CRYPTOGRAPHIE QUANTIQUE: TRANSMISSION DE CLÉ

C O N T E X T E

Comment fonctionne la cryptographie classique ?

Information

0 1 1 0 0 1 1 1 0 1 0 1 0 1

Déterministe

C O N T E X T E

Comment fonctionne la cryptographie classique ?

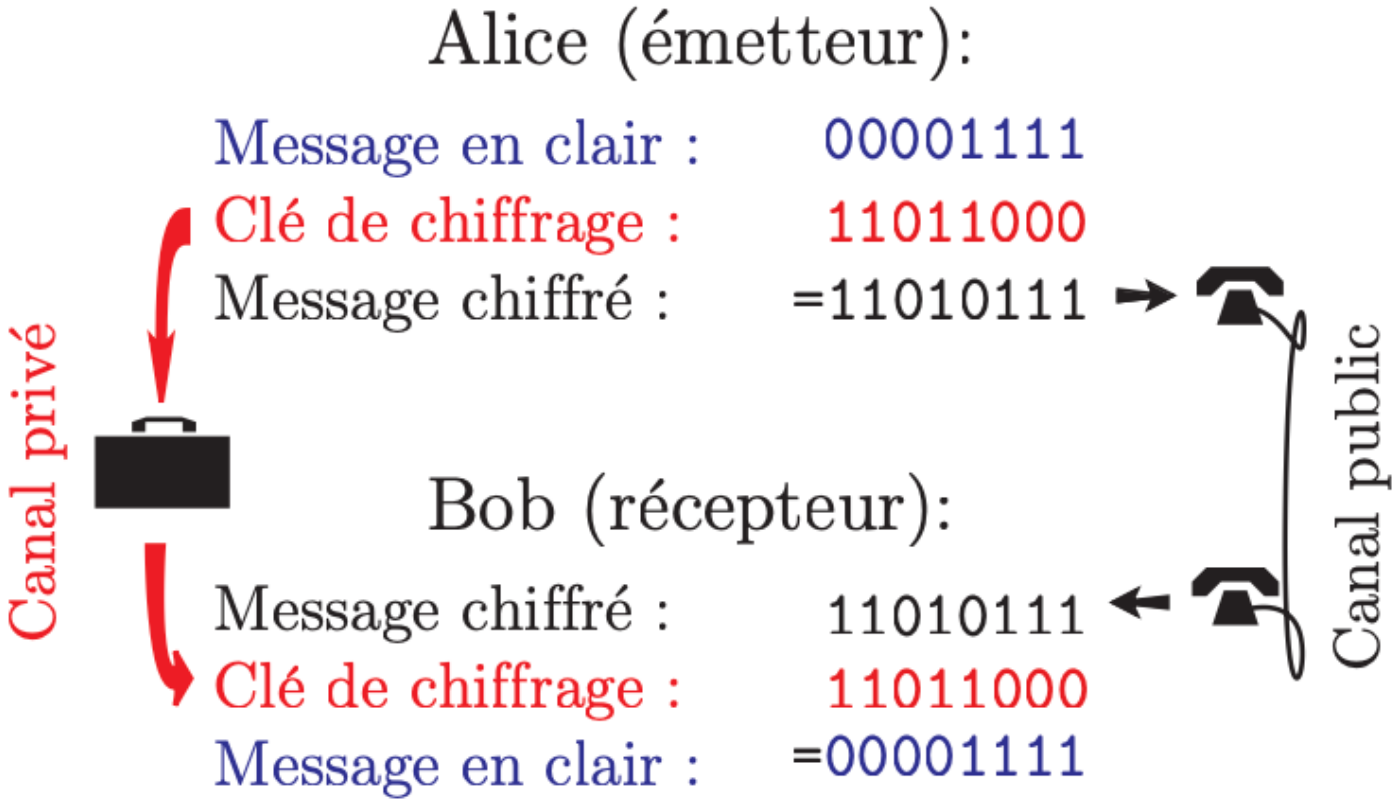
Clé de chiffrage

1 0 1 0 1 1 1 0 1 0 0 1 0 0

Aléatoire

CONTEXTE

Comment fonctionne la cryptographie classique ?



C O N T E X T E

Comment fonctionne la cryptographie classique ?

RSA

ENIGMA

DES

CONTEXTE

Comment fonctionne la cryptographie classique ?

RSA

ENIGMA

DES

sont très difficiles à décoder

mais **PAS IMPOSSIBLE** techniquement

CONTEXTE

Problématique

Comment échanger des clés de manière sécurisée ?

CONTEXTE

Problématique

Comment échanger des clés de manière sécurisée ?

=> Quantique ?

CONTEXTE

Cryptographie Quantique
Le Protocole BB84

Bennett & **B**rassard

proposé en 19**84**


New Journal of Physics

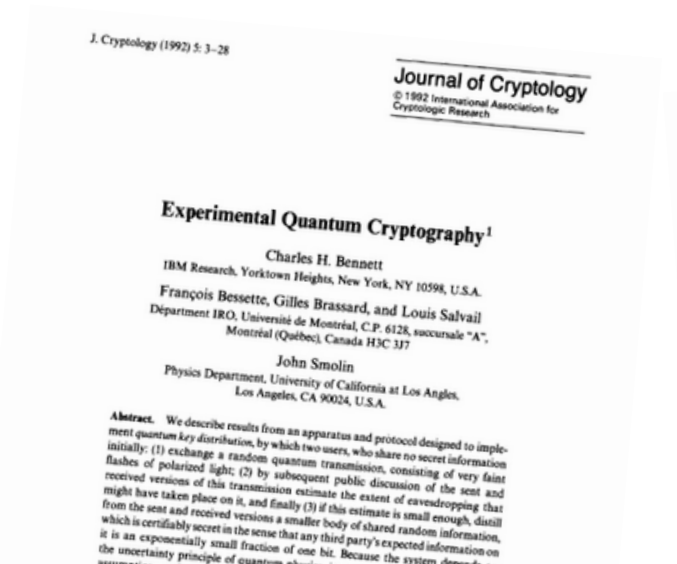
Experimental open-air quantum key distribution with a single-photon source

R Alléaume[1], F Treussart[1], G Messin[2], Y Dumeige[1], J-F Roch[1], A Beveratos[2], R Brouri-Tualle[2], J-P Poizat[2] and P Grangier[2]

[1] Laboratoire de Photonique Quantique et Moléculaire, UMR 8537 du CNRS, ENS Cachan, 61 avenue du Président Wilson, 94235 Cachan Cedex, France
[2] Laboratoire Charles Fabry de l'Institut d'Optique, UMR 8501 du CNRS, F-91403 Orsay, France
E-mail: treussar@physique.ens-cachan.fr

New Journal of Physics 6 (2004) 92
Received 13 February 2004
Published 29 July 2004
Online at http://www.njp.org/

6


J. Cryptology (1992) 5: 3–28

Journal of Cryptology
© 1992 International Association for Cryptologic Research

Experimental Quantum Cryptography[1]

Charles H. Bennett
IBM Research, Yorktown Heights, New York, NY 10598, U.S.A.

François Bessette, Gilles Brassard, and Louis Salvail
Département IRO, Université de Montréal, C.P. 6128, succursale "A", Montréal (Québec), Canada H3C 3J7

John Smolin
Physics Department, University of California at Los Angles, Los Angeles, CA 90024, U.S.A.

Abstract. We describe results from an apparatus and protocol designed to implement *quantum key distribution*, by which two users, who share no secret information initially: (1) exchange a random quantum transmission, consisting of very faint flashes of polarized light; (2) by subsequent public discussion of the sent and received versions of this transmission estimate the extent of eavesdropping that might have taken place on it, and finally (3) if this estimate is small enough, distill from the sent and received versions a smaller body of shared random information, which is certifiably secret in the sense that any third party's expected information on it is an exponentially small fraction of one bit. Because the system depends the uncertainty principle of quantum

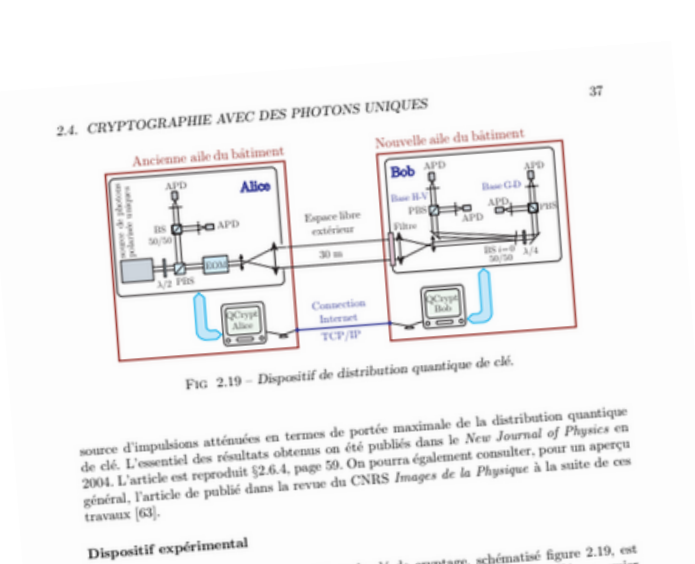

2.4. CRYPTOGRAPHIE AVEC DES PHOTONS UNIQUES 37

FIG 2.19 – Dispositif de distribution quantique de clé.

source d'impulsions atténuées en termes de portée maximale de la distribution quantique de clé. L'essentiel des résultats obtenus on été publiés dans le *New Journal of Physics* en 2004. L'article est reproduit §2.6.4, page 59. On pourra également consulter, pour un aperçu général, l'article de publié dans la revue du CNRS *Images de la Physique* à la suite de ces travaux [63].

Dispositif expérimental

CONTEXTE

Objectifs de BB84

Permet de générer et diffuser une

clé de chiffrage

constituée de **QUBITs**

= photons polarisés

C O N T E X T E

Comment est crée QUBIT ?

0 ou **1** dans une base choisie

Rectiligne

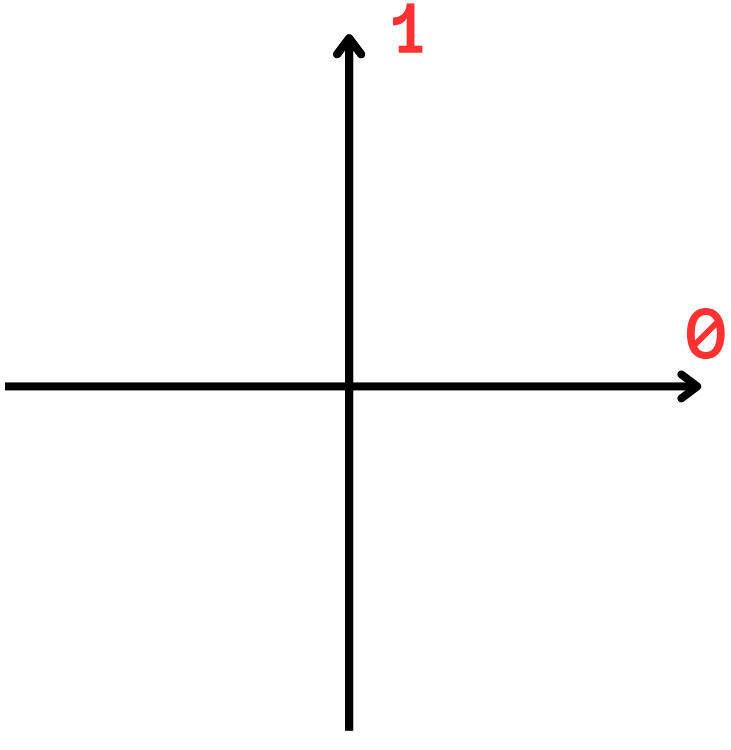
Diagonale

Circulaire

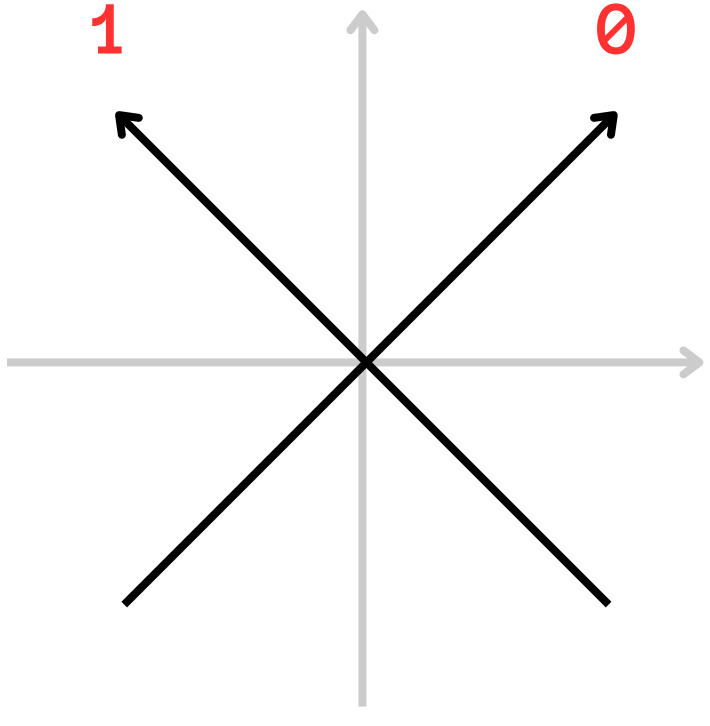
C O N T E X T E

Comment est crée QUBIT ?

Rectiligne



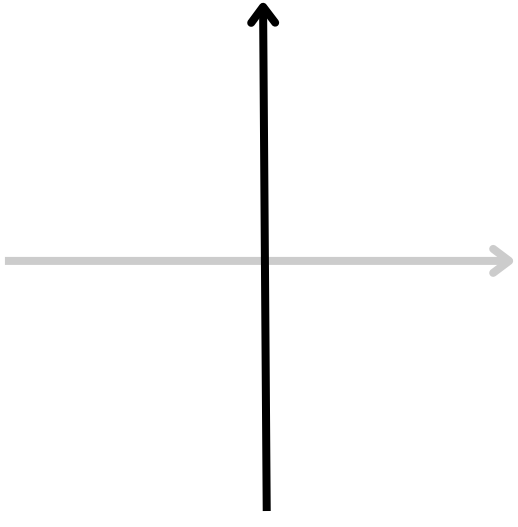
Diagonale



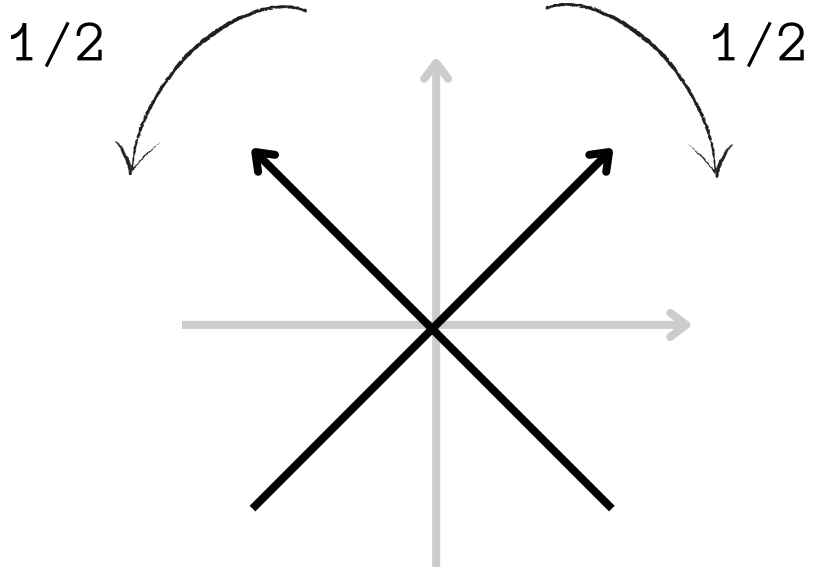
CONTEXTE

Réception d'un QUBIT

1 en base rectiligne



Aléatoire en base diagonale



C O N T E X T E

Pourquoi BB84 est révolutionnaire ?

L‘espion ne peut **jamais** récupérer la clé

Mécanique Quantique

intercepter et réémettre un QUBIT le modifie

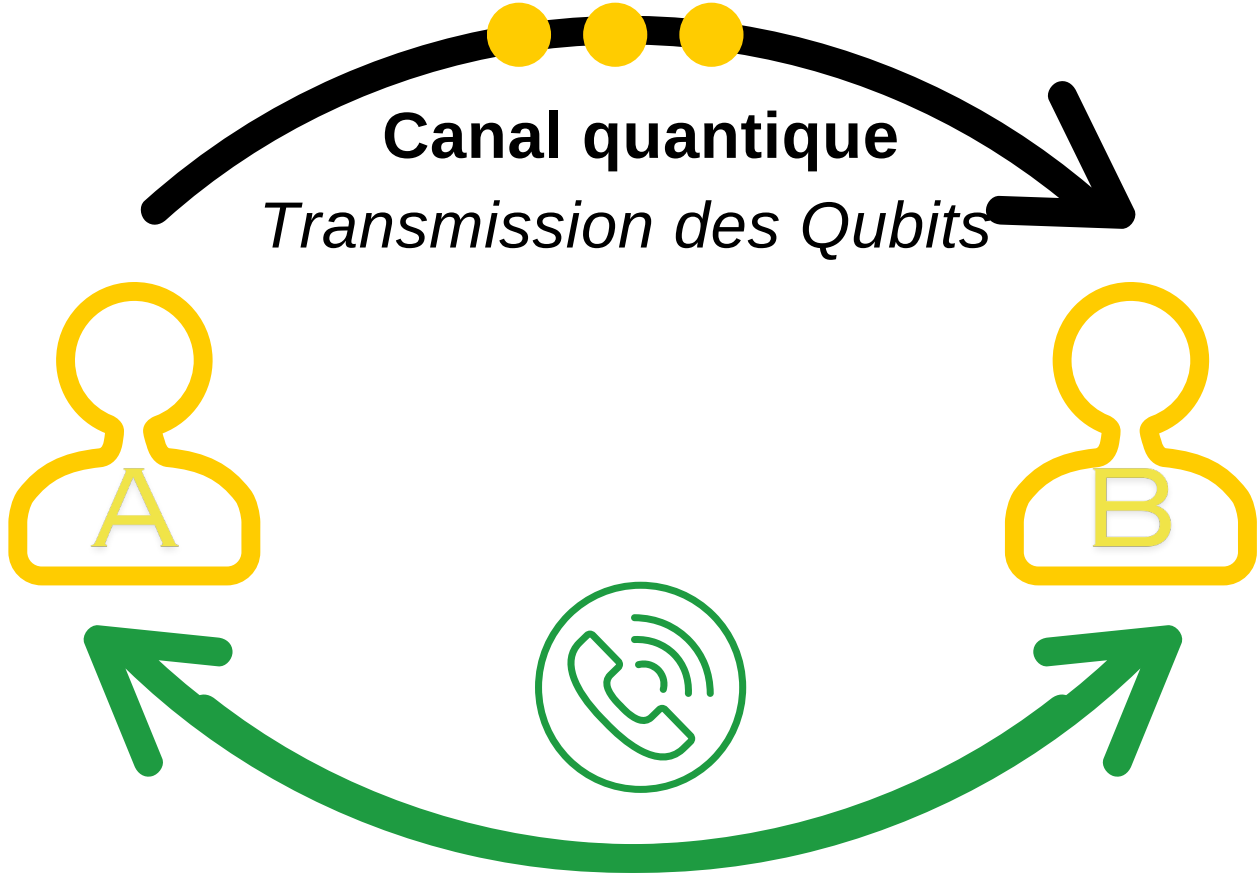
CONTEXTE

Objectif

Établir un protocole simple pour réaliser BB84 et permettre à deux interlocuteurs de s'échanger des clés en toute sécurité

PROTOCOLE BB84

Principe de la distribution quantique de clé



PROTOCOLE BB84

Protocole

Canal quantique

1. Choix de base, codage bit

Base Alice	R	D	D	R
Bit Alice	1	0	1	1
Base de mesure Bob				
Bit mesuré par Bob				
Clef				

Protocole BB84

Canal quantique

1. Choix de base, codage bit
2. Transmission

Base Alice	R	D	D	R
Bit Alice	1	0	1	1
Base de mesure Bob				
Bit mesuré par Bob				
Clef				

PROTOCOLE BB84

Protocole

Canal quantique

1. Choix de base, codage bit
2. Transmission
3. Choix base de mesure

Base Alice	**R**	**D**	**D**	**R**
Bit Alice	1	0	1	1
Base de mesure Bob	D	R	D	R
Bit mesuré par Bob	0	1	1	1
Clef				

PROTOCOLE BB84

Protocole

Canal quantique

1. Choix de base, codage bit
2. Transmission
3. Choix base de mesure

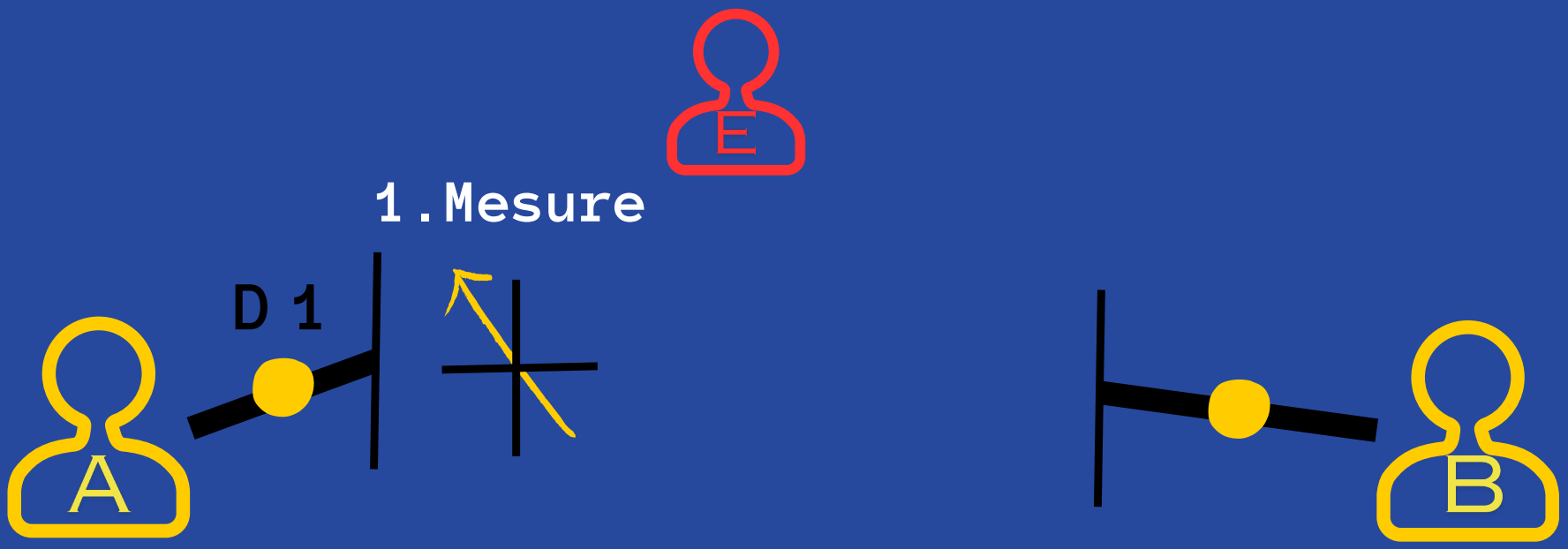
Base Alice	**R**	**D**	**D**	**R**
Bit Alice	1	0	1	1
Base de mesure Bob	D	R	D	R
Bit mesuré par Bob	0	1	1	1
Clef			1	1

Après comparaison des bases choisies :

DONNEES FILTREES

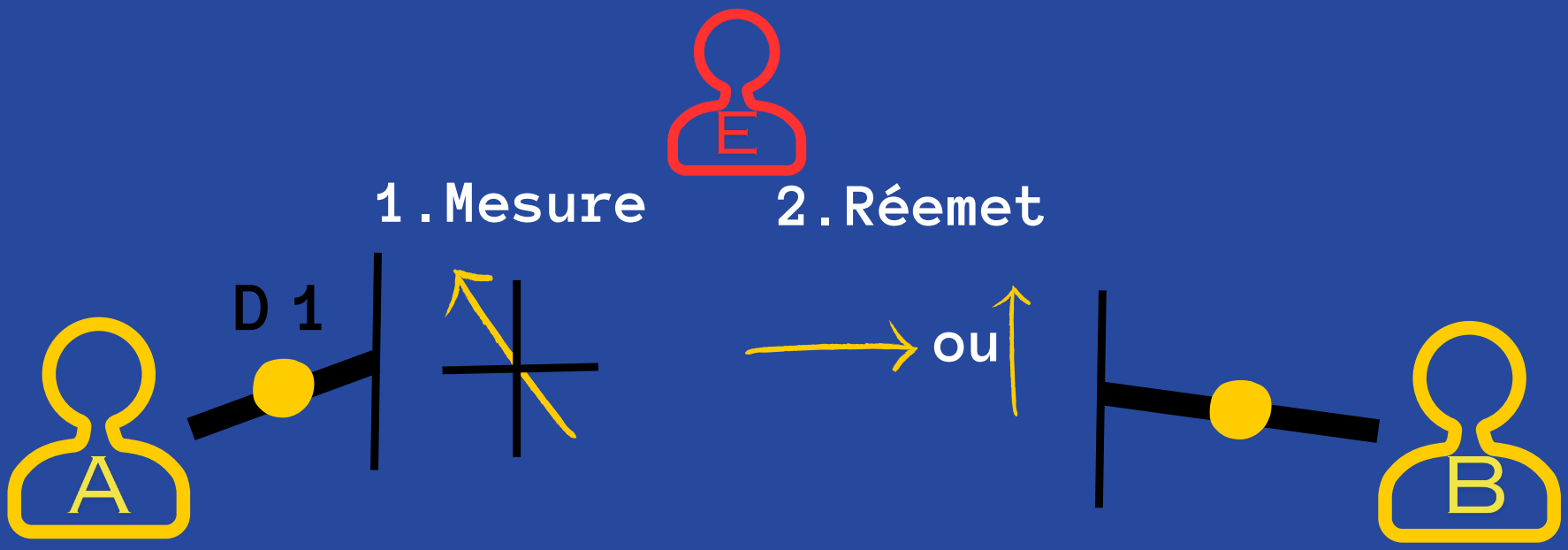
PROTOCOLE BB84

Détecter l'espion



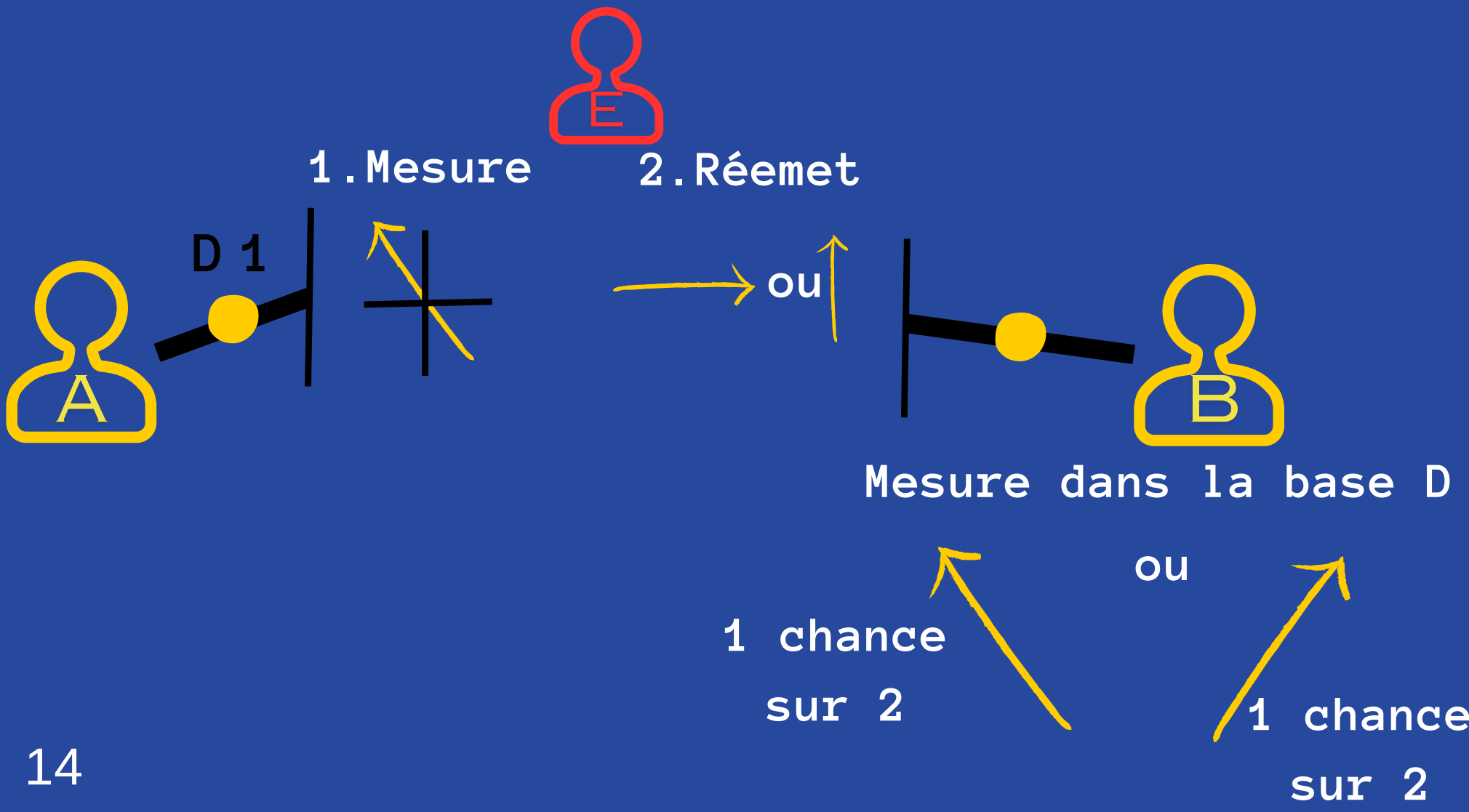
PROTOCOLE BB84

Détecter l'espion



PROTOCOLE BB84

Détecter l'espion



DETECTER L'ESPION

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

Base Alice	R	D	D	R	D	D	R
Bit Alice	0	1	1	1	0	1	0
Espion R							
Base Bob							
Bit Bob							
Clef							

DETECTER L'ESPION

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

Base Alice	R	D	D	R	D	D	R
Bit Alice	0	1	1	1	0	1	0
Espion R							
Base Bob							
Bit Bob							
Clef							

DETECTER L'ESPION

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

Base Alice	R	D	D	R	D	D	R
Bit Alice	0	1	1	1	0	1	0
Espion R							
Base Bob							
Bit Bob							
Clef							

DETECTER L'ESPION

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

Base Alice	R	D	D	R	D	D	R
Bit Alice	0	1	1	1	0	1	0
Espion R	0	0	1	1	1	0	0
Base Bob	D	D	R	R	R	D	R
Bit Bob							
Clef							

DETECTER L'ESPION

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

Base Alice	R	D	D	R	D	D	R
Bit Alice	0	1	1	1	0	1	0
Espion R	0	0	1	1	1	0	0
Base Bob	D	D	R	R	R	D	R
Bit Bob	0	1	1	1	1	0	0
Clef							

DETECTER L'ESPION

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

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

PROTOCOLE EXPÉRIMENTAL

Expérience :

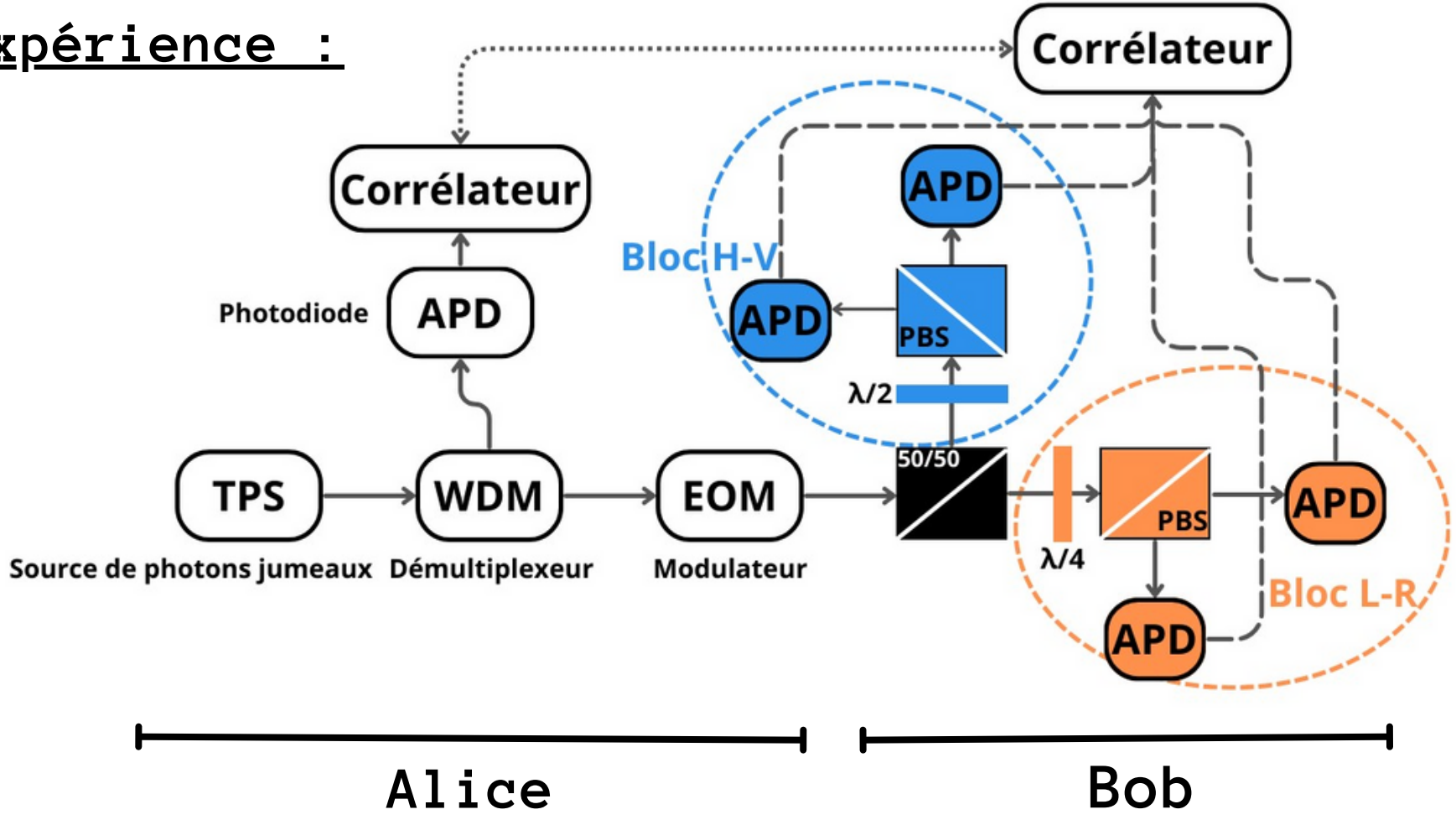


Schéma de principe

COMPOSITION DU MONTAGE

TPS_1550_II

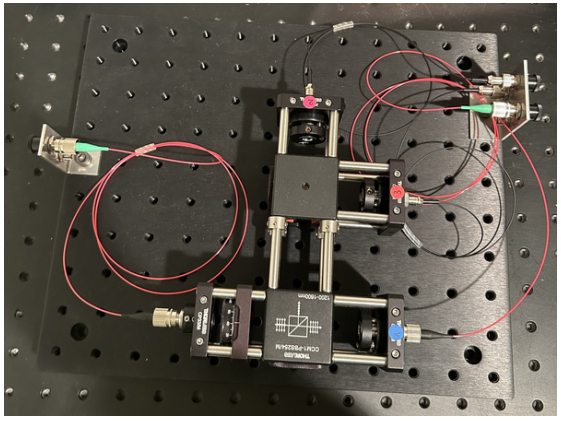
Générateur de photons jumeaux

SPD_OEM_NIR_C

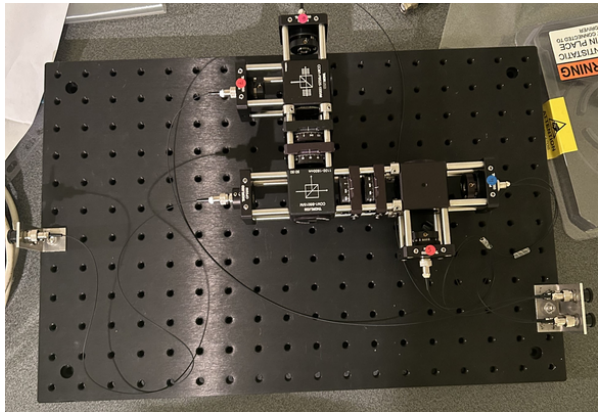
Détecteur et compteur de photons

CHRONOXEA

Corrélateur temporel



Alice



Bob

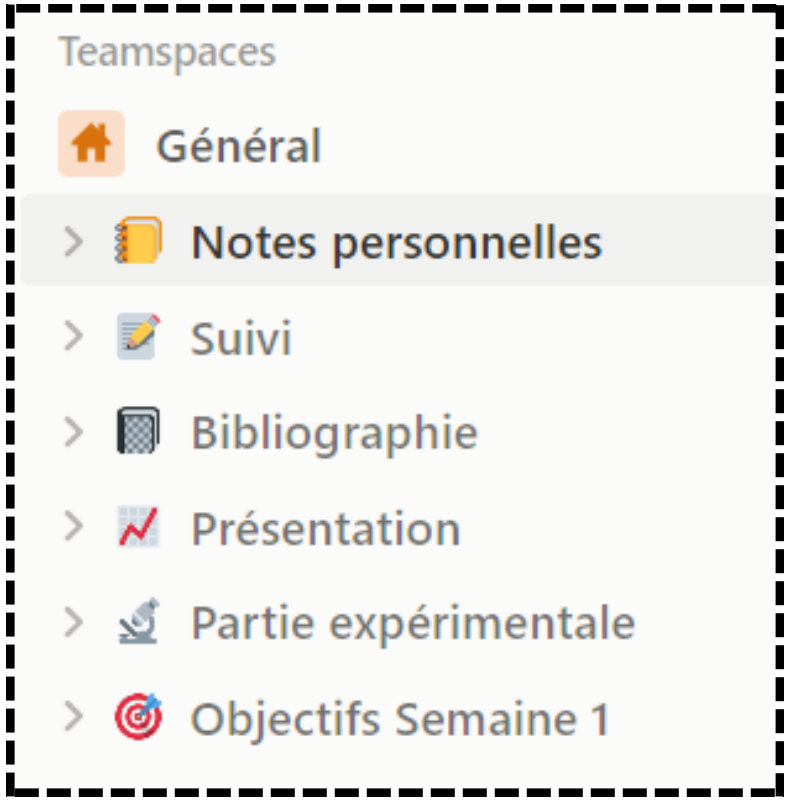
PLANIFICATION DES DIFFÉRENTES ÉTAPES

Difficultés à anticiper

- Coder la communication du **canal classique**
- **Synchronisation temporelle** d'Alice et Bob

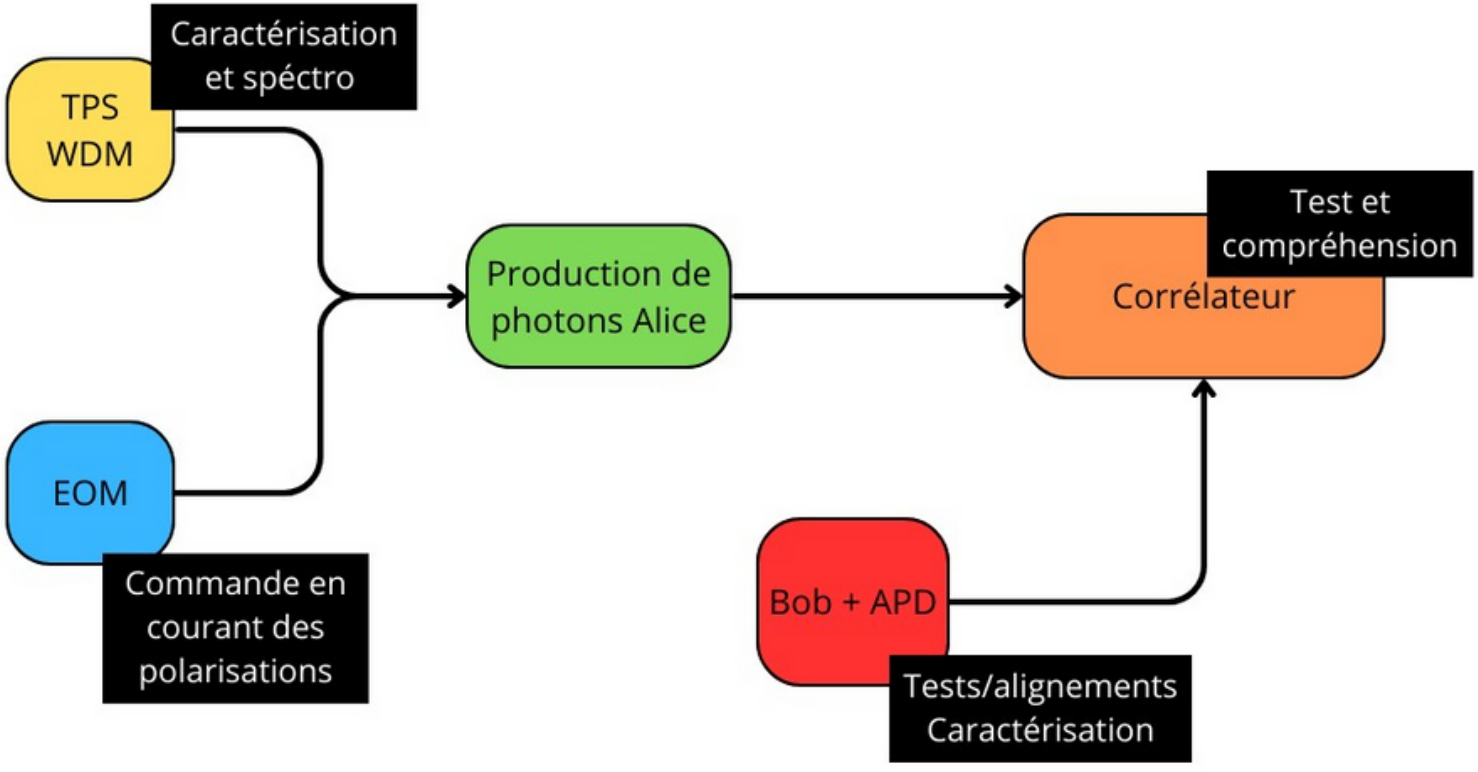
PLANIFICATION DES DIFFÉRENTES ÉTAPES

Utilisation de Notion



PLANIFICATION DES DIFFÉRENTES ÉTAPES

Expérimentations Préparatoires



PLANIFICATION DES DIFFÉRENTES ÉTAPES

Compétences acquises à la fin du projet

- **Salomé** Mobiliser et associer les ressources, moyens et compétences nécessaires au système complet
- **Maxime et Enzo** intégrant les facteurs contextuels qui déterminent sa bonne réalisation d'un système
- **Isaline et Martin** Concevoir et dimensionner une solution technique en photonique pertinente en identifiant les méthodes numériques pertinentes de traitement du signal

MERCI DE VOTRE ECOUTE !

Des questions ?

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] = Journal of Cryptology – Experimental Quantum Cryptography – Charles H. Bennett – 1992

[5] = CCAP + CCTP Kit d'enseignement et de prototypage de communication quantique IOGS – 2022

[6] = Acquisition d'un Kit d'enseignement et de prototypage de communication quantique – Proposition technique et commerciale Aurea Technologie, IOGS – 2022

[7] = La cryptographie quantique : l'incertitude quantique au service de la confidentialité – Frédéric Grosshans, Philippe Grangier – 2014