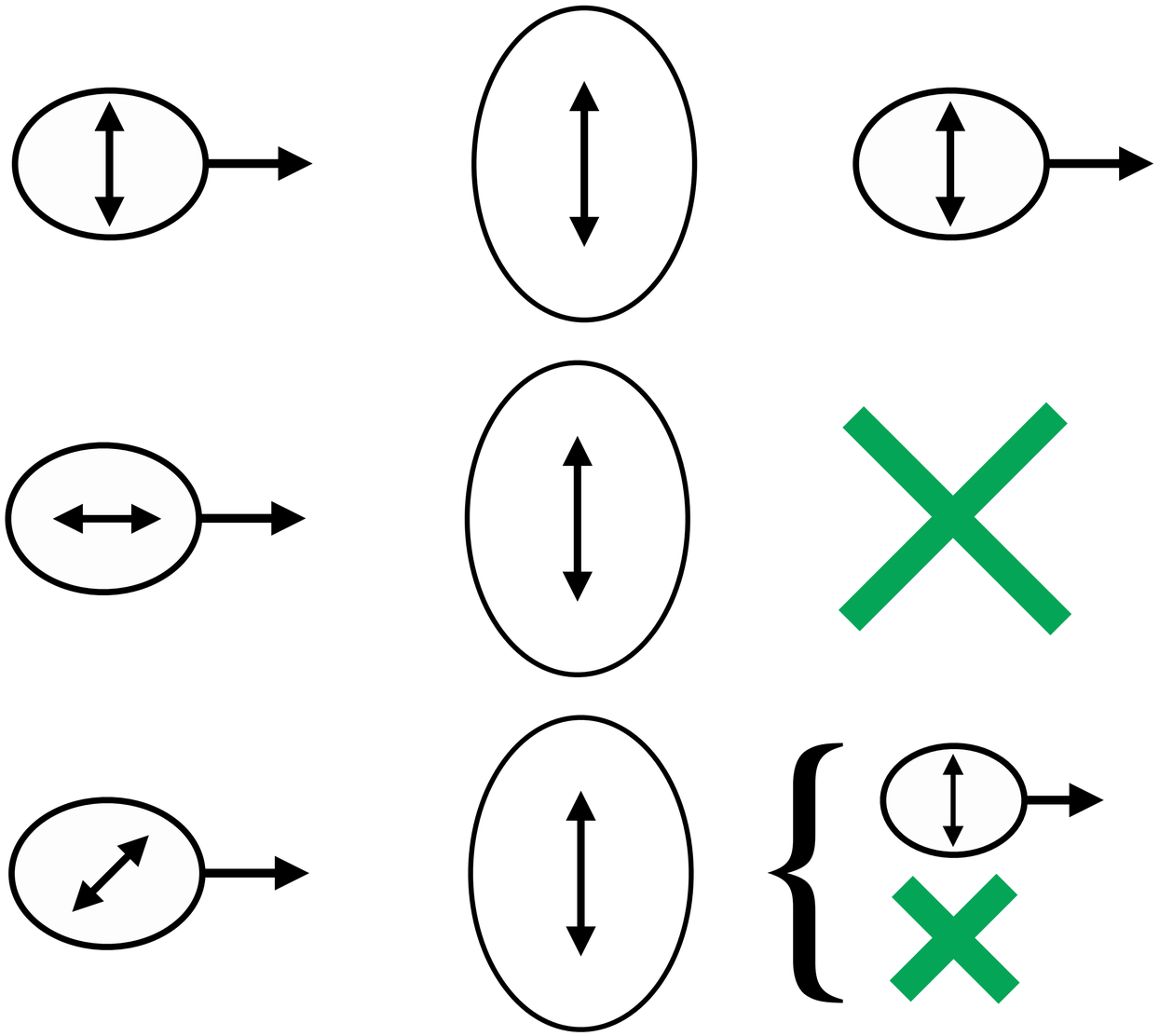
Le polariseur

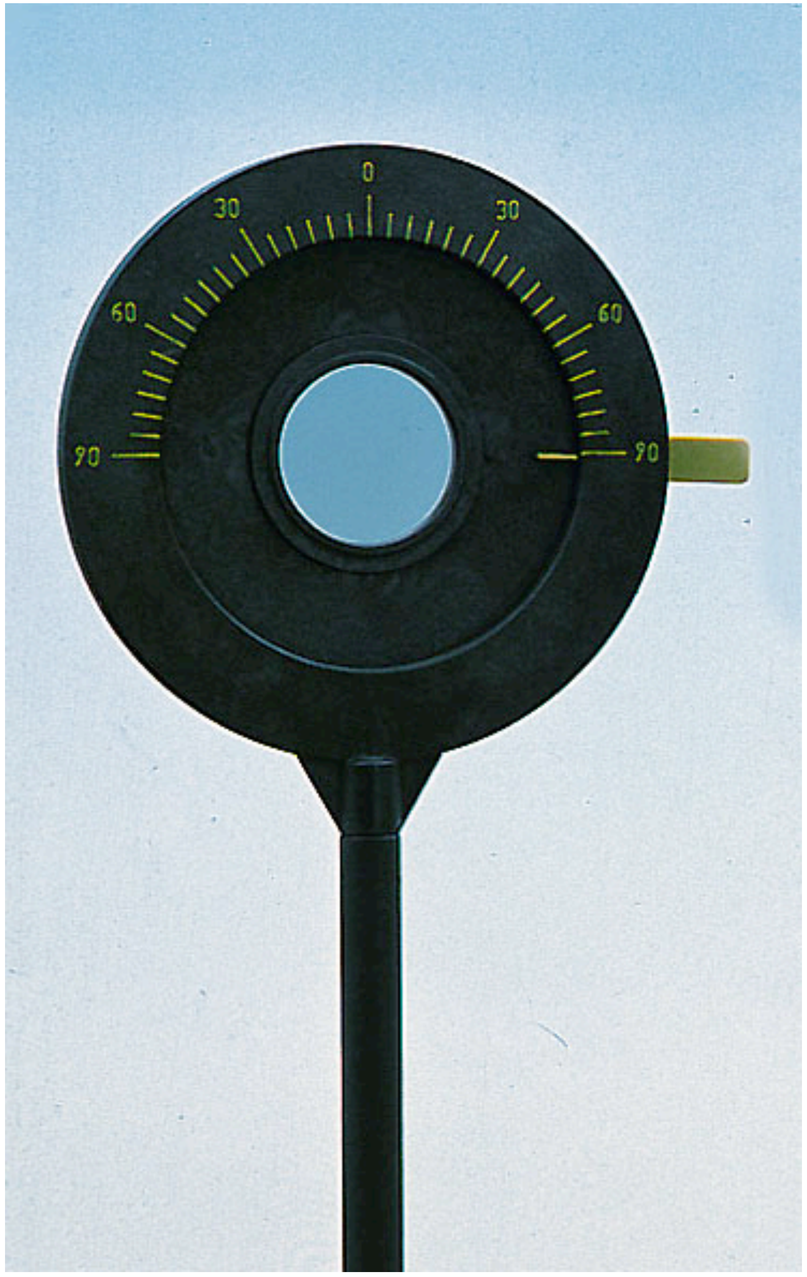




https://www.leybold-shop.fr/

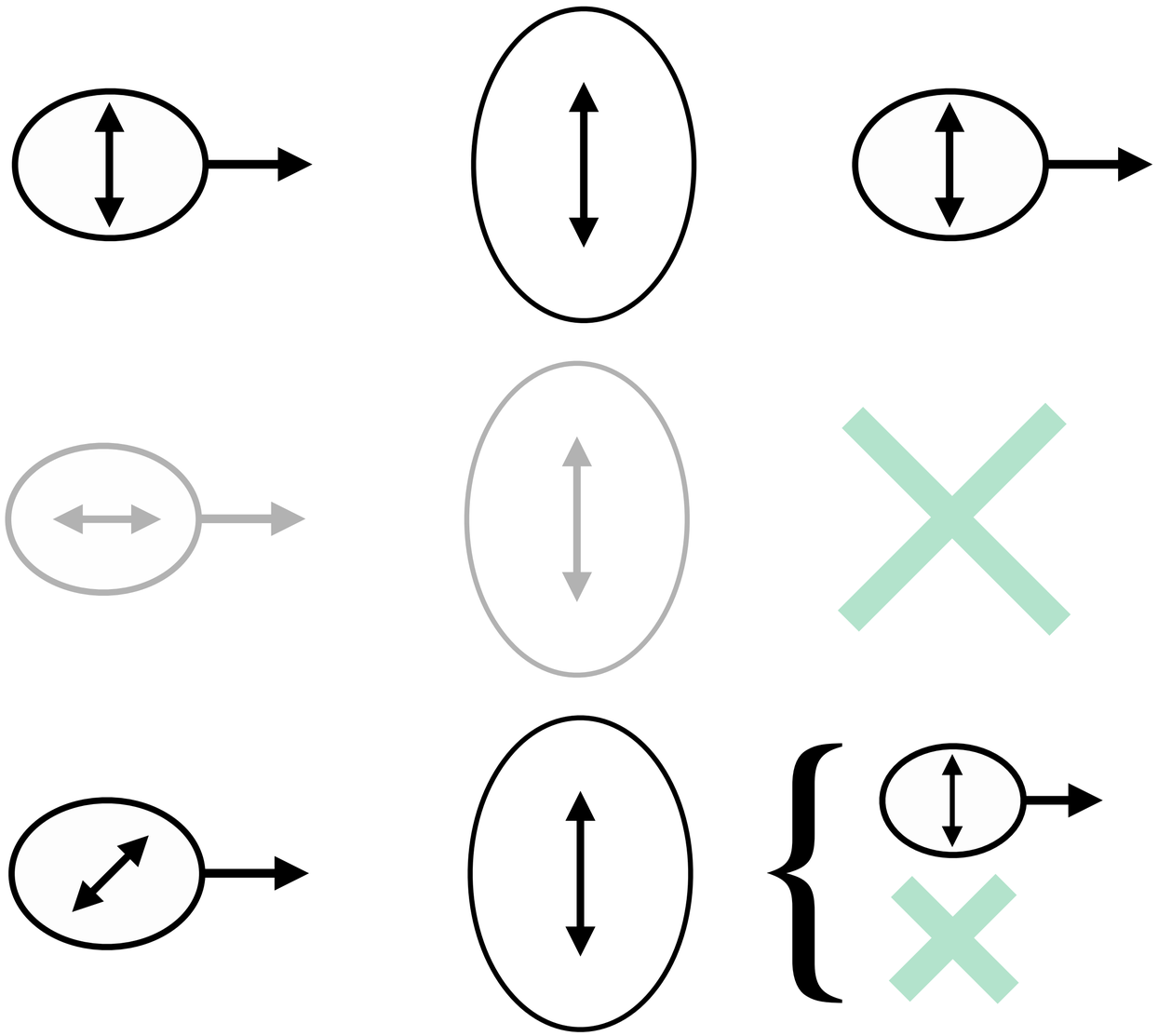
Le polariseur

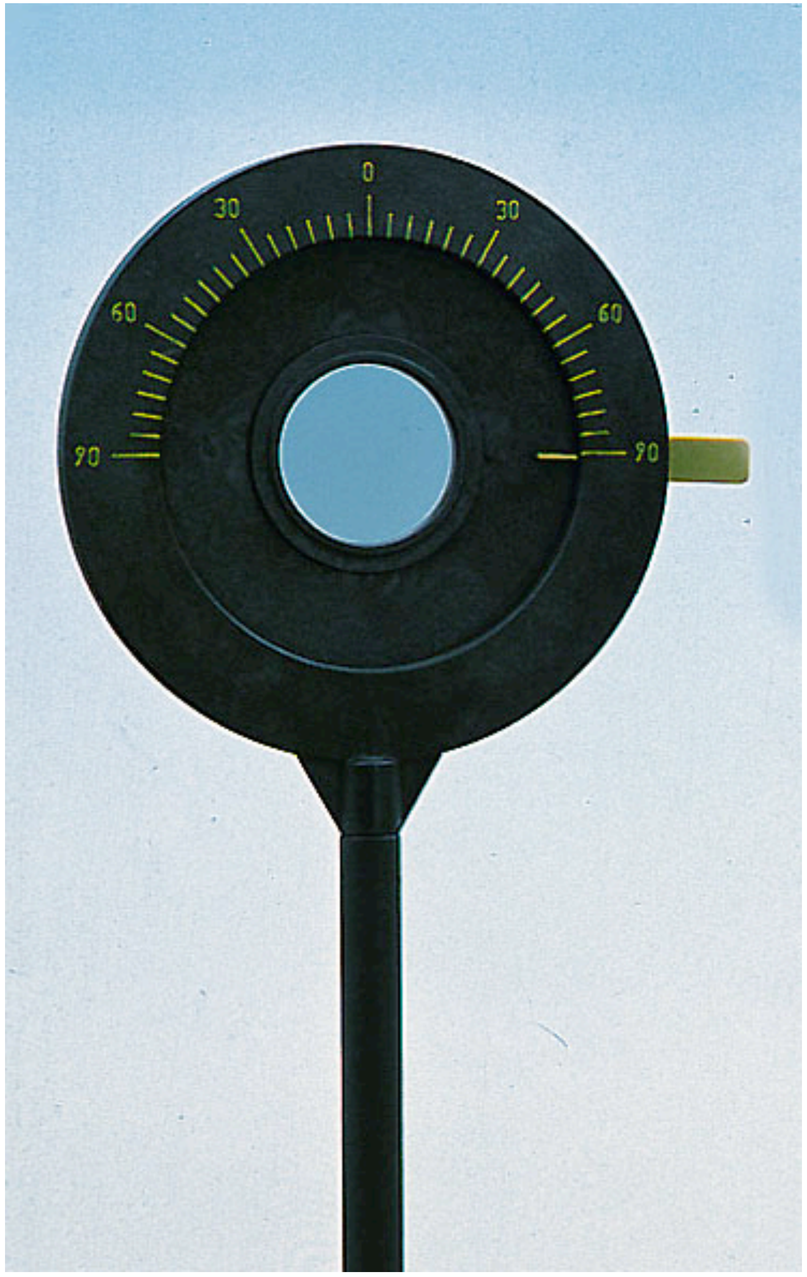




https://www.leybold-shop.fr/

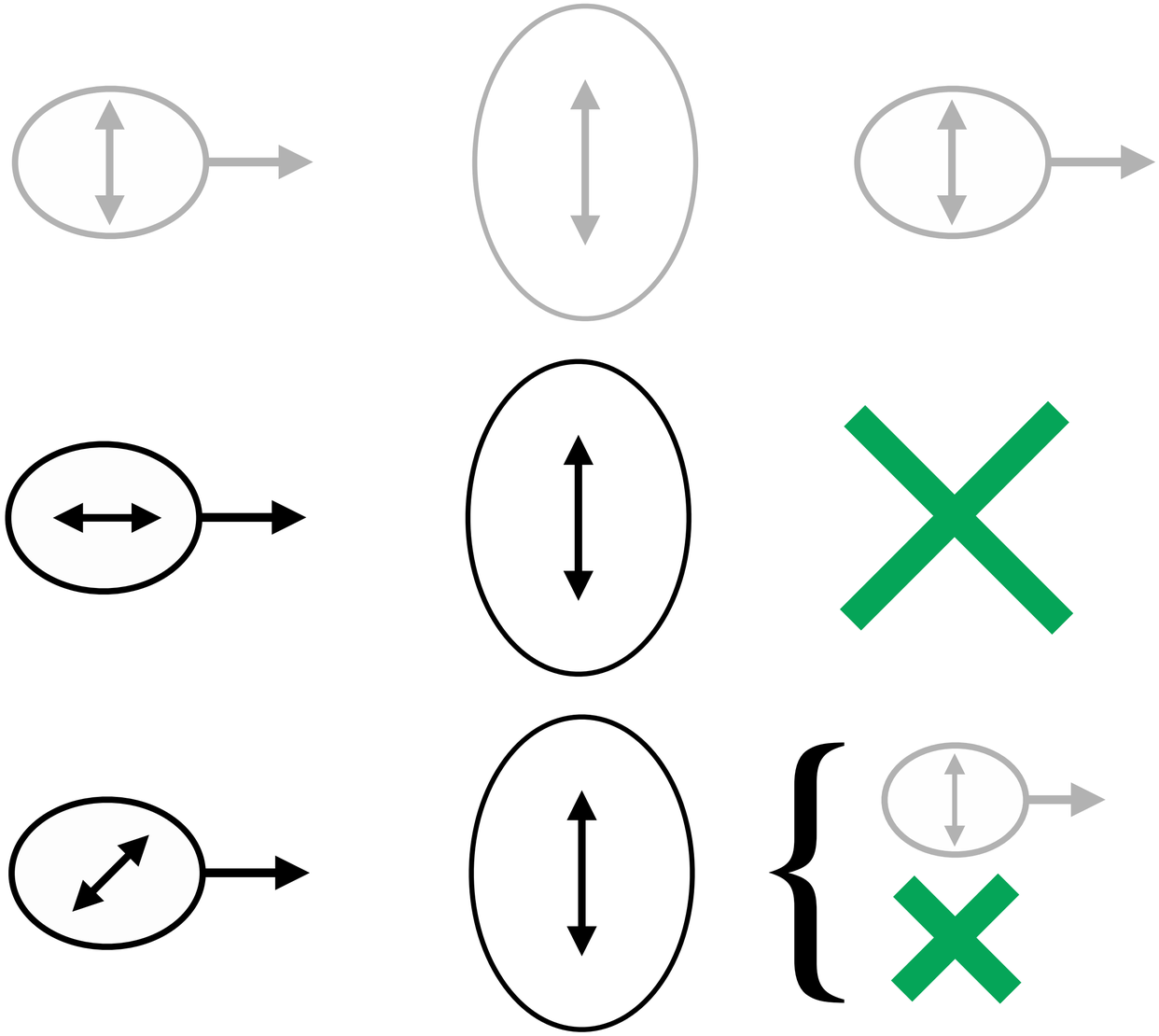
Le polariseur

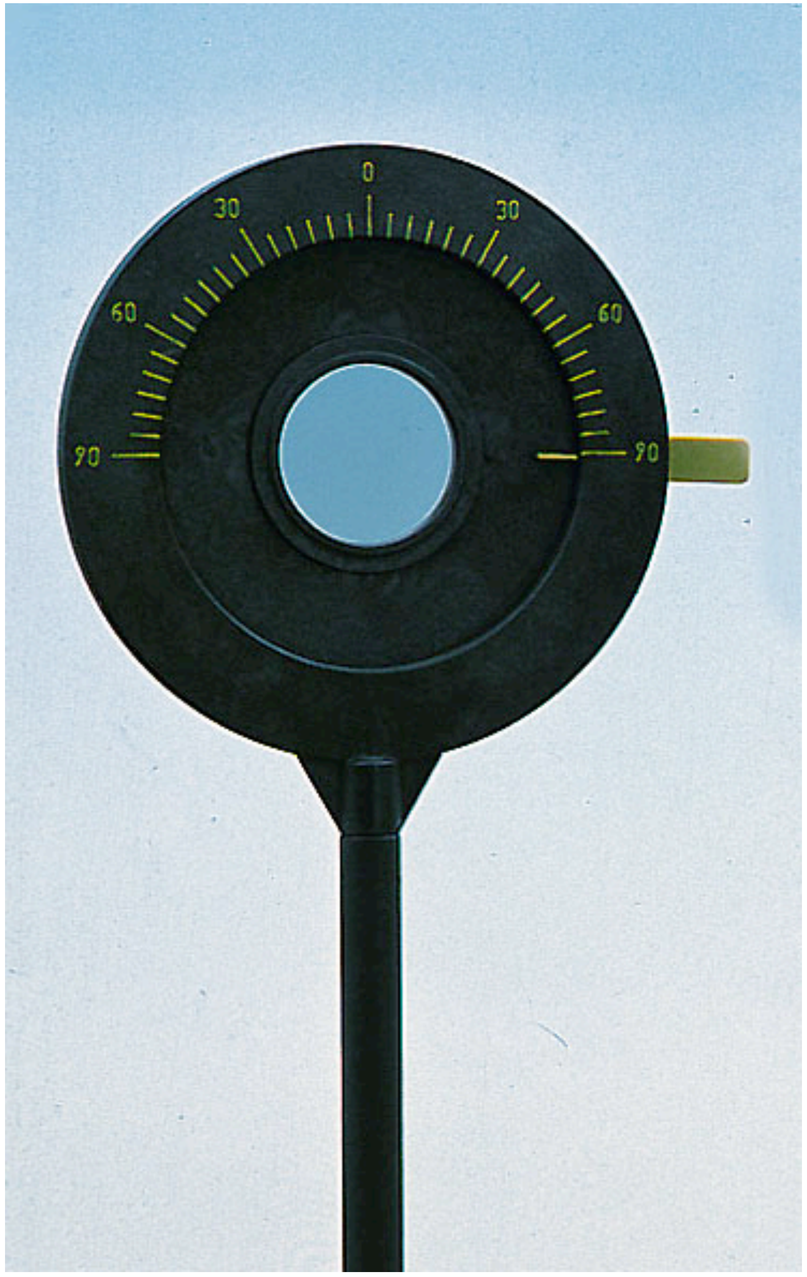




https://www.leybold-shop.fr/

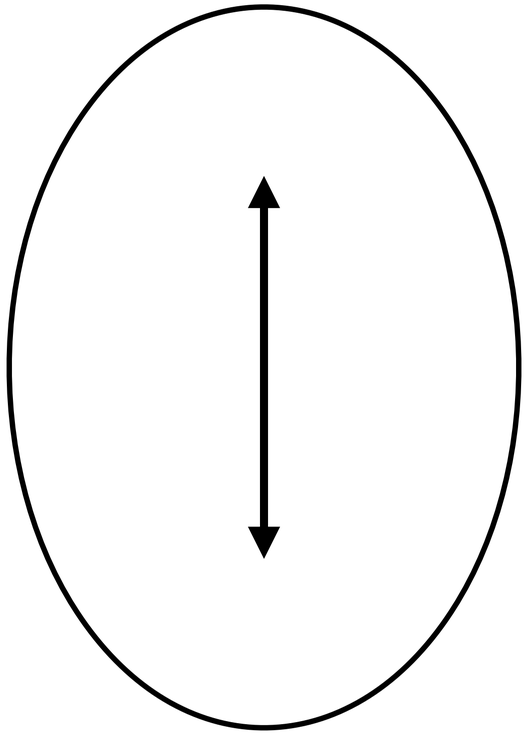
Le polariseur



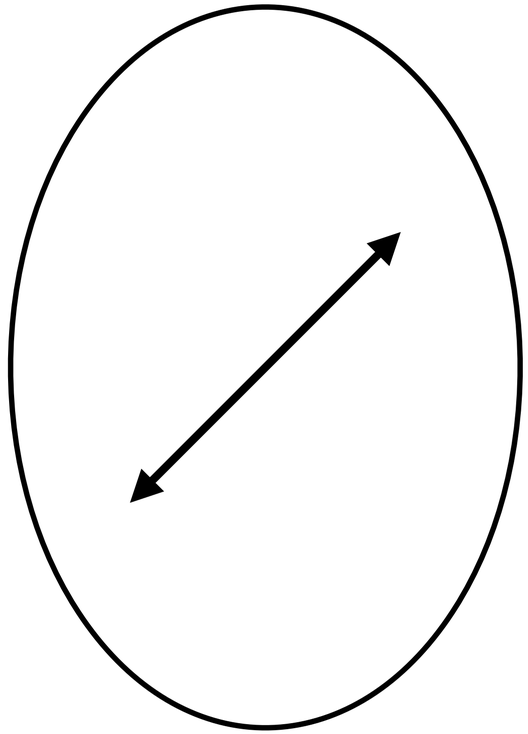


https://www.leybold-shop.fr/

Base de mesure

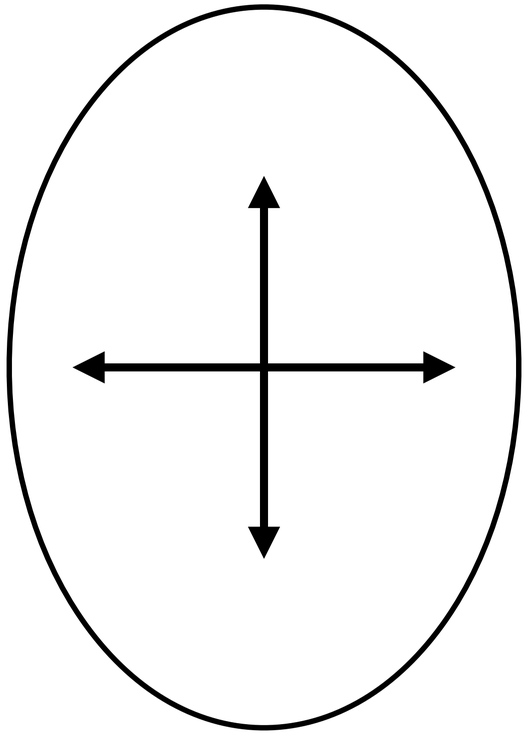


Base Verticale

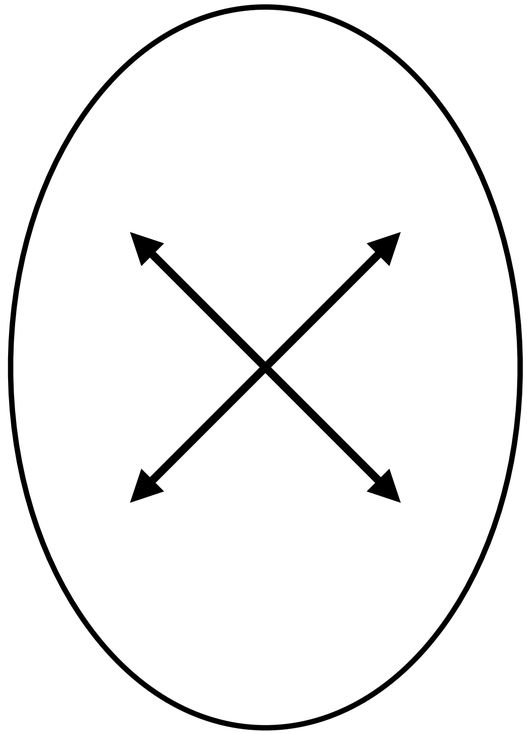


Base Diagonale

Base de mesure

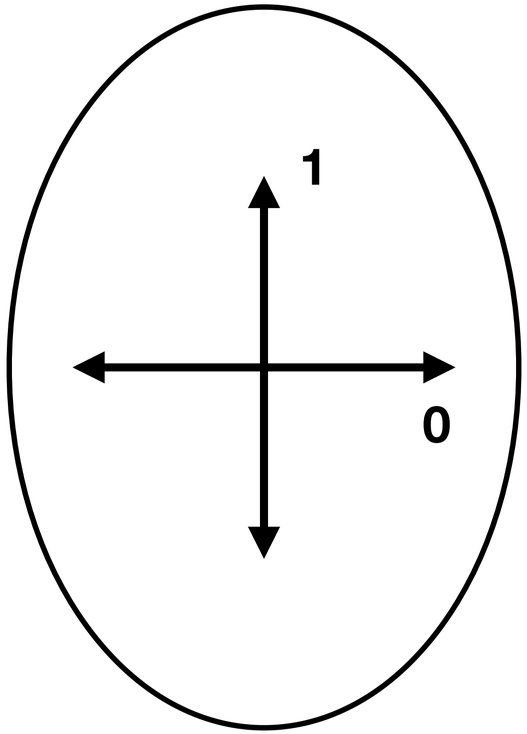


Base Verticale

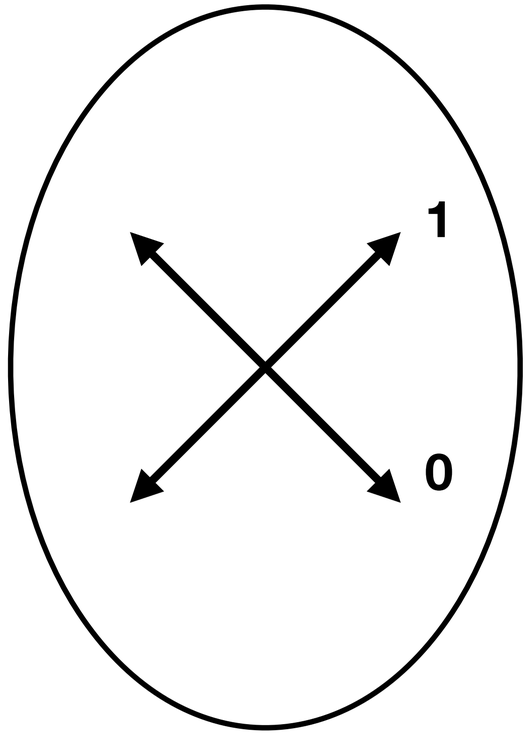


Base Diagonale

Base de mesure

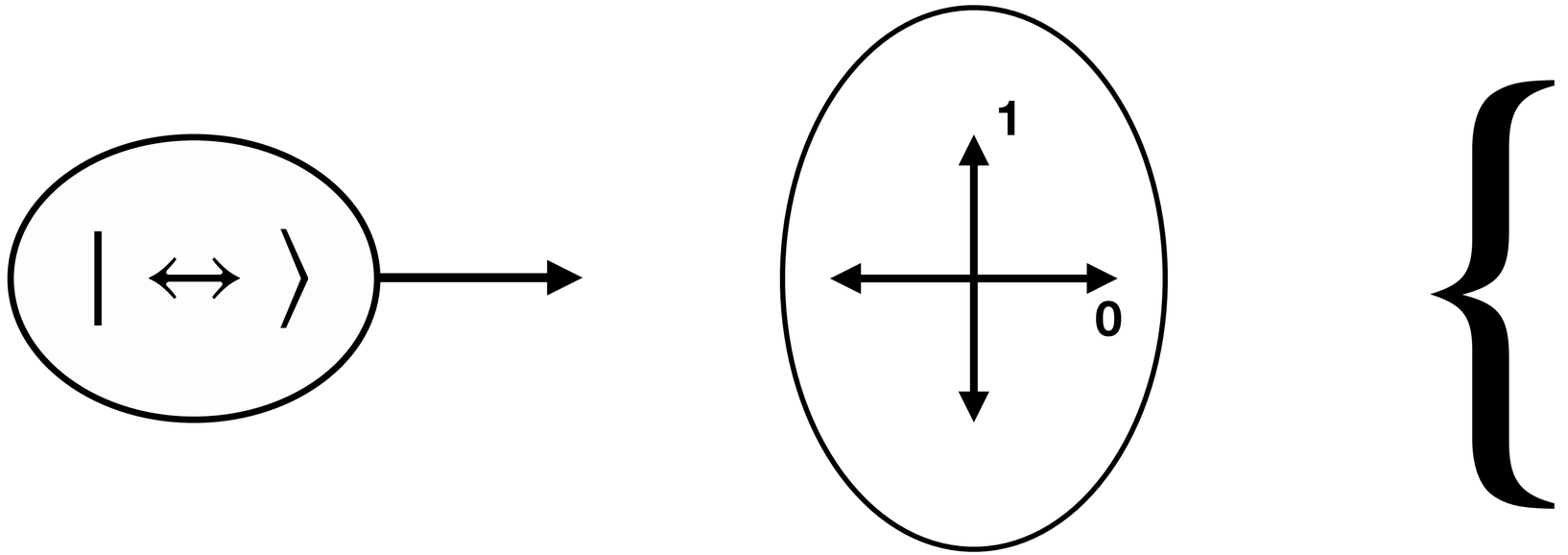


Base Verticale



Base Diagonale

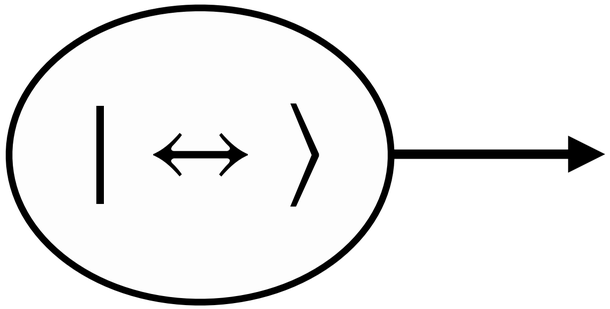
Mesure

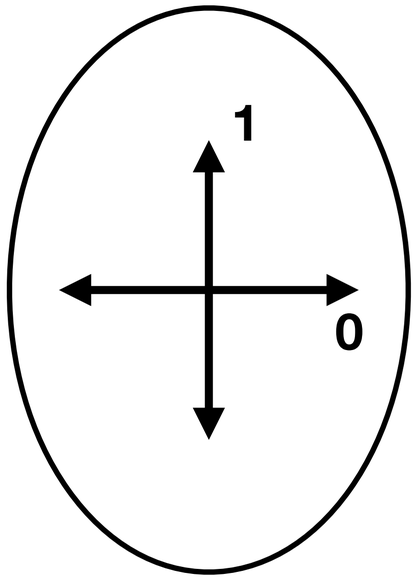


$|90°\rangle \equiv |\updownarrow\rangle$

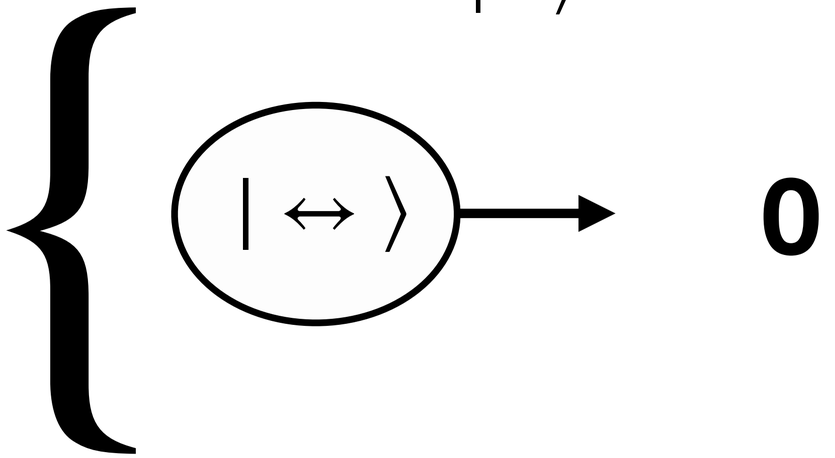
$|0°\rangle \equiv |\leftrightarrow\rangle$

Mesure





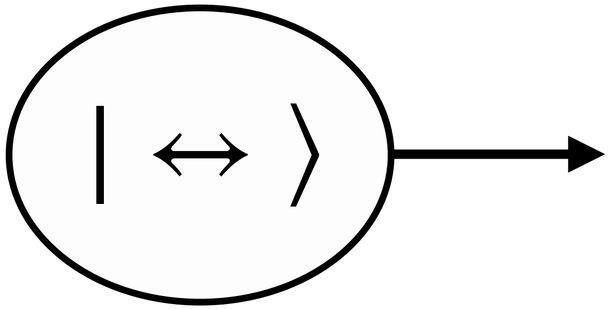
$$P_{|\leftrightarrow\rangle} = 1$$



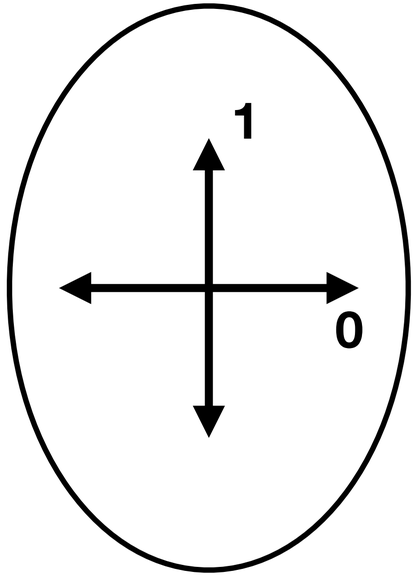
$|90°\rangle \equiv |\updownarrow\rangle$

$|0°\rangle \equiv |\leftrightarrow\rangle$

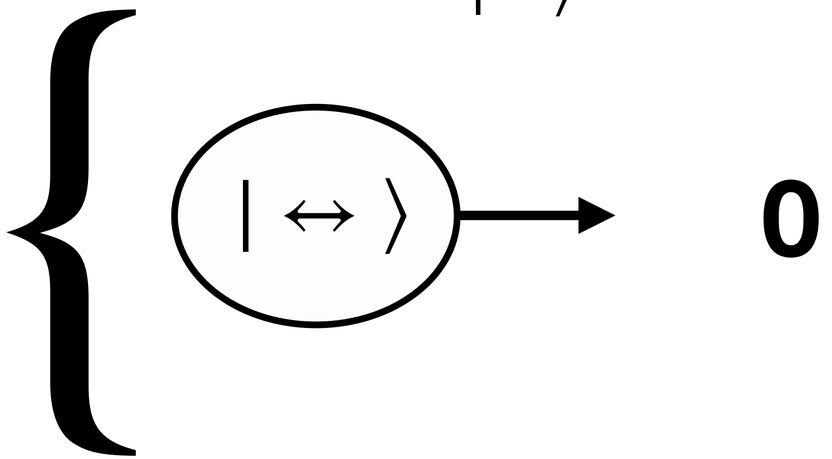
Mesure



$1|\leftrightarrow\rangle + 0|\updownarrow\rangle$



$P_{|\leftrightarrow\rangle} = 1$



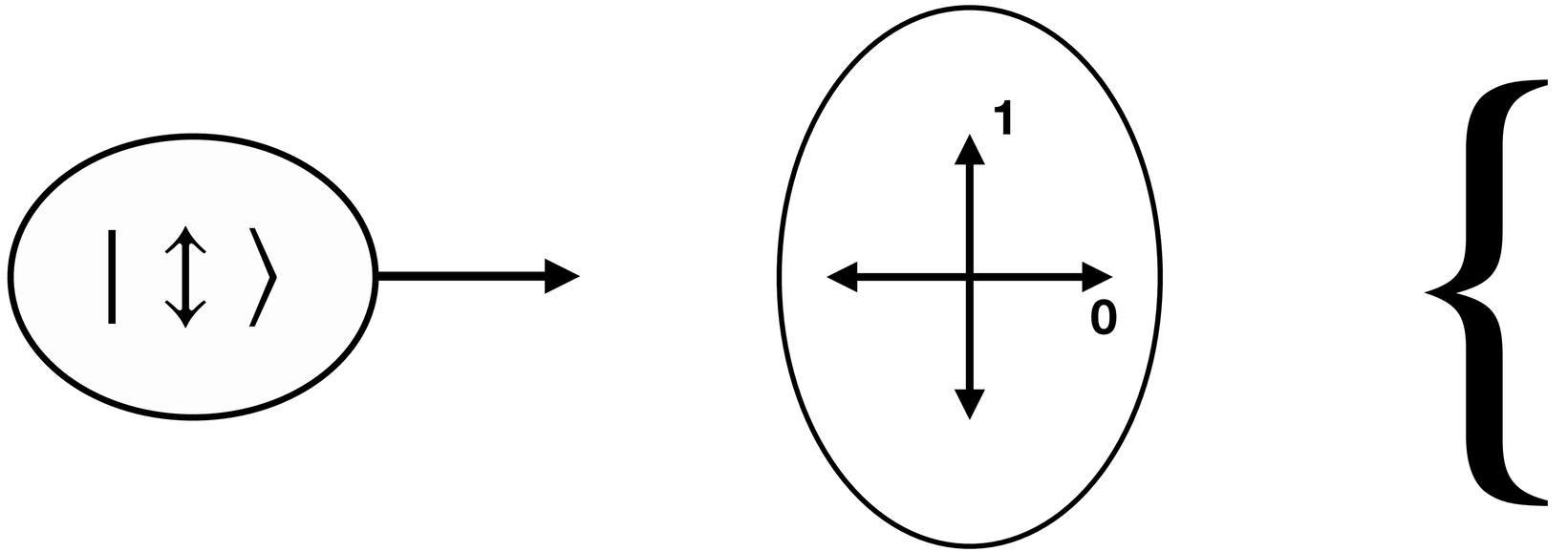
$|90°\rangle \equiv |\updownarrow\rangle$

$|0°\rangle \equiv |\leftrightarrow\rangle$

$P_{|\leftrightarrow\rangle} = |1|^2$

$P_{|\updownarrow\rangle} = |0|^2$

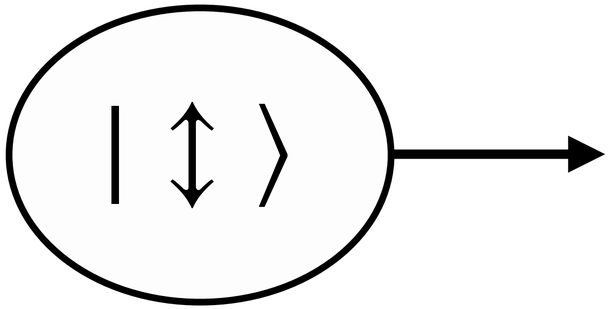
Mesure

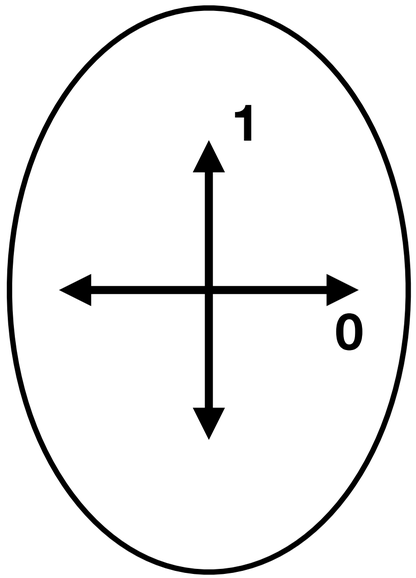


$|90°\rangle \equiv |\updownarrow\rangle$

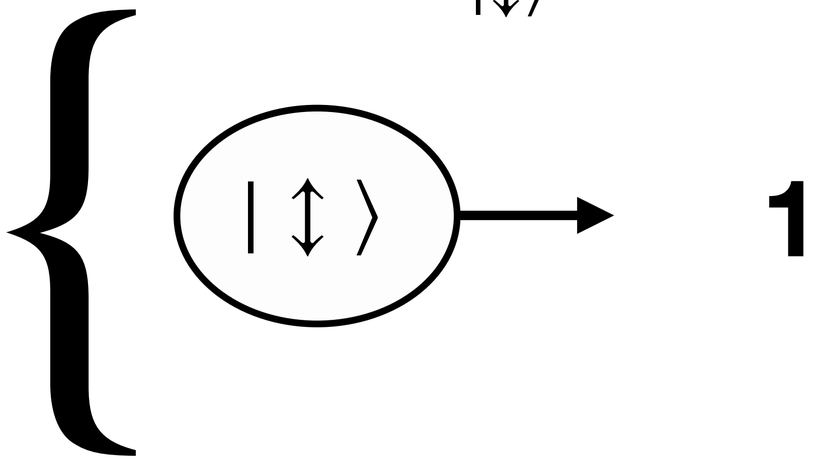
$|0°\rangle \equiv |\leftrightarrow\rangle$

Mesure



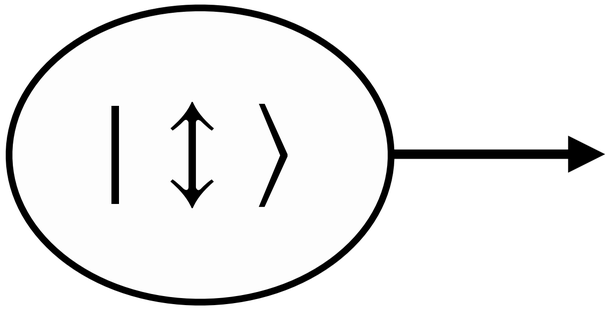


$$P_{|\updownarrow\rangle} = 1$$

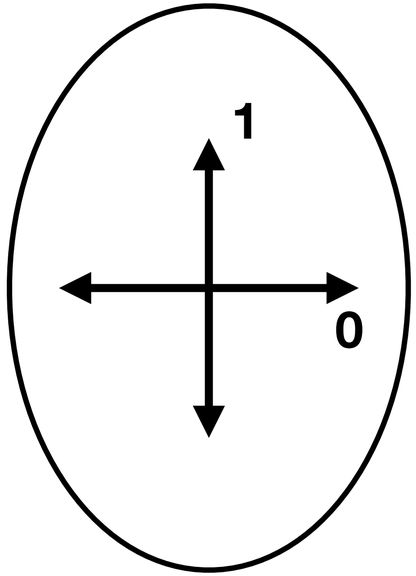


$$|90°\rangle \equiv |\updownarrow\rangle$$
$$|0°\rangle \equiv |\leftrightarrow\rangle$$

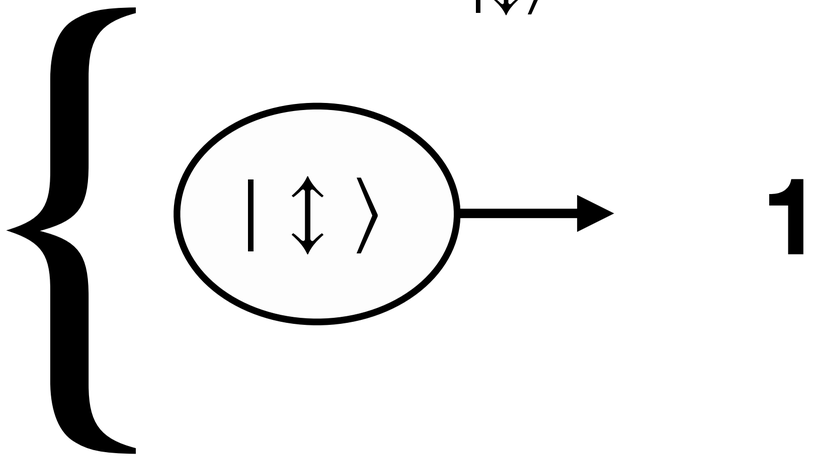
Mesure



$0\,|\leftrightarrow\rangle + 1\,|\updownarrow\rangle$



$P_{|\updownarrow\rangle} = 1$

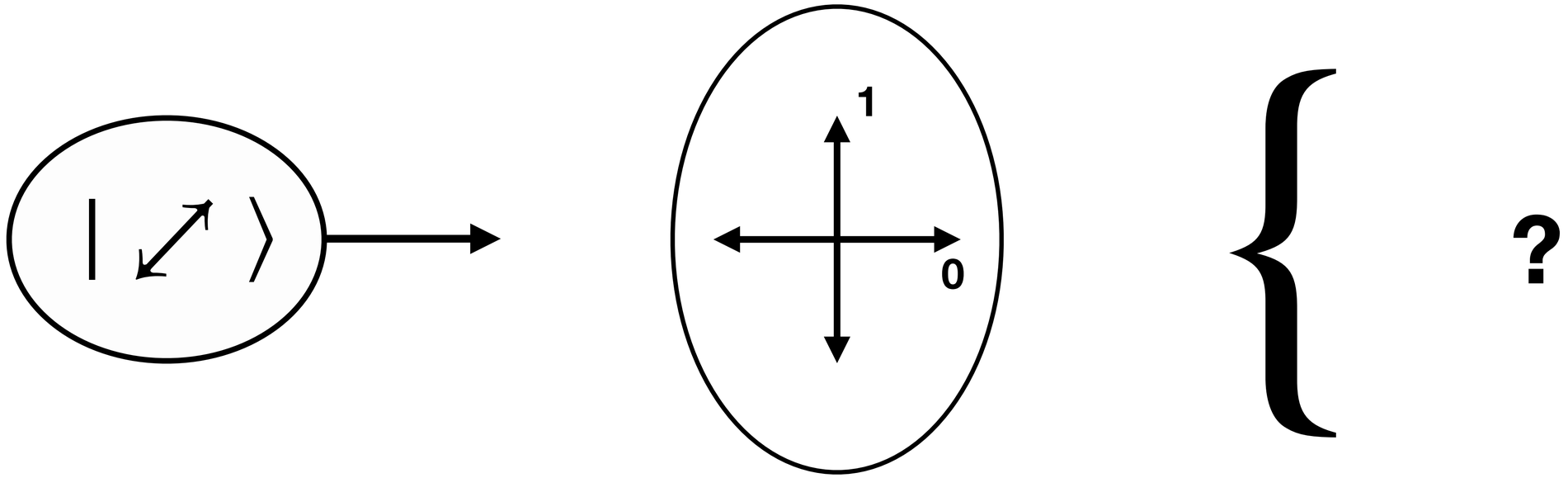


$|90°\rangle \equiv |\updownarrow\rangle$

$|0°\rangle \equiv |\leftrightarrow\rangle$

$P_{|\leftrightarrow\rangle} = |0|^2 \quad P_{|\updownarrow\rangle} = |1|^2$

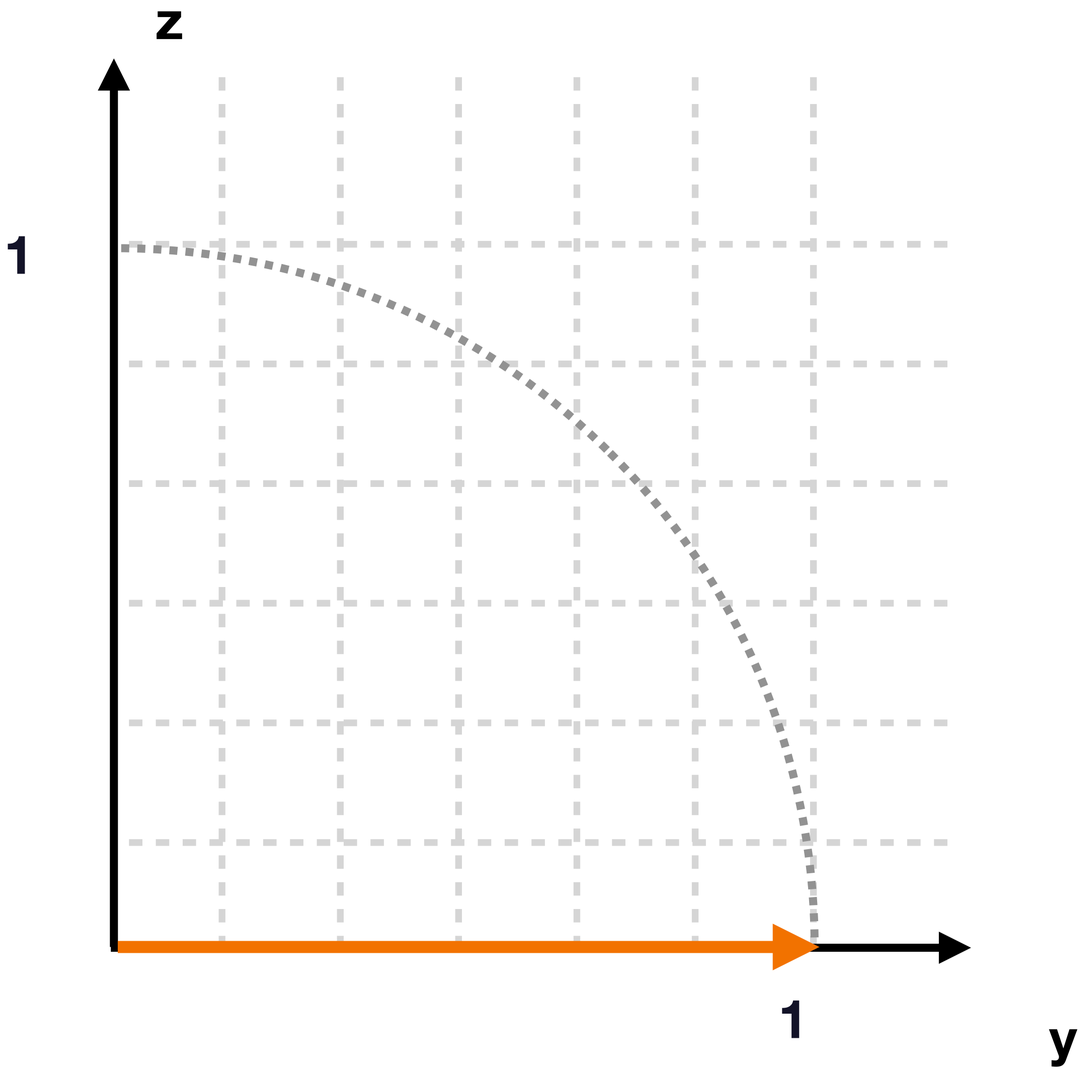
Mesure



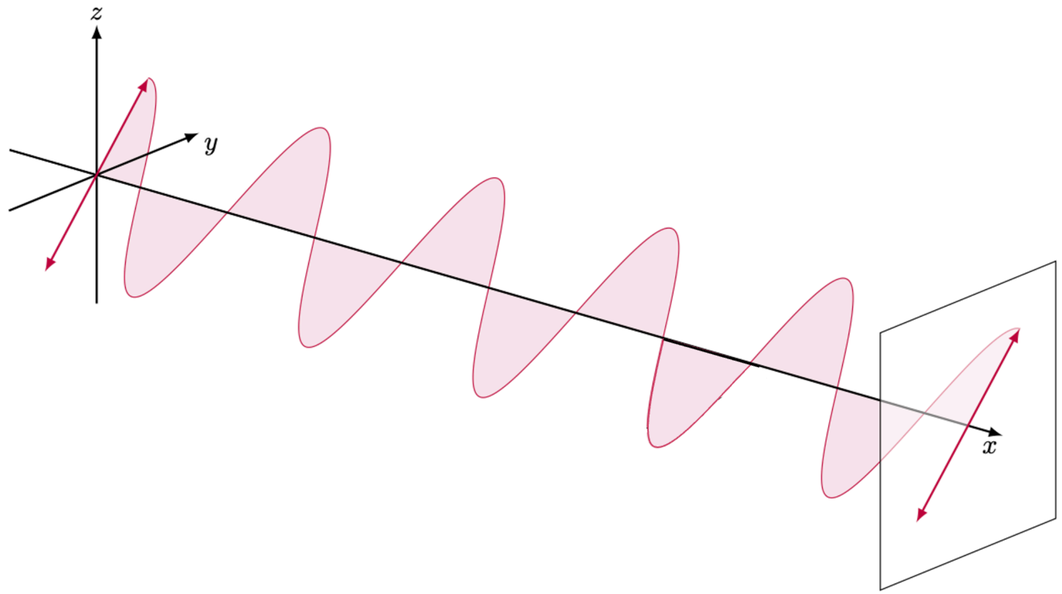
$|45°\rangle \equiv |\ \nearrow\ \rangle$

$|135°\rangle \equiv |\ \nwarrow\!\!\searrow\ \rangle$

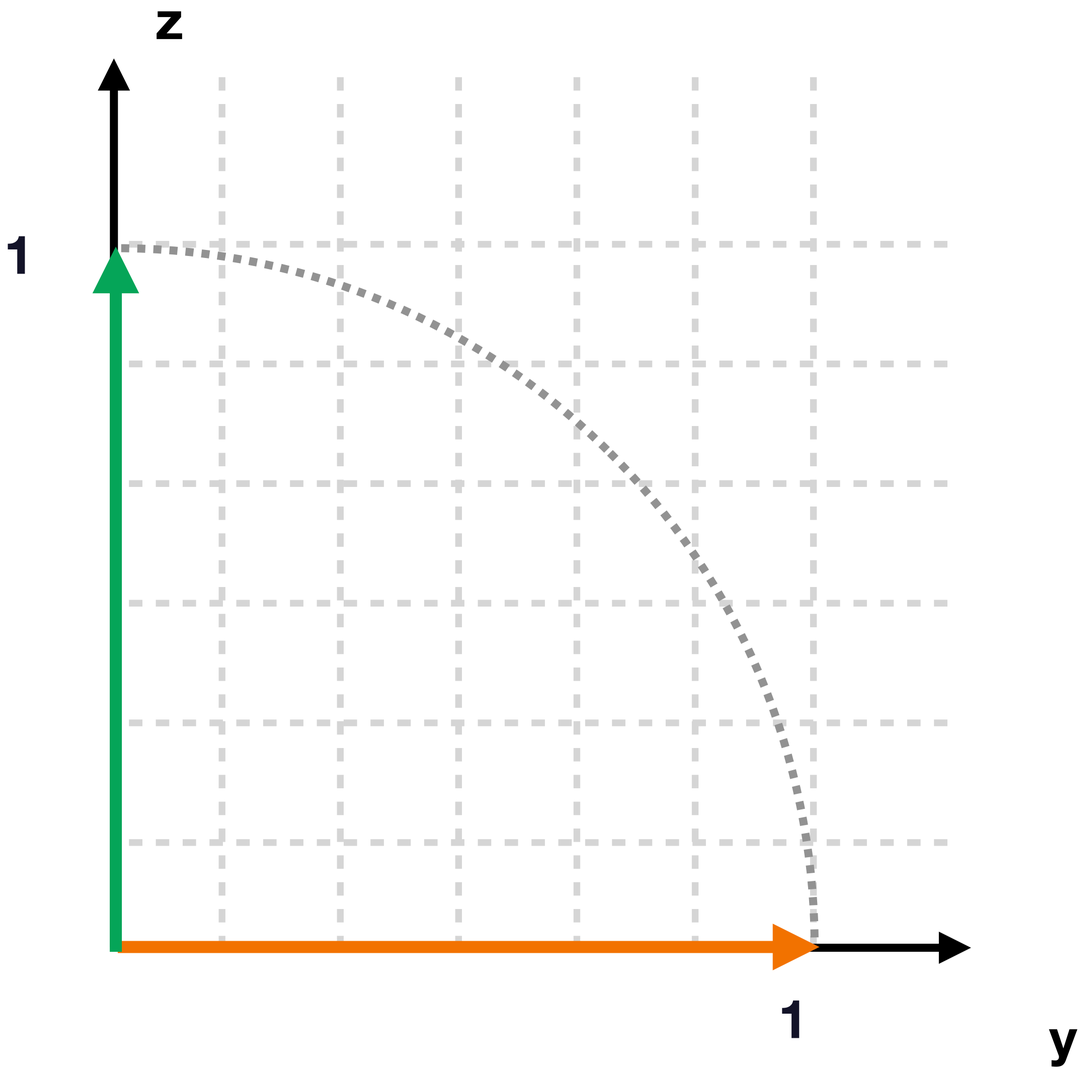
Mesure



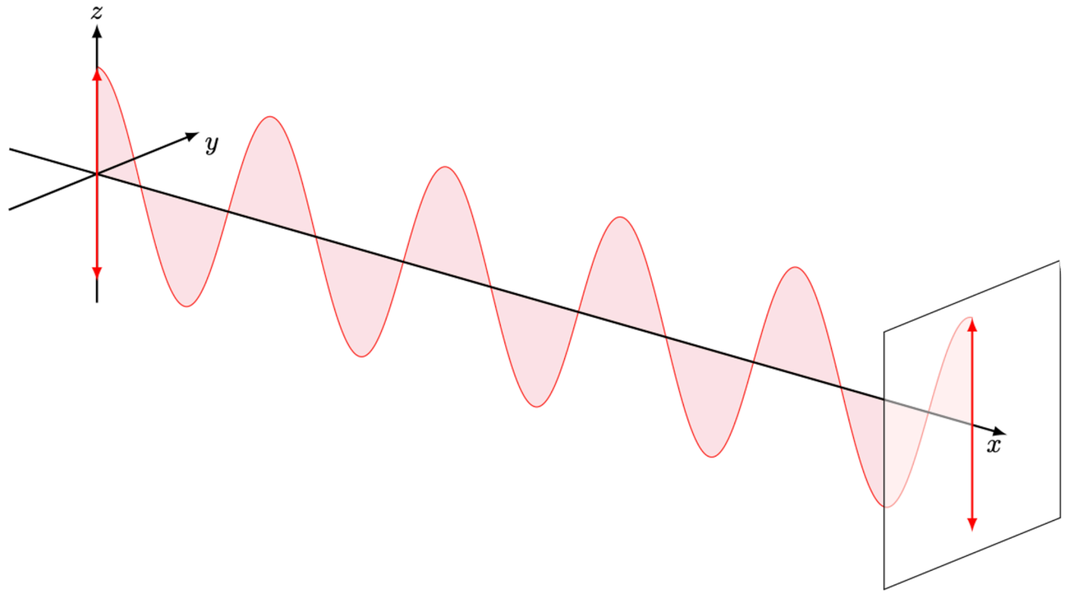
$$|\leftrightarrow\rangle$$



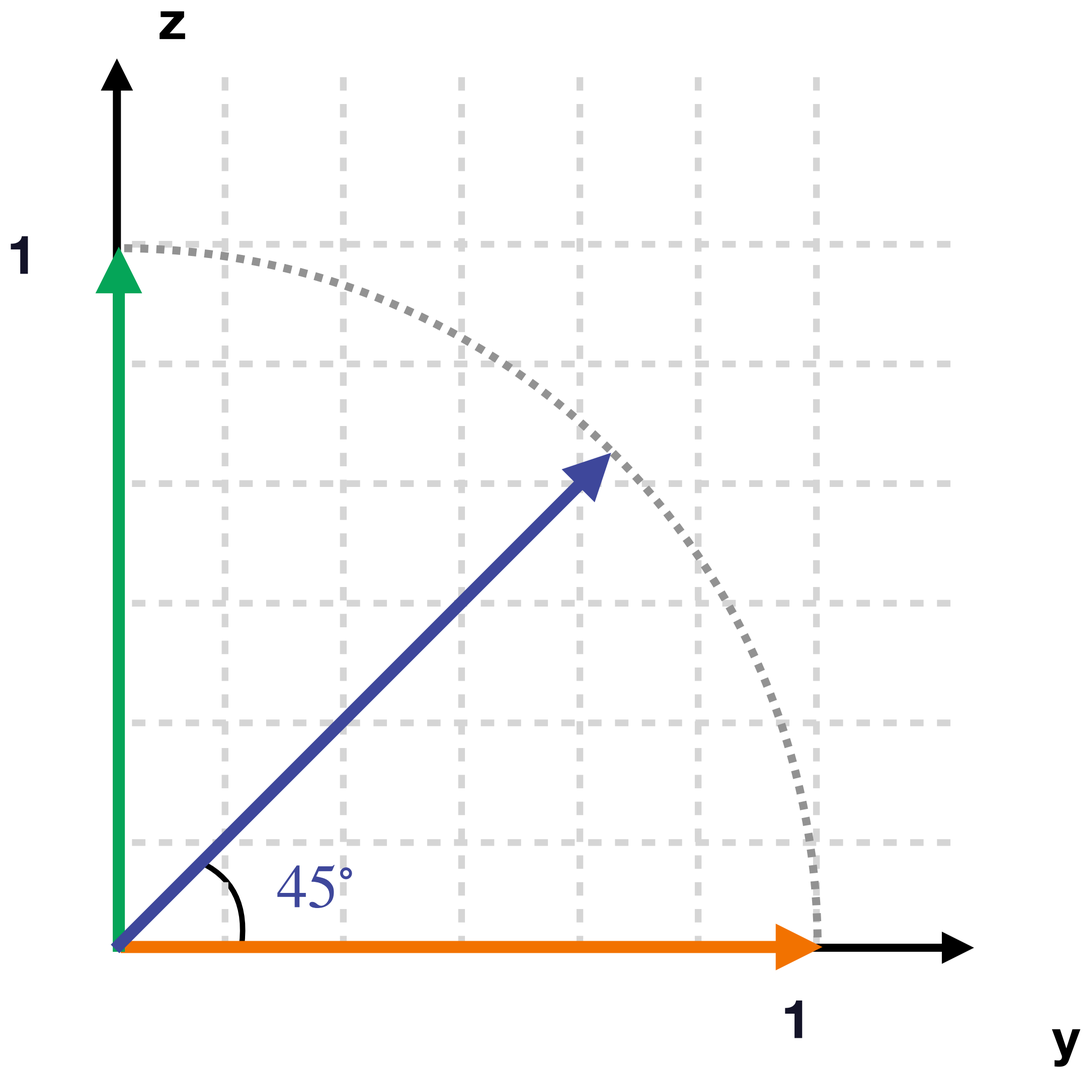
Mesure



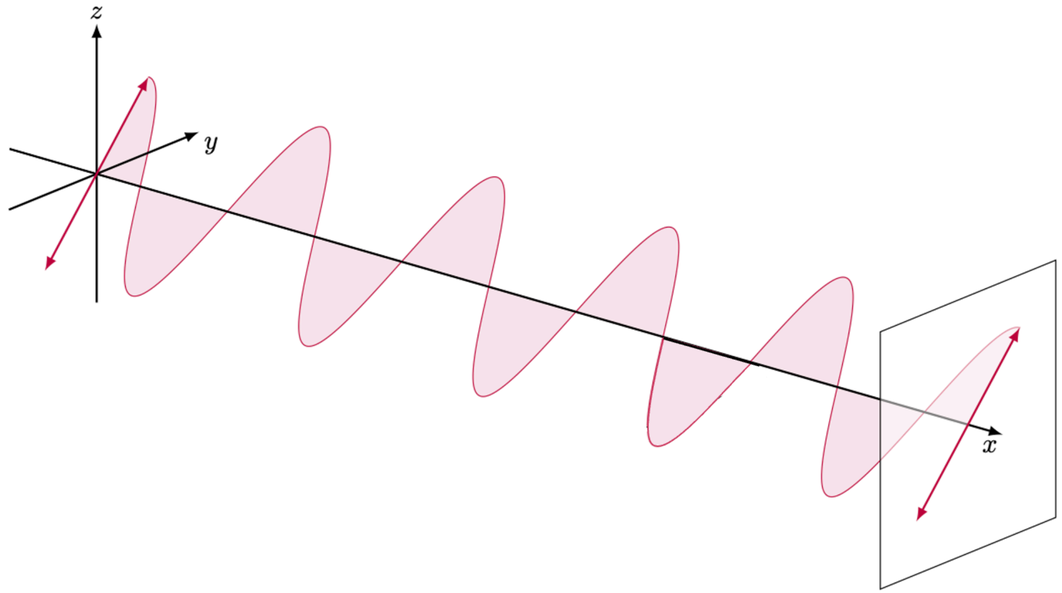
$|\leftrightarrow\rangle$ $|\updownarrow\rangle$



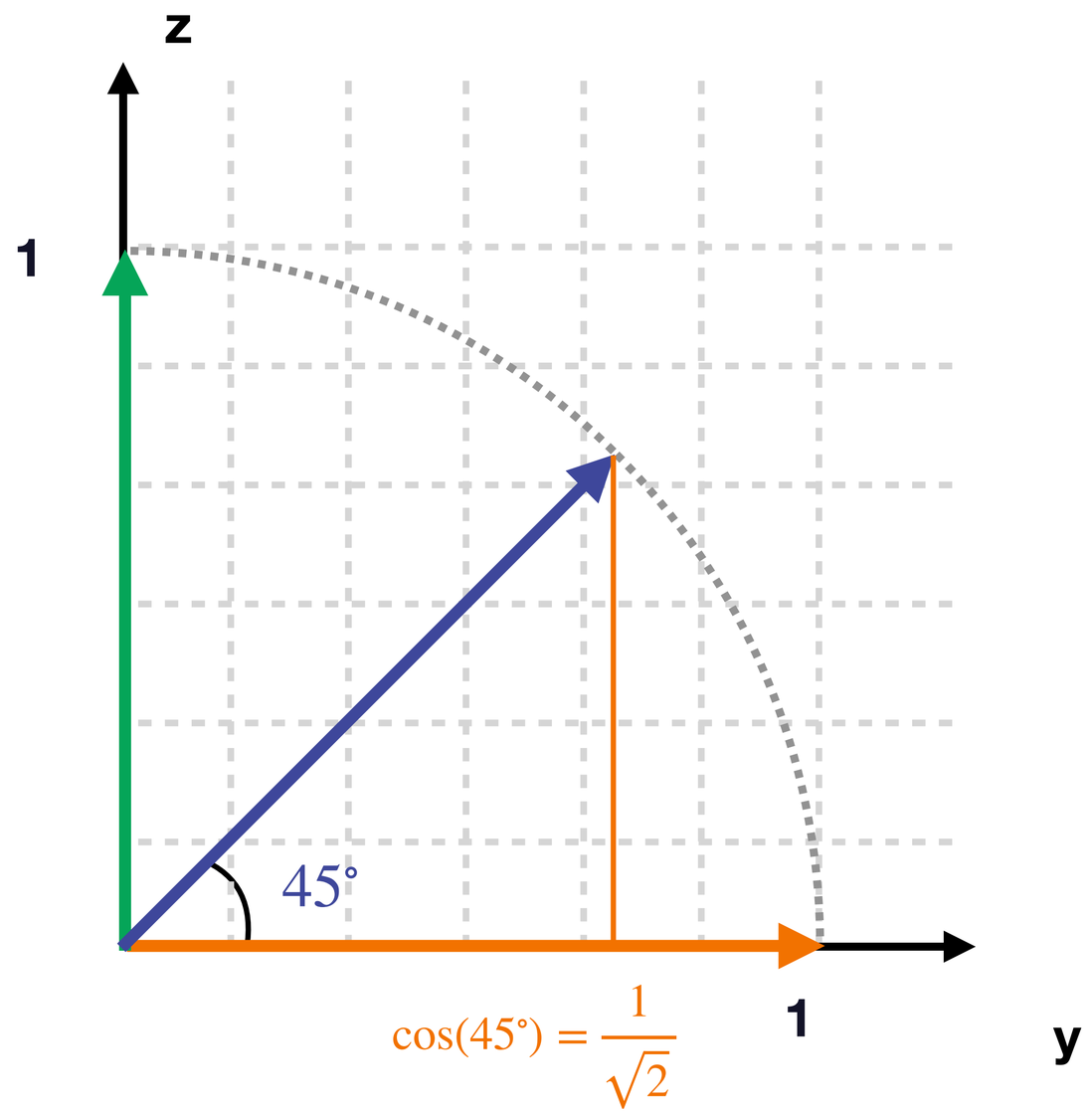
Mesure



$$|\leftrightarrow\rangle \qquad |\updownarrow\rangle \qquad |\nearrow\rangle$$



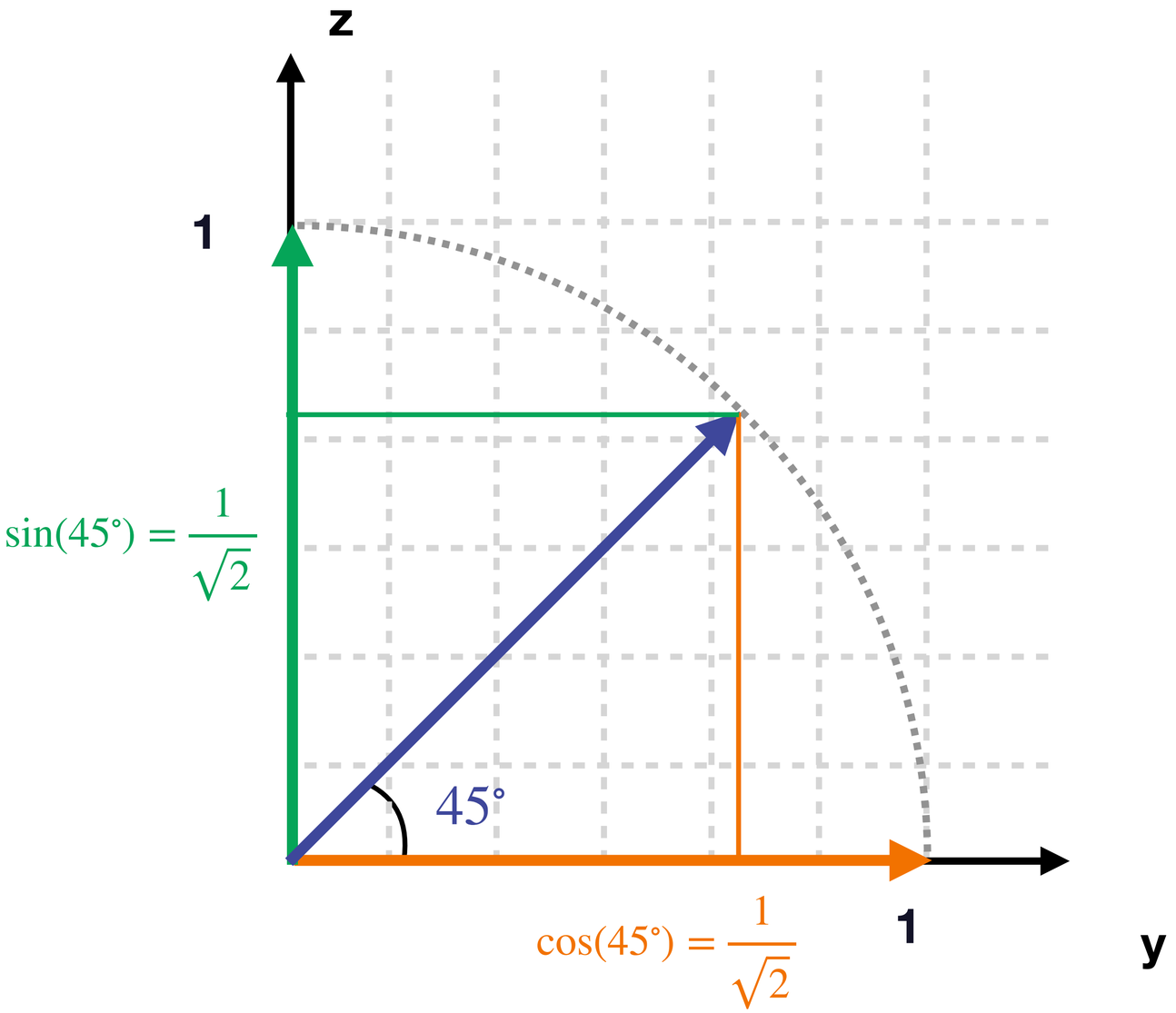
Mesure



$$|\leftrightarrow\rangle \quad |\updownarrow\rangle \quad |\nearrow\swarrow\rangle$$

$$|\nearrow\swarrow\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle +$$

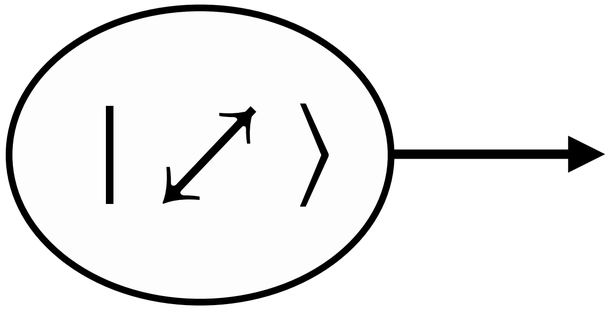
Mesure

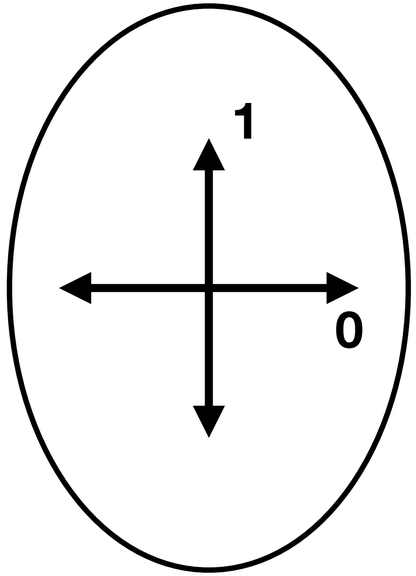


$$|\leftrightarrow\rangle \quad |\updownarrow\rangle \quad |\nearrow\swarrow\rangle$$

$$|\nearrow\swarrow\rangle = \frac{1}{\sqrt{2}}|\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\rangle$$

Mesure





?

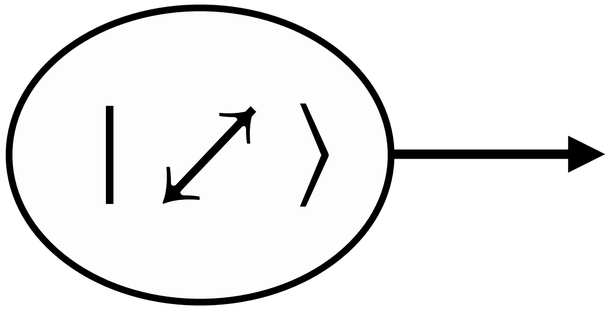
$$\frac{1}{\sqrt{2}}|\leftrightarrow\rangle + \frac{1}{\sqrt{2}}|\updownarrow\rangle$$

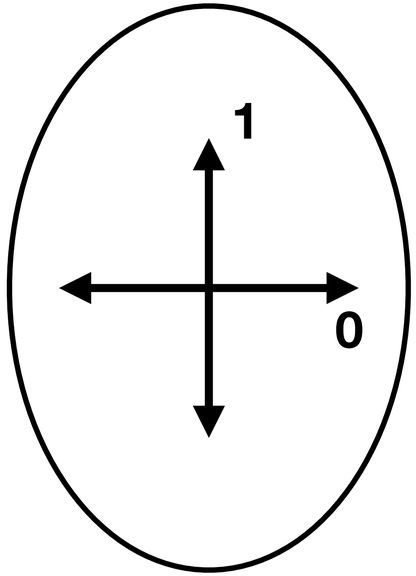
$|45°\rangle \equiv |\ \swarrow\ \rangle$

$|135°\rangle \equiv |\ \nwarrow\ \rangle$

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

Mesure



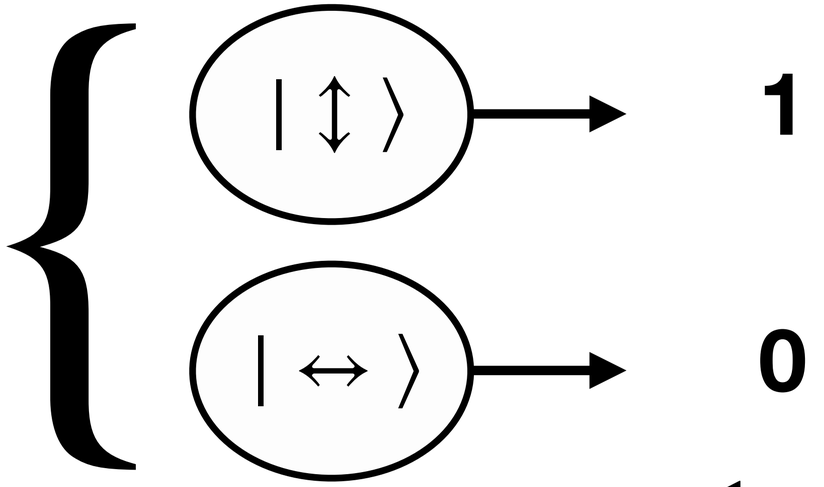


$$\frac{1}{\sqrt{2}}|\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\rangle$$

$$|45°\rangle \equiv |\swarrow\rangle$$

$$|135°\rangle \equiv |\searrow\rangle$$

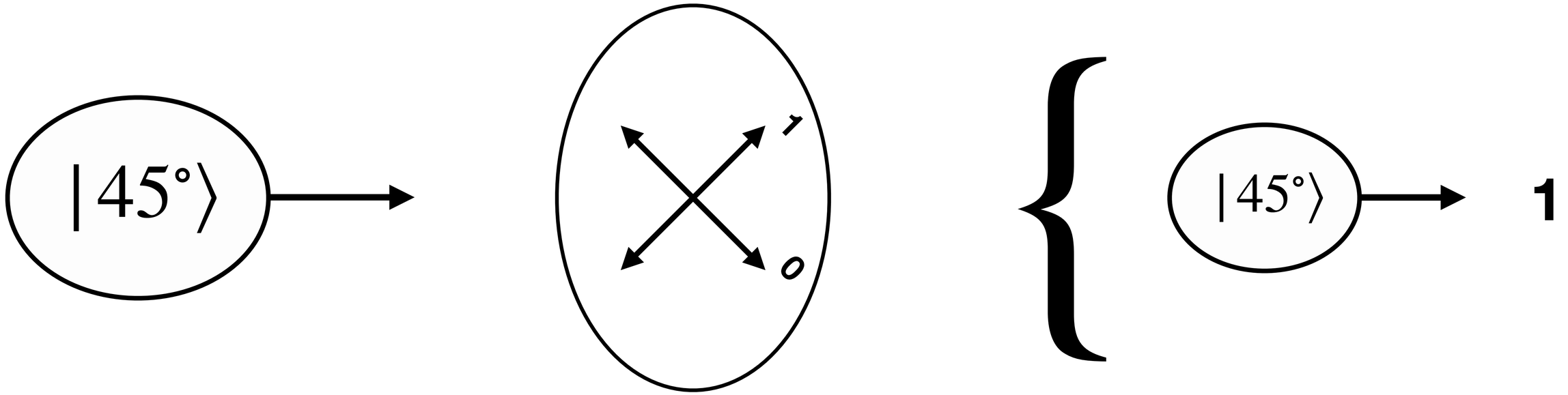
$$P_{|\updownarrow\rangle}=\frac{1}{2}$$



$$P_{|\leftrightarrow\rangle}=\frac{1}{2}$$

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

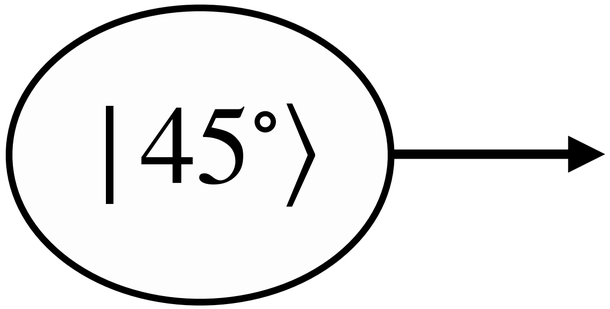
Mesure



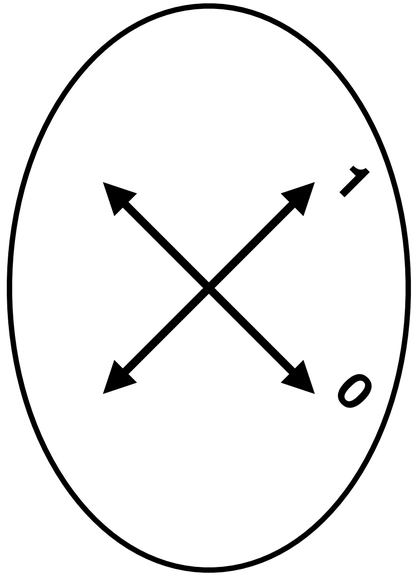
$|45°\rangle \equiv |\ \nearrow\ \rangle$

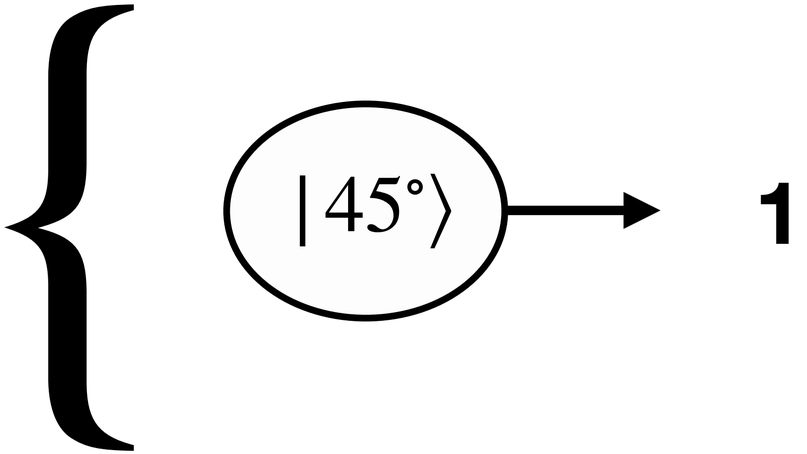
$|135°\rangle \equiv |\ \nwarrow\ \rangle$

Mesure



$$1|45°\rangle + 0|135°\rangle$$



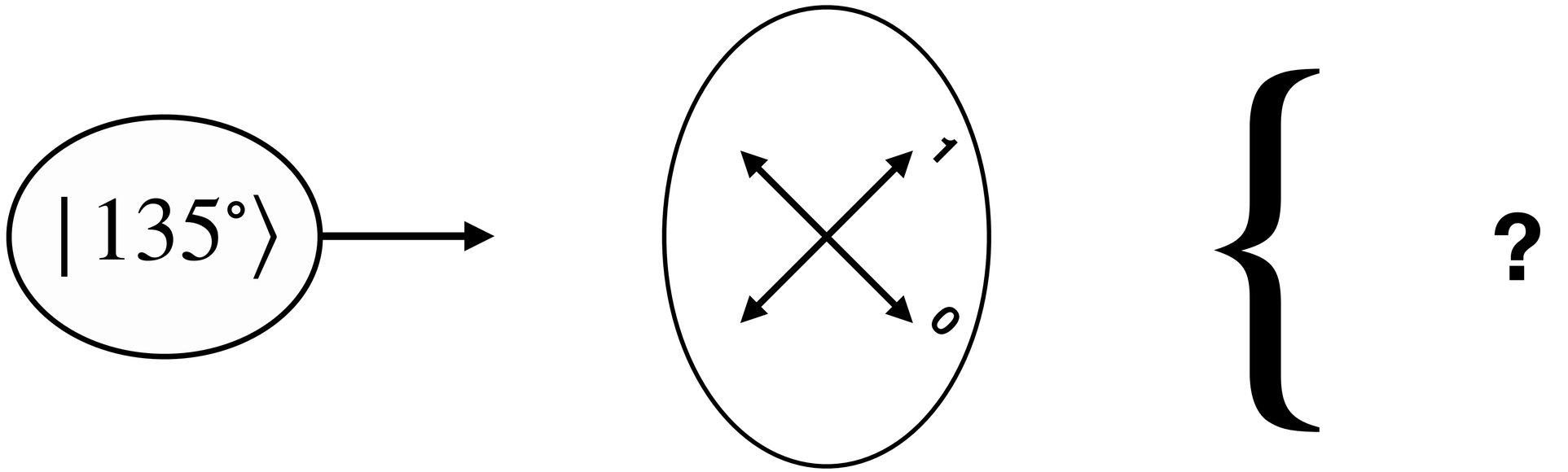


$|45°\rangle \equiv |\ \nearrow\ \rangle$

$|135°\rangle \equiv |\ \nwarrow\ \rangle$

$$P_{|45°\rangle} = |1|^2 \qquad P_{|135°\rangle} = |0|^2$$

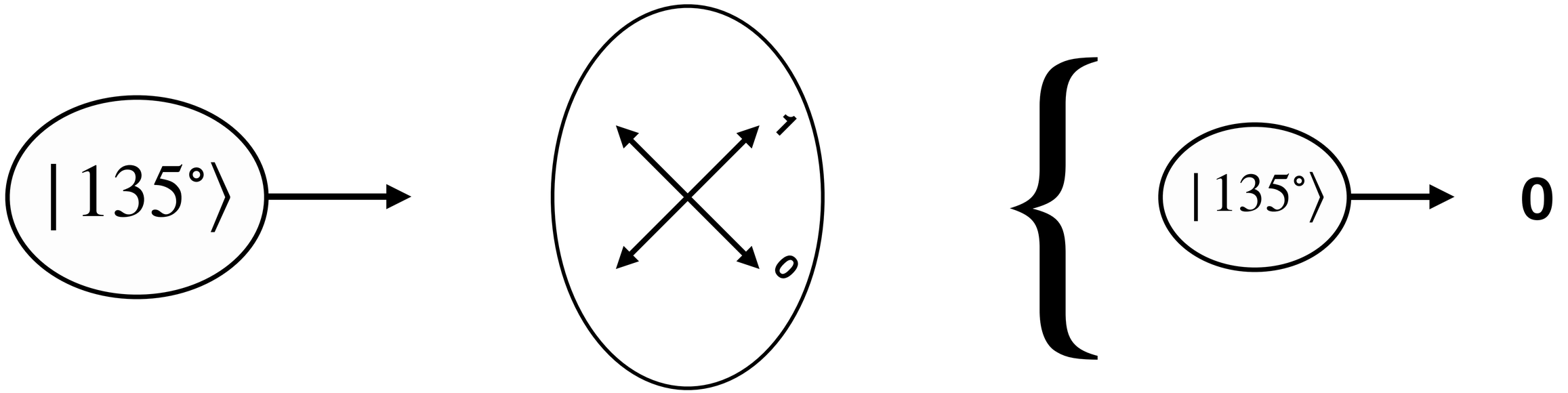
Mesure



$|45°\rangle \equiv |\ \nearrow\ \rangle$

$|135°\rangle \equiv |\ \nwarrow\ \rangle$

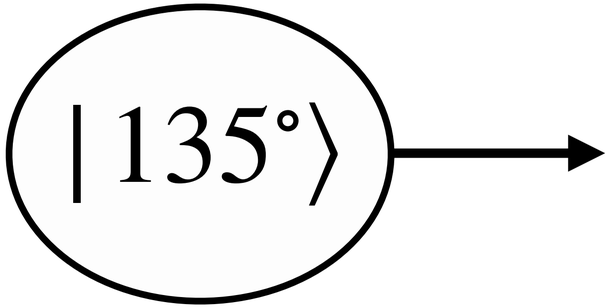
Mesure



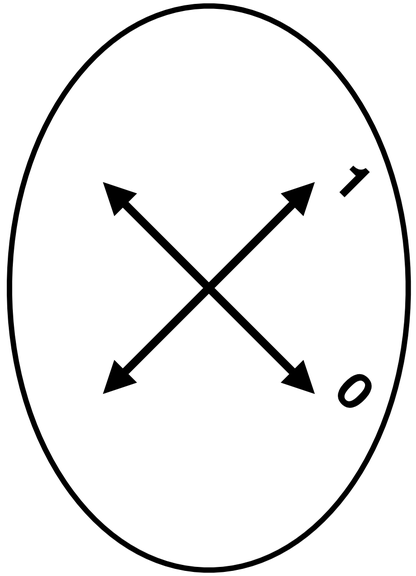
$|45°\rangle \equiv |\ \nearrow\ \rangle$

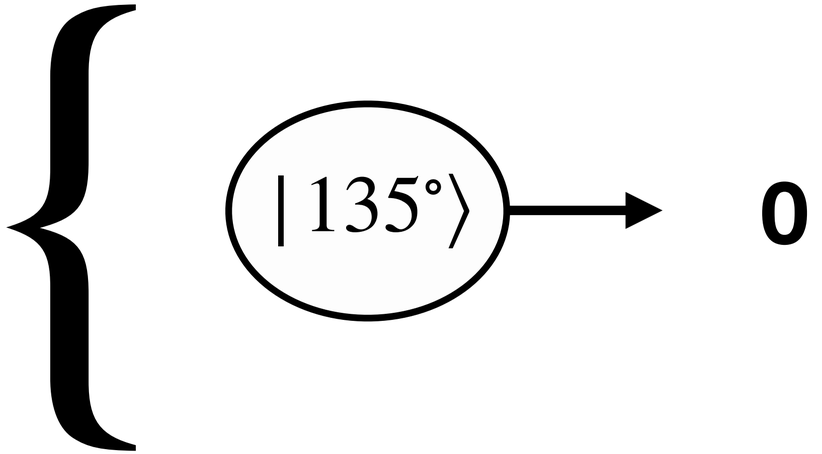
$|135°\rangle \equiv |\ \nwarrow\ \rangle$

Mesure



$1|0°\rangle + 0|90°\rangle$





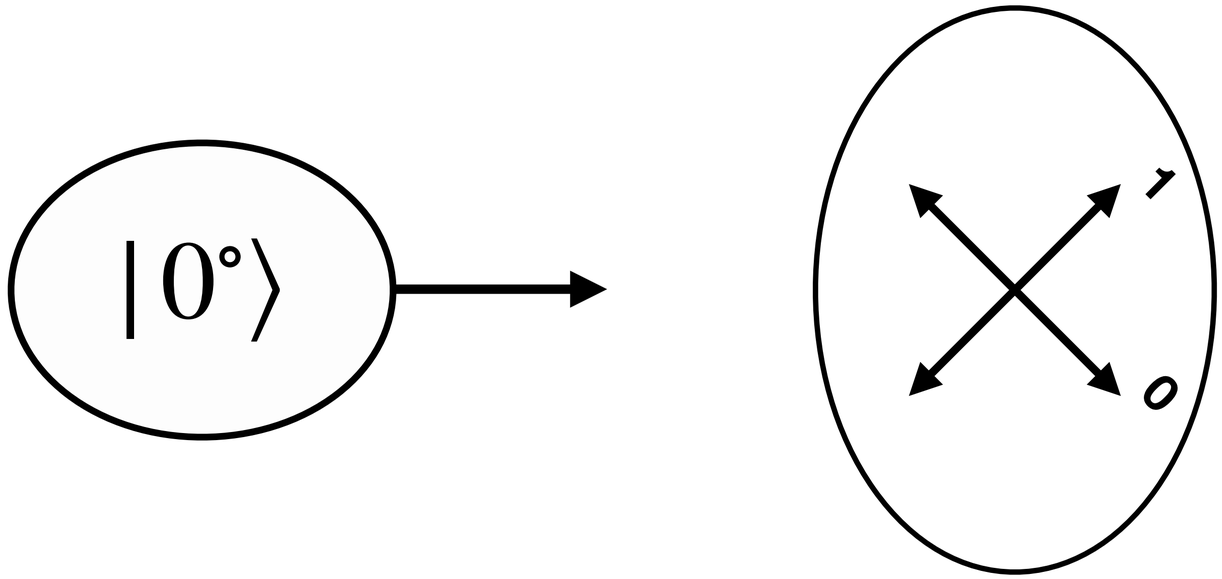
$|45°\rangle \equiv |\ \nearrow\ \rangle$

$|135°\rangle \equiv |\ \nwarrow\ \rangle$

$P_{|0°\rangle} = |1|^2$

$P_{|90°\rangle} = |0|^2$

Mesure

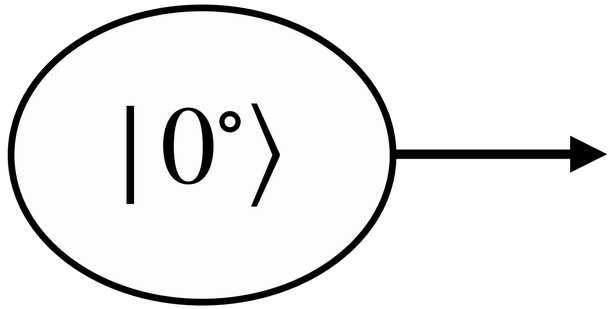


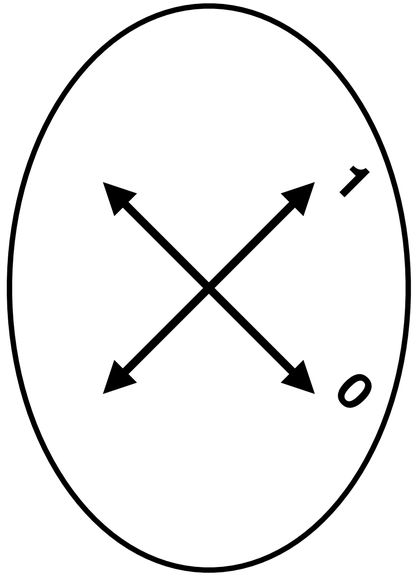
?

$|45°\rangle \equiv |\ \nearrow\ \rangle$

$|135°\rangle \equiv |\ \nwarrow\ \rangle$

Mesure





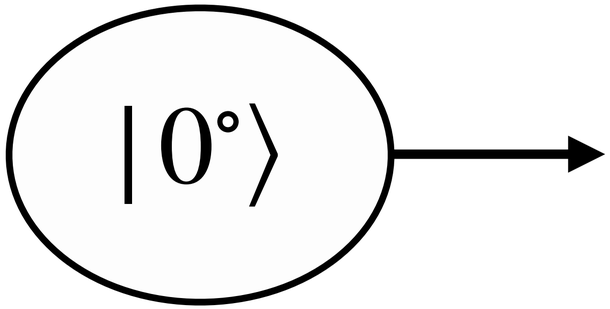
{ ?

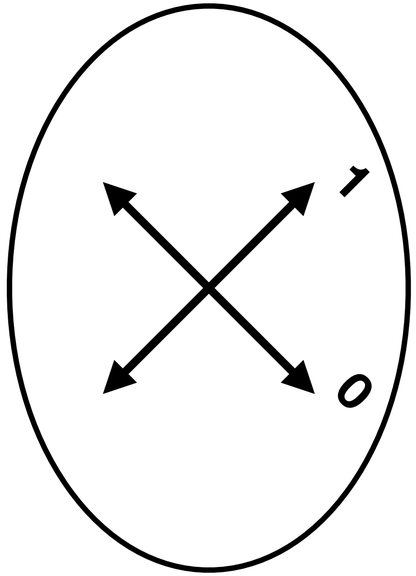
$$\frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|135°\rangle$$

$|45°\rangle \equiv |\ \nearrow\ \rangle$

$|135°\rangle \equiv |\ \nwarrow\ \rangle$

Mesure



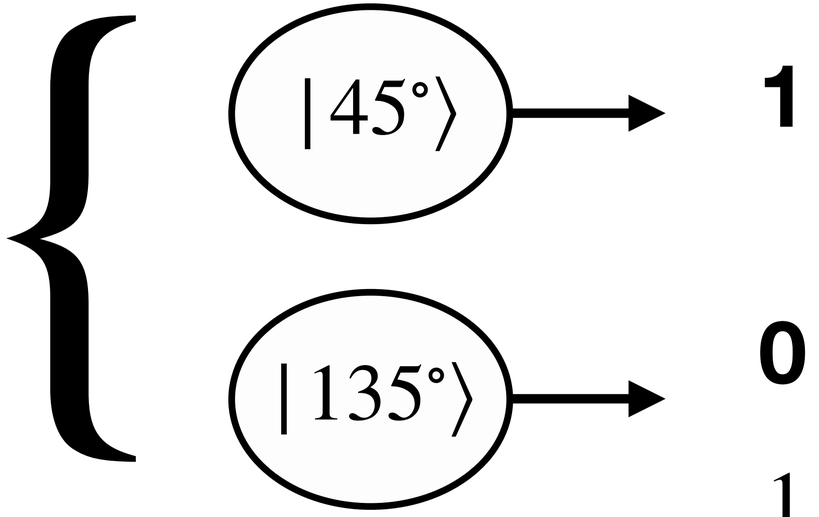


$$\frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|135°\rangle$$

$$|45°\rangle \equiv |\nearrow\rangle$$

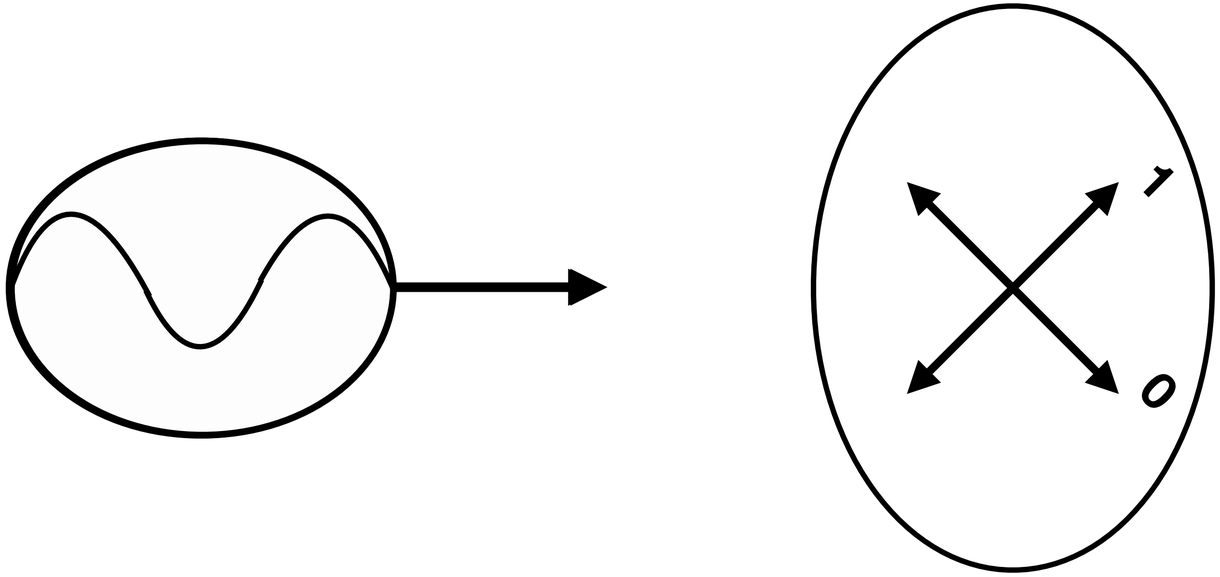
$$|135°\rangle \equiv |\nwarrow\rangle$$

$$P_{|45°\rangle} = \frac{1}{2}$$



$$P_{|135°\rangle} = \frac{1}{2}$$

Mesure



$$P_{|45°\rangle} = |\alpha|^2$$

$$P_{|135°\rangle} = |\beta|^2$$

$|45°\rangle \equiv |\ \nearrow\ \rangle$

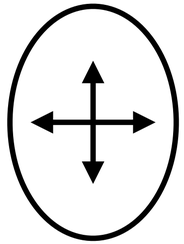
$|135°\rangle \equiv |\ \nwarrow\ \rangle$

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

Superposition & Mesure quantique

Points clés

- La mesure quantique fait s’effondrer la polarisation dans un des états de base de la base de mesure



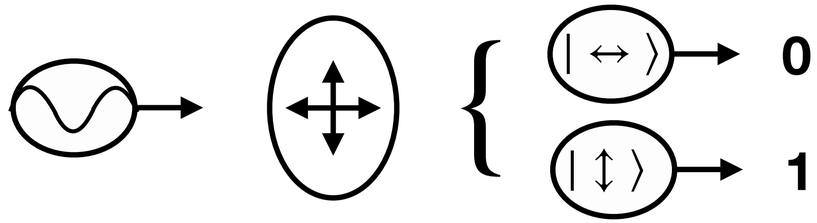
$|\updownarrow\rangle$ ou $|\leftrightarrow\rangle$

Superposition & Mesure quantique

Points clés

- La mesure quantique fait s’effondrer la polarisation dans un des états de base de la base de mesure

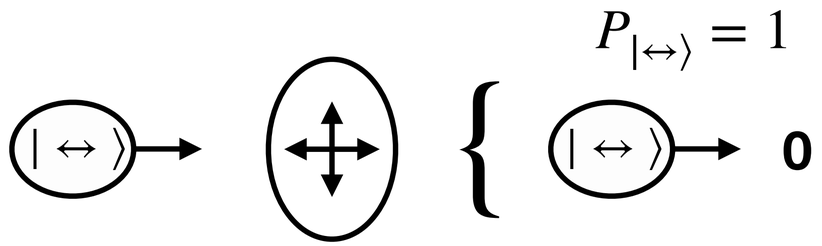
- Si le photon incident est dans un état de superposition, le résultat de mesure est aléatoire



Superposition & Mesure quantique

Points clés

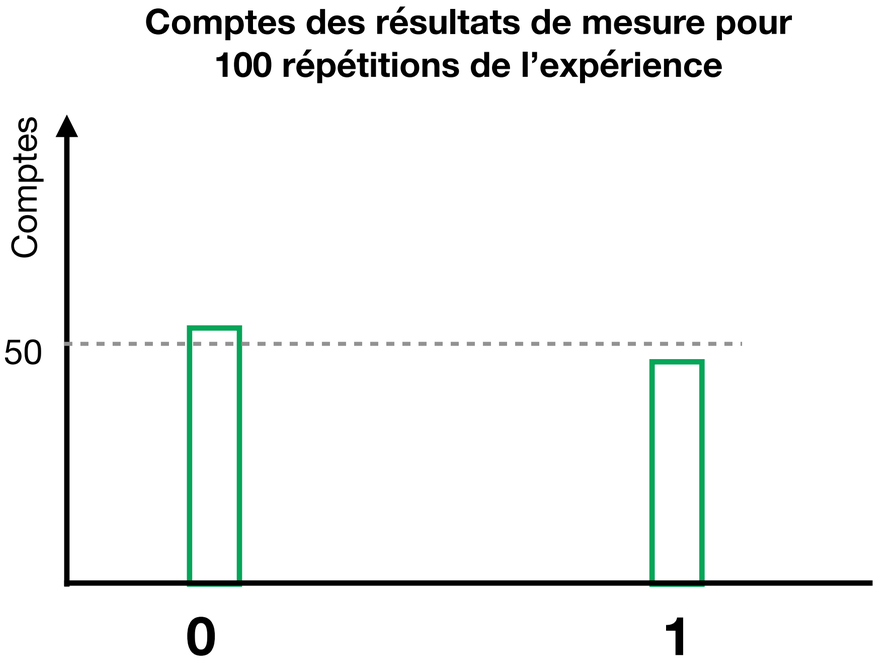
- La mesure quantique fait s’effondrer la polarisation dans un des états de base de la base de mesure
- Si le photon incident est dans un état de superposition, le résultat de mesure est aléatoire
- Si le photon incident est dans un état de base de la base de mesure, le résultat sera toujours le même



Superposition & Mesure quantique

Points clés

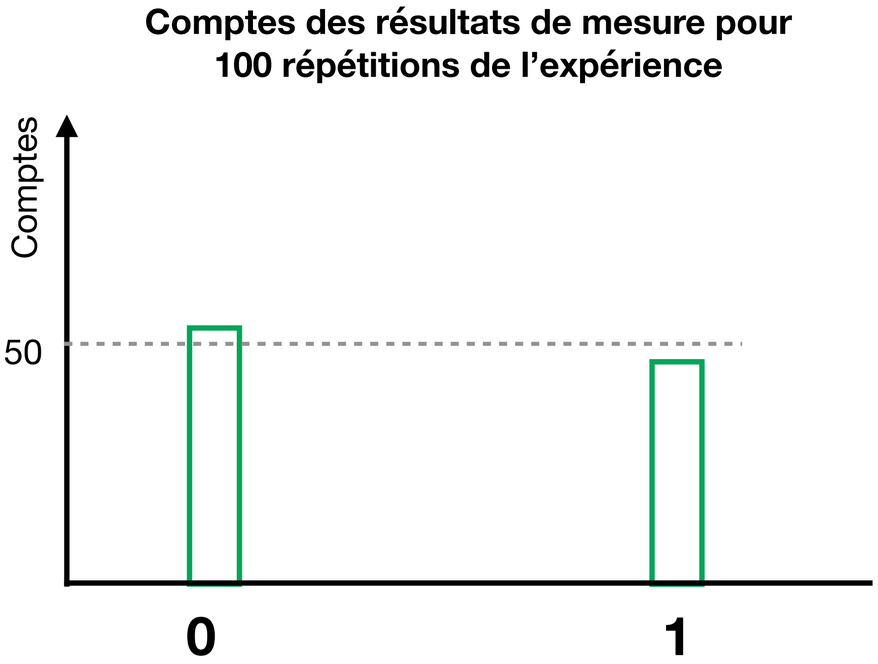
- La mesure quantique fait s’effondrer la polarisation dans un des états de base de la base de mesure
- Si le photon incident est dans un état de superposition, le résultat de mesure est aléatoire
- Si le photon incident est dans un état de base de la base de mesure, le résultat sera toujours le même
- Pour pouvoir décrire l’état quantique d’un photon incident, il faut répéter plusieurs fois l’expérience de la mesure et compiler des statistiques



Superposition & Mesure quantique

Points clés

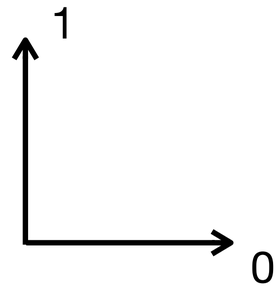
- La mesure quantique fait s’effondrer la polarisation dans un des états de base de la base de mesure
- Si le photon incident est dans un état de superposition, le résultat de mesure est aléatoire
- Si le photon incident est dans un état de base de la base de mesure, le résultat sera toujours le même
- Pour pouvoir décrire l’état quantique d’un photon incident, il faut répéter plusieurs fois l’expérience de la mesure et compiler des statistiques
- Autrement, on ne peut rien dire



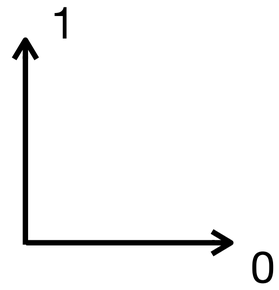
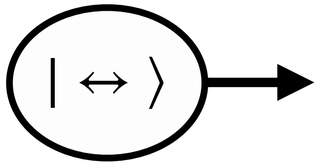
Encodage de l’information

Bit à transmettre	
0	
1	

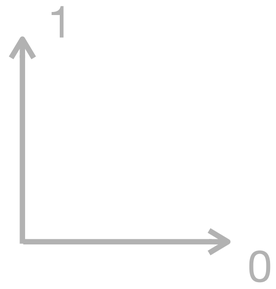
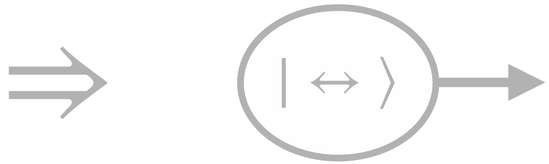
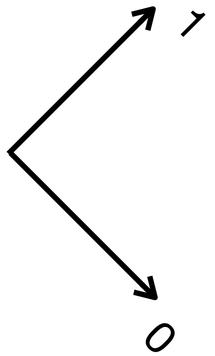
Encodage de l’information

Bit à transmettre	Base de mesure
0	
1	

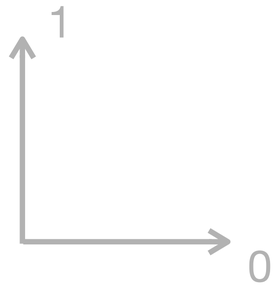
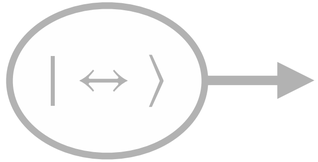
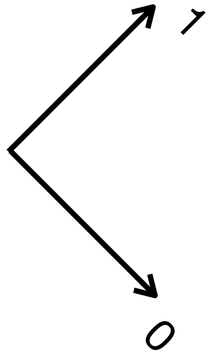
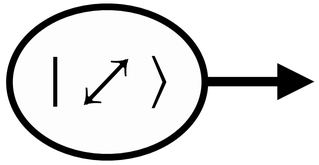
Encodage de l’information

Bit à transmettre	Base de mesure		Photon encodé
0		⇒	
1			

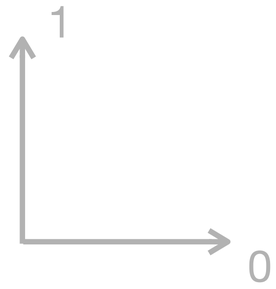
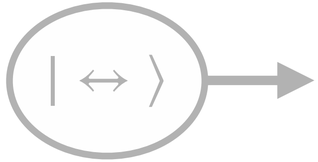
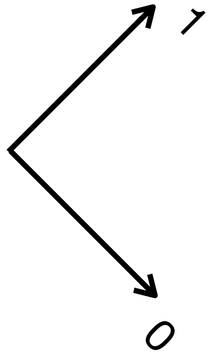
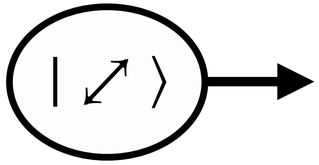
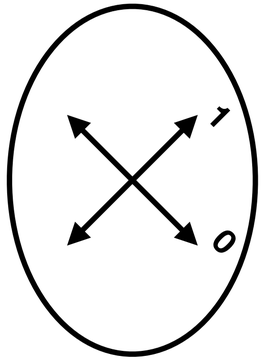
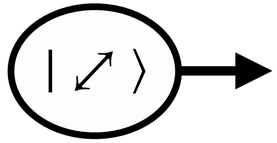
Encodage de l’information

Bit à transmettre	Base de mesure	Photon encodé
0		
1		

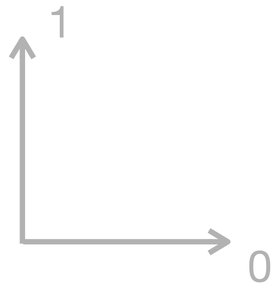
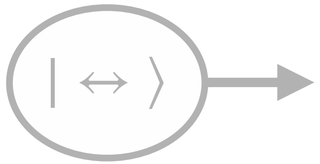
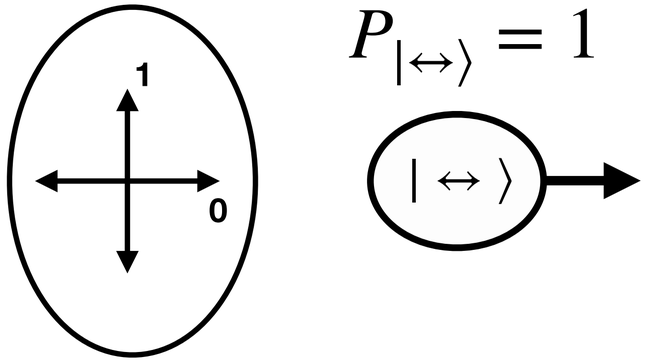
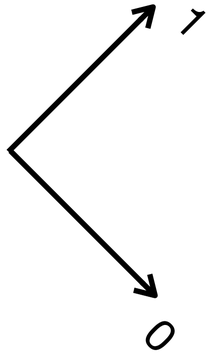
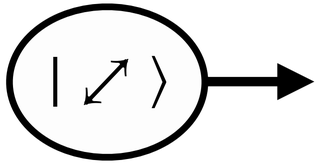
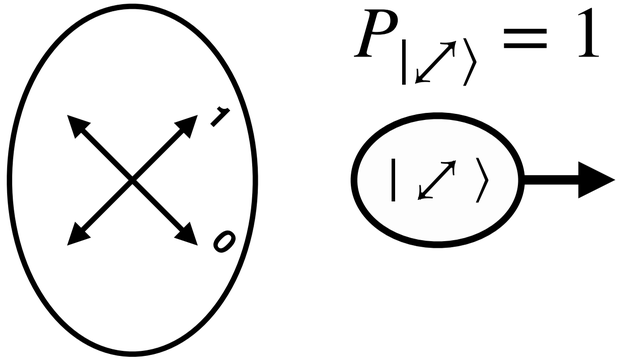
Encodage de l’information

Bit à transmettre	Base de mesure	Photon encodé
0		⇒ 
1		⇒ 

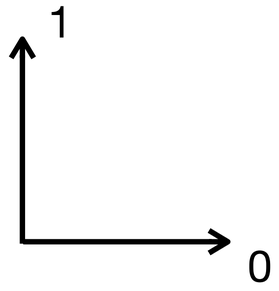
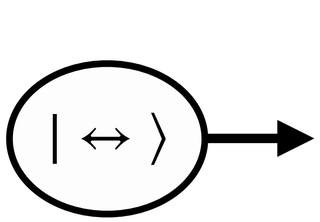
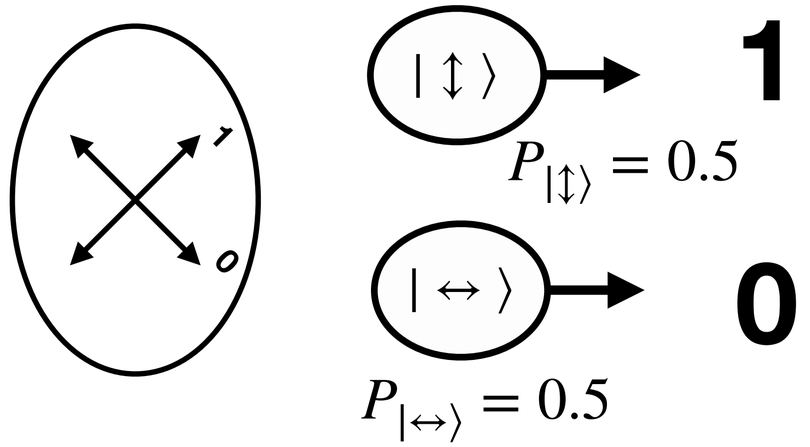
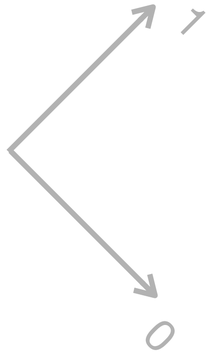
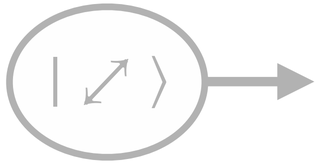
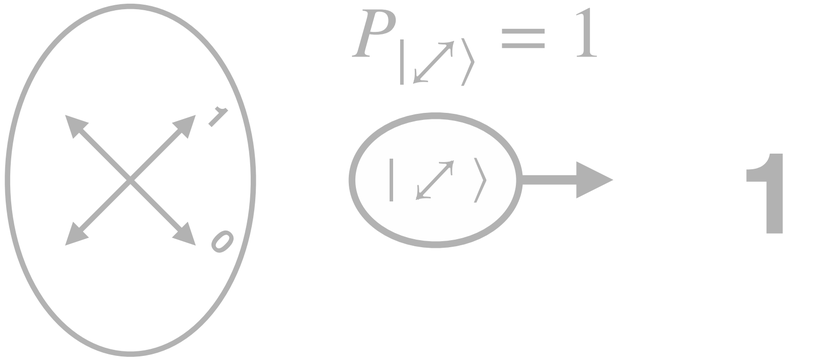
Encodage de l'information

Bit à transmettre	Base de mesure	Photon encodé	Bit transmis
0		⇒ 	
1		⇒   $P_{\|\swarrow\rangle} = 1$ 	1

Encodage de l'information

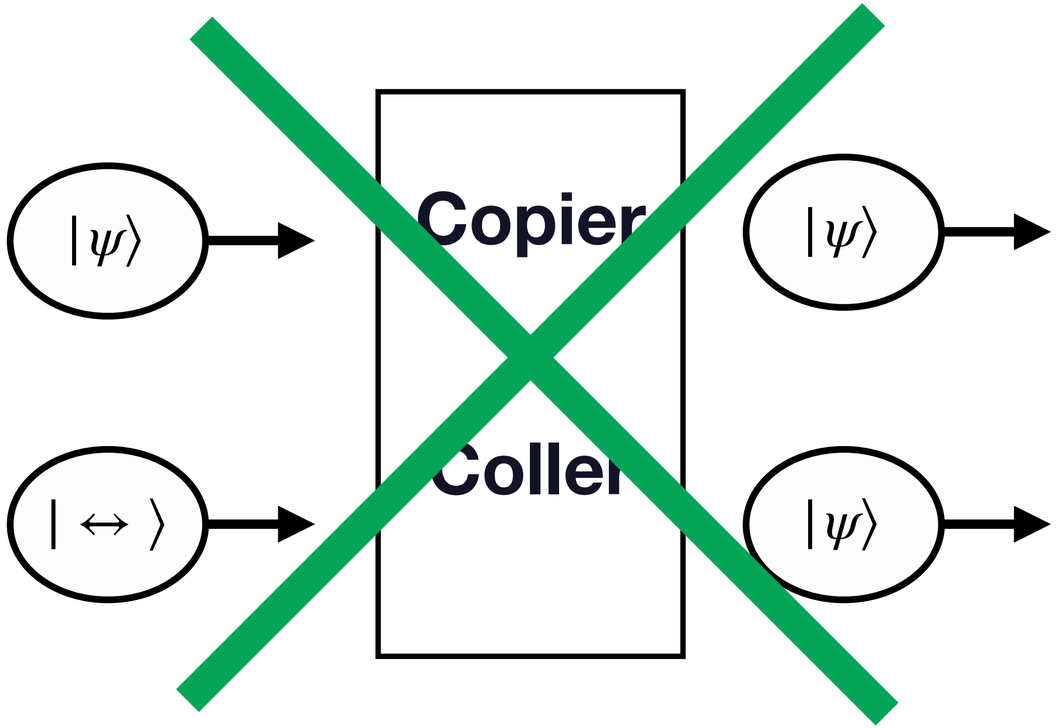
Bit à transmettre	Base de mesure	Photon encodé	Bit transmis
0		⇒ 		0
1		⇒ 		1

Encodage de l'information

Bit à transmettre	Base de mesure	Photon encodé	Bit transmis
0			
1			

Théorème de non-clonage

"Il est impossible de copier l'état quantique d'un photon dans celui d'un deuxième photon"



Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

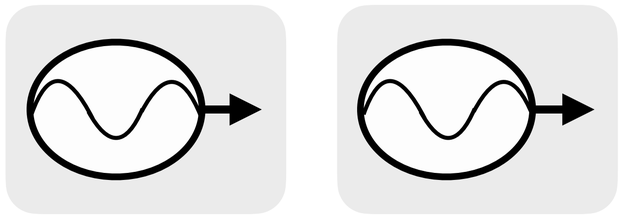
INSTITUT QUANTIQUE UdS

USHERBROOKE.CA/IQ

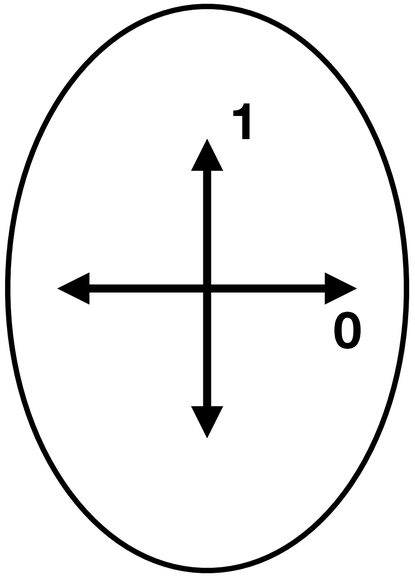
Plan

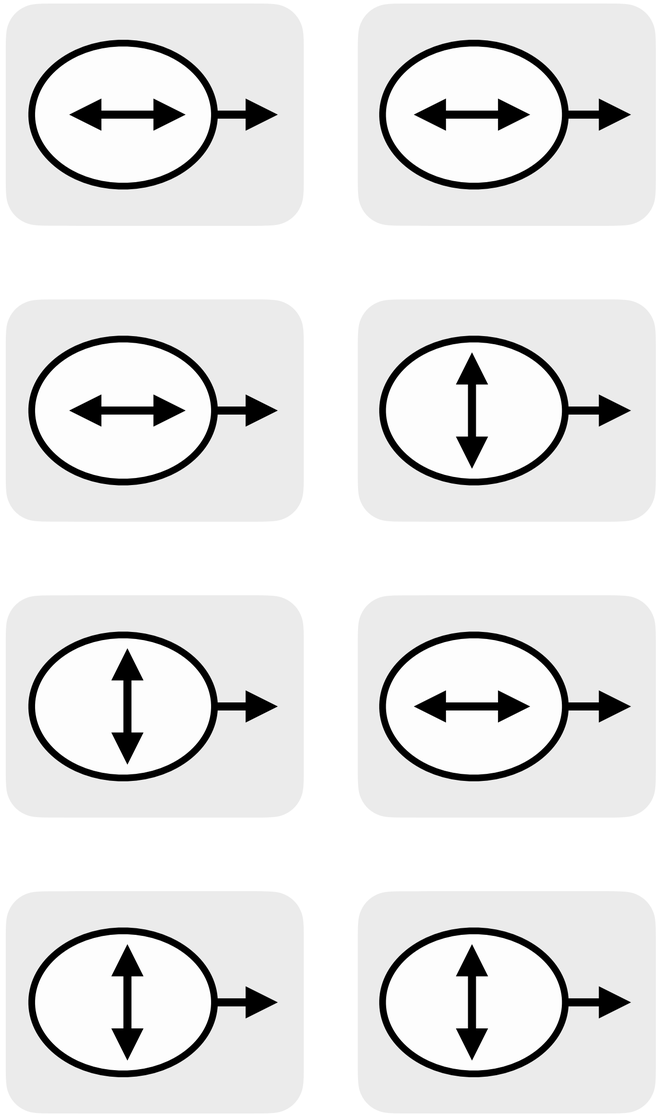
- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Intrication



$$\alpha|\leftrightarrow\leftrightarrow\rangle+\beta|\leftrightarrow\updownarrow\rangle$$
$$+\delta|\updownarrow\leftrightarrow\rangle+\gamma|\updownarrow\updownarrow\rangle$$





$$P_{|\leftrightarrow\leftrightarrow\rangle}=|\alpha|^2$$

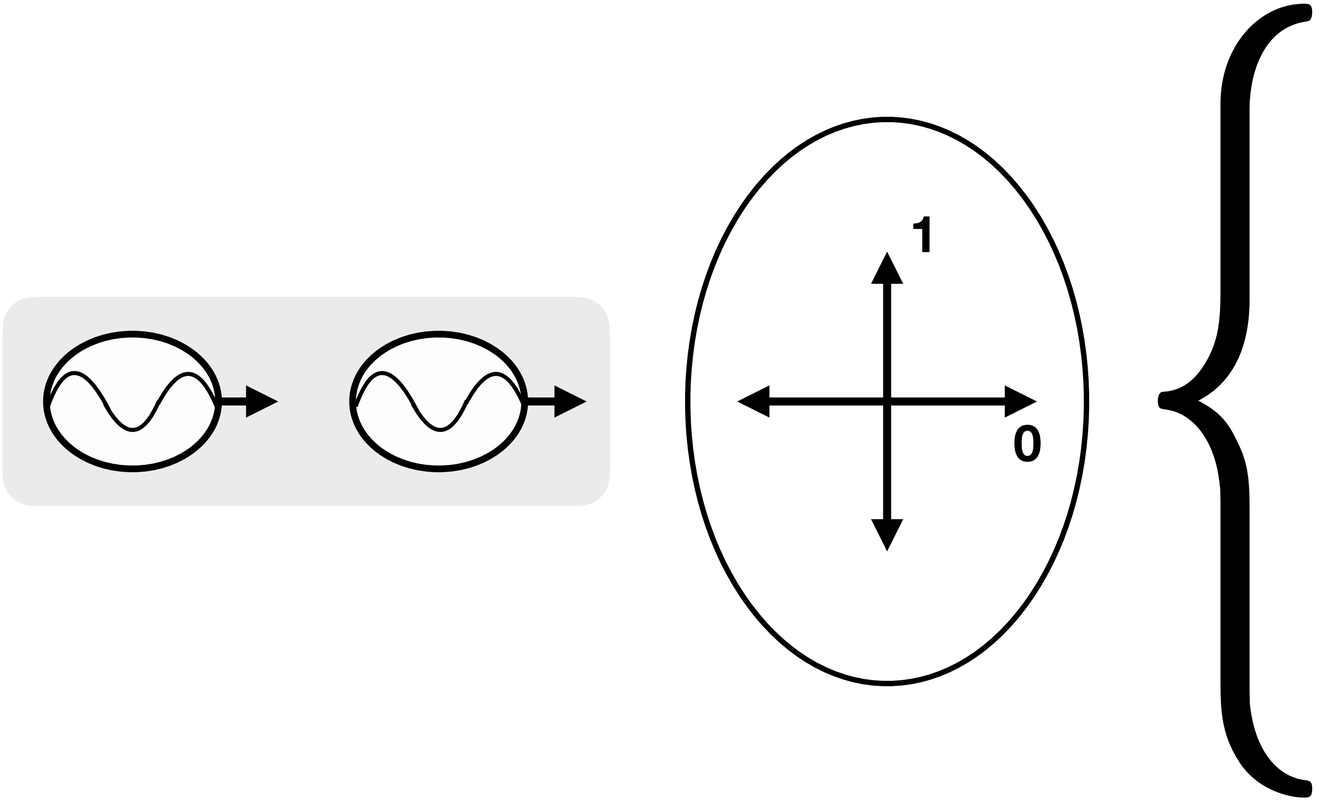
$$P_{|\leftrightarrow\updownarrow\rangle}=|\beta|^2$$

$$P_{|\updownarrow\leftrightarrow\rangle}=|\delta|^2$$

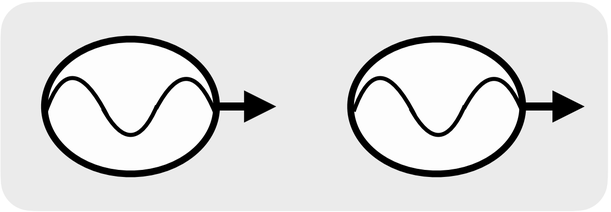
$$P_{|\updownarrow\updownarrow\rangle}=|\gamma|^2$$

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

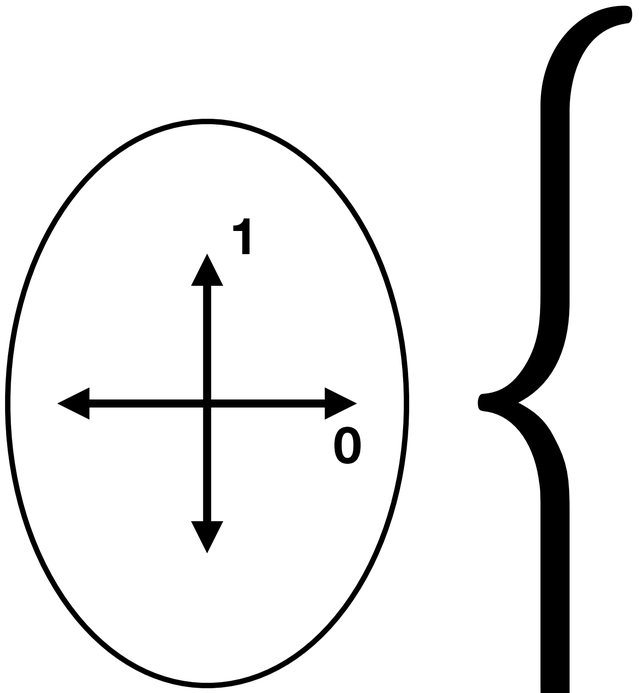
Intrication



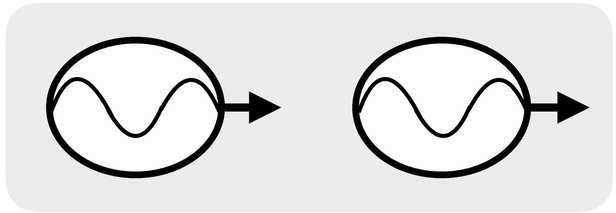
Intrication



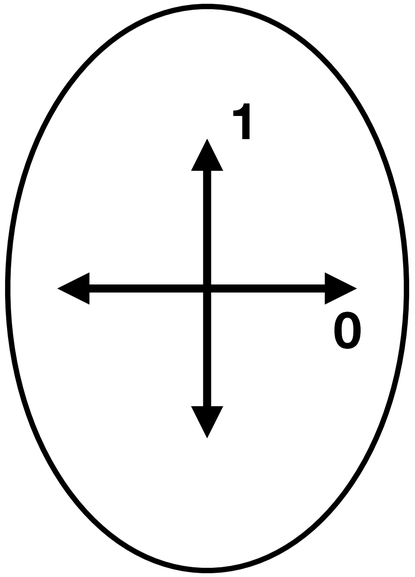
$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

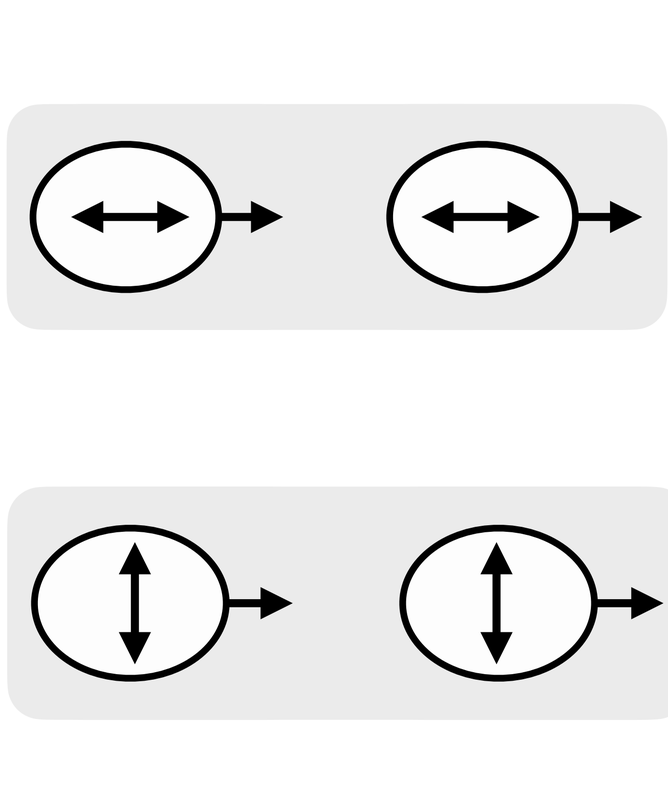


Intrication



$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

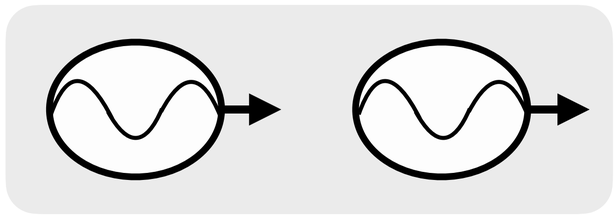




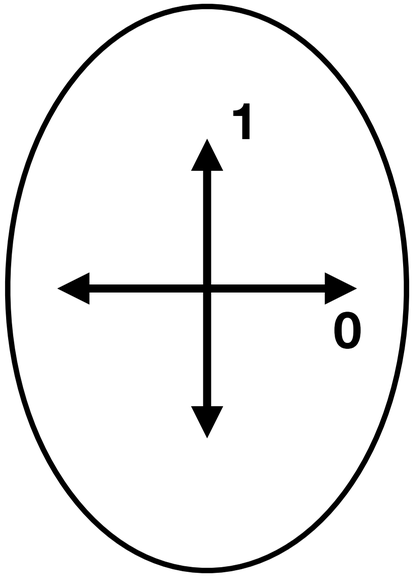
$$P_{|\leftrightarrow\leftrightarrow\rangle}=\frac{1}{2}$$

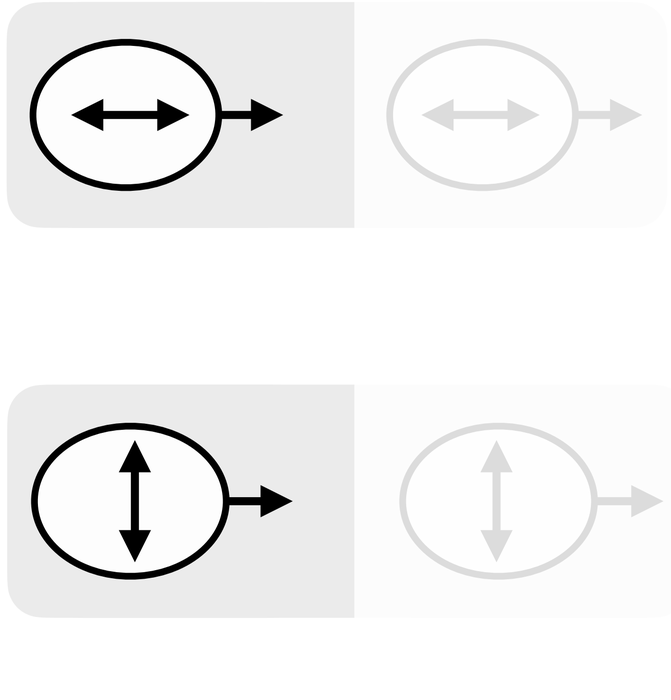
$$P_{|\updownarrow\updownarrow\rangle}=\frac{1}{2}$$

Intrication



$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$





$$P_{|\leftrightarrow\leftrightarrow\rangle}=\frac{1}{2}$$

$$P_{|\updownarrow\updownarrow\rangle}=\frac{1}{2}$$

Paires de Bell

$$\Phi^+$$

$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

$$\Phi^-$$

$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle-\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

$$\Psi^+$$

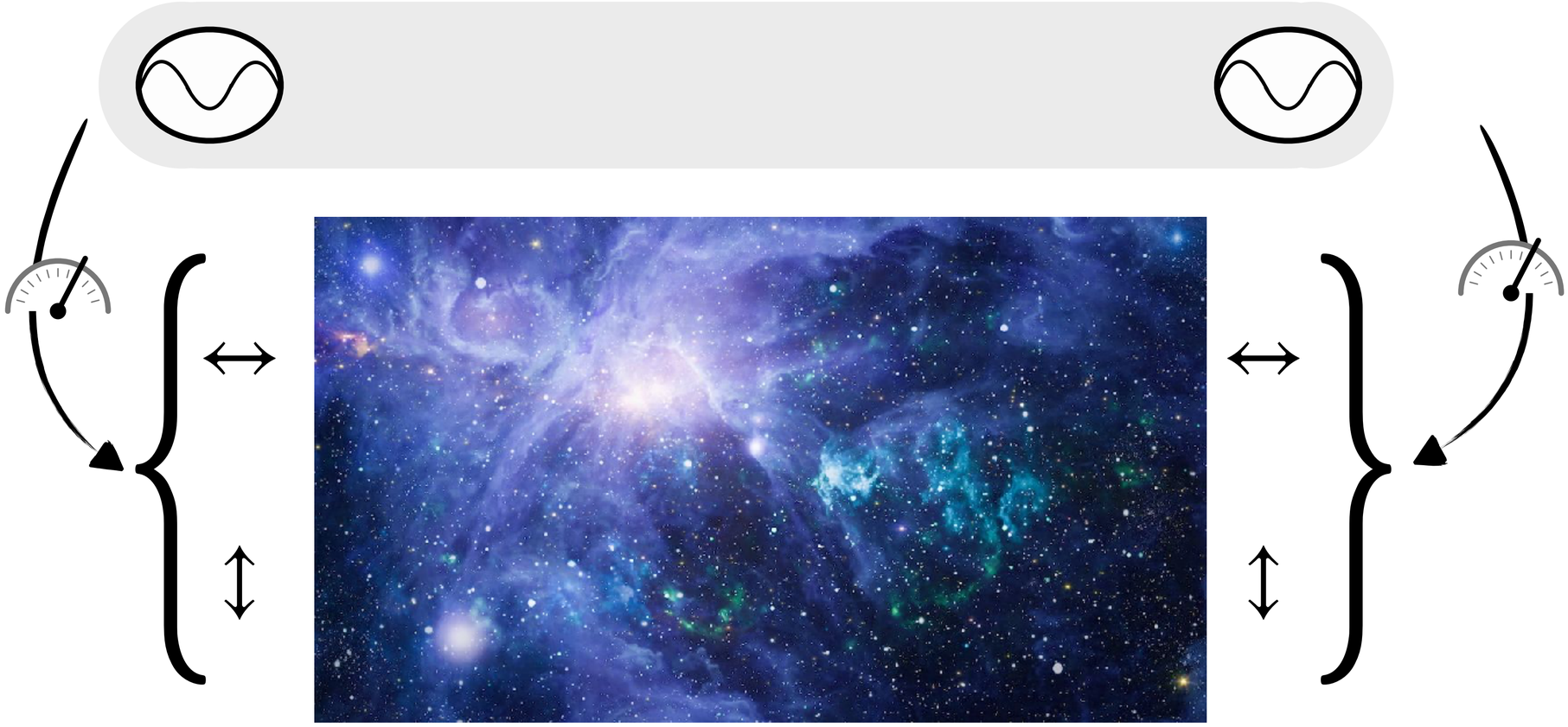
$$\frac{1}{\sqrt{2}}|\leftrightarrow\updownarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\leftrightarrow\rangle$$

$$\Psi^-$$

$$\frac{1}{\sqrt{2}}|\leftrightarrow\updownarrow\rangle-\frac{1}{\sqrt{2}}|\updownarrow\leftrightarrow\rangle$$

Corrélations indépendantes de la distance

$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$

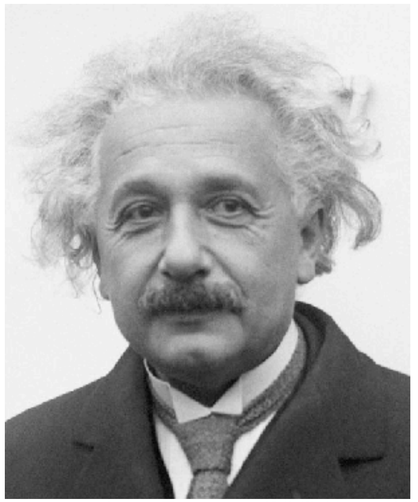


© Shutterstock

Interprétation de l’intrication

AB Lagrelius & Westphal

La mesure du premier photon intriqué fixe l’état du deuxième instantanément peu importe la distance!

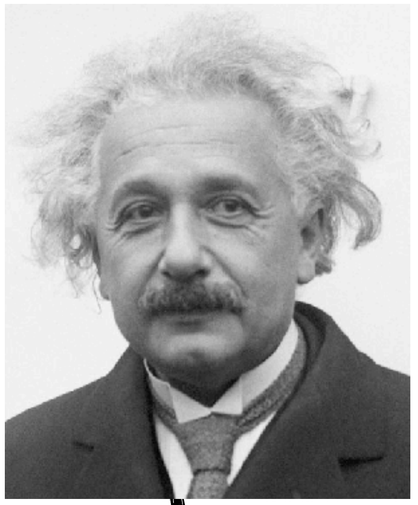


(Image credit: Bettmann / Contributor via Getty Images)

Interprétation de l’intrication

AB Lagrelius & Westphal

La mesure du premier photon intriqué fixe l’état du deuxième instantanément peu importe la distance!



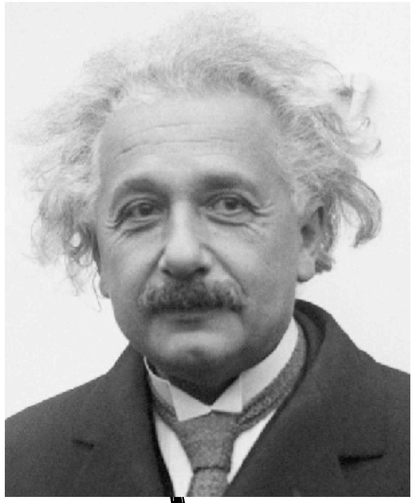
(Image credit: Bettmann / Contributor via Getty Images)

Impossible!
Le choix de l’état doit être déterminé avant la mesure! Il doit y avoir des variables cachées!

Interprétation de l’intrication

AB Lorelius & Westphal

non localité!



(Image credit: Bettmann / Contributor via Getty Images)

Impossible!
Le choix de l’état doit être déterminé avant la mesure! Il doit y avoir des variables cachées!

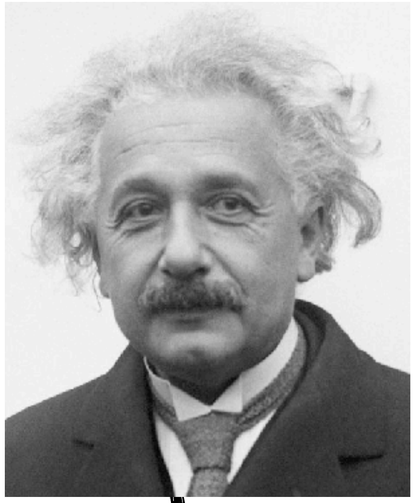
Interprétation de l’intrication

AB Lorelius & Westphal

non localité!

En fait, j’ai une façon de vérifié expérimentalement s’il y a des variables cachées ou non!

1974, CERN



(Image credit: Bettmann / Contributor via Getty Images)

Impossible!
Le choix de l’état doit être déterminé avant la mesure! Il doit y avoir des variables cachées!

Interprétation de l’intrication

1974, CERN

Interprétation de l’intrication

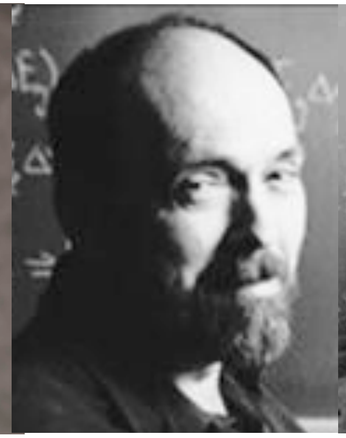
1974, CERN

1964

Inégalité de Bell

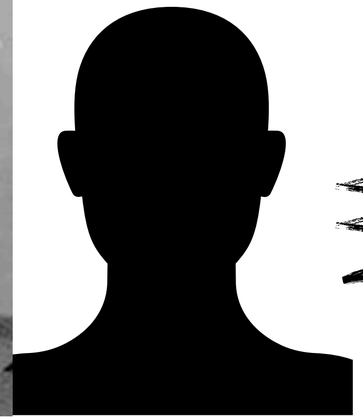
1969

John Clauser



Michael Horne

Abner Shimony



Richard Holt

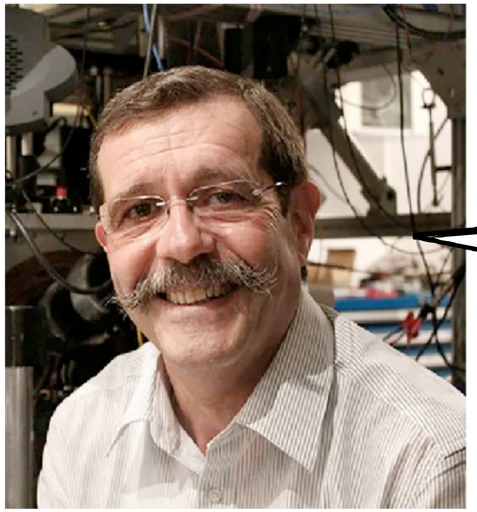
Inégalité CHSH

Interprétation de l’intrication

1974, CERN

1964

Inégalité de Bell



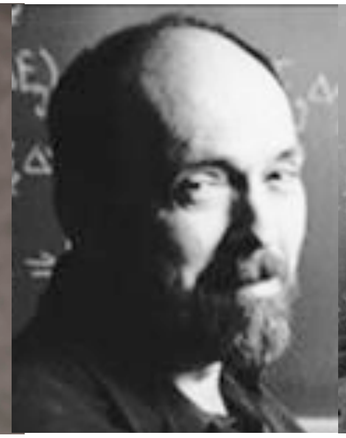
1982

On ne peut pas expliqué l’intrication par une théorie aux variables cachées!

APPROUVÉ EXPÉRIMENTALEMENT

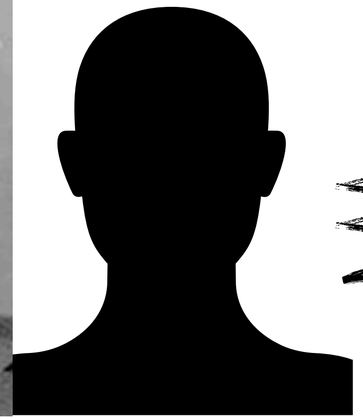
1969

John Clauser



Michael Horne

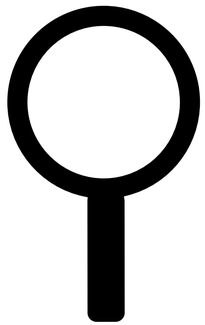
Abner Shimony

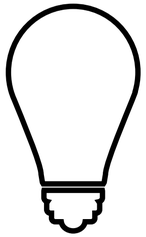


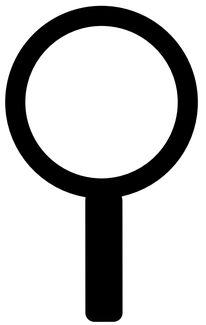
Richard Holt

Inégalité CHSH

Test de Bell







A

Bases: a_1, a_2

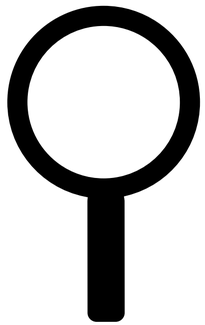
résultats: {0, 1}

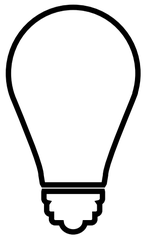
B

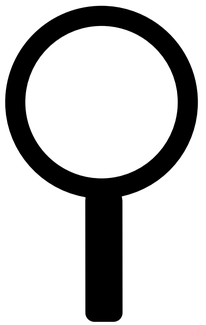
Bases: b_1, b_2

résultats: {0, 1}

Test de Bell







A

Bases: a_1, a_2

résultats: ~~{0, 1}~~

{+1, -1}

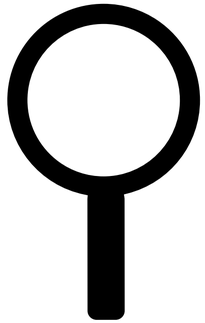
B

Bases: b_1, b_2

résultats: ~~{0, 1}~~

{+1, -1}

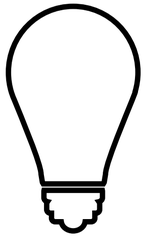
Test de Bell



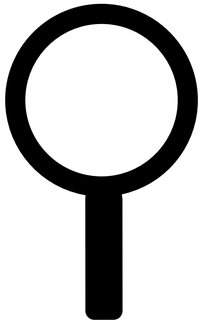
A

Bases: a_1, a_2

résultats: ~~{0, 1}~~
{+1, -1}



a_i	b_j	$a_i b_j$
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

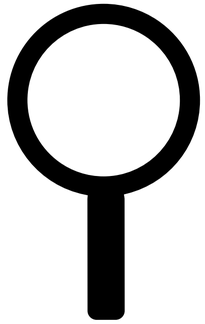


B

Bases: b_1, b_2

résultats: ~~{0, 1}~~
{+1, -1}

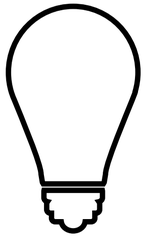
Test de Bell



A

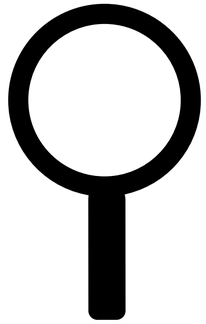
Bases: a_1, a_2

résultats: ~~{0, 1}~~
{+1, -1}



a_i	b_j	$a_i b_j$
+1	**+1**	**+1**
+1	-1	-1
-1	+1	-1
-1	**-1**	**+1**

Mêmes valeurs détectées en A et B

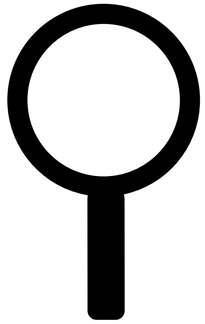


B

Bases: b_1, b_2

résultats: ~~{0, 1}~~
{+1, -1}

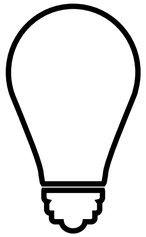
Test de Bell



A

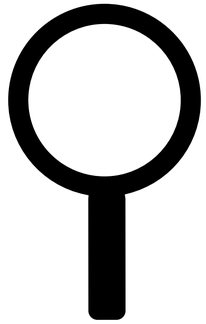
Bases: a_1, a_2

résultats: ~~{0, 1}~~
{+1, -1}



a_i	b_j	$a_i b_j$
+1	+1	+1
+1	**-1**	**-1**
-1	**+1**	**-1**
-1	-1	+1

Différentes valeurs détectées en A et B

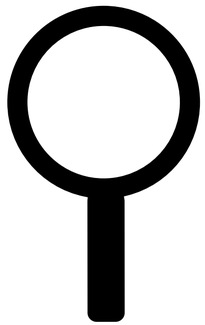


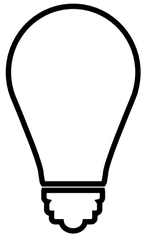
B

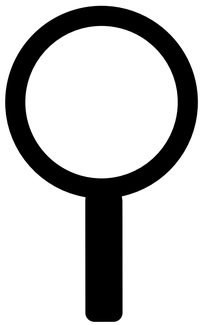
Bases: b_1, b_2

résultats: ~~{0, 1}~~
{+1, -1}

Test de Bell







A

Bases: a_1, a_2

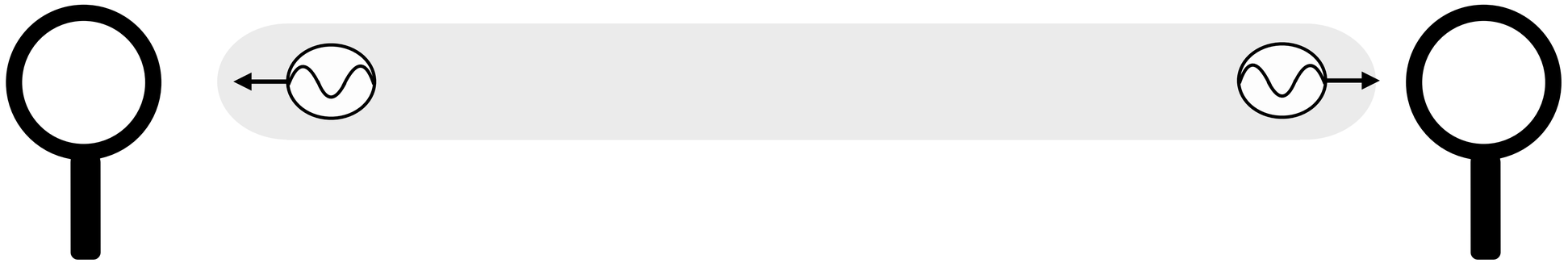
résultats: {+1, -1}

B

Bases: b_1, b_2

résultats: {+1, -1}

Test de Bell



A

Bases: a_1, a_2

résultats: {+1, -1}

B

Bases: b_1, b_2

résultats: {+1, -1}

Test de Bell

Bases: a_1, a_2

résultats: {+1, -1}

Bases: b_1, b_2

résultats: {+1, -1}

Test de Bell

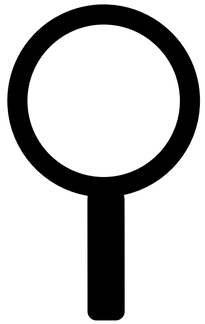
Bases: a_1, a_2

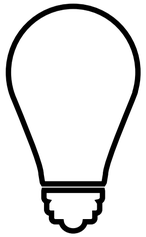
résultats: {+1, -1}

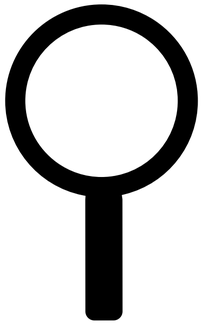
Bases: b_1, b_2

résultats: {+1, -1}

Test de Bell







A

Bases: a_1, a_2

résultats: {+1, -1}

B

Bases: b_1, b_2

résultats: {+1, -1}

x **N**

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

E_{a_i,b_j}	**Interprétation**
1	$a_i = b_j$ est toujours vrai
-1	$a_i = -b_j$ est toujours vrai
0	a_i et b_j sont indépendants l'un de l'autre

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$S' = a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2$$

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

Les résultats peuvent être expliqués par des variables cachées

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}|$$

$$E_{a_i,b_j} = \frac{1}{n}\sum_{k=0}^{n} a_i b_j$$

$$\begin{aligned} S' &= a_1 b_1 + a_1 b_2 + a_2 b_2 - a_1 b_2 \\ &= a_1(b_1 - b_2) + a_2(b_1 + b_2) \end{aligned}$$

b_1	b_2	$b_1 - b_2$	$b_1 + b_2$
+1	+1	0	2
+1	-1	2	0
-1	+1	-2	0
-1	-1	0	-2

$$|S'| \leq 2$$

Classique

Les résultats peuvent être expliqués par des variables cachées

Inégalité CHSH

$$S = | E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2} | \begin{cases} \leq 2 & \text{Classique} \end{cases}$$

Inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Avec des paires de Bell!} \end{cases}$$

Inégalité CHSH

$$S = | E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2} | \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

A		B		
Base	résultat	Base	résultat	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_i,b_j} = \frac{1}{n} \sum_{k=0}^{n} a_i b_j$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

A		B		
Base	résultat	Base	résultat	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

A		B		
Base	résultat	Base	résultat	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

A		B		
Base	résultat	Base	résultat	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

A		B		
Base	résultat	Base	résultat	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

$$S = 0.33 + 0 + 1 - 0 = 1.33 \leq 2$$

Calcul de l'inégalité CHSH

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

A		B		
Base	résultat	Base	résultat	$a_i \cdot b_j$
a_1	+1	b_1	+1	+1
a_1	+1	b_1	-1	-1
a_1	-1	b_1	-1	+1
a_2	+1	b_1	+1	+1
a_2	-1	b_1	+1	-1
a_2	+1	b_2	+1	+1

$$E_{a_1,b_1} = \frac{1 - 1 + 1}{3} = \frac{1}{3}$$

$$E_{a_2,b_1} = \frac{1 - 1}{3} = 0$$

$$E_{a_2,b_2} = \frac{1}{1} = 1$$

$$E_{a_1,b_2} = 0$$

$$S = 0.33 + 0 + 1 - 0 = 1.33 \leq 2$$

Pas assez de mesures pour faire émettre une conclusion!

PAUSE

Retour à

00:00

INSTITUT QUANTIQUE UdS

USHERBROOKE.CA/IQ

Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

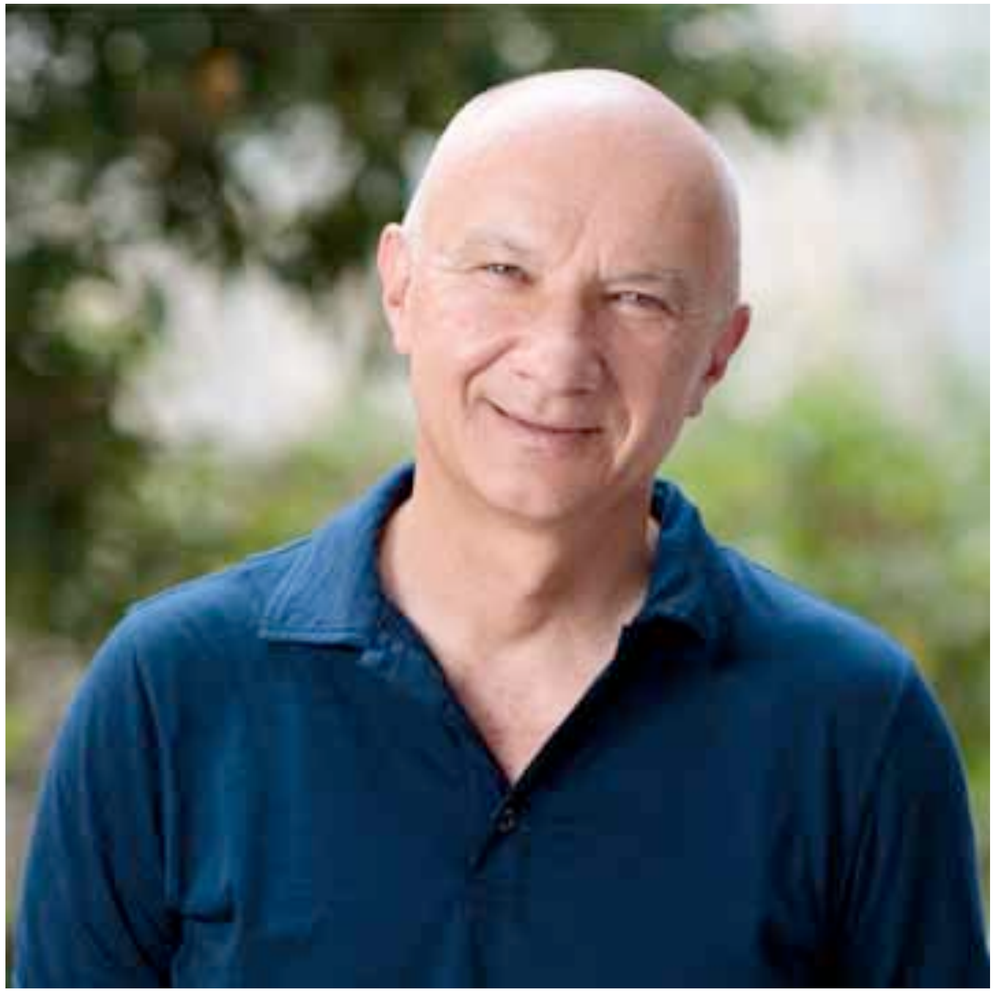
Protocole E91

Créé par **Artur Ekert** en **1991**

Protocole de distribution d’une clé symétrique quantique (QKD)

Sécurité théorique parfaite

basée sur:



https://www.cqt.sg/groups/artur-ekert/

Protocole E91

Créé par **Artur Ekert** en **1991**

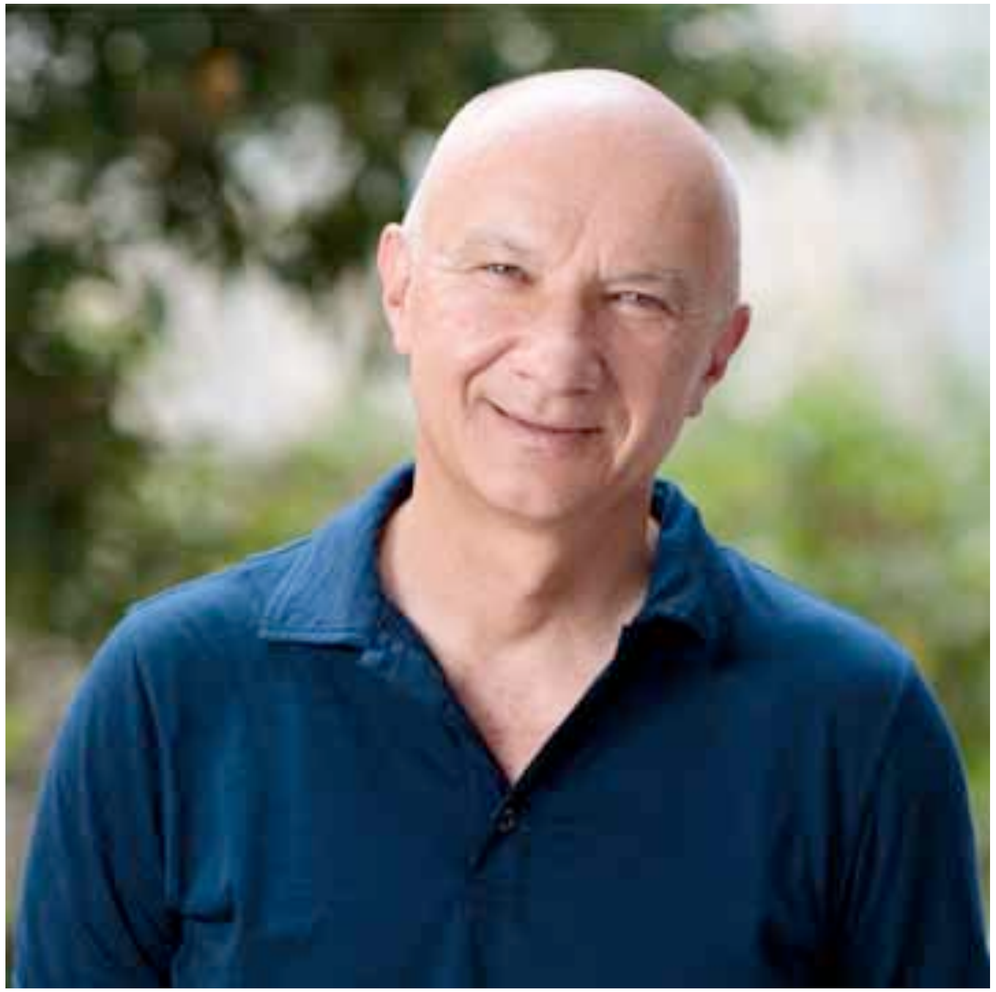
Protocole de distribution d’une clé symétrique quantique (QKD)

Sécurité théorique parfaite

basée sur:

La mesure quantique

Distribution de la clé symétrique



https://www.cqt.sg/groups/artur-ekert/

Protocole E91

Créé par **Artur Ekert** en **1991**

Protocole de distribution d’une clé symétrique quantique (QKD)

Sécurité théorique parfaite

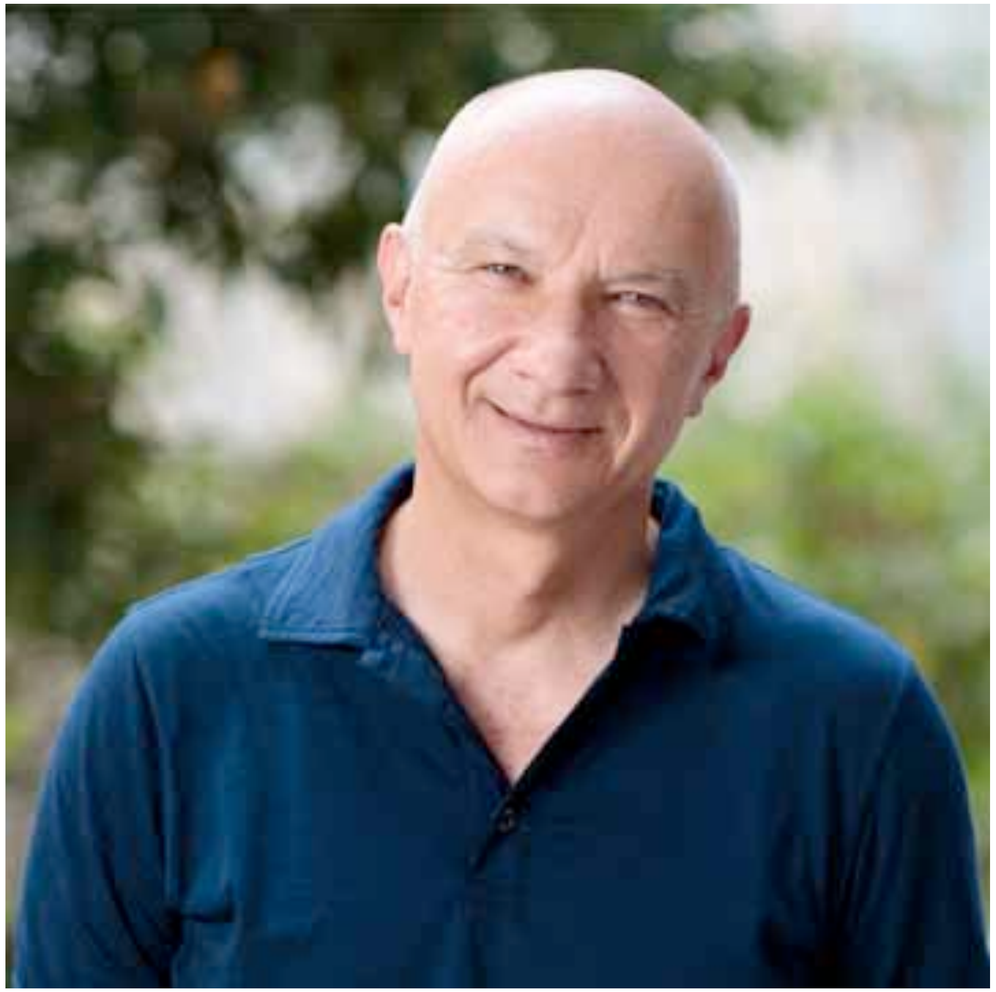
basée sur:

La mesure quantique

Distribution de la clé symétrique

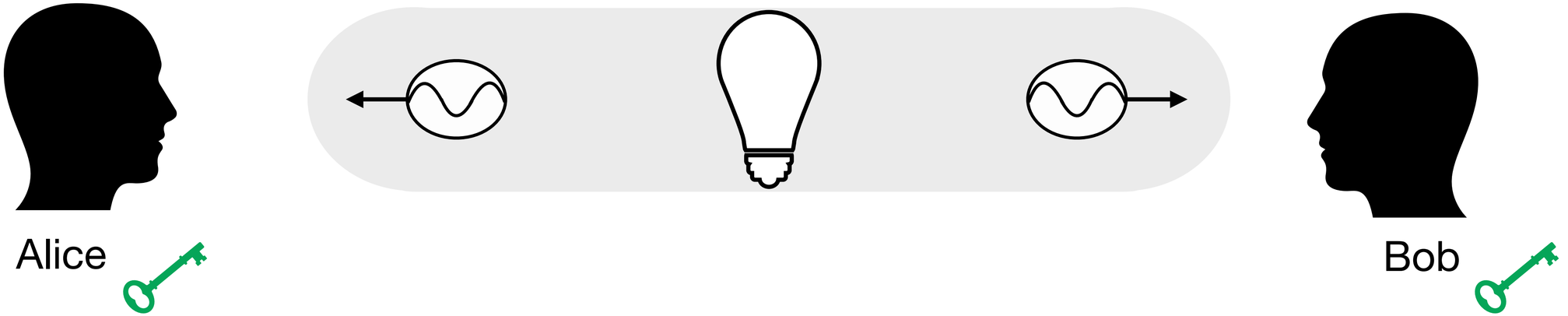
L’intrication et l’inégalité CHSH

Détection d’espions



https://www.cqt.sg/groups/artur-ekert/

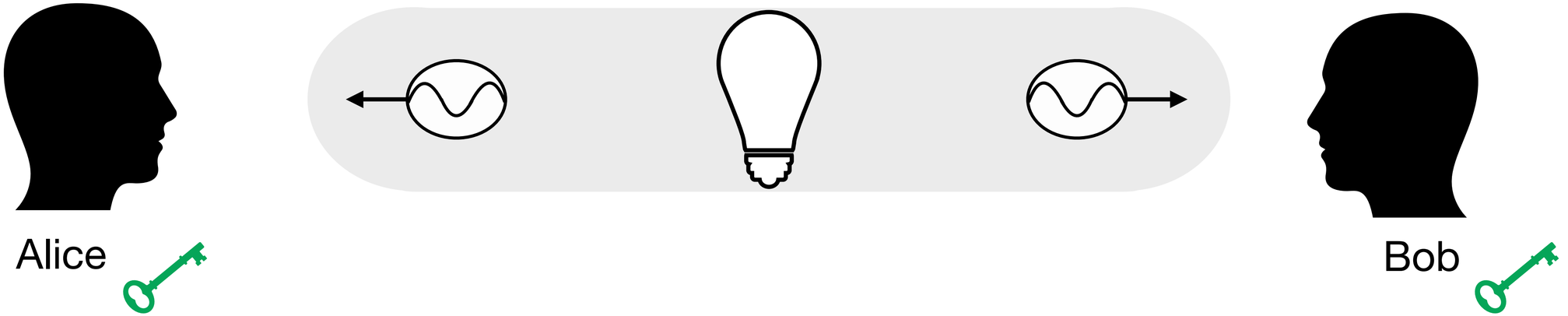
Étapes du protocole



But

Établir une clé symétrique secrète entre Alice et Bob

Étapes du protocole

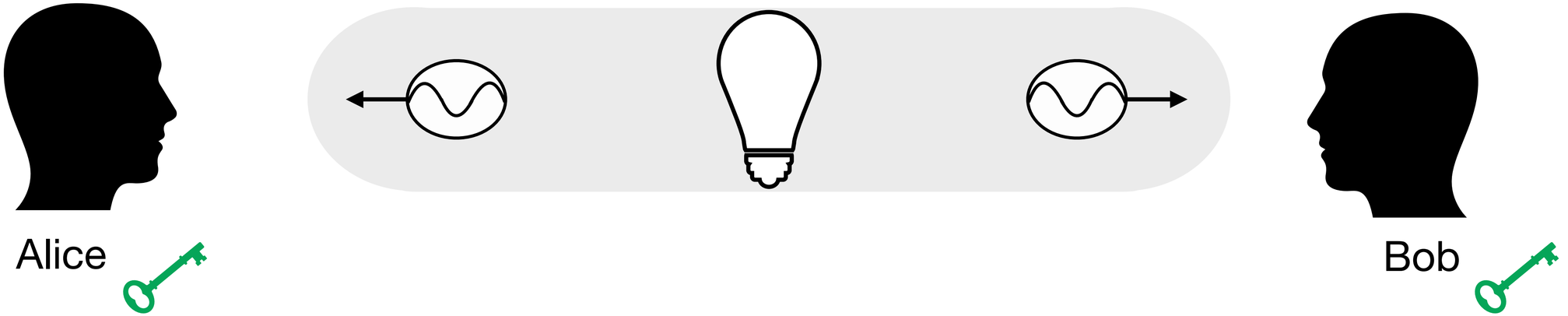


But

Établir une clé symétrique secrète entre Alice et Bob

1. Réception de photons intriqués

Étapes du protocole

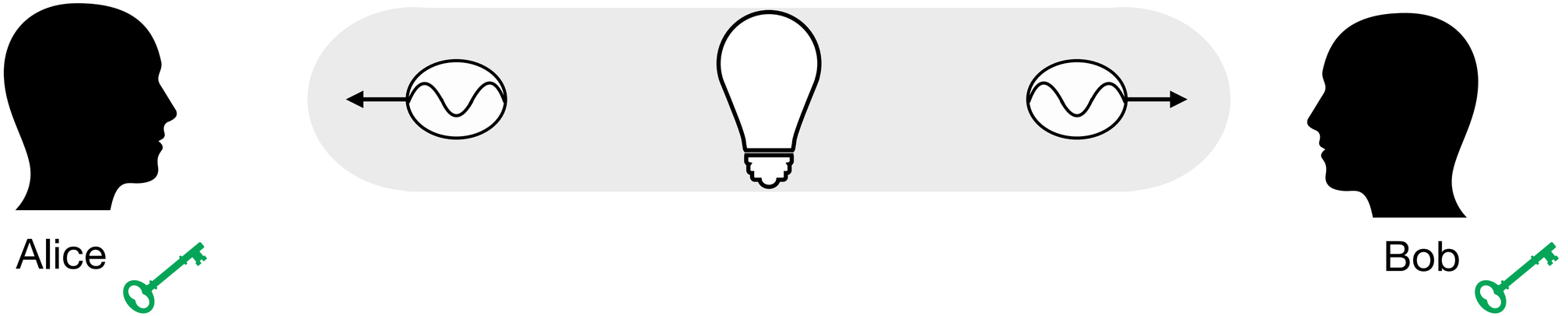


But

Établir une clé symétrique secrète entre Alice et Bob

1. Réception de photons intriqués
2. Annonce des bases de mesures

Étapes du protocole



But

Établir une clé symétrique secrète entre Alice et Bob

1. Réception de photons intriqués
2. Annonce des bases de mesures
3. Détection d’erreur et/ou d’espion

Étape 1: Réception des photons intriqués

Alice et Bob reçoivent chacun un photon d’une paire intriquée

Alice

(0°, 45°, 90°)

Bob

(45°, 90°, 135°)

Étape 1: Réception des photons intriqués

Alice et Bob reçoivent chacun un photon d’une paire intriquée

Alice

(0°, 45°, 90°)

Bob

(45°, 90°, 135°)

Choix aléatoire d’une base

0°

90°

Étape 1: Réception des photons intriqués

Alice et Bob reçoivent chacun un photon d’une paire intriquée

Alice

(0°, 45°, 90°)

Bob

(45°, 90°, 135°)

Choix aléatoire d’une base

0°

90°

Mesure du photon

0 ou 1

0 ou 1

Étape 1: Réception des photons intriqués

$N \times$

Alice et Bob reçoivent chacun un photon d'une paire intriquée

Alice

$(0°, 45°, 90°)$

Bob

$(45°, 90°, 135°)$

Choix aléatoire d'une base

$0°$

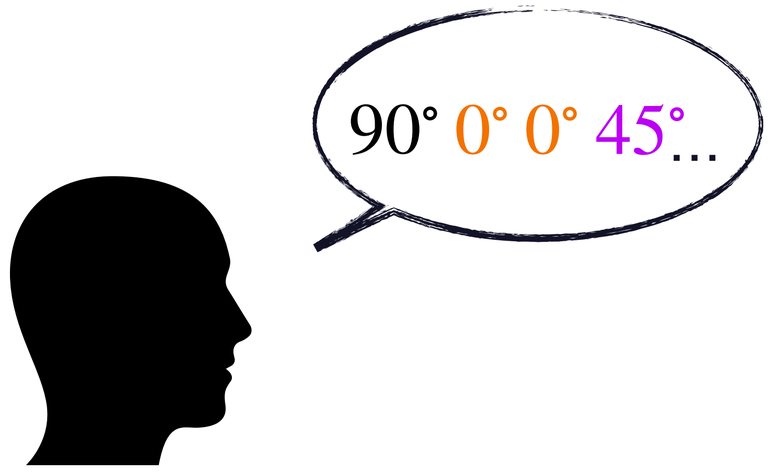
$90°$

Mesure du photon

0 ou 1

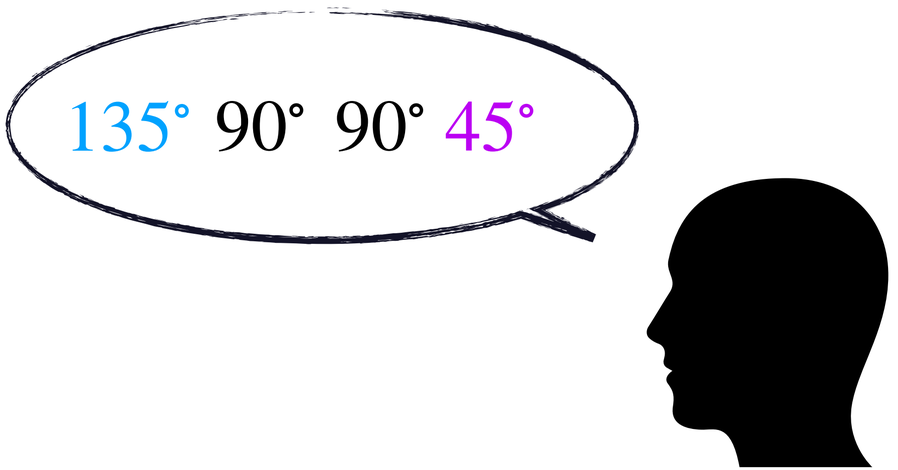
0 ou 1

Étape 2: Annonce des bases



Alice

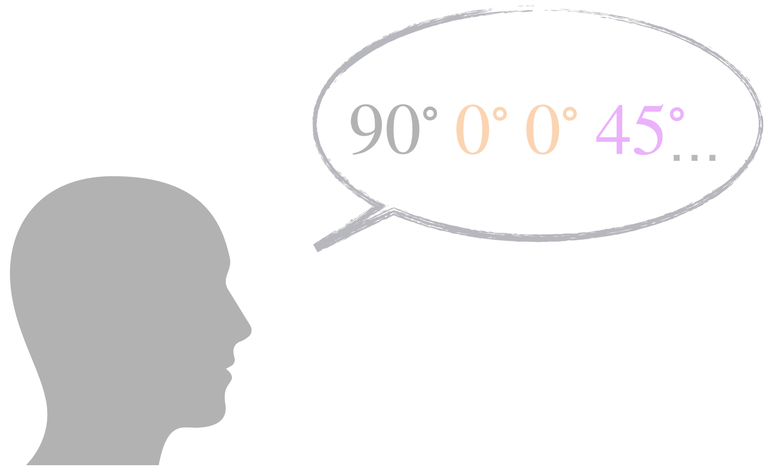
(0°, 45°, 90°)



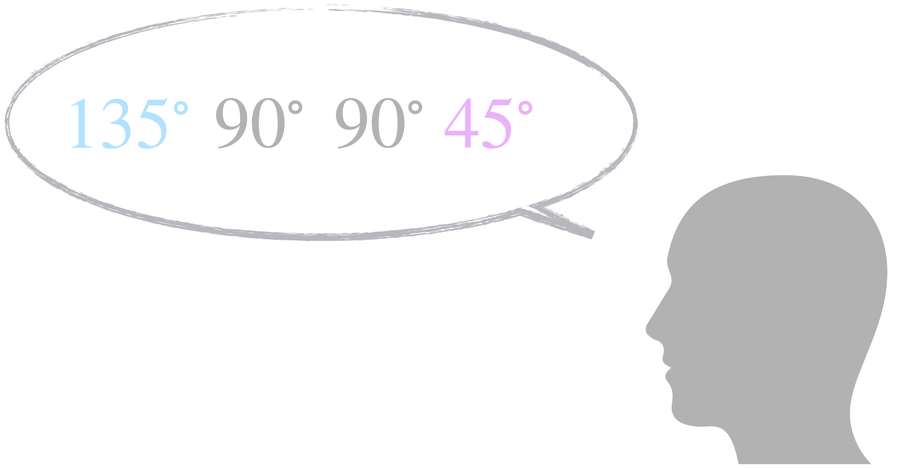
Bob

(45°, 90°, 135°)

Étape 2: Annonce des bases



(0°, 45°, 90°)



(45°, 90°, 135°)

9 combinaisons

(0°, 45°) (0°, 90°) (0°, 135°) (45°, 45°) (45°, 90°) (45°, 135°) (90°, 45°) (90°, 90°) (90°, 135°)

Étape 2: Annonce des bases

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Étape 2: Annonce des bases

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Étape 2: Annonce des bases

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d’espion

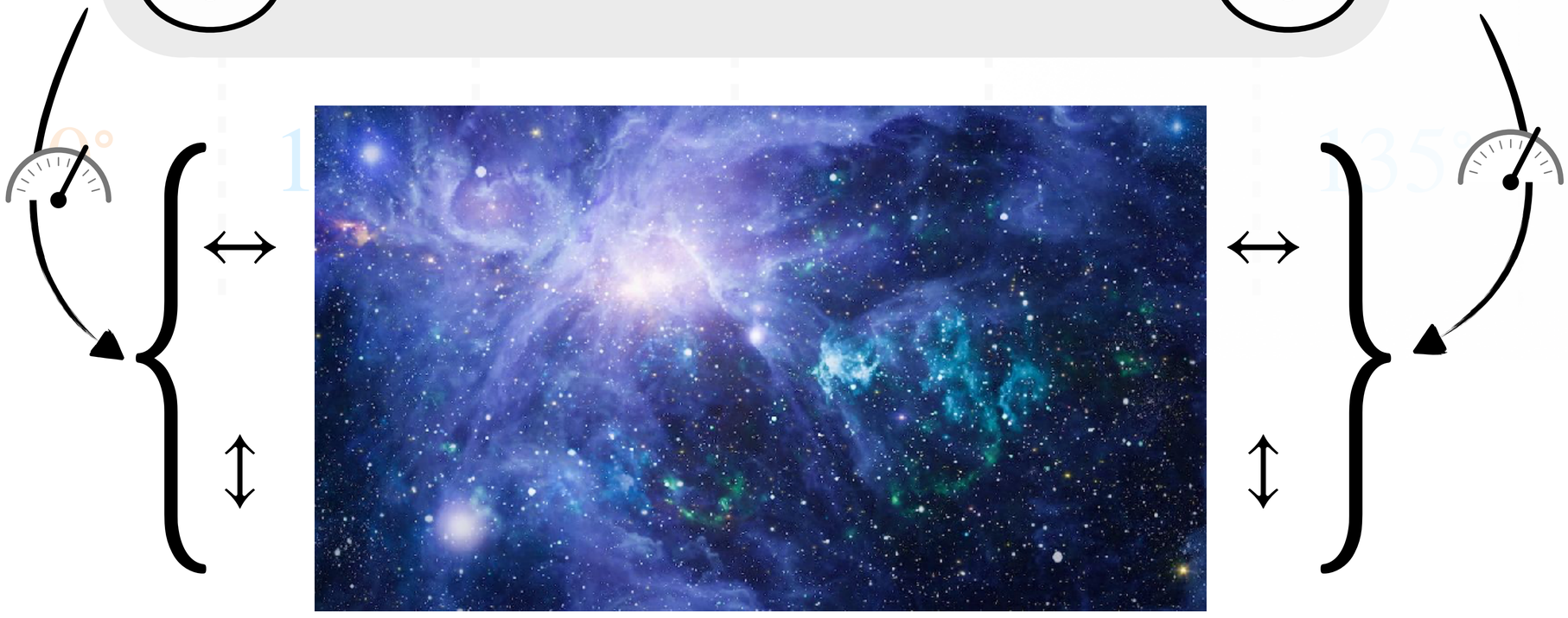
Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Création de la clé symétrique

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°

Création de la clé symétrique

$$\frac{1}{\sqrt{2}}|\leftrightarrow\leftrightarrow\rangle+\frac{1}{\sqrt{2}}|\updownarrow\updownarrow\rangle$$



© Shutterstock

Création de la clé symétrique

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°

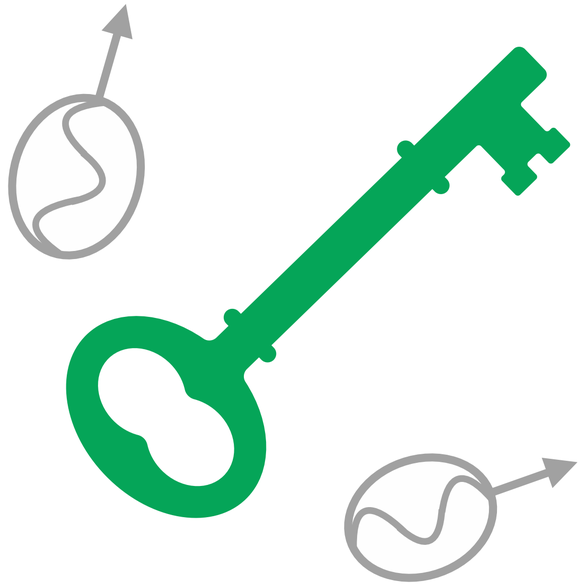
Création de la clé symétrique

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7
Alice	0°	135°	0°	45°	90°	135°	90°
Bob	0°	135°	0°	45°	90°	135°	90°
	1	1	0	0	1	0	0

Propriétés de la clé symétrique quantique

Binaire

Les résultats de mesure quantique sont étiquetés 0 ou 1.



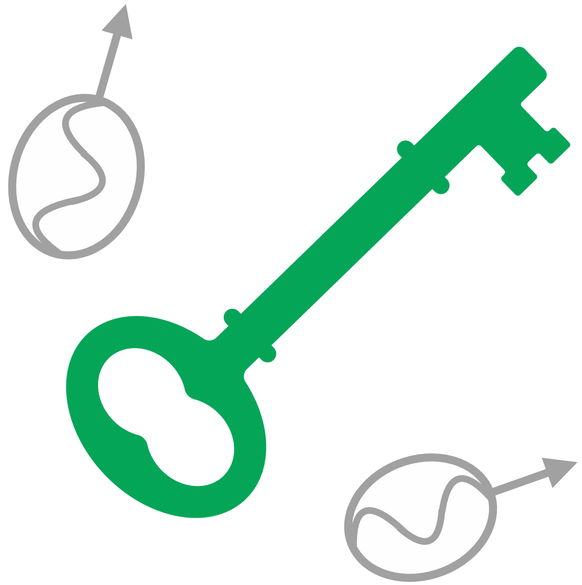
Propriétés de la clé symétrique quantique

Binaire

Les résultats de mesure quantique sont étiquetés 0 ou 1.

Identique

La mesure quantique des photons d’une paire intriquée dans la même base garantie la même mesure chez Alice et Bob.



Propriétés de la clé symétrique quantique

Binaire

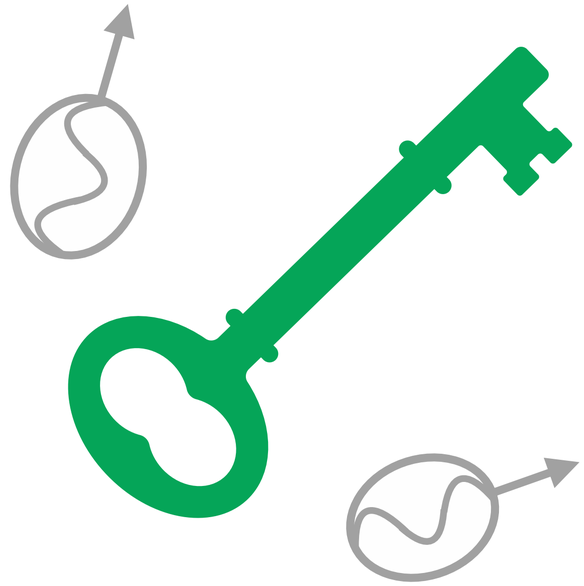
Les résultats de mesure quantique sont étiquetés 0 ou 1.

Identique

La mesure quantique des photons d’une paire intriquée dans la même base garantie la même mesure chez Alice et Bob.

Parfaitement aléatoire

La mesure quantique d’une paire intriquée garantie l’aléatoire.



Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d'espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d’espion

Alice	Bob
0°	45°
0°	90°
0°	135°
45°	90°
45°	135°
90°	45°
90°	135°

Étape 3: Détection d’erreur et/ou d’espion

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d’espion

Alice	Bob	
0°	45°	✓
0°	90°	
0°	135°	✓
45°	90°	
45°	135°	
90°	45°	✓
90°	135°	✓

Étape 3: Détection d’erreur et/ou d’espion

Combinaisons de bases utilisées: $(0°, 45°)(0°, 135°)(90°, 45°)(90°, 135°)$

Alice $\{0°, 90°\}$

Bob $\{45°, 135°\}$

Étape 3: Détection d'erreur et/ou d'espion

Combinaisons de bases utilisées: $(0°, 45°)\,(0°, 135°)\,(90°, 45°)\,(90°, 135°)$

Alice $\{0°, 90°\}$ $\{a_1, a_2\}$

Bob $\{45°, 135°\}$ $\{b_1, b_2\}$

Étape 3: Détection d'erreur et/ou d'espion

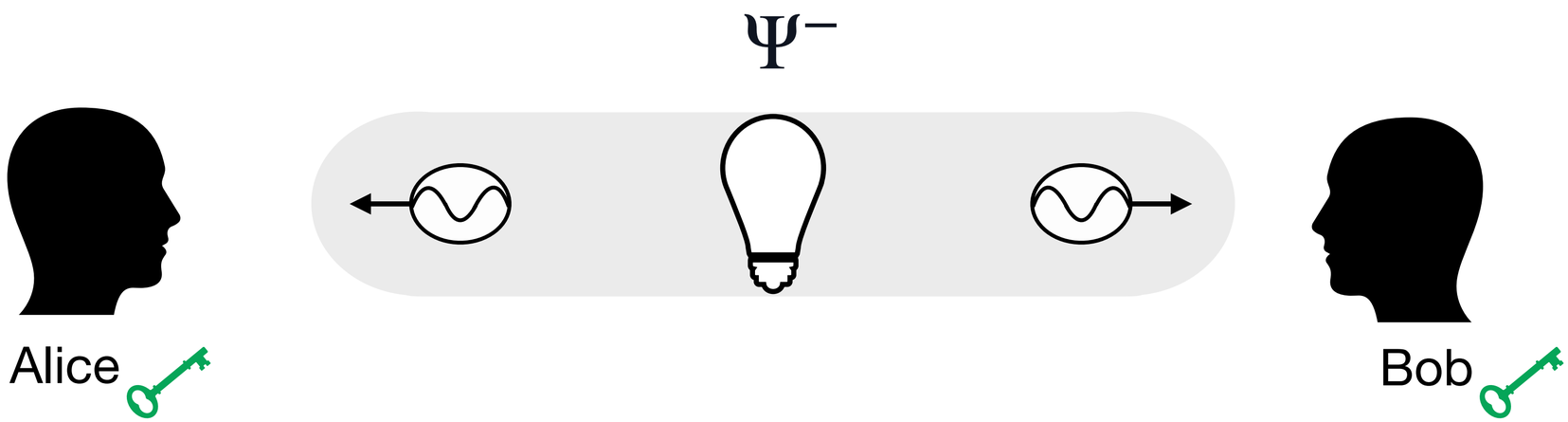
Combinaisons de bases utilisées: $(0°, 45°)\,(0°, 135°)\,(90°, 45°)\,(90°, 135°)$

Alice $\{0°, 90°\}$ $\{a_1, a_2\}$

Bob $\{45°, 135°\}$ $\{b_1, b_2\}$

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

Cas 1: Utilisation de paires de Bell



$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 \text{ Classique} \\ \in]2, 2\sqrt{2}] \text{ Maximum quantique} \end{cases}$$

Cas 2: Ève l’espionne écoute la conversation

Cas 2: Ève l’espionne écoute la conversation

Choix de base

45°

135°

90°

Cas 2: Ève l’espionne écoute la conversation

Choix de base	Résultat de mesure
45°	{0 ,1}
135°	{0 ,1}
90°	{0 ,1}

Cas 2: Ève l’espionne écoute la conversation

Choix de base	Résultat de mesure	Encodage
45°	{0 ,1}	{ $\|\searrow\rangle$, $\|\swarrow\rangle$ }
135°	{0 ,1}	{ $\|\searrow\rangle$, $\|\swarrow\rangle$ }
90°	{0 ,1}	{ $\|\leftrightarrow\rangle$, $\|\updownarrow\rangle$ }

Cas 2: Ève l’espionne écoute la conversation

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

Cas 2: Ève l'espionne écoute la conversation

$$S = |E_{a_1,b_1} + E_{a_2,b_1} + E_{a_2,b_2} - E_{a_1,b_2}| \begin{cases} \leq 2 & \text{Classique} \\ \in]2, 2\sqrt{2}] & \text{Maximum quantique} \end{cases}$$

Enjeux du nombre de mesures

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d’espion

Alice	Bob	
0°	45°	✓
0°	90°	
0°	135°	✓
45°	90°	
45°	135°	
90°	45°	✓
90°	135°	✓

Enjeux du nombre de mesures

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

$\frac{2}{9}$ ~ 22% Création de clé

Détection d’espion

Alice	Bob	
0°	45°	✓
0°	90°	
0°	135°	✓
45°	90°	
45°	135°	
90°	45°	✓
90°	135°	✓

Enjeux

Longueur de la clé

Enjeux du nombre de mesures

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

$\frac{2}{9}$ ~ 22% Création de clé

$\frac{4}{9}$ ~ 45% Détection d’espion

Détection d’espion

Alice	Bob	
0°	45°	✓
0°	90°	
0°	135°	✓
45°	90°	
45°	135°	
90°	45°	✓
90°	135°	✓

Enjeux

Longueur de la clé

Sécurité de la clé

Enjeux du nombre de mesures

Création de la clé symétrique

Alice	Bob
45°	45°
90°	90°

Détection d’espion

Alice	Bob	
0°	45°	✓
0°	90°	
0°	135°	✓
45°	90°	
45°	135°	
90°	45°	✓
90°	135°	✓

$\frac{2}{9}$ ~ 22% Création de clé

$\frac{4}{9}$ ~ 45% Détection d’espion

$\frac{3}{9}$ ~ 33% Poubelle

Enjeux

Longueur de la clé

Sécurité de la clé

Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

Plan

- Présentation
- Cryptographie
- Le qubit
- Le photon: messager d’information quantique
- Intrication et inégalité CHSH
- Protocole E91
- Atelier pratique

INSTITUT QUANTIQUE UdS

USHERBROOKE.CA/IQ

Plan

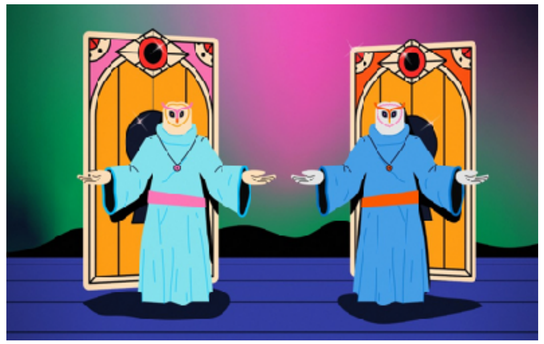
- [x] Présentation
- [x] Cryptographie
- [x] Le qubit
- [x] Le photon: messager d’information quantique
- [x] Intrication et inégalité CHSH
- [x] Protocole E91
- [ ] Atelier pratique

Partie pratique

https://github.com/algolab-quantique/CMAI-E91-Students.git

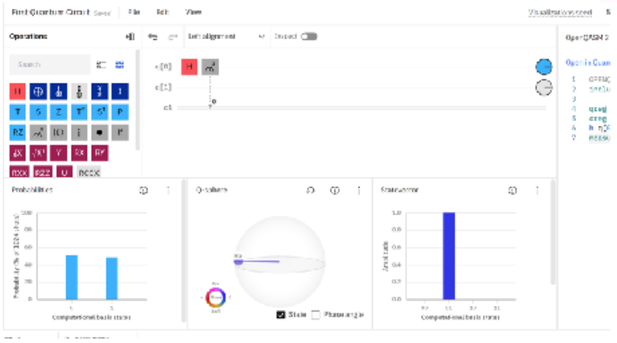
Conclusion

Références à consulter

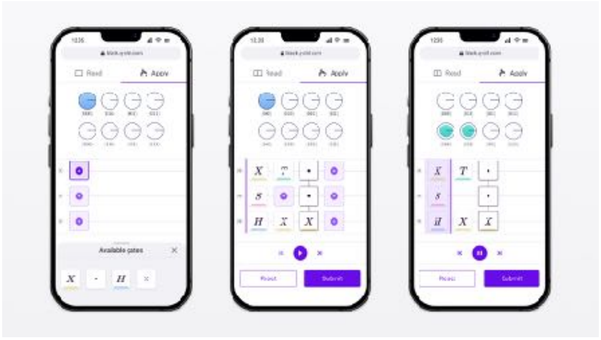


Les Énigmes quantiques (lien)

SkillsBuild (lien)



IBM Quantum learning (lien)



Black Opal de Q-CTRL (lien)

Azure Quantum katas (lien)

Inscription à l’infolettre

Lien examen

https://forms.office.com/r/LshFpNT8nE?origin=lprLink

Vous avez 24 heures pour compléter l’évaluation

INSTITUT QUANTIQUE UdS

INSTITUT POUR LA MOBILITÉ ET L’AÉROSPATIALE AU CANADA