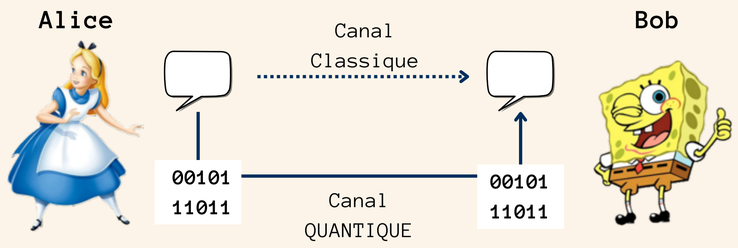
Distribuer des Clés Quantiques

Présentations de projets étudiants

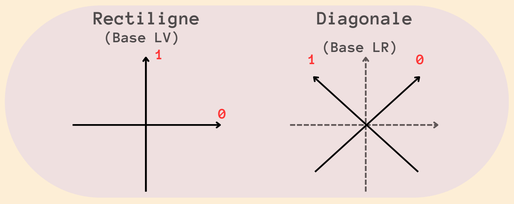
Projet DEPHI 2023-2024 encadré par ***Benjamin Vest*** et réalisé par ***Maxime Laurendin, Enzo Sebiane, Isaline Duperon, Martin Pearlstein*** et ***Salomé Perrin***

La Cryptographie Quantique pour détecter l'espion

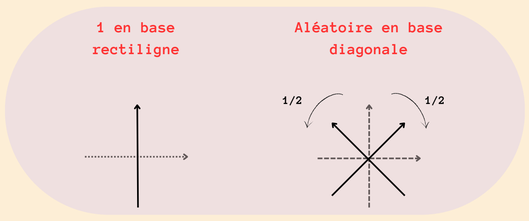


Qu'est-ce qu'un QUBIT ?

1. Choix d'une base de mesure de la polarisation :



2. Mesure d'un photon polarisé aléatoirement (par exemple ↑) : obtention d'un **QUBIT**



Un espion ? Pas de problème !

S'il choisit la **bonne base**, l'espion ne **modifie pas** le bit.

Dans la **mauvaise base**, il a **1 chance sur 2** de le modifier.

Ainsi, un espion **modifie de nombreux** bits.
Sur des milliers, impossible de ne pas le remarquer.

Ainsi, contrairement à tous les outils de cryptographie classique, même les plus puissants, **l'espion peut être détecté**.

Si Alice et Bob ne peuvent pas contourner l'espion, ils peuvent au moins savoir si la clé a été interceptée ou non.

Comment faire ? Le protocole BB84

1. Alice choisit une base (Diagonale D ou Rectiligne R) et un bit (0 ou 1)
2. Elle transmet le bit choisi sur le canal quantique
3. Bob choisit une base dans laquelle le recevoir
4. Il obtient un bit et compare les bases choisies et certains bits obtenus avec Alice
5. Bob et Alice obtiennent leur clé en ne gardant qu'une partie des bits restés secrets

Cas *sans* espion

Base Alice	D	R	D	D	R
Bit Alice	1	1	0	1	0
Base Bob	D	R	R	D	R
Bit Bob	1	1	1	1	0
Clé	1	1		1	0

Cas *avec* espion

Base Alice	D	R	D	D	R
Bit Alice	1	1	0	1	0
Espion	**0**	**1**	**1**	**0**	**0**
Base Bob	**D**	R	**R**	**D**	R
Bit Bob	**1**	1	**1**	**0**	0
Clé	1	1		**0**	0

Si pour un même choix de base **les bits obtenus sont différents**, on peut en déduire **statistiquement la présence d'un espion.**
Alice et Bob n'échangent pas avec cette clé. Donc l'espion ne peut **qu'empêcher la communication et non obtenir son contenu**

Chaque composant est testé seul avant d'être progressivement assemblé avec les autres sur le montage final

EOM

(Générateur d'Etats de Polarisation)

composant actif permettant de **choisir l'état de polarisation** de sortie d'un photon incident polarisé verticalement

```
File   Edit   Setup   C
Current State: RCP
Current State: RCP
Current State: LCP
Current State: LCP
Current State: LVP
Current State: RCP
Current State: LCP
Current State: LVP
Current State: LHP
Current State: L.-45
```

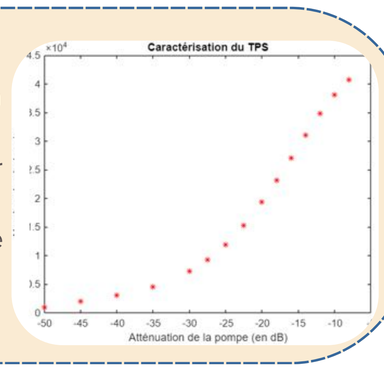
Fonctionne à l'aide d'une interface codée en **C++** et d'une **carte nucléo**

A titre d'exemple, en base circulaire, *RCP = Right Circular Polarisation* et *LCP = Left Circular P.*

6 APD

(Avalanche Photodiode)

En traçant le nb de photons/s en fonction de la puissance, on constate un effet laser attendu du TPS. Un utilise le WDM comme filtre pour que l'APD ne sature pas.

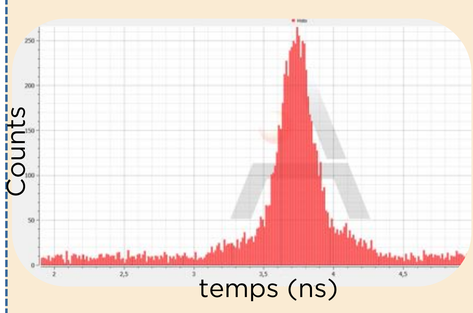


Corrélateur

Mesure les retards entre les signaux des APDs jusqu'à 0,013 ns

Cross correlation

Le corrélateur sert à apparier la détection d'un photon chez Alice avec le photon jumeau détecté par Bob.



Pic de corrélation obtenu

Commander le corrélateur en Python

Fournie par AUREA

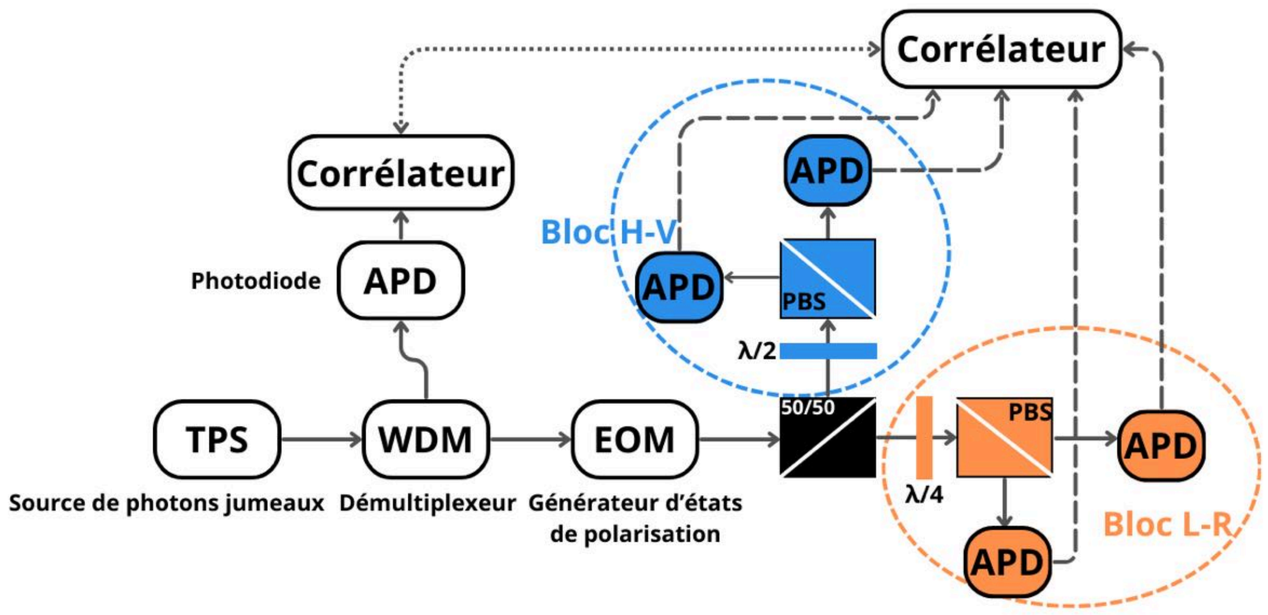
En partie écrit par AUREA, complété par nous

Ecrit en DEPHI *Merci Villou <3*

A écrire par un prochain groupe

Corrélateur
↓ C++
librairie.dll
↓
wrapper.py
(=lien C++ vers Python)
↓
Cross correlation.py
↓
Distribution clef.py

Schéma de principe:



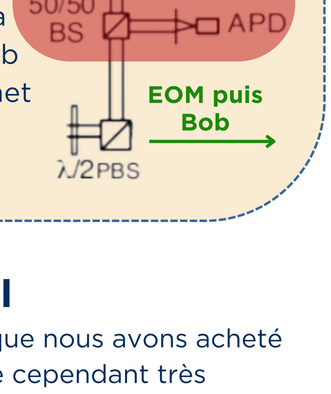
TPS

(Source de Photons Jumeaux)

Par un processus d'optique **non linéaire (conversion paramétrique de type II)**, le cristal génère une paire de photons de **polarisations orthogonales** à λ=1550,3 nm

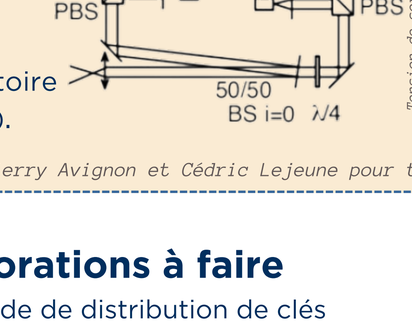
ALICE

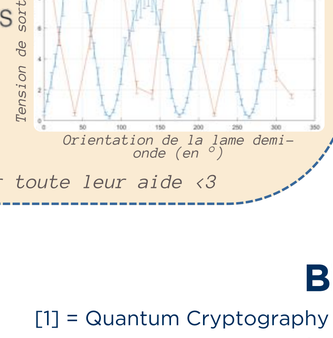
Reconstituer la paire : chaque photon détecté sera associé à un détecté par Bob grâce au corrélateur + permet d'introduire un choix **complètement** aléatoire



BOB

La base de mesure est choisie de manière aléatoire (lame 50/50).





Merci à Thierry Avignon et Cédric Lejeune pour toute leur aide <3

Impact environnemental

- de notre projet: la fabrication par AUREA du matériel que nous avons acheté neuf (561 tonnes eCO2 - la méthode de calcul reste cependant très approximative : connaissant très peu la manière dont le matériel a été fabriqué, on calcule (valeur en €) x 3.3 kg eCO2
- de la **technologie QKD si elle est déployée**: moyen de communication peu énergivore par rapport aux moyens "sans fil" car la propagation est guidée

Améliorations à faire

- Ecrire le code de distribution de clés
- Synchroniser le générateur de polarisation et les deux corrélateurs
- Relier tous les éléments et effectuer un réglage plus durable du montage (aujourd'hui très sensible)

Bibliographie

[1] = Quantum Cryptography : Public Key Distribution & Coin Tossing - Charles H. Benett, Gilles Brassard - 1984
[2] = New Journal of Physics - Experimental open-air quantum key distribution with a single-photon source - R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J-F Roch, A. Beveratos, R. Brouri-Tualle, J-P. Poizat and P. Grangier - 2004
[3]=HDR - Cryptographie quantique avec des photons uniques - Gaëtan Messin
[4] = Notices fournies par Aurea