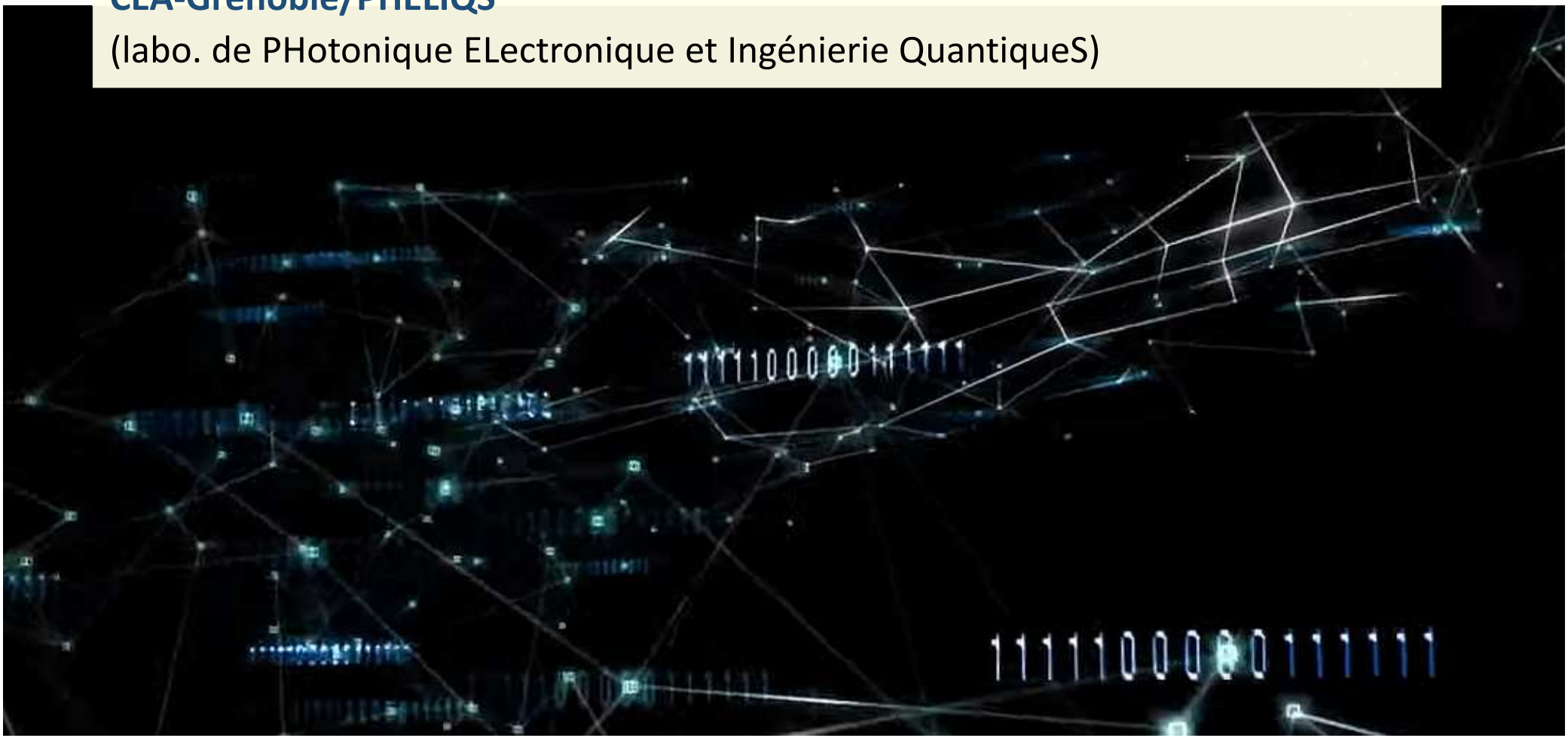
Les technologies quantiques:
Une introduction au qubit photonique et à la cryptographie quantique

Kuntheak KHENG

CEA-Grenoble/PHELIQS

(labo. de PHotonique ELectronique et Ingénierie QuantiqueS)



Exploiter des propriétés de superposition quantique d'états d'un objet physique, ou l'intrication quantique de plusieurs sous-parties de cet objet pour des applications nouvelles:

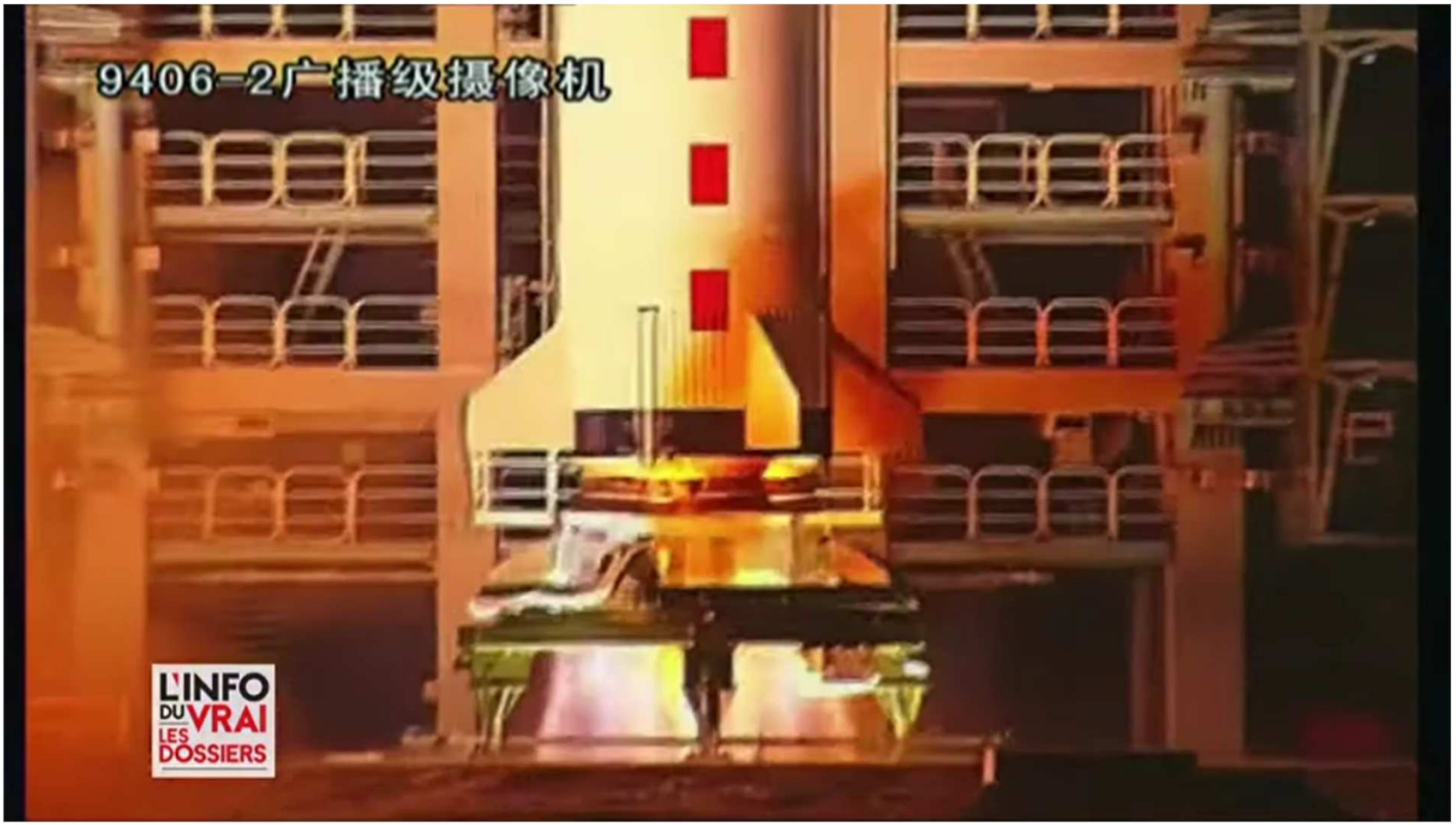
- ordinateurs quantiques: capables d'effectuer certains calculs de manière bien plus efficace qu'avec des ordinateurs classiques
- capteurs quantiques et métrologie: sensibilité inégalée , horloges atomiques des satellites GPS , gravimètres quantiques à atomes…
- simulateurs quantiques: simuler le comportement de systèmes quantiques qu'on ne sait pas calculer
- communications quantiques: assurer l'inviolabilité d'une communication

Objet quantique: élément de la structure microscopique de la matière et du rayonnement → **atomes, électrons, photons, etc…**

Communication quantique spatiale

2016: satellite Micius, Chine

→ Premières expériences de communication quantique à l'échelle spatiale



Extrait de L'info du vrai: Ordinateurs quantiques : un enjeu technologique et géostratégique ? https://www.youtube.com/watch?v=Bp7uZPU8wC4

2024: satellite Eagle-1

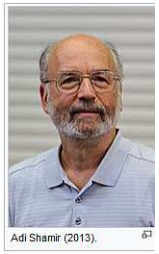
→ 1er système spatial européen de distribution quantique de clé (ESA, Thalès,…)

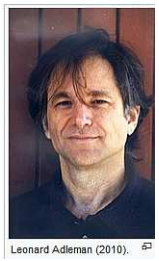
* Chiffrement Asymétrique : 2 clés, une publique et une privée

Cryptographie Asymétrique: https://www.youtube.com/watch?v=MuNyEoU5tSo

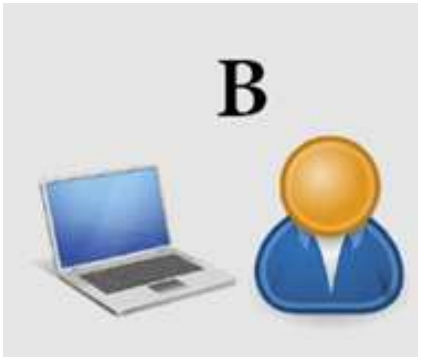
Chiffrement RSA

(Rivest, Shamir, Adleman)





Message chiffré = f(message, K_A)



Envoie clé publique K_A

clé publique K_A=(e,N) pour chiffrer
clé privé k_A=(d,N) pour déchiffer

K_A=(e,N)

N=p.q

La connaissance de p et q permet de déchiffrer le message

N=99 → (p,q)=(9,11) ou (3,33)
N=52 991 584 …235 (p,q)= ???
Factorisation d'un grand nombre est très long pour une ordinateur classique

Problème: ce serait très rapide avec un ordinateur quantique (algorithme de Shor) !

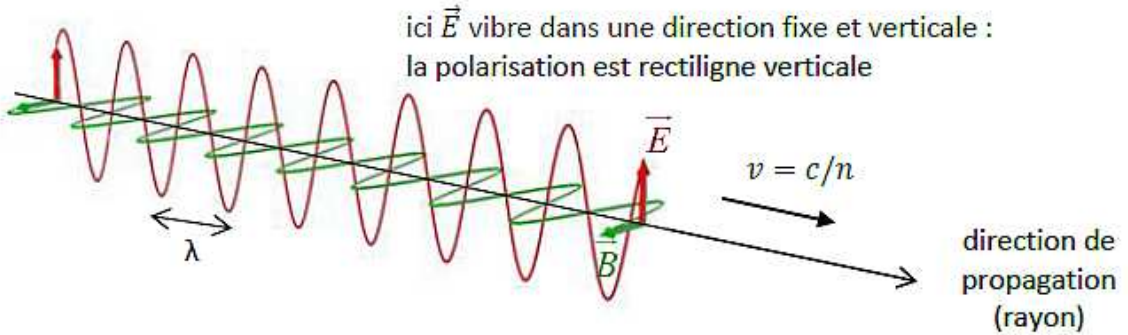
* Chiffrement Symétrique : 1 seule clé servant à chiffrer et déchiffrer le message

Problème: arriver à échanger la clé de façon sûre → cryptographie quantique

Polarisation linéaire

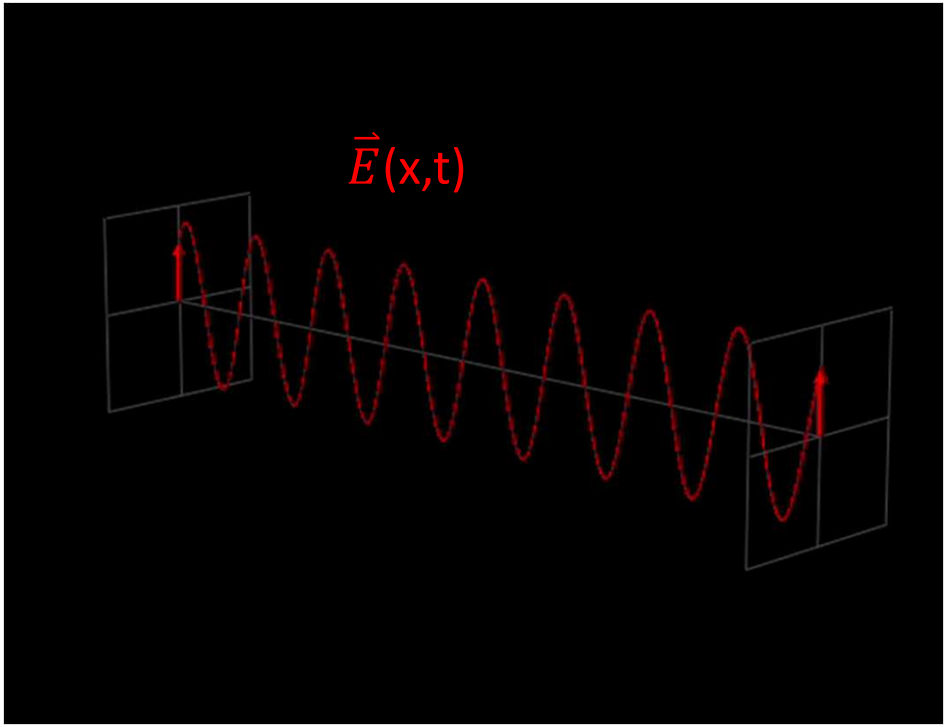
Lumière= onde électromagnétique $\vec{E}$ et $\vec{B}$

Polarisation= direction de **vibration** champs $\vec{E}$

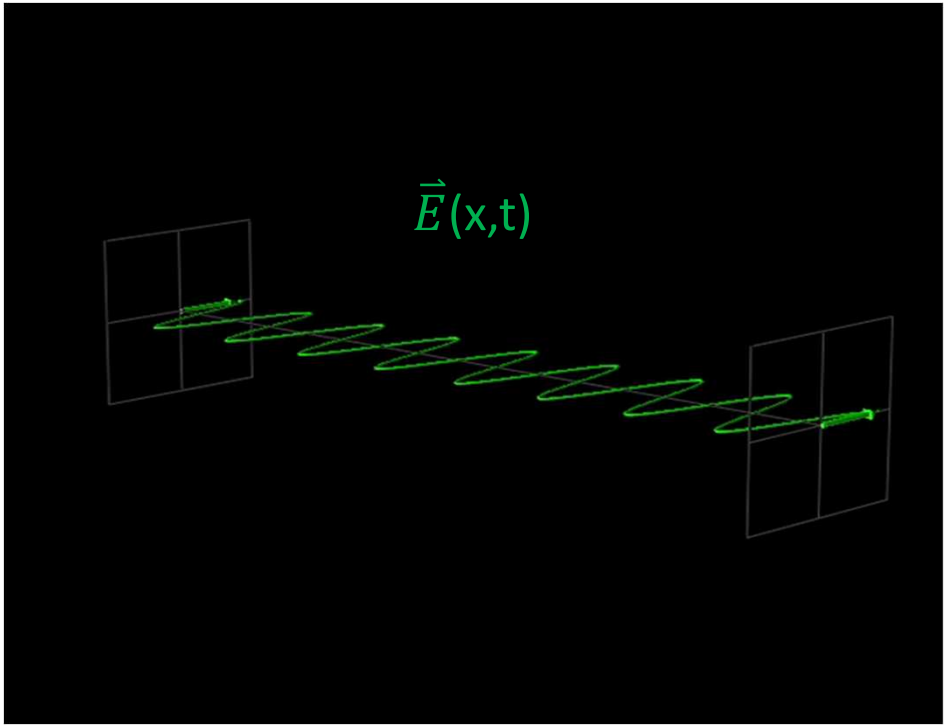


intensité lumineuse I =a E^2

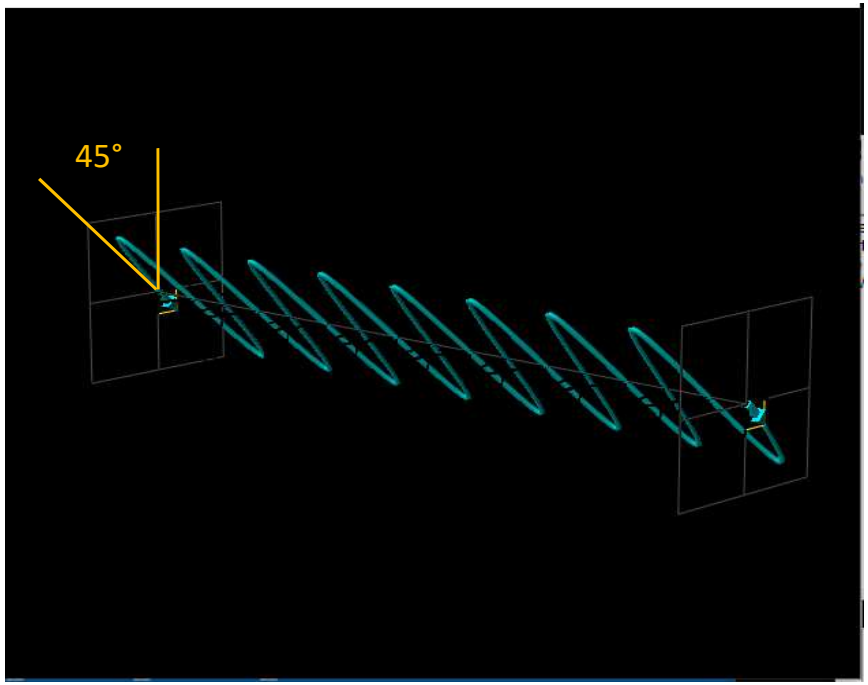
Polarisation Verticale

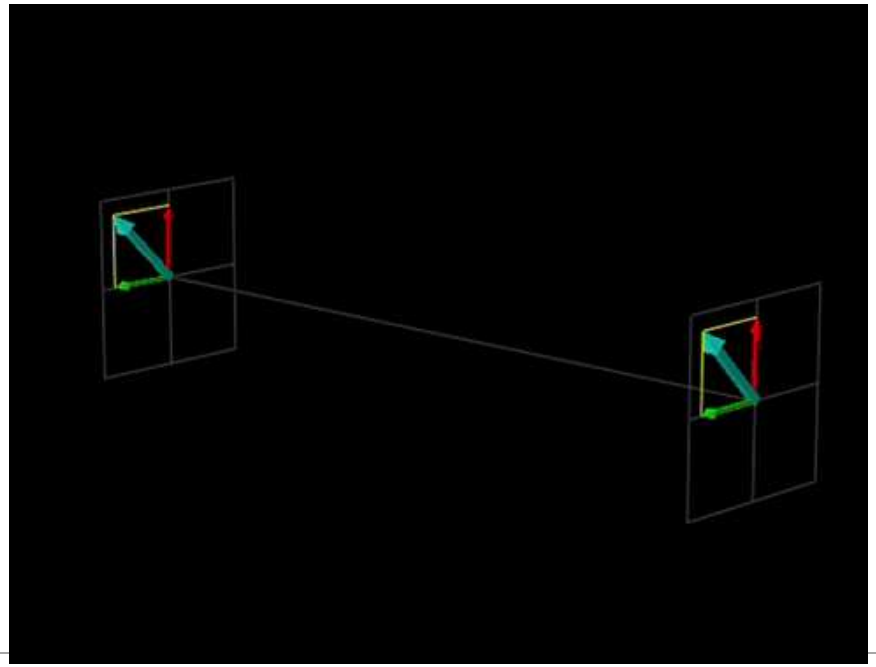


Polarisation Horizontale

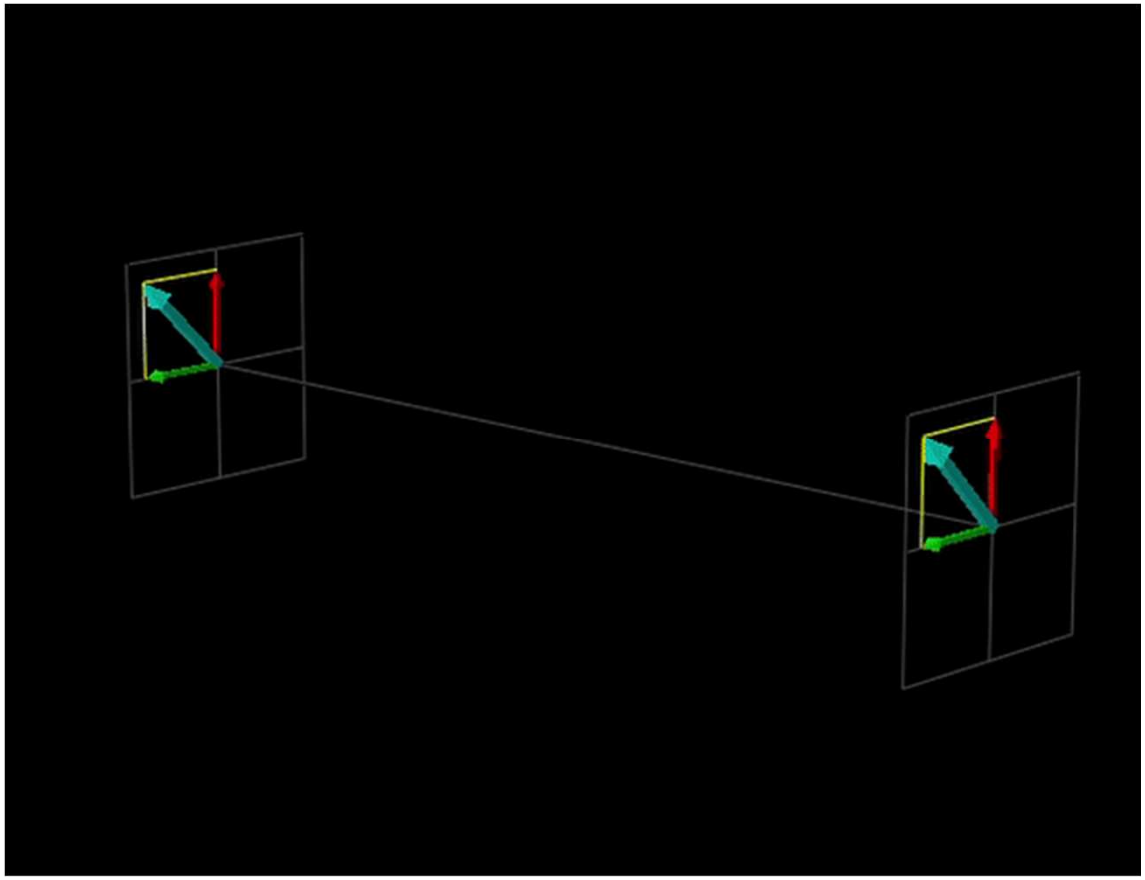


Polarisation linéaire

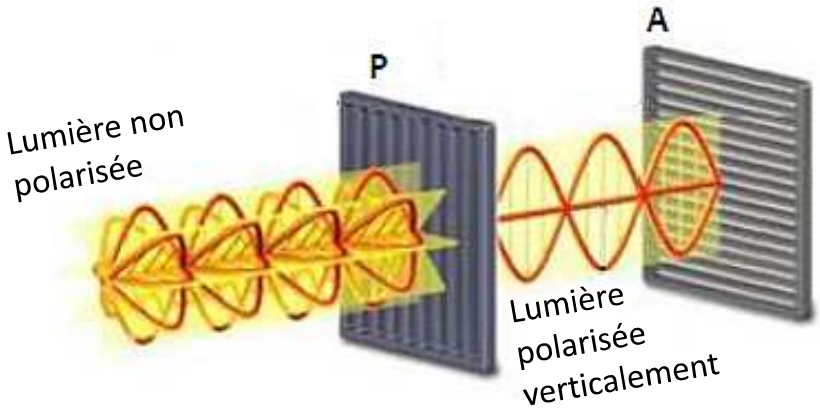




Polarisation à 45° de la verticale



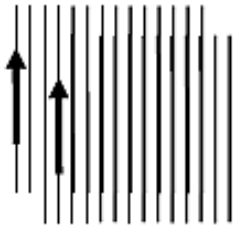
Effet d'un filtre polarisant rectiligne



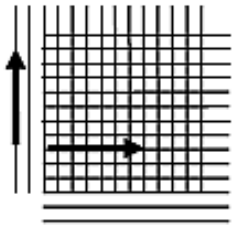
→ extinction si P ⊥ A (on dit qu'on est entre **polariseur et analyseur croisés**)

→ maximum de lumière transmise si P // A (**polariseur et analyseur parallèles**)

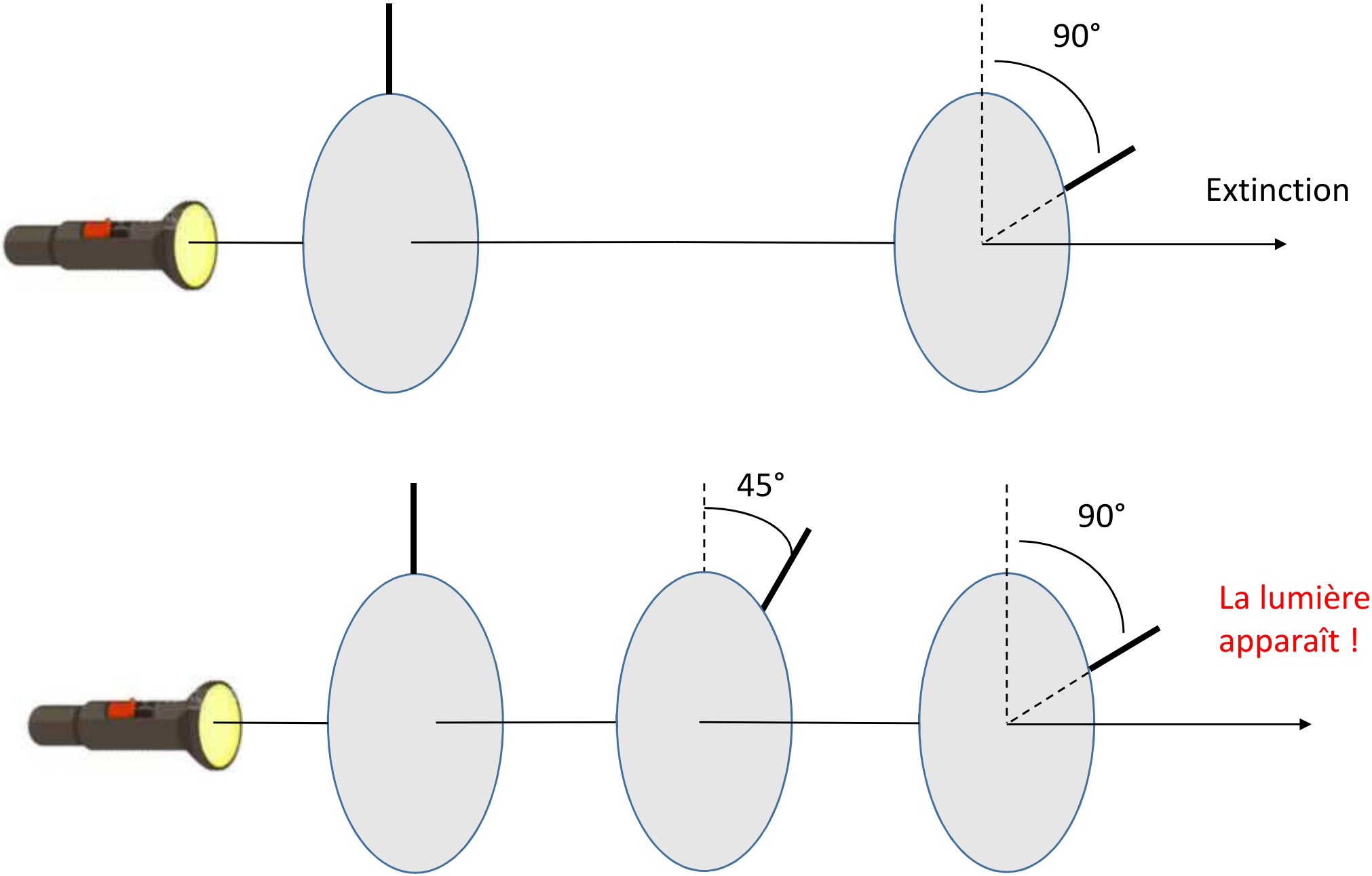
P // A :
la lumière passe



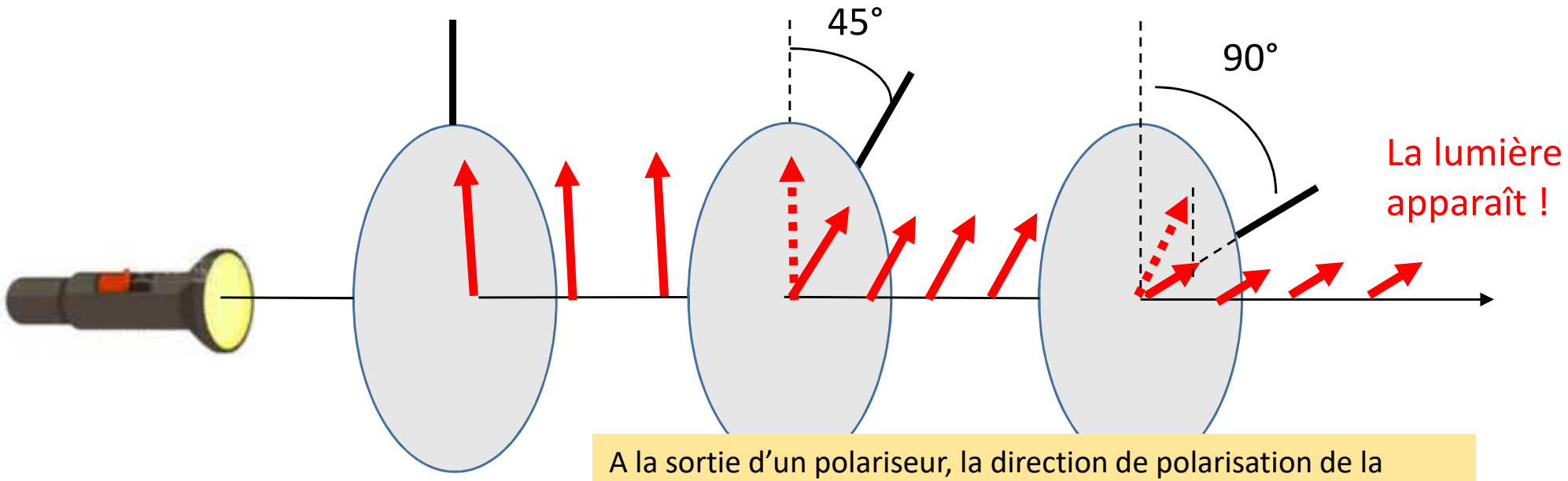
P⊥A :
extinction



Expérience étonnante de polarisation

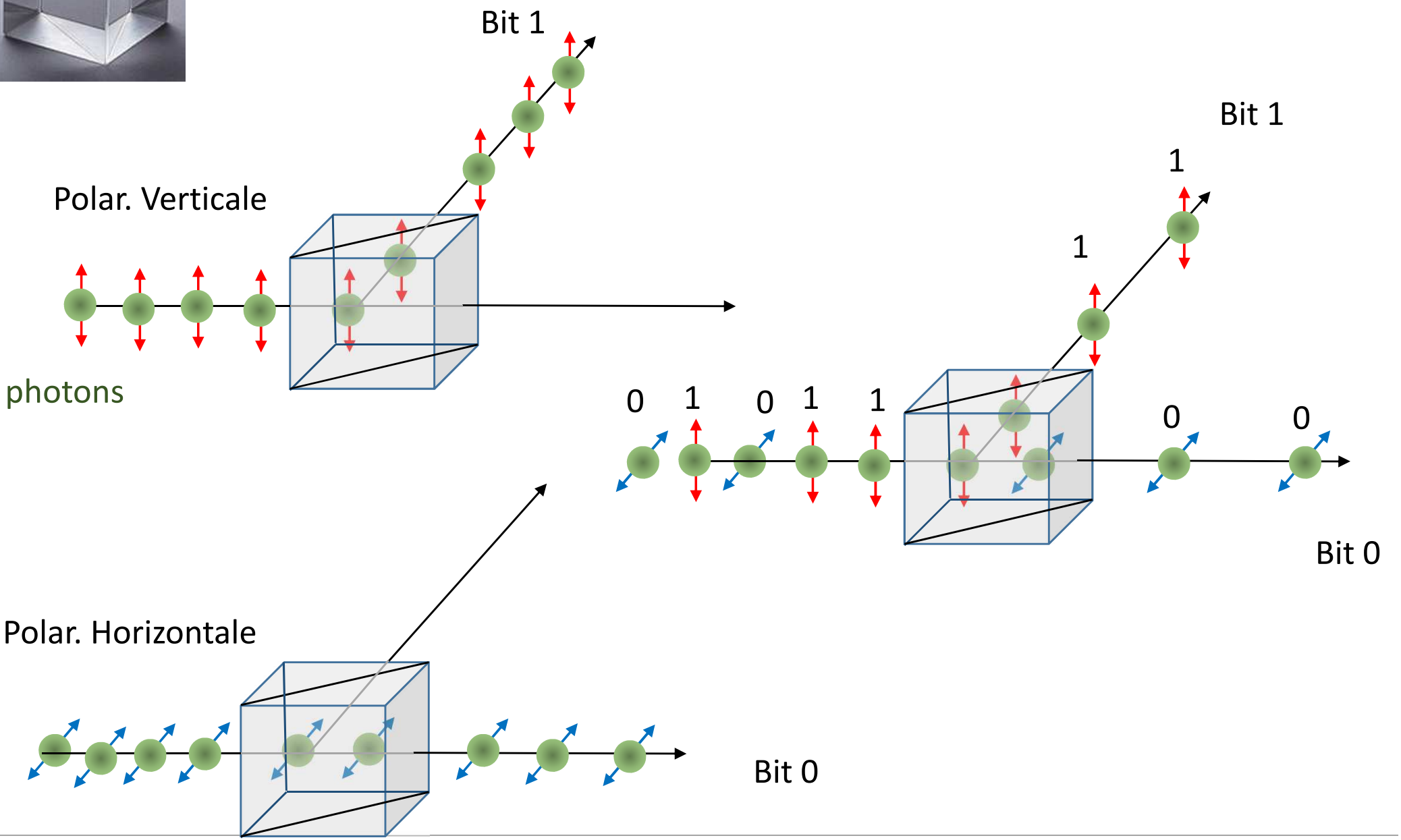


Expérience étonnante de polarisation

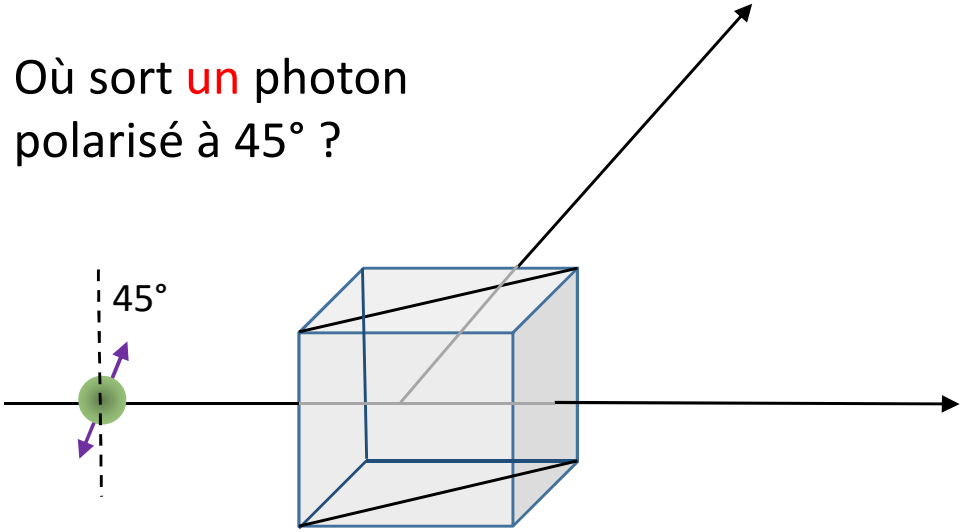


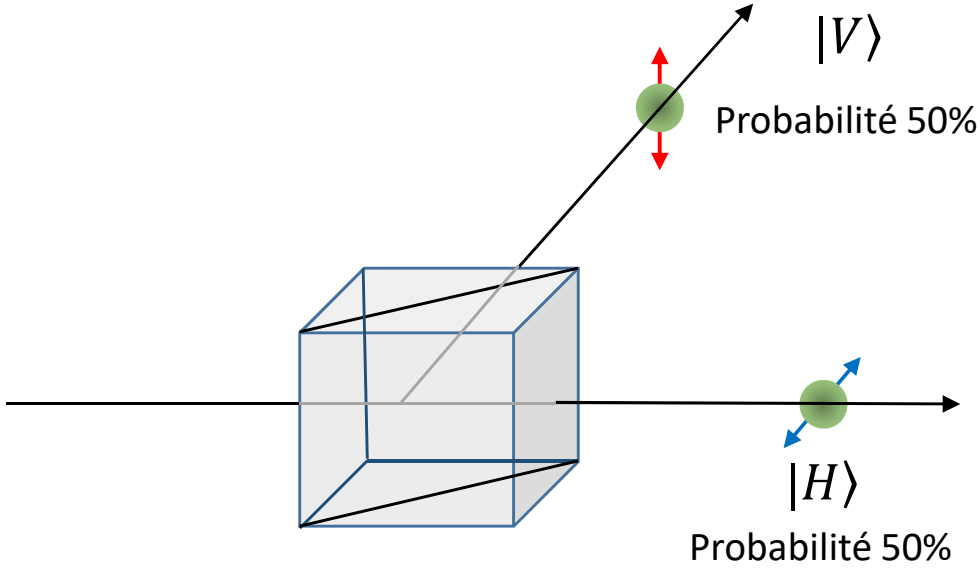
A la sortie d'un polariseur, la direction de polarisation de la lumière est imposée par l'axe du polariseur.

Cube séparatrice de polarisation



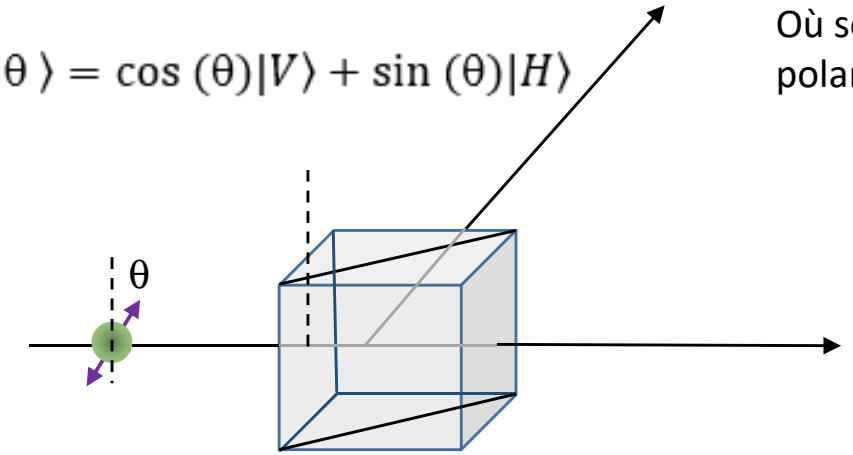
Où sort un photon polarisé à 45° ?



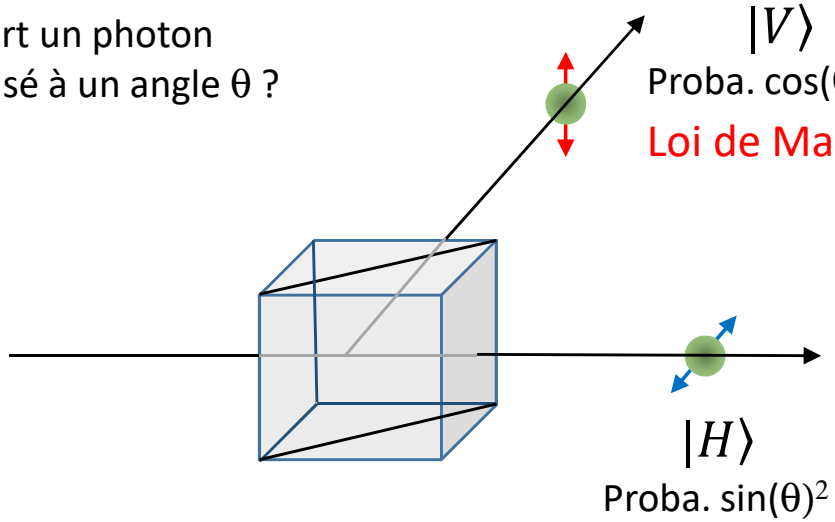


$$|45°\rangle = \frac{1}{\sqrt{2}}(|V\rangle + |H\rangle)$$ *Superposition d'états de polarisation*

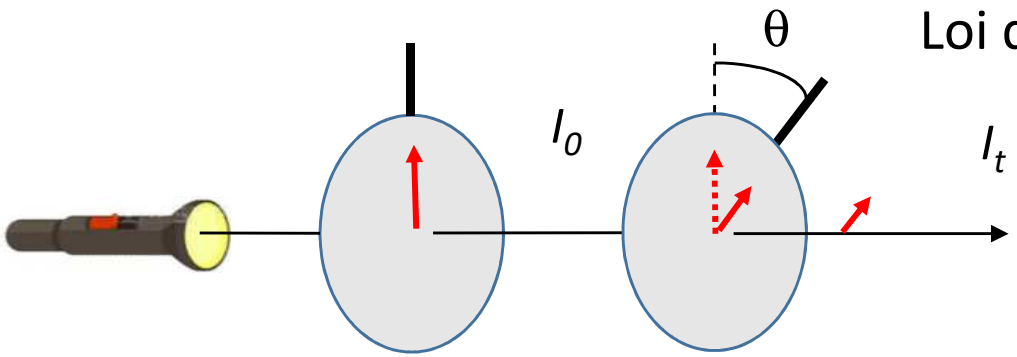
$$|\theta\rangle = \cos(\theta)|V\rangle + \sin(\theta)|H\rangle$$



Où sort un photon polarisé à un angle θ ?



Transmission d'une lumière polarisée à travers un analyseur



Loi de Malus

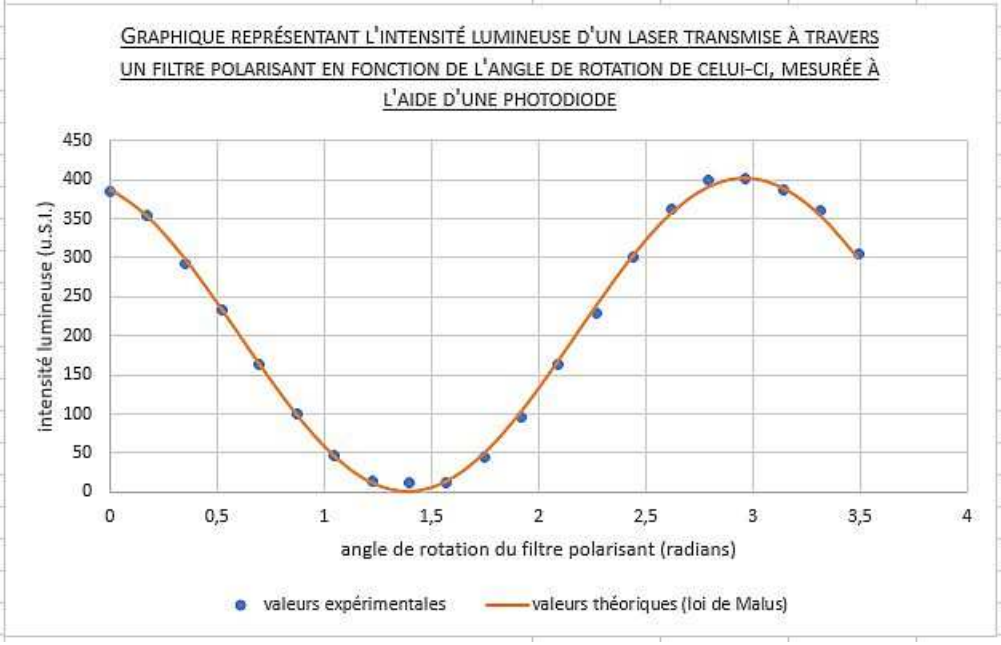
$I_t = I_0 \cos(\theta)^2$

Etienne Louis Malus
(1775-1812)

angle (°)	I mesuré	I théorique
0	384	389,12
10	354	353,55
20	293	299,59
30	233	233,74
40	164	163,93
50	100	98,60
60	46,6	45,62
70	14,7	11,38
80	12,7	0,01
90	11,3	12,88
100	43,8	48,45
110	96	102,41
120	164	168,26
130	229	238,07
140	301	303,40
150	362	356,38
160	400	390,62
170	402	401,99
180	388	389,12
190	360	353,55
200	306	299,59

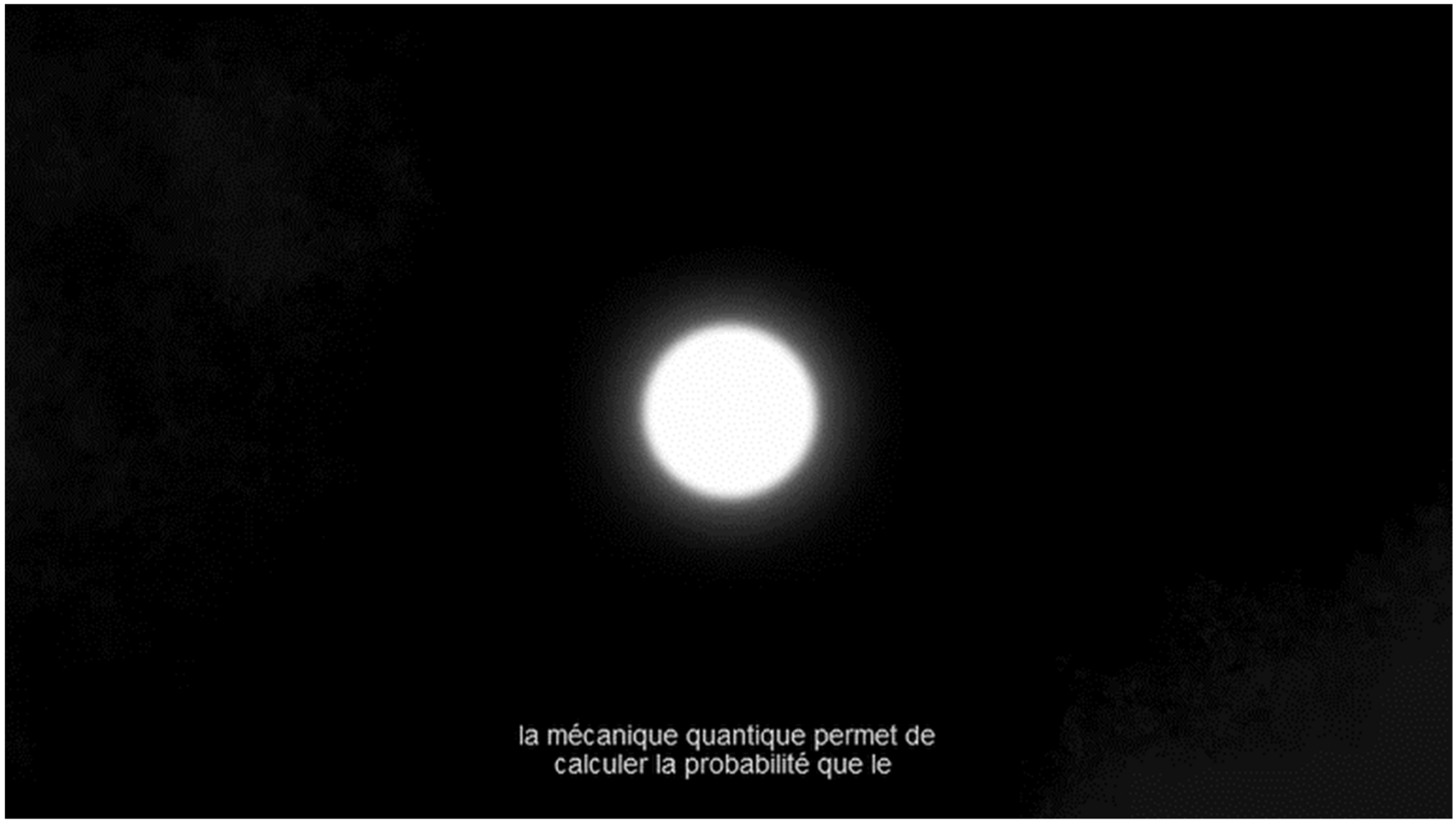
loi de Malus : I'=I*cos^2(θ)

ici on a
I' : I théorique
I : intensité maximale mesurée (=402 usi)
θ : angle de rotation du filtre (rad)
Donc I'=402*cos^2(θ+0,18)
NB : +0,18 correspond à la correction de l'angle pour l'ajustement des courbes



Mesures de TP (étudiante en L1 à l'UGA)

En résumé



Extrait « Intrication Quantique (2/4) : Les inégalités de Bell »
https://www.youtube.com/watch?v=xduUcFflYX0

Alain Aspect:
prix Nobel de Physique 2022

Cryptographie quantique

Utiliser des photons *uniques* pour une communication ultra-sécurisée

Cryptographie quantique: protocole BB84

→ Échange de Qbits photoniques

proposé en 1984 par C. Bennett et G.Brassard

Alice

base	+	+	+	+	+	+	+	+	+
Polar.	→	↑	↑	→	↑	→	→	→	↑
bit	0	1	1	0	1	0	0	0	1

Si Alice et Bob utilise toujours la même base + (ou x),

Bob

base	+	+	+	+	+	+	+	+	+
Polar.	→	↑	↑	→	↑	→	→	→	↑
bit	0	1	1	0	1	0	0	0	1

Cryptographie quantique: protocole BB84

→ Échange de Qbits photoniques

proposé en 1984 par C. Bennett et G.Brassard

Alice

base	+	+	+	+	+	+	+	+	+
Polar.	→	↑	↑	→	↑	→	→	→	↑
bit	0	1	1	0	1	0	0	0	1

Si Alice et Bob utilise toujours la même base + (ou x),

+	+	+	+	+	+	+	+	+
→	↑	↑	→	↑	→	→	→	↑

Eve

Alors Eve peut capter un photon et le renvoyer sans se faire détecter

Bob

base	+	+	+	+	+	+	+	+	+
Polar.	→	↑	↑	→	↑	→	→	→	↑
bit	0	1	1	0	1	0	0	0	1

Cryptographie quantique: protocole BB84

→ Échange de Qbits photoniques

proposé en 1984 par C. Bennett et G.Brassard

Alice

utilise une **séquence aléatoire** de base + ou x

base	+	+	x	x	x	+	x	x	+
Polar.	→	↑	↗	↖	↗	→	↖	↖	↑
bit	0	1	1	0	1	0	0	0	1

Bob

utilise aussi une **séquence aléatoire** de base + ou x

base	+	x	x	x	+	+	x	+	+
Polar.	→	ou ↖ ↗	↗	↖	↑ ou →	→	↖	↑ ou →	↑
bit	0	0 ou 1	1	0	0 ou 1	0	0	0 ou 1	1

Cryptographie quantique: protocole BB84

→ Échange de Qbits photoniques

proposé en 1984 par C. Bennett et G.Brassard

Alice

base	+	+	X	X	X	+	X	X	+
Polar.	→	↑	↗	↖	↗	→	↖	↖	↑
bit	0	1	1	0	1	0	0	0	1

Eve

+	X	+	X	X	+	+	+	X
→		↑ ou ↓	↖		→	↑ ou ↓		ou

Bob

base	+	X	X	X	+	+	X	+	+
Polar.	→	ou	ou	↖	ou	→	ou	ou	ou
bit	0	0 ou1	0 ou 1	0	0 ou 1	0	0 ou 1	0 ou 1	0 ou 1

Proj(t)ection quantique

Alice

Polar. verticale

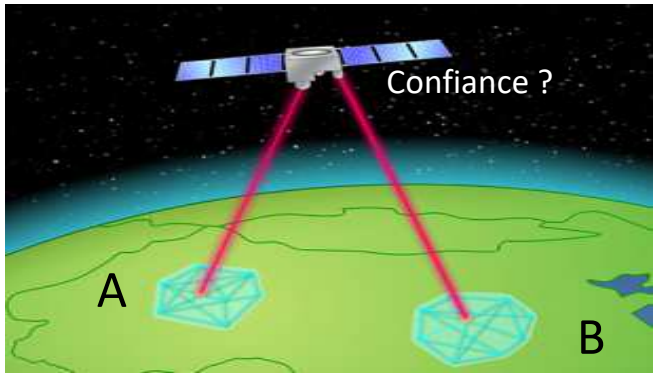
Projection de l'état (polarisation) du photon sur une direction diagonale

Eve

Bob

- Si Alice et Bob échangent N Qbits corrects,
- Eve renvoie environ N/2 mauvais bits à Bob
- Proba pour que Eve ne soit pas détectée $(1/2)^{N/2}$
- N=2000→ 1 chance su $2^{1000} \sim 10^{300}$
- Proba. de remporter le jackpot à l'Euromillion 1 sur 1,39 10^8

Communication à grande distance
→ Nécessite un relai

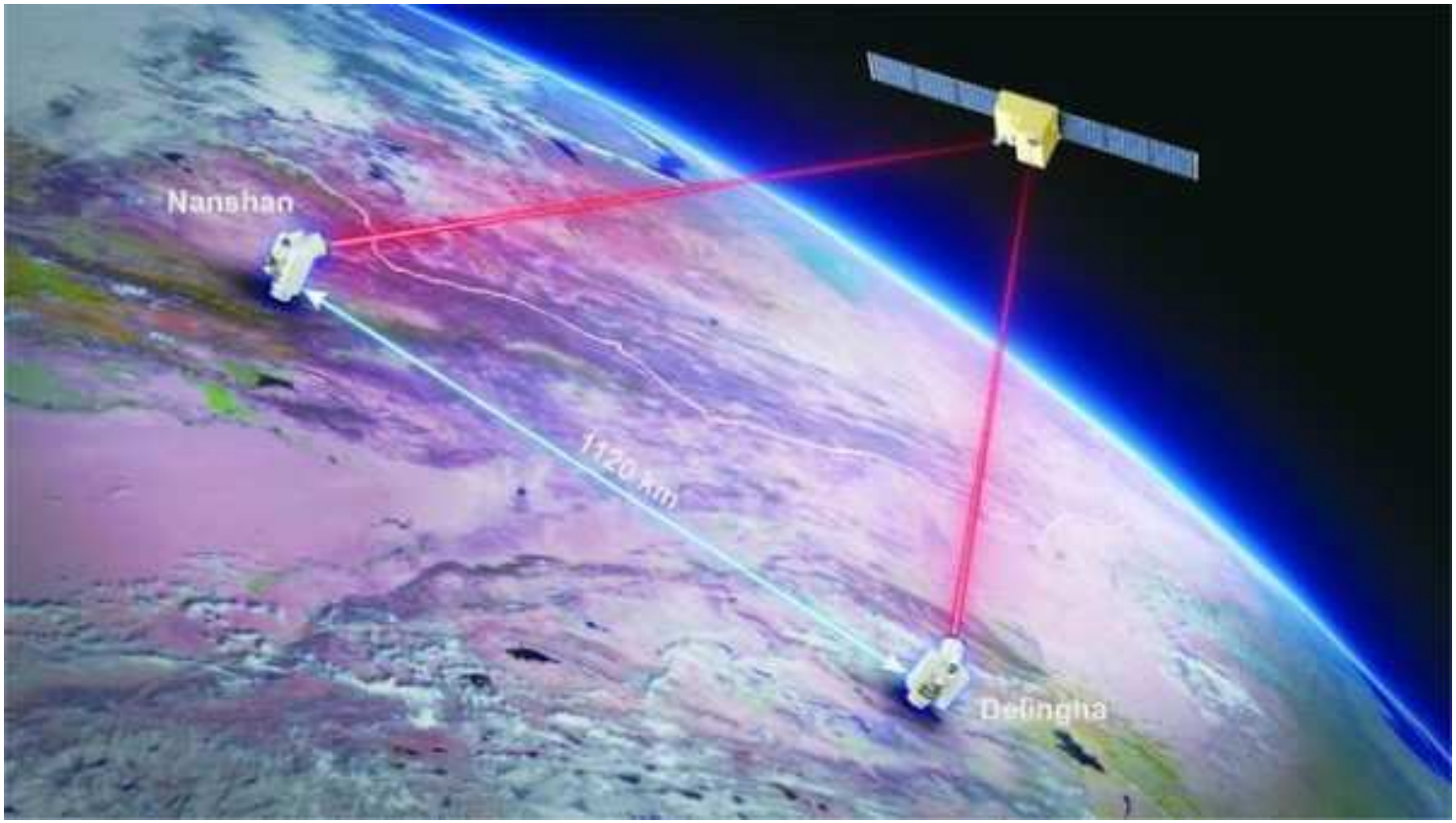


Intérêt des photons intriqués

Paire de photons intriqués
Photons jumeaux

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(|VV\rangle + |HH\rangle)$$

Extrait « Intrication Quantique (2/4) : Les inégalités de Bell »
https://www.youtube.com/watch?v=xduUcFflYX0



Entanglement-based secure quantum cryptography over 1120 kilometers through the Micius quantum science satellite

J. Yin, JW Pan etal., *Nature* **volume 582**, pages501–505 (2020)

University of Science and Technology of China, 2021

https://www.youtube.com/watch?v=OqOM2qh62Pw

Vers un réseau de télécommunication ultra-sécurisée