INSTITUT d'OPTIQUE GRADUATE SCHOOL | IngénIOGS 2025 - 2026 Présentations de projets étudiants

DISTRIBUTION DE CLÉS QUANTIQUES BASÉE SUR LE PROTOCOLE BBM92

Réalisé par ***Amandine LAURET***, ***Aurèle MONCEAU***, ***Enzo GAUTHIER*** et ***Julia CHETRIT*** (Promo 2027), encadré par ***Benjamin VEST***, ***Thierry AVIGNON*** et ***Cédric LEJEUNE***

CRYPTOGRAPHIE QUANTIQUE

On souhaite distribuer une **clé quantique** (suite de 0 et de 1) **aléatoire et secrète**, de manière sécurisée, à Alice (A) et Bob (B).

- Une fois la clé générée, le message que l'on veut transmettre est **crypté**.
- Alice et Bob peuvent alors **décrypter** le message **grâce à leur clé**.
- Lors de la distribution de clé, il faut pouvoir **détecter** si un **espion** tente de l'intercepter : si la présence d'un espion est détectée, la **distribution** de clé est **arrêtée**.

PROTOCOLE BBM92

Protocole basé sur l'**intrication quantique**.

1. Une source émet des paires de **photons intriqués** : leurs polarisations sont corrélées (orthogonales), mais chaque polarisation individuelle est indéfinie avant la mesure.

2. Alice et Bob reçoivent chacun un photon et choisissent indépendamment une **base de mesure** (ex. : rectiligne ou diagonale).

3. Si Alice et Bob mesurent dans la même base, leurs résultats sont parfaitement **corrélés** : ce résultat partagé devient un bit de clé.

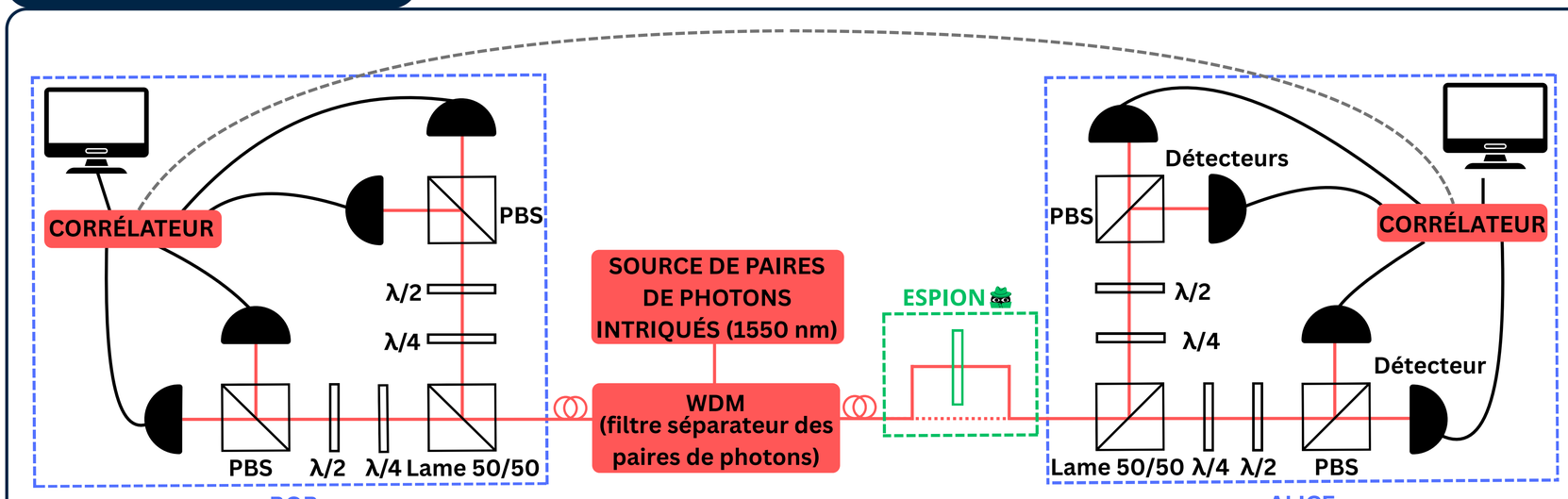
4. Via un canal classique, ils **comparent leurs bases de mesure** (sans révéler les résultats) et ne gardent que les résultats des mesures effectués dans les mêmes bases : cela forme la clé brute.

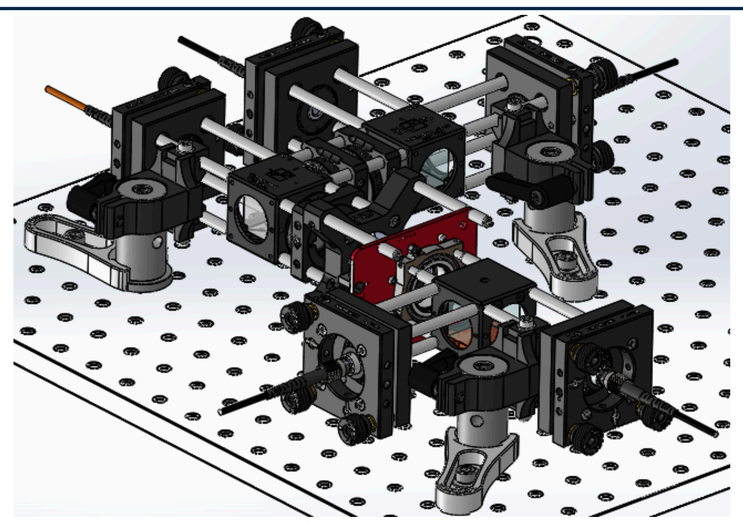
5. Un **espion** qui tente d'intercepter la clé doit effectuer une mesure, ce qui **perturbe les corrélations** quantiques et introduit des erreurs détectables. Si le taux d'erreur dépasse un seuil, la clé est abandonnée.

	A	B	A	B	A	B	A	B	A	B	A	B	A	B	A	B
Base	⤫	✣	⤫	⤫	✣	⤫	✣	✣	⤫	⤫	✣	⤫	✣	✣	⤫	⤫
Mesure	⤢	↕	↘	⤢	↔	⤢	↕	↔	⤢	↘	↕	↘	↔	↕	⤢	↘
Conversion en bit	1	1	0	1	0	1	1	0	1	0	1	0	0	1	1	0
Même base ?	✗		✓		✗		✓		✓		✗		✓		✗	
Bob inverse son bit			0	0			1	1	1	1			0	0		
Sécurité (Test aléatoire)			Oui				Non		Non				Non			
Clé finale							1		1				0			

Tableau explicatif de la distribution d'une clé par le protocole BBM92 [4]

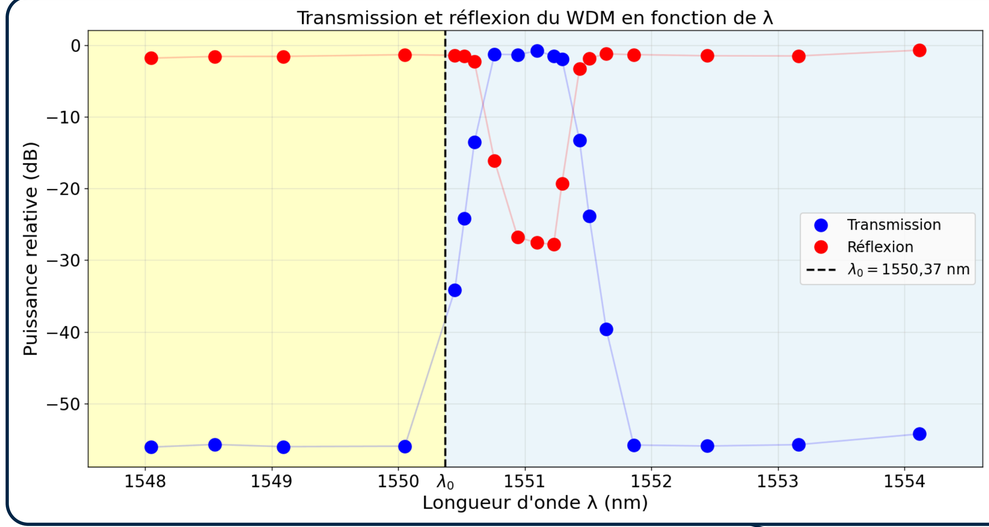
SCHÉMA DU MONTAGE





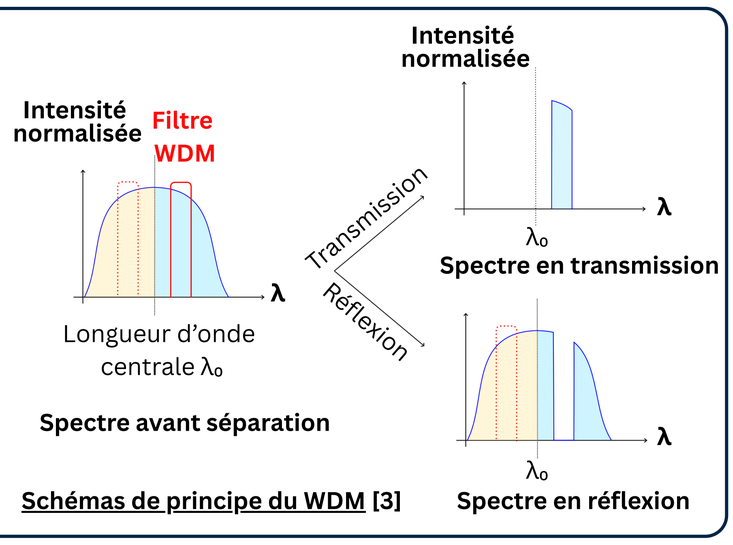
Modélisation Solidworks de la partie Alice

WDM (WAVELENGTH DEMULTIPLEXER)



- Les photons intriqués en polarisation ont une énergie symétrique par rapport à la longueur d'onde centrale λ_0.
- Les photons jaunes peuvent être corrélés aux photons bleu clair, mais deux photons jaunes ne peuvent pas être corrélés car ils ne sont pas de la même paire.
- Transmission : ne contient que des photons simples non corrélés (leurs jumeaux intriqués se trouvent dans la sortie réfléchie)

← **Courbe expérimentale de caractérisation du WDM**



Schémas de principe du WDM [3]

ALICE ET BOB

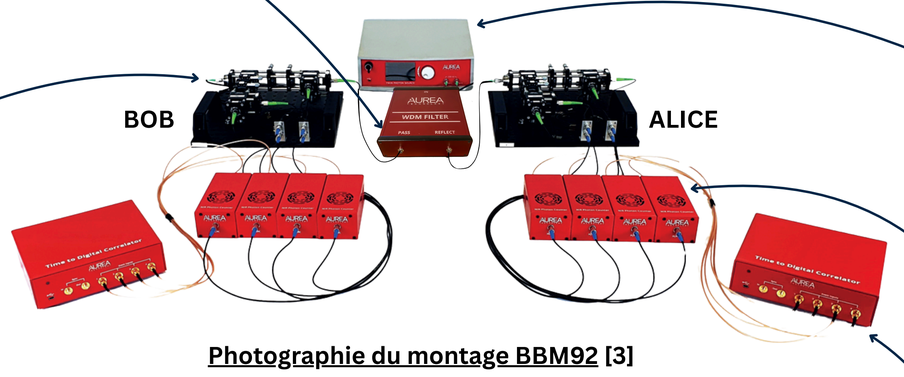
L'état intriqué en polarisation incident est le suivant :

$$|\psi\rangle = \frac{|H_{BOB}V_{ALICE}\rangle + |V_{BOB}H_{ALICE}\rangle}{\sqrt{2}}$$

Pour chaque paire de photons intriqués, Alice reçoit un photon et Bob reçoit l'autre. On a alors :

$$\begin{matrix} P_{V_{ALICE}}(H_{BOB}) = 1 \\ P_{D_{ALICE}}(A_{BOB}) = 1 \end{matrix} \quad P(H_{BOB}) = P(V_{BOB}) = \frac{1}{2}$$

Les probabilités individuelles sont aléatoires mais les résultats d'Alice et Bob parfaitement corrélés !



Photographie du montage BBM92 [3]

SOURCE DE PHOTONS INTRIQUÉS

- Le cristal génère des **paires** de photons **intriqués en polarisation**, de longueurs d'onde complémentaires.
- Processus **non linéaire** : Conversion Paramétrique Spontanée (SPDC type II) : les photons sont **corrélés** en énergie et en **polarisation** (polarisations orthogonales entre elles).
- **Spectres** des deux photons **confondus**, à la température de **dégénérescence** : T = 51.25 °C

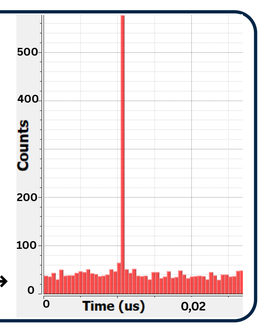
DÉTECTEURS

Les **photodétecteurs à avalanche** récupèrent les photons issus de chaque base. Ce sont des **semiconducteurs InGaAs** qui fonctionnent par impulsions TTL. Les résultats d'Alice et Bob sont comparés grâce aux corrélateurs.

CORRÉLATEURS

Les deux corrélateurs mesurent les **retards entre les voies** ("cross correlation"). Cela permet d'**apparier** la **détection** d'un photon côté Alice avec son jumeau détecté côté Bob.

Pic de corrélation expérimental →



INÉGALITÉS DE BELL

Elles permettent de quantifier l'**intrication** entre 2 photons.
On note **S** le paramètre de Bell :

$$S = E(a,b) - E(a,b') + E(a',b) + E(a',b') \quad \text{avec}$$

$$E(a,b) = \frac{N(a,b) + N(a+90,b+90) - N(a,b+90) - N(a+90,b)}{N(a,b) + N(a+90,b+90) + N(a,b+90) + N(a+90,b)}$$

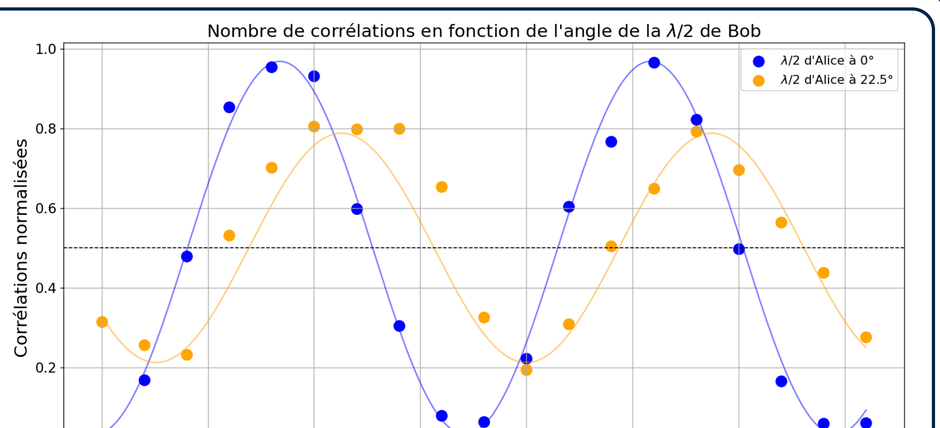
Inégalités :

$|S| \leq 2$: Approche **classique**

$2 < |S| \leq 2\sqrt{2}$: Approche **quantique**

La présence d'un **espion brise l'intrication** et nous donne un résultat **classique** : l'espion est détecté !

Résultats expérimentaux →



IMPACT ENVIRONNEMENTAL

- Emballages des composants optiques : environ 117L d'eau eq, et 33.08kg CO2e pour le montage total [2].
- Matières premières : environ 5kg d'aluminium correspondant approximativement à 45kg CO2e.
- Consommation : source de photons (alim. : 42W max).

LIMITES & AMÉLIORATIONS

- **Automatisation** du calcul des inégalités de Bell grâce aux moteurs déjà montés.
- **Vérification** des alignements (moteurs etc.) pour avoir des meilleurs résultats en corrélation
- **Calcul de S** avec présence de l'**espion** pour comparer.

RÉFÉRENCES

[1] Quantum cryptography without Bell's theorem - C. H. Bennett, G. Brassard, and N. D. Mermin (1992)
[2] Site Internet Thorlabs
[3] Documents techniques et site Internet Aurea
[4] Introduction aux Communications Quantiques - N.Fabre, 2024