Gott würfelt nicht

Albert Einstein vs Niels Bohr, 1927

Ce qu'il fallait retenir

Ce qu'il fallait retenir

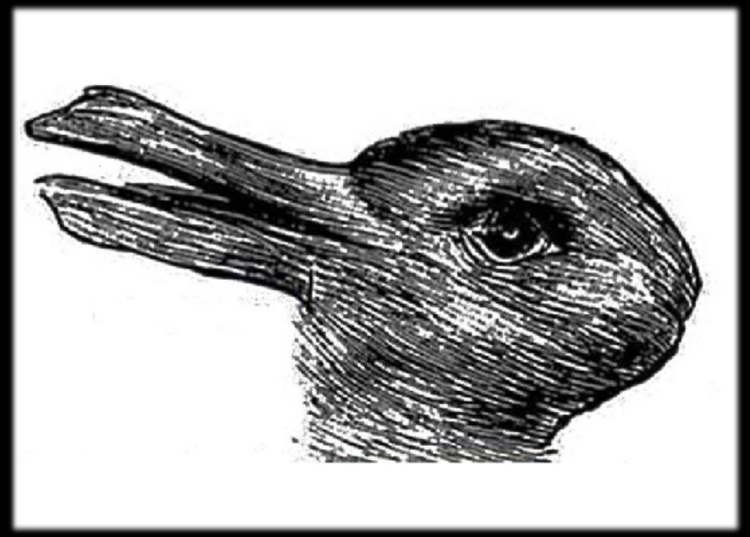
Gott würfelt nicht

et la sirène de Copenhague

Albert Einstein vs Niels Bohr, 1927

- Mécanique quantique = synthèse formelle et conceptuelle de la mécanique des matrices et de la mécanique ondulatoire
- Un formalisme redoutablement efficace
- Une interprétation très débattue : réalité quantique ? causalité quantique ? rôle de la mesure ? Dieu joue-t-il aux dés ?

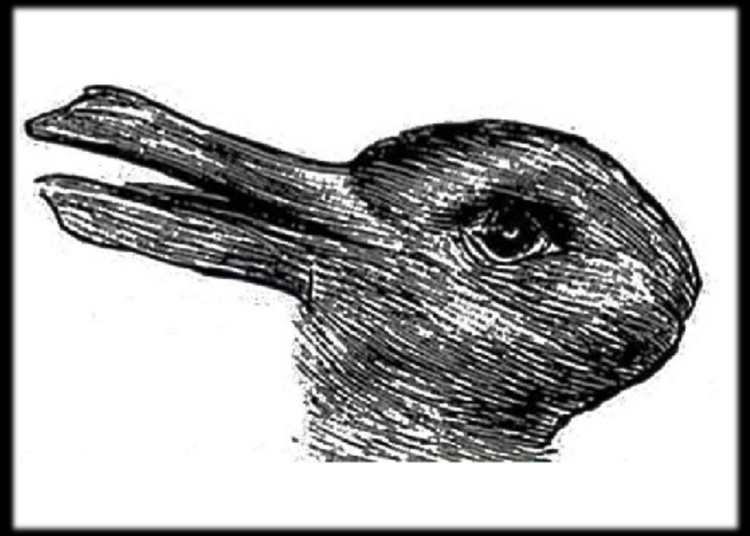
L'interprétation de Copenhague



- Pas de réalité objective sans mesure

$$|\text{image}\rangle = \frac{1}{\sqrt{2}}|\text{canard}\rangle + \frac{1}{\sqrt{2}}|\text{lapin}\rangle$$

L'interprétation de Copenhague



$$|\text{image}\rangle = \frac{1}{\sqrt{2}}|\text{canard}\rangle + \frac{1}{\sqrt{2}}|\text{lapin}\rangle$$

- Pas de réalité objective sans mesure
- Prédit la distribution de probabilité du résultat des mesures

L'interprétation de Copenhague

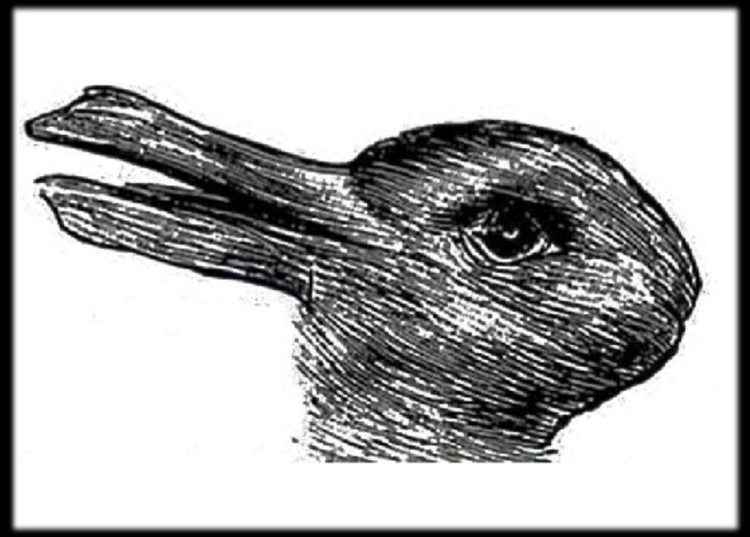
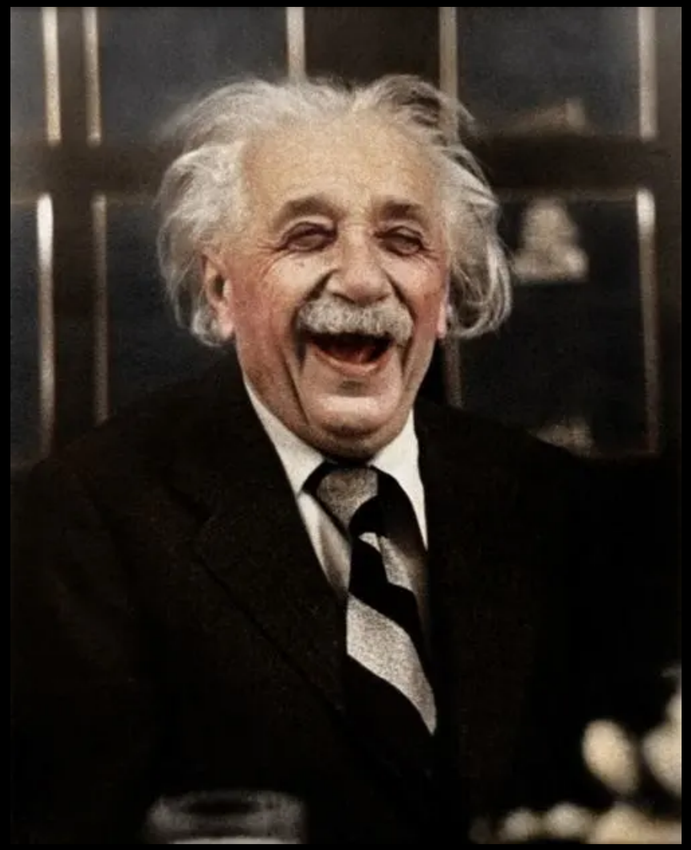


image = canard ou lapin

- Pas de réalité objective sans mesure
- Prédit la distribution de probabilité du résultat des mesures
- La mesure réduit le système à une seule des valeurs possibles

L'interprétation de Copenhague

- Pas de réalité objective sans mesure
- Prédit la distribution de probabilité du résultat des mesures
- La mesure réduit le système à une seule des valeurs possibles
- Principe d'indétermination (Heisenberg) + interprétation statistique (Born) + principe de complémentarité (Bohr)



De l'atome antique à l'atome quantique

La nature insolite de l'univers quantique

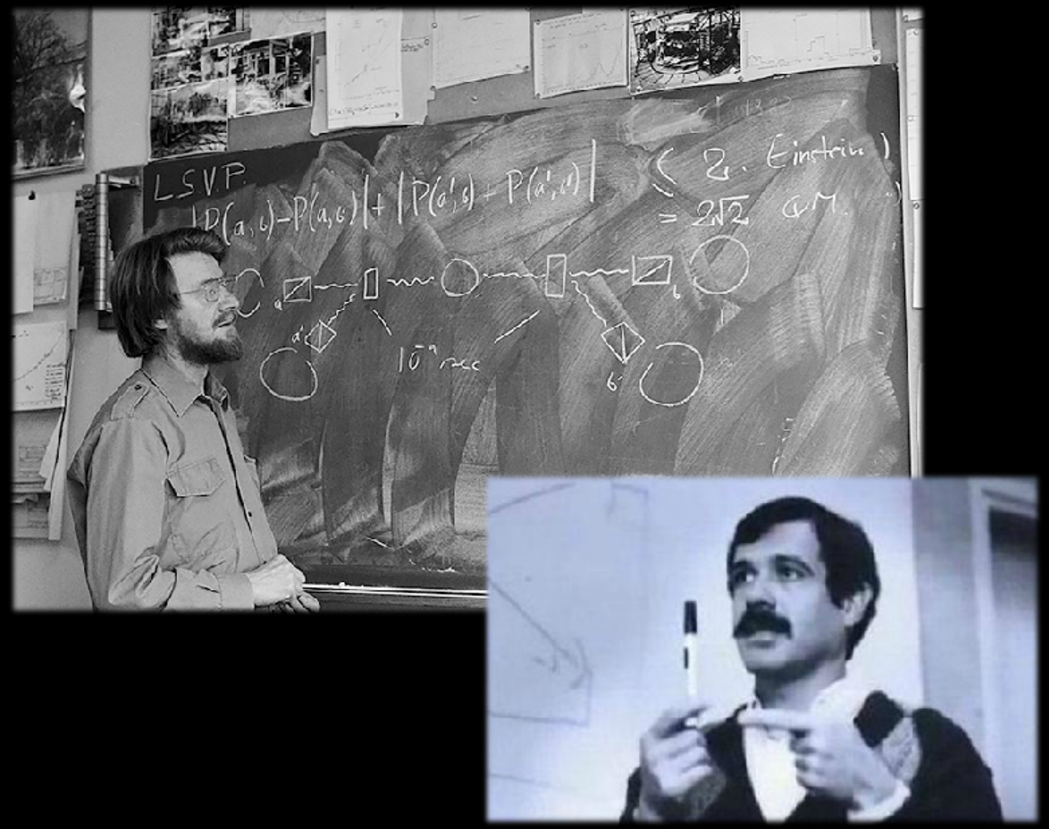
1. Il moto è come nullo, Galileo Galilei, 1610
2. Fiat quantum et photon fuit, Albert Einstein, 1905
3. Gott würfelt nicht, Albert Einstein vs Niels Bohr, 1927
4. Le jeu de Bell, Alain Aspect, 1982
5. La masse est dite ! CERN, 2012

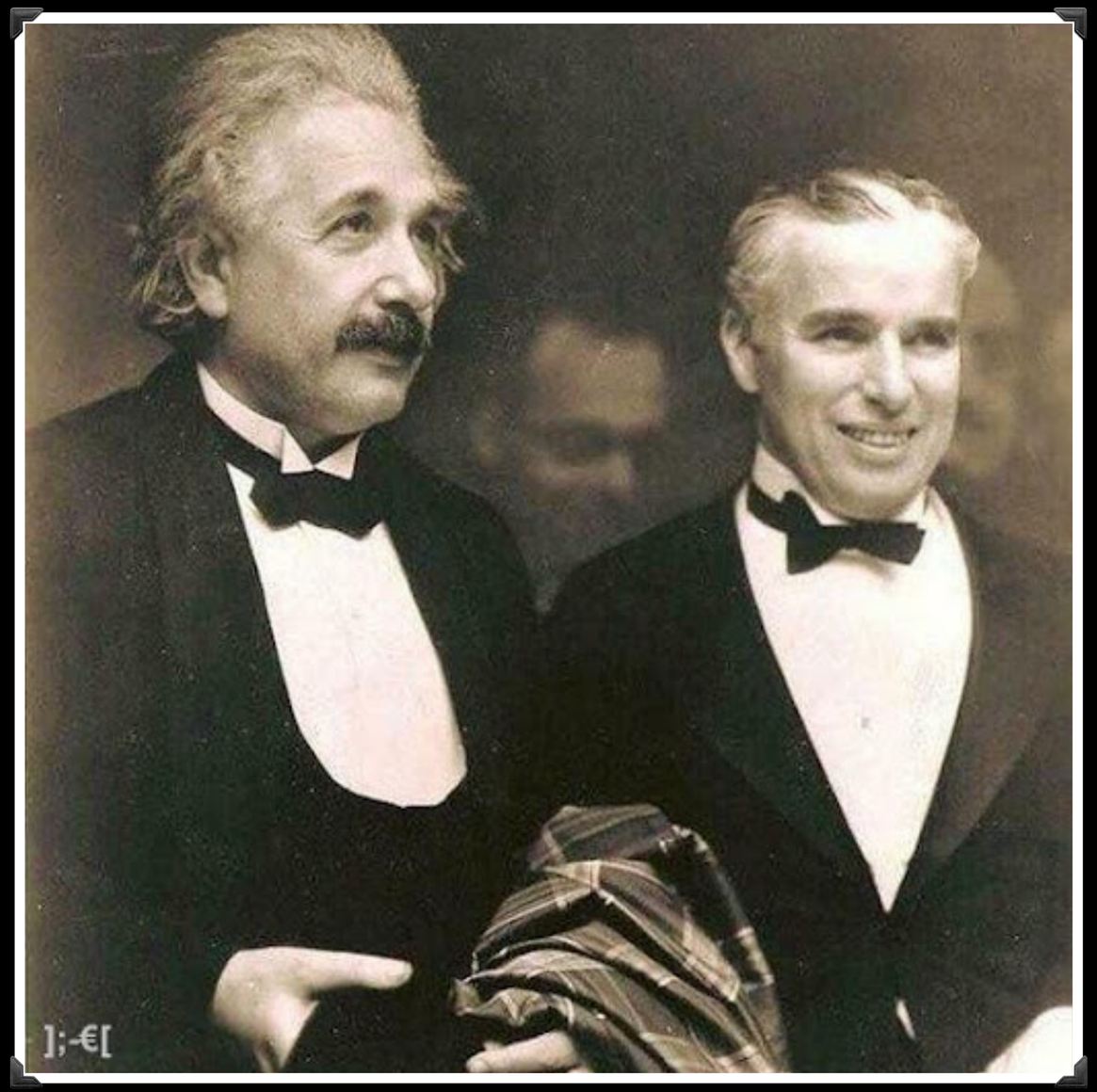
De l'atome antique à l'atome quantique

Epoque 4

Le jeu de Bell

Alain Aspect, 1982





Einstein, Podolski, Rosen (1935)

Einstein, Podolski, Rosen (1935)

The New York Times.

Copyright, 1935, by The New York Times Company.

Entered as Second-Class Matter, Postoffice, New York, N. Y.

NEW YORK, SATURDAY, MAY 4, 1935. P TWO CENTS

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

Einstein, Podolski, Rosen (1935)

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

In a complete theory there is an element corresponding to each element of reality. A sufficient condition for the reality of a physical quantity is the possibility of predicting it with certainty, without disturbing the system. In quantum mechanics in the case of two physical quantities described by non-commuting operators, the knowledge of one precludes the knowledge of the other. Then either (1) the description of reality given by the wave function in quantum mechanics is not complete or (2) these two quantities cannot have simultaneous reality. Consideration of the problem of making predictions concerning a system on the basis of measurements made on another system that had previously interacted with it leads to the result that if (1) is false then (2) is also false. One is thus led to conclude that the description of reality as given by a wave function is not complete.

Einstein, Podolski, Rosen (1935)

- EPR : critère de réalité physique → les particules individuelles sont des entités qui possèdent des propriétés propres, véhiculées avec elles.
- MQ : principe d'indétermination → x et p ne peuvent pas avoir de réalité simultanée.

EPR : expérience de pensée → x et p peuvent être déterminés simultanément !

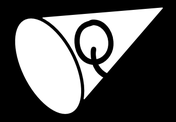
Einstein, Podolski, Rosen (1935)

Expérience de pensée

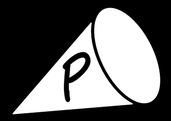
$$\Delta p \times \Delta q \geq \frac{h}{2\pi}$$

$Q_{mesuré} = x$

$P_{déduit} = -p$



$P_{mesuré} = p$



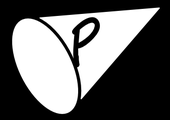
$p \quad -p$

Einstein, Podolski, Rosen (1935)

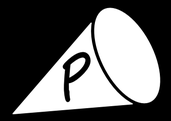
Expérience de pensée

$$\Delta p \times \Delta q \geq \frac{h}{2\pi}$$

$$\psi_{12} = \sum_n a_n |p_n p_n\rangle$$



$$\psi_2 = \sum a_n |p_n\rangle \rightarrow a_i |-p_i\rangle$$



$$\psi_1 = \sum a_n |p_n\rangle \rightarrow a_i |p_i\rangle$$ ..... bip .....

Einstein, Podolski, Rosen (1935)

Conclusion

- EPR : critère de réalité physique → les particules individuelles sont des entités qui possèdent des propriétés propres, véhiculées avec elles.
- ~~MQ : principe d'indétermination → x et p ne peuvent pas avoir de réalité simultanée.~~

EPR : La physique quantique est incomplète + variables cachées

Einstein, Podolski, Rosen (1935)

Réponse de Bohr

OCTOBER 15, 1935 PHYSICAL REVIEW VOLUME 48

Can Quantum-Mechanical Description of Physical Reality be Considered Complete?

N. BOHR, *Institute for Theoretical Physics, University, Copenhagen*

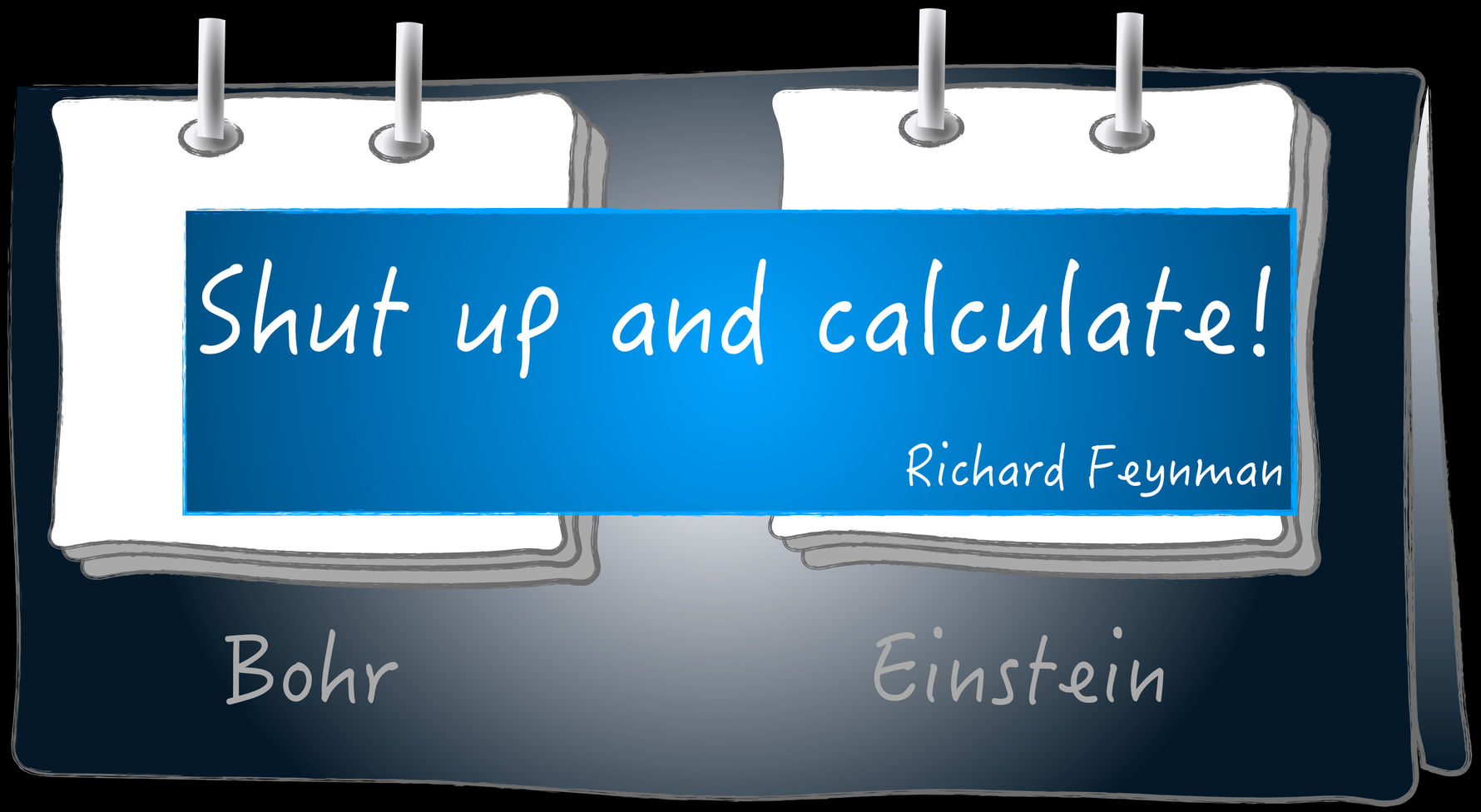
(Received July 13, 1935)

It is shown that a certain "criterion of physical reality" formulated in a recent article with the above title by A. Einstein, B. Podolsky and N. Rosen contains an essential ambiguity when it is applied to quantum phenomena. In this connection a viewpoint termed "complementarity" is explained from which quantum-mechanical description of physical phenomena would seem to fulfill, within its scope, all rational demands of completeness.

Einstein, Podolski, Rosen (1935)

Réponse de Bohr

- **non séparabilité** : l'ensemble des deux particules et des deux appareils de mesure constituent un tout inséparable (intrication)
- **non localité** : la mesure portant sur une particule réagit instantanément sur l'état de l'autre particule éloignée

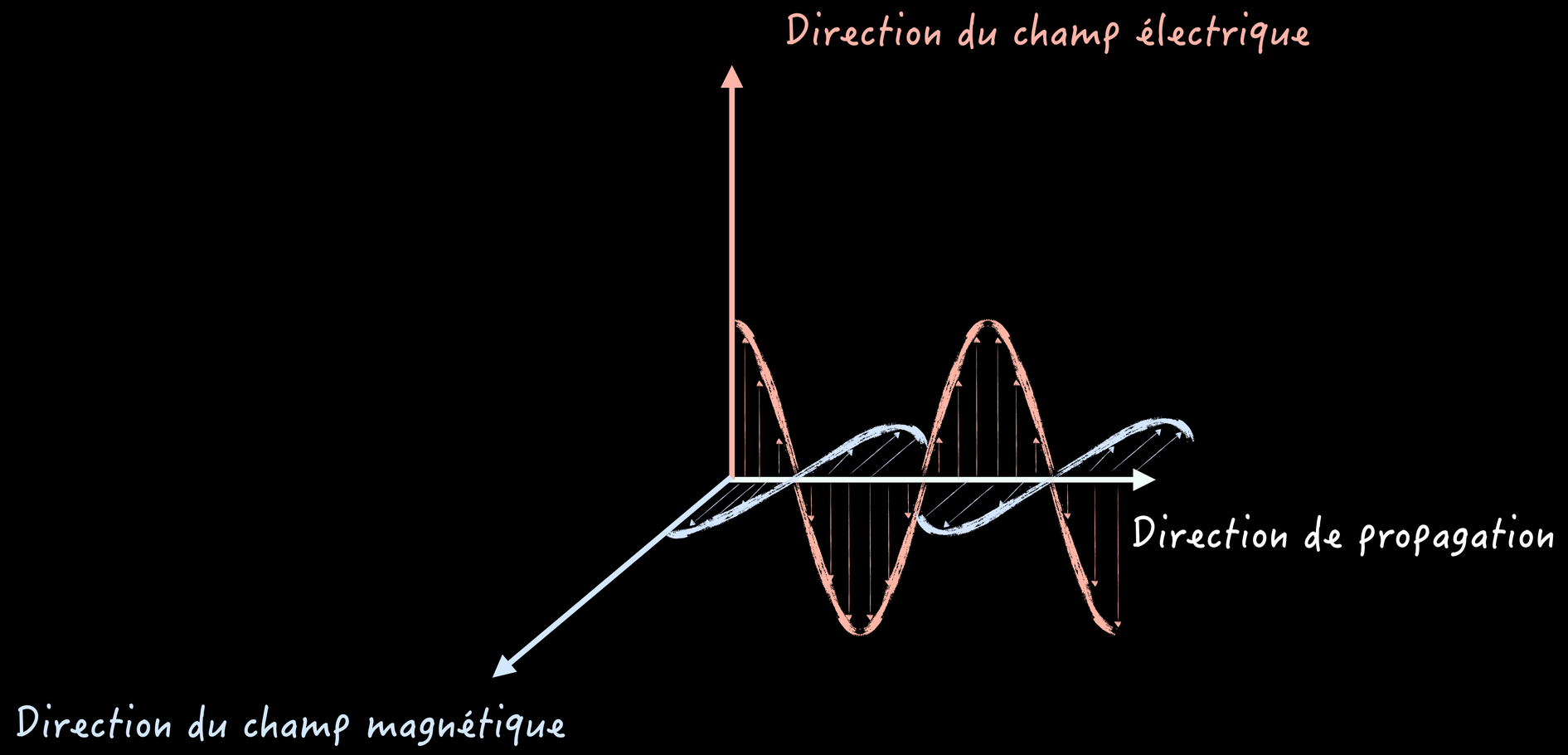

Shut up and calculate!
Richard Feynman
Bohr
Einstein

VIRTH
RFEF
CTA

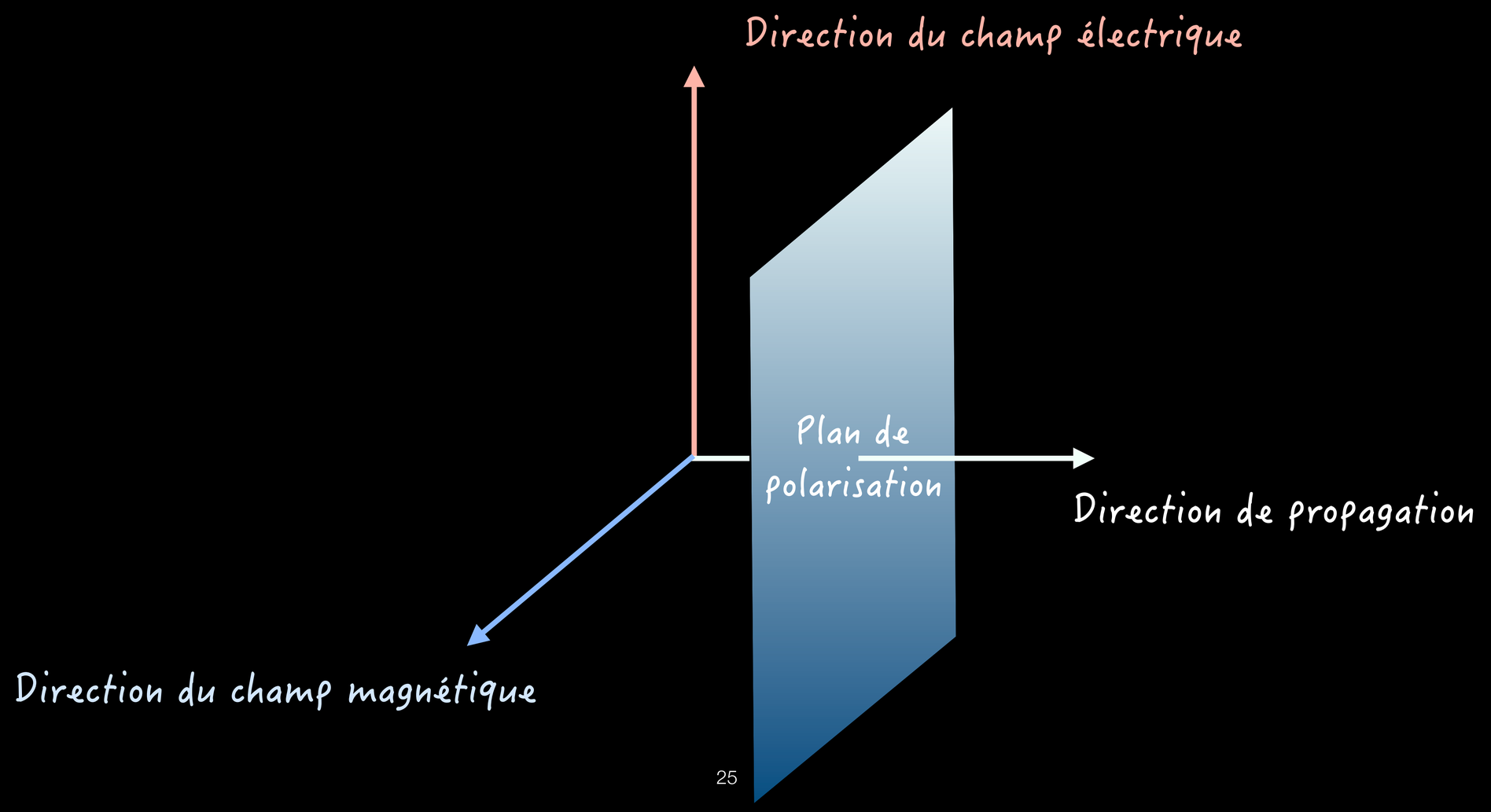
Polarisation de la lumière

b.a - ba

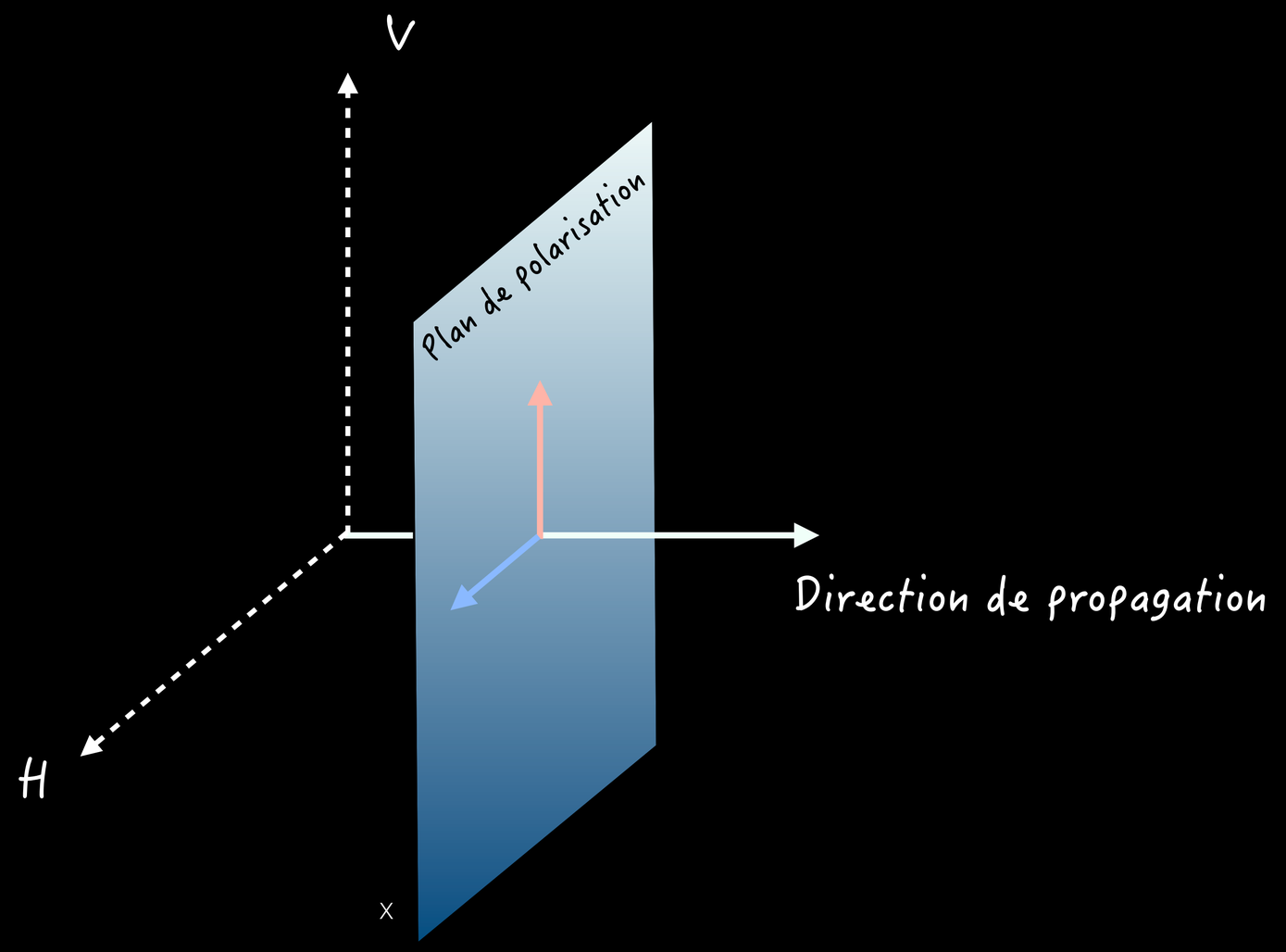
Lumière = onde électromagnétique (Maxwell)



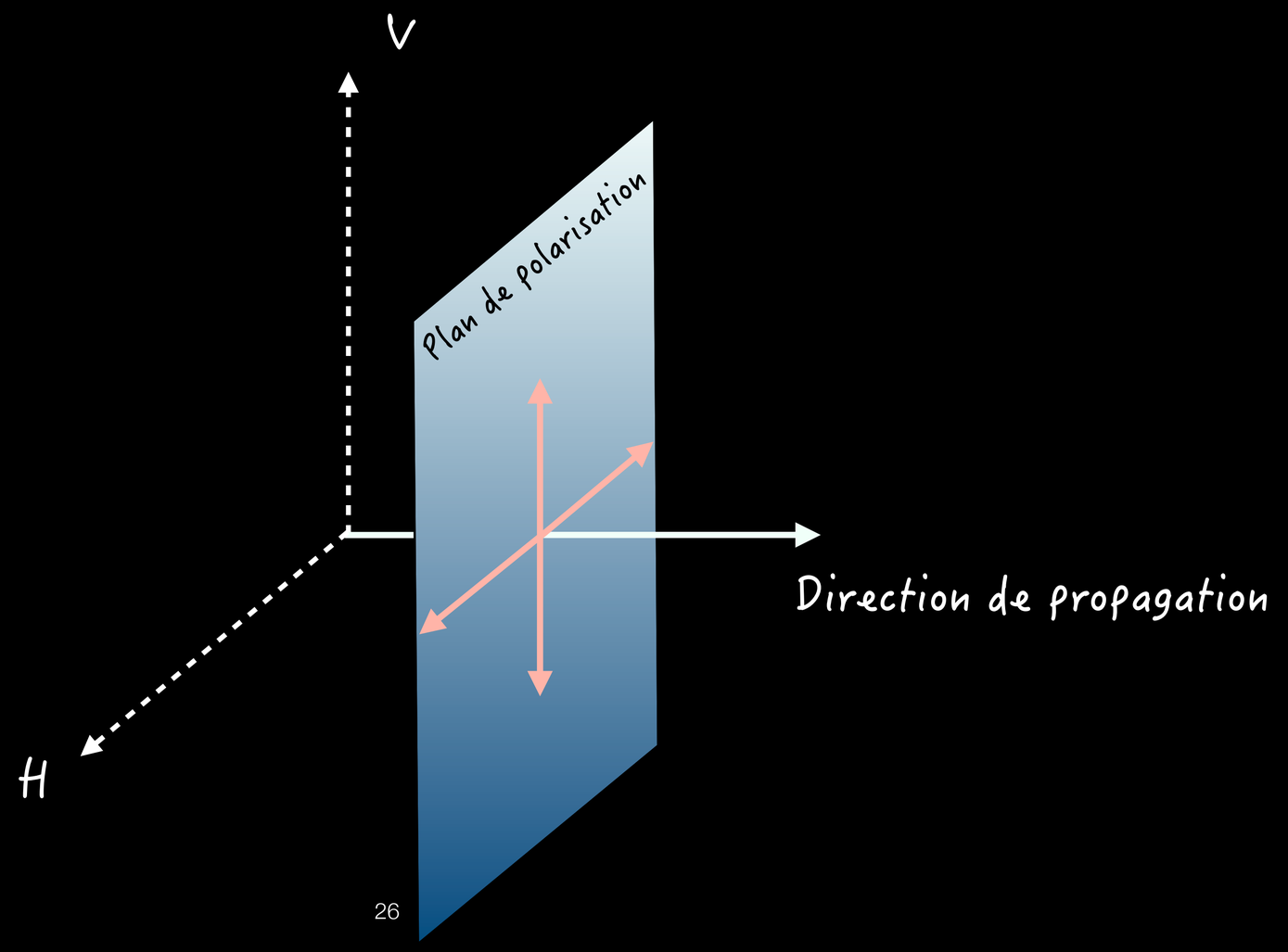
Plan de polarisation



Plan de polarisation

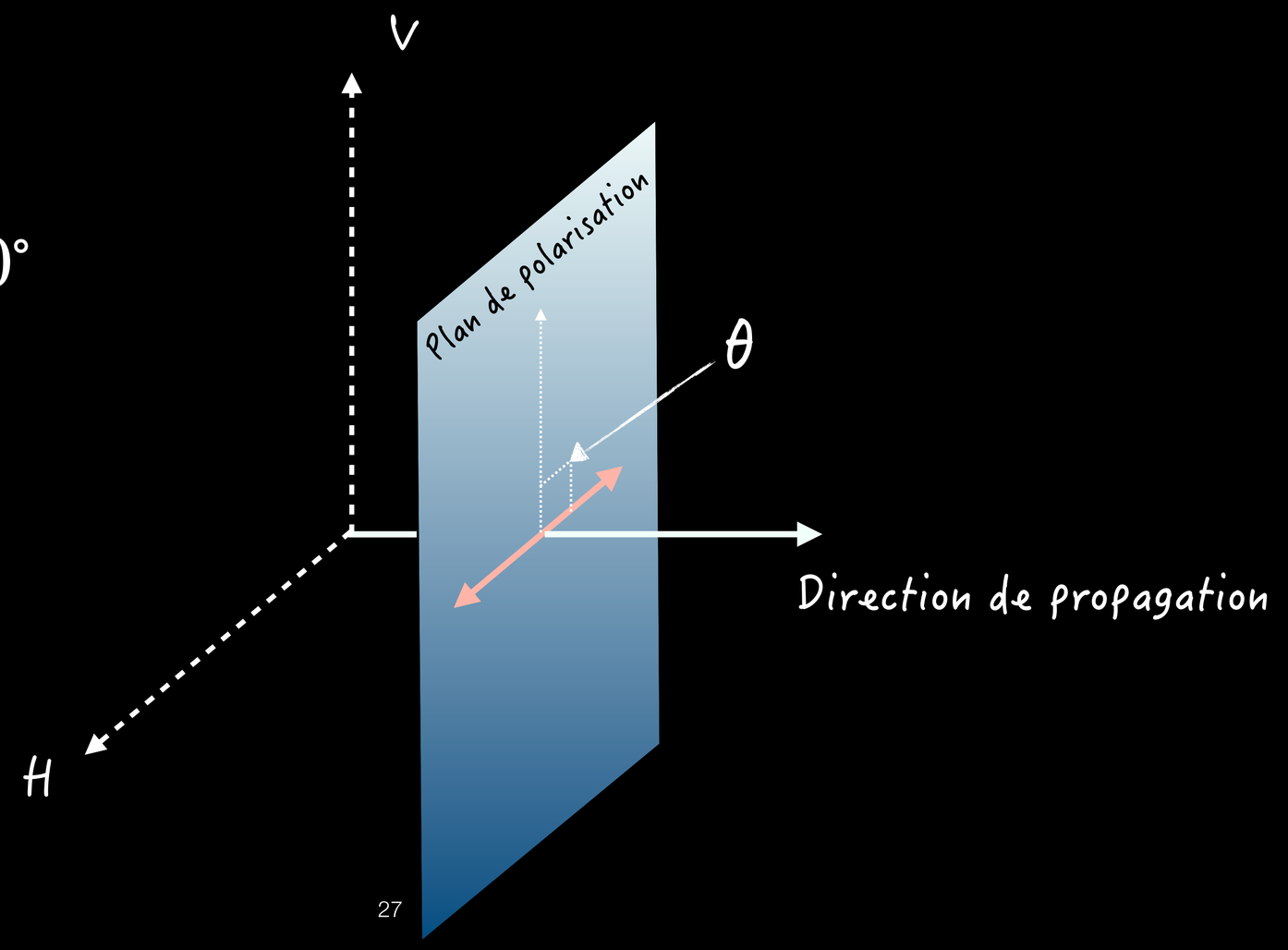


Plan de polarisation



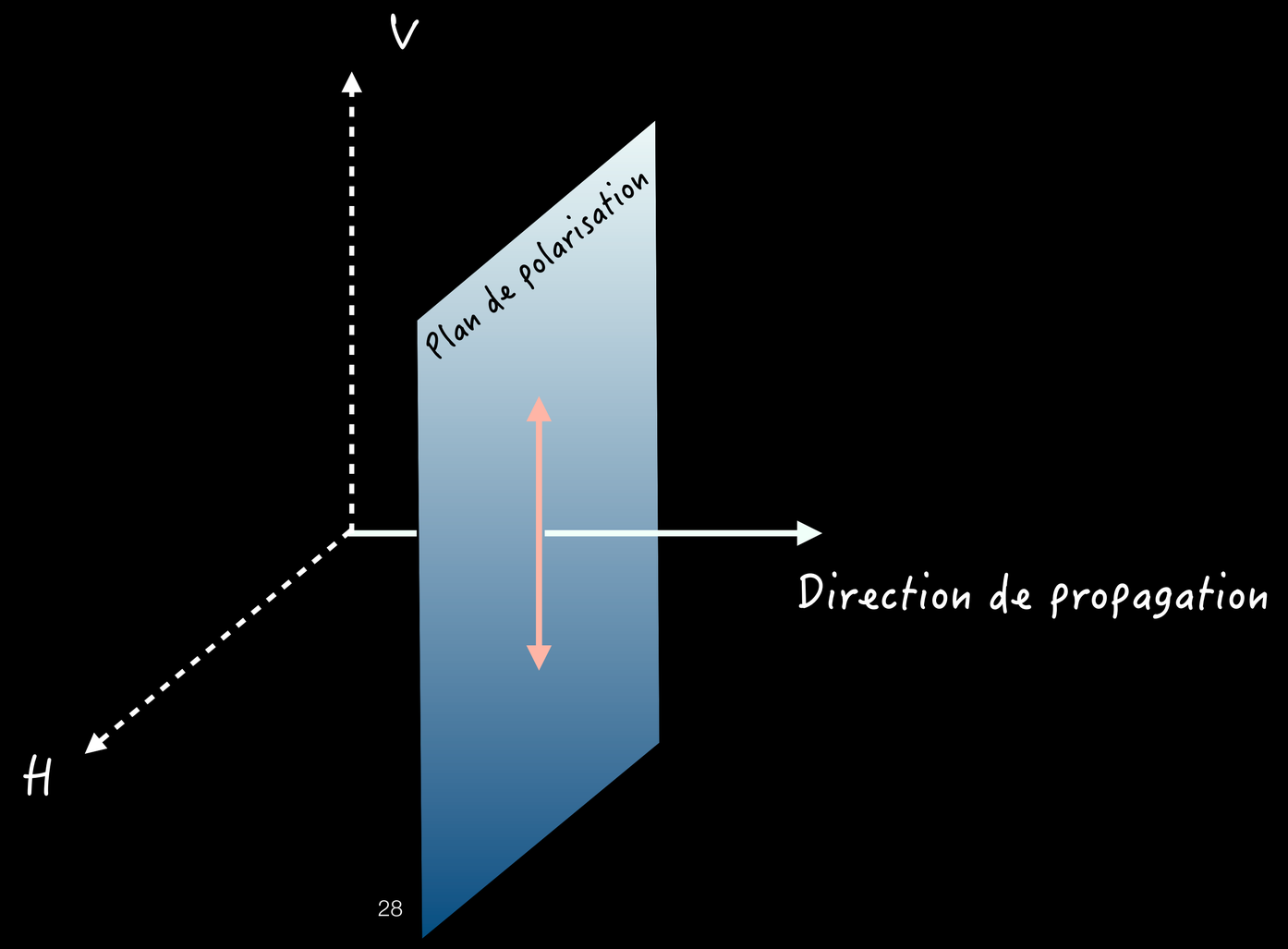
Polarisation horizontale H

$$H \rightarrow \theta = 90^\circ$$



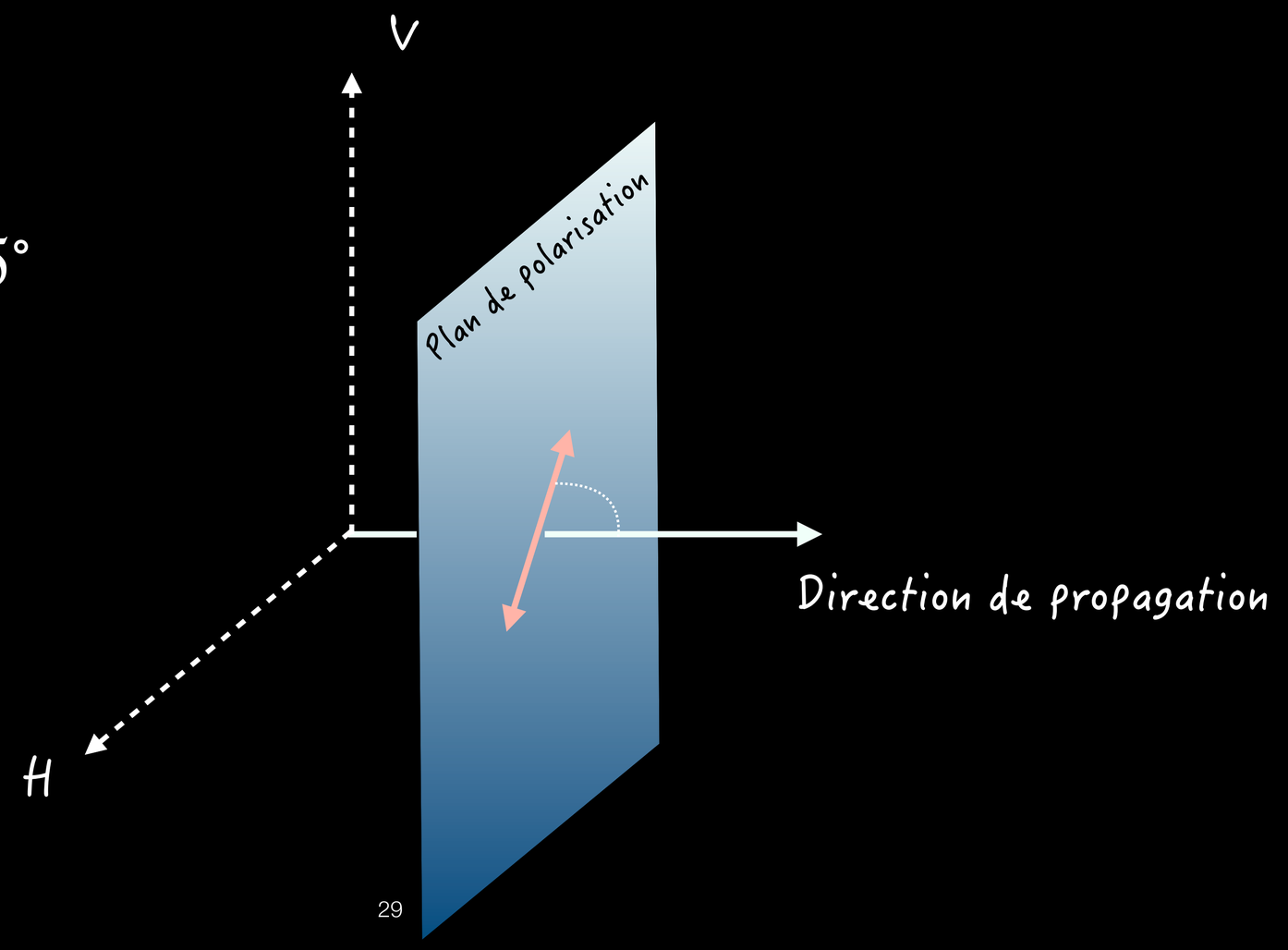
Polarisation verticale V

$$V \rightarrow \theta = 0^\circ$$



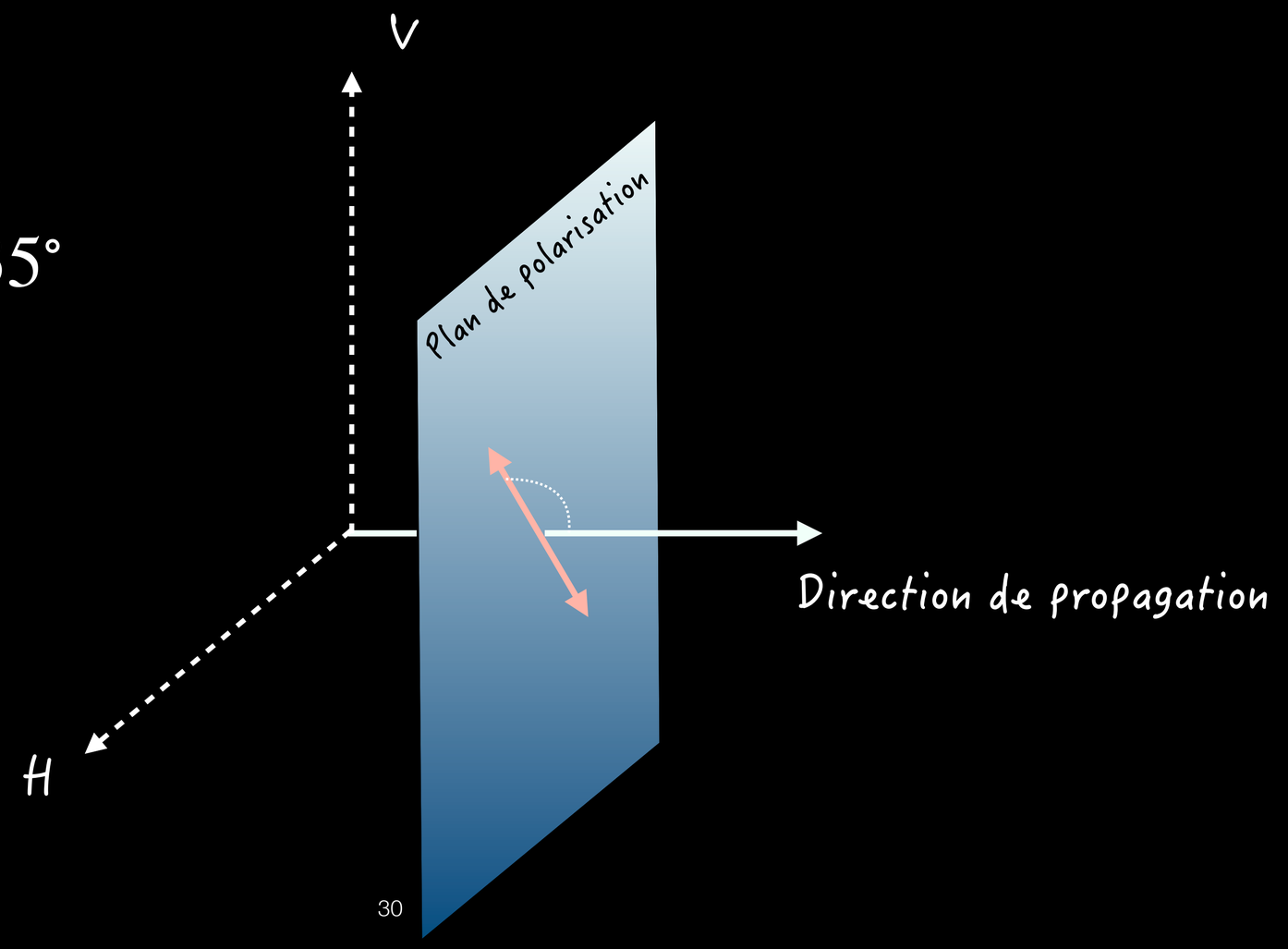
Polarisation diagonale D

$$D \rightarrow \theta = 45°$$



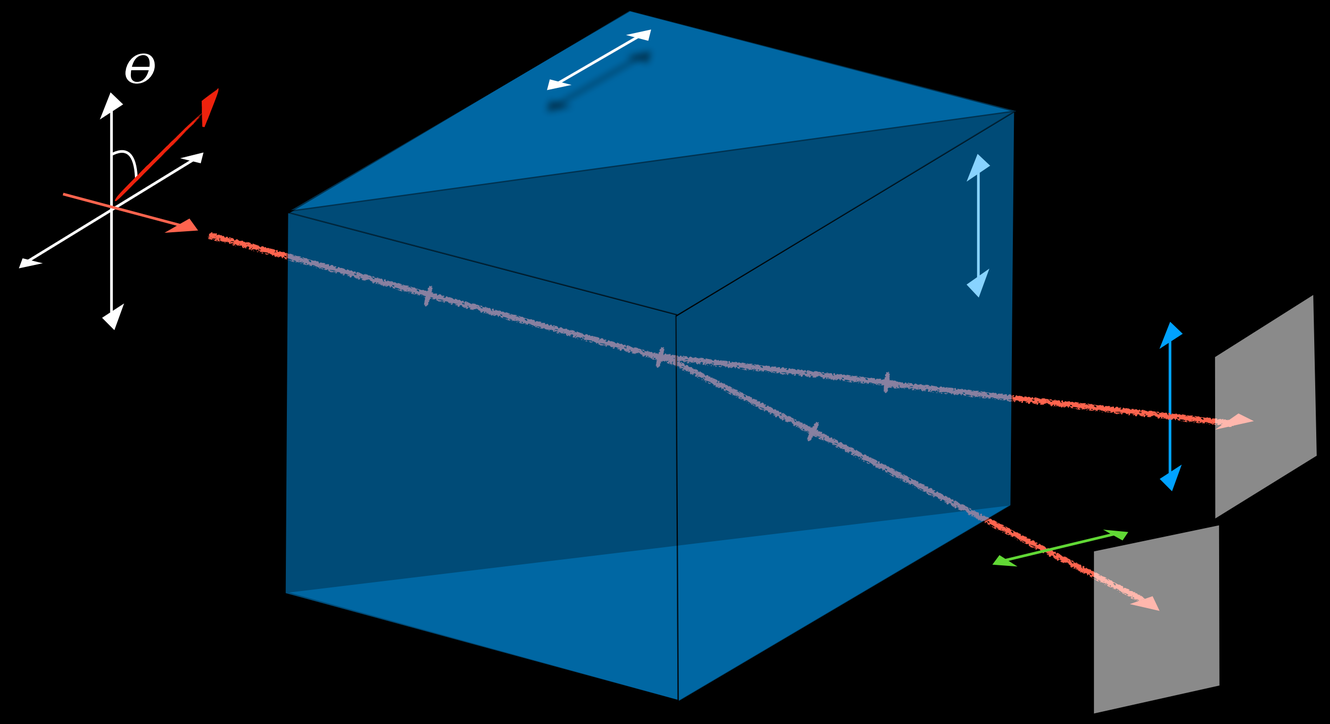
Polarisation diagonale A

$$A \rightarrow \theta = 135^\circ$$



Polariseur

faisceau de lumière

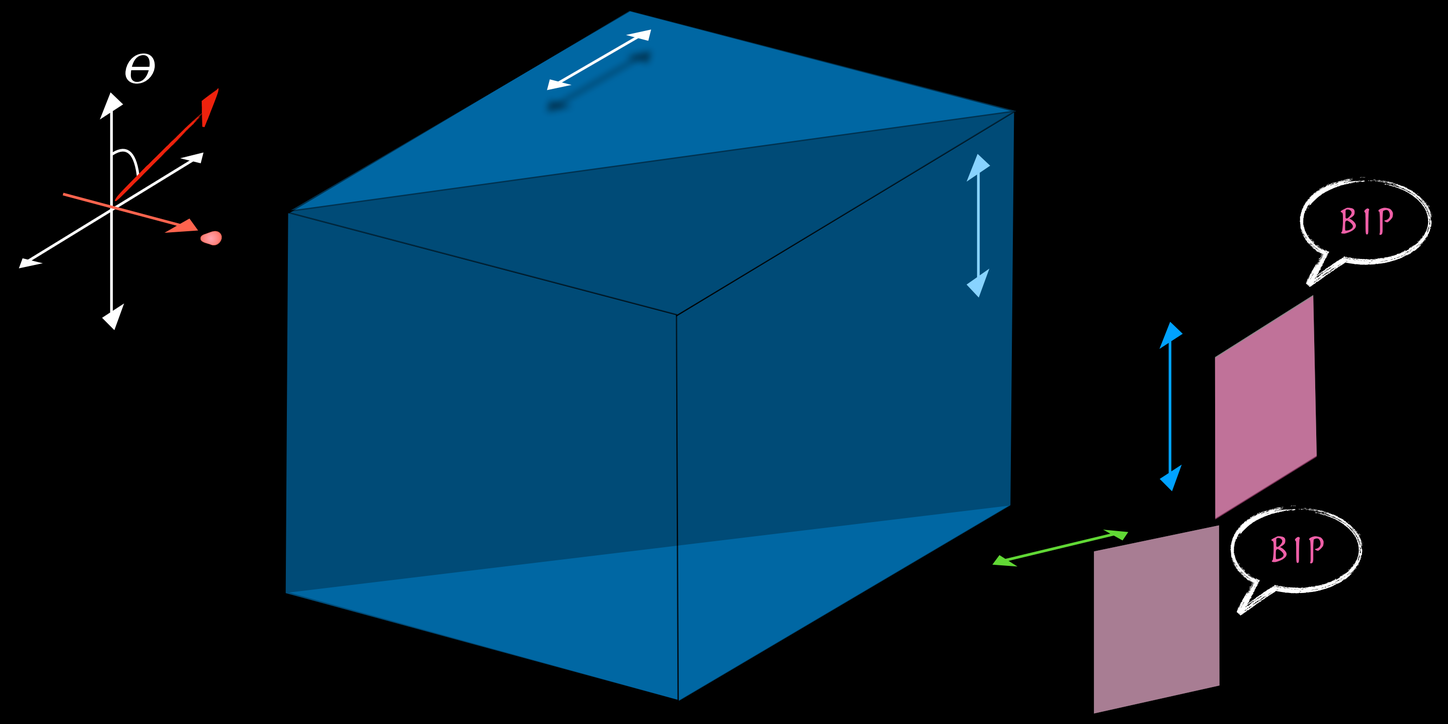


$$I_V = I_{incident} \times \cos^2\theta$$

$$I_H = I_{incident} \times \sin^2\theta$$

Polariseur

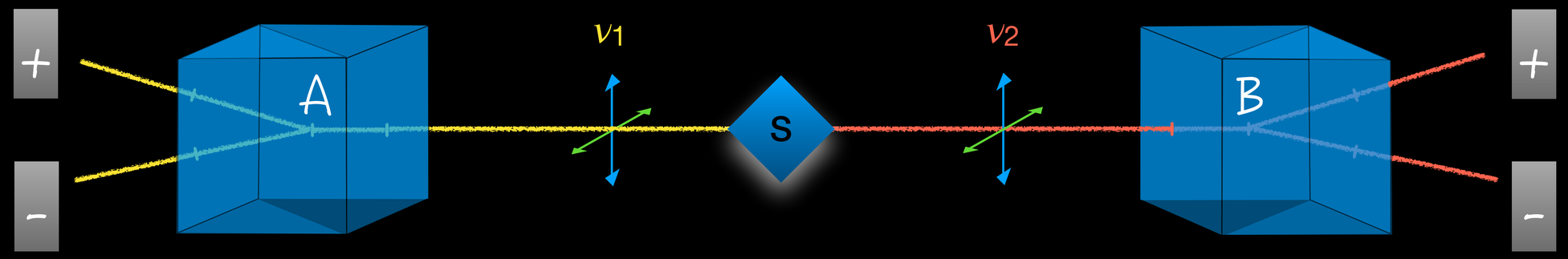
photon unique



V	H	
1	0	$P = \cos^2\theta$
0	1	$P = \sin^2\theta$

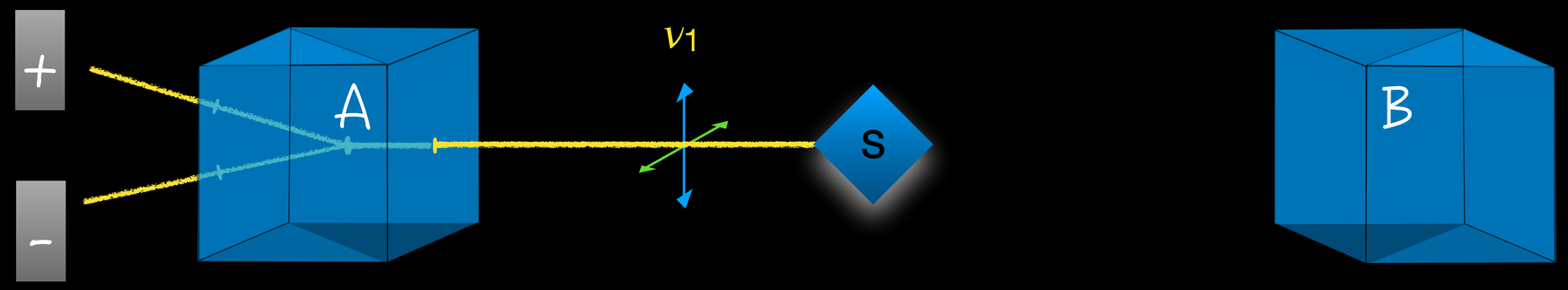
Photons intriqués

$$\psi(\nu_1, \nu_2) = \frac{1}{\sqrt{2}} |HH> + \frac{1}{\sqrt{2}} |VV>$$



Photons intriqués

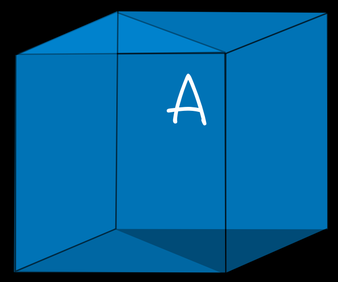
$$\psi(\nu_1) = \frac{1}{\sqrt{2}}|H> + \frac{1}{\sqrt{2}}|V>$$

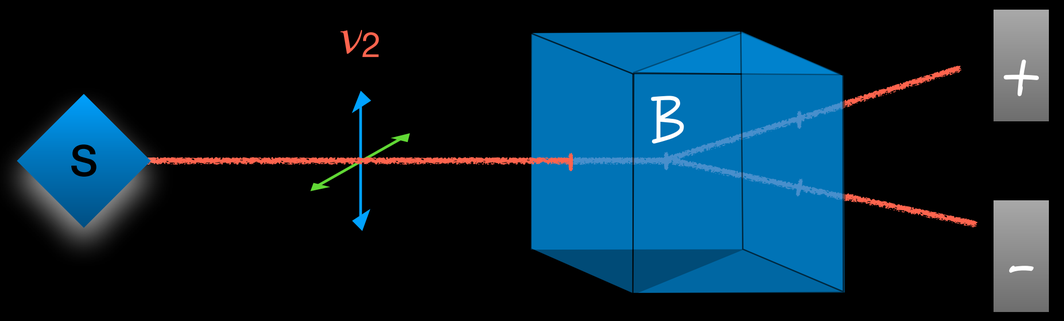


P_{A+}	$\frac{1}{2}$
P_{A-}	$\frac{1}{2}$

Photons intriqués

$$\psi(\nu_2) = \frac{1}{\sqrt{2}}|H> + \frac{1}{\sqrt{2}}|V> \quad P = |\psi|^2$$

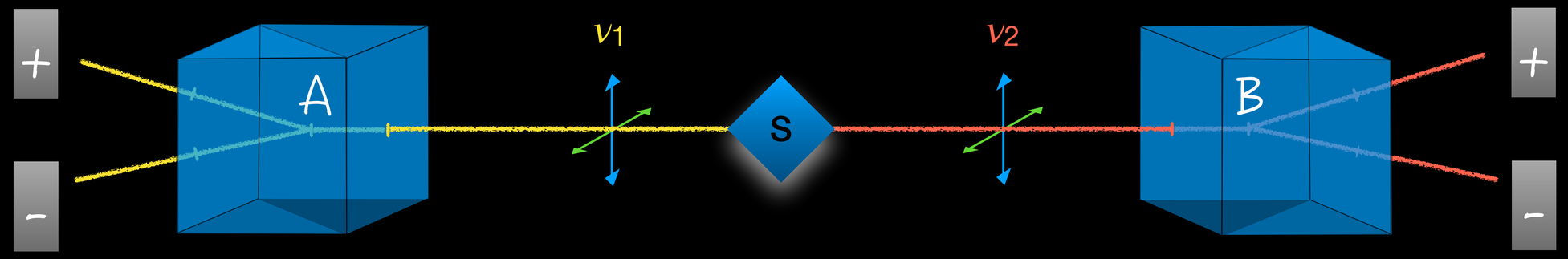




P_{A+}	$\frac{1}{2}$
P_{A-}	$\frac{1}{2}$
P_{B+}	$\frac{1}{2}$
P_{B-}	$\frac{1}{2}$

Photons intriqués

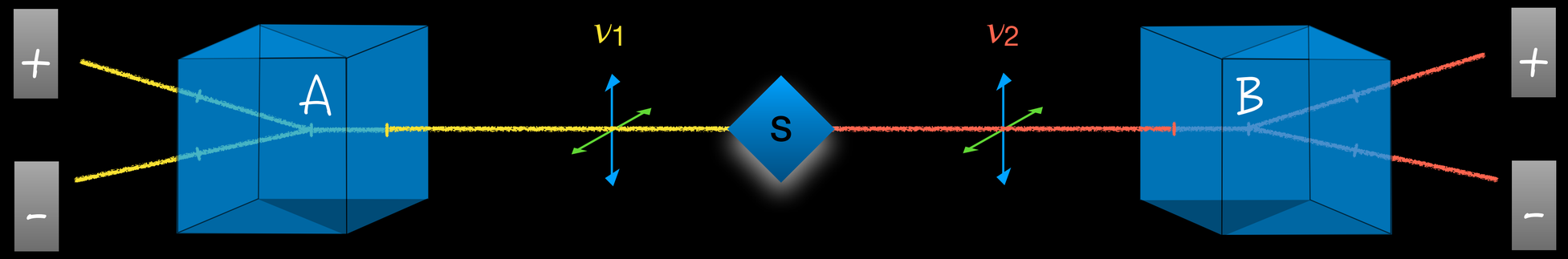
$$\psi(\nu_1, \nu_2) = \frac{1}{\sqrt{2}}|HH> + \frac{1}{\sqrt{2}}|VV>$$



P_{A+}	$\frac{1}{2}$	P_{A+B+}	$\frac{1}{2}$
P_{A-}	$\frac{1}{2}$	P_{A-B-}	$\frac{1}{2}$
P_{B+}	$\frac{1}{2}$		
P_{B-}	$\frac{1}{2}$		

Photons intriqués

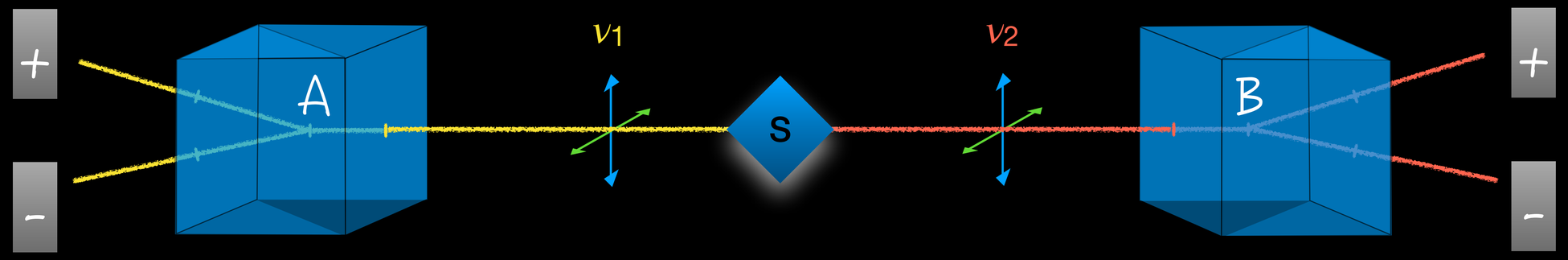
$$\psi(\nu_1, \nu_2) = \frac{1}{\sqrt{2}}|HH> + \frac{1}{\sqrt{2}}|VV>$$



P_{A+}	$\frac{1}{2}$	P_{A+B+}	$\frac{1}{2}$
P_{A-}	$\frac{1}{2}$	P_{A-B-}	$\frac{1}{2}$
P_{B+}	$\frac{1}{2}$	P_{B+A-}	0
P_{B-}	$\frac{1}{2}$	P_{B-A+}	0

Photons intriqués

$$\psi(\nu_1, \nu_2) = \frac{1}{\sqrt{2}}|HH> + \frac{1}{\sqrt{2}}|VV>$$



$$\phi_{AB} = 0$$

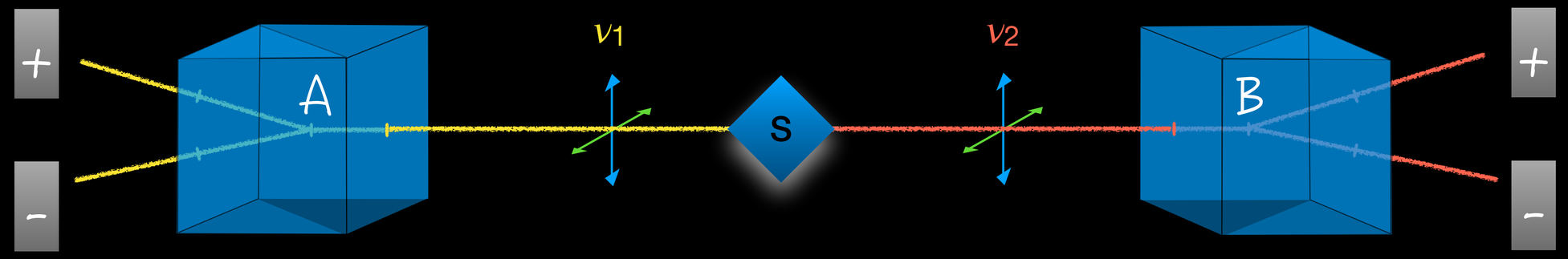
P_{A+}	$\frac{1}{2}$	P_{A+B+}	$\frac{1}{2}$
P_{A-}	$\frac{1}{2}$	P_{A-B-}	$\frac{1}{2}$
P_{B+}	$\frac{1}{2}$	P_{B+A-}	0
P_{B-}	$\frac{1}{2}$	P_{B-A+}	0

$$= \frac{1}{2}\cos^2\phi_{AB}$$

$$= \frac{1}{2}\sin^2\phi_{AB}$$

Photons intriqués

$$\psi(\nu_1, \nu_2) = \frac{1}{\sqrt{2}}|HH> + \frac{1}{\sqrt{2}}|VV>$$

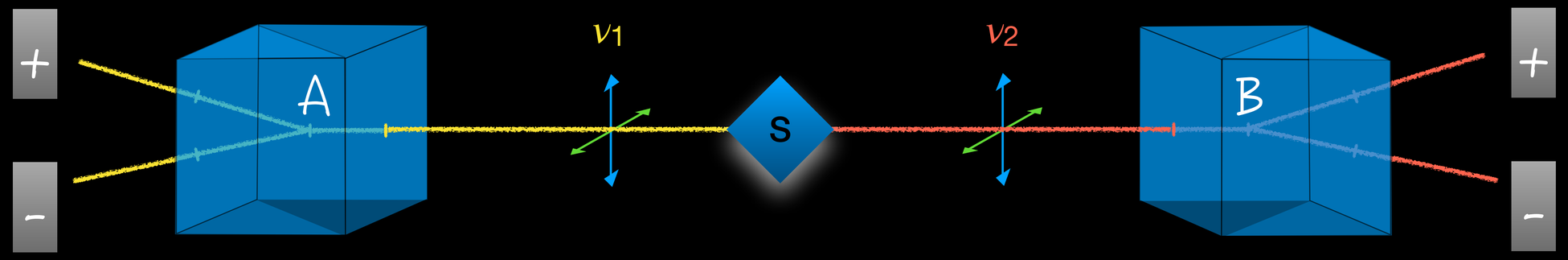


	$\phi_{AB} = 0$
P_{A+B+}	$\frac{1}{2}$
P_{A-B-}	$\frac{1}{2}$
P_{A-B+}	0
P_{A+B-}	0

$$E_{MQ} = P_{A+B+} + P_{A-B-} - P_{A-B+} - P_{A+B-}$$
$$= 1$$

Photons intriqués

$$\psi(\nu_1, \nu_2) = \frac{1}{\sqrt{2}}|HH> + \frac{1}{\sqrt{2}}|VV>$$



$\phi_{AB} = 0$

P_{A+B+}	$\frac{1}{2}$	$= \frac{1}{2}\cos^2\phi_{AB}$
P_{A-B-}	$\frac{1}{2}$	
P_{A-B+}	0	$= \frac{1}{2}\sin^2\phi_{AB}$
P_{A+B-}	0	

$$E_{MQ} = P_{A+B+} + P_{A-B-} - P_{A-B+} - P_{A+B-}$$
$$= \cos 2\phi_{AB}$$

John Bell (1928-1990)

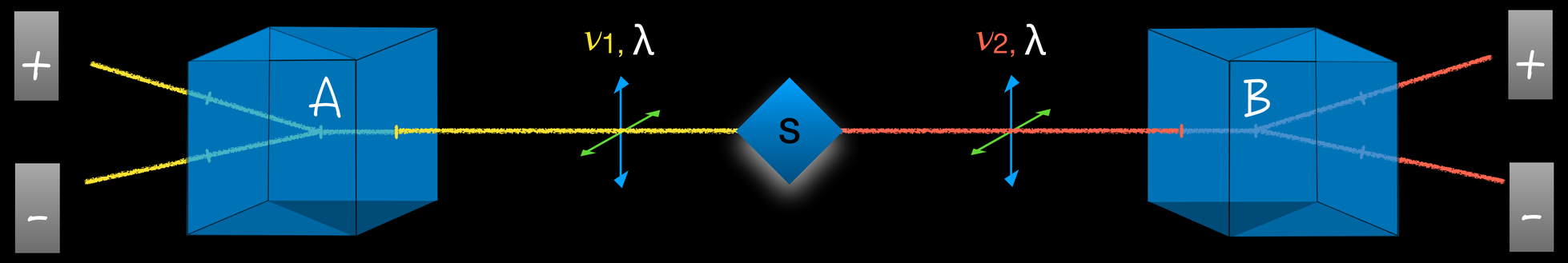
John Bell

Théorie locale à variables cachées

- Localité : si un événement est la cause d'un autre, alors il faut que la distance entre les deux événements puisse être parcourue à une vitesse finie inférieure ou égale à la vitesse de la lumière
- Variable cachée : il existe une réalité dans la fonction d'onde qui, si on la connaissait, nous permettrait de prédire exactement le résultat de la mesure.

John Bell (1964)

Le jeu



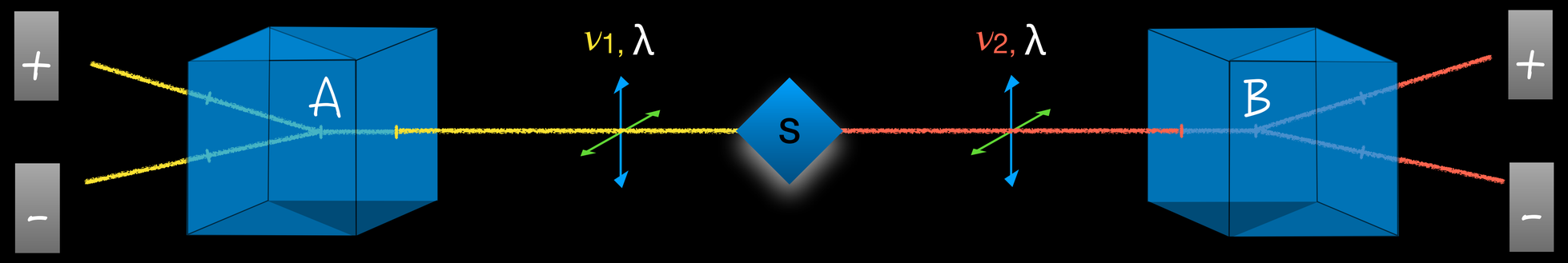
1. Mesure en A n'influe pas la mesure en B

2. Mesure ne dépend pas de l'orientation relative A et B

3. λ ne dépend pas de la configuration de A et B

John Bell (1964)

Le jeu



1. Mesure en A n'influe pas la mesure en B
2. Mesure ne dépend pas de l'orientation relative A et B
3. λ ne dépend pas de la configuration de A et B

$$-2 \leq E(A_1, B_1) - E(A_1, B_2) + E(A_2, B_1) + E(A_2, B_2) \leq 2$$

$E_{MQ} = P_{A+B+} + P_{A-B-} - P_{A-B+} - P_{A+B-}$

$(A1, B1) = (A2, B1) = (A2, B2) = \phi$ et $(A1, B2) = 3\phi$

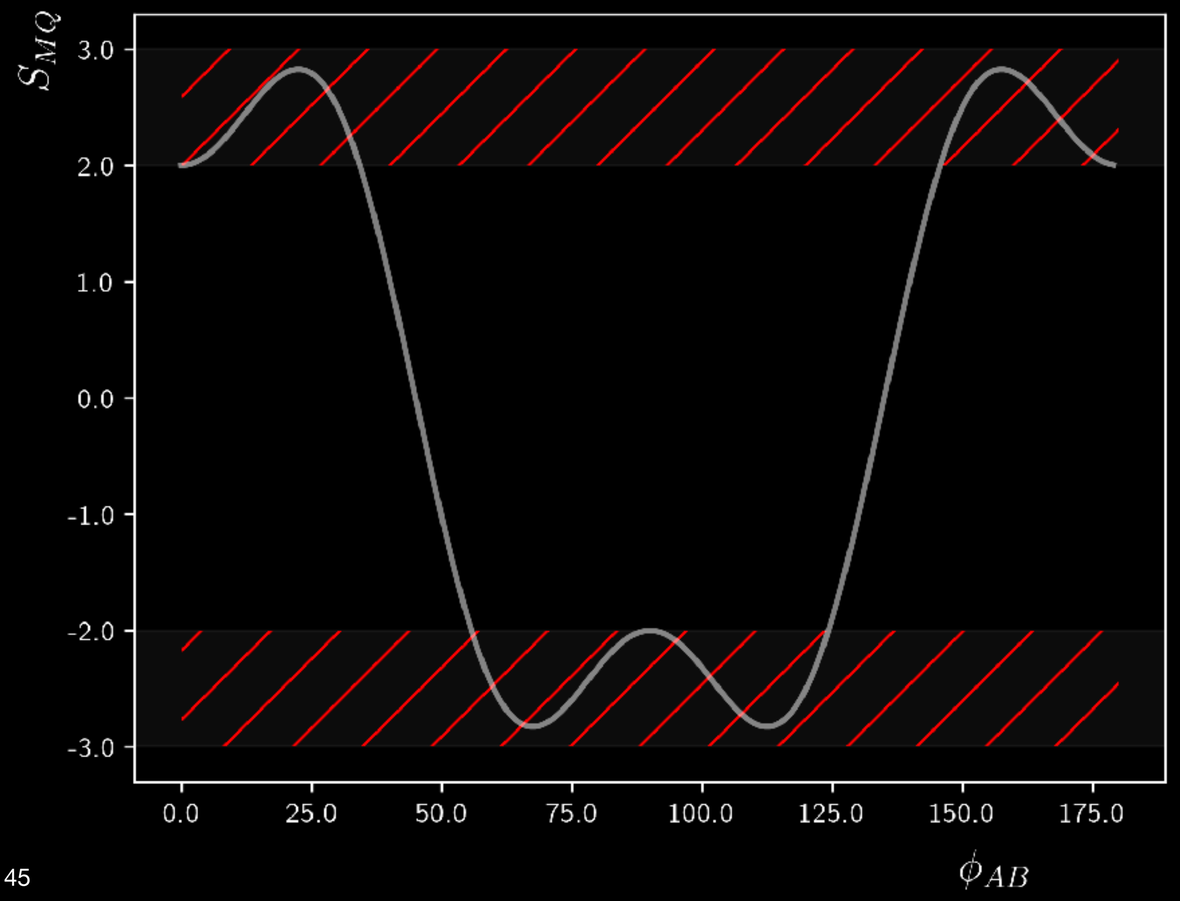
John Bell (1964)

Variable cachée & réalisme local vs Mécanique Quantique

$$-2 \leq E(A_1, B_1) - E(A_1, B_2) + E(A_2, B_1) + E(A_2, B_2) \leq 2$$

$$E_{MQ}(A,B) = \cos 2\phi_{AB}$$

$$S_{MQ} = 3\cos 2\phi_{AB} - \cos 6\phi_{AB}$$



$(A1, B1) = (A2, B1) = (A2, B2) = \phi$ et $(A1, B2) = 3\phi$

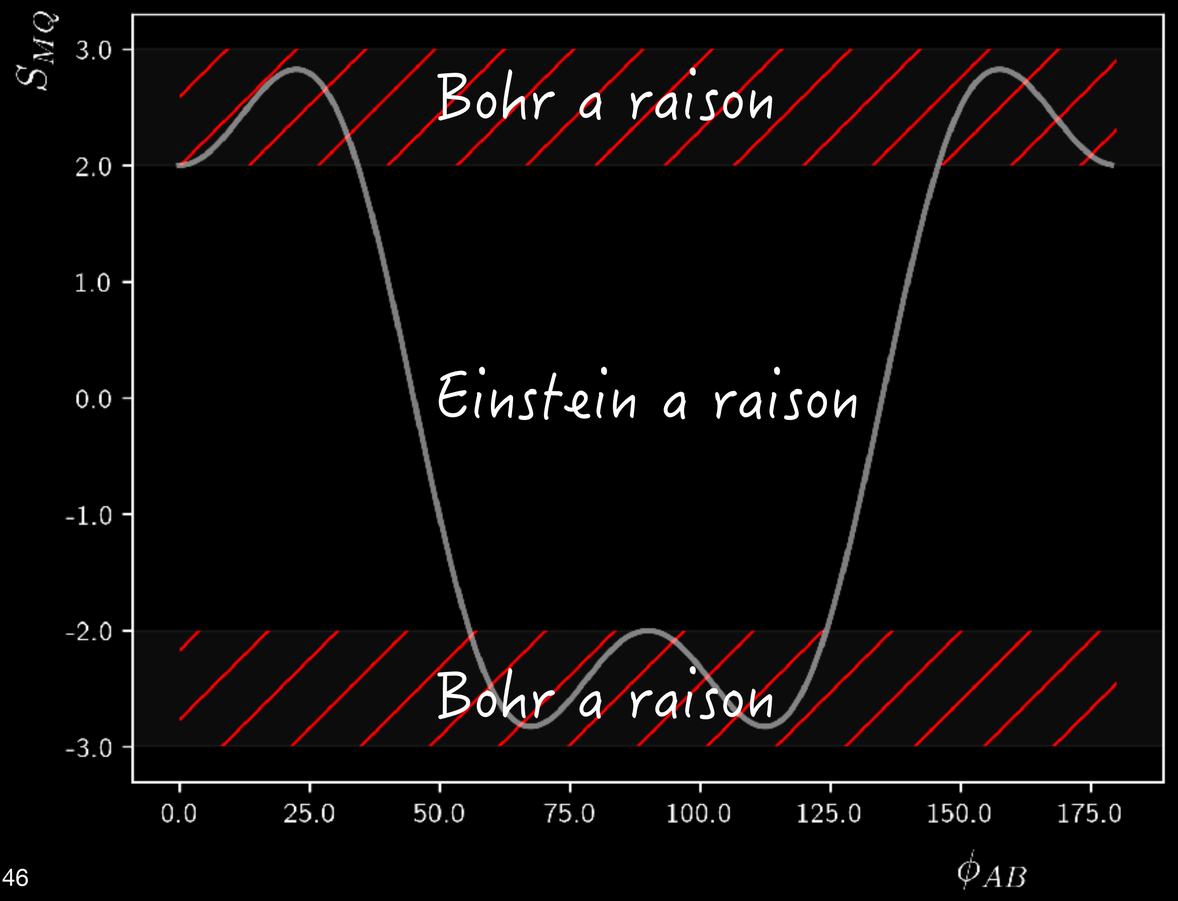
John Bell (1964)

Variable cachée & réalisme local vs Mécanique Quantique

$$-2 \leq E(A_1, B_1) - E(A_1, B_2) + E(A_2, B_1) + E(A_2, B_2) \leq 2$$

$$E_{MQ}(A,B) = \cos 2\phi_{AB}$$

$$S_{MQ} = 3\cos 2\phi_{AB} - \cos 6\phi_{AB}$$



$(A1, B1) = (A2, B1) = (A2, B2) = \phi$ et $(A1, B2) = 3\phi$

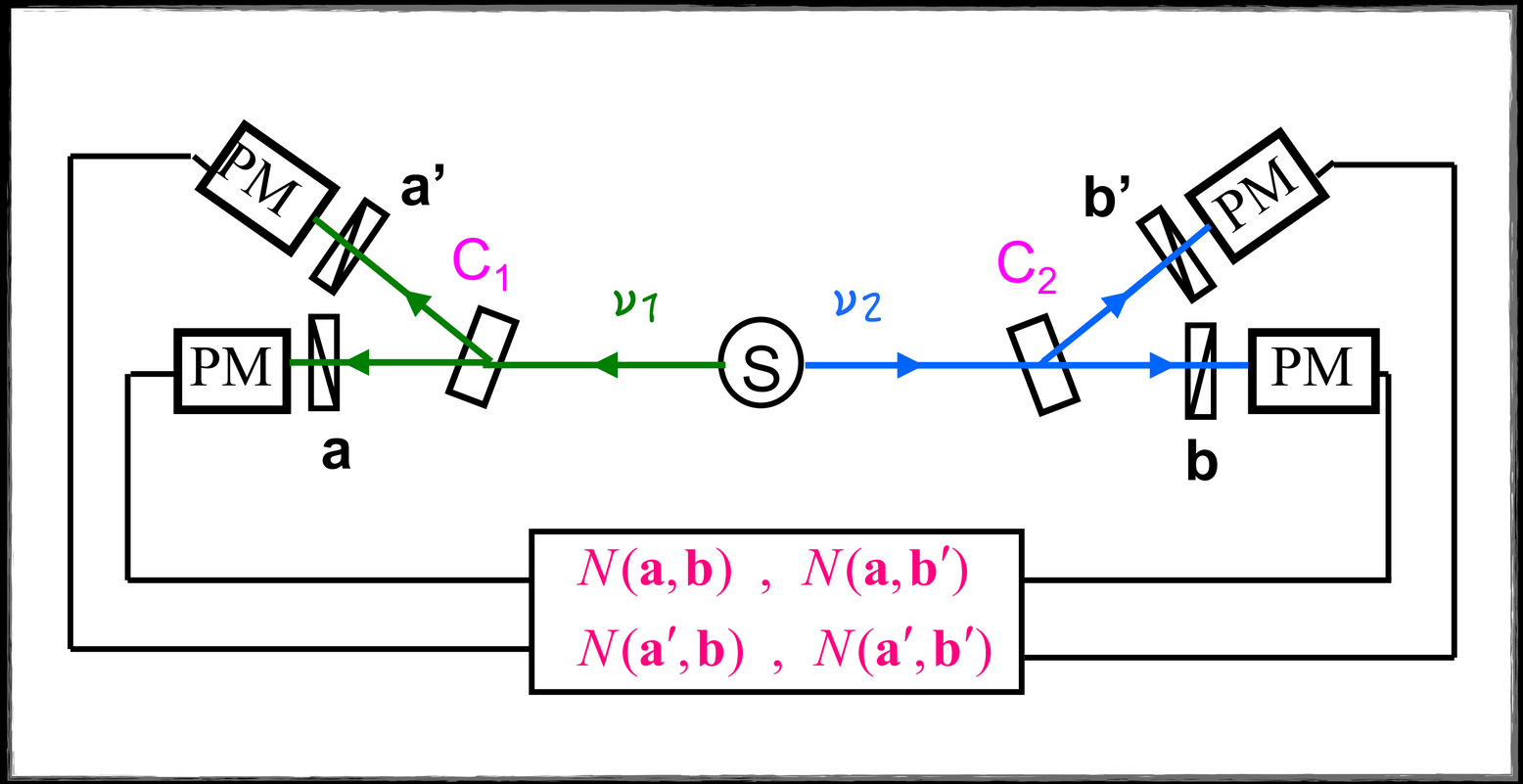
Alain Aspect (1947-)

Alain Aspect (1982)

Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,[a] and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France

(Received 27 September 1982)

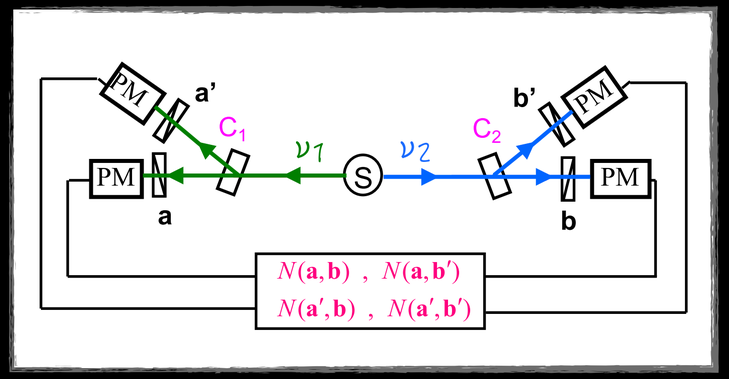


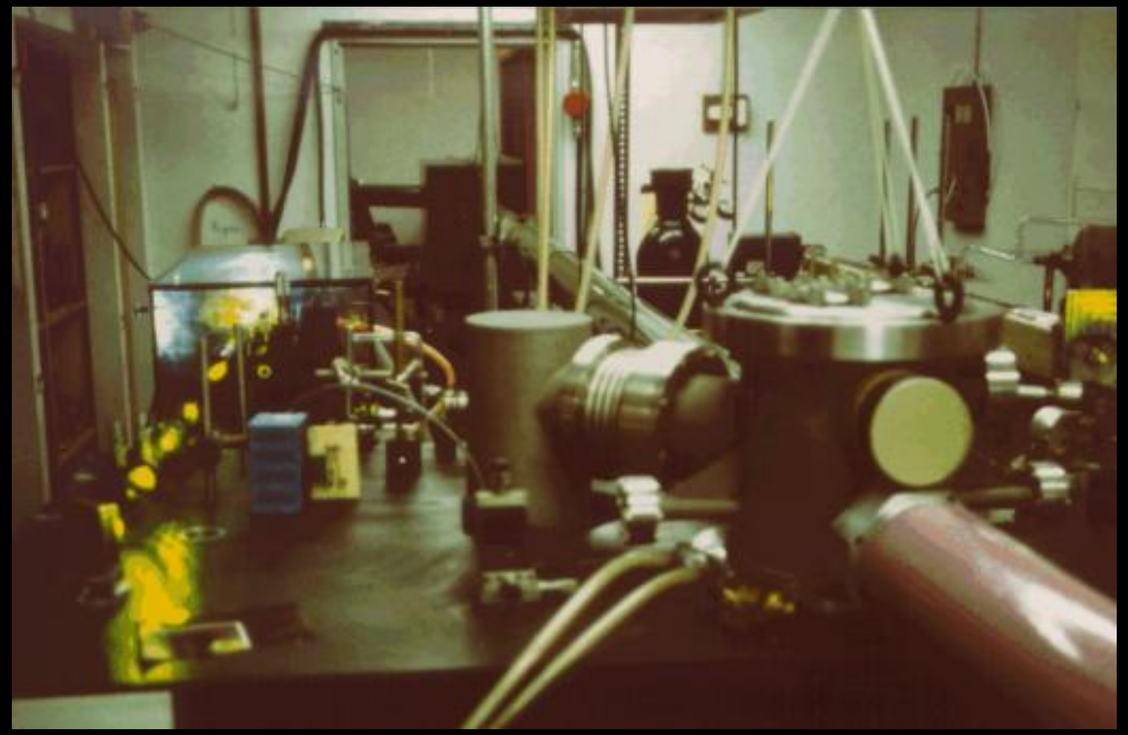
Alain Aspect (1982)

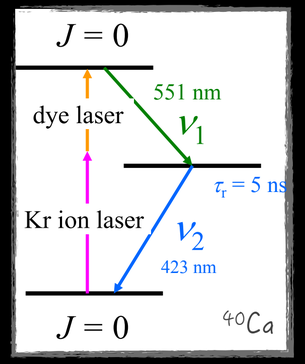
Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,[a] and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France

(Received 27 September 1982)





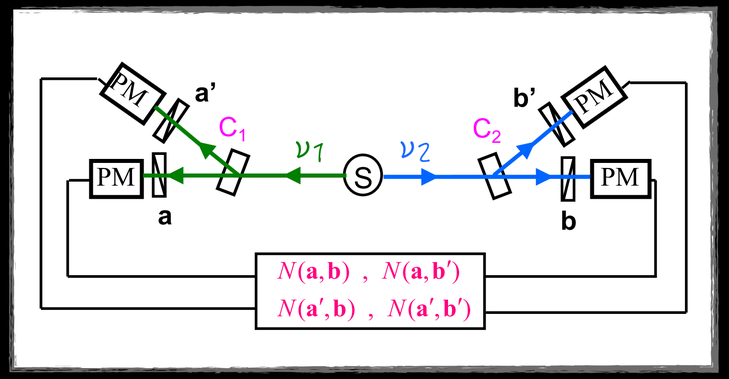


Alain Aspect (1982)

Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,[a] and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France

(Received 27 September 1982)

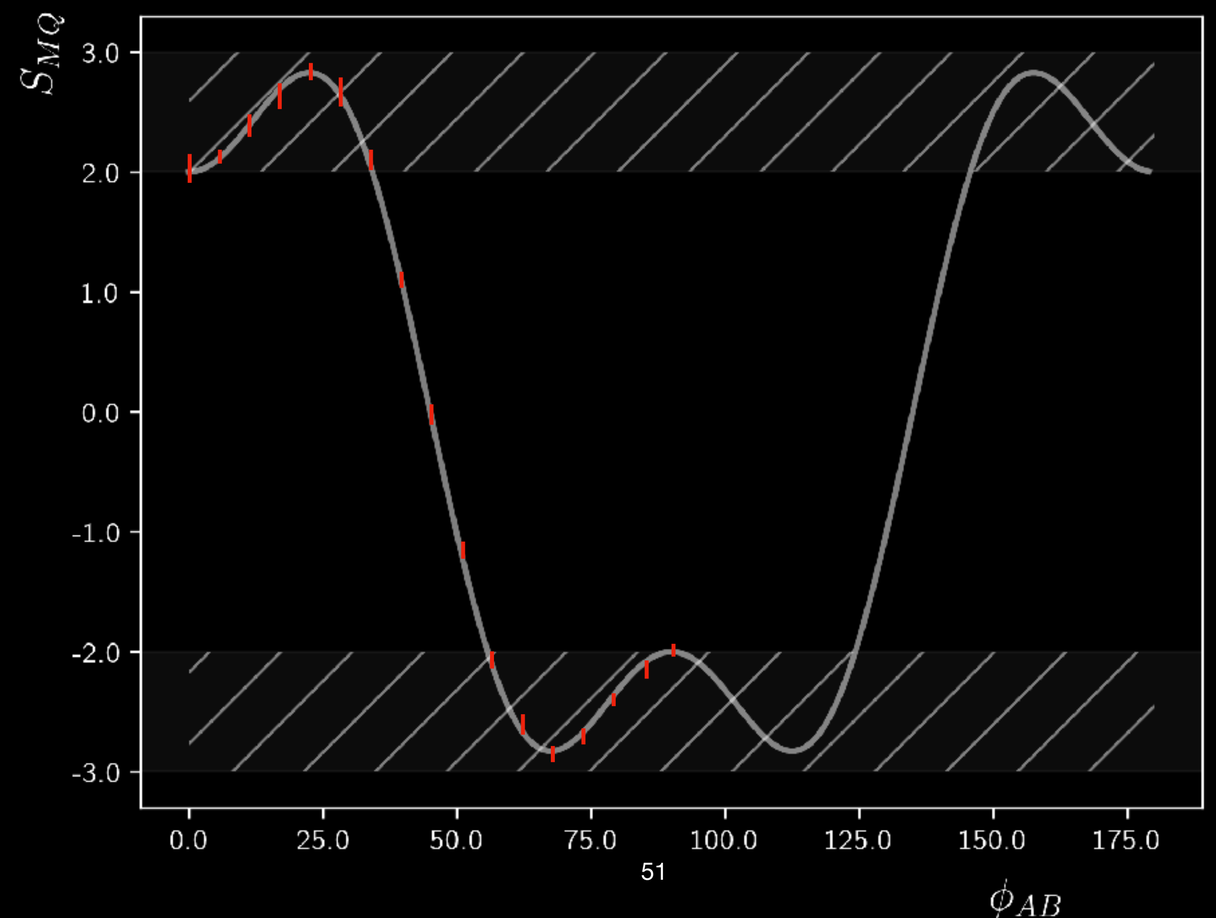


Alain Aspect (1982)

Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,[a] and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France

(Received 27 September 1982)

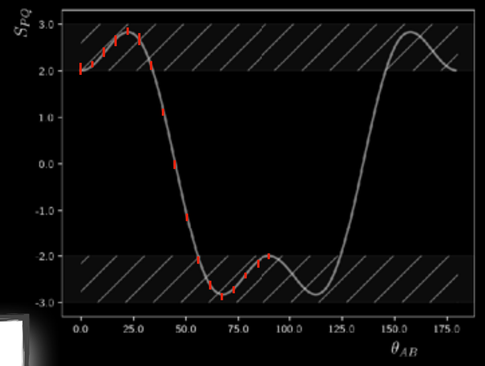


Alain Aspect (1982)

Experimental Test of Bell's Inequalities Using Time-Varying Analyzers

Alain Aspect, Jean Dalibard,[a] and Gérard Roger
Institut d'Optique Théorique et Appliquée, F-91406 Orsay Cédex, France

(Received 27 September 1982)



In conclusion, our experiment yields the strongest violation of Bell's inequalities ever achieved, and excellent agreement with quantum mechanics. Since it is a straightforward transposition of the ideal Einstein-Podolsky-Rosen-Bohm scheme, the experimental procedure is very simple, and needs no auxiliary measurements as in previous experiments with single-channel polarizers. We are thus led to the rejection of realistic local theories if we accept the assumption that there is no bias in the detected samples: Experiments support this natural assumption.

Actualités

Published: 14 August 2008

Testing the speed of 'spooky action at a distance'

Daniel Salart, Augustin Baas, Cyril Branciard, Nicolas Gisin & Hugo Zbinden

Nature **454**, 861–864(2008) | Cite this article

432 Accesses | **125** Citations | **41** Altmetric | Metrics

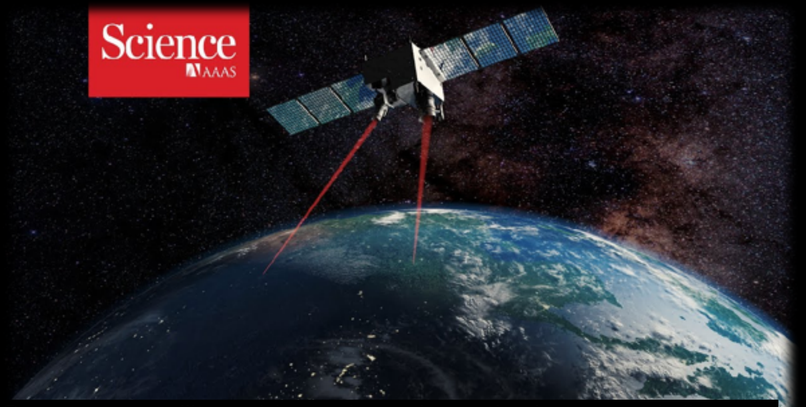
Published: 21 October 2015

Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres

B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau & R. Hanson

Nature **526**, 682–686(2015) | Cite this article

9871 Accesses | **795** Citations | **1327** Altmetric | Metrics



Quantum satellite achieves 'spooky action' at record distance

Le triomphe de l'interprétation de Copenhague

- Absence de réalisme quantique
- Etats superposés
- Probabilités et déterminisme quantique
- Rôle de l'observateur
- Réduction de la fonction d'onde

Le triomphe de l'interprétation de Copenhague

- Absence de réalisme quantique
- Rôle de l'observateur
- Probabilités et déterminisme quantique
- Etats superposés
- Réduction de la fonction d'onde

Un monde des idées accessibles par les équations quantiques

Un monde des formes perçus par nos instruments

Comment la superposition quantique, omniprésente dans le monde microscopique, échappe-t-elle à notre perception quotidienne ?

Chat de Schrödinger

$|\Psi\rangle = A_{vivant}|\text{atome non désintégré, chat vivant}\rangle + A_{mort}|\text{atome désintégré, chat mort}\rangle$

Serge Haroche (1944-)

2012 - P

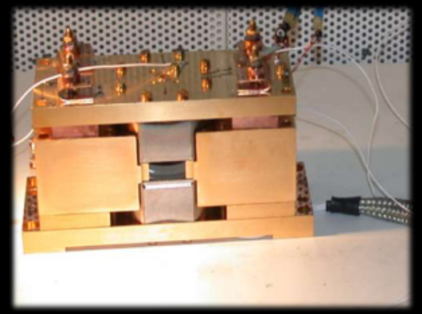
Serge Haroche (2007)

Compte les photons

Published: 15 March 2007

Quantum jumps of light recording the birth and death of a photon in a cavity

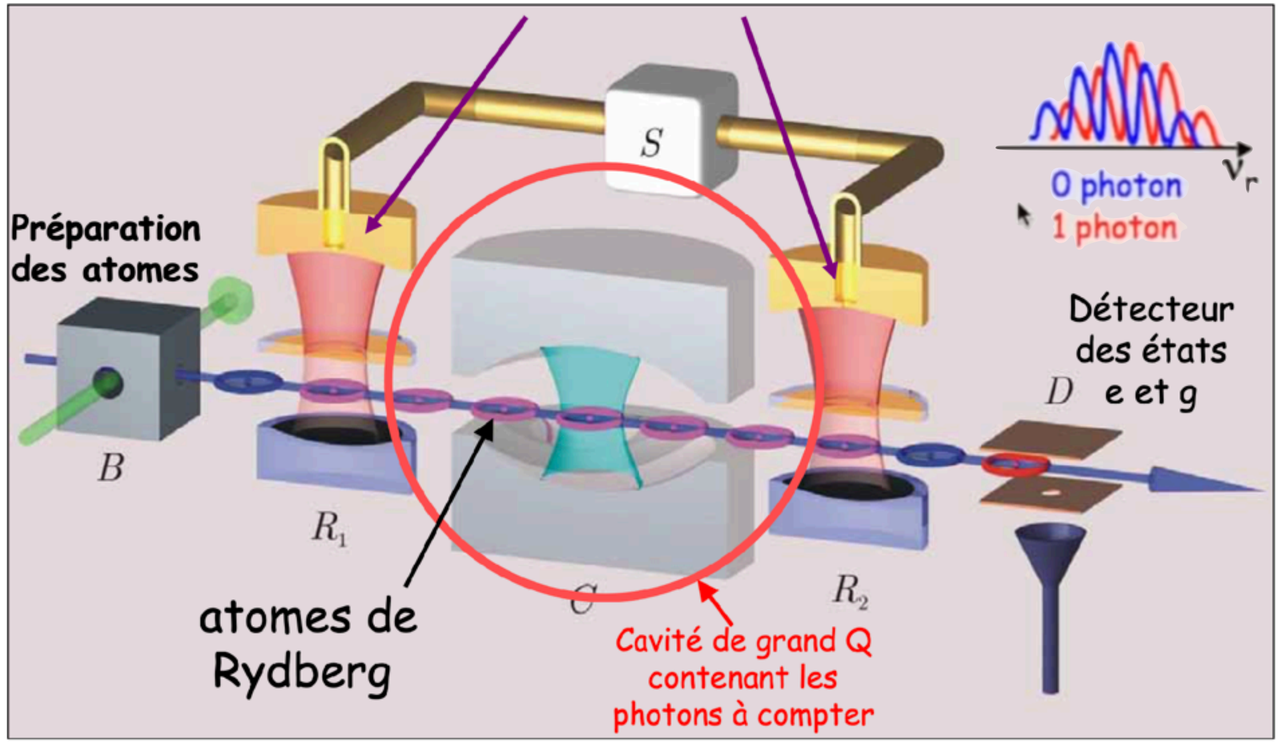
Sébastien Gleyzes, Stefan Kuhr, Christine Guerlin, Julien Bernu, Samuel Deléglise, Ulrich Busk Hoff, Michel Brune, Jean-Michel Raimond & Serge Haroche



Comment compter les photons avec l'horloge?

La lumière, piégée dans une cavité à l'intérieur de l'horloge, modifie, sans être absorbée, la fréquence de rotation du « spin-aiguille »

Impulsions micro-onde
(préparant et détectant le dipôle)



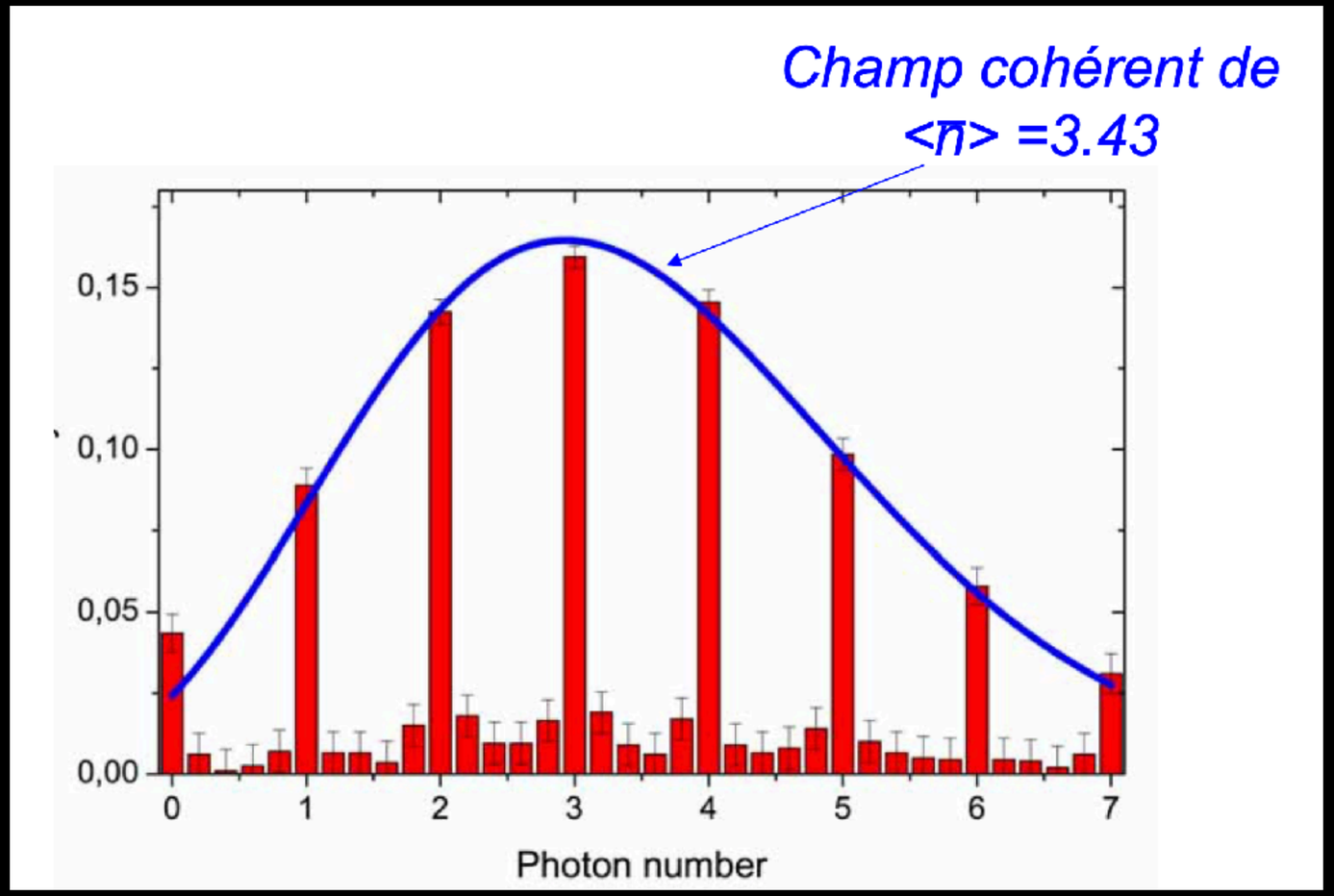
Serge Haroche (2007)

Compte les photons

Serge Haroche (2006)

Mesure de la fonction d'onde

$$|\psi\rangle = \sum_n a_n |n\rangle, \; P_n = a_n^2$$



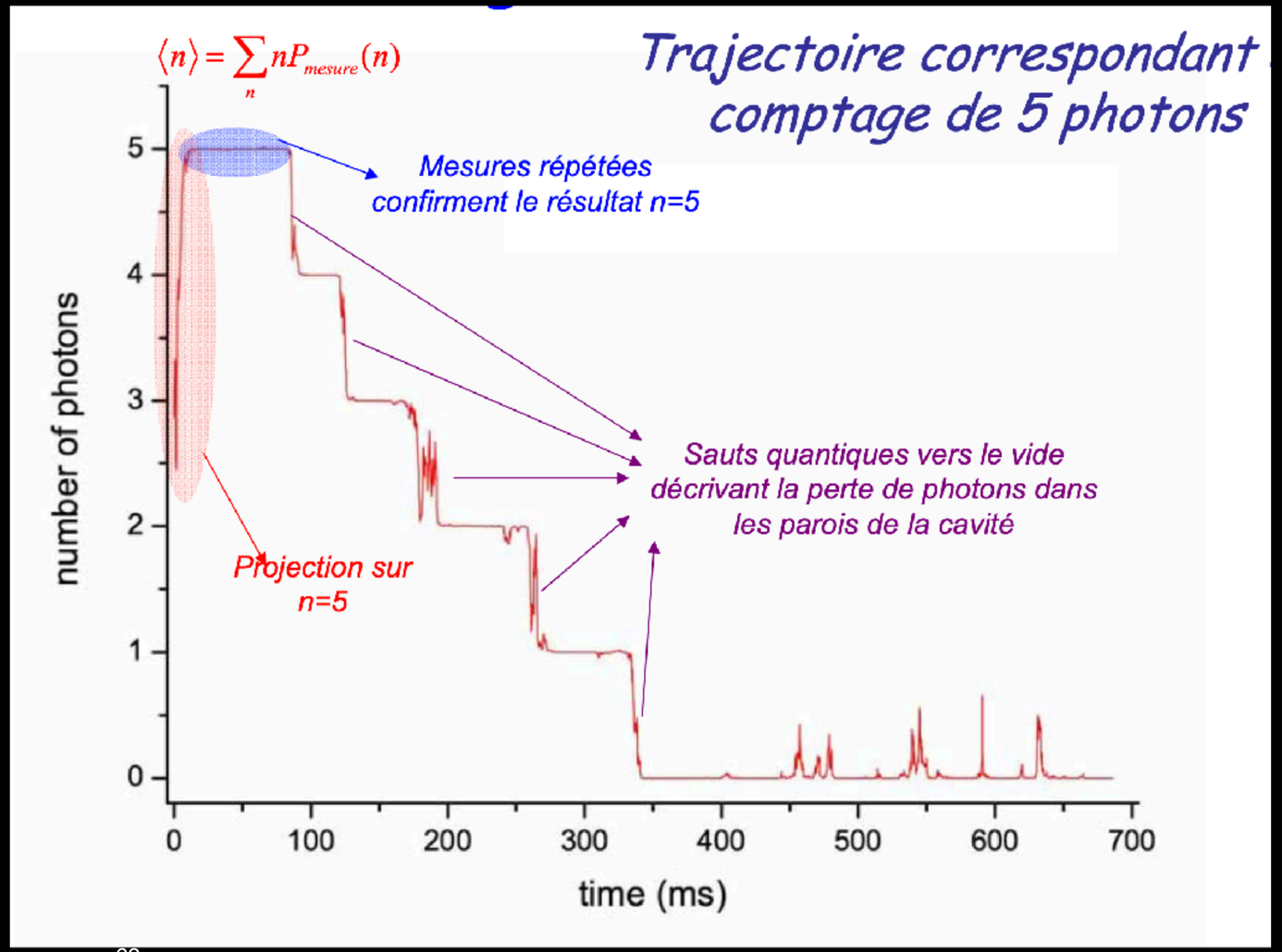
Serge Haroche (2006)

Effondrement de la fonction d'onde

$$|\psi\rangle = \sum_n a_n |n\rangle, \; P_n = a_n^2$$

$$\downarrow$$

$$|\psi\rangle = a_5 |5\rangle$$



Le chat est soit mort, soit vivant !

Les interactions avec l'environnement arrêtent le cours quantique des choses

A retenir

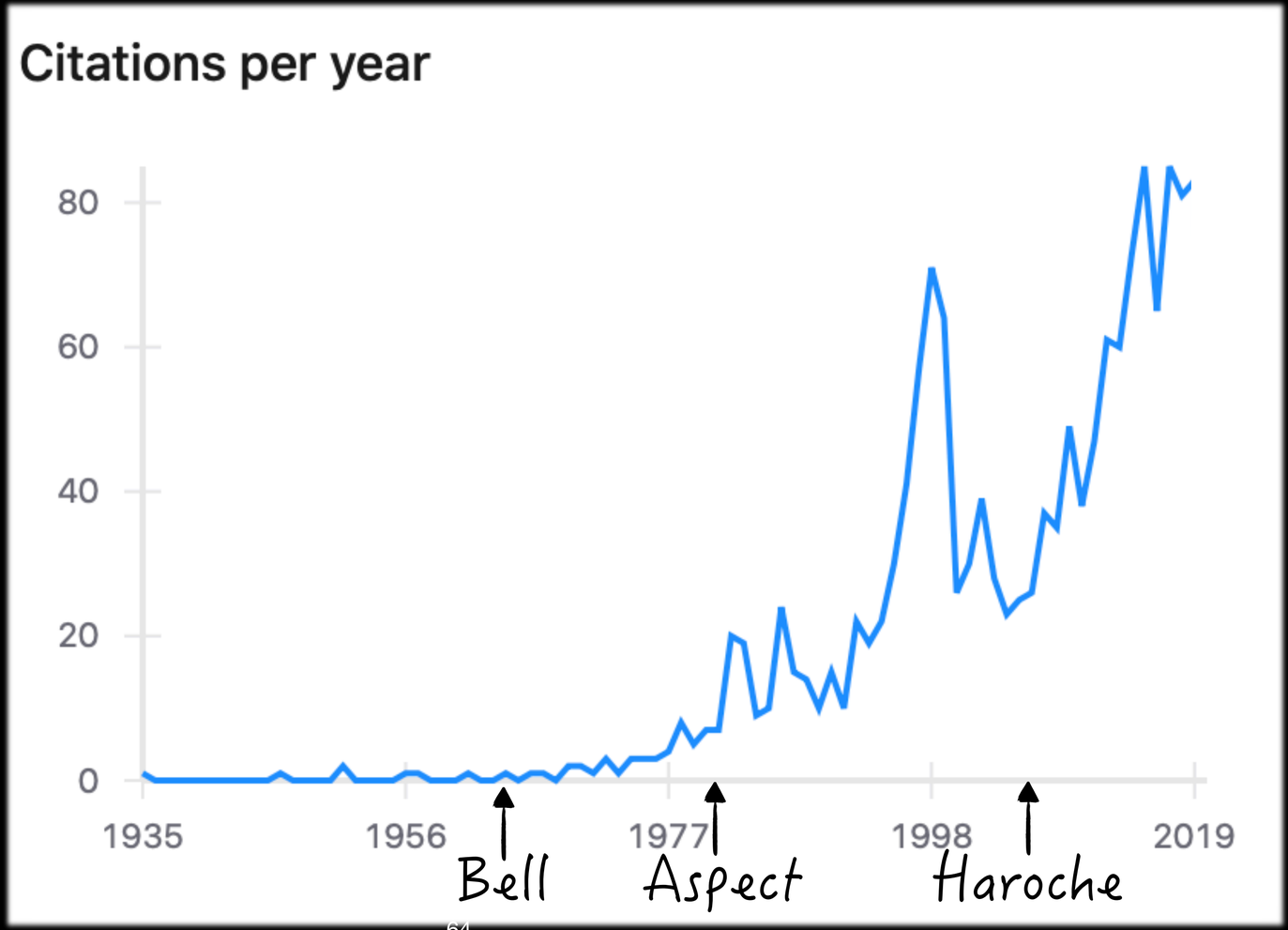
Le phénomène EPR

MAY 15, 1935 PHYSICAL REVIEW VOLUME 47

Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?

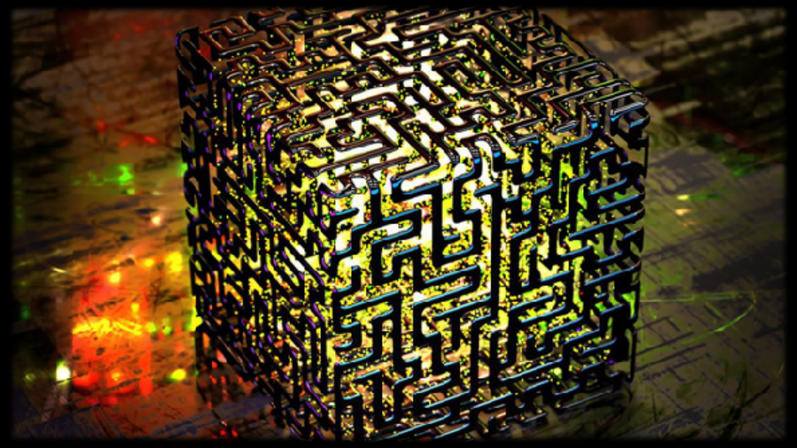
A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*

(Received March 25, 1935)

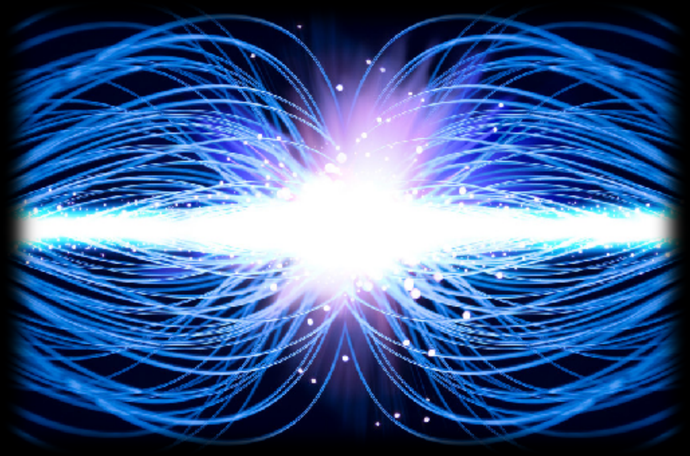


La mécanique quantique au service des technologies de l'information

Génération de nombres aléatoires



Ordinateur Quantique



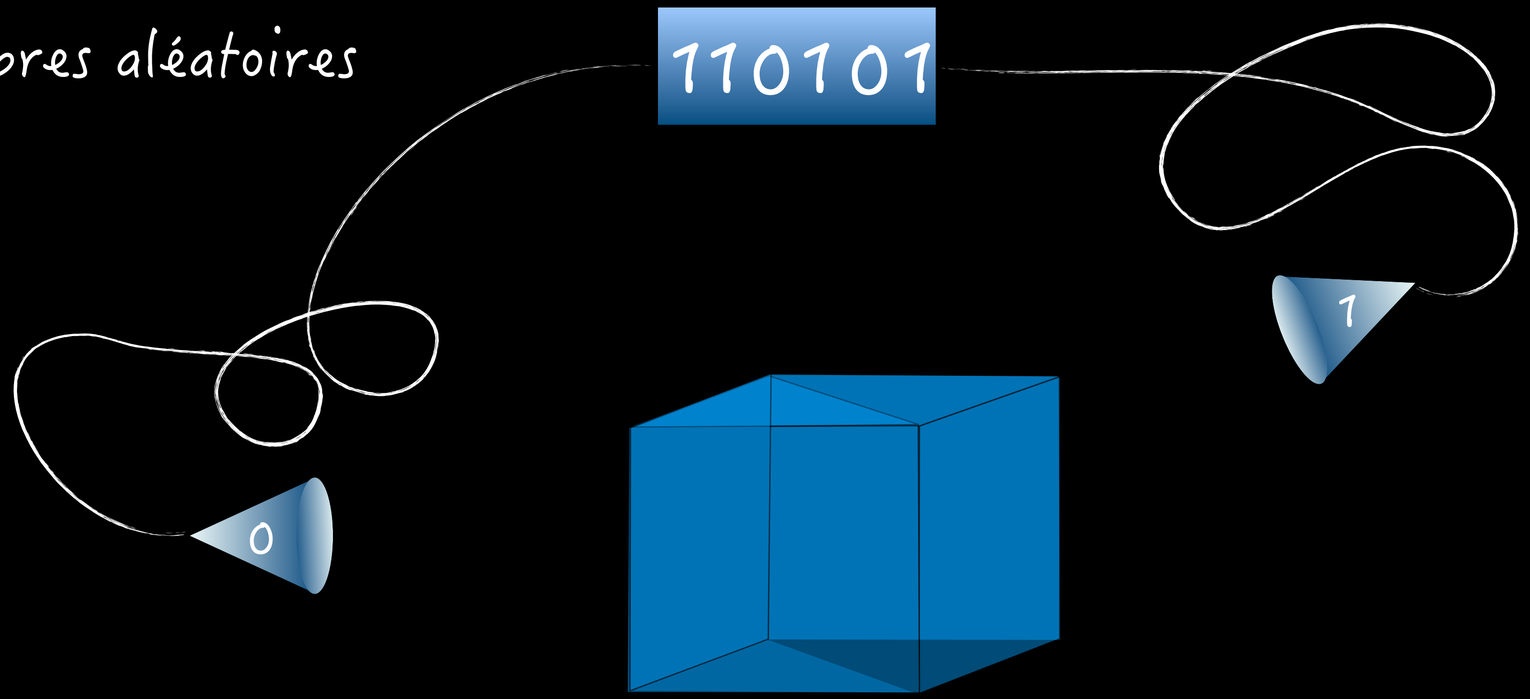
Téléportation

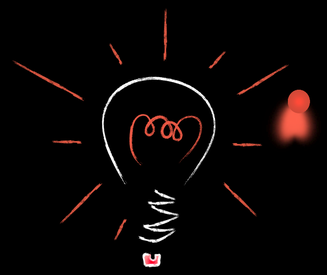
Cryptographie quantique

Finalement, de quoi sommes nous faits ?

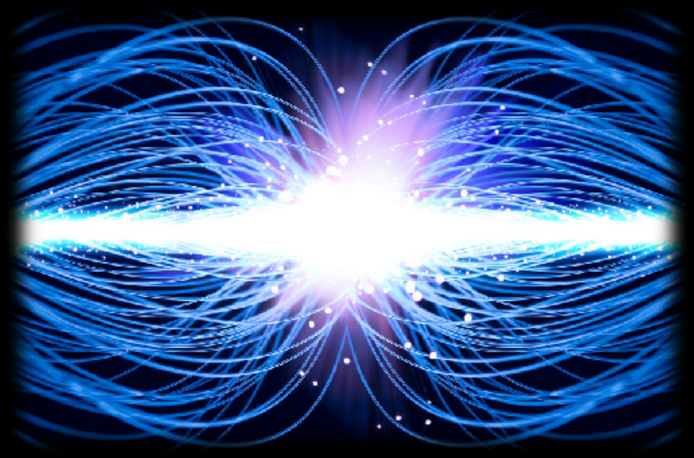
Génération de nombres aléatoires

Génération de nombres aléatoires





$$\psi(\upsilon) = \frac{1}{\sqrt{2}}|H> + \frac{1}{\sqrt{2}}|V>$$



Téléportation

Téléportation

Substance & forme

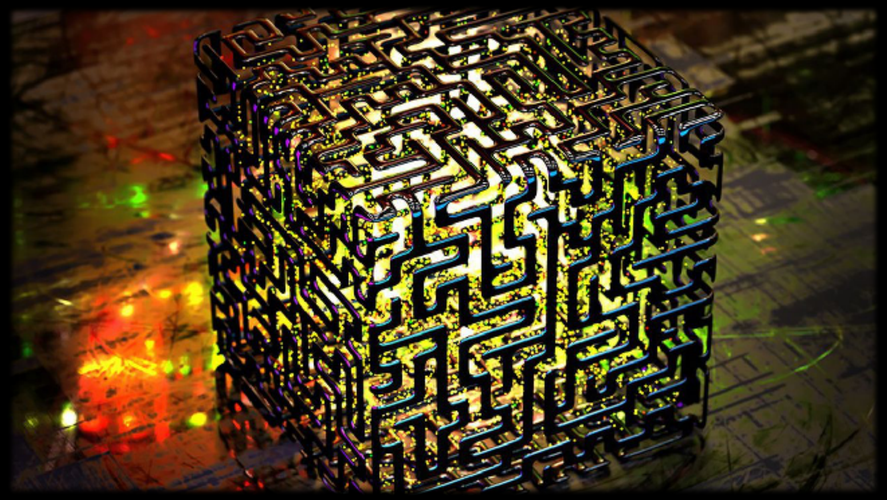
Letter | Published: 23 December 2019

Chip-to-chip quantum teleportation and multi-photon entanglement in silicon

Daniel Llewellyn, Yunhong Ding, Imad I. Faruque, Stefano Paesani, Davide Bacco, Raffaele Santagati, Yan-Jun Qian, Yan Li, Yun-Feng Xiao, Marcus Huber, Mehul Malik, Gary F. Sinclair, Xiaoqi Zhou, Karsten Rottwitt, Jeremy L. O'Brien, John G. Rarity, Qihuang Gong, Leif K. Oxenlowe, Jianwei Wang & Mark G. Thompson

Nature Physics **16**, 148–153(2020) | Cite this article

8608 Accesses | **2** Citations | **458** Altmetric | Metrics



Ordinateur Quantique

Exploite les propriétés quantique (superposition, intrication, interférence…) de la matière pour faire des calculs

Qbit

- Bit = unité d'information binaire (0, 1)
- Qbit = superposition d'états

1 : $\alpha_1|0\rangle + \alpha_2|1\rangle$

2 : $\alpha_1|00\rangle + \alpha_2|01\rangle + \alpha_3|10\rangle + \alpha_4|11\rangle$

3 : $\alpha_1|000\rangle + \alpha_2|010\rangle + \alpha_3|001\rangle + \alpha_4|011\rangle + \alpha_5|100\rangle + \alpha_6|110\rangle + \alpha_7|101\rangle + \alpha_8|111\rangle$

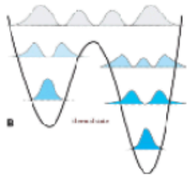
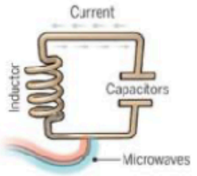
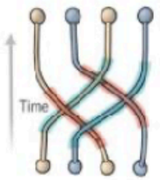
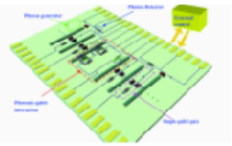
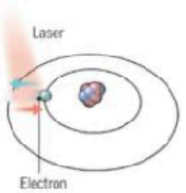
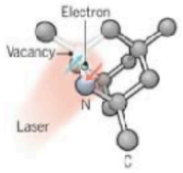
N : 2^N informations

$N = 75 \rightarrow 37\ 778\ 931\ 862\ 957\ 161\ 709\ 568$ informations

Les défis

- Fabriquer des Qbits
- Les conserver … durant le temps du calcul
- La lecture … qui détruit irrémédiablement
- La programmation

Pour en savoir plus : https://home.cern/fr/news/announcement/computing/online-introductory-lectures-quantum-computing-6-november

	recuit quantique	boucles supra-conductrices	qubits topologiques	optique linéaire	quantum dots silicium	ions piégés	cavités diamants
							
qubit	supraconducteur effet Josephson	supraconducteur effet Josephson	quasi-particules faites de paires d'anyons	photons individuels	spin d'électrons dans semi-conducteur	ions piégés magnétiquement	spin de noyau d'atomes
# qubit	**2048 qubits** (D-Wave)	**50 qubits** (IBM) **72 qubits** (Google)	**N/A**	**quelques-uns**	**49 qubits** (Intel)	**53 qubits** (IonQ) **51 qubits** (MIT) **20 qubits** (IQOQI)	**6 qubits** (QDTI)
état	sens du courant	phase ou énergie de résonnance ou sens du courant	sens de l'anyon	phase de photon	spins d'électrons	niveau énergétique de l'ion piégé	niveau d'énergie de la cavité
portes	micro-ondes 5 GHz et effet Josephson	micro-ondes 5 GHz et effet Josephson	inversions 2D d'anyons	filtres polarisants et dichroïques	micro-ondes	laser	laser
mesure	magnétomètre	magnétomètre	fusion d'anyons	détecteurs de photons	consersion spins to charge	fluorescence	fluorescence

Comprendre l'informatique quantique, Olivier Ezratty

IBM Q

Cryptographie

01100001

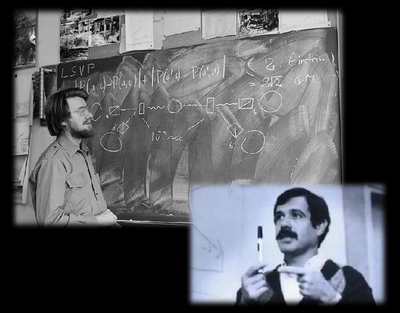
Photons	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Alice																
Bob																

Photons	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Alice																
Bob	1	1	0	0	0	0	1	1	1	1	0	1	1	0	0	1
Eve R																
Eve T																

02071011

Le jeu de Bell

Alain Aspect, 1982

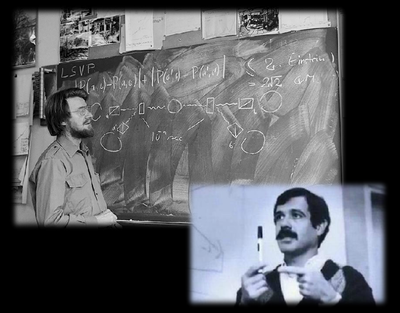


A retenir

A retenir

Le jeu de Bell

Alain Aspect, 1982



- Le formalisme quantique n'exprime aucune réalité
- La seule réalité est celle du monde classique qui inclut l'expérimentateur et ses instruments
- Le mystère de l'intrication : non localité et holisme quantiques
- La cohérence quantique est détruite dans les objets macroscopiques
- Applications concrètes

Cryptographie

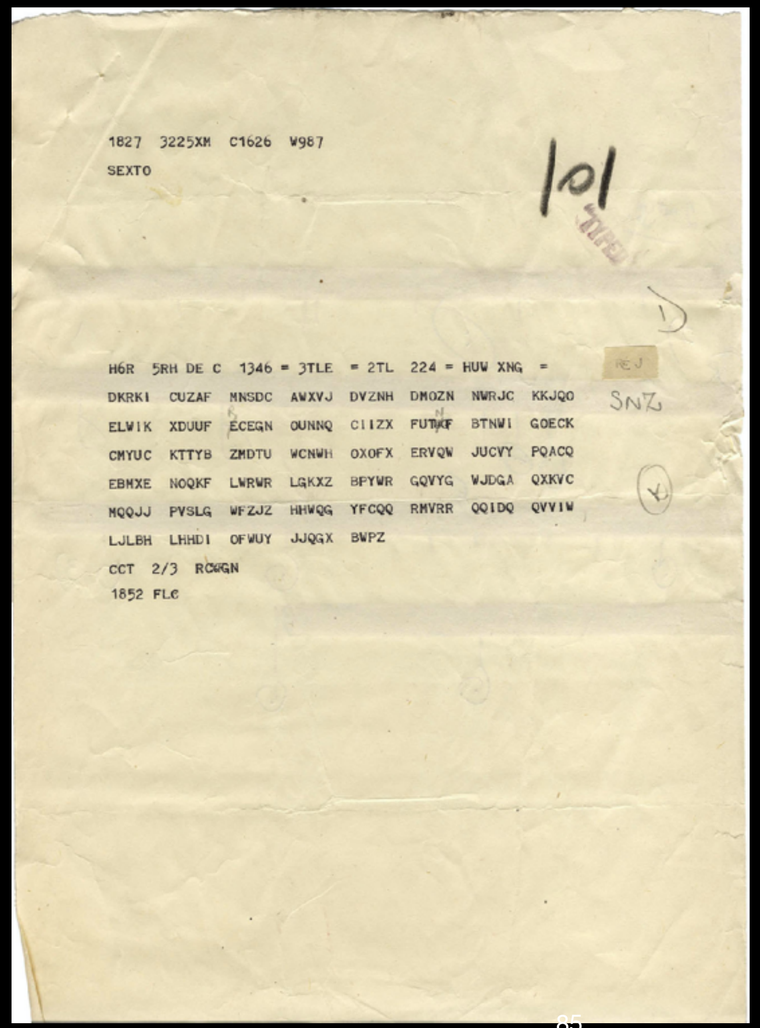
Alphabet de substitution

CAESAR AD SENATUM : YHQLYHTLYLFL

VENI, VEDI, VICI

Cryptographie

Alphabets de substitution



1827 3225XM C1626 W987
SEXTO

101

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =
DKRKI CUZAF MNSDC AWXVJ DVZNH DMOZN NWRJC KKJQO
ELWIK XDUUF ECEGN OUNNQ CIIZX FUTKF BTNWI GOECK
CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCVY PQACQ
EBMXE NOQKF LWRWR LGKXZ BPYWR GQVYG WJDGA QXKVC
MQQJJ PVSLG WFZJZ HHWQG YFCQQ RMVRR QQIDQ QVVIW
LJLBH LHHDI OFWUY JJQGX BWPZ
CCT 2/3 RCWGN
1852 FLC

Cryptographie

Chiffrement à clé

Message : 01110110 01100101 01101110 01101001 01110110 01101001 01100100 01101001 01110110 01101001 01100011 01101001 00001010 00001010 00100000

Clé : 01110110 01100101 01101110 01101001 01110110 01101001 01100100 01101001 01110110 01101001 01100011 01101001 00001010 00001010 00100000

Texte : 01110110 01100101 01101110 01101001 01110110 01101001 01100100 01101001 01110110 01101001 01100011 01101001 00001010 00001010 00100000

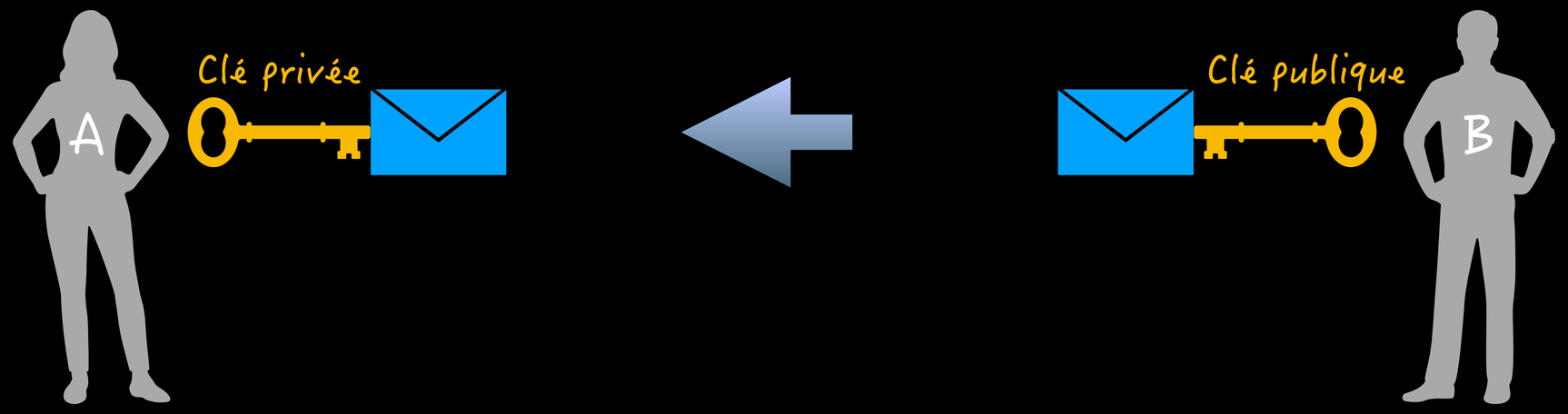
Les règles

Cryptographie

Chiffrement à clés privée & publique

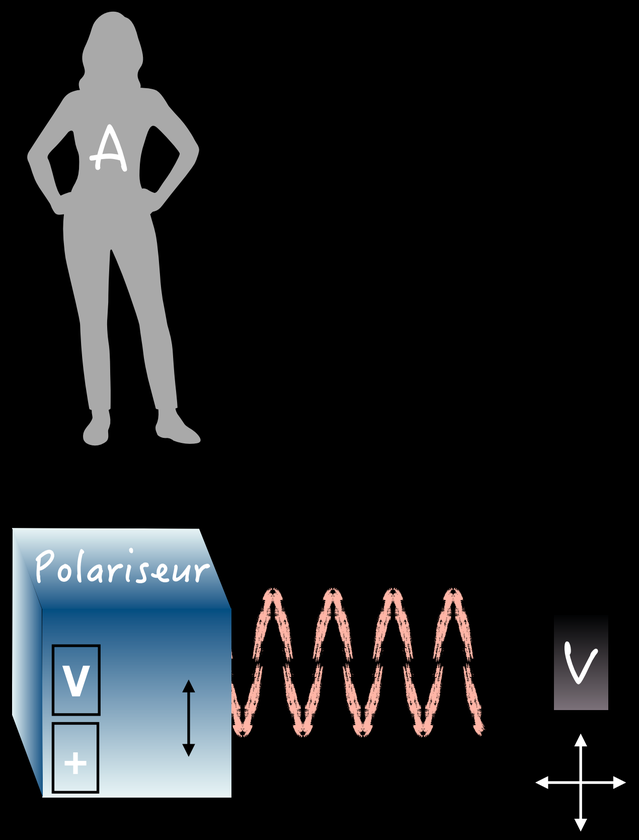
Clé publique : $N = p \times q$, p et q nombres premiers

Clé privée : $f(N, p, q)$



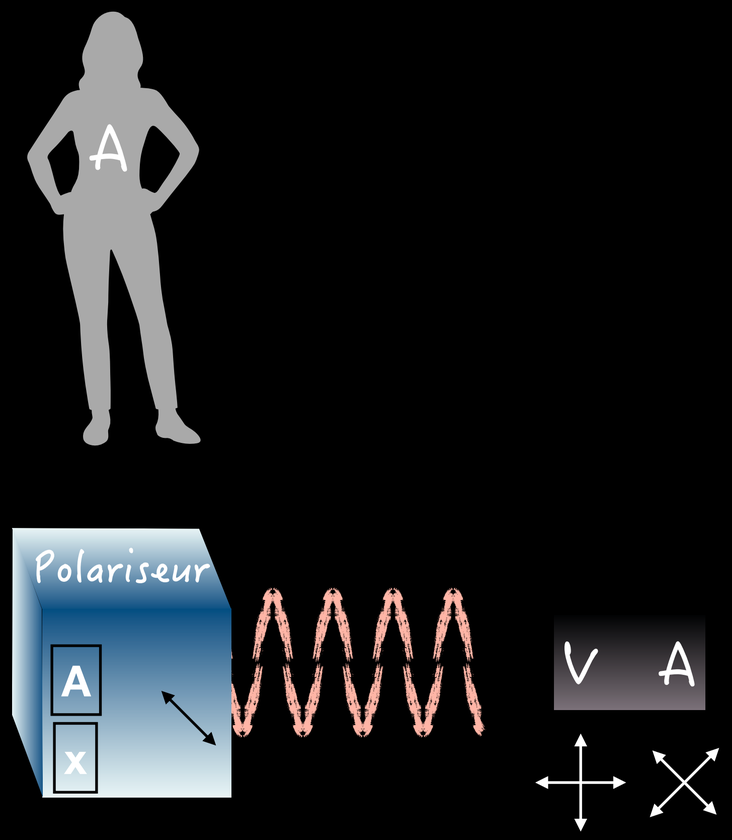
Cryptographie

Clé quantique



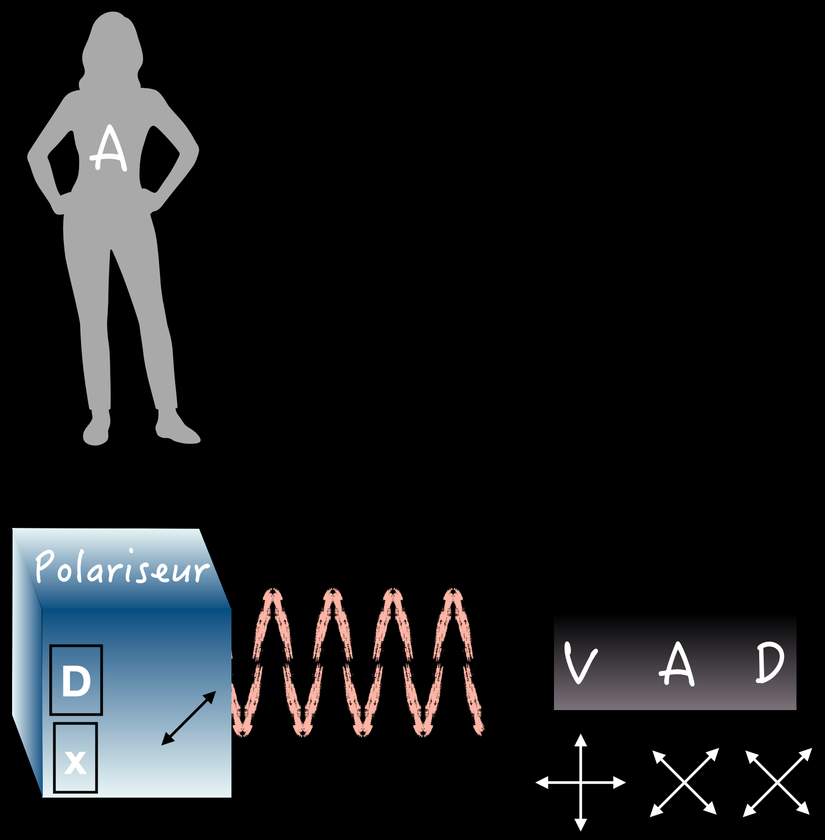
Cryptographie

Clé quantique



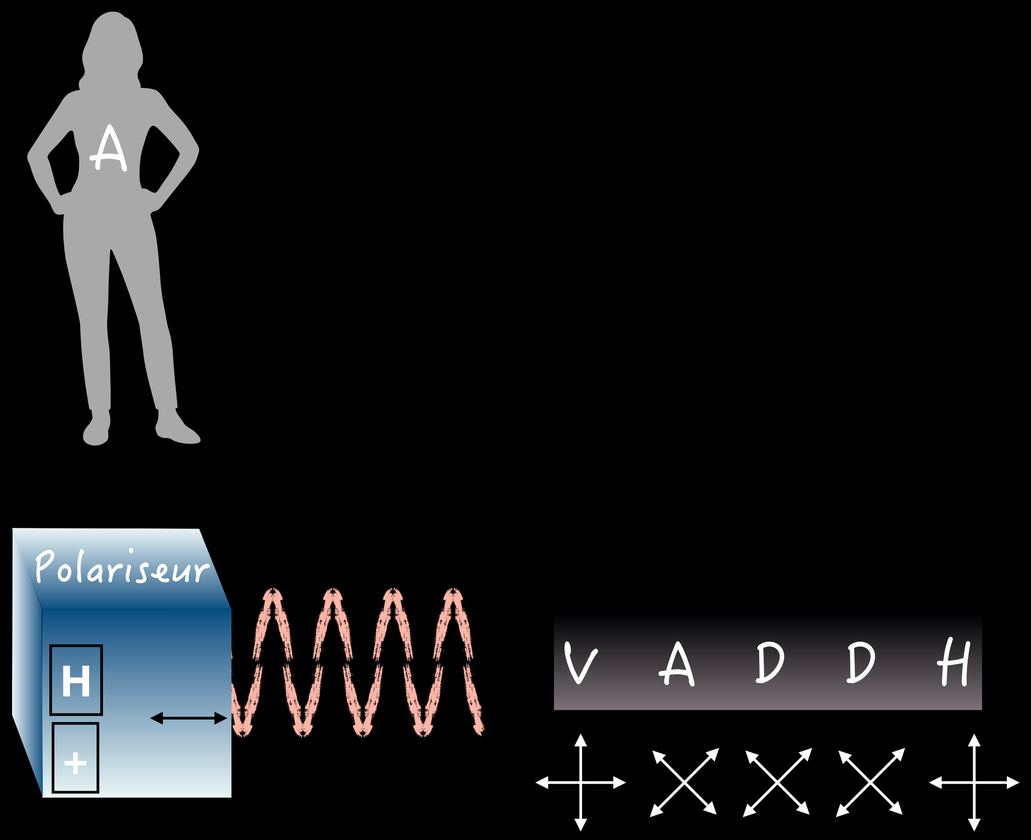
Cryptographie

Clé quantique



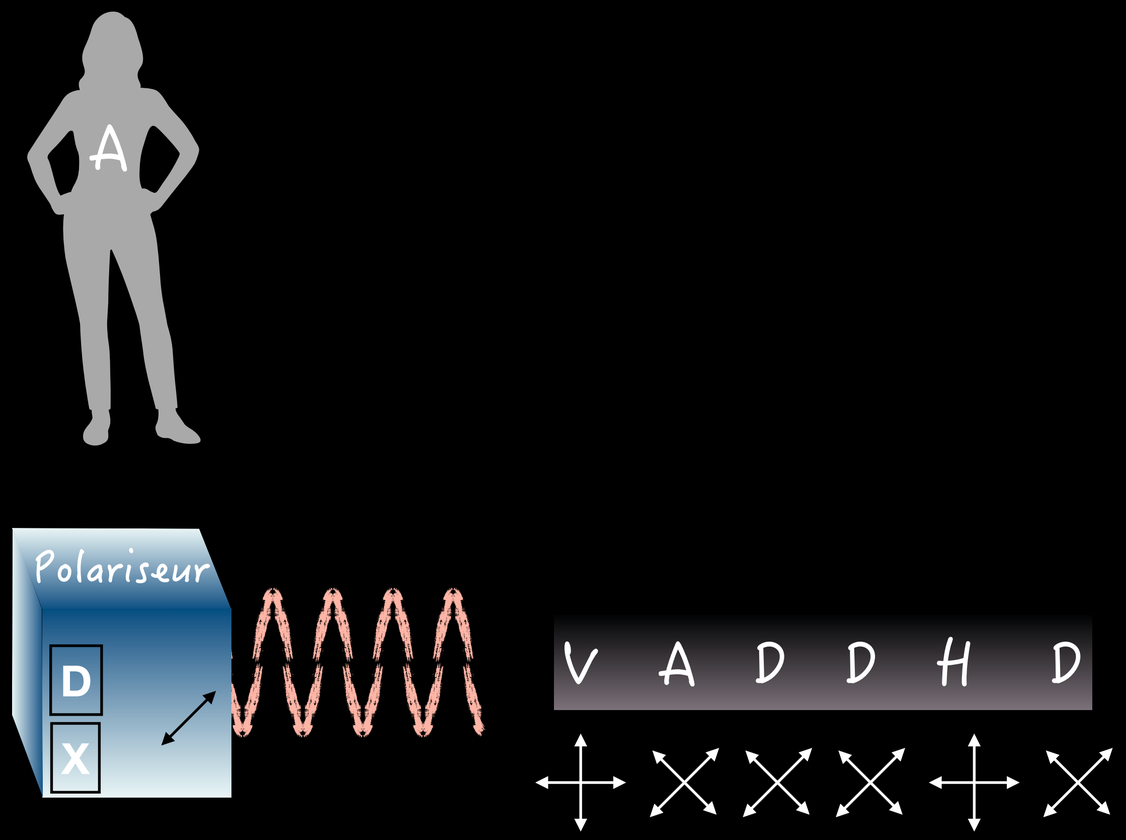
Cryptographie

Clé quantique



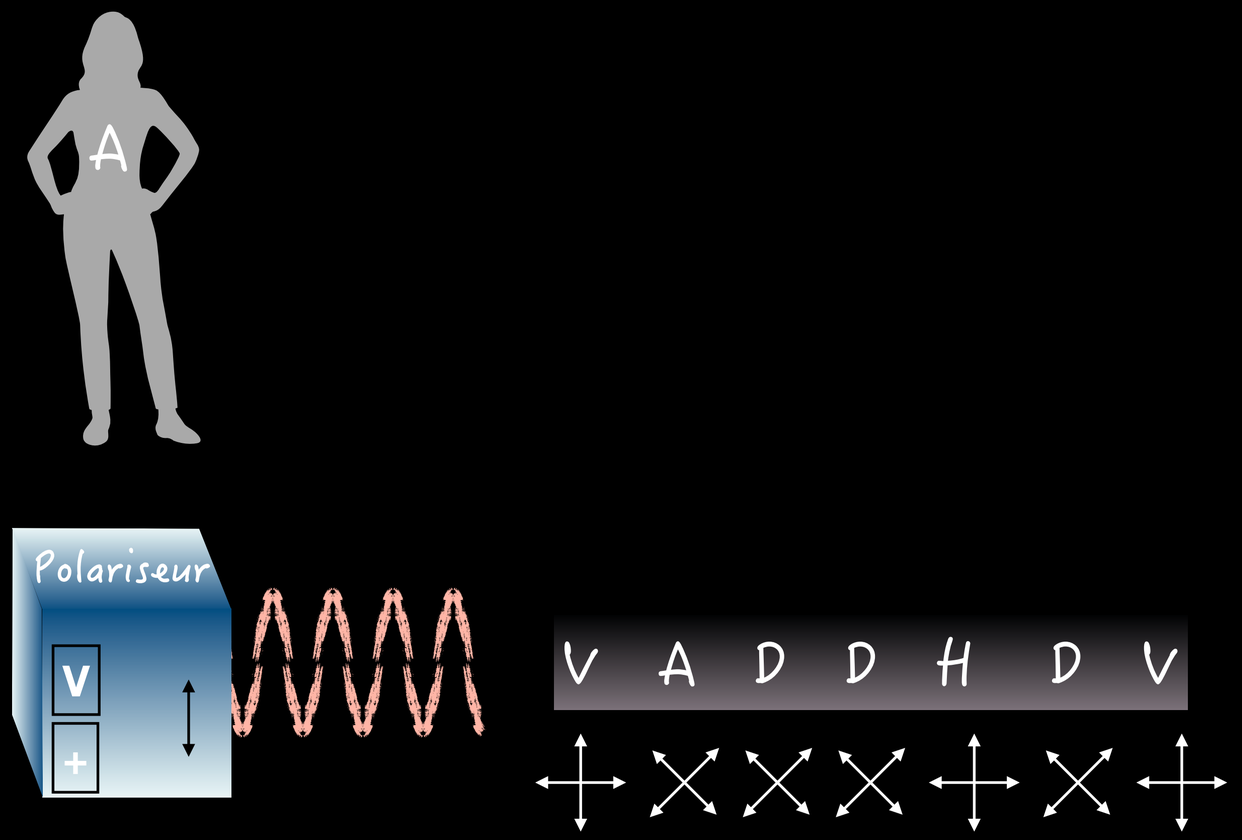
Cryptographie

Clé quantique



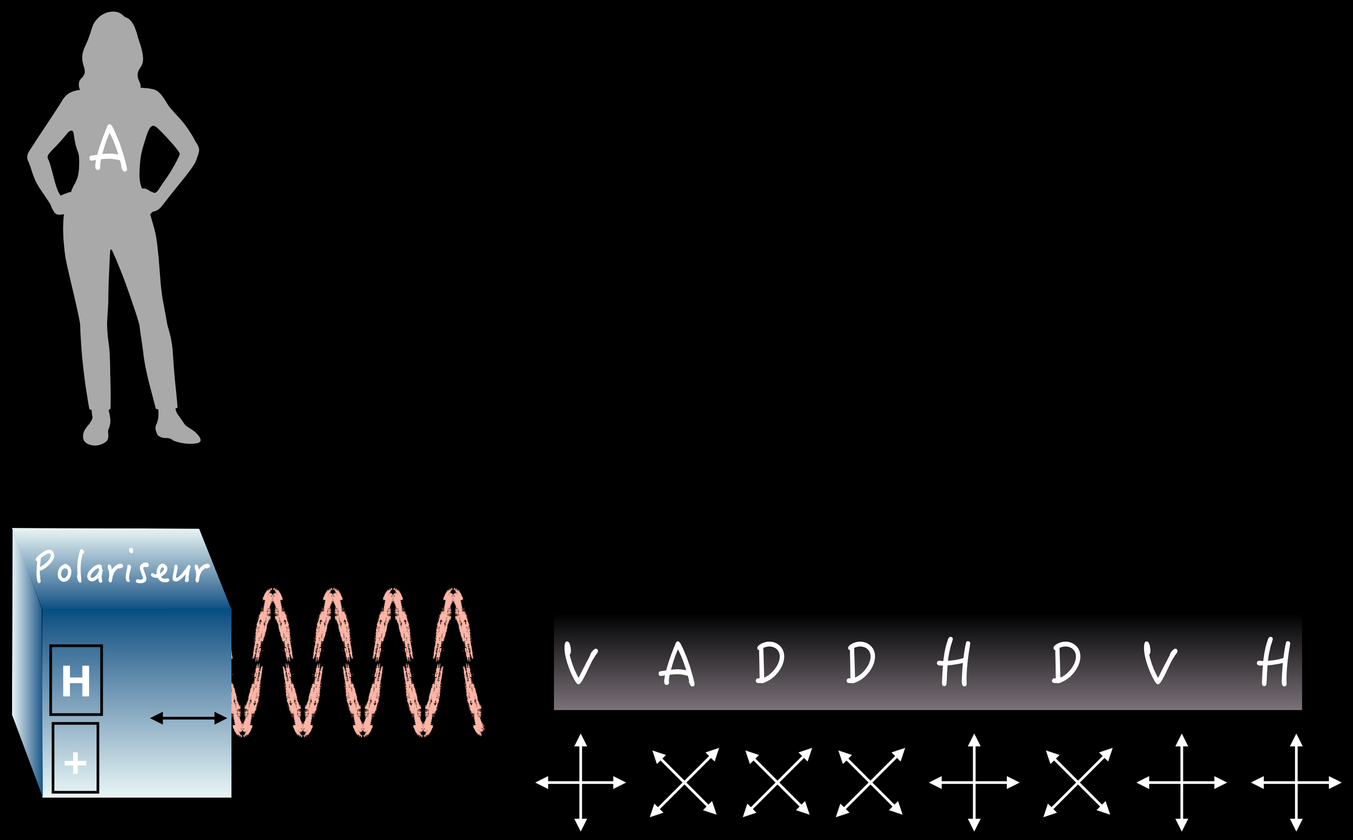
Cryptographie

Clé quantique



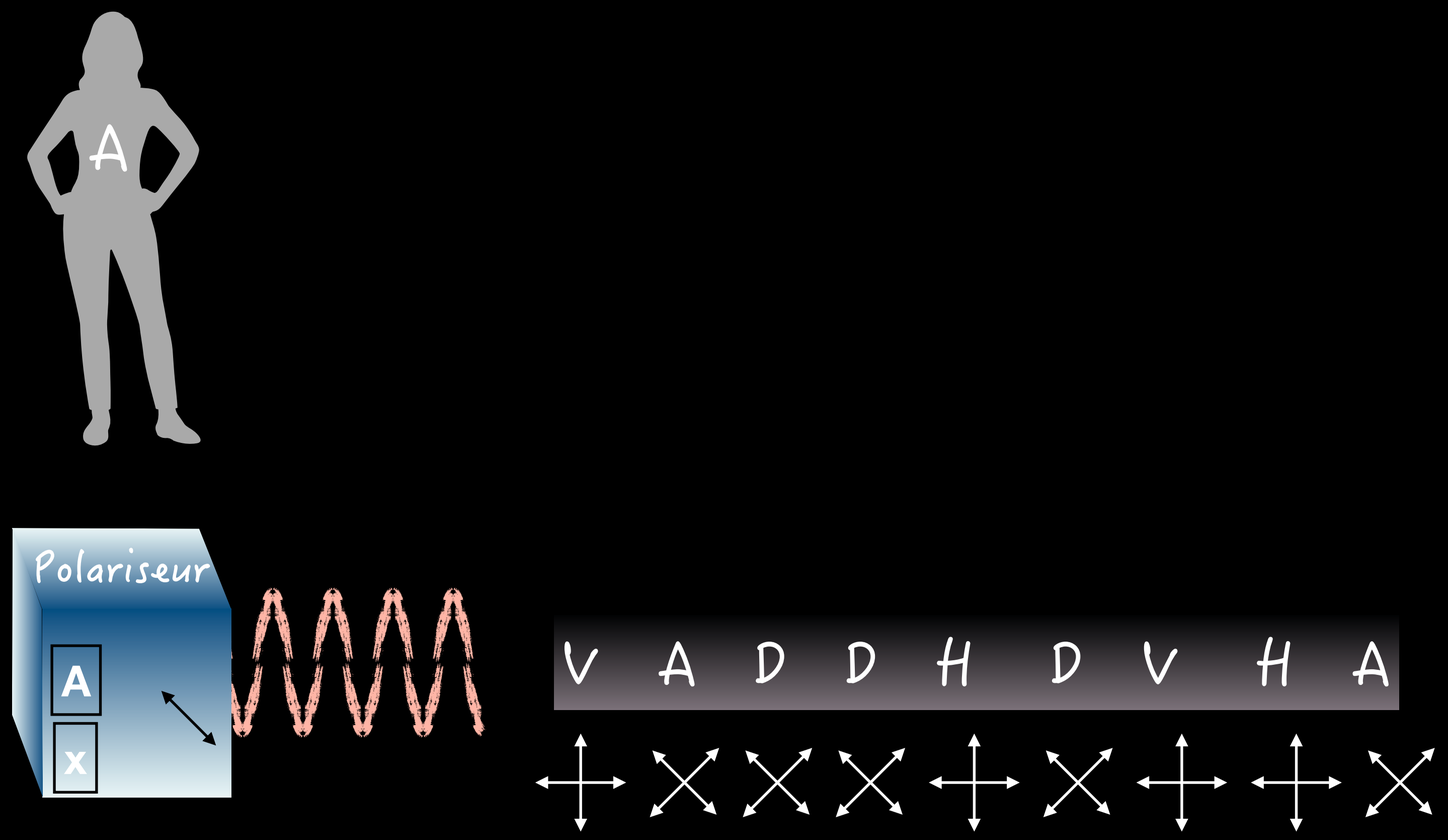
Cryptographie

Clé quantique



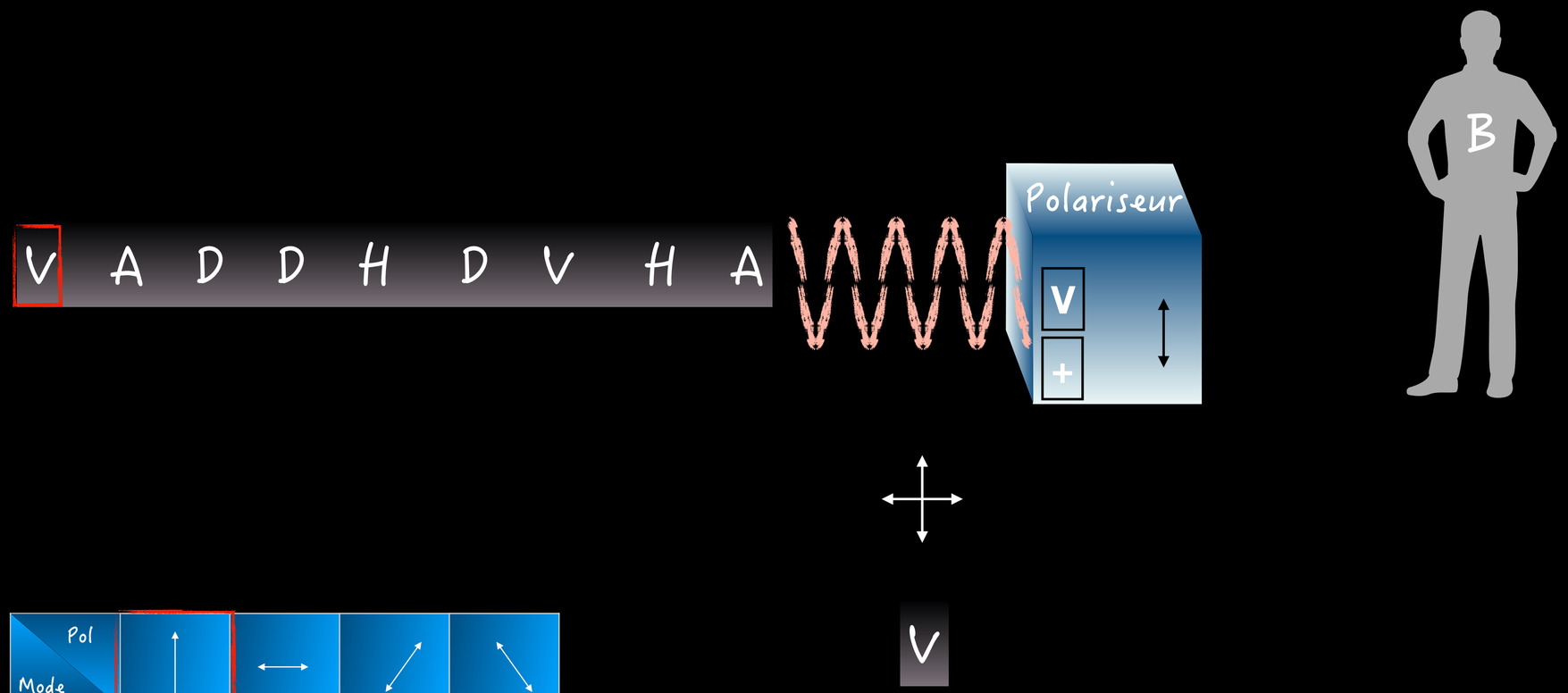
Cryptographie

Clé quantique



Cryptographie

Clé quantique

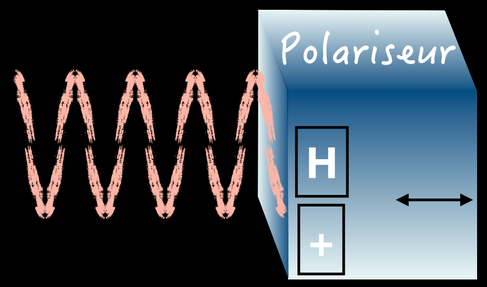


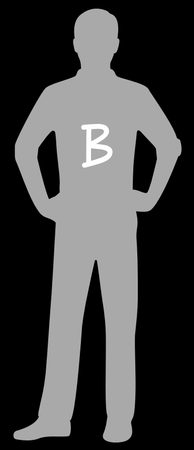
Pol / Mode	↕	↔	↗	↘
✚	V	H	H ou V	H ou V
✖	D ou A	D ou A	D	A

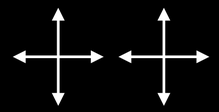
Cryptographie

Clé quantique

V A D D H D V H A







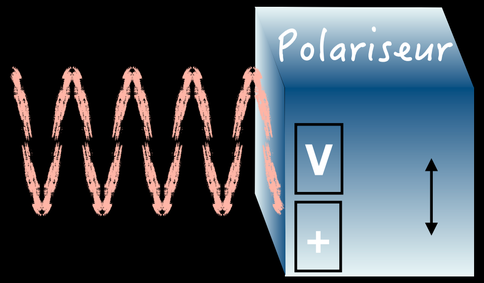
V H

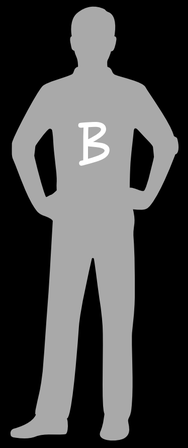
Pol / Mode	↕	↔	↗	↘
✚	V	H	H ou V	H ou V
✖	D ou A	D ou A	D	A

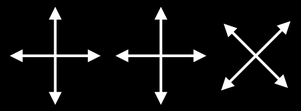
Cryptographie

Clé quantique

V A D D H D V H A







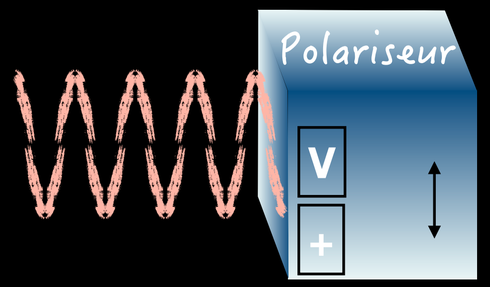
V H D

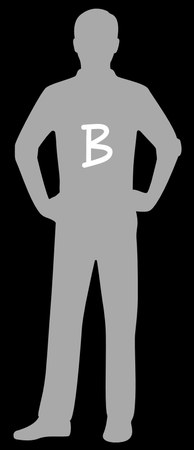
Pol / Mode	↕	↔	↗↙	↖↘
↕ ↔	V	H	H ou V	H ou V
✕	D ou A	D ou A	D	A

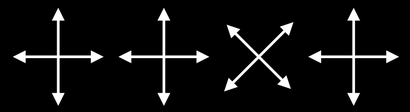
Cryptographie

Clé quantique

V A D D H D V H A







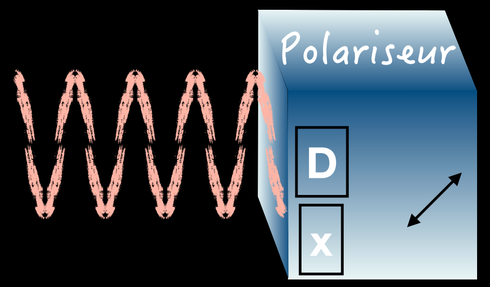
V H D V

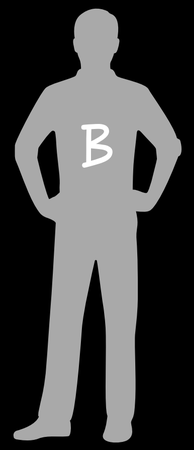
Pol / Mode	↕	↔	↗	↘
✚	V	H	H ou V	H ou V
✕	D ou A	D ou A	D	A

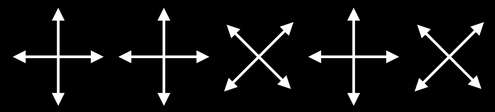
Cryptographie

Clé quantique

V A D D H D V H A







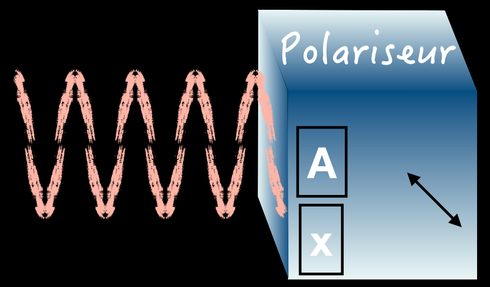
V H D V A

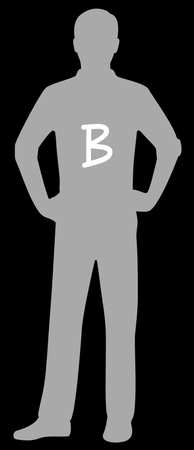
Pol / Mode	↕	↔	↗	↘
↕ ↔	V	H	H ou V	H ou V
↗ ↘	D ou A	D ou A	D	A

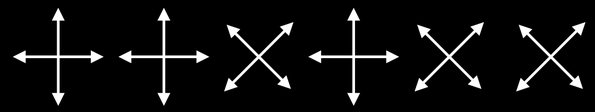
Cryptographie

Clé quantique

V A D D H D V H A







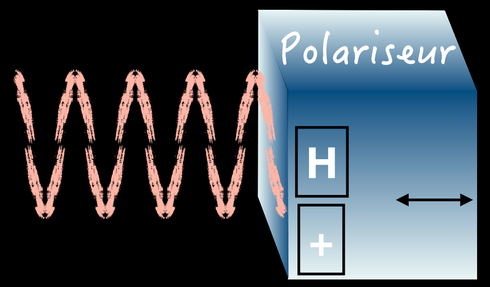
V H D V A D

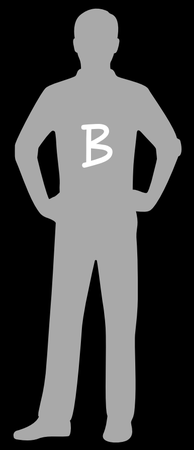
Pol / Mode	↕	↔	↗	↘
↕ ↔	V	H	H ou V	H ou V
⤫	D ou A	D ou A	D	A

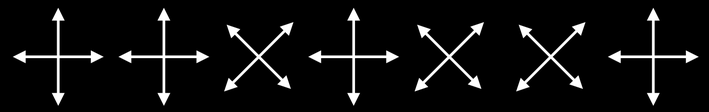
Cryptographie

Clé quantique

V A D D H D V H A





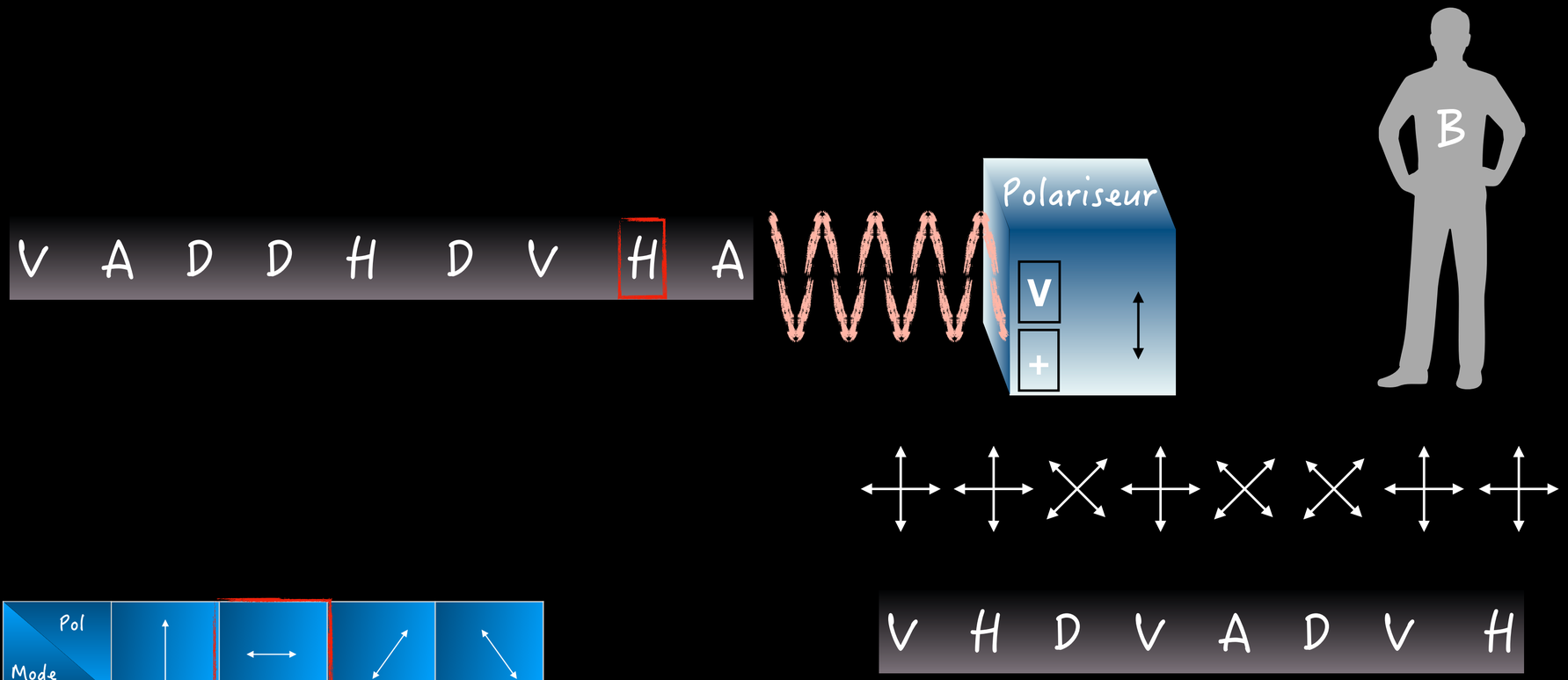


V H D V A D V

Pol / Mode	↕	↔	↗	↘
↕ ↔	V	H	H ou V	H ou V
⤫	D ou A	D ou A	D	A

Cryptographie

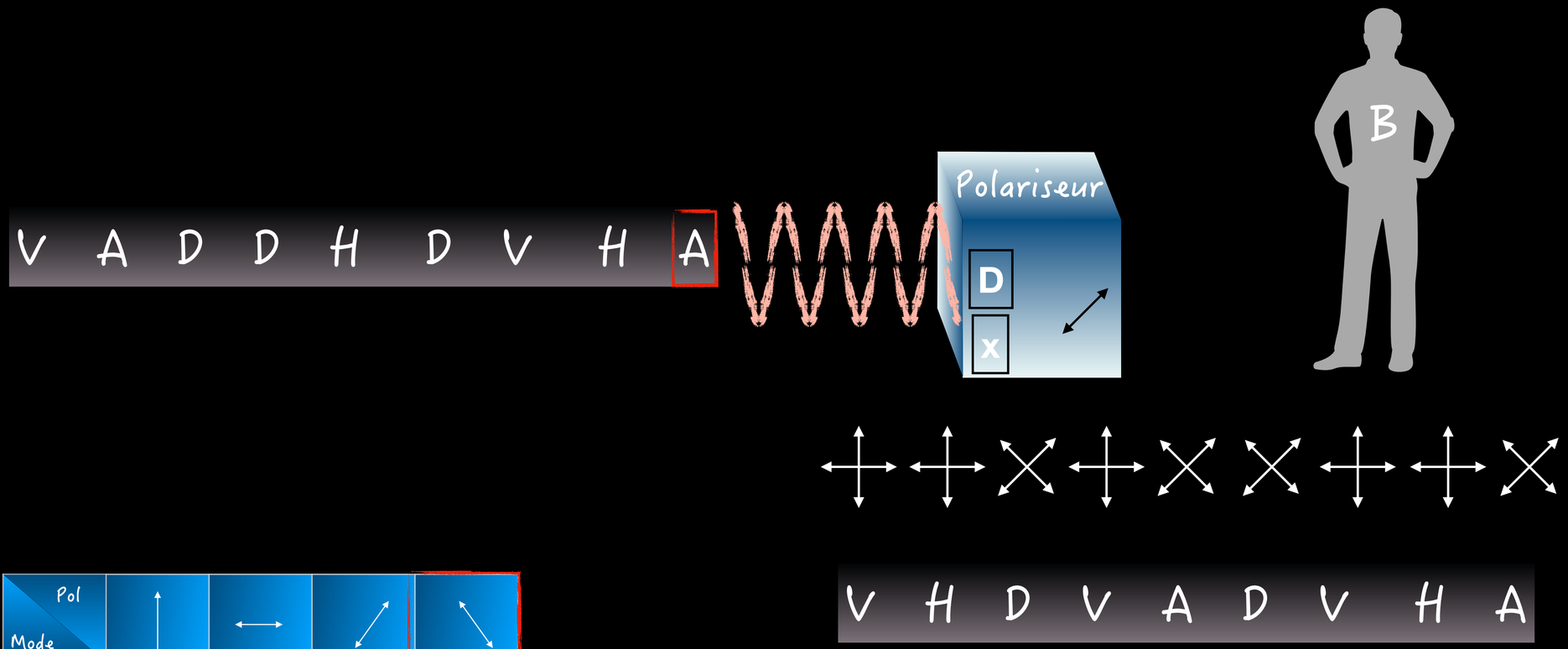
Clé quantique



Pol / Mode	↕	↔	↗	↘
↕ ↔	V	H	H ou V	H ou V
↗ ↘	D ou A	D ou A	D	A

Cryptographie

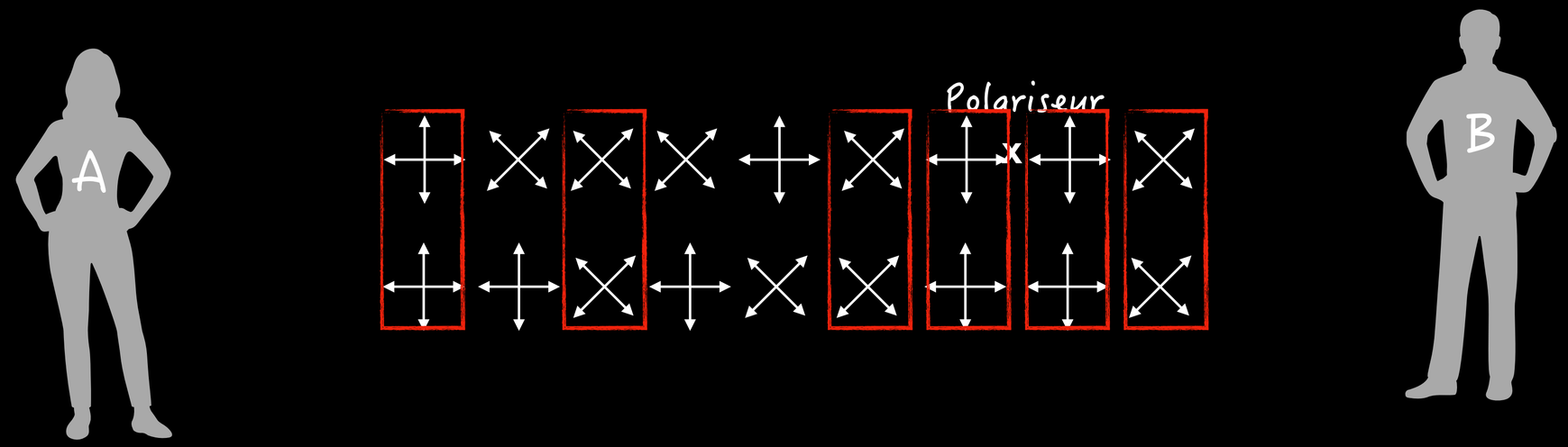
Clé quantique



Pol / Mode	↕	↔	↗	↘
↕ ↔	V	H	H ou V	H ou V
↗ ↘	D ou A	D ou A	D	A

Cryptographie

Clé quantique

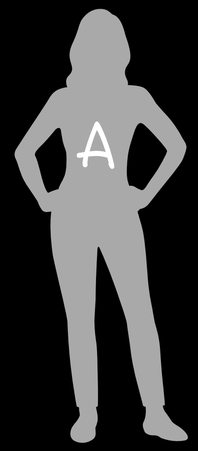


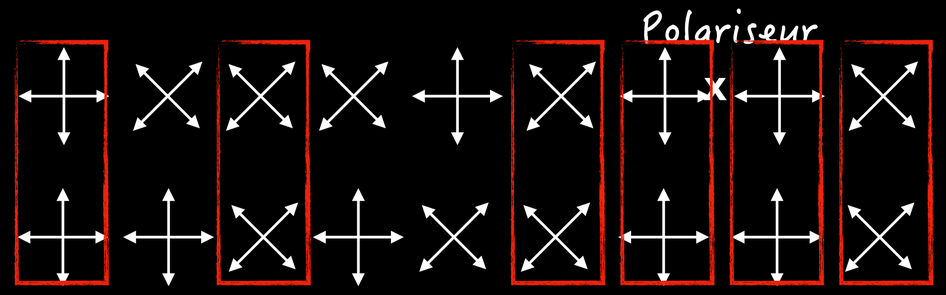
V A D D H D V H A

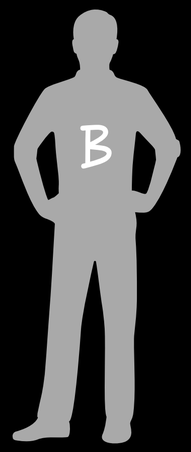
V H D V A D V H A

Cryptographie

Clé quantique







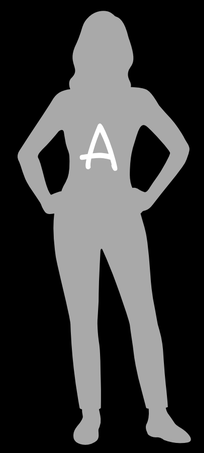
V	A	D	D	H	D	V	H	A
1		0			0	1	0	1

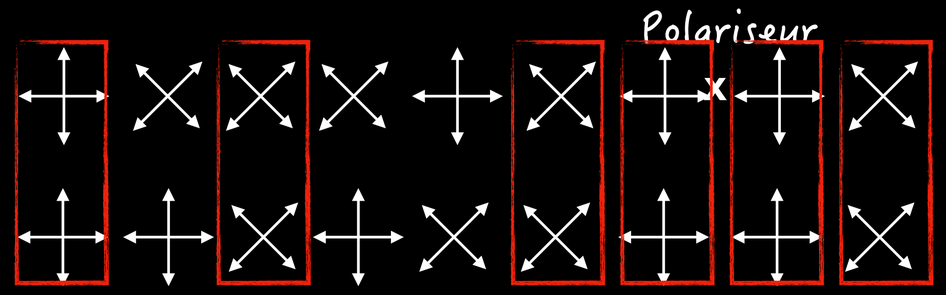
V	H	D	V	A	D	V	H	A
1		0			0	1	0	1

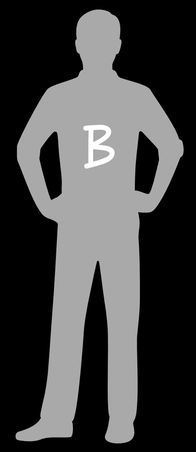
V, A = 1
H, D = 0

Cryptographie

Clé quantique







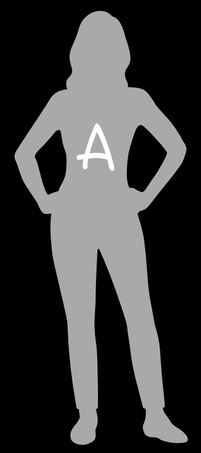
V	A	D	D	H	D	V	H	A
1		0			0	1	0	1

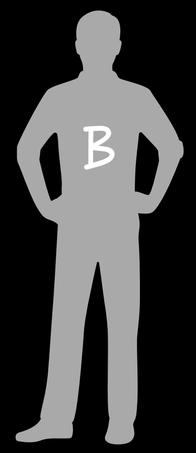
V	H	D	V	A	D	V	H	A
1		0			0	1	0	1

Clé retenue : 11

Cryptographie

Clé quantique





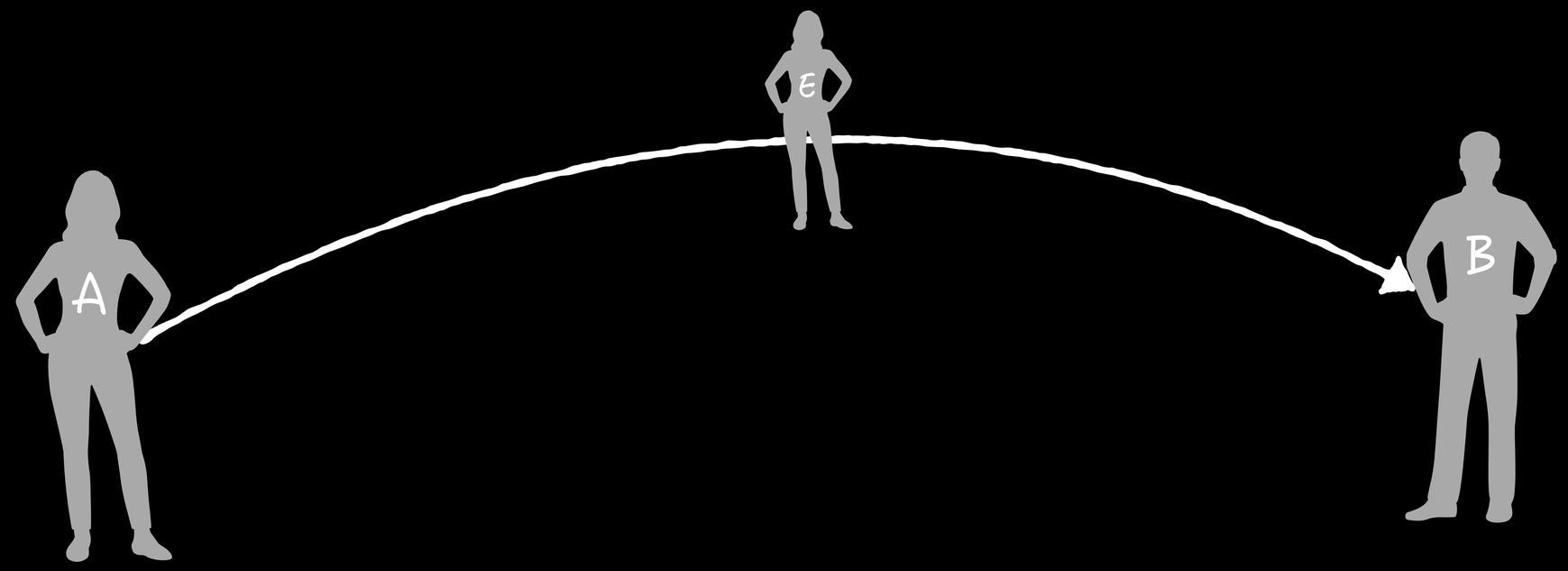
V	A	D	D	H	D	V	H	A
1		0			0	1	0	1

V	H	D	V	A	D	V	H	A
1		0			0	1	0	1

Vérification erreurs

Cryptographie

Clé quantique



V	A	D	D	H	D	V	H	A
1		0			0	1	0	1

V	H	V	V	A	D	V	H	A
1		1			0	1	0	1

Vérification erreurs !! Erreur !!

Si vous m'avez compris, c'est que je n'ai pas été clair !

Richard Feynman

Si vous ne m'avez pas compris, c'est que je n'ai pas été clair !

Yves Schutz