Contribution à l'étude et la réalisation de systèmes de transmissions optiques sécurisées

Quyen Dinh Xuan

N° ENSC – 2007/51

THÈSE DE DOCTORAT
DE L'ÉCOLE NORMALE SUPÉRIEURE DE CACHAN

présentée par

DINH XUAN Quyen

pour obtenir le grade de

DOCTEUR DE L'ÉCOLE NORMALE SUPÉRIEURE DE CACHAN

domaine
SCIENCES PHYSIQUES

Sujet de la thèse :

CONTRIBUTION À L'ÉTUDE ET LA RÉALISATION DE SYSTÈMES DE TRANSMISSIONS OPTIQUES SÉCURISÉES

Soutenue à Cachan le 12 juillet 2007 devant le jury composé de :

M. Jean-Claude SIMON (ENSSAT, Lannion)……...Président
Mme Françoise PERROT (Université Cergy-Pontoise)……..Rapporteur
M. Emmanuel BIGLER (ENSMM, Besançon)……. Rapporteur
M. Sylvain ALLANO (ENS Cachan)…….……...Examinateur
M. Bernard JOURNET (ENS Cachan)...……...……Examinateur
Mme Mireille TADJEDDINE (ENS Cachan)……...……Examinateur
M. VU Van Luc (ASTV, Vietnam)……...…Examinateur

Laboratoire Systèmes et Applications des Technologies de l'Information et de l'Energie
ENS CACHAN/CNRS/UMR 8029
61, avenue du Président Wilson, 94235 CACHAN CEDEX (France)

****

Remerciements

Je remercie M. Sylvain Allano, directeur du Laboratoire Systèmes et Applications des Technologies de l'Information et de l'Energie, de m'y avoir accueilli et d'avoir accepté d'être directeur de thèse. Un très grand merci à Mme Mireille Tadjeddine pour son soutien depuis mon arrivée en France et tout au long de ma thèse.

Je voudrais remercier mon directeur de thèse M. Sylvain Allano ainsi que mon directeur des travaux de thèse M. Bernard Journet de m'avoir encadré et d'être disponibles pendant mes quatre ans de thèse. C'est bien sûr à Bernard que je souhaite présenter mes plus vifs remerciements pour avoir principalement dirigé ma thèse et lui présenter l'expression de ma profonde gratitude pour tout ce qu'il a fait pour moi tant dans la vie personnelle que dans le métier scientifique. Je suis très touché par sa générosité et sa gentillesse. C'est Bernard qui m'a beaucoup appris au niveau de la physique et l'électronique par son expertise dans la compréhension des phénomènes physiques et électroniques. Un très grand merci à Jean-François Roch, François Treussart, Romain Alléaume et Xiao Liantuan avec qui j'ai eu le plaisir de collaborer (et d'apprendre sur plusieurs points) sur un projet de détection de la statistique poissonienne des sources laser depuis le début de ma thèse. J'aimerais remercier sincèrement M. Vu Van Luc, responsable du laboratoire Laser Semiconducteur de l'Institut des Sciences des Matériaux (Académie des Sciences et de la Technologie du Viêt Nam à Hà Nôi), et son équipe pour m'avoir accueilli pendant mes séjours de recherche au Vietnam.

Je remercie également l'Ambassade de France à Hanoï (Vietnam), l'Ecole Normale Supérieure de Cachan, M. Pham Xuân-Yêm, M. Odon Vallet, M. Tran Thanh Vân et Père Troger pour leur soutien financier qui m'a permis de réaliser cette thèse. Je tiens à remercier M. Thierry Maurin et l'ensemble du personnel de l'Ecole Doctorale Sciences Pratiques pour leurs aides administratives et leurs programmes de formation d'anglais. Un grand merci aussi à Gilliane Valéro et Martine Grelot pour leur aide au niveau administratif au laboratoire.

Je remercie Nguyen Chi Thành et Jean-Pierre Madrange pour leur aide dans la mise en œuvre du Fabry-Pérot de haute résolution. Je tiens à remercier Jean-Marie Desagulier, Stéphane Callier et Marie-Line Ellapin pour leurs travaux d'élaboration des cartes électroniques. Je tiens à remercier André Clouqueur pour la réalisation du boîtier « CKG-1 » et l'amplificateur de haute tension.

Je remercie tout le personnel et les thésards qui m'ont accompagné tout au long de cette thèse : François Duport, Lam Duy, Luong Vu Hai Nam, etc. Ce travail n'aurait pu être effectué sans les soutiens moraux de nombreuses personnes. Je remercie particulièrement mes parents, mes amis Phong Lan, Lan Huong etc. qui m'ont toujours soutenu de loin ou de près pendant les moments difficiles !

Table des matières

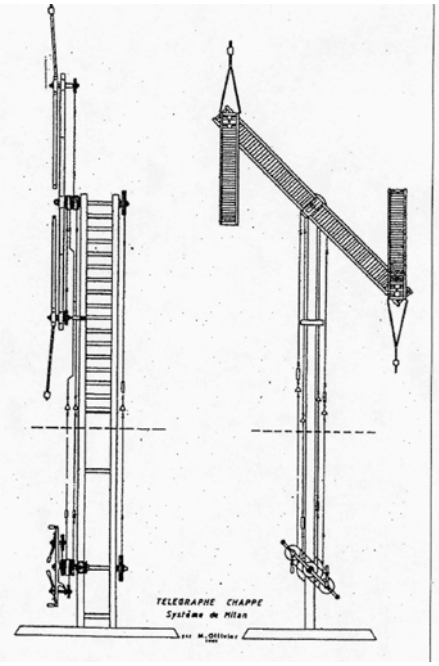
1 Introduction

Le terme « télécommunications » a été employé pour la première fois en 1904 par Edouard Estaunié et signifie « communiquer à distance ». Le but des télécommunications est donc de transmettre un signal, porteur d'une information (voix, musique, images, données…), d'un lieu à un autre lieu situé à distance.

Communication visuelle

On a vu naître divers dispositifs de communication depuis des temps très anciens. Les Romains avaient un système de signaux militaires qui permettait de faire circuler assez vite, de poste en poste, les ordres et les nouvelles d'importance.

Télégraphe optique



Il fallut attendre la fin du XVIIIe siècle pour voir apparaître le premier système permettant de communiquer à distance des messages complets construits avec des phrases. Cette réalisation des frères Chappe en 1794, le télégraphe optique de Claude Chappe, est une sorte de sémaphore constitué d'un grand bras le « régulateur », portant deux petits bras, les « indicateurs » (fig. 1-1) permettant de représenter 2x7x7 = 98 signaux différents, soit deux positions distinctes pour le régulateur et 7 pour chaque indicateur. Chaque point est émetteur et récepteur.

Les stations sont distantes de 9 à 12 km. Un signal pouvait parcourir Paris-Lille en 9 minutes mais un message de 36 signaux nécessitait 32 minutes. Ce télégraphe était développé jusqu'en 1852 sur tout le territoire français.

Figure 1-1. Station de Chappe
(http://www-phase.c-strasbourg.fr/~morel/chappe/t1.html)

Télégraphe électrique

La révolution suivante fut celle du télégraphe électrique inventé par Samuel Morse en 1832. Le morse est un code binaire (il n'utilise que 2 signes, le — et le ·). Chaque lettre et chaque chiffre est indiqué par une combinaison de traits et de points : · — · · · . La transmission est assurée par une ligne électrique (fil de cuivre) ; un opérateur s'occupe de traduire le code ; un point n'est qu'émetteur ou que récepteur. Cette invention était la première

application pratique des lois de l'électromagnétisme. C'est ce principe qui servira plus tard pour réaliser les premières liaisons radio.

Téléphone

En 1854, le français Charles Bourseul écrivait : « imaginez que l'on parle près d'une plaque mobile assez flexible pour ne perdre aucune des vibrations produites par la voix, que cette plaque établisse et interrompe successivement la communication avec une pile, vous pourrez avoir à distance une autre plaque qui exécutera en même temps exactement les mêmes vibrations. En 1876, l'américain Alexander Graham Bell inventa le téléphone : enfin, la voix humaine pouvait être transportée au-delà de l'horizon sonore.

Radio

Mais le fil de cuivre qui était à la base même de ces dispositifs de communication était très pénalisant : coûts de construction et de maintenance très importants, impossibilité de communiquer avec un bateau en mer… La découverte des ondes hertziennes allait ouvrir l'ère du « sans fil » et métamorphoser les lourds, fragiles et coûteux câbles de cuivre en liaisons invisibles que constituent les ondes électromagnétiques. Marconi Guglielmo (italo-irlandais) est reconnu comme l'inventeur de la radio sans fil. Il permit à plusieurs stations d'émettre simultanément, et sans interférence, sur des longueurs d'ondes différentes. En 1921 des émissions expérimentales sont diffusées depuis la Tour Eiffel d'où sont transmis les premiers journaux parlés et émissions musicales en direct.

Internet

L'origine de l'internet se trouve dans une initiative de la défense américaine, prise au temps de la guerre froide, visant à réaliser un réseau de transmission de données grande distance entre différents centres, capable de résister à une destruction partielle. Paul Baran est considéré comme un des acteurs principaux de la création d'internet. Il eu l'idée, en 1964, de créer un réseau sous forme de grande toile. Il avait réalisé qu'un système centralisé était vulnérable car la destruction de son noyau provoquait l'anéantissement des communications. Il mit donc au point un réseau hybride d'architectures étoilées et maillées dans lequel les données se déplaceraient de façon dynamique, en « cherchant » le chemin le moins encombré, et en « patientant » si toutes les routes étaient encombrées. Cette technologie fut appelée « packet switching ». En août 1969, indépendamment de tout objectif militaire, le réseau expérimental ARPANET fut créé par l'ARPA (Advanced Research Projects Agency dépendant du Department of Defense) afin de relier quatre instituts universitaires :

- Le Stanford Institute ;
- L'université de Californie à Los Angeles ;
- L'université de Californie à Santa Barbara ;
- L'université d'Utah.

Le réseau ARPANET est aujourd'hui considéré comme le réseau précurseur d'internet. Il comportait déjà à l'époque certaines caractéristiques fondamentales du réseau actuel : un ou plusieurs nœuds du réseau pouvait être détruits sans perturber son fonctionnement ; la com-

munication entre machines se faisait sans machine centralisée intermédiaire ; les protocoles utilisés étaient basiques. Fin 1990, Tim Berners-Lee met au point le protocole HTTP (Hyper Text Tranfer Protocol), ainsi que le langage HTML (HyperText Markup Language) permettant de naviguer à l'aide de liens hypertextes, à travers les réseaux. Le World Wide Web est né. Aujourd'hui, l'ADSL2+ est opérationnelle, c'est une technologie qui permet d'atteindre un débit de 20 mégabits/s sur des liaisons de moins de 2 km entre le répartiteur et l'abonné.

Télécommunications sur fibres optiques

En septembre 1972, des chercheurs de la firme américaine Corning annonçaient à Genève l'obtention de fibres de verre d'atténuation inférieure à 4 décibels par km. Ces fibres, de très petites dimensions (de l'ordre de 100 µm à 200 µm de diamètre), formées de deux zones concentriques de verres différents (le cœur et la gaine), peuvent être classées en deux catégories selon leurs caractéristiques géométriques : monomodes ou multimodes. Les fibres monomodes possèdent un cœur très petit (10 µm) et permettent de ne propager qu'un seul mode en liaison avec les lois générales de l'électromagnétisme. Depuis quelques années, grâce à une bande passante grande et un très haut débit des fibres, le développement des systèmes de télécommunications a rendu indispensable l'utilisation des transmissions optiques par rapport aux moyens de transmissions électriques. La croissance de l'informatique a suscité un important développement des réseaux de communications. Dans un même réseau, se partagent le transport des données informatiques et le trafic des voix par téléphone. Pour les liaisons optiques à haut débit, la technique de WDM (Wavelength Division Multiplexing) a été développée afin d'augmenter les débits. Le fait d'envoyer les signaux dans N canaux en entrée, permet de récupérer en sortie une densité d'information N fois plus grande. Le débit par canal est typiquement de 10 ou 40 Gbit/s, et les canaux sont espacés de 0,8 nm (100 GHz), 0,4 nm (50 GHz), et atteindront 0,2 nm (25 GHz) dans le futur. Une autre technique en cours de développement, est le multiplexage temporel optique OTDM (Optical Time Domain Multiplexing). Il s'agit d'entrelacer N trains d'impulsions.

Cryptographie

Parmi les différents types de données à transmettre figurent des données « sensibles » dans différents secteurs d'activité tant économiques que militaires et nécessitant la confidentialité. La cryptographie est employée pour protéger ces données. Les études concernant la cryptographie concernent un champ immense que ce soit pour les techniques de codage que pour les méthodes de transmission des données. Le codage permet à partir d'une clé, c'est-à-dire une suite de caractères, de modifier un texte afin de le rendre incompréhensible. Seule la connaissance de la clé permet de reconstituer les données initiales. Un problème majeur est donc de communiquer la clé en toute sécurité. Une réponse est apportée par la cryptographie quantique qui peut assurer la confidentialité totale.

Objectifs de cette thèse

Cette thèse porte sur les systèmes de transmission optique, notamment dans le cadre de l'application de la cryptographie quantique. Le but de la thèse est de construire un système applicable à la cryptographie quantique. L'essentiel du travail a consisté à la définition et la réalisation des divers éléments du système qui sera présenté. Pour cela, nous étudions les composants indispensables d'une ligne de transmission optique, qui sont les sources laser, la transmission des données et les détecteurs.

Le premier chapitre est donc une brève introduction aux télécommunications. Dans le deuxième chapitre, nous présentons brièvement les généralités de la cryptographie quantique qui se base sur les lois de la physique quantique. Nous décrivons les protocoles de cryptage, la sécurité souvent dite « absolue » en cryptographie quantique et puis nous résumons quelques résultats expérimentaux de différents laboratoires travaillant dans ce domaine.

Dans le troisième chapitre, nous étudions le comportement et les caractéristiques d'une source de photons. Nous mesurons la statistique poissonienne d'une source laser à l'aide de la détection homodyne équilibrée.

Dans le chapitre suivant, nous décrivons une méthode de transmission simultanée de la clé de cryptage et de l'horloge de synchronisation à travers de deux longueurs d'onde dans une seule fibre optique. Pour cela, nous utilisons un modulateur acousto-optique servant à créer deux longueurs d'onde très proche, des modulateurs électro-optiques (type Mach-Zehnder) et un filtre Fabry-Pérot de haute résolution pour les séparer au niveau de la détection.

Dans le dernier chapitre, nous présentons les détecteurs, les modes de fonctionnement des compteurs de photons et le refroidissement thermoélectrique des détecteurs. Nous avons mis en œuvre une émission et une détection de clés de cryptage.

2 Cryptographie quantique

Sommaire

Selon la théorie, les lois physiques qui régissent les échanges protégés par la cryptographie quantique permettent d'assurer une inviolabilité totale. La technologie reste des plus prometteuses et les systèmes commercialisés se multiplient. Selon la société MagiQ Technologies, fournisseur de solutions de cryptographie quantique basé à New York, le marché devrait atteindre les 200 millions de dollars d'ici quelques années. Les applications sont nombreuses, tout comme les secteurs d'activités concernés : défense, télécoms, finance, sécurité, etc.

2.1 Généralités

La cryptographie est la science du codage (ou cryptage) et décodage (ou décryptage) de messages, dans un souci de confidentialité et d'authentification. La cryptographie est seulement devenue une partie de la théorie de mathématiques et d'information ce siècle, vers la fin des années 40, principalement grâce aux travaux de Shannon [1]. Aujourd'hui, on peut brièvement définir la cryptographie comme un système mathématique de transformation d'information de sorte qu'il soit inintelligible et donc inutile à ceux qui n'ont pas droit de lui accéder. C'est la théorie quantique qui forme la base de la cryptographie quantique. A l'aide de la technologie de fibre, il sera possible d'établir un canal quantique comme un milieu où des signaux basés sur le phénomène quantique peuvent être transportés. Toute tentative d'écouter la ligne perturbera le signal de telle manière que les utilisateurs soient alertés. Cet effet augmente parce que dans la théorie quantique, certaines propriétés physiques se complètent dans le sens que la mesure d'une propriété perturbe nécessairement l'autre. Cette relation, appelée le principe d'incertitude de Heisenberg, se présente dans toutes les mesures possibles des propriétés quantiques. La plus petite unité ou le quantum, de lumière est le photon. En élaborant le photon avec un état quantique particulier, il est possible dans la théorie d'établir un canal quantique absolument sécurisé à travers d'une fibre optique en ce qui concerne l'espionnage dû aux propriétés quantiques de la lumière. L'information sera emportée par les photons uniques dont chacun représente un bit. Son état quantique décide la valeur du bit (0 ou 1).

2.1.1 Essentiel de la cryptographie quantique

La mécanique quantique décrit un phénomène très fondamental qui se relie avec l'état de polarisation d'un photon individuel. Supposons qu'un photon a quatre états de polarisation possible notamment horizontale, verticale, 45 degrés et 135 degrés. Nous ne pouvons pas distinguer ces quatre possibilités avec certitude. Ce concept donne naissance au cryptage quantique. Nous considérerons les propriétés de base de la mécanique quantique pour comprendre ce concept comme les suivantes [2-5] :

- (1) on ne peut pas prendre une mesure sans perturber le système.
- (2) il y a une loi physique dans la mécanique quantique appelée théorème de *non-clonage* qui déclare qu'un état quantique inconnu ne peut pas être copié.
- (3) donné un système quantique préparé dans l'un de deux états non-orthogonaux prescrits, toute tentative de distinguer les deux possibilités mène nécessairement à la perturbation.
- (4) on ne peut pas simultanément mesurer la polarisation d'un photon dans la base vertical-horizontale et simultanément dans la base diagonale.
- (5) une mesure sur un état quantique inconnu arbitraire est un processus irréversible qui introduit la perturbation au système.

Ces cinq propriétés réfutent la possibilité de surveillance passive des signaux quantiques. La mesure quantique est une projection : après une mesure, le système est projeté dans l'état propre correspondant au résultat de la mesure. Par conséquent, l'espionnage des canaux quantiques perturbe nécessairement le signal et ce dernier est considéré comme déjà détecté.

2.1.2 Théorème de non-clonage quantique

Ce théorème concerne la question suivante : peut-on copier ou cloner un état quantique de polarisation spécifique ? La réponse est NON. Ce théorème de non-clonage déclare qu'un état quantique inconnu ne peut pas être parfaitement copié. Il n'est pas possible d'acquérir l'information qui distingue les états quantiques non-orthogonaux sans perturber les états. La démonstration simplifiée de ce théorème est la suivante [2].

Si on a une machine à cloner alors on pourra faire :

$$|A_0\rangle|\psi\rangle \mapsto |A_\psi\rangle\,|\psi\psi\rangle \tag{2-1-1}$$

où $|A_0\rangle$ est l'état « prêt » de la machine et $|A_\psi\rangle$ est son état final. Le symbole $|\psi\psi\rangle$ représente l'état du champ de rayonnement dans lequel il y a deux photons de polarisation $|\psi\rangle$. On peut réaliser la même opération pour la polarisation $|\varphi\rangle$:

$$|A_0\rangle|\varphi\rangle \mapsto |A_\varphi\rangle\,|\varphi\varphi\rangle \tag{2-1-2}$$

On supposera que $|\psi\rangle$ représente la polarisation verticale et $|\varphi\rangle$ représente la polarisation horizontale. Pour une polarisation de type combinaison linéaire, on a une superposition de (2-1-1) et (2-1-2) :

$$|A_0\rangle\big(\alpha|\psi\rangle + \beta|\varphi\rangle\big) \mapsto \alpha|A_\psi\rangle|\psi\psi\rangle + \beta|A_\varphi\rangle|\varphi\varphi\rangle \tag{2-1-3}$$

Par exemple, pour une polarisation de 45° alors on a $\alpha = \beta = 1/\sqrt{2}$.

Si les états $|A_\psi\rangle$ et $|A_\varphi\rangle$ ne sont pas identiques alors les deux photons issus de la machine portent une polarisation mixte. Si $|A_\psi\rangle$ et $|A_\varphi\rangle$ sont identiques alors ces deux photons ont un état pur :

$$\alpha|\psi\psi\rangle + \beta|\varphi\varphi\rangle \tag{2-1-4}$$

Dans ni l'un ni l'autre de ces cas l'état final est le même que l'état avec deux photons qui ont tous les deux la polarisation $\alpha|\psi\rangle + \beta|\varphi\rangle$. Si la machine est un amplificateur parfait, cet état peut être écrit :

$$\frac{1}{\sqrt{2}}\left(\alpha a_\psi^+ + \beta a_\varphi^+\right)^2|0\rangle = \alpha^2|\psi\psi\rangle + \sqrt{2}\alpha\beta|\psi\varphi\rangle + \beta^2|\varphi\varphi\rangle \tag{2-1-5}$$

qui est un état pur différent de celui acquis au dessus par superposition (éq. 2-1-4). Il n'existe donc pas une telle machine qui puisse amplifier une polarisation arbitraire.

2.2 Protocoles de cryptage

2.2.1 Théorème de Shannon

a) Introduction

Nous commençons par quelques notions fondamentales de probabilité, de théorie de l'information et de cryptage en mathématique. Dans la pratique, nous disons qu'un système est informatiquement sécurisé si le meilleur algorithme connu pour le casser exige un temps de calcul déraisonnablement grand.

Soient X et Y les variables aléatoires, alors

- $p(X = x)$ est la probabilité que X prend la valeur de x ;
- $p(Y = y)$ est la probabilité que Y prend la valeur de y.

La probabilité conditionnelle est définie par :

- $\mathrm{p}(\mathrm{X} = x \mid \mathrm{Y} = y)$ est la probabilité que X prend la valeur de x étant donné que Y prend la valeur de y. Alors,

$$\mathrm{p}(\mathrm{X} = x, \mathrm{Y} = y) = \mathrm{p}(\mathrm{X} = x \mid \mathrm{Y} = y).\mathrm{p}(\mathrm{Y} = y) \quad (2\text{-}1\text{-}6)$$

$$\mathrm{p}(\mathrm{X} = x, \mathrm{Y} = y) = \mathrm{p}(\mathrm{Y} = y \mid \mathrm{X} = x).\mathrm{p}(\mathrm{X} = x) \quad (2\text{-}1\text{-}7)$$

On dénote : P = l'ensemble de textes en clair possible.
K = l'ensemble de clés possible.
C = l'ensemble de textes cryptés possible.

Considérons que P, K, C sont associés aux variables aléatoires avec les probabilités :

$$p(P = m),\ p(K = k),\ p(C = c)$$

et une hypothèse raisonnable est que P et K sont indépendants. Alors, l'ensemble de textes cryptés sous la clé k est défini par :

$$C(k) = \{e_k(m) : m \in P\} \quad (2\text{-}1\text{-}8)$$

On a une relation :

$$p(C = c) = \sum_{\{k:c \in C(k)\}} p(K = k).p(P = d_k(c)) \quad (2\text{-}1\text{-}9)$$

Pour $c \in C$ et $m \in P$, on peut calculer la probabilité que c est le texte crypté étant donné que m est le texte en clair :

$$\mathrm{p}(\mathrm{C} = c \mid \mathrm{P} = m) = \sum_{\{k:m \in d_k(c)\}} p(K = k) \quad (2\text{-}1\text{-}10)$$

Pour casser ce chiffre, il faut connaître les probabilités du texte en clair étant donné un certain texte crypté. Nous calculons donc la probabilité que m est le texte en clair étant donné que c est le texte crypté :

$$\mathrm{p}(\mathrm{P}=m \mid \mathrm{C}=c)=\frac{\mathrm{p}(\mathrm{C}=c \mid \mathrm{P}=m).\mathrm{p}(\mathrm{P}=m)}{\mathrm{p}(\mathrm{C}=c)}=\frac{p(P=m).\sum_{k:m\in d_k(c)} p(K=k)}{\sum_{k:c\in C(k)} p(K=k).p(P=d_k(c))} \qquad (2\text{-}1\text{-}11)$$

Elle est peut être calculée par tous les gens qui connaissent les distributions de probabilité de P, K et la fonction de cryptage.

Un exemple :

- Supposons que nous avons deux messages *aa* et *bb*. Nous écrivons P = {*aa*,*bb*}. La distribution de probabilité de P est : *p(P=aa)* = 1/4 ; *p(P=aa)* = 3/4.
- Supposons que nous avons trois clés *k1*, *k2* et *k3*. Nous écrivons K = {*k1*,*k2*,*k3*}. La distribution de probabilité de K est : *p(K=k1)* = 1/2 ; *p(K=k2)* = *p(K=k3)* = 1/4.
- Supposons que nous avons C = {*1*,*2*,*3*,*4*} avec le cryptage donné par :

$e_k(m)$	aa	bb
k1	1	2
k2	2	3
k3	3	4

Nous pouvons calculer les probabilités (d'après l'éq. 2-1-9) :

$$\mathrm{p}(\mathrm{C}=1)=\frac{1}{2}\times\frac{1}{4}=\frac{1}{8}$$
$$\mathrm{p}(\mathrm{C}=2)=\frac{1}{2}\times\frac{3}{4}+\frac{1}{4}\times\frac{1}{4}=\frac{7}{16}$$
$$\mathrm{p}(\mathrm{C}=3)=\frac{1}{4}\times\frac{3}{4}+\frac{1}{4}\times\frac{1}{4}=\frac{1}{4}$$
$$\mathrm{p}(\mathrm{C}=4)=\frac{1}{4}\times\frac{3}{4}=\frac{3}{16}$$

et probabilités conditionnelles (éq. 2-1-11) :

$$\mathrm{p}(\mathrm{P}=aa \mid \mathrm{C}=1)=\frac{1/2\times1/4}{1/8}=1 \;;\; \mathrm{p}(\mathrm{P}=bb \mid \mathrm{C}=1)=\frac{0\times3/4}{1/8}=0$$
$$\mathrm{p}(\mathrm{P}=aa \mid \mathrm{C}=2)=\frac{1/4\times1/4}{7/16}=\frac{1}{7} \;;\; \mathrm{p}(\mathrm{P}=bb \mid \mathrm{C}=2)=\frac{1/2\times3/4}{7/16}=\frac{6}{7}$$
$$\mathrm{p}(\mathrm{P}=aa \mid \mathrm{C}=3)=\frac{1/4\times1/4}{1/4}=\frac{1}{4} \;;\; \mathrm{p}(\mathrm{P}=bb \mid \mathrm{C}=3)=\frac{1/4\times3/4}{1/4}=\frac{3}{4}$$
$$\mathrm{p}(\mathrm{P}=aa \mid \mathrm{C}=4)=\frac{0\times1/4}{3/16}=0 \;;\; \mathrm{p}(\mathrm{P}=bb \mid \mathrm{C}=4)=\frac{1/4\times3/4}{3/16}=1$$

Donc,

- Si nous voyons le texte crypté 1 alors nous **savons** que le message est *aa*
- Si nous voyons le texte crypté 4 alors nous **savons** que le message est *bb*
- Si nous voyons le texte crypté 3 alors nous **devinons** que le message est *bb*
- Si nous voyons le texte crypté 2 alors nous **devinons** que le message est *bb*

Par conséquent, dans l'exemple ci-dessus, le texte crypté indique des informations sur texte en clair. C'est ce que nous souhaitons éviter à l'aide d'un système de cryptage qui ne fournit aucune information sur le texte en clair. Ce système est dit de secret parfait ou sans conditions, il vérifie :

$$\mathrm{p}(\mathrm{P} = m \mid \mathrm{C} = c) = \mathrm{p}(\mathrm{P} = m) \text{ pour tous } m \in P \text{ et } c \in C \qquad (2\text{-}1\text{-}12)$$

C'est-à-dire, la probabilité que le texte en clair est *m* étant donné que le texte crypté *c* est observé, est identique que la probabilité qu'il est *m* sans voir *c*. En d'autres termes, savoir *c* n'indique aucune information sur *m*.

b) Théorème de Shannon

Supposons que (P, C, K, $e_k(.)$,$e_k(.)$) est le système de cryptage avec #P = #C = #K. Le système de cryptage offre un secret parfait si et seulement si toutes les clés sont utilisées avec la même probabilité 1/#K, et pour chaque $c \in C$ et $m \in P$, il y a une clé unique *k* telle que $e_k(m) = c$.

La démonstration du théorème de Shannon se trouve dans l'annexe B.

2.2.2 Cryptage de Caesar (shift cipher)

Le cryptage de Caesar, dit également cryptage à décalage, est un exemple direct du théorème de Shannon. Nous avons

- $\mathrm{P} = \mathrm{K} = \mathrm{C} = Z_{26}$
- $m, c, k \in Z_{26}$
- $e_k(m) = m + k \mod 26$ (cryptage)
- $d_k(c) = c - k \mod 26$ (décryptage)

Ici, Z_{26} représentent l'ensemble {0,1,…,25} avec dont l'addition et la multiplication sont modulo de 26. Les lettres alphabétiques sont identifiées par les nombres :

$$\mathrm{A} = 0, \mathrm{B} = 1, \ldots, \mathrm{Z} = 25$$

Le théorème de Shannon implique un secret parfait si nous cryptons une lettre. Pour un texte en clair de longueur *n,* on a (une nouvelle clé pour chaque lettre) :

$$\mathrm{P} = \mathrm{K} = \mathrm{C} = (Z_{26})^n \text{ et } p(K = k) = \frac{1}{26^n}$$

Par exemple, supposons que $k = 9$ et une seule clé pour toutes les lettres ; on change chaque lettre en la déplaçant 9 positions vers la droite. Le texte en clair « rendezvous » devient ANWMNIEXDB comme la démonstration dans la figure (2-1).

Texte en clair	r	e	n	d	e	z	v	o	u	s
	17	4	13	3	4	25	21	14	20	18
$+k$	0	13	22	12	13	8	4	23	3	1
Texte crypté	A	N	W	M	N	I	E	X	D	B

Figure 2-1. Exemple d'application du cryptage à décalage (de Caesar) avec la clé $k = 9$.

Il y aura une question : le cryptage de Caesar est-il sûr ? Naturellement NON, puisqu'il y a seulement 26 clés possibles, il est facile d'être cassé par recherche de clé approfondie. En fait, si on décale chaque lettre du mot ANWMNIEXDB vers la gauche, on trouve le texte original : rendezvous (k = 9). En moyenne, un texte en clair sera calculé après 26/2 = 13 essais.

2.2.3 Cryptage de Vernam

Le cryptage de Vernam, dit aussi Vernam one-time-pad ou cryptage de masque jetable, utilise le cryptage à décalage mais avec modulo 2 à la place de modulo 26. L'arithmétique binaire ou le OU exclusif (XOR) est définie comme :

$\oplus$	0	1
0	0	1
1	1	0

Gilbert Vernam a inventé ce cryptage en 1926 pour le chiffrage et déchiffrage des messages de télégraphe [6]. Pour que ce système soit sécurisé sans conditions, trois exigences sont imposées à la clé :

- La clé doit être aussi longue que le message. Un bit secret est donc nécessaire pour crypter chaque bit du message.
- Elle doit être purement aléatoire.
- Chaque clé peut être utilisable une fois et seulement une fois, d'où le nom *Vernam one-time-pad*.

Voici le détail de la méthode de Vernam :

Alice veut communiquer à Bob le message m. Elle possède une clé k, de même longueur que m, qui est secrète et partagée avec Bob. Alice obtient le cryptogramme $e_k(m) = c$ en additionnant bit à bit modulo 2 le message et la clé, à savoir $c = m \oplus k$. Au côté de Bob, après la réception du cryptogramme, il obtient le message en faisant la même opération, soit $c \oplus k = m \oplus k \oplus k = m$. Comme la clé est complètement aléatoire, chaque bit du cryptogramme l'est aussi. Ce système vérifie le théorème de Shannon (cf. 2.2.1), ce qui implique que la connaissance du cryptogramme ne fournit aucune information sur le message. Bien entendu, nous ne pouvons pas employer la même clé deux fois à cause de l'attaque suivante :

- Eve (espion) génère un message m et demande à Alice (expéditeur) de le crypter.
- Eve reçoit $c = m \oplus k$ de Alice.
- Eve peut maintenant calculer la clé $k = c \oplus m$.
- Alors Eve peut décrypter tous les messages cryptés avec la clé k.

L'inconvénient principal et la difficulté essentielle à résoudre, pour utiliser concrètement ce moyen de cryptage, consistent au fait que la clé ne peut être réutilisée et la génération de la clé secrète n'est sécurisée autrement que par des moyens conventionnels comme une rencontre préalable entre Alice et Bob, ou encore, par l'utilisation d'un messager honnête. Par conséquent, l'implantation sur grande distance et pour un grand nombre de participants demande trop de ressources et la sécurité serait difficile à garantir. Jusqu'à présent, les Etats les transportaient par le biais de la valise diplomatique, même si ce canal n'est pas totalement inviolable. Ce cryptage a jusqu'à présent trouvé des applications principalement dans les services militaires et diplomatiques. Comme on le verra dans la prochaine partie, la difficulté de la distribution de clés secrètes peut être enlevée en vertu de la distribution de clé quantique.

Un exemple de transmission d'un message crypté par le cryptage de Vernam est montré ci-dessous. La clé est absolument aléatoire et identique pour le cryptage et le décryptage (fig. 2-2).

Transmission de clé de cryptage : Canal privé

Alice (émetteur)	
Message en clair :	0101010101
Clé de cryptage :	⊕ 1101101100
Message crypté :	*1000111001*
Bob (récepteur)	
Message crypté :	*1000111001*
Clé de cryptage :	⊕ 1101101100
Message en clair :	0101010101

Transmission du message crypté : Canal public

Figure 2-2. Exemple d'application du cryptage de Vernam one-time-pad. La clé est absolument aléatoire et identique pour le cryptage et le décryptage. Le ⊕ représente la fonction logique XOR (OU exclusif).

2.2.4 Protocole de Bennett et Brassard BB84

Notion de qubit

On parle tout d'abord des bits quantiques ou qubits. Un qubit est une description générique d'un système quantique dont une observable (au sens donnée par la mécanique quantique [3]) possède deux niveaux accessibles (et nécessairement orthogonaux) que nous désignons par $|0\rangle$ et $|1\rangle$. Ces deux niveaux font partie d'une base orthonormée. En général, la dimension de cette base peut être supérieure à deux. Cependant, les conditions expérimentales sont telles que seuls ces deux états sont accessibles. Par exemple, l'état du spin de l'électron

dans un champ magnétique aligné selon z pourrait constituer un qubit avec les états de base $\left|\uparrow\right\rangle_z \equiv \left|0\right\rangle$ et $\left|\downarrow\right\rangle_z \equiv \left|1\right\rangle$. Parfois, il faut ignorer certains degrés de liberté. C'est le cas du photon, où l'on peut crypter un qubit dans sa polarisation en ignorant le nombre d'onde.

L'utilisation de la mécanique quantique va permettre de résoudre la difficulté essentielle du code de Vernam ci-dessus (difficulté dans l'échange des clés, cf. 2.2.3). Cette fois, la sécurité est garantie non par des théorèmes mathématiques, mais par les lois fondamentales de la physique comme le principe d'incertitude d'Heisenberg qui affirme que certaines quantités ne peuvent pas être mesurées simultanément. Dans le transport de clé « quantique », l'information est transportée par les photons, ces composants élémentaires de la lumière. Chaque photon peut être polarisé, c'est-à-dire que l'on impose une direction à son champ électrique. La polarisation est mesurée par un angle qui varie de 0° à 180°. Nous parlons ici du premier protocole bien connu de la cryptographie quantique : protocole BB84 qui était inventé en 1984 par Charles Bennett du groupe de recherche d'IBM et Gilles Brassard de l'université de Montréal. Ce protocole a été expérimentalement démontré pour une transmission plus de 30 km et 50 km par fibre optique [7-9] et également dans l'espace libre sur plus de cent mètres [10-11]. Les expériences pour la communication de la terre vers le satellite sont aussi en cours. Nous décrivons maintenant le protocole BB84 en termes d'états de polarisation d'un photon individuel. Une description détaillée de ce protocole est donnée par [12]. La polarisation peut prendre 4 valeurs : 0°, 45°, 90°, 135°. Pour les photons polarisés de 0° à 90°, on parle de polarisation rectiligne ; pour ceux polarisés de 45° à 135°, de polarisation diagonale :

Figure 2-3. Représentation de la polarisation des photons.

Nous avons donc un émetteur et un récepteur. L'émetteur (appelé par convention, Alice) va émettre les photons avec un des quatre angles de polarisation 0, 45, 90 ou 135 degrés. Le destinataire (Bob) pourra, à l'aide de son récepteur, mesurer l'angle de polarisation. La transmission est assurée par une fibre optique et l'équipement de trans-mission, appelé canal quantique.

Pour détecter la polarisation des photons, Bob utilisera un filtre polarisant suivi d'un photodétecteur. Si un photon polarisé à 0° rencontre un filtre polarisant orienté à 0°, il traverse ce filtre polarisant et est enregistré par le détecteur placé juste après. Si un photon polarisé à 90° rencontre le même filtre, il est immédiatement arrêté, et le détecteur n'enregistre rien. Maintenant, si le photon est polarisé diagonalement (45° ou 135°), une fois sur deux, il traverse le filtre, et une fois sur deux, il est arrêté. Si on peut distinguer entre une polarisation à 0° et à 90°, il est impossible de distinguer en même temps entre une polarisation à 45° et à 135° ! De la même façon, on peut utiliser un filtre polarisant orienté à 45° : il laisse passer les photons polarisés à 45°, arrête ceux polarisés à 135°, et se comporte aléatoirement avec ceux à 0° et 90° ! (fig. 2-4)

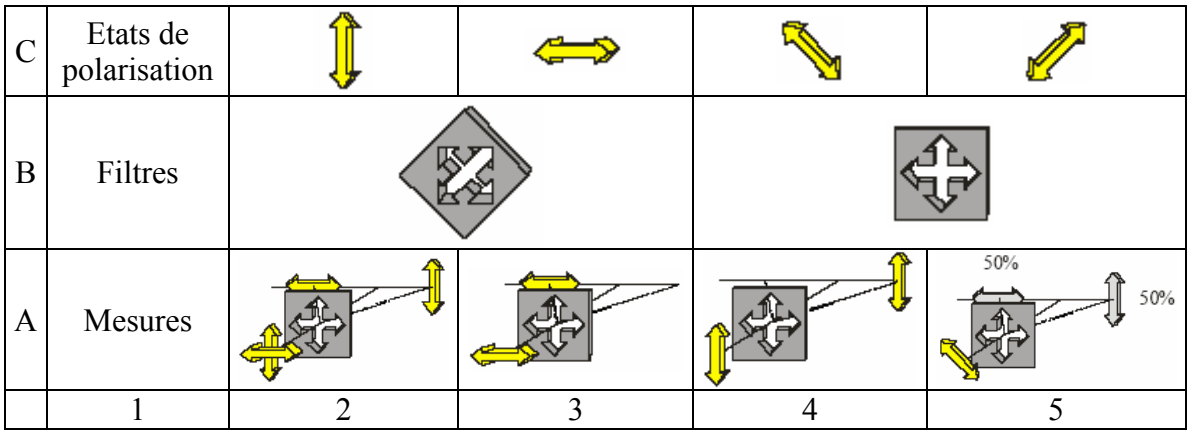


Figure 2-4. La figure représente la convention décidée par Alice et Bob. Un filtre permet de distinguer entre des photons polarisés verticalement et horizontalement ; un autre entre des photons polarisés en diagonale. Quand un photon traverse le filtre correct, sa polarisation n'est pas affectée (images 2A, 3A, 4A). En revanche, quand un photon traverse le faux filtre sa polarisation se transforme de façon aléatoire (image 5A).

Décrivons alors le protocole qu'Alice et Bob doivent respecter pour qu'Alice envoie à Bob une clé secrète constituée de 0 et de 1 ; ils disposent de 2 canaux d'échange : un canal quantique, où ils peuvent s'échanger des photons polarisés, et un canal radio ; non protégé, où ils peuvent discuter. Ils conviennent que les photons polarisés à 0° ou 45° représentent 0, et ceux polarisés à 90° ou 135° représentent 1. Alice émet, sur le canal quantique, une suite de photons polarisés au hasard parmi 0°, 45°, 90° et 135°. A l'autre bout, Bob reçoit les photons et mesure aléatoirement ou leur polarisation rectiligne (filtre placé à 0°), ou leur polarisation diagonale (filtre placé à 45°). Si le photon traverse le filtre, Bob note 0, sinon il note 1.

Voici le détail du processus :

---------- sur un canal quantique :

1) Pour une série de nombres binaires (exemple : 01101001), Alice envoie à l'aide de photons dont la polarisation est choisie par hasard entre les quatre états : angles de polarisation 0, 90, 45 ou 135. Il enregistre l'orientation dans une liste.

2) Les photons sont envoyés le long du canal quantique.

3) Bob décide au hasard avec quelle polarisation il lit les photons. Bien sûr, certaines mesures de Bob (en moyenne, une sur deux) n'ont pas d'intérêt : il a pu essayer de mesurer la polarisation rectiligne d'un photon polarisé à 45°, ce qui n'a pas de sens et donne un résultat aléatoire (par exemple, le photon a été bloqué par le filtre, Bob note donc 1 alors qu'Alice avait envoyé 0).

---------- sur un canal public (Internet, téléphone, radio, etc.) :

4) Pour éliminer ces bits sans sens, Bob indique à Alice, par le canal public, quel type de mesure (rectiligne ou diagonale) il a faite pour chaque photon.

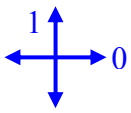
5) Alice répond à Bob, par oui ou non, si les modes étaient corrects. Si c'est le cas, alors Bob saura qu'il pourra correctement interpréter les résultats reçus. Par exemple, si le mode est rectiligne, Bob pourra savoir si c'est 0 ou 90 degrés. Dans aucun cas Alice et Bob discutent sur le canal public des données transmises, seulement des modes. Les données ainsi obtenues (i.e. le résultat des qubits interprétables) formeront la clé de cryptage.

6) Alice et Bob échangent ensuite une petite partie de la clé pour s'assurer qu'elle est identique. La moindre erreur voudra dire que le message a été enregistré ou intercepté par une troisième personne.

Il faut encore vérifier que ce protocole est sûr. Si Eve écoute le canal quantique, elle peut faire la même chose que Bob, c'est-à-dire intercepter les photons en plaçant un filtre polarisant tantôt rectiligne, tantôt diagonal. Pour que Bob ne se doute de rien, Eve doit réémettre un photon polarisé. Elle va essayer d'envoyer le même photon qu'Alice, mais comme elle a une chance sur deux d'avoir choisi le mauvais filtre, elle a une chance sur deux de se tromper. Quand Bob reçoit le photon, s'il est mal polarisé par Eve, il a une chance sur deux d'avoir un résultat différent qu'avec le photon original, et finalement, pour chaque photon intercepté par Eve, il y a une chance sur 4 que Bob reçoive une information erronée. On peut aussi penser au cas où Eve copie parfaitement les états de polarisation. Cependant, le théorème de non-clonage (cf. partie 2-1-2) l'interdit de le faire.

Alice et Bob décident alors de « sacrifier » une partie de leur clé commune. Parmi tous les bits qu'ils ont en commun, ils en choisissent quelques-uns au hasard, et les compare publiquement par le canal radio : s'ils sont différents, ils ont une preuve qu'ils ont été écoutés, et ils oublient vite cette clé. En comparant suffisamment de bits, ils ont une garantie presque absolue de ne pas avoir écouté. Bien sûr, il reste des problèmes pratiques à résoudre : émettre des photons un par un, conserver la polarisation sur de grandes distances...

Exemples du protocole BB84 (fig. 2-5 et 2-6). Utilisation de deux bases de codage :

En polarisation		
	Base à 0° - rectiligne	Base à 45° - diagonale

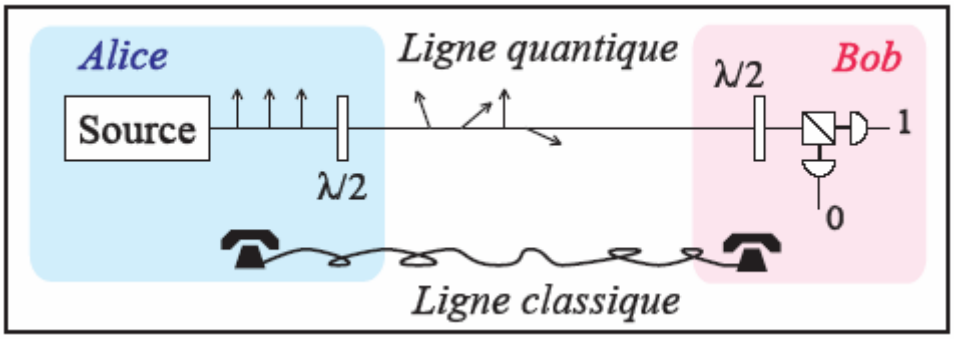


Figure 2-5. Illustration du principe du protocole de BB84 [12].

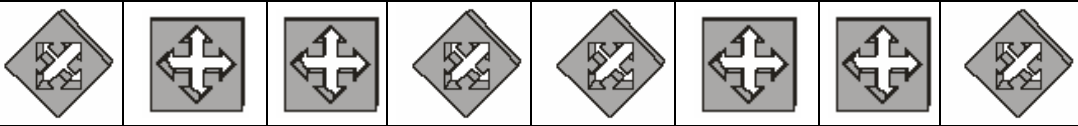
1. Emission bit	0	1	1	0	1	0	0	1
2. Photon code								
3. Réception-filtre								
4. Photon détection								
5. Détection bit	1	1	0	0	1	1	0	0
6. Vérification		√		√	√		√	
7. Clé		**1**		**0**	**1**		**0**	

Figure 2-6. Protocole fondamental de la distribution de clés quantiques [12].

1. La séquence de bits envoyée par Alice.
2. Alice envoie une séquence aléatoire de photons polarisés horizontalement, verticalement et diagonalement.
3. Bob mesure la polarisation des photons avec deux bases aléatoires (rectiligne et diagonale).
4. Résultats de la mesure de Bob (on suppose que tous les photons sont détectés).
5. La séquence de bits correspondante à la détection.
6. Bob annonce à Alice quelle base il a utilisé pour chaque photon reçu. Alice lui dit les bases correctes.
7. Alice et Bob ne gardent que la séquence binaire correctement mesurée.

2.2.5 Protocole de Bennett B92

Bennett a proposé en 1992 le protocole B92 [13]. Le protocole B92 est aussi appelé protocole à deux états de phase (phase-based protocol) car il prononce que tout état quantique peut être représenté par deux vecteurs dans l'espace de Hilbert. Comme décrit dans [12], ce protocole sera décrit en termes de préparations et mesures dans un espace de Hilbert bidimensionnel tel que celui d'une particule de spin-1/2.

Alice prépare deux états non-orthogonaux : $|\uparrow\rangle$ ('0') ou $|\rightarrow\rangle$ ('1'). On peut penser aux états en tant qu'un spin-haut de l'axe *z* et un spin-haut de l'axe *x*. Les états le long des axes *x* sont reliés aux états des axes *z* par :

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle + |\downarrow\rangle\right) \text{ et } |\leftarrow\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\rangle - |\downarrow\rangle\right).$$

Il est important que les opérateurs de projection correspondant aux deux états qu'Alice envoie ne permutent pas. Ceci peut s'écrire $\left[P_{|\rightarrow\rangle\langle\rightarrow|}, P_{|\uparrow\rangle\langle\uparrow|}\right] \neq 0$. Les états sont non-orthogonaux et ne peuvent pas être des états propres de deux opérateurs. Un espion

s'effondrera la fonction d'onde sur un des états propres de l'opérateur de projection par la mesure. Si l'état transmis n'est pas un état propre de l'opérateur de projection, l'espion ne sait pas quelle fonction d'onde à transmettre, et par conséquent, il reproduira l'état original dans seulement 50% des intervalles. Bob fait deux mesures non-orthogonales : $P_{|\rightarrow\rangle\langle\rightarrow|}$ ou $P_{|\uparrow\rangle\langle\uparrow|}$.

La raison de choisir ces états particuliers est qu'un photon sera produit quand les données de Bob et d'Alice se coïncident. Les opérateurs alternatifs de projection auraient donné zéro quand les données d'Alice et de Bob étaient égales, mais puisque la probabilité pour avoir un photon dans l'intervalle est petite (~ 0,05) il n'est pas possible de différencier entre les données correctes et photon de fuite. Noter que quand Alice et Bob ont le même bit, la probabilité que Bob détecte un photon est de 0,5. Ceci signifie que seulement 25% des intervalles de bit sont employés dans une transmission idéale d'un photon unique dans chaque intervalle. Même une autre diminution se produise car le fait est que la probabilité d'avoir des photons dans chaque impulsion lumineuse est plus petite que 1.

Exemple :

1. Séquence Alice	1	0	1	0	1	1	0	1	0
2. Photon code	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\uparrow\rangle$
3. Séquence Bob	0	0	1	1	0	0	1	1	0
4. Opérateur	$\|\leftarrow\rangle\langle\leftarrow\|$	$\|\leftarrow\rangle\langle\leftarrow\|$	$\|\downarrow\rangle\langle\downarrow\|$	$\|\downarrow\rangle\langle\downarrow\|$	$\|\leftarrow\rangle\langle\leftarrow\|$	$\|\leftarrow\rangle\langle\leftarrow\|$	$\|\downarrow\rangle\langle\downarrow\|$	$\|\downarrow\rangle\langle\downarrow\|$	$\|\leftarrow\rangle\langle\leftarrow\|$
5. Résultat	0	$\frac{1}{\sqrt{2}}\|\leftarrow\rangle$	$\frac{1}{\sqrt{2}}\|\downarrow\rangle$	0	0	0	0	$\frac{1}{\sqrt{2}}\|\downarrow\rangle$	$\frac{1}{\sqrt{2}}\|\leftarrow\rangle$
6. Vérification	0	0	1	0	0	0	0	1	1
7. Clé	**-**	**-**	**1**	**0**	**-**	**-**	**0**	**1**	**-**

Figure 2-7. Protocole fondamental de la distribution de clés quantiques [12].

2.2.6 Distribution de clé cryptographique basée sur l'intrication

L'intrication peut servir à la transmission d'information si on la combine avec une ligne de communication classique. La cryptographie quantique en fournit un premier exemple. Alice et Bob partagent un ensemble de paires de qubits dans un état de Bell. Ils effectuent sur ces qubits des mesures locales d'observables qui ne commutent pas, choisies aléatoirement et indépendamment l'une de l'autre (par exemple σz et σx). Ils comparent ensuite (ligne publique) leur choix de base et ne gardent que les résultats pour lesquels leurs choix coïncident.

Ils disposent alors d'une clé secrète identique pour coder (Alice) et décoder (Bob) des messages transmis publiquement. Si Eve intercepte les qubits et les mesure avant de les renvoyer à Bob, elle perturbe nécessairement leurs corrélations, ce dont Bob et Alice peuvent se rendre compte par des tests sur des échantillons de leurs clés qu'ils comparent publiquement avant de les jeter.

2.3 Sécurité en cryptographique quantique

2.3.1 Généralités

Depuis sa découverte, la cryptographie quantique a été démontrée par un certain nombre de groupes en utilisant les états cohérents faibles, dans les systèmes à fibres [14] et dans l'espace libre [10, 15-16]. Ces expériences sont vraisemblablement bloquées contre toutes les attaques d'espionnage basées sur la technologie actuellement disponible ; cependant, il y a certaines attaques imaginables auxquelles elles pourraient être vulnérables par exemple, les impulsions utilisées contiennent nécessairement plus d'un photon : un espion pourrait en principe utiliser ces événements pour écouter la ligne (la clé) sans n'introduire aucune erreur supplémentaire [17-18]. L'utilisation de véritables sources de photons uniques peut fermer cette lacune potentielle de sécurité ; cependant, bien que la lacune existe toujours en utilisant des paires de photons par ex. de la fluorescence paramétrique (parametric down-conversion : parce que de temps en temps il y aura de paires doubles), on a montré que des montages peuvent permettre des transmissions sécurisées sur de longues distances [19-22].

Ekert [23] a prouvé qu'on peut employer les corrélations pour élaborer une clé aléatoire secrète entre deux parties, en tant qu'un élément d'un protocole de cryptographie complètement sécurisé [24]

Comme expliqué plus haut, l'utilisation des clés (publiques ou secrète) dans la cryptographie moderne est incontournable. Nous avons aussi mentionné que cette cryptographie est basée sur des mathématiques non vérifiées et n'importe qui peut avoir accès au texte crypté. Avec le cryptage quantique, les choses fonctionnent un peu différemment.

On pourra utiliser une phrase tout à fait appropriée pour exprimer cette notion : « Les donnés quantiques ne peuvent pas être lues à moins que des informations sur l'état avec lesquelles ils ont été préparés soit connu. Toute tentative de lecture ou de copie des donnés sans l'information requise, modifiera les donnés de façon significative ». Ce qui veut dire en clair que le texte crypté ainsi que la clé ne peuvent pas être lus ou interceptés. Comme on le savait, il s'agit d'une application directe de la physique quantique expliqué plus haut.

Il y a trois principaux crypto-systèmes quantiques pour la distribution des clés :

- Un crypto-système qui encode pour deux observateurs qui ne se connaissent pas : le protocole de Bennett et Brassard en 1984 [25].
- Un crypto-système qui encode selon les propriétés de l'intrication quantique et du théorème de Bell : proposé par Ekert en 1991 [24].
- Un crypto-système qui encode à partir des deux vecteurs d'états non orthogonaux : proposé par Bennett en 1992 [13].

2.3.2 Communications sécuritaires fiables

Lorsqu'ils se retrouvent en petits nombres, les photons se comportent d'une façon bien différente. Les progrès technologiques nous permettent maintenant de manipuler individuellement les photons [26], ce qui ouvre la voie à de nouvelles découvertes scientifiques basées sur les phénomènes de mécanique quantique.

À l'heure actuelle, la sécurité quantique ne peut être assurée qu'entre les deux extrémités d'une même fibre optique. Cependant, il pourrait être souhaitable que plusieurs abonnés puissent communiquer entre eux. À cette fin, une équipe de chercheurs à Toronto, Waterloo, Hamilton, Ottawa et Montréal est à mettre au point de nouveaux concepts. L'article 'Towards an implementation of quantum key distribution in optical fibre telecommunication networks' présente la recherche en cours à Montréal où les chercheurs transmettent plusieurs signaux sur la même fibre à différentes longueurs d'onde (multiplexage en longueur d'onde). Il s'agit d'une méthode dont l'utilisation est répandue en télécommunications et qui fait appel à des composants de très haut raffinement qui existent déjà. Le Canada a d'ailleurs été une des principales sources de ces composants au moment de l'essor des communications optiques au début du siècle. Employé dans les systèmes de cryptage quantique, le multiplexage en longueurs d'onde permet à deux utilisateurs de générer une clé secrète qui est inconnue même du serveur qui distribue les photons. Selon les chercheurs, quand deux utilisateurs communiquent dans un réseau qui comporte plusieurs serveurs, la moitié seulement des serveurs doit être sécurisée, ce qui impose moins de contraintes sur la conception du réseau.

Afin de réaliser un tel système, on doit produire, à la longueur d'onde désirée, des photons en paire dans un état que l'on dit « intriqué ». Ces photons demeurent liés l'un à l'autre peu importe la distance qui les sépare. La connaissance de l'un informe au sujet de l'existence de l'autre. Le groupe développe présentement une source pour produire ces paires de photons en se basant sur une approche optique non linéaire révolutionnaire. Il met aussi au point des systèmes de codage/décodage présentant la stabilité nécessaire pour détecter l'état quantique des photons.

La sécurité quantique résulte de l'impossibilité pour Eve de dupliquer les signaux reçus ou d'en distraire une partie significative sans signer son intervention par une modification importante du taux d'erreur des signaux reçus par Bob. La sécurité repose sur les erreurs résultant d'observations incompatibles d'un même objet quantique, comme la mesure de la polarisation (ou la phase) d'un photon unique sur deux bases différentes, ou comme la mesure simultanée des deux quadratures d'un même état cohérent. Un faible taux d'erreur garantit alors, de manière rétrospective, la confidentialité de la liaison.

2.4 Cryptographie quantique expérimentale

2.4.1 Principe

La cryptographie quantique résout le problème principal de distribution en permettant l'échange d'une clé cryptographique entre deux parties à distance avec la sécurité absolue, garanti par les lois de la physique. Contraire à ce qu'on pourrait penser, le principe est relativement simple. Il exploite le fait que selon la physique quantique, l'observation (la mesure) d'un objet quantique le perturbe d'une manière irréparable de façon irrémédiable. Cette interaction entre l'observateur et l'objet observé est fondamentale en physique quantique. Cette perturbation cause des erreurs dans la séquence de bits échangée par l'expéditeur et le destinataire. Par la vérification de la présence de telles erreurs, les deux parties peuvent vérifier si leur clé a été arrêtée ou pas.

De nos jours, les systèmes modernes de communication échangent les informations au moyen d'impulsions lumineuses voyageant sur des réseaux de fibres optiques. Pour chaque bit, une impulsion est émise et transmise, au travers d'une fibre optique, au récepteur qui la détecte et la transforme en signal électronique. Ces impulsions sont typiquement constituées de millions de particules de lumière ou photons. En cryptographie quantique, on suit le même principe mais avec des impulsions constituées d'un unique photon. Un photon représente une quantité d'énergie minuscule – en lisant cette page, vos yeux en détectent des milliards à chaque seconde – qui constitue un système quantique élémentaire. En particulier, il n'est pas possible de le casser en deux. Ainsi, un espion ne peut pas prendre un demi-photon, tout en laissant l'autre moitié poursuivre sa route. S'il veut intercepter le bit échangé, il lui faut détecter le photon et donc interrompre la communication. Il est clair que dans ce cas, rien ne l'empêche de préparer un nouveau photon selon le résultat qu'il a obtenu pour l'envoyer au destinataire.

Toutefois en cryptographie quantique, Alice et Bob coopèrent pour empêcher Eve de suivre cette stratégie, en s'assurant qu'elle ne pourra le faire sans introduire des erreurs. Il est important de noter que cette vérification a lieu après l'échange d'information et que la présence de l'espion peut être décelée seulement a posteriori. C'est pourquoi cette technologie doit être employée pour échanger une clé et non un message valable. Une fois que la clé est validée, elle peut être employée pour crypter des données. La physique quantique montre que l'interception de la clé sans perturbation est impossible.

2.4.2 Caractéristiques importantes du système QKD

La première caractéristique importante d'un système de cryptographie quantique est le débit de clé. Il est typiquement de quelques centaines à quelques milliers de bits par seconde, suivant la distance. Cette valeur est basse par rapport au débit des systèmes de télécommunication actuels. Il s'agit toutefois du prix à payer en échange d'une sécurité absolue garantie par les lois de la physique quantique. Il faut se rappeler que le système n'est utilisé que pour échanger une clé. Les données cryptées peuvent ensuite transiter par un canal à haut débit.

La seconde caractéristique importante d'un système de cryptographie quantique est la distance de transmission. Les fibres optiques sont constituées de verre de très haute qualité. Elles ne sont toutefois pas parfaitement transparentes. Il arrive ainsi qu'un photon soit absorbé lors de sa propagation et n'atteigne pas l'extrémité de la fibre optique. Dans les systèmes de télécommunication conventionnels, des répéteurs sont utilisés pour régénérer le signal. Ils sont espacés environ de 80 km et amplifient le signal optique. En cryptographie quantique, il n'est pas possible d'utiliser de tels répéteurs. Tout comme un espion, ils corrompent la transmission et introduisent des erreurs. Ainsi, le débit décroît avec la distance, puisque de moins en moins de photons atteignent l'extrémité de la fibre. Les photons perdus ne sont simplement pas pris en compte pour la constitution de la clé. Finalement quand la distance devient trop grande, le nombre de photons transmis devient trop faible pour permettre l'établissement d'une clé.

Le prototype d'id Quantique a été testé entre Genève et Lausanne, sur une distance de 67 km [27]. La technologie actuelle permet ainsi d'atteindre une distance de l'ordre de 200 km [21]. Comme la transparence des fibres optiques est proche de sa limite physique, il y a peu d'améliorations à attendre de ce côté-là. Pour augmenter la distance de transmission, il serait

bien entendu possible de chaîner les liens grâce à des stations intermédiaires sécurisées, auxquelles Eve n'aurait pas accès. Une autre solution consiste à supprimer la fibre optique. Il est ainsi possible d'échanger une clé entre une station terrestre et un satellite en orbite basse. Le satellite se déplace et se trouve quelques heures plus tard au dessus d'une seconde station, située à des milliers de kilomètres de la première et à laquelle il retransmet la clé. Dans ce cas, le satellite est implicitement considéré comme une station sécurisée. Pourtant, un tel échange avec un satellite n'a encore été réalisé.

Finalement, des chercheurs ont aussi proposé de réaliser des répéteurs quantiques relayant des qubits, sans les mesurer et donc sans les perturber. Ces travaux n'en sont encore qu'à un stade théorique. En principe, ils devraient permettre d'atteindre des distances arbitrairement grandes. Néanmoins, la technologie nécessaire à la réalisation de ces répéteurs n'est pas encore maîtrisée. La technologie de la cryptographie quantique est suffisamment mûre pour permettre le déploiement des premiers systèmes d'échange de clé sur fibre optique et ce sur des distances de plusieurs dizaines de kilomètres. Elle permet de sécuriser toutes les transactions (voix, données, etc.) entre deux sites d'un réseau métropolitain. On peut par exemple penser aux échanges d'informations entre un bâtiment bancaire et un centre d'archivage. De façon similaire, la sécurité des échanges entre des bâtiments gouvernementaux dans une capitale pourrait aussi bénéficier de cette technologie. Un des types de répéteurs est le répéteur quantique basé sur la purification et la permutation des états intriqués a été abordé [28], cependant, pour réaliser un tel système, nous devons surmonter un certain nombre de défis technologiques. Ces défis incluent la capacité de capturer des paires de photon intriqué dans des mémoires quantiques par la technique de cavité QED [114], et par le stockage des qubits d'information dans des mémoires quantiques de temps de cohérence assez long typiquement de 1 à 10 secondes.

2.5 Actualité de la cryptographie quantique

Nous citons dans cette partie le progrès dans la recherche des détecteurs de photons uniques pour l'usage dans les systèmes pratiques de cryptographie quantique. Les capteurs qui détectent et comptent les photons individuels, les plus petites quantités de lumière, avec 88% d'efficacité quantique ont été démontrés par des physiciens à l'Institut national (Etats-Unis) de la norme et technologie (National Institute of Standard and Technology - NIST) [http://www.nist.gov]. Cette efficacité record est une étape importante vers les détecteurs fiables de photons uniques utilisés dans les systèmes pratiques de cryptographie quantique, la méthode la plus sécurisée connue pour assurer l'intimité d'une voie de transmissions.

Décrit dans l'issue de juin 2005 de la revue Physical Review A, Rapid Communications, les détecteurs de NIST se composent de petite couche carrée de tungstène, 25 μm x 25 μm et d'épaisseur de 20 nm, refroidie à température d'environ 110 mK, la température de transition entre la conductivité normale et la supraconductivité. Quand une ligne à fibre optique émet un photon à la couche de tungstène, sa température s'élève et résulte d'une augmentation de la résistance électrique. Le changement de la température est proportionnel à l'énergie de photon, permettant au détecteur de déterminer le nombre de photons dans une impulsion de lumière monochromatique (voir plus de détail de fonctionnement dans la partie 5.3.3).

Ce type de détecteur a typiquement une efficacité limitée car quelques photons sont reflétés de la surface et d'autres sont transmis complètement dans le tungstène. Les scientifiques de NIST améliorent l'efficacité de détection au cours des deux dernières années

en déposant le tungstène au-dessus d'un miroir métallique et en le complétant avec une couche anti-réfléchissante, pour permettre l'absorption de plus de lumière dans la couche de tungstène.

Les détecteurs de NIST fonctionnent à la longueur d'onde de la lumière proche infrarouge utilisée pour des communications de fibre optique et produisent des coups d'obscurité négligeables. Leurs simulations indiquent qu'il devrait être possible d'augmenter l'efficacité quantique du détecteur bien au-dessus de 99% à n'importe quelle longueur d'onde dans la gamme de fréquence de l'ultraviolet au proche-infrarouge, en établissant une structure optique avec plus de couches et un contrôle plus fin d'épaisseur de couche.

En 2001, une expérience de QKD est réalisée sur une distance de 80 km avec l'aide des détecteurs InGaAs. Le taux d'erreurs QBER est de 4% sur 51 km et 9% sur 80 km dans la fibre à 1550 nm [29]. Un système qui est fabriqué à Genève (en Suisse) et actuellement commercialisé donne un taux d'échange de 50 bits par seconde sur une distance de 60 km [27].

En 2005, O.L. Gurreau *et al.* [30] présentent une méthode utilisant le protocole BB84 et une référence laser forte pour montrer que cette référence rend le système sécurisé contre l'attaque de division de nombre de photons des sources imparfaites. Pourtant, cette méthode n'utilise pas de photons uniques.

En juin 2006, Hiskett *et al.* [21] ont publié de nouveaux résultats record sur la transmission optique des clés quantiques. Ils nous ont montré que l'on peut transmettre avec succès les clés quantiques sur une distance de 184,6 km. En effet, en utilisant les impulsions laser fortement atténuées ayant un nombre moyen de photon de 0,5 on a réussi à récupérer les clés au bout d'une fibre optique de longueur de 184,6 km. Si le nombre moyen de photon est 0,1 alors la distance maximale est de 148,7 km. La clé de leur succès consiste à l'utilisation les Transition Edge Sensors ou TES qui sont supraconducteurs à très basse température. Le principal avantage de ce composant est qu'il est très sensible aux faibles variations de température. Ces derniers seront refroidis jusqu'à des températures inférieures à 0,3 K et disposés sous forme de matrice pour améliorer leur sensibilité.

3 Statistique de photons

Sommaire

3.1 Généralités

3.1.1 Définition

Une source de photons uniques (SPU) est un dispositif capable d'émettre à la demande des impulsions lumineuses contenant un et un seul photon. L'émission d'un photon unique consiste à mettre en œuvre un émetteur unique présentant des états électroniques discrets, tel qu'une molécule [31], un centre coloré [32-33], un atome [34-35] ou une nanostructure semi-conductrice [36-37]. Certains centres colorés du diamant, en particulier le centre « NV » formé par association d'une lacune et d'une impureté azote, sont stables à température ambiante et constituent un système électronique assez voisin des molécules uniques [32, 38-39].

La source de photons uniques est un élément clé dans beaucoup d'utilisations potentielles de l'information quantique. Par exemple, un ensemble de telles sources, associé à des éléments d'optique linéaire (lames séparatrices) et de photo-détecteurs, pourrait être utilisé pour réaliser un ordinateur quantique [40]. L'idée physique la plus simple pour réaliser une source émettant les photons « à la demande » est d'utiliser une excitation impulsionnelle d'un système quantique à deux niveaux [41-42]. Pour chaque impulsion d'excitation, le système émet un et un seul photon. Idéalement, la source de photons uniques doit avoir les caractéristiques suivantes :

- Un taux de répétition élevé, et donc une courte durée de vie du dipôle émetteur.
- Une grande efficacité quantique, toutes les impulsions d'excitation étant alors transformées en photons uniques.
- Une émission des photons dans un seul mode spatial avec une polarisation définie.
- Une largeur spectrale égale à la transformée de Fourier de la durée de l'impulsion.
- Et bien sûr un et un seul photon à la fois.

Pour la cryptographie quantique, la condition sur la largeur spectrale n'est pas exigée. Néanmoins, un spectre fin permet de mieux isoler la lumière provenant du système quantique par rapport au bruit environnant. La longueur d'onde d'émission devra être adaptée au milieu de propagation. En vue d'applications, on exige aussi du système d'être stable dans le temps, simple d'utilisation, et de préférence peu cher.

Caractéristiques générales des « sources de photons uniques » utilisables dans les laboratoires:

- Emission d'un photon pour chaque instant de déclenchement.
- Taux de répétition élevé : ce taux influence sur la statistique et le débit d'information.
- Bonne stabilité d'émission et de polarisation.
- Statistique d'émission : la proportion d'impulsions contenant plus d'un photon devant être aussi faible que possible.

3.1.2 Nécessité d'une source de photons uniques

La distribution quantique de clé (QKD – Quantum Key Distribution) exige des photons uniques afin de garantir la fiabilité du canal quantique à toute tentative d'espionnage. En pratique, la « sensibilité à l'espionnage » est diminuée par les erreurs expérimentales et il apparaît une limite sur le taux d'erreur de la transmission entre Alice et Bob.

Dans le principe même de la cryptographie quantique, il est fondamental de ne transmettre les informations du type clés de cryptage que sous la forme de photons uniques. Les sources de photons uniques sont actuellement à l'étude (en particulier au sein du laboratoire LPQM de l'ENS de Cachan) mais sont encore loin d'être commercialisables. Il est donc admis de les remplacer par des sources imparfaites telles que les impulsions cohérentes atténuées. De telles sources sont réalisées en diminuant, à l'aide de densités optiques, l'amplitude d'un laser ordinaire ou en utilisant des amplificateurs optiques à semi-conducteur (SOA). Celles-ci offrent l'avantage d'être faciles à obtenir à partir d'un laser fonctionnant directement en régime impulsionnel (modulation directe) ou bien à partir d'un faisceau continu dans lequel on crée des impulsions au moyen de modulateurs électro-optiques ou acousto-optiques. Evidemment, les impulsions laser atténuées présentent des inconvénients, notamment du fait que certaines impulsions contenant deux photons existent toujours.

3.2 Production de photons uniques

3.2.1 Différentes sources

A l'heure actuelle, on peut distinguer essentiellement 4 types de sources de photons uniques qui sont utilisées ou recherchées dans les laboratoires scientifiques :

- Des émetteurs quantiques (molécule, atome, centre coloré, semiconducteurs), composants capables d'émettre des impulsions lumineuses contenant un unique photon. Les émetteurs disponibles à ce jour ne sont pas encore sortis du laboratoire et présentent des imperfections (nous verrons que la probabilité d'émettre effectivement un photon est de l'ordre de 40% pour les meilleurs émetteurs [43-44]).

- Des sources lasers très fortement atténuées, si bien qu'il ne reste que bien moins d'un photon en moyenne par impulsion [45]. Ces sources constituent une approximation d'une SPU. Cela est lié à la statistique poissonnienne d'arrivée des photons dans une source laser standard : on a pu réduire le nombre moyen de photons par impulsion, il restera toujours certaines impulsions contenant deux photons ou plus. A cause de l'occurrence inévitable d'impulsions contenant plus d'un photon, une sécurité absolue de la liaison quantique n'est obtenue que dans un domaine très restreint de l'espace (débit-portée) [46]. Le remplacement d'un laser atténué par une SPU parfaite permettrait au choix d'augmenter la portée d'une liaison sur fibre optique à 1,3 μm par un facteur 2 à 3, ou son débit d'un facteur 100 typiquement.

- Des sources de photons jumeaux [47-48], dans lesquelles l'un des deux photons sert uniquement à déclencher le détecteur qui va recevoir le deuxième photon. Autrement dit, la détection d'un photon peut être utilisée pour prononcer la présence du photon complémentaire [49]. Dans ce type de protocole, on utilise essentiellement un photon unique pour la communication quantique, mais le photon jumeau permet de n'ouvrir le détecteur que lorsque cela est nécessaire, et de diminuer ainsi les coups de bruits dans ce détecteur.

- Des sources de photons jumeaux dans lesquelles l'intrication en polarisation ou en énergie-temps est utilisée au cœur même du protocole de communication quantique [50].

3.2.2 Un exemple

Il est bien difficile de savoir aujourd'hui quel type de source sera préféré dans les systèmes de cryptographie quantique de demain. Considérons le principe physique le plus simple pour réaliser une source de photons uniques, qui est d'exciter un dipôle unique avec une impulsion laser. Essayons tout d'abord de préciser intuitivement les caractéristiques des impulsions qu'il faut utiliser pour réaliser une telle source, synchronisée sur une horloge externe. Le système à deux niveaux, qui est initialement dans l'état fondamental, est porté dans l'état excité par l'impulsion. Il y reste en moyenne pendant la durée de vie du niveau excité, puis retombe vers l'état fondamental en émettant un photon. Il restera dans cet état fondamental jusqu'à la prochaine impulsion. Il est alors clair que la durée de vie de l'émetteur doit être grande devant la durée de l'impulsion, mais courte devant l'intervalle entre impulsions successives [51].

En notant δT la durée de l'impulsion d'excitation, T la séparation entre deux impulsions successives, et Γ^{-1} la durée de vie de l'émetteur, on doit donc avoir : $\Gamma\delta T << 1$ et $\Gamma T >> 1$. Une telle source a été mise en œuvre au laboratoire LPQM de l'ENS de Cachan [19].

3.3 Fonction d'auto-corrélation

Pour savoir si l'on a un émetteur unique, on analyse la statistique de sa lumière de fluorescence en mesurant la fonction d'auto-corrélation d'intensité. L'unicité du centre est donnée par une signature particulière de la fonction d'auto-corrélation. L'étude complète de la photodétection et de la fonction d'auto-corrélation est traitée dans plusieurs références [52-55], et on se limitera ici à la description des résultats obtenus.

Une fonction de corrélation de second ordre est une fonction de corrélation d'intensité-intensité, donnant l'information à la fois sur des statistiques de photon et la dynamique du processus de génération de lumière d'une source lumineuse. Elle a été présentée la première fois par Hanbury Brown et Twiss afin de mesurer la séparation angulaire des étoiles doubles [56]. Plus récemment, il a été employé en mesurant la nature non classique de la lumière telle qu'antibunching [57] et la statistique sub-Poissonienne de photon [58].

3.3.1 Fonction de corrélation classique

La fonction de corrélation est très souvent utilisée pour caractériser l'évolution d'un système. On peut mesurer la corrélation d'une variable entre les instants t et t', ainsi que la corrélation entre deux variables, pour voir si elles sont reliées. Dans notre cas, nous allons considérer la corrélation temporelle de l'intensité lumineuse. La fonction de corrélation d'ordre 2, appelée aussi fonction d'auto-corrélation d'intensité est définie par :

$$g^{(2)}(t_1,t_2)=\frac{<E^*(t_1)E^*(t_2)E(t_2)E(t_1)>}{<|E(t_1)|^2><|E(t_2)|^2>}=\frac{<I(t_1)I(t_2)>}{<I(t_1)><I(t_2)>} \qquad (3\text{-}3\text{-}1)$$

où $I(t_i)=E^*(t_i)E(t_i)$ est l'intensité du champ électrique à l'instant t_i et $E^*(t_i)$ est le conjugué complexe de $E(t_i)$.

a) Propriétés

Dans le cas d'une lumière semi-classique, on peut établir quelques propriétés de la fonction d'auto-corrélation à partir de l'équation 3-3-1. Tout d'abord, l'inégalité de Cauchy-Schwartz implique que :

$$\left(\sum_k a_k b_k\right)^2 \leq \sum_k a_k^2 \sum_k b_k^2 \tag{3-3-2}$$

et par conséquent :

$$< I_k(t_1) I_k(t_2) >^2 \leq < I_k^2(t_1) >< I_k^2(t_2) > \tag{3-3-3}$$

De plus pour un processus stationnaire on a : $< I_k^2(t_1) > = < I_k^2(t_2) >$. En effectuant le changement de variables $\tau = t_2 - t_1$, on obtient l'inégalité suivante :

$$< I(t) I(t+\tau) >^2 \leq < I^2(t) > \tag{3-3-4}$$

$$g^{(2)}(\tau) \leq g^{(2)}(0) \tag{3-3-5}$$

Cette inégalité montre que la fonction d'auto-corrélation classique est maximale en $\tau = 0$. Cette propriété est appelée groupement de photons : les photons arrivent par paquets.

Par ailleurs, en utilisant l'inégalité :

$$\left(I(t) - < I(t) >\right)^2 \geq 0 \tag{3-3-6}$$

on obtient :

$$< I(t)^2 > \geq < I(t) >^2 \tag{3-3-7}$$

On en déduit que pour $\tau = 0$:

$$g^{(2)}(0) \geq 1 \tag{3-3-8}$$

La fonction d'auto-corrélation classique est forcément supérieure à 1 au temps $\tau = 0$. Remarquons que la valeur $g^{(2)}(0) = 1$ correspond à une absence de corrélation entre deux photodétections simultanées : les deux photons sont détectés « par hasard » au même instant. Classiquement la corrélation peut être plus grande que cette valeur aléatoire, mais pas plus petite : il ne peut pas y avoir d'« anti-corrélation » entre les photodétections.

b) Fonction d'auto-corrélation d'une lumière thermique

On peut montrer que pour une lumière thermique (ou chaotique), la fonction d'auto-corrélation s'écrit sous la forme [71, 115] :

$$g^{(2)}(\tau) = 1 + \left|g^{(1)}(\tau)\right|^2 \tag{3-3-9}$$

où $g^{(1)}(\tau)$ est la fonction de corrélation du champ électrique. Pour une lumière thermique :

- Avec élargissement Doppler (spectre gaussien), ce terme s'écrit [116-117] :

$$\left|g^{(1)}(\tau)\right| = e^{-\gamma^2\tau^2} \tag{3-3-10}$$

où γ est la largeur de raie.

- Dans le cas où l'élargissement est plutôt dû aux collisions entre émetteurs, la raie de résonance est lorentzienne et nous avons [116] :

$$\left|g^{(1)}(\tau)\right| = e^{-\gamma|\tau|} \tag{3-3-11}$$

Dans ces deux cas, on remarque que $g^{(2)}(0) = 2$ (voir fig. 3-1).

3.3.2 Fonction de corrélation quantique

Pour avoir une description plus complète de la fonction d'auto-corrélation il faut tenir compte de la nature quantique de la lumière. Dans une description quantique du champ électromagnétique, le champ électrique s'écrit :

$$E(x) = E^+(x) + E^-(x) \tag{3-3-12}$$

où le terme $E^-(x)$ est le conjugué hermitien du terme $E^+(x)$. La fonction de corrélation d'ordre 2 est alors donnée par l'expression suivante (éq. 3-3-1) :

$$g^{(2)}(t_1, t_2) = \frac{< E^-(t_1)E^-(t_2)E^+(t_2)E^+(t_1) >}{< E^-(t_1)E^+(t_1) >< E^-(t_2)E^+(t_2) >} \tag{3-3-13}$$

que l'on peut écrire :

$$g^{(2)}(\tau) = \frac{< I(t+\tau)I(t) >}{< I(t) >^2} \tag{3-3-14}$$

La différence fondamentale entre les équations 3-3-13 et 3-3-1 est le fait que $E^+(t_1)$ et $E^+(t_2)$ ne commutent pas. On ne peut donc plus appliquer le théorème de Cauchy-Schwartz et $g^{(2)}(0)$ peut s'annuler. Dans le cas d'une onde monomode, l'expression 3-3-14 devient

$$g^{(2)}(0) = \frac{< a^+a^+aa >}{< a^+a >^2} = \frac{< \hat{n}(\hat{n}-1) >}{< \hat{n} >^2} \tag{3-3-15}$$

où $\hat{n} = a^+a$ est l'opérateur « nombre de photons », et $\langle\hat{n}\rangle$ est le nombre moyen de photons dans le mode.

Cas d'une lumière cohérente

Considérons une source cohérente de lumière, par exemple la lumière d'un laser, décrite par un état cohérent $|\alpha\rangle$. En utilisant la relation $a|\alpha\rangle = \alpha|\alpha\rangle$ et l'équation 3-3-15, on obtient que $g^{(2)}(t_1, t_2) = 1$ pour tous les instants t_1 et t_2. Ce résultat est identique à celui donné par la théorie semi-classique pour une onde monochromatique sans fluctuations. En effet, la distribution statistique des photons pour une source cohérente est poissonnienne, et donc il n'y a aucune corrélation entre les différentes photodétections.

3.3.3 Résumé

La figure 3-1 résume les différentes valeurs de la fonction d'auto-corrélation pour quelques types usuels de source lumineuse. Pour une lumière thermique, on retrouve le phénomène de groupement de photons qui implique que la probabilité de détecter un deuxième photon est maximale juste après avoir détecté le premier (voir fig. 3-2). Dans le cas d'une source quantique comme un système à deux niveaux, la probabilité d'avoir deux photons simultanés est nulle (anti-corrélation), et la fonction d'auto-corrélation est minimale à l'origine (dégroupement). L'expression 3-3-15 montre que la valeur de $g^{(2)}(0)$ a une influence directe à la distribution de probabilité du nombre de photons.

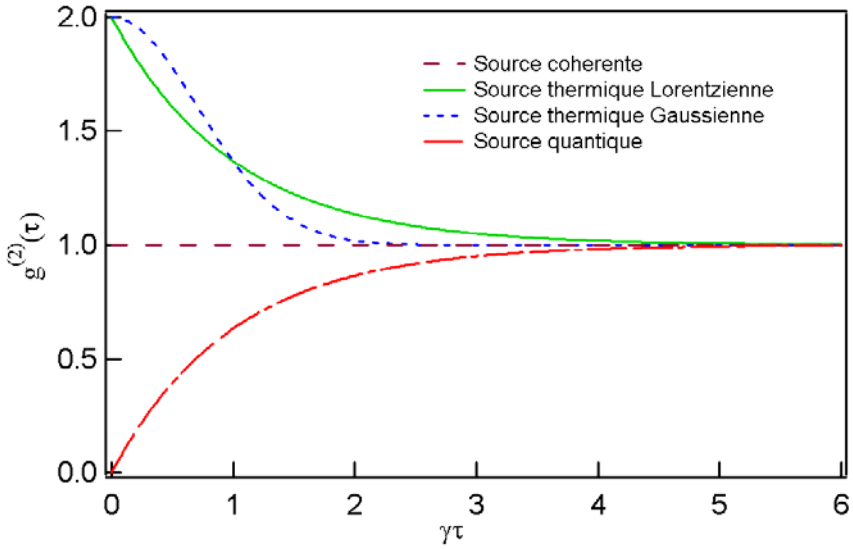


Figure 3-1. Valeur de la fonction d'auto-corrélation pour les différentes sources lumineuses. A l'origine (en $\tau = 0$), la fonction d'auto-corrélation $g^{(2)}(\tau)$ est minimale = 0 (phénomène de dégroupement de photons) dans la cas d'une source de photons uniques idéale (source quantique), et maximale = 2 pour une lumière thermique (groupement de photons). Pour une source cohérente, $g^{(2)}(\tau) = 1$, le champs présente une statistique poissonienne.

L'étude sur la corrélation d'intensité est très utile dans les méthodes de traitements de signal qui suivent car la transformée de Fourier d'une fonction d'auto-corrélation nous donnera un spectre dit densité spectrale de puissance $S(\omega)$:

$$S(\omega) = \int_{-\infty}^{+\infty} g^2(\tau) e^{-j\omega\tau} d\tau \qquad (3\text{-}3\text{-}16)$$

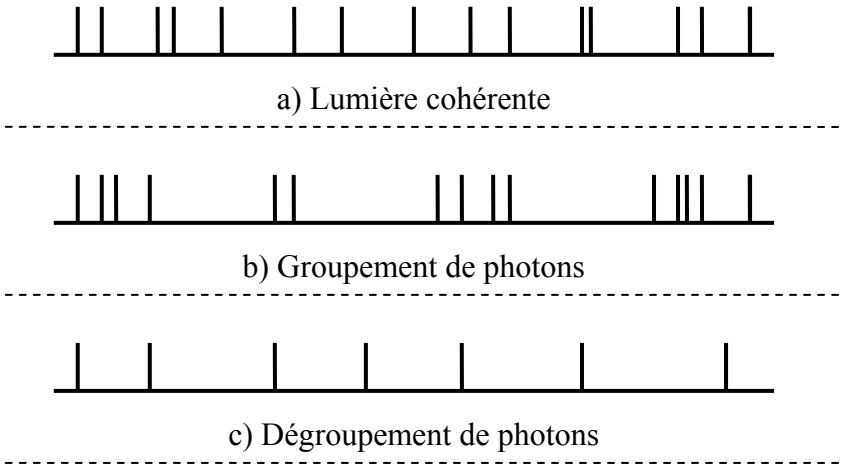


Figure 3-2. Représentation schématique des temps d'arrivée des photons en fonction de la valeur de l'auto-corrélation d'intensité. a) Lumière cohérente : $g^{(2)}(\tau) = 1$, les photons arrivent aléatoirement, sa distribution a pour profil poissonien ; b) groupement de photons : les photons arrivent par paquets ; c) dégroupement de photons : possibilité d'émettre un photon à intervalles de temps réguliers ou sur commande.

3.3.4 Mesure de corrélation de photons

On utilise un émetteur de photons [39]. Cette mesure pour laquelle le schéma expérimental est donné dans la figure 3-3 a pour but d'assurer qu'il n'y a qu'un seul photon émis dans un intervalle de temps considéré. On enregistre les corrélations temporelles entre les photons de fluorescence (fig. 3-4). Le faisceau de fluorescence est séparé en deux parties de même intensité à l'aide d'une lame semi-réfléchissante, de part et d'autre de laquelle sont disposées deux photodiodes à avalanche au silicium fonctionnant en régime de comptage de photons.

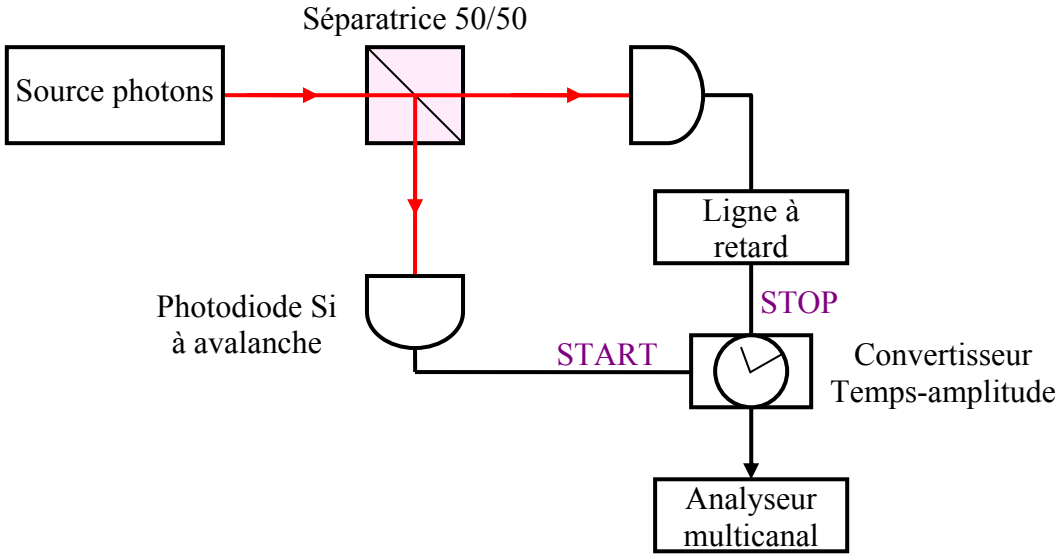


Figure 3-3. Mesure de corrélation de photons dans le visible avec les photodiodes au silicium.

Un « convertisseur temps-amplitude » transforme le retard entre un photon détecté sur l'une des photodiodes (« Start ») et le suivant sur l'autre photodiode (« Stop »), en une tension

proportionnelle à ce retard. Cette dernière alimente un « analyseur multicanal » dont la fonction est de construire en temps réel l'histogramme des retards entre photons consécutivement détectés.

Le diagramme obtenu (fig. 3-4) présente une série de pics régulièrement espacés de la période de répétition du laser de pompe (ici 188 ns). Ces pics, qui correspondent aux coïncidences entre photons provenant d'impulsions décalées dans le temps, ont une largeur directement reliée à la durée de vie radiative du centre coloré, qui est ici proche de 20 ns. Les retards négatifs sont réalisés en faisant passer le signal provenant de l'une des deux photodiodes dans une ligne à retard (fig. 3-3).

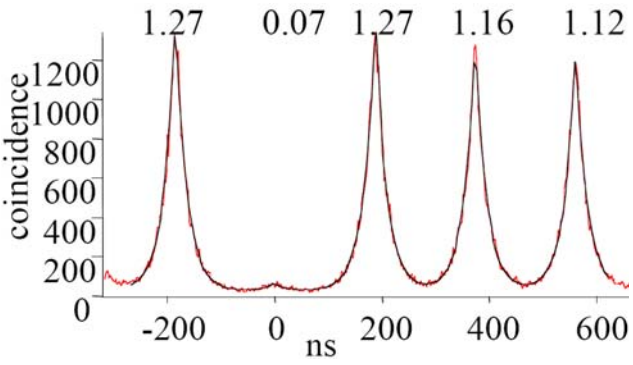


Figure 3-4. Diagramme de corrélation de photons [39].

On observe au milieu de la fenêtre temporelle d'analyse le pic correspondant au retard nul, c'est-à-dire à une détection en coïncidence de part et d'autre de la lame séparatrice. Ce pic possède une aire beaucoup plus petite que celle de ses voisins et il disparaîtrait totalement pour une source de photons uniques idéale, car la détection simultanée de deux photons (ou plus), un sur chaque détecteur, est alors impossible. La persistance d'un pic résiduel révèle que la source comporte encore quelques événements mutiphotoniques, liés à la lumière parasite. Remarquons que l'existence d'un deuxième centre coloré dans le même nanocristal conduirait à une hauteur du pic central environ moitié de celle des pics adjacents. Une telle expérience démontre clairement l'unicité du centre émetteur, ainsi que du photon émis.

3.4 Etude des fluctuations d'intensité

3.4.1 Principe général

Une façon directe de mesure des fluctuations, où le bruit, de la lumière est d'enregistrer les valeurs d'intensité $I(t)$ dans le temps et d'évaluer la variance $\Delta I^2(t)$ pour un certain intervalle de temps de détection. La variance est définie comme la suivante :

$$\Delta I^2(t) = \mathrm{Var}(I(t)) = \left\langle \left(I(t) - \langle I \rangle\right)^2 \right\rangle - \left\langle I(t) - \langle I \rangle \right\rangle^2 \qquad (3\text{-}4\text{-}1)$$

où $\langle I \rangle$ est l'intensité moyenne et les parenthèses dénotent une moyenne pendant un intervalle de temps de détection.

On a donc la moyenne quadratique :

$$\mathrm{RMS}(I(t)) = \sqrt{\mathrm{Var}(I(t))} = \sqrt{\Delta I^2(t)} \tag{3-4-2}$$

Une mesure plus efficace est le spectre de bruit d'intensité. Toute information portée par la lumière, même le bruit, peut s'exprimer dans une combinaison de modulation d'amplitude et de phase. Toute modulation, à son tour, peut être exprimée en termes de bandes de modulation correspondantes.
L'amplitude des bandes de modulation à une fréquence contient toute l'information du bruit classique à cette fréquence particulière. Un spectre de bruit présente la largeur des fluctuations mesurées pour une gamme de fréquences de détection Ω. La transformée de Fourier de $I(t)$ nous donne les composantes de $I(\Omega)$.

D'une façon identique de la précédente, on a :

$$\Delta I^2(\Omega) = \mathrm{Var}(I(\Omega)) = \left\langle \left(I(\Omega) - \langle I(\Omega) \rangle \right)^2 \right\rangle - \left\langle I(\Omega) - \langle I(\Omega) \rangle \right\rangle^2 \tag{3-4-3}$$

Si on utilise une photodiode pour détecter cette lumière alors la photodiode enregistrera l'intensité lumineuse moyenne et sa modulation. Ceci s'écrit :

$$I_{\mathrm{mod}}(t) = m(t)\langle I \rangle \tag{3-4-4}$$

où $m(t)$ est la fonction de modulation. En composantes de Fourier de $M(\Omega)$, on a :

$$M(\Omega) = F\{m(t)\}\langle I \rangle \tag{3-4-5}$$

$M(\Omega)$ représente le changement relative de l'intensité lumineuse à une fréquence de modulation. S'il s'agit d'une modulation harmonique monofréquence et d'une mesure sur l'oscilloscope, la grandeur de $M(\Omega)$ est égale au carré de l'amplitude AC.

Le rapport signal-bruit (SNR) vaut :

$$\mathrm{SNR} = \frac{M(\Omega)^2}{\mathrm{Var}(I(\Omega))} \tag{3-4-6}$$

3.4.2 Calcul de l'excès de bruit

Nous abordons le calcul théorique. Le rapport signal sur bruit (SNR – signal to noise ratio) est donné par :

$$SNR = \frac{V1_{\mathrm{signal}}(\Omega) - V1_{\mathrm{bruit\ quantum}}(\Omega)}{V1_{\mathrm{bruit\ quantum}}(\Omega)} \tag{3-4-7}$$

où V1 est la variance du signal laser de l'entrée.

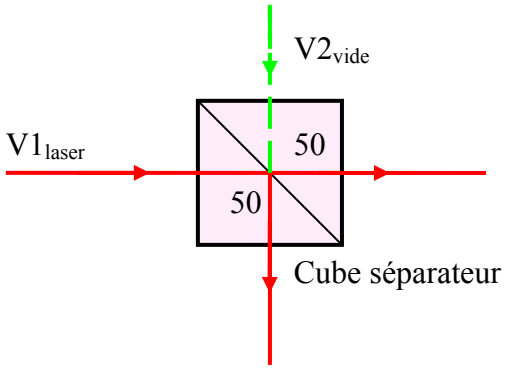


Figure 3-5 : Représentation schématique d'un cube séparateur optique. V1 et V2 sont les variances des deux entrées (laser et vide) du cube séparateur.

Le SNR à la sortie de la séparatrice s'écrit :

$$\mathrm{SNR}_{\mathrm{sortie}} = \varepsilon \mathrm{SNR}_{\mathrm{entrée}} \tag{3-4-8}$$

où ε est le coefficient de réflexion de la séparatrice.

Lorsqu'on dispose d'un atténuateur à l'entrée laser, la variance des photocourants avec l'atténuation s'exprime :

$$V1_{out} - V_{SN\_out} = \sqrt{T}\left(V1_{in} - V_{SN\_in}\right) \tag{3-4-9}$$

$$V_{SN\_in} = \sqrt{T}.V_{SN\_out} \tag{3-4-10}$$

Ici, on note : 'in' = avant atténuateur et 'out' = après atténuateur.

Nous avons donc :

$$\left(\frac{V1_{in}}{V_{SN\_in}} - 1\right)T = \frac{V1_{out}}{V_{SN\_out}} - 1 \Leftrightarrow \left(SNR_{in} - 1\right)T = SNR_{out} - 1 \tag{3-4-11}$$

ou

$$SNR_{out} = 1 + T\left(SNR_{in} - 1\right) \tag{3-4-12}$$

En unité dB, nous pouvons écrire :

$$SNR_{out}[dB] = 10\log\left[1 + T(10^{SNR_{in}[dB]/10} - 1\right] \tag{3-4-13}$$

Par conséquent, le bruit d'excès vaut :

$$\left(P^{+} - P^{-}\right)^{in} = 10\log\left[1 + \frac{1}{T}\left(10^{\left(P^{+} - P^{-}\right)^{out}/10} - 1\right)\right] \tag{3-4-14}$$

avec $T = \dfrac{\text{puissance optique après atténuateur}}{\text{puissance optique avant atténuateur}}$.

Il est intéressant de voir ce qui se passe dans les deux cas de limites suivants :

a) Si $10^{\left(P^+ - P^-\right)^{out}/10} >> 1$ alors $\left(P^+ - P^-\right)^{in} = \left(P^+ - P^-\right)^{out} - 10\log T$

b) Si $\left(P^+ - P^-\right)^{out} = 0$ alors $\left(P^+ - P^-\right)^{in} = 0$ ce qui n'a pas de sens car $\left(P^+ - P^-\right)^{out}$ ne tend qu'asymptotiquement vers 0.

3.4.3 Mesure expérimentale

a) Caractérisation du bruit d'une diode laser

Il est important de caractériser le bruit de la diode laser en fonction des conditions de fonctionnement. Les mesures sont effectuées à l'aide d'un analyseur de spectre avec une détection homodyne équilibrée [59]. Le schéma de l'expérience est présenté dans la figure 3-6.

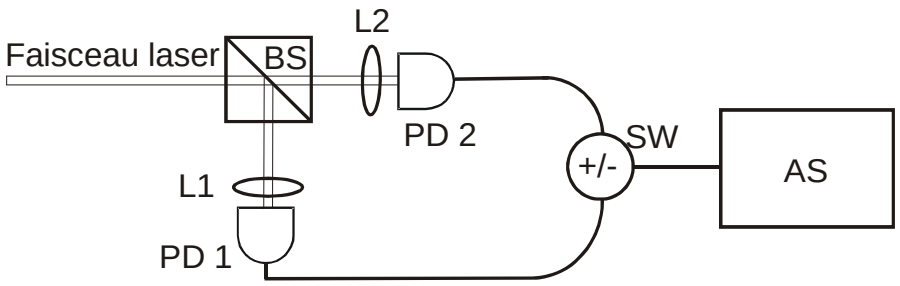


Figure 3-6. Système expérimental employé pour la détection homodyne équilibrée. BS : cube séparateur ; L : lentilles ; PD : photodiodes BPX65 ; SW : interrupteur pour fonction somme (switch +) ou différence (switch -) ; AS : analyseur de spectre pour la mesure de la densité spectrale de puissance (HP4396A). Le faisceau laser à 785 nm est généré par une diode HL7851G.

Le cube séparateur envoie le bruit classique vers deux détecteurs. Pour le bruit optique classique, les photocourants créés par deux photodiodes sont corrélés ; ils peuvent donc être soustraits ou éliminés. Pour le bruit quantique, l'effet de la séparatrice est différent car les deux photocourants obtenus ne sont pas corrélés. Cela signifie que les bruits quantiques dans les deux voies de la détection homodyne s'ajoutent en quadrature pour à la fois la fonction somme (switch +) et différence (switch -). En plus, il est évident que le bruit électronique de deux détecteurs n'est pas corrélé ; il s'ajoute en quadrature. Il n'est donc pas facile à le distinguer du bruit quantique.

Finalement, le dispositif peut supprimer tout le bruit technique et classique de la lumière et laisser uniquement le bruit électronique et optique quantique. Heureusement, dans ce montage le bruit électronique est souvent de beaucoup inférieur au le bruit quantique et donc peut être négligé.

La fréquence de mesure varie de 1 à 7 MHz sur l'analyseur de spectre et les mesures sont faites pour différentes valeurs du courant direct dans la diode laser. Le facteur d'excès de

bruit de la diode laser est donné par la formule 3-4-15 où il est exprimé en fonction du bruit global détecté N_d, du bruit de grenaille N_s et du bruit électronique N_e. Le switch employé permet d'obtenir en position « somme » le bruit global des détecteurs N_d, et en position « différence » le bruit de grenaille N_s. Le bruit électronique est lui mesuré en condition d'obscurité.

$$N_{excess} = N_d - N_s - N_e \tag{3-4-15}$$

Nous notons que le bruit électronique N_e sera négligé dans le calcul parce qu'il est beaucoup plus faible par rapport au bruit de grenaille (voir fig. 3-7).

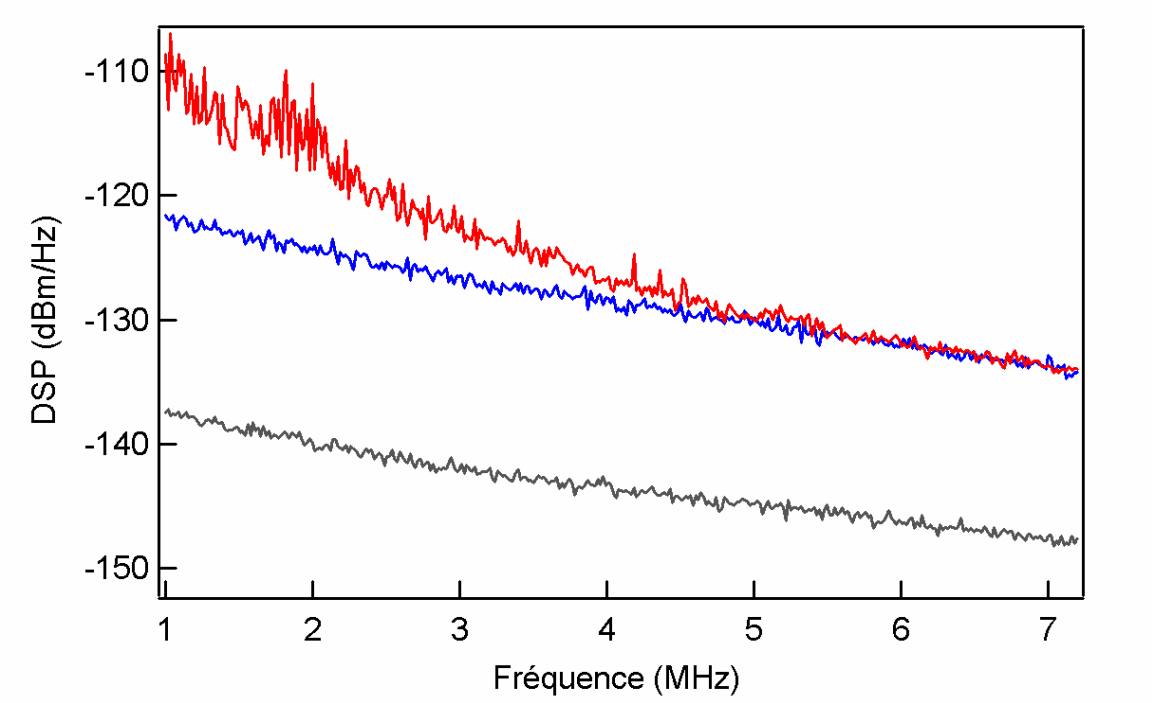


Figure 3-7. Visualisation sur l'analyseur de spectre du résultat de la détection homodyne de la diode laser 785 nm (HL 7851G) : la densité spectrale de puissance de bruit (DSP) en fonction de la fréquence. La courbe supérieure (en rouge) est la DSP ou bruit global des détecteurs pour un courant direct de 97 mA ($I/I_{th} = 2{,}35$), correspond à la somme de deux détecteurs (switch +) ; la courbe du milieu (en bleu) est le bruit de photon, correspond à la différence de deux détecteurs (switch -) ; la courbe inférieure est bruit électronique des détecteurs. A partir de 5 MHz, le bruit global des détecteurs a le même niveau du bruit de photon.

Comme le temps mort dans le système de détection est plus grand que la largeur d'impulsion, on ne peut détecter qu'un seul photon par détecteur pour chaque impulsion. Si l'impulsion contenant deux photons tombe sur un détecteur, ce dernier va compter uniquement un photon. Les résultats sont rassemblés sur la figure 3-7. A la fréquence inférieure à 5 MHz, le bruit de système est dominé par celui des détecteurs mais à partir de 5 MHz, ce bruit a le même niveau du bruit de photon. Cette conclusion dépend forcément du courant direct de la diode laser.

On représente aussi le facteur d'excès de bruit à la fréquence de 5 MHz dans la figure 3-8. Le niveau de bruit électronique est situé 16 dB en dessous du bruit de photon et il est donc

négligeable dans l'équation 3-4-15. L'excès de bruit diminue lorsque le courant direct dans la diode augmente, et à partir d'un courant de $2{,}8 \times I_{th}$, on peut considérer que le bruit d'intensité de la diode laser est limité par le bruit de photon.

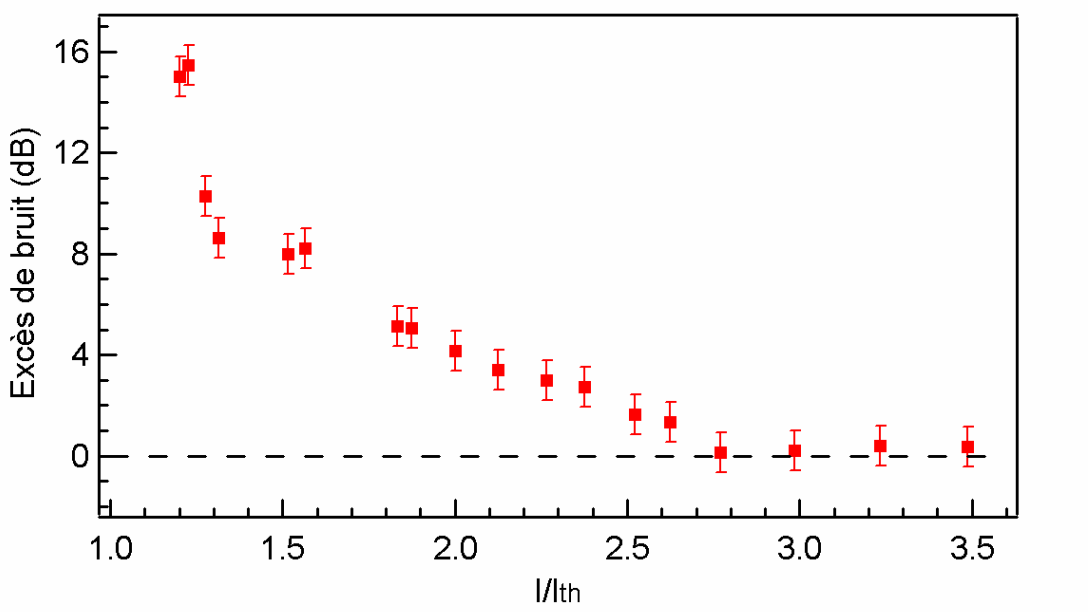


Figure 3-8. Excès de bruit de l'intensité de la diode laser, mesuré à 5 MHz, en fonction du courant dans la diode I/I_{th} ($\mathbf{I_{th}}$= 40 mA). L'excès de bruit atteint à zéro à grandes valeurs de courant direct de la diode laser (courant direct supérieur à 100 mA)

3.4.4 Paramètre de Mandel

Le paramètre (ou facteur) de Mandel est introduit pour étudier la statistique du nombre de photons dans la fluorescence de résonance (resonance fluorescence) [60]. Il est un critère très utile et efficace pour distinguer une lumière non-classique de celle classique et caractériser la statistique de photon. Le paramètre de Mandel Q est défini par [60-61] :

$$Q = \frac{\left\langle (\Delta n)^2 \right\rangle - \langle n \rangle}{\langle n \rangle} = \frac{\left\langle n^2 \right\rangle - \langle n \rangle^2}{\langle n \rangle} - 1 \qquad (3\text{-}4\text{-}16)$$

où $\left\langle (\Delta n)^2 \right\rangle$ est la variance du nombre de photons, $\Delta n = n - \langle n \rangle$, $\langle n \rangle$ est le nombre moyen de photons, $\langle\ \rangle$ doit être compris comme la valeur moyenne sur un ensemble de mesures ayant toutes le même intervalle d'observation, n est le nombre de photons émis pendant un certain intervalle de temps. Une distribution de Poisson est caractérisée par Q = 0, pour l'instant, la lumière cohérente appartient à cette catégorie. Le paramètre de Mandel devient positif Q > 0 (comportement super-Poissonnien) pour toute lumière classique qui possède une variance du nombre de photon supérieure au nombre moyen de photons. Le paramètre de Mandel devient négatif Q < 0 (comportement sub-Poissonnien) si la variance du nombre de photons est inférieure au nombre moyen de photons et la lumière correspondante est considérée comme non-classique.

Notre point de départ est la formule donnant la probabilité pour laquelle *n* événements sont détectés dans un intervalle de temps limité de t à $t+T$ quand la lumière arrive sur une photodiode [62-63], qui peut être convertie en une expression pour la probabilité d'avoir n photons émis pendant l'intervalle $[t, t+T]$:

$$p(n)=\left\langle \frac{1}{n!}\left[\int_{t}^{t+T} I(t')dt'\right]^{n} \times \exp\left[-\int_{t}^{t+T} I(t')dt'\right]\right\rangle \qquad (3\text{-}4\text{-}17)$$

Ici, $I(t)$ est le flux total de photons exprimé en unité de photons par second.

3.4.5 Distribution de Poisson

Avec une source cohérente, la probabilité de trouver *n* photons s'exprime par :

$$P(n)=\frac{\alpha^{n}}{n!}e^{-\alpha} \qquad (3\text{-}4\text{-}18)$$

où α est le nombre moyen de photons par impulsion et n = 0, 1, 2. La probabilité d'un signal de multiphotons est théoriquement de $P(>1)=1-P(0)-P(1)=1-e^{-\alpha}(1+\alpha)$, ce qui vaut approximativement $\frac{\alpha^{2}}{2}$ pour $\alpha<1$.

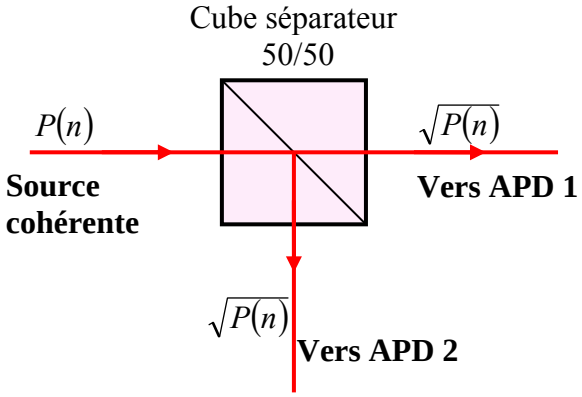


Figure 3-9. Probabilité de réception de la lumière cohérente avec une séparatrice ou un cube séparateur 50/50 (50% transmission – 50% réflexion). C'est à cause de temps mort de détection que l'on emploie deux détecteurs qui augmentent donc les chances de détecter des photons.

En pratique, la probabilité de réception des photons est mesurée d'après le schéma de manip comprenant 2 photodétecteurs (fig. 3-9).

- La probabilité de trouver 0 photon = $P_{coh}(0)$ se présente lorsque deux photodiodes ne reçoivent aucun photon simultanément : $P_{coh}=P(0)=e^{-\alpha}$
- On cherche la probabilité de trouver 1 photon = $P_{coh}(1)$

$P_{coh}(1)$ résulte des impulsions contenant exactement 1 photon *ou* des impulsions contenant plus 1 photon (car une APD ne peut pas détecter plus d'un photon par impulsion). De plus, dans ce cas, l'APD1 reçoit 1 photon *et* l'APD2 ne reçoit aucun photon, et inversement.
Par conséquent :

$$P_{coh}(1) = \left\{\left[P(1)+P(>1)\right]_{APD1} + \left[P(1)+P(>1)\right]_{APD2}\right\} \times P_{APD1\,ou\,APD2}(0), \qquad (3\text{-}4\text{-}19)$$

et donc :

$$P_{coh}(1) = 2\left(1 - P_{APD1}(0)\right) \times P_{APD2}(0) = 2\left(1 - e^{-\alpha/2}\right) \times e^{-\alpha/2}. \qquad (3\text{-}4\text{-}20)$$

- Et la probabilité de trouver 2 photons = $P_{coh}(2)$?

Deux APD reçoivent 2 photons en même temps. Alors,

$$P_{coh}(2) = \left[P(1)+P(>1)\right]_{APD1} \times \left[P(1)+P(>1)\right]_{APD2} \qquad (3\text{-}4\text{-}21)$$

$$P_{coh}(2) = \left(1 - P_{APD1}(0)\right) \times \left(1 - P_{APD2}(0)\right) = \left(1 - e^{-\alpha/2}\right)^2 \qquad (3\text{-}4\text{-}22)$$

Le nombre moyen de photons détectés par impulsion peut s'exprimer :

$$\overline{n}_{coh} = \sum_i P_i n_i = n_0 P_{coh}(0) + n_1 P_{coh}(1) + n_2 P_{coh}(2) \qquad (3\text{-}4\text{-}23)$$

$$\overline{n}_{coh} = 0 + 1P_{coh}(1) + 2P_{coh}(2) \qquad (3\text{-}4\text{-}24)$$

$$\overline{n}_{coh} = 2e^{-\alpha/2}\left(1 - e^{-\alpha/2}\right) + 2\left(1 - e^{-\alpha/2}\right)^2 = 2\left(1 - e^{-\alpha/2}\right) \qquad (3\text{-}4\text{-}25)$$

On en déduit que :

$$Q_{coh} = e^{-\overline{n}_{coh}/2} - 1 \cong \frac{-\overline{n}_{coh}}{2} \qquad (3\text{-}4\text{-}26)$$

$$Q_{coh} = \frac{-\overline{n}_{coh}}{2} < 0 \qquad (3\text{-}4\text{-}27)$$

Il peut arriver que le paramètre de Mandel soit négatif dans le cas d'une distribution de Poisson. La discussion détaillée de ce problème se trouve à la partie 3.5.3.

3.4.6 Relation entre le facteur de Mandel Q et le bruit d'intensité

La fonction de corrélation d'intensité nous donne l'information sur la statistique et la distribution temporelle des fluctuations d'intensité de la lumière. Pour la lumière classique, la présence des fluctuations d'intensité mènera au groupement des photons détectés pendant la

période de fortes fluctuations d'intensité. Un laser classique fonctionnant loin au-dessus du seuil aura des fluctuations d'intensité nulles [cf. partie 3.4.3]. Dans le traitement quantique, l'intensité du laser qui est caractérisée par le nombre de photons *n* obéira à la loi statistique de Poisson [cf. partie 3.5.3]. La fonction de corrélation d'intensité peut être établie en analysant les fluctuations du courant issu d'un détecteur ou en mesurant directement les coïncidences de deux photons.

D'après Mandel [63], la probabilité d'obtenir *n* photodétection dans un détecteur idéal, de temps mort nul, pendant l'intervalle *T* (petit par rapport au temps de corrélation de la lumière), peut s'exprimer par :

$$p(n) = \int_0^\infty p(W) \frac{e^{-W} W^n}{n!} dW = \left\langle \frac{e^{-W} W^n}{n!} \right\rangle \tag{3-4-28}$$

où $W = \alpha IT$, la parenthèse représente une moyenne d'ensemble, α est l'efficacité quantique du détecteur, I est l'intensité optique aléatoire d'incident exprimée en photons par unité de temps, et $p(W)$ est considérée comme la densité de probabilité de W. L'expression 3-4-28 est appliquée pour la détection mais elle a la même forme que 3-4-17.

En utilisant l'expression 3-4-16 et en tenant compte le fait que l'intensité I est proportionnelle au nombre de photons par unité de temps, nous pouvons réécrire le facteur de Mandel :

$$Q = \frac{\left\langle (\Delta I)^2 \right\rangle}{I} - 1 \tag{3-4-29}$$

3.5 Statistique de photons

Le but de cette partie est de présenter les résultats concernant une étude de la statistique de photons. Dans le cadre de la cryptographie quantique des impulsions laser fortement atténuées sont employées à la place de photons uniques qu'il est encore difficile de produire. Le comportement poissonien de ce type d'impulsion a donc été testé dans une expérience de comptage de photons, pour différentes techniques de réalisation des impulsions. Les résultats de cette étude ont donné lieu à des publications en congrès [p1 et p2] et en revue internationale [p7].

3.5.1 Introduction

La cryptographie quantique est employée dans le but de transmettre les clés de cryptage d'un document [12]. La fiabilité de cette méthode repose sur les propriétés fondamentales de la mécanique quantique appliquées à des photons uniques [39]. Ce n'est que récemment que de telles émissions ont pu être obtenues de façon expérimentale [27]. Les travaux sur la distribution de clés quantiques ont donc été fondés sur des impulsions laser fortement atténuées et simulant ainsi des photons uniques [64]. Les auteurs font l'hypothèse que la statistique d'émission des photons est du type Poisson pour la mise en œuvre du traitement des données [65].

Bien que l'on a récemment démontré par de nombreuses expériences la cryptographie quantique à vrais photons uniques [39, 66], la plupart des réalisations de cryptographie quantique pratique s'appuient sur l'atténuation simple des impulsions laser [67]. Les impulsions cohérentes fortement atténuées (Weak Coherent Pulses – WCPs) avec un nombre moyen de photon inférieur à l'unité sont effectivement une solution facile pour la réalisation des sources de photons uniques car elles exigent seulement des éléments optiques de base comme lasers semiconducteurs standard et atténuateurs linéaires calibrés. Tandis que la preuve de sécurité de la cryptographie quantique demande une transmission pure des photons uniques, l'usage des impulsions laser atténuées est une porte ouverte pour la fuite d'information vers un espion [68].

Il existe plusieurs façons pour assurer sans conditions la sécurité dans le montage pratique qui utilise les impulsions atténuées WCPs à la place des impulsions pures de photons individuels. Une solution simple est l'augmentation du niveau d'atténuation dans le canal quantique afin de minimiser l'apparition des impulsions contenant deux photons ou plus. En réalité, les impulsions laser encodées correspondraient à un nombre moyen de photons par impulsion bien inférieur à l'unité.

3.5.2 Production et détection d'impulsions laser

Le système expérimental permettant la production des impulsions laser ainsi que la détection et le comptage des photons est présenté dans la figure 3-10.

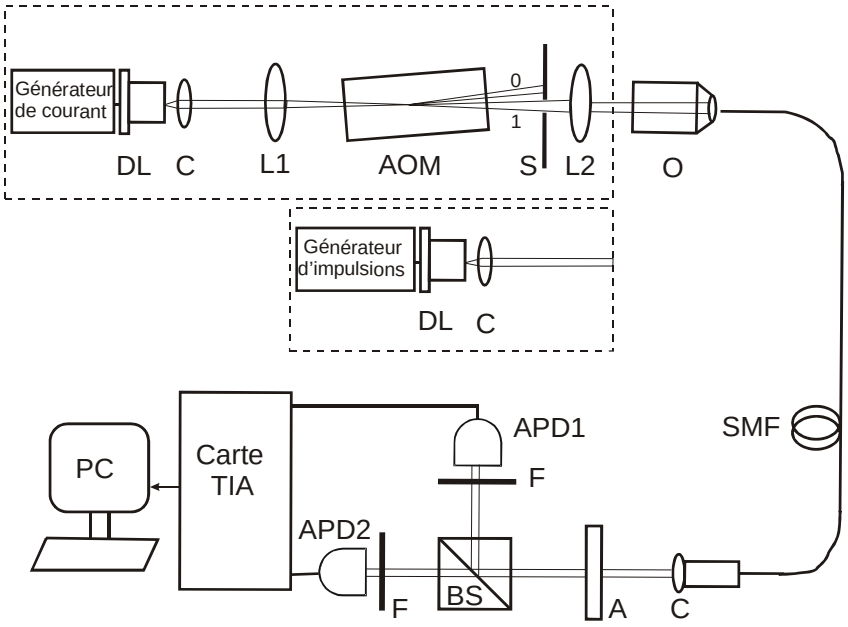


Figure 3-10. Montage expérimental pour la mesure de la statistique de photons dans des impulsions laser atténuées. DL : diode laser ; C : collimateur ; L : lentille ; AOM : modulateur acousto-optique ; S : diaphragme ; O : objectif de microscope ; SMF : fibre monomode ; A : atténuateur (densité optique) ; BS : cube séparateur ; F : filtre ; APD : photodiode à avalanche ; TIA : carte "time interval analyzer".

La diode laser employée (Hitachi HL7851G) est une diode de type à puits quantique, de longueur d'onde centrée à 785 nm. Les impulsions laser sont obtenues de deux façons. La

première consiste à faire fonctionner la diode en continu, pilotée ici par une source de courant commerciale LDC8002 de la société Profile Optics System. La diode fonctionne soit à son seuil de déclenchement $I_{th} \approx 40\,mA$ soit à 3,5 fois ce seuil c'est à dire 140 mA. Une modulation externe du faisceau est appliquée par l'intermédiaire d'un modulateur acousto-optique (AA.MT110), l'ordre '1' du faisceau diffracté étant sélectionné par un diaphragme. Les impulsions obtenues ont une largeur d'environ 8 ns. La deuxième méthode consiste à commander directement la diode par des impulsions de courant de durée 8 ns, le circuit de commande étant réalisé au laboratoire. Les impulsions de courant ont à peu près les mêmes niveaux qu'en cas de fonctionnement continu. Les impulsions laser sont ensuite atténuées de façon à ne contenir qu'en moyenne 1 photon par impulsion. L'atténuation optique servant à la génération de photons individuels est déterminée par la puissance mesurée. Cette méthode est décrite ci-dessous.

La puissance optique (juste avant atténuateur) de la diode laser est de 1 μW ; elle fonctionne dans le mode impulsionnel de 5 MHz. La puissance moyenne de ces impulsions est :

$$P_{moyenne} = Nh\nu f = 1\ \mu\text{W} = 10^{-6}\ \text{W} \tag{3-5-1}$$

où N est le nombre de photons par impulsion, h est la constante de Planck, ν est la fréquence des photons, f est le taux de répétition d'impulsion. Comme la puissance moyenne d'un photon individuel généré à un taux de répétition f est :

$$P_{un\ photon} = h\nu f = h\frac{c}{\lambda}f \tag{3-5-2}$$

On a donc $P_{un\ photon} = 6{,}626.10^{-34}.3.10^{8}.5.10^{6}.(1{,}55.10^{-6})^{-1} = 6{,}41.10^{-13}$ W. L'énergie d'un photon est $W_{un\ photon} = h\nu = h\frac{c}{\lambda} = 1{,}28.10^{-19}$ J = 0,8 eV. Le nombre de photons N dans une impulsion est :

$$N = \frac{P_{moyenne}}{P_{un\ photon}} \tag{3-5-3}$$

Pour atteindre le niveau d'atténuation de photon unique, ATTEN, il faut avoir :

$$ATTEN = \frac{1}{N} = \frac{P_{un\ photon}}{P_{moyenne}} \tag{3-5-4}$$

Alors, $N = 10^{-6} / 6{,}41.10^{-13} = 1{,}56 \times 10^{6}$. Par conséquent, d'après 3-5-4, le niveau d'atténuation de la génération de photons uniques est de 10log(ATTEN) = - 61,93 dB. Avec cette diminution on obtiendra une puissance optique équivalente à un photon dans une impulsion. Le nombre moyen de photons est donc 1, qui est utilisé comme source de photons uniques dans notre expérience. Pour assurer la génération de photons uniques, nous disposons d'une atténuation de - 70 dB à - 80 dB pour que l'on ait seulement un photon dans toutes les 10 impulsions, c'est-à-dire, le nombre moyen de photon est de 0,1.

Une fois les impulsions laser atténuées de façon à ne contenir qu'en moyenne 0,1 photon par impulsion, le faisceau laser est injecté dans une fibre optique monomode pour aller vers le système de détection constitué de deux détecteurs à photodiode à avalanche, le faisceau ayant été divisé en deux parties équilibrées. Les événements correspondants aux arrivées de photons sont comptés dans une carte GT653 de la société GuideTech qui a une profondeur mémoire de 32 kB, un temps mort de 250 ns et une résolution temporelle de 75 ps. C'est à cause de ce temps mort que l'on emploie deux détecteurs qui augmentent donc les chances de détecter des photons. Des filtres sont placés devant les détecteurs pour éviter le phénomène de cross-talk (diaphonie) optique entre les deux détecteurs [69].

3.5.3 Critère « poissonien »

Dans cette expérience il s'agit de tester le caractère poissonien de la statistique de photons dans les impulsions fortement atténuées. La statistique de photons est souvent étudiée par la fonction de corrélation du second ordre que l'on détermine expérimentalement par la technique « Start-Stop » conduisant ainsi aux probabilités de détecter un certain nombre de photons [70]. Mais le critère retenu dans cette étude est le paramètre de Mandel [71], défini en fonction de la variance du nombre de photons par impulsion, notée $<(\Delta n)^2>$, et du nombre moyen de photons par impulsion, noté $<n>$:

$$Q = \frac{<(\Delta n)^2>}{<n>} - 1 \tag{3-5-5}$$

Avec cette définition il apparaît que :

- $Q = 0$: caractérise une statistique de type Poisson,
- $Q < 0$: une statistique sub-poissonienne
- $Q > 0$: une statistique super-poissonienne

où n représente le nombre de photons détectés par impulsion [72].

Néanmoins la statistique est faussée par le temps mort propre aux détecteurs et à la carte de comptage. En fait pour une *source cohérente* contenant un nombre moyen de photons par impulsion noté α, il est possible de calculer la distribution de probabilité de comptage *P(n),* pour $n = 0, 1, 2$ photons et l'on obtient :

$$P(0) = e^{-\alpha} \tag{3-5-6}$$

$$P(1) = 2e^{-\alpha/2}\left(1 - e^{-\alpha/2}\right) \tag{3-5-7}$$

$$P(2) = \left(1 - e^{-\alpha/2}\right)^2 \tag{3-5-8}$$

Le nombre moyen, noté $\overline{n}$, de photons détectés par impulsion est donné par :

$$\overline{n} = 2\left(1 - e^{-\alpha/2}\right) \tag{3-5-9}$$

Le paramètre de Mandel doit être corrigé et devient alors :

$$Q = Q_C = e^{-\bar{n}/2} - 1 \qquad (3\text{-}5\text{-}10)$$

Dans ces conditions, le caractère « poissonien », « sub-poissonien » ou « super-poissonien » ne se détermine donc non plus par comparaison à $Q = 0$ mais par comparaison à $Q_C = e^{-\bar{n}/2} - 1$ qui serait inférieur à zéro, comme indiqué dans la figure 3-11. Il est important de se rappeler que ceci est dû à la prise en compte des temps morts dans le comptage de photons. Par exemple, pour $\bar{n} = 0{,}1$, on prévoit $P(0) = 0{,}904837$, $P(1) = 0{,}092784$, $P(2) = 2{,}378 \times 10^{-3}$ et $Q_C = -0{,}0488 < 0$ (d'après les équations 3-5-6, 3-5-7, 3-5-8).

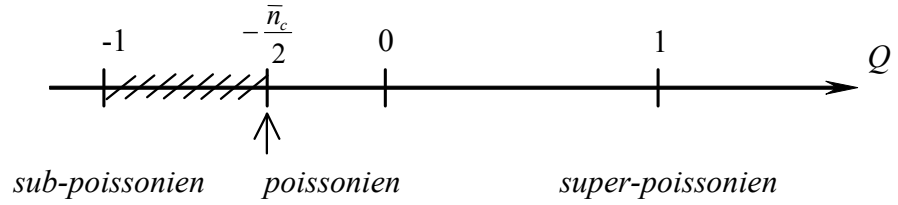


Figure 3-11. Terminologie employée selon les valeurs du paramètre de Mandel Q.

Il est important de noter que les pertes entraînées par le cube séparateur et par les détecteurs ne changent pas la statistique de photons en elle-même mais seulement la valeur moyenne du nombre de photons.

Enfin à titre de comparaison considérons une source de photons uniques déclenchés. Le paramètre de Mandel pour une telle source non bruitée serait $Q_S = -1$ car $< (\Delta n)^2 > = 0$. Cependant compte tenu de l'efficacité quantique non unitaire à la détection, le paramètre de Mandel mesuré dépend de Q_S selon la relation $Q = \eta \times Q_S$ [73], où η est l'efficacité quantique globale. Ainsi pour une telle source : $Q = -\eta$. Cette prédiction a été vérifiée expérimentalement très récemment [74]. Pour $\bar{n} = 0{,}1$, on mesurerait $Q \approx -0{,}1$ dans le cas d'une source de photons uniques. C'est une valeur inférieure à celle prévue pour une source cohérente présentant le même nombre moyen de photons détectés par impulsion, indiquant une réduction du bruit attendu pour un tel flux de photons.

3.5.4 Traitement des données

Un exemple typique d'une séquence d'acquisition conduit à 284397 impulsions dont 29896 pulses à 1 photon et 708 pulses à deux photons soit un total de (29896 + 708 × 2) = 31312 photons. Le traitement consiste à synchroniser l'horloge de la carte TIA avec les données puis à définir une fenêtre de comptage qui englobe bien l'impulsion à traiter sans toutefois être trop large afin de ne pas introduire trop de coups d'obscurité. Quelques résultats sont rassemblés dans le tableau 3-5-4.

On constate donc un léger écart systématique entre le paramètre de Mandel théorique Q_C (obtenu donc dans le cas d'un statistique de type Poisson) et le paramètre mesuré Q_M. Les impulsions pourraient donc être considérées comme de type très légèrement super-poissonien.

Néanmoins cet écart ne semble pas suffisamment net pour être vraiment retenu et donc même dans le cas d'impulsions laser fortement atténuées la statistique de photons est bien de type poissonien.

Mod.	I (mA)	I/I_{th}	att (dB)	$\bar{n}$	Q_M	Q_C
AO	40	1	80	0,09875	-0,04928	-0,04818
AO	140	3,5	100	0,10466	-0,05286	-0,05098
PE	40	1	80	0,09973	-0,04974	-0,04864
PE	120	3	100	0,09912	-0,05112	-0,04835

Tableau 3-5-4. *Quelques résultats des paramètres de Mandel théoriques Q_C et mesurés Q_M , selon le type de modulation et l'intensité du courant passant dans la diode laser (AO modulation externe, PE modulation par impulsion de courant).*

3.5.5 Conclusion

Une méthode de mesure du bruit d'intensité dans des impulsions laser fortement atténuées a été présentée dans ce chapitre. Les impulsions utilisées contenaient un nombre moyen de 0,1 photon par impulsion. Les mesures sont effectuées directement dans le domaine temporel, évitant de mettre en œuvre une détection homodyne utilisée en général dans le domaine fréquentiel [75]. Les résultats obtenus montrent que la statistique de photons dans des impulsions laser atténuées est très sensiblement de type poissonien. Et ceci est valable pour les deux techniques de production des impulsions, soit la modulation directe du courant dans la diode laser soit un découpage du faisceau par un modulateur acousto-optique. L'atténuation appliquée était de 80 à 100 dB. L'étude a été complétée par des mesures d'excès de bruit du faisceau laser en fonction de l'intensité du courant de polarisation de la diode, il apparaît que pour des courants de polarisation supérieurs à environ 2,8 fois le courant de déclenchement, le bruit d'intensité de la diode laser est limité par le bruit de photon (cf. partie 3-4-3 de ce chapitre).

4 Système de transmission optique

Sommaire

4.1 Télécommunications optiques

Le terme « télécommunications » fut inventé en 1904 par E. Estaunié et signifie « communiquer à distance ». Le but des télécommunications est donc de transmettre un signal, porteur d'une information (voie, musique, images, données…), d'un lieu à un autre lieu situé à distance.

4.1.1 Les éléments d'une liaison à fibre optique

Une liaison par fibre optique est composée essentiellement par les éléments suivants : émetteurs, modulateurs, fibres, répéteurs, amplificateurs, récepteurs (fig. 4-1). Dans une liaison optique de longue distance, nous utilisons des fibres optiques pour transmettre les informations. La fibre optique est un choix évident puisqu'elle fournit de faibles pertes et de grande bande passante. L'atténuation dans la fibre est de 0,2 dB par km à la longueur d'onde 1,55 µm. Par conséquent, les répéteurs ne sont nécessaires que tous les 100 km (la puissance de sortie au bout de 100 km est égale à 1% de celle d'entrée).

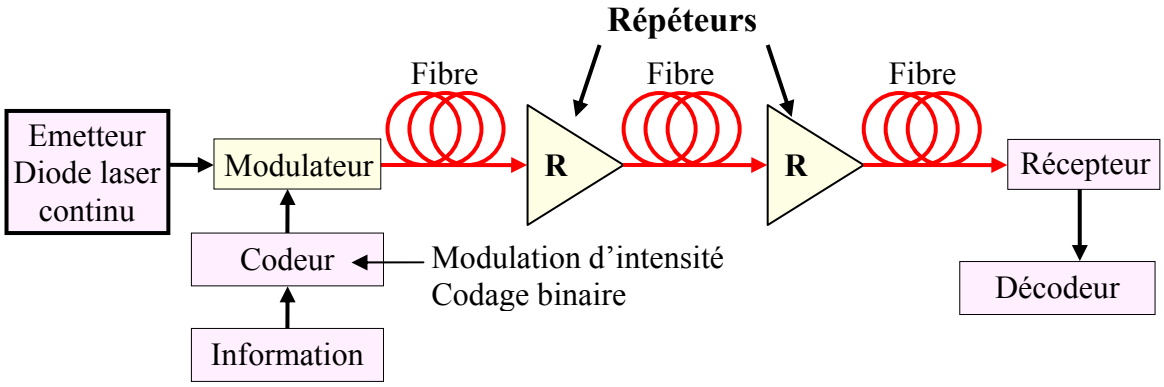


Figure 4-1. Exemple d'un système de transmission sur fibre optique. Il est essentiellement composé par : émetteurs, modulateurs, fibres, répéteurs, amplificateurs, récepteurs.

Depuis 1995, les répéteurs utilisés sont de type répéteur optique comme amplificateurs à fibre dopée à l'erbium (EDFA – Erbium Doped Fiber Amplifier) à 1,5 µm (fig. 4-2), qui remplace les répéteurs optoélectroniques (fig. 4-3). Ces derniers ont une bande passante « limitée » à 500 Mbits/s.

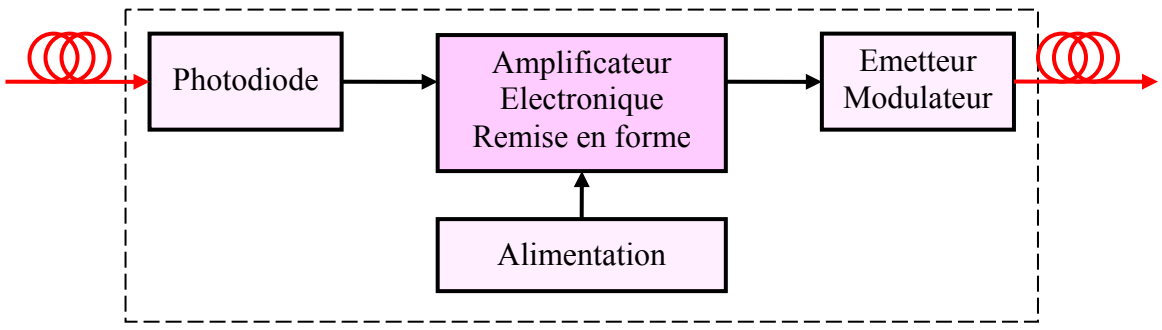


Figure 4-2. Amplificateur optoélectronique

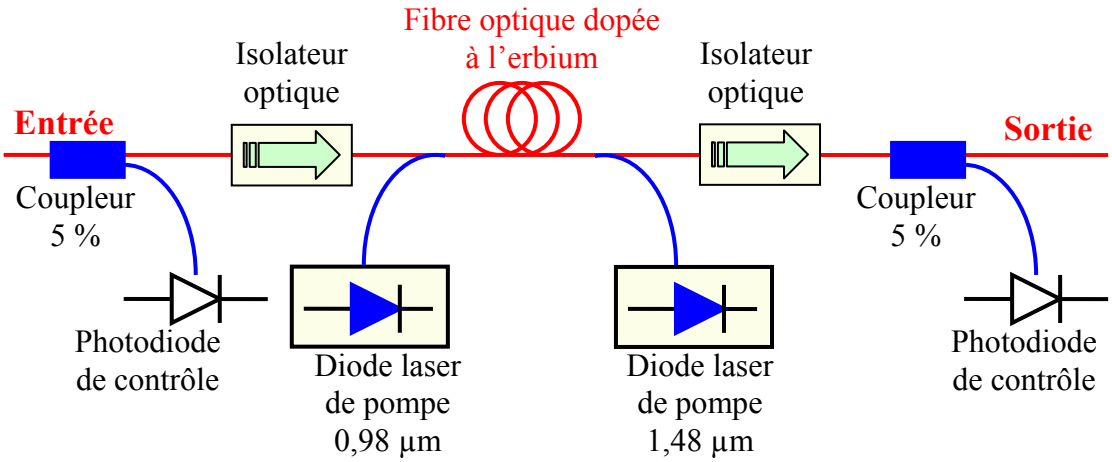


Figure 4-3. Amplificateur à fibre dopée à l'erbium [88].

Dans l'amplificateur tout-optique (fig. 4-3), la bande passante atteint à 40 Gbits/s. On a aussi développé le multiplexage en longueur d'onde (Wavelength Division Multiplexing) sur la bande d'amplification de l'ion erbium dans la matrice de silice (1530-1560 nm) et on arrive à multiplexer jusqu'à 40 voies ce qui correspond à une bande passante 10^{12} bits/s.

4.1.2 Pourquoi les transmissions optiques ?

L'utilisation de l'optique en télécommunication est une transposition naturelle de la transmission Hertzienne à des fréquences nettement plus élevées (de l'ordre de 10^{14} Hz) et moins perturbées : l'information à transmettre module un faisceau lumineux en amplitude (intensité lumineuse), éventuellement en phase ou en fréquence.

a) Intérêts de la transmission par fibres optiques

Ils sont nombreux et plus ou moins décisifs selon l'application.

- Performances de transmission : très faible atténuation (jusqu'à 0,1 dB/km = 0,25% /km), très grande passante (~ 25 Terahertz), multiplexage possible de plusieurs signaux et de plusieurs utilisateurs. Portée et capacité bien supérieure aux câbles.
- Mise en œuvre : faible poids, faible taille (cœur de quelques microns dans une gaine de quelques centaines de microns).
- Sécurité électrique : isolation totale entre terminaux, utilisation possible en ambiance explosive, sous fortes tensions, en applications médicales et électromagnétiques. La fibre n'est pas sensible aux parasites électriques et n'en crée pas.
- Inviolabilité : difficile d'interception d'un signal véhiculé sur une fibre optique.
- Avantage économique : le coût de la transmission optique n'est pas élevé, souvent moins cher que sur cuivre. La mise en œuvre (connexions, raccordements) devient de moins en moins complexe et coûteuse.

b) Domaines d'utilisation

- Télécommunications : liaisons urbaines et interurbaines (grande capacité), liaisons sous-marines sur des tronçons de plus de 200 km sans amplification optique ou répéteurs.

- Câbles sous-marins : exemple entre les USA et l'Europe à 1,28 Tbps. Alcatel est numéro 1 mondial (40 % du réseau 230 000 km au fond des océans).
- Vidéocommunications : nombreuses expériences mais développement ralenti par le coût. La distribution reste en coaxial tandis que les liaisons centrales utilisent la fibre.
- Liaison et réseaux de données : sur de courtes distances, l'insensibilité aux perturbations électromagnétiques, peut être un avantage décisif.
- Liaisons industrielles : ce sont des applications variées (télémesures, télécommandes, surveillance vidéo, bus de terrain) où l'insensibilité de la fibre aux parasites est un avantage essentiel.
- Capteurs et instrumentation : les capteurs utilisent la fibre optique elle-même comme élément sensible servant en même temps de support de transmission.
- Transport de lumière : les applications classiques (éclairage, visualisation, endoscopie) ou plus récentes (transport de faisceaux laser pour l'industrie, la mesure, la médecine) ont vu leurs performances s'améliorer, et leur coût baisser, grâce au développement des technologies des fibres optiques.

4.2 Conception d'un système de transmission d'impulsions optiques

4.2.1 Généralités

Le domaine d'application est celui de la sécurité en cryptographie quantique. Cette dernière exige des sources de photons uniques pour la distribution de clés quantiques. En réalité, comme il n'y a aucune source de photons uniques actuellement commercialisée, on utilise des impulsions laser fortement atténuées au lieu des photons individuels. La détection de tel signal transmis est par conséquent difficile en raison de la puissance très basse du signal ($\propto 10^{-12}$ W, cf. 3.5.2) et également en raison de l'efficacité plutôt basse des photodiodes d'avalanche, particulièrement à 1,55 µm, la longueur d'onde de télécommunication standard. Mais il semble possible de profiter de l'horloge employée pour produire les impulsions avec l'information quantique ; il nous est capable de savoir exactement quand les impulsions atténuées arrivent sur les détecteurs. Ainsi le problème est de choisir une méthode pour envoyer simultanément les deux genres d'information, le signal de clés quantiques et un signal de synchronisation.

La première possibilité pourrait devoir utiliser deux canaux séparés, par exemple une fibre optique pour des clés quantiques et un canal classique de cuivre pour le signal d'horloge, mais dans ce cas les vitesses de propagation sont trop différentes et les signaux n'arriveront pas du tout synchronisés. Une autre solution est d'employer une ou deux fibres transmettant deux longueurs d'onde différentes [29, 76], mais l'effet de dispersion chromatique pourrait affecter la synchronisation des canaux de transmission. Le retard dû à la dispersion chromatique est donné par l'équation suivante :

$$\Delta\tau = \frac{d\tau}{d\lambda_0}\Delta\lambda_0 = -\frac{L}{c}\lambda_0\frac{d^2n}{d\lambda_0^2}\Delta\lambda_0 \qquad (4\text{-}2\text{-}1)$$

A titre d'exemple, dans la silice avec 1,3 µm et 1,55 µm, le retard dû à la dispersion est de 3,2 ns/km, et ainsi pour 100 km de distance le retard sera de 0,32 µs qui est trop grand ! Un générateur de retard pourrait être employé pour la compensation mais seulement pour une expérience de laboratoire [77] ; ce n'est pas une solution industrielle.

4.2.2 Idée générale

Le principe du système est présenté dans la figure 4-4. Deux signaux doivent être transmis simultanément dans une fibre monomode et doivent présenter un effet de dispersion aussi faible que possible.

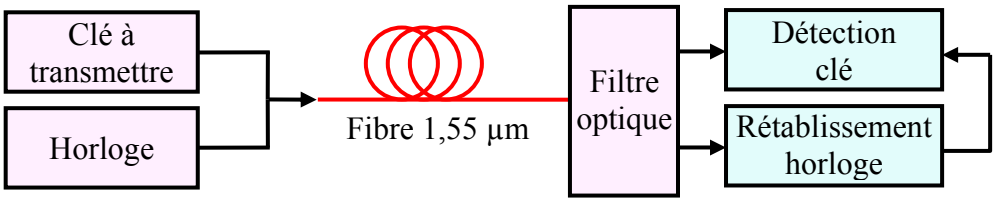


Figure 4-4. Représentation schématique du système de transmission optique. Deux signaux optiques sont mélangés et transmis dans une seule fibre et filtrés dans l'étage de détection.

La solution proposée ici pour obtenir ces deux signaux est basée sur le fait qu'avec un modulateur acousto-optique la longueur d'onde à la sortie du 1er ordre est décalée d'une fréquence $\Delta\nu$ (fréquence RF) par rapport à l'ordre zéro. La variation dans la longueur d'onde est liée à la différence de fréquence selon l'équation :

$$\Delta\lambda = \frac{\lambda^2}{c}\Delta\nu \qquad (4\text{-}2\text{-}2)$$

Ainsi, on aura un écart en longueur d'onde très petit et donc une dispersion très faible. Pour la suite de ces travaux, une partie du faisceau initial est utilisée pour l'envoi de l'horloge de 10 MHz (cf. 4.2.3) et le faisceau de sortie au premier ordre de l'AOM est employé pour l'envoi des clés. Le modulateur acousto-optique choisi pour le système est un AA.MGAS.110 fonctionnant avec une fréquence de RF de 110 mégahertz, conduite par un signal de basse fréquence (quelques mégahertz). Avec une fréquence RF de 110 mégahertz, la différence en longueur d'onde (d'après éq. 4-2-2) entre les faisceaux de sortie à l'ordre zéro et au premier ordre sera 1,3 pm ; alors le retard (d'après éq. 4-2-1) entre les deux signaux sera seulement de 18 fs/km, menant à 1,8 ps pour une distance de 100 km, ce qui est beaucoup plus petit que les 0,32 µs (178 milles fois plus petit), évoqués précédemment.

4.2.3 Description détaillée

Le système complet est présenté sur la figure 4-5. Dans la partie d'émission les deux longueurs d'onde λ_0 correspondant à l'ordre zéro (signal d'horloge) et λ_1 correspondant au premier ordre (clés de cryptage) doivent être modulées à l'aide de deux modulateurs électro-optiques puis injectées dans la même fibre monomode. Cette voie pourra être atténuée jusqu'à un niveau d'intensité très faible (niveau des photons uniques) avant d'entrer dans la fibre. Le premier modulateur est dédié au signal horloge à 10 MHz, le deuxième au signal correspondant à la clé de cryptage que nous avons choisi de coder sur 128 bits dans ce prototype.

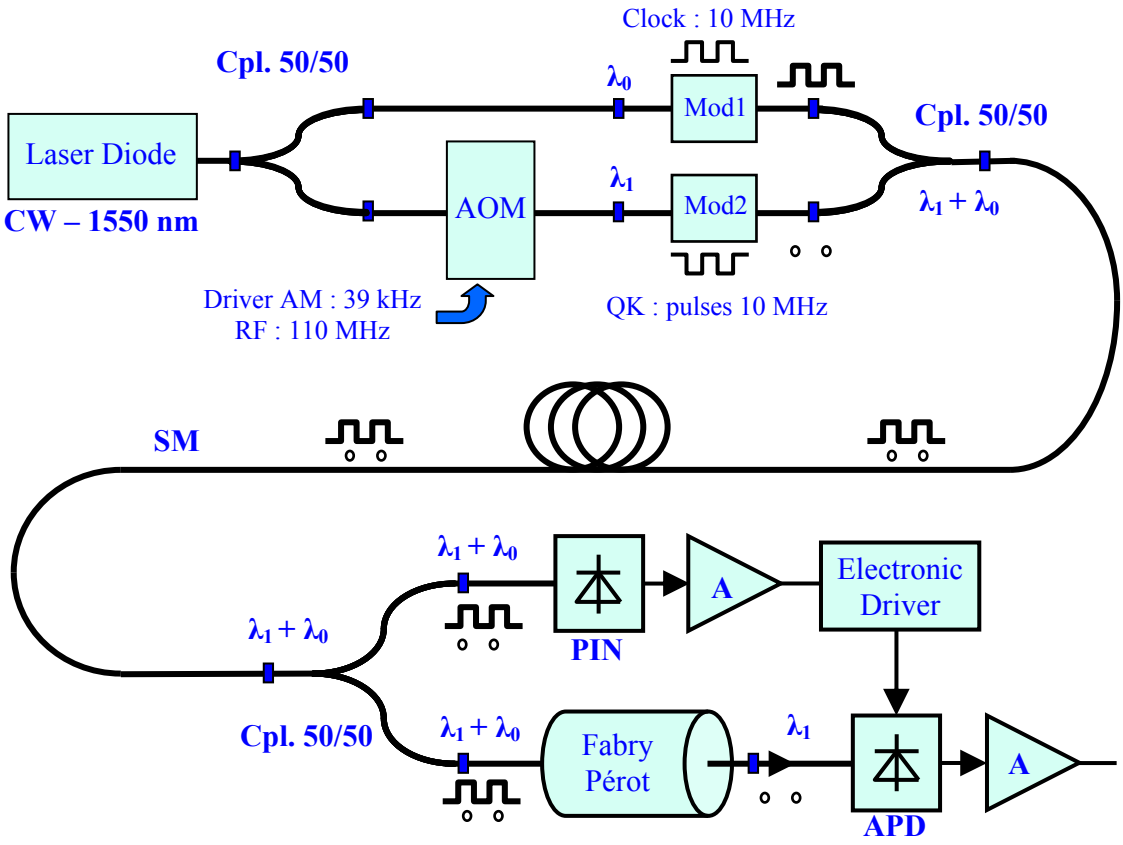


Figure 4-5. Représentation schématique de la transmission optique avec l'AOM : parties émission et réception. Les modulateurs Mod1 et Mod2 sont de type Mach-Zehnder.

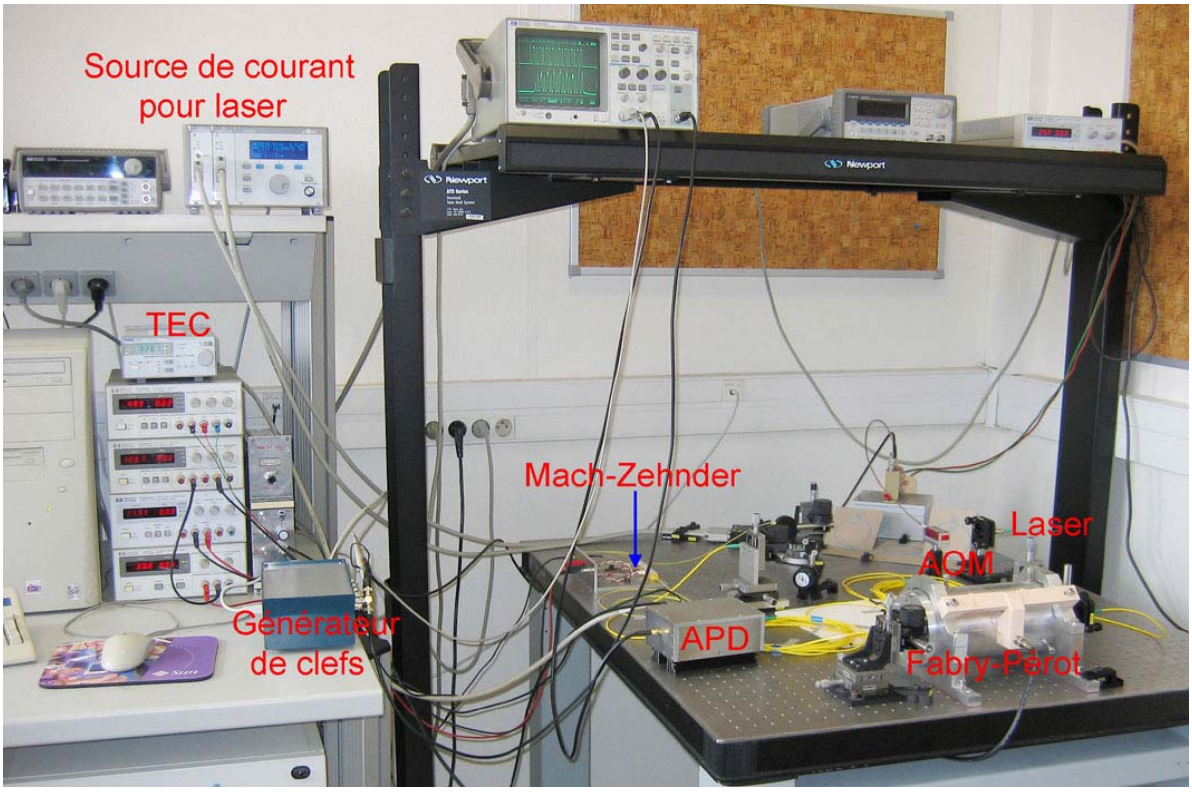


Figure 4-6. Photo du système de transmission optique au laboratoire SATIE – ENS de Cachan.

A la sortie de la fibre le signal doit être séparé dans deux parts. Une voie avec le signal horloge est détectée par une photodiode PIN et donne le signal de synchronisation de 10MHz. La deuxième voie correspond aux impulsions (clés) atténuées et doit être précisément filtré. Pour cela un interféromètre de Fabry-Pérot de très haute résolution a été conçu, à 1,55 µm. Les détecteurs sont des photodiodes PIN et photodiodes à avalanche. On parlera de ces détecteurs en détail dans le chapitre 5. La photo du montage d'élaboration et de filtrage de deux longueurs d'onde est montrée dans la figure 4-6 ci-dessus.

4.3 Modulateur acousto-optique

Dans un modulateur acousto-optique (AOM), un rayon laser interagit avec une onde ultrasonore à haute fréquence à l'intérieur d'une cellule constituée d'un cristal ou milieu d'interaction. En orientant soigneusement le laser, le faisceau peut être réfracté par les fronts d'onde acoustiques (diffraction de Bragg). Par conséquent, quand l'onde ultrasonore est présente le faisceau est dévié et quand elle est absente le faisceau passe sans déviation. En changeant très rapidement l'onde acoustique ON et OFF, le faisceau dévié apparaît et disparaît (modulation numérique). En changeant l'amplitude de l'onde acoustique, l'intensité du faisceau dévié peut être modulée de façon similaire (modulation analogique).

4.3.1 Principe de fonctionnement

Ce modulateur sert à élaborer deux longueurs d'onde très proches par phénomène de diffraction de Bragg dans le cristal. Les ultrasons sont générés par un transducteur, habituellement un wafer mince en niobate de lithium (LiNbO3), qui est collé sur le milieu d'interaction en utilisant un processus de liaison métallique avancé (la soudure froide). Quand un signal électrique à haute fréquence est appliqué au transducteur, il vibre, produisant l'onde acoustique. Le signal est dérivé d'un driver RF, qui génère un signal (modulation d'amplitude) de haute fréquence qui est modulé par une entrée analogique ou numérique.

Nous utilisons un modulateur fabriqué par la société A.A. Opto-électronic (fig. 4-7). Ce dispositif est composé d'un cristal de $Ge_{33}As_{12}Se_{55}$ (verre) sur lequel est collé un transducteur de niobate de lithium $LiNbO_3$. Ce modulateur acousto-optique est piloté par un générateur RF de fréquence de 110 MHz (fig. 4-8), dont l'amplitude peut être réglée proportionnellement à la tension d'entrée qui est appliquée sur l'entrée « input » du boîtier électronique de commande (voir le synoptique du fonctionnement du modulateur qui est représenté très schématiquement sur la figure 4-10). L'AOM peut être utilisé pour changer le faisceau laser "on" et "off" par un signal numérique TTL externe.

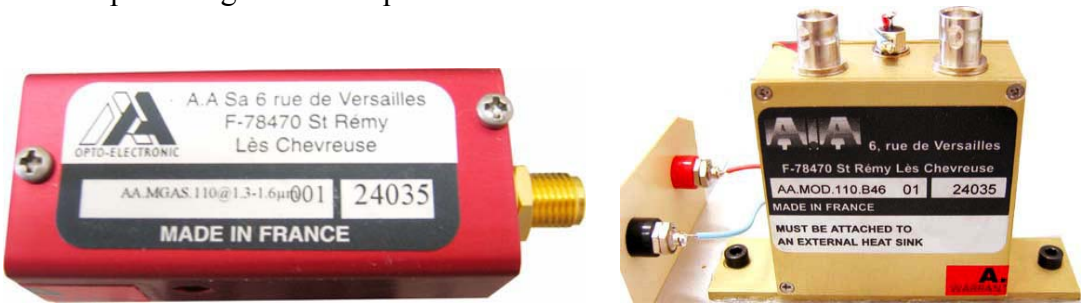


Figure 4-7. Modulateur acousto-optique AA.MGAS.110 (à gauche) et son driver AA.MOD-110.B46, fabriqués par A.A. Opto-électronic, fonctionnant à 1,55 µm avec génération interne de 110 MHz.

L'amplitude d'entrée du driver doit être positive et comprise entre 0 et +5V (signal TTL standard). Il permet de contrôler le driver ON et OFF. En appliquant le niveau « 0 » (inférieur à 0,8 V) à l'entrée « input », on n'a pas de signal de sortie. En appliquant le niveau « 1 » (supérieur à 2 V) à l'entrée « input », on obtient un niveau maximum du signal de sortie. Le signal de sortie $v_s(t)$ du driver est une modulation d'amplitude de forme :

$$v_s(t) = V_p\left[1 + kV_m F(\omega_m, t)\right]\cos(\omega_p t)$$

- V_p et $\omega_p = 2\pi f_p$ sont respectivement l'amplitude et la pulsation de la porteuse générée par le driver. Ici, f_p = 110 MHz, V_p = 5 V (fig. 4-8).
- V_m et $\omega_m = 2\pi f_m$ sont respectivement l'amplitude et la pulsation du signal modulant.
- $kV_m = m$ est l'indice de modulation.

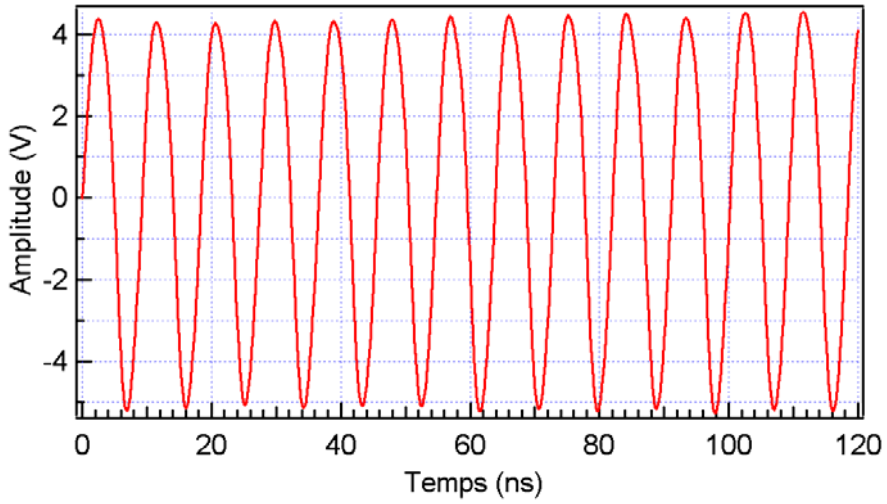


Figure 4-8. Signal sinusoïdal de haute fréquence (110 MHz) généré par le driver AA.MOD-110.B46 du modulateur acousto-optique.

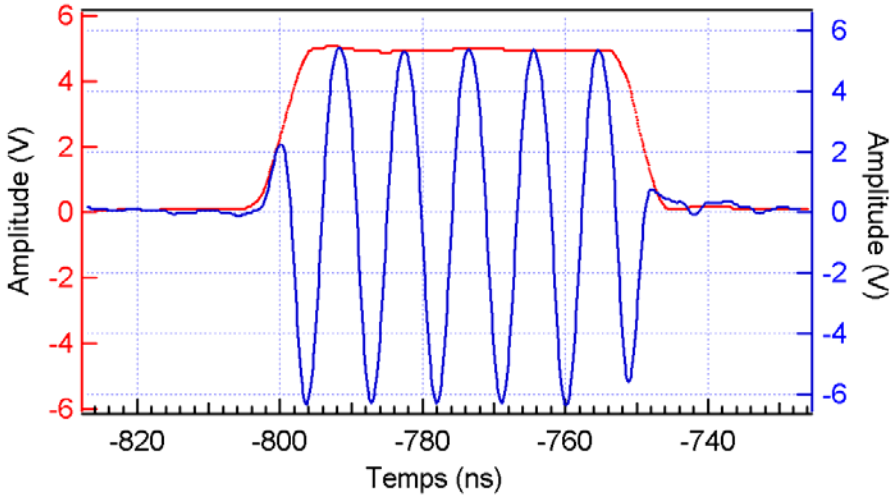


Figure 4-9. Signal de sortie du driver AA.MOD.110.B46. Il est le résultat d'une modulation d'amplitude. Ici, la porteuse de 110 MHz est contenue dans une enveloppe carrée de 10 MHz. Le signal carré a un temps de montée et descente de 5 ns. Dans la manip cette thèse, on utilisera une enveloppe carrée de fréquence de 39,06 kHz (cf. 4.6.3).

En se réfléchissant au fond de la cellule, l'onde ultrasonore forme une onde stationnaire de pression, donc d'indice de réfraction, de période $\Lambda/2$, Λ étant la longueur d'onde acoustique dans le cristal $Ge_{33}As_{12}Se_{55}$ (verre). Sur l'écran d'observation qui se trouve après la cellule, on observe une modulation de l'intensité du faisceau laser, due à la réfraction par les ondes stationnaires de pression dans le cristal. La diffraction de la lumière par une onde ultrasonore est mise à profit dans les modulateurs acousto-optiques. Le schéma de principe du modulateur dont nous disposons est le suivant (d'après la notice d'utilisation) :

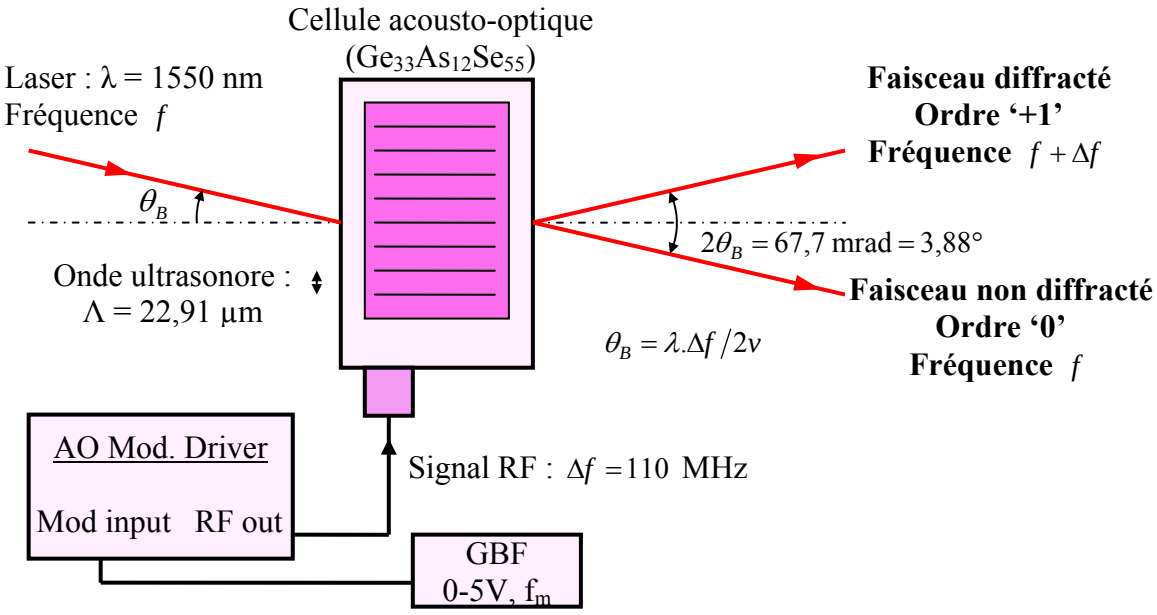


Figure 4-10. Représentation schématique du modulateur acousto-optique de A.A. Opto-electronic.

4.3.2 Propriétés de l'AOM dans le montage

Le générateur haute fréquence génère dans le cristal une onde acoustique de longueur d'onde $\Lambda = v/\Delta f$ où v = 2520 m/s (dans $Ge_{33}As_{12}Se_{55}$) donc Λ = 22,91 µm. Le faisceau laser est diffracté par cette onde ultrasonore. Pour qu'un maximum d'intensité soit diffracté dans l'ordre '1', on doit orienter la cellule pour avoir un angle d'incidence égal à l'angle de Bragg : $\theta_B = \lambda/2\Lambda$ = 33,8 mrad = 1,94°. Par conséquent, les deux faisceaux laser les plus lumineux (ordres '0' et '1') sont dévié d'un angle $2\theta_B = \lambda/\Lambda$ = 67,7 mrad = 3,88°.

Mesure de θ_B :

θ_B est l'angle d'incidence (entre le faisceau incident et l'onde acoustique) particulier qui rend la diffraction efficace en un seul ordre de diffraction. Cet angle dépend de la longueur d'onde et la fréquence RF (radio frequency). Régler l'orientation de la cellule de façon à avoir un maximum d'intensité dans l'ordre '1' (utiliser une photodiode pour plus de précision). A une distance de 31 ± 0,1 cm de la cellule, la séparation des deux faisceaux principaux (ordres '0' et '1') est de 2,1 ± 0,1 cm. On mesure donc un angle $2\theta_B \approx$ 2,1/3
1 = 67,7 mrad = 3,881°.

Modulation : L'amplitude de l'onde ultrasonore peut être modulée par un générateur externe (GBF 0-5V) de basse fréquence.
Dans l'expérience, seulement deux ordres '0' et '1' sont utilisés.

Sortie à l'ordre zéro : fréquence *f* correspondant au faisceau directement transmis.
Sortie au premier ordre : fréquence $f + \Delta f$ (ordre +1) ou fréquence $f - \Delta f$ (ordre -1) correspond au faisceau diffracté.

Le faisceau directement transmis a une fréquence optique f qui est identique à celle du faisceau incident. Au contraire, le faisceau diffracté à l'ordre '+1' (ou '-1') a une fréquence optique qui est la somme (ou la différence) de la fréquence optique du faisceau incident et la fréquence du son ultrasonore, à savoir $f + \Delta f$ ou $f - \Delta f$. L'idée principale est que l'on transmet à la fois les clés (quantiques) et le signal de synchronisation en utilisant ces deux faisceaux. Le faisceau dévié (1er ordre) est employé dans pour les clés ; son intensité peut être réglée de zéro à plus de 80% du rayon incident. Le principe de fonctionnement est très bien présenté dans l'ouvrage de Jia-Ming LIU [118].

4.3.3 Caractéristiques du modulateur et de son driver

Caractéristiques du modulateur utilisé :

- AA.MGAS.110, 1,3 – 1,6 µm.
- Fréquence de pilotage : 110 MHz.
- Temps de montée : $t_r =$ 262 ns/mm diamètre du faisceau ($t_r = 0{,}66\ D/v$)
- Fréquence de modulation : $f_m = 0{,}35/t_r = 1{,}3$ MHz.
- Matériel : $Ge_{33}As_{12}Se_{55}$ (verre).
- Transmission optique : 95%, efficacité au premier ordre : < 80%
- Refroidissement : non.
- Angle de séparation en 0 et 1er ordre : 3,88° à 1550 nm. (l'ordre zéro est le faisceau directement transmis à travers la cellule. Le premier ordre est le faisceau de diffraction généré quand le faisceau laser interagit avec l'onde acoustique).

Caractéristiques du driver :

- AA.MOD.110.B46.
- Fréquence interne : 110 MHz.
- Temps de montée/descente : < 8 ns.
- Alimentation : 24 V_{DC}
- Entrée modulation : 0 V – 5 V / 50 Ω.

On s'aperçoit que si le faisceau du laser utilisé a un diamètre de *d* (unité mm) alors le cristal doit mettre un temps de 262 ns x *d* pour établir son état de fonctionnement correct. Le cristal a donc une bande passante de l'ordre de quelques MHz avec un faisceau laser de *d* = 1 mm. Le paramètre important dans notre montage est celui de fréquence de modulation. Par une mesure rapide avec un modulateur acousto-optique, un générateur de signal et un détecteur d'intensité optique, on peut vérifier la réponse fréquentielle de ce modulateur (voir la figure 4-11).

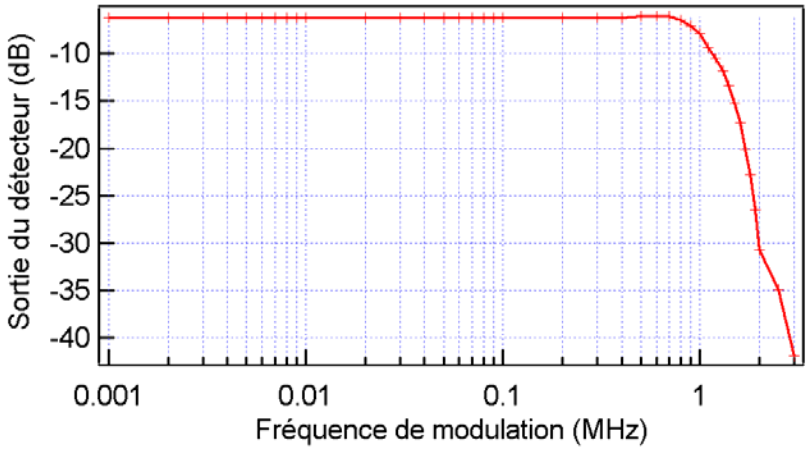


Figure 4-11. La réponse en fréquence de modulation du cristal de l'AOM. La fréquence de coupure à -3dB est de 1,1 MHz. Cette bande passante satisfait largement au système car une modulation en créneau de 39,06 kHz sera appliquée à l'AOM pour la suite de notre montage.

4.4 Filtre de haute résolution Fabry-Pérot

Ce type de filtre joue un rôle très important dans notre expérience ; il assure la séparation de deux longueurs d'onde proches. Nous en parlerons en détail dans cette partie.

4.4.1 Interféromètre Fabry-Pérot confocal

Le filtre (souvent appelé interféromètre) Fabry-Pérot utilisé est une cavité confocale qui se compose de deux miroirs sphériques de rayon de courbure $\Re = L = 20\,\text{cm}$ et de coefficient de réflexion R_1 et R_2 (deux miroirs identiques, $R_1 = R_2 = R$) séparés d'une distance L qui est égale au rayon des miroirs et contenant un milieu d'indice $n_{air} = 1$. Ce type de Fabry-Pérot présente la propriété particulière suivante : tout rayon parallèle à l'axe se reboucle sur lui-même après un trajet en « 8 » de longueur $4L$ (fig. 4-12).

4.4.2 Propriétés de la cavité confocale

a) Interférences à ondes multiples

Supposons que E_0 soit l'amplitude de l'onde incidente sur l'interféromètre, t soit coefficient de transmission en champ électrique de deux miroirs et, r soit respectivement coefficient de réflexion en champ électrique correspondante.

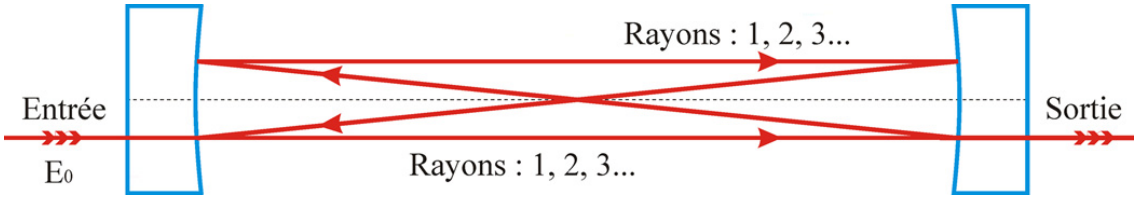


Figure 4-12. Représentation du Fabry-Pérot composé de deux miroirs sphériques dans la configuration confocale. La distance entre deux miroirs est égale au rayon des miroirs (ici 20 cm). Tout rayon parallèle à l'axe se reboucle sur lui-même après un trajet en « 8 ».

En construisant ce tableau ci-dessous

Rayon	1	2	3	…	N
Transmission	t^2	t^2	t^2	t^2	t^2
Réflexion	r^4	r^8	r^{12}	…	r^{4N}

nous pouvons établir l'amplitude totale transmise E_T par la formule :

$$E_T = \sum_{N=0}^{\infty} E_N = E_0 \left|t^2\right| \sum_{N=0}^{\infty} r^{4N} \exp(iN\varphi) \tag{4-4-1}$$

où $\varphi = \frac{2\pi}{\lambda} 4L\cos\theta$ est le décalage de phase pour un tour complet de la lumière, qui inclut aussi n'importe quel décalage de phase à cause de passage à travers les deux miroirs.
On se souvient qu'en absence d'absorption, avec $R = |r|^2$ et $T = |t|^2$: $T + R = 1$. D'où :

$$E_T = E_0 T \sum_{N=0}^{\infty} R^{2N} \exp(iN\varphi) = E_0 T \frac{1}{1 - R^2 e^{i\varphi}} \tag{4-4-2}$$

(on a utilisé la formule déjà démontrée : $\sum_{N=0}^{\infty} R^N \exp(iN\varphi) = \frac{1}{1 - \mathrm{Re}^{i\varphi}}$)

Alors, l'éclairement (intensité) s'écrit (en s'exprimant $|E_0|^2 = I_0$) :

$$I \propto |E_T|^2 = I_0 T^2 \frac{1}{\left(1 - R^2 e^{i\varphi}\right)\left(1 - R^2 e^{-i\varphi}\right)} = \frac{I_0 (1-R)^2}{1 - 2R^2 \cos\varphi + R^4} \tag{4-4-3}$$

dont le dénominateur peut s'écrire :

$$1 - 2R^2 \cos\varphi + R^4 = \left(1 - R^2\right)^2 + 2R^2 (1 - \cos\varphi) = \left(1 - R^2\right)^2 + 4R^2 \sin^2 \frac{\varphi}{2} \tag{4-4-4}$$

Ainsi

$$I = I_0 \frac{(1-R)^2}{\left(1 - R^2\right)^2 + 4R^2 \sin^2 \frac{\varphi}{2}} \tag{4-4-5}$$

L'équation (4-4-5) correspond à la fonction d'Airy.

Alors,

- L'intensité I_M maximale correspond à $\sin \frac{\varphi_M}{2} = 0$ d'où $\varphi_M = 2p\pi$, $p \in N$ et

$$I_M = I_0 \frac{1}{(1+R)^2} \tag{4-4-6}$$

- L'intensité I_m minimale correspond à $\sin^2 \frac{\varphi_M}{2} = 1$ et alors

$$I_m = I_0 \left(\frac{1-R}{1+R^2} \right)^2 \tag{4-4-7}$$

La largeur $\Delta\varphi$ à mi-hauteur est telle que $I = \frac{I_M}{2}$, donc pour $\varphi_L = \varphi_M + \Delta\varphi/2$ on a :

$$\frac{(1-R)^2}{(1-R^2)^2 + 4R^2 \sin^2 \frac{\varphi_L}{2}} = \frac{1}{2(1+R)^2} \tag{4-4-8}$$

d'où $$\sin^2 \frac{\varphi_L}{2} = \left(\frac{1-R^2}{2R} \right)^2 \tag{4-4-9}$$

La fonction étant périodique, pour $p = 0$, $\varphi_L = \Delta\varphi/2$ et $\sin \frac{\Delta\varphi}{4} = \left(\frac{1-R^2}{2R} \right) << 1$

d'où la largeur à mi-hauteur d'un pic de transmission :

$$\Delta\varphi \approx 2 \frac{1-R^2}{R} \tag{4-4-10}$$

b) Finesse du Fabry-Pérot

On définit la finesse comme le rapport de l'intervalle entre les pics et la largeur d'un pic :

$$F = \frac{\text{période}}{\text{largeur}} = \frac{2\pi}{\Delta\varphi} = \frac{\pi R}{1-R^2} \tag{4-4-11}$$

Application numérique :

Nous disposons de deux miroirs identiques ayant le coefficient de réflexion $R = 0{,}99$. Alors, la finesse vaut 156.

En présence d'absorption *A*, on a $R + T + A = 1$ et

$$I = I_0 (1-R-A)^2 \frac{1}{(1-R^2)^2 + 4R^2 \sin^2 \frac{\varphi}{2}} \tag{4-4-12}$$

Tout se passe comme si I_0 était plus faible mais les variations relatives (ex. le contraste $C = \frac{I_M - I_m}{I_M + I_m}$) ne sont pas affectées et on a toujours même finesse : $F = \frac{\pi R}{1 - R^2}$.

c) Résolution d'analyse spectrale

Lorsqu'on fait varier l'épaisseur (longueur de la cavité) du FP en incidence normale, la différence de marche $\delta = 4L$ varie et on observe un maximum lorsque :

$$\delta = 4L = p\lambda \ ; \ p \in N \tag{4-4-13}$$

On rappelle que pour qu'une onde monochromatique de fréquence ν résonne dans la cavité confocale, il faut avoir : $\nu = p\frac{c}{4L}$; $p \in N$ et c est la célérité de la lumière dans le vide. La quantité $\Delta\nu_{ISL} = \frac{c}{4L}$ est appelée intervalle spectral libre (ISL) du Fabry-Pérot confocal.

On peut montrer qu'un rayon lumineux quelconque dans la cavité se superpose à lui-même après deux réflexions sur chaque miroir. Il a parcouru alors $4L$. La condition de résonance de la cavité (on parle aussi de condition d'accord de phase) s'écrit dans ces conditions : $4L = p\lambda$.

On fait varier la longueur de la cavité en appliquant une tension à un cristal piézo-électrique. Ces variations sont très faibles et l'on note :

$$L = L_0 + \Delta L \,, \ \Delta L << L \tag{4-4-14}$$

La condition de résonance n'est alors plus vérifiée pour la même longueur d'onde ou pour la même valeur de l'ordre d'interférence p. En plaçant un photodétecteur en sortie du FP, on reçoit un signal pour les différentes longueurs d'onde (à un ordre p donné) ou les différents ordres (à un λ donné) qui satisfont à la condition de résonance. Supposons que la condition de résonance soit vérifiée pour la distance L_0 et la longueur d'onde λ_1. On a

$$4\left(L_0 + \Delta L_1\right) = p\lambda_1 \tag{4-4-15}$$

Pour l'ordre d'interférence suivant, on doit avoir une variation ΔL de la longueur de la cavité telle que

$$4\left(L_0 + \Delta L_1 + \Delta L\right) = \left(p+1\right)\lambda_1 \tag{4-4-16}$$

soit

$$\Delta L = \frac{\lambda_1}{4} \tag{4-4-17}$$

En revenant à l'ordre p, on a une résonance pour une longueur d'onde λ_2 si

$$4\left(L_0 + \Delta L_2\right) = p\lambda_2 \tag{4-4-18}$$

soit

$$\Delta L_1 - \Delta L_2 = \frac{p}{4}\left(\lambda_1 - \lambda_2\right) \tag{4-4-19}$$

On travaille ici avec les fréquences. Les deux équations précédentes s'écrivent

$$\Delta L = \frac{c}{4\nu_1} \text{ et } \Delta L_1 - \Delta L_2 = \frac{pc}{4}\left(\frac{1}{\nu_1} - \frac{1}{\nu_2}\right) \tag{4-4-20}$$

Ces deux quantités sont celles que l'on peut mesurer. En revanche, on ne connaît pas *p*. Mais il est légitime de le supposer grand. En effet, dans la condition (4-4-13), si on prend *L* = 20 cm et $\lambda_1 = 1{,}55$ µm alors $p \approx$ 516 000. On a alors $p \approx \frac{4L}{\lambda_1}$. De plus, dans ce travail on utilise les deux fréquences optiques très proches. Les deux équations (4-4-20) s'écrivent donc en introduisant $\nu = \left(\nu_1 + \nu_2\right)/2$ la fréquence autour de laquelle on travaille :

$$\Delta L = \frac{c}{4\nu} \text{ et } \Delta L_1 - \Delta L_2 = \frac{L}{\nu}\left(\nu_1 - \nu_2\right) \tag{4-4-21}$$

Soit au final :

$$\frac{\Delta L_1 - \Delta L_2}{\Delta L} = \frac{\left(\nu_1 - \nu_2\right)}{c/4L} = \frac{\left(\nu_1 - \nu_2\right)}{\Delta\nu_{ISL}} \tag{4-4-22}$$

On peut donc déterminer l'écart de fréquence entre deux modes du laser par une simple règle de trois en mesurant à l'écran de l'oscilloscope la distance entre ces deux modes et la distance entre deux pics analogues correspondant au même mode mais à deux ordres d'interférence successifs. Les écarts de distance sont proportionnels au temps car on applique une rampe de tension sur le cristal piézo-électrique.

Application numérique :

- L'intervalle spectral libre (ISL) ou en anglais Free Spectral Range (FSR) $\Delta\nu_{ISL}$ est une propriété importante du FP et ne dépend que *L*. Pour le modèle de FP dont on dispose, on a *L* = 20 cm, c = 3.10^8 m/s, ce qui donne $\Delta\nu_{ISL} = \frac{c}{4L}$ = 375 MHz.

- La résolution théorique est de $\Delta\nu_{ISL}/F$ = 375 MHz / 156 = 2,4 MHz. En réalité, en tenant compte des erreurs du coefficient de réflexion des miroirs, le réglage imparfait du montage, etc., la résolution expérimentalement obtenue est de l'ordre de 5 MHz.

d) Technique de balayage de longueur d'onde

Le choix de la longueur d'onde consiste, d'après (4-4-15), à modifier la longueur de la cavité. Ce fait est réalisé en faisant déplacer un miroir de l'interféromètre à l'aide d'une céramique piézoélectrique. Les caractéristiques de ce composant sont données ci-dessous.

Piézoélectrique céramique, type P1 91, de la société Saint-Gobain Quartz :

- Cylindre creux, élongation longitudinale
- Hauteur L = 22 mm
- Diamètre intérieur Φ_{int} = 18 mm
- Diamètre extérieur Φ_{ext} = 22 mm
- Electrode + : à l'intérieur

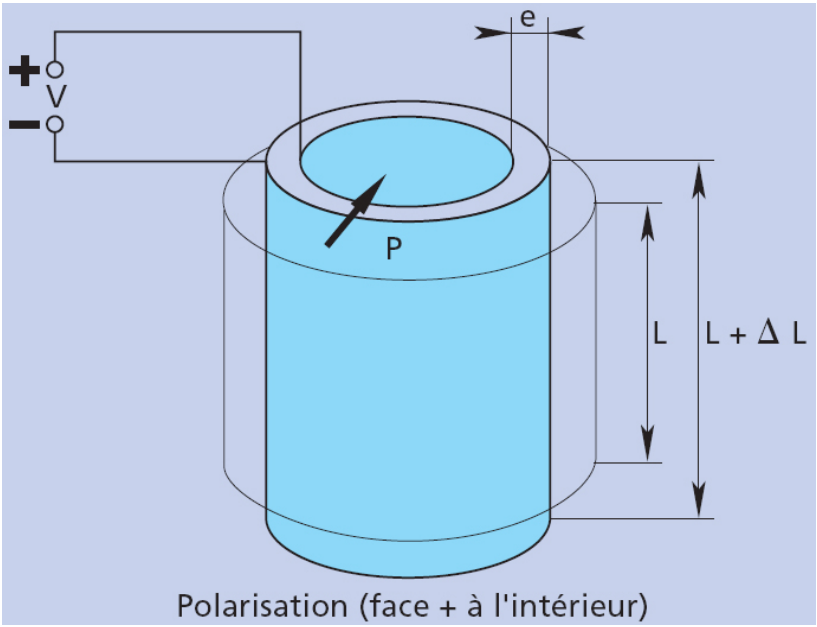


Figure 4-13. Représentation schématique de la céramique piézoélectrique P1 91. Elle est un cylindre creux d'élongation longitudinale. Son électrode « + » est à l'intérieur.

En présence de la polarisation V, la céramique piézoélectrique se déforme longitudinalement. Sa déformation ΔL respecte la relation :

$$d_{31} = \frac{\Delta L / L}{V / e} \text{ soit } \Delta L = d_{31} V \frac{L}{e} \qquad (4\text{-}4\text{-}23)$$

où d_{31} est la constante piézoélectrique (coefficient) de charge.

En appliquant (4-4-17), pour balayer d'un ISL, la tension appliquée V doit satisfaire :

$$\Delta L = d_{31} V \frac{L}{e} = \frac{\lambda}{4} \text{ soit } V = \frac{e\lambda}{4 d_{31} L} \qquad (4\text{-}4\text{-}24)$$

Notons que comme $d_{31} < 0$ et $V > 0$ alors nous avons $\Delta L < 0$. On en déduit, en supposant que V_1 correspond à L_1 et V_0 correspond à L_0 (voir aussi fig. 4-25) :

$$\text{Quand } V_1 > V_0 \text{ alors } L_1 < L_0 \text{ et } \lambda_1 < \lambda_0 \qquad (4\text{-}4\text{-}25)$$

Application numérique :

λ = 1550 nm, L = 22 mm, e = 2 mm, d_{31} = -247.10^{-12} m/V [Saint Gobain Quartz].
Alors, l'expression 4-4-24 nous donne V = 143 volts, ce qui correspond à un déplacement de $\frac{\lambda}{4}$ = 387,5 nm.

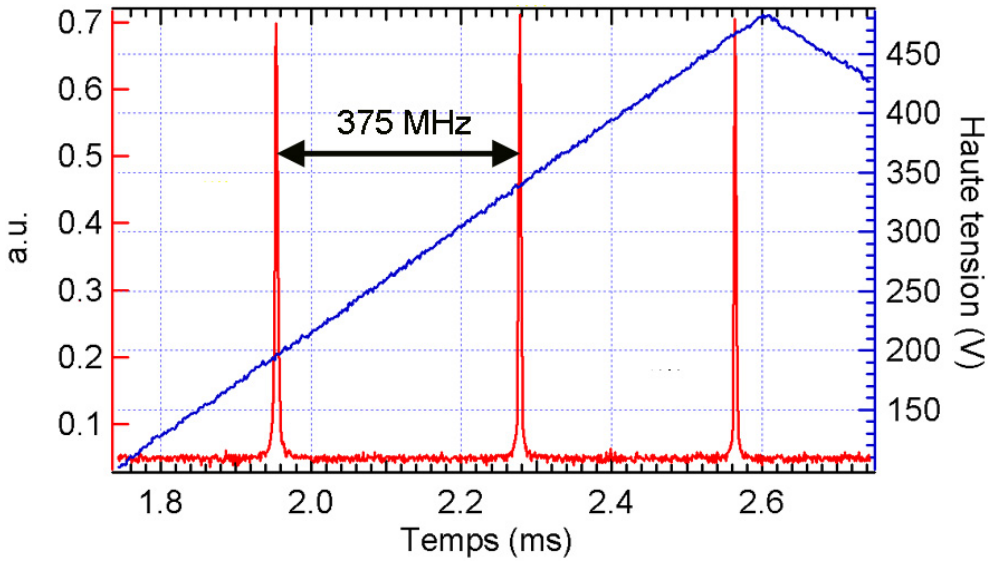


Figure 4-14. Transmission à travers le Fabry-Pérot confocal avec le coefficient de réflexion des miroirs = 99%. Les trois pics (courbe rouge) représentent les modes de résonance suivant une commande par signal triangulaire. La distance entre les pics successifs correspond à l'intervalle spectral libre de la cavité, qui vaut 375 MHz.

4.4.3 Structure de la cavité

La figure 4-15 représente le dessin de la cavité de Fabry-Pérot. Elle est composée des parties suivantes :

	Nomenclature	**Matière**
1	Entretoises	Invar
2	Supports supérieurs des miroirs	Inox 304L
3	Tiges	Invar
4	Joints toriques pour les supports	
5	Miroirs concaves (r = 200 ; R = 0,99)	BK7
6	Joints toriques pour les miroirs	Nitrile
7	Couvercle de bonnette (côté piézo)	Aluminium
8	Bonnette de miroir (côté piézo)	Aluminium
9	Support du piézo-électrique	Inox 304L
10	Support inférieur du miroir	Inox 304L
11	Cale piézo-électrique	Céramique
12	Vis de réglage (M6, pas 0,5)	Bronze

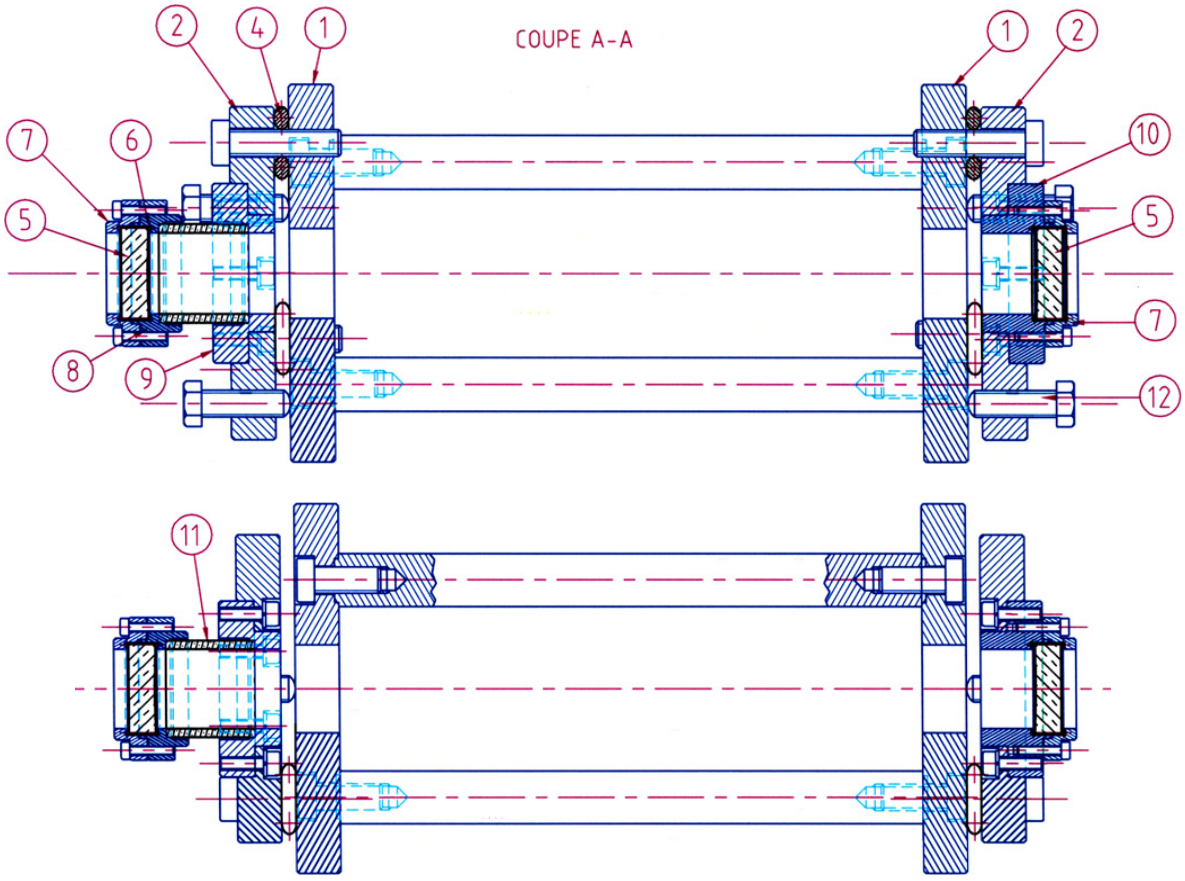


Figure 4-15. Structure de la cavité de l'interféromètre de Fabry-Pérot confocal. Ce dessin a été réalisé par Nguyen Chi Thành du LPQM – ENS de Cachan.

Le montage de l'ensemble de l'interféromètre est montré dans les figures 4-16 et 4-17 ci-dessous. La distance entre deux miroirs (longueur de la cavité) est de 20 cm et pourra être réglée par les vis de réglage (12).

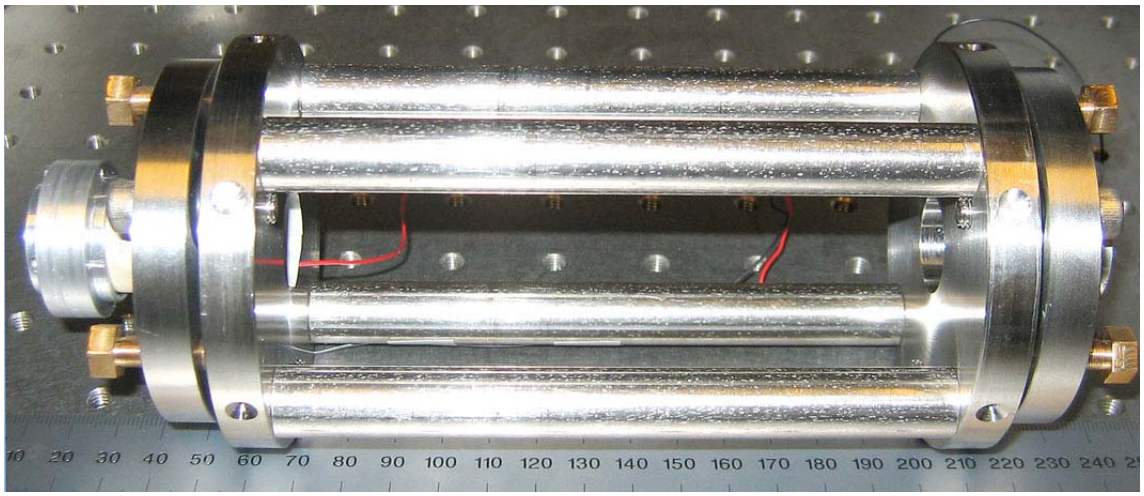


Figure 4-16. Photo de la cavité confocale Fabry-Pérot. Le miroir mobile se trouve à gauche sur une céramique piézoélectrique. Les vis en laiton (6 vis chaque côté) régleront la position et l'orientation des miroirs. Cette cavité sera montée horizontalement sur un support adapté.

Figure 4-17. Réalisation d'un interféromètre Fabry-Pérot.

4.4.4 Montage et réglage

Le réglage du FP consiste à rendre :

- Les axes optiques des deux miroirs coïncidents ;
- La distance entre deux miroirs égale au rayon des miroirs.

Premièrement, nous disposons d'un laser He-Ne de bonne qualité qui puisse nous donner les interférences à travers le FP, c'est-à-dire la longueur de cohérence de la source est assurée supérieure à la différence de marche des rayons d'interférences. Le montage dans les figures 4-18 et 4-19 est très utile pour l'alignement du FP confocal.

Il se réalise comme suivant :

- Coupler le laser He-Ne dans une fibre (connecteur fibre FC/APC).
- Avec un objectif microscope, créer un faisceau presque parallèle, de diamètre de 4 mm, parallèle au sol.
- Les miroirs plans M1 et M2 servent à régler le faisceau dans le plan XY perpendiculaire à l'axe optique.
- Disposer d'un écran d'observation et d'un détecteur infrarouge très sensible.

On injecte du côté d'entrée le laser HeNe (lumière rouge) et centre ce faisceau aux sommets de deux miroirs du FP. En rajustant les vis en laiton (fig. 4-17) on obtiendra une figure d'interférences composée d'anneaux concentriques sur un écran d'observation qui se trouve juste après le FP.

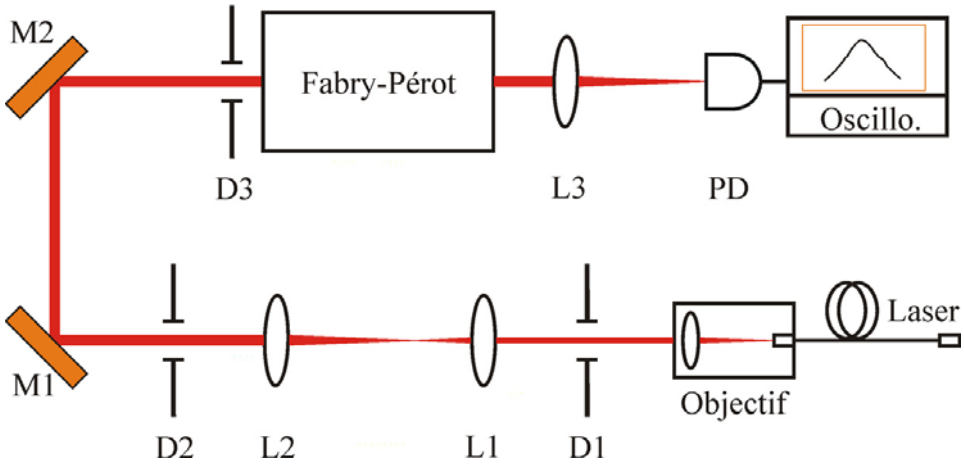


Figure 4-18. Schéma du montage d'alignement pour le FP. L : lentille convergente ; M : miroir ; D : diaphragme ; PD : photodiode et son amplification adaptée. M1 et M2 aident à orienter le faisceau dans deux sens vertical et horizontal. L1 et L2 forment un télescope de Galilée inverse qui sert à élargir le faisceau si nécessaire.

Le faisceau incident est divisé en une multitude de faisceaux secondaires de faibles amplitudes grâce à la réflectivité partielle des miroirs. Lorsque la configuration confocale se présente, les faisceaux rebouclent sur eux-mêmes après un aller-retour complet dans la cavité. Leurs amplitudes s'ajoutent entre elles et interfèrent. Le très grand intérêt du FP tient à sa finesse de résolution spectrale. Cela signifie que le FP fonctionne comme un filtre qui ne laisse passer que certaines longueurs d'onde provenant de la source de lumière, suivant la distance séparant les miroirs.

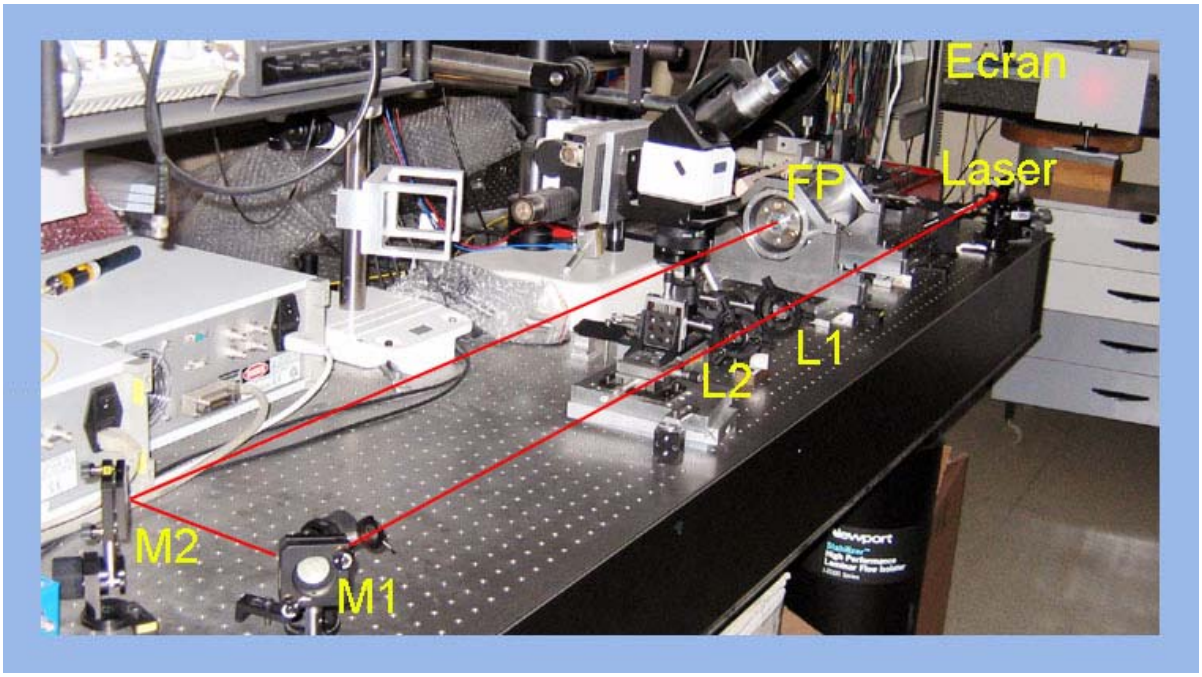


Figure 4-19. Photo du montage d'alignement pour le FP au laboratoire LPQM-ENS de Cachan. Laser, L1, L2, M1, M2, FP (cavité Fabry-Pérot) correspondent aux composants dans la figure 4-18.

Pour une distance donnée entre les miroirs, on obtient des pics de transmission régulièrement espacés en longueur d'onde. Chaque pic a une largeur qui est inversement proportionnelle à cette distance. Le rapport de la distance entre chaque pic à cette largeur est d'autant plus grand que la réflectivité des miroirs est grande. Donc plus la distance entre chaque pic est grande, plus le filtre sélectionne une bande spectrale fine, et donc meilleure est la sélectivité. En faisant varier la distance entre les miroirs, on ajuste le filtre à la longueur d'onde souhaitée.

4.5 Signal optique

4.5.1 Dispersion chromatique

Lorsque l'on envoie un signal lumineux, il y a plusieurs longueurs d'onde présentes, soit parce que la source est étendue, soit parce que la source présente en réalité un pic centré sur *l*. Par exemple, une LED (light emitting diode), a un pic d'une largeur de 10 nm ; le spectre de la diode laser FLD5F6CX a une largeur de 0,2 nm.

Quand une impulsion temporelle se propage dans un milieu homogène, elle se déplace avec une vitesse de groupe v_g donnée par l'équation :

$$v_g = \frac{1}{dk/d\omega} \text{ où } k(\omega) = \frac{\omega}{c} n(\omega) \tag{4-5-1}$$

$k(\omega)$ représente la constante de propagation et $n(\omega)$ représente l'indice de réfraction dépendant de la fréquence. Ainsi,

$$\frac{1}{v_g} = \frac{dk}{d\omega} = \frac{d}{d\omega}\left[\frac{\omega}{c} n(\omega)\right] = \frac{1}{c}\left[n(\omega) + \omega \frac{dn}{d\omega}\right] \tag{4-5-2}$$

Si nous posons $\lambda_0 = \frac{2\pi c}{\omega}$, alors $\omega \frac{dn}{d\omega} = \frac{2\pi c}{\lambda_0}\left[\frac{dn}{d\lambda_0}\left(-\frac{2\pi c}{\omega^2}\right)\right] = -\lambda_0 \frac{dn}{d\lambda_0}$.

Par conséquent, on écrit :

$$\frac{1}{v_g} = \frac{1}{c}\left[n(\lambda_0) - \lambda_0 \frac{dn}{d\lambda_0}\right] \tag{4-5-3}$$

Note : l'énergie se déplace avec la vitesse de l'enveloppe et ça signifie que v_g est la vitesse de propagation de l'énergie.

Le temps nécessaire pour qu'une impulsion transverse la longueur L de la fibre s'exprime par :

$$\tau = \tau(\lambda_0) = \frac{L}{v_g} = \frac{L}{c}\left[n(\lambda_0) - \lambda_0 \frac{dn}{d\lambda_0}\right] \tag{4-5-4}$$

qui est dépendant de la longueur d'onde λ_0. La quantité $N(\lambda_0) = n(\lambda_0) - \lambda_0\, dn/d\lambda_0$ est appelée l'indice de groupe. Si la source considérée est caractérisée par une largeur spectrale $\Delta\lambda_0$ alors chaque longueur d'onde composante se propagera avec une différente vitesse de groupe. Ceci résulte l'étalement temporel de l'impulsion. Cet étalement est donné par

$$\Delta\tau = \frac{d\tau}{d\lambda_0}\Delta\lambda_0 = -\frac{L}{c}\lambda_0\frac{d^2n}{d\lambda_0^2}\Delta\lambda_0 \qquad (4\text{-}5\text{-}5)$$

ou encore

$$\Delta\tau = -\frac{L}{c}\left(\lambda_0^2\frac{d^2n}{d\lambda_0^2}\right)\left(\frac{\Delta\lambda_0}{\lambda_0}\right) \qquad (4\text{-}5\text{-}6)$$

La quantité $\left(\lambda_0^2.d^2n/d\lambda_0^2\right)$ est sans dimension. L'étalement ci-dessus est appelé dispersion du matériau ou dispersion chromatique et se produit quand une impulsion traverse tout milieu dispersif. Comme la dispersion chromatique D_m est proportionnelle à la largeur spectrale $\Delta\lambda_0$ et aussi à la longueur L du milieu, elle est exprimée en unité de picosecondes par kilomètre (longueur de la fibre) par nanomètre (largeur spectrale de la source). On a :

$$D_m = \frac{\Delta\tau}{L\Delta\lambda_0} = -\frac{1}{\lambda_0 c}\left(\lambda_0^2\frac{d^2n}{d\lambda_0^2}\right)\times 10^{12}\ \text{(ps.km}^{-1}\text{.nm}^{-1}\text{)} \qquad (4\text{-}5\text{-}7)$$

où λ_0 est mesurée en micromètre et $c = 3\times10^8$ (m/s).

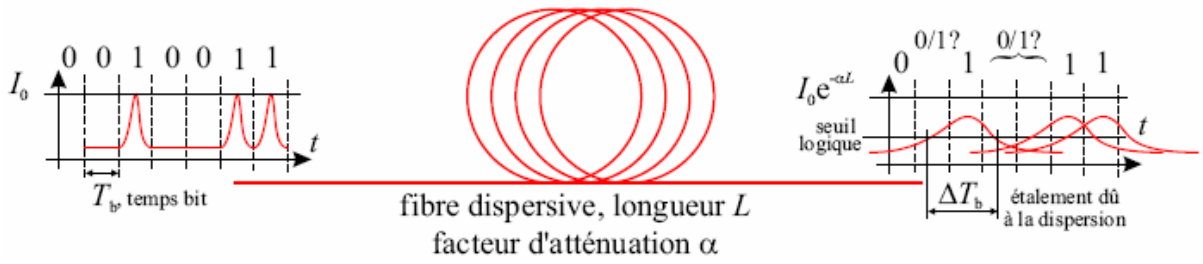


Figure 4-20. Principale conséquence de la dispersion sur les transmissions de données : effet d'étalement spectral dû à la dispersion.

Comme toute source de lumière aurait une certaine largeur spectrale $\Delta\lambda_0$ et chaque composant spectral en général se propage avec une vitesse de groupe différente, nous aurions toujours la dispersion chromatique.

Calcul de la dispersion chromatique

Exemple de la dispersion matériau dans la silice pure

λ_0 (µm)	n (λ_0)	$\frac{dn}{d\lambda_0}$ (µm^{-1})	$\frac{d^2n}{d\lambda_0^2}$ (µm^{-2})
0,65	1,45685128	-0,02714381	0,10309425
0,80	1,45363725	-0,01725159	0,03997833
1,30	1,44726325	-0,01125037	-0,00055057
1,55	1,44438815	-0,01189888	-0,00416491

Table 1. Variation de n, $dn/d\lambda_0$, $d^2n/d\lambda_0^2$ selon λ_0 pour silice pure (source : Thorlabs)

Source 1,55 µm de largeur spectrale de 2 nm :

A $\lambda_0 = 1{,}55$ µm, $\frac{d^2n}{d\lambda_0^2} = 0{,}004$ µm^{-2} impose une dispersion de 20 ps/km/nm. Par conséquent, pour une diode laser à 1,55 µm avec $\Delta\lambda_0 \cong 2$ nm, nous avons $\Delta\tau \cong 40$ ps/km.

Décalage temporel de deux signaux 1,55 µm et 1,30 µm :

- Si $\lambda_0 = 1{,}55$ µm et $N(\lambda_0) = n(\lambda_0) - \lambda_0 \frac{dn}{d\lambda_0}$ alors N(1550) = 1,46283141
- Si $\lambda_0 = 1{,}30$ µm, N(1300) = 1,46188873

On a :

$\Delta\tau = \tau(1550) - \tau(1300) = \frac{L}{c}\left[N(1550) - N(1300)\right] \cong 3{,}14 \times L$ (ns) où L s'exprime en km.

L = 1 km, $\Delta\tau \cong$ 3,14 ns
L = 100 km, $\Delta\tau \cong$ 314 ns

Source 1,55 µm de largeur spectrale de 110 MHz :

Nous avons $\nu = \frac{c}{\lambda}$ et donc $d\nu = -\frac{c}{\lambda^2} d\lambda$. Par conséquent, nous obtenons

$\Delta\nu = \frac{c}{\lambda^2}\Delta\lambda$ ou $\Delta\lambda = \frac{\lambda^2}{c}\Delta\nu$

et nous avons déjà eu : $\Delta\tau = \frac{d\tau}{d\lambda_0}\Delta\lambda_0 = -\frac{L}{c}\lambda_0 \frac{d^2n}{d\lambda_0^2}\Delta\lambda_0$

Applications numériques :

- L = 1 km
- c = 3.10^5 km/s
- $\lambda_0 = 1{,}55$ µm
- $\frac{d^2n}{d\lambda_0^2}$ = -0,00416491 µm^{-2}
- $\Delta\nu = 110$ MHz

$$\Delta\lambda = \frac{\lambda^2}{c}\Delta\nu = \frac{\left(1{,}55.10^{-6}\right)^2}{3.10^8}110.10^6 = 0{,}88.10^{-6}\ \mu\text{m}.$$

Et $\Delta\tau = -\frac{L}{c}\lambda_0\frac{d^2n}{d\lambda_0^2}\Delta\lambda_0 = 1{,}89.10^{-14}$ s

Autrement dit, nous avons : $\Delta\tau = 1{,}89.10^{-17}$ (s/m) (seconds par mètre)

Cela veut dire qu'au bout d'une fibre optique de longueur 10 km, cette impulsion s'étale une quantité de $1{,}89.10^{-17}$ s/m × 10 000 m = 0,189 ps.

4.5.2 Dispersion de polarisation

Un autre problème est posé par la polarisation de la lumière dans la fibre optique. Les imperfections de fabrication produisent un coeur de forme légèrement elliptique. De plus, à l'utilisation, les courbures déforment aussi la fibre ; on a alors un milieu anisotrope : au vu du faisceau, il y a des indices différents selon la direction. Dans la fibre, on constate une biréfringence : un rayon non polarisé incident est décomposé en deux rayons (extraordinaire et ordinaire) polarisés linéairement mais l'un en mode transverse magnétique (TM) et l'autre en mode transverse électrique (TE). Il y a donc des pertes de polarisation lors de la propagation.

4.5.3 Perte de puissance

La matière première de la fibre optique est la silice, mais elle est rarement parfaitement pure et est accompagnée de petites impuretés. On peut caractériser l'atténuation spectrale de la silice. On voit que plusieurs paramètres contribuent à faire perdre de la puissance au signal optique (fig. 4-21) :

- Tout d'abord ce que l'on appelle la diffusion Rayleigh qui traduit à la fois l'effet des impuretés, des imperfections, des craquelures et des variations d'indice. La diffusion Rayleigh est d'autant plus grande que la longueur d'onde est courte avec une variation en λ^{-4}), ce qui explique que les communications optiques soient dans l'infrarouge. C'est la limite physique qu'on ne peut dépasser.
- Ensuite les effets de vibration de la liaison hydroxyde (ion OH^- - oxygène hydrogène de l'eau), que l'on ne peut pas supprimer, et qui présentent un pic de forte atténuation autour de 1430 nm.

En superposant les profils d'atténuation, on remarque trois fenêtres spectrales à l'atténuation assez faible (flèches noires sur la figure) :

- Autour de 900 nm
- Autour de 1300 nm
- Et autour de 1550 nm

Ces trois fenêtres sont celles que l'on utilise couramment.

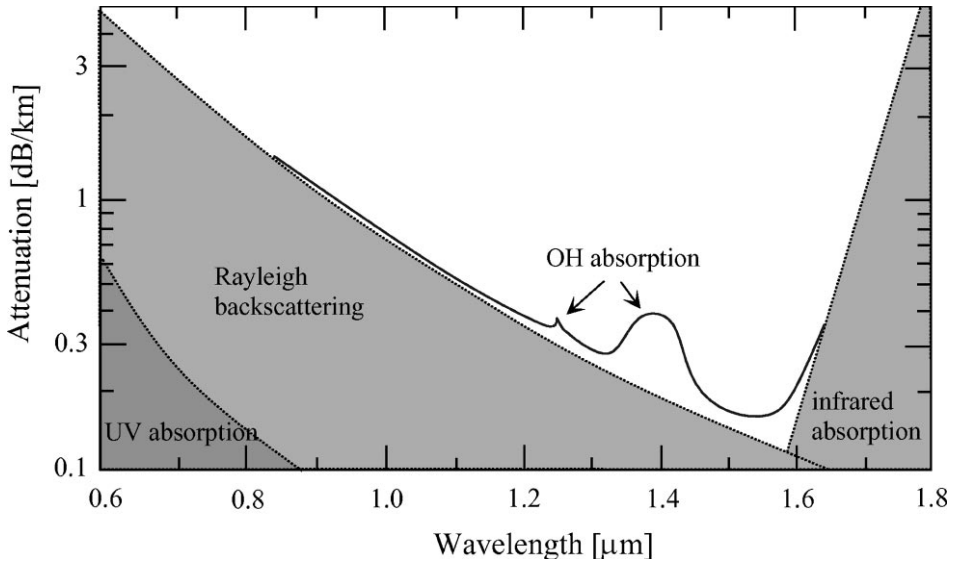


Figure 4-21. Profil de l'atténuation spectrale (exprimée en dB/km) en fonction de longueur d'onde de la fibre optique faite de silice [7].

Il n'est pas possible de supprimer totalement tous les effets qui atténuent le signal. Ainsi, le signal pour parcourir une longue distance doit être ré-amplifié régulièrement (cf. 4.1.1). Pour cela, on utilise ce que l'on appelle des EDFA (Erbium Doped Fiber Amplifier ou amplificateur à fibre dopée à l'erbium). Le dopage est une technique qui consiste à inclure un élément chimique dans la composition de la fibre. On choisit un élément qui possède des propriétés intéressantes au niveau de sa structure électronique. On privilège ce que l'on appelle les terres rares (de la famille de lanthanides comme le Praseodymium, le Terbium, l'Ytterbium ou encore l'Erbium).

4.6 Résultats expérimentaux

Nous discutons dans cette partie les résultats de mesure du filtre FP et du système.

4.6.1 Fonction de transfert

En appliquant une tension à la céramique piézoélectrique, nous sommes capables de produire un changement petit et contrôlable dans la longueur de la cavité. L'équation (4-4-17) a montré que la longueur de la cavité doit être changée d'une quantité de $\lambda/4$ pour déplacer le peigne des modes longitudinaux un intervalle modal. La figure 4-22 représente un pic de la fonction de transfert du FP. Le profil du pic est presque gaussien. La réponse est obtenue en faisant varier la longueur de la cavité, par l'intermédiaire de la haute tension appliquée à la céramique piézoélectrique elle même commandée par une tension en dent de scie ; donc variant linéairement avec le temps.

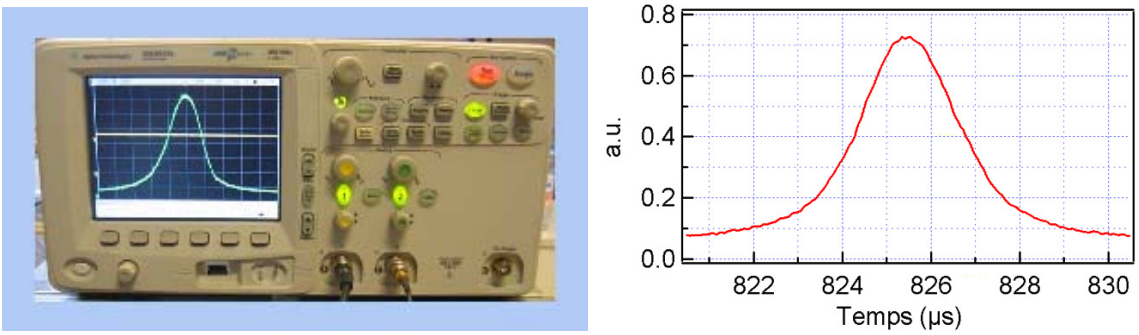


Figure 4-22. Le zoom d'un pic de la fonction de transfert du FP. La photo d'un pic de transmission sur l'oscilloscope (à gauche) et par enregistrement numérique (à droite)

La figure 4-23 illustre sur l'oscilloscope un intervalle modal du filtre. La commande du piézoélectrique est une rampe triangulaire qui fait apparaître deux pics de résonance. La différence de tension appliquée entre deux pics est de 143 volts qui coïncide avec le calcul (4-4-25).

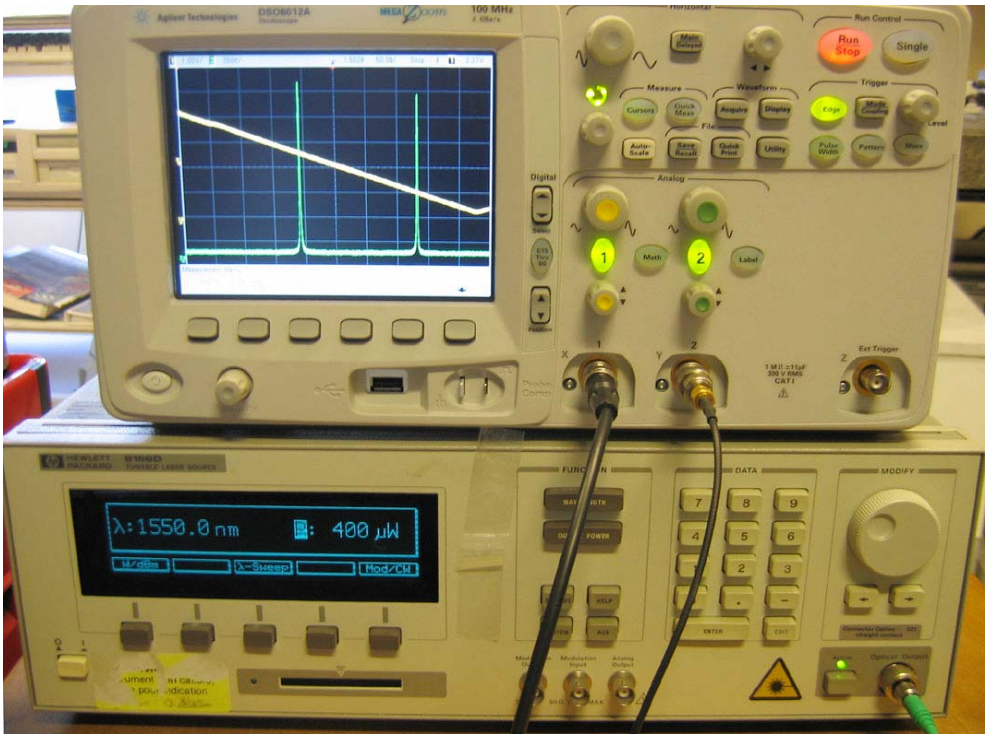


Figure 4-23. Photos de la source laser (en bas) et de l'oscilloscope (en haut) dans le montage d'alignement pour le FP. L'entrée est le laser 1550 nm de puissance de 0,4 mW. La commande du piézoélectrique est une rampe triangulaire qui balaie largement un intervalle modal ; La différence de tension appliquée entre deux pics est de l'ordre de 143 volts qui coïncide avec le calcul (4-4-25).

4.6.2 Mesure de résolution du filtre

A l'aide de l'oscilloscope, on peut déterminer la finesse et la résolution par les mesures temporelles. Dans l'expérience d'alignement du FP (fig. 4-18), on applique au piézoélectrique une rampe triangulaire, de fréquence de 1 kHz et d'amplitude de 0-500 volts. On voit apparaître dans la rampe descendante (également dans la rampe montante) deux pics de résonance du filtre. La distance entre ces deux pics (aussi dit, intervalle modal) est de 156,5 ms. La largeur du pic de résonance est de 1,12 ms. On en déduit la valeur estimée de la finesse du filtre : $\text{Finesse} = \frac{\text{intervalle modal}}{\text{largeur de pic}} = \frac{145{,}6}{1{,}12} \approx 130$. (Valeur théorique = 156)

Résolution = 375 MHz / 130 = 2,9 MHz.

a) Filtrage fréquentiel

Nous vérifions pour la suite la capacité de filtrage fréquentiel du filtre. Pour cela, nous utilisons l'expérience montrée dans la figure 4-24. Ce montage est légèrement différent par rapport au schéma dans la page 58 (fig. 4-5). Le but est de pouvoir cacher successivement l'une et l'autre de deux sorties de l'AOM pour que nous puissions confirmer notre choix de longueur d'onde. Ici, on utilise l'ordre '0' en sortie de l'AOM comme longueur d'onde initiale λ_0.

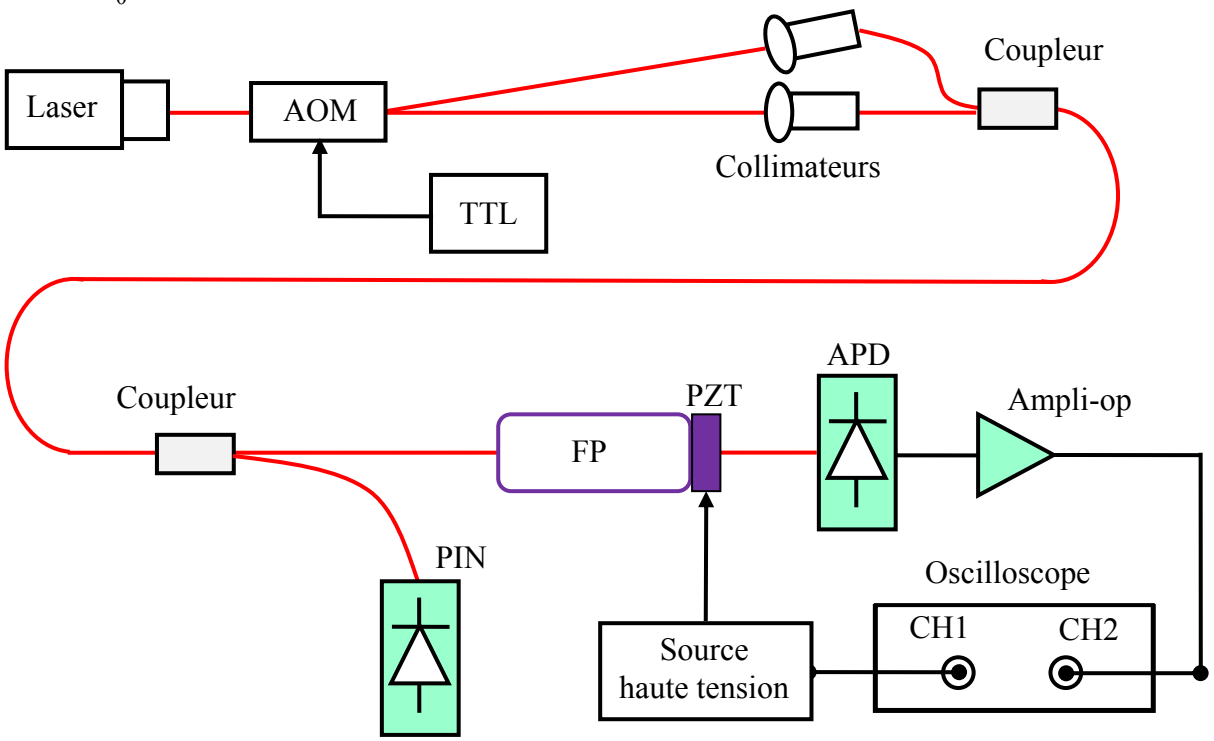


Figure 4-24. L'expérience de filtrage fréquentiel. AOM : modulateur acousto-optique, PZT : transducteur piézoélectrique, APD : photodiode à avalanche, PIN : photodiode PIN.

En injectant un faisceau laser continu (diode laser FLD5F6CX) au modulateur AOM, on crée les deux faisceaux laser de longueurs d'onde différentes. Ces deux faisceaux sont récupérés par deux collimateurs puis mélangés dans un coupleur optique. Le signal transmis dans la fibre contient donc deux longueurs d'onde sortant de l'AOM. Ce signal passe à la fois au filtre FP et au détecteur basé sur une photodiode PIN.

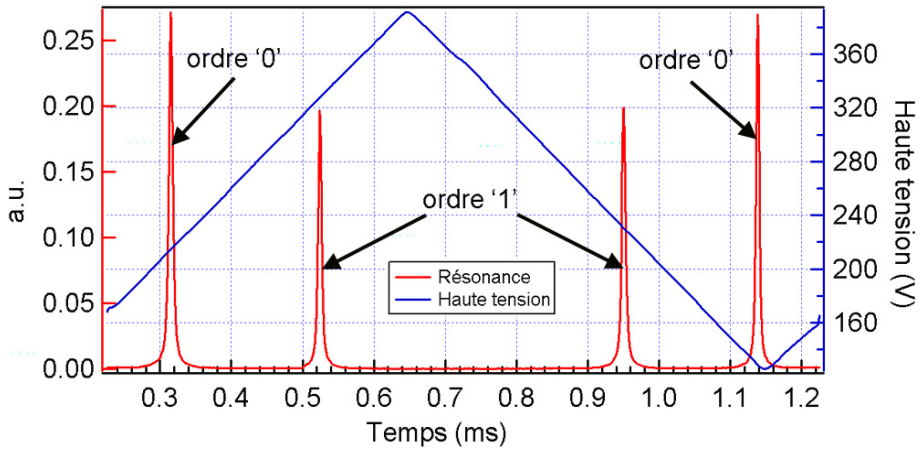
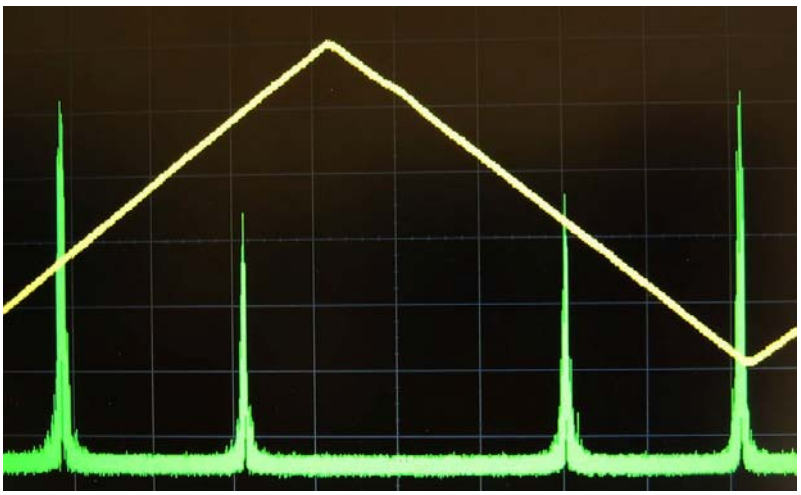
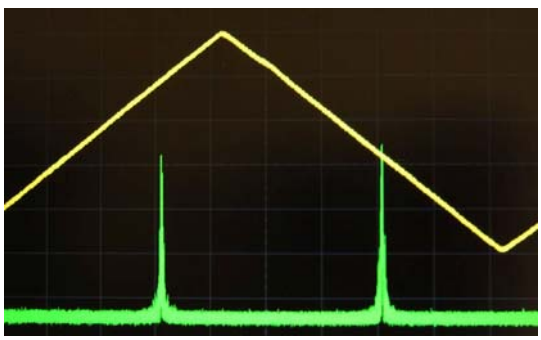


Figure 4-25. Transmission à travers le Fabry-Pérot confocal. Les pics (courbe rouge) représentent les modes de résonance avec la présence d'un faisceau laser composant de deux longueurs d'onde λ1 et λ0. Deux pics au centre viennent du 1er ordre et deux pics d'extrémité (intensité plus élevée) viennent de l'ordre '0' dans la sortie de l'AOM. Ici, on voit que $\lambda_1 < \lambda_0$, d'après l'expression 4-4-25.

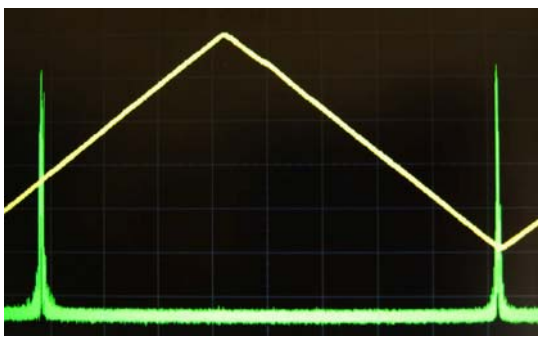
Les figures 4-25 et 4-26 représentent les pics de résonance de ce signal dans la cavité FP. En cachant la voie 1 ou 2 (fig. 4-24), on peut faire apparaître seulement les pics de longueur d'onde désirée λ_1 (fig. 4-26b) ou λ_0 (fig. 4-26c) respectivement.



4-26a)



4-26b)



4-26c)

Figure 4-26. Illustration de la capacité à séparer les longueurs d'onde du FP : a) séries de pics de résonance représentant deux longueurs d'onde différentes issues de l'AOM (ordres '0' et '1') ; b) les pics du 1er ordre ; c) les pics de l'ordre 0. On obtient ces résultats en cachant respectivement une des entrées du FP, c'est-à-dire, la voie λ1 ou λ0 (voir fig. 4-24).

4.6.3 Préparation des clés à transmettre

On utilise une interface d'électronique numérique, boîtier CKG-1, pour créer les clés à transmettre. Elle est un nous donne possibilité de créer des séquences de 128 bits servant à encoder « une clé ». La photo du boîtier CKG-1 est montrée dans la figure 4-27 ci-dessous. Elle est composée de principaux composants : registre à décalage XC3042A-7C, registre intermédiaire XC1736EPC, émetteur-récepteur octal SN74LS245N, monostable SN74LS123, interface USB FTDI FT245AM.

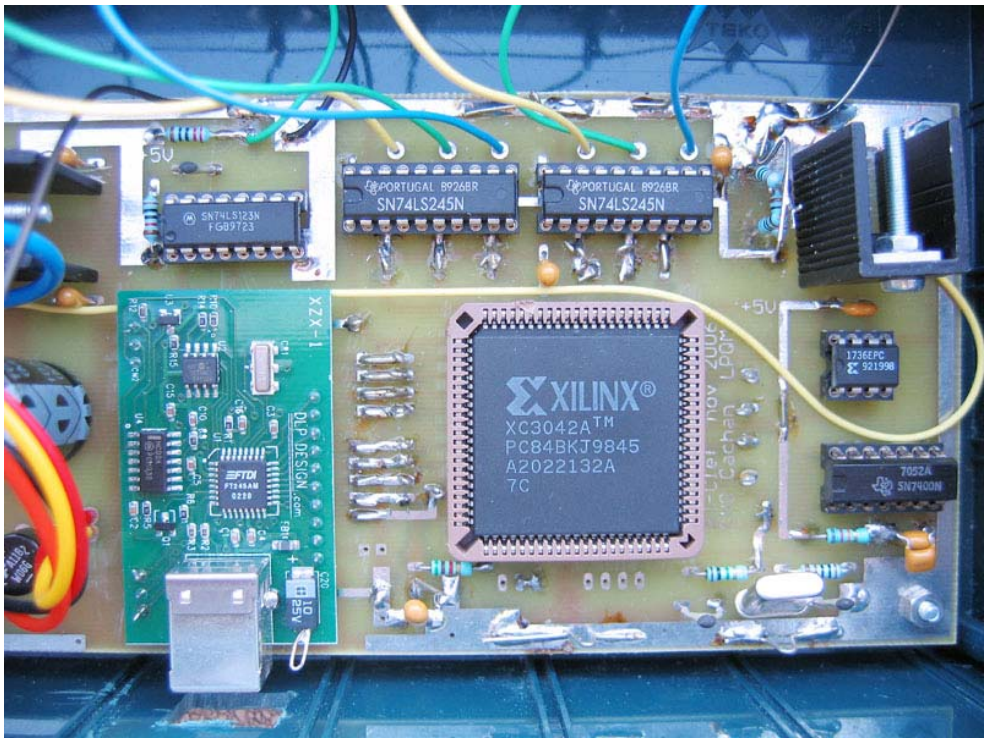


Figure 4-27. Photo du boîtier CKG-1. Créateur : André Clouqueur. Il est composé des composants : registre à décalage XC3042A-7C, registre intermédiaire XC1736EPC, émetteur-récepteur octal SN74LS245N, monostable SN74LS123, interface USB FTDI FT245AM, etc.

L'interface USB FTDI FT245AM fournit une méthode facile et efficace de transfert de données d'un ordinateur à un périphérique avec un débit jusqu'à 1 mégaoctets par seconde (8 Mbps) par liaison série à travers le port USB de l'ordinateur. C'est le type de fonctionnement comme premier entré-premier sorti (FIFO : First-In/First-Out) qui le rend facile de connecter à n'importe quel ordinateur par le contrôle des dispositifs par l'intermédiaire des portes d'entrée/sortie.

Pour envoyer les données du périphérique au PC hôte, on écrit simplement les données de largeur de byte dans le dispositif quand la commande de vider la mémoire de l'émetteur n'est pas encore active. Les données écrites sont stockées dans la mémoire tampon FIFO (FIFO Transmit Buffer, fig. 4-28). Si la mémoire tampon d'émission (384 bytes) se remplit, le dispositif s'impose de vider la mémoire afin d'arrêter d'autres données étant écrites au dispositif jusqu'à ce que certaines des données FIFO aient été transférées via le port USB.

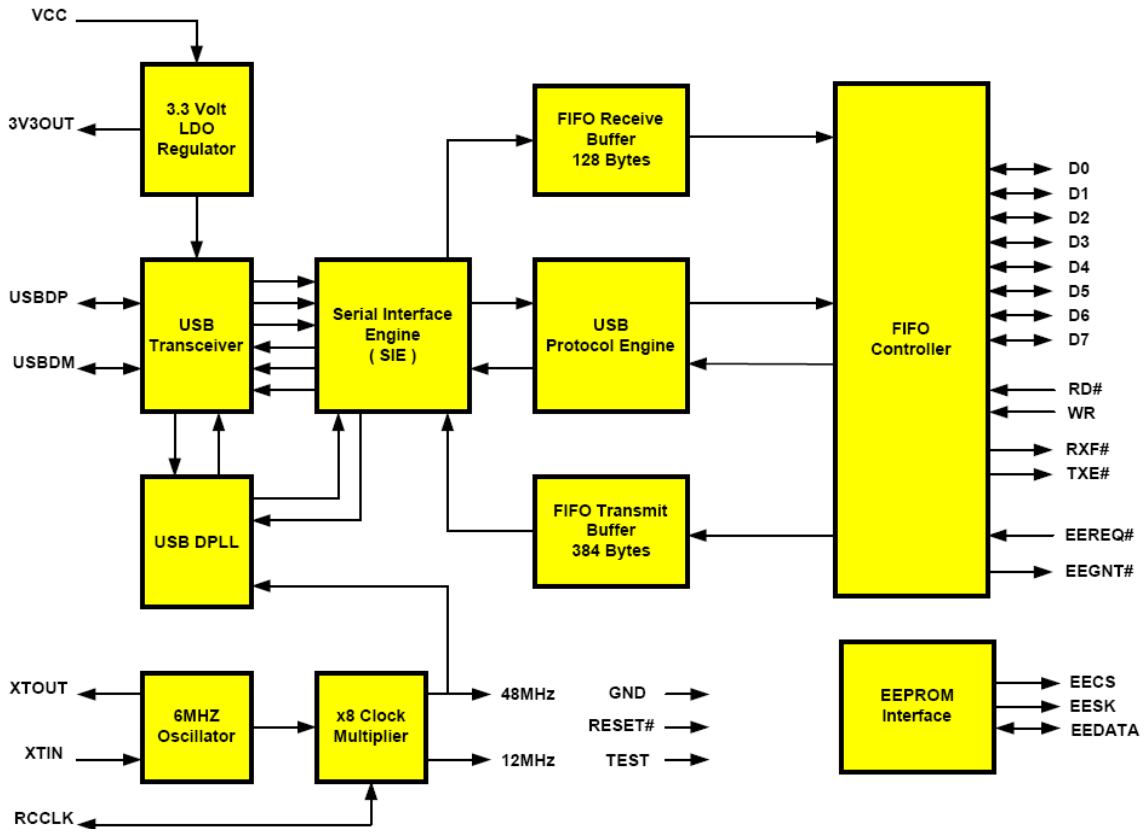


Figure 4-28. Diagramme block simplifié du FTDI FT245AM [78].

Quand le PC envoie des données au périphérique à travers le port USB, les données sont d'abord stockées dans le FIFO Receive Buffer (fig. 4-28) puis le dispositif impose au récepteur le statut de mémoire pleine pour informer le périphérique que les données sont disponibles. Le périphérique va recevoir (lire) les données jusqu'au moment où le statut de mémoire pleine du récepteur est désactivé, indiquant que plus de données ne sont disponibles pour lire. En employant le driver créant des portes COM virtuelles, le périphérique ressemble à une porte COM standard d'application des logiciels (fig. 4-28).

L'architecture du registre à décalage Xilinx XC3042A, se présente sous forme de deux couches :

- une couche appelée circuit configurable,
- une couche réseau mémoire SRAM (Static Random Access Memory).

La couche dite « circuit configurable » est constituée d'une matrice de blocs logiques configurables CLB permettant de réaliser des fonctions combinatoires et des fonctions séquentielles. Tout autour de ces blocs logiques configurables, nous trouvons des blocs entrées/sorties IOB dont le rôle est de gérer les entrées-sorties réalisant l'interface avec les modules extérieurs (fig. 4-29). La programmation du circuit FPGA appelé aussi LCA (logic cells arrays) consistera par le biais de l'application d'un potentiel adéquat sur la grille de certains transistors à effet de champ à interconnecter les éléments des CLB et des IOB afin de réaliser les fonctions souhaitées et d'assurer la propagation des signaux. Ces potentiels sont tout simplement mémorisés dans le réseau mémoire SRAM.

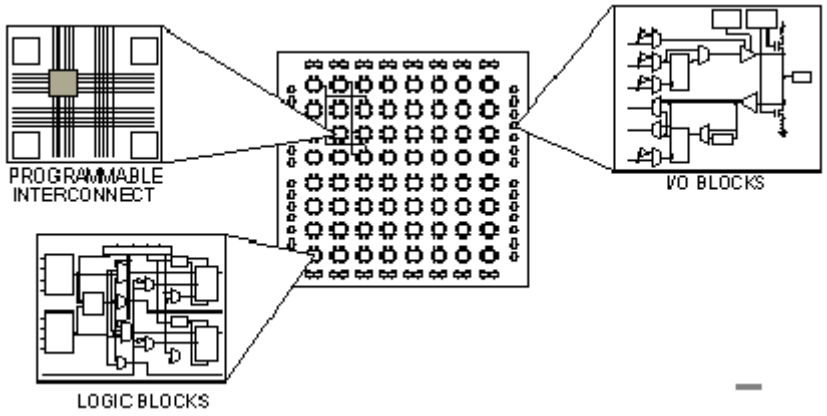


Figure 4-29. Architecture interne du FPGA [79].

Dans le mode principal (dit mode Master), le FPGA charge automatiquement les données de configuration d'un bloc de mémoires externe. Il y a de trois modes Master qui emploient la source de synchronisation interne pour fournir l'horloge de configuration (CCLK : configuration clock) pour chronométrer les données d'entrée. Le mode Master série emploie des données de configuration périodiques fournies à D_{IN} d'une source périodique synchrone comme la PROM de configuration périodique de Xilinx (ex. XC1736EPC).

Les IOB (input output bloc)

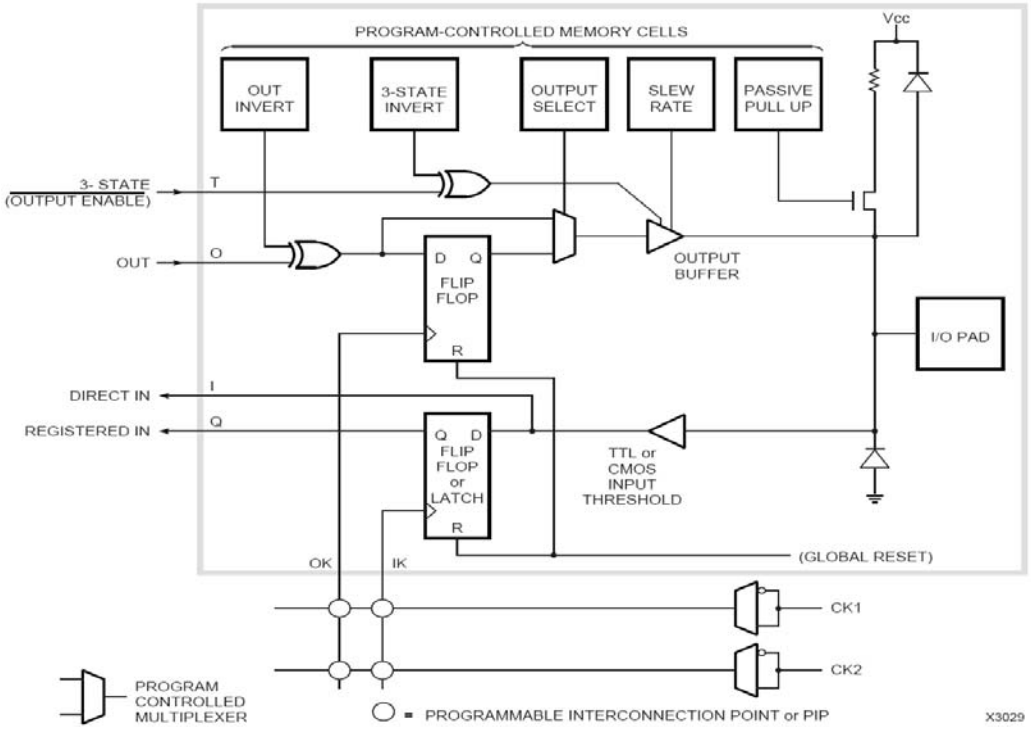


Figure 4-30. Bloc entrée/sortie (IOB) [79].

La figure 4-30 présente la structure de ce bloc. Ces blocs entrée/sortie permettent l'interface entre les broches du composant FPGA et la logique interne développée à l'intérieur du composant. Ils sont présents sur toute la périphérie du circuit FPGA. Chaque bloc IOB

contrôle une broche du composant et il peut être défini en entrée, en sortie, en signaux bidirectionnels ou être inutilisé (haute impédance).

Les CLB (configurable logic bloc)

Les 144 blocs logiques CLB du XC3042A sont disposés dans une matrice de 12 rangées et 12 colonnes. Les CLB sont les éléments déterminants des performances du FPGA. Chaque CLB a une partie logique combinatoire, deux bascules et une unité de commande interne (fig. 4-31). Chaque bascule présente deux modes de fonctionnement : un mode « flip-flop » avec comme donnée à mémoriser et un mode latch. La donnée peut être mémorisée sur un front montant ou descendant de l'horloge (K). Les sorties de ces deux bascules correspondent aux sorties X et Y du CLB.

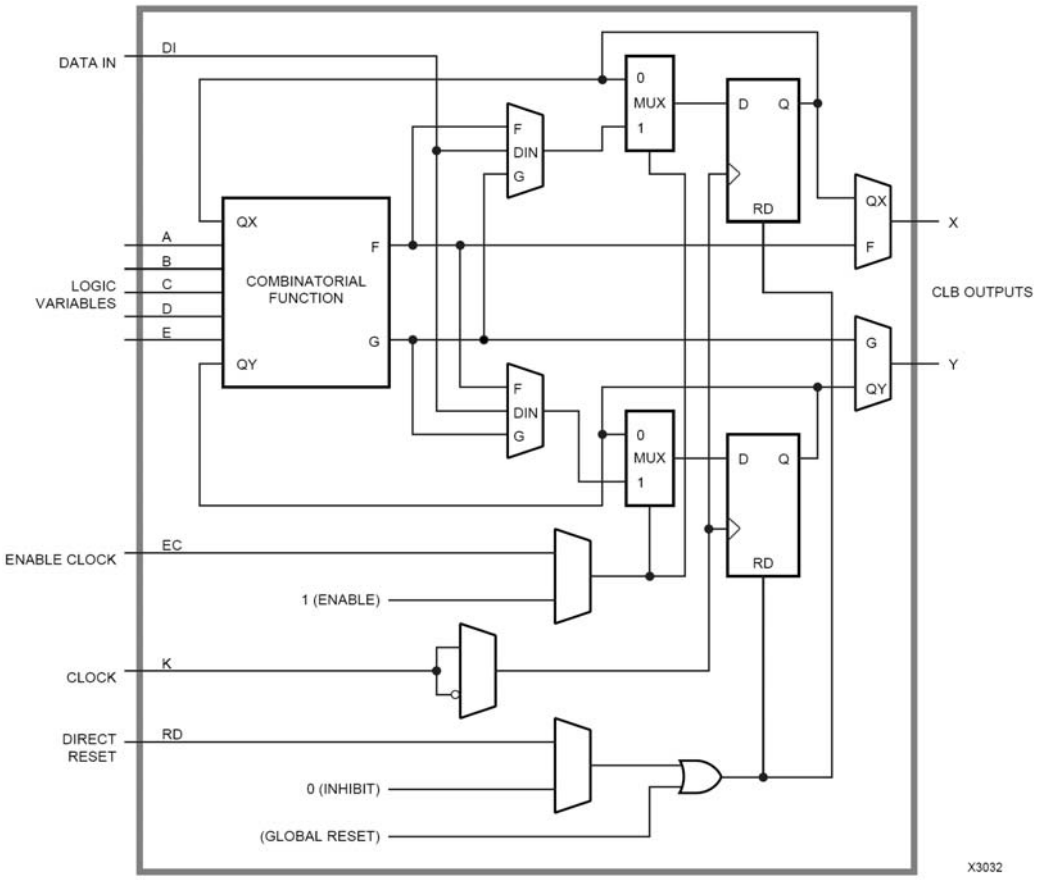


Figure 4-31. Bloc logique configurable CLB [79].

Un bloc logique configurable CLB possède :

- cinq entrées logiques (A, B, C, D et E) ;
- une entrée de données directe (DI) ;
- une entrée d'horloge commune (K) ;
- une entrée reset directe asynchrone (RD) ;
- un enable clock (EC).
- Deux sorties X et Y.

Tous peuvent être conduits par l'interconnexion ressources à côté des blocs. Chaque CLB a également deux sorties (X et Y) qui peuvent conduire des réseaux d'interconnexion. L'entrée de données pour l'une ou l'autre bascule dans un CLB est assurée à partir des sorties de fonction F ou G de la logique combinatoire, ou entrée de bloc, DI.

Le XC1736EPC est une mémoire morte programmable (PROM – Programmable Read Only Memory) de configuration qui fournit une méthode efficace pour le stockage les trains de bits de configuration du FPGA XC3042A. Quand le FPGA fonctionne en mode Master série, il génère une horloge de configuration qui conduit la PROM. Un temps très court après le front montant d'horloge, les données apparaissent à la sortie DATA de la PROM (fig. 4-32) ; cette sortie est connectée à l'entrée DI du FPGA. Le FPGA génère un nombre approprié d'impulsions d'horloge pour compléter la configuration. Une fois que c'est fait, il met la PROM hors service.

Avec une résistance et une capacité externes convenables, le monostable SN74LS123 donnera le signal d'horloge de 100 ns qui est connecté à l'entrée RD (Reset direct) du registre FPGA (fig. 4-31).

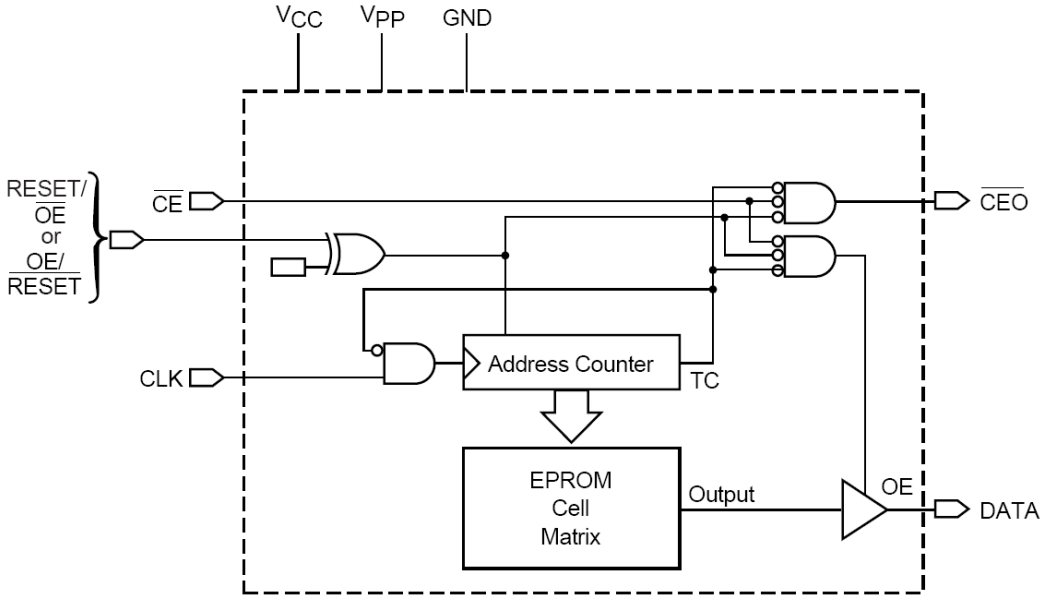


Figure 4-32. Diagramme bloc simplifié du registre XC1736EPC [79].

Fonctionnement du boîtier CKG-1

L'ordinateur charge des bits au boîtier à travers le FT245AM. A l'aide des logiciels actuellement disponible comme LabView ou Igor WaveMetric, on peut programmer les envois des données bit à bit en série de type FIFO via l'interface USB. On charge donc dans le registre intermédiaire – le XC1736EPC – une 'tête' de 2 bits, une 'queue' de 2 bits et les 4 mots intermédiaires de 4 bits. Un mot d'état dans le registre FPGA XC3042C se compose de 4 mots intermédiaires de 4 bits (fig. 4-33). On pourra charger les 8 mots d'état (P0, P1, …, P7) par les 4 registres intermédiaires différents ou identiques de 4 bits (RI0, RI1, RI2, RI3).

Finalement, on a donc une clé de 8 x 4 x 4 bits = 128 bits. Le signal transmis a une longueur de 132 bits, y compris les 2 bits de tête et 2 bits de de queue.

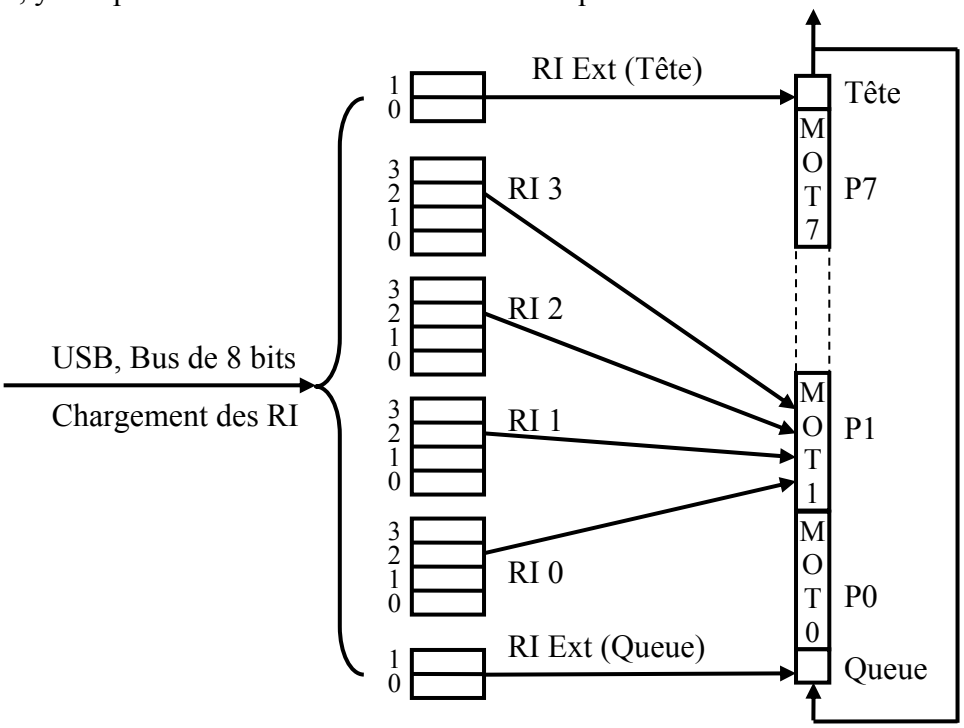


Figure 4-33. Schéma de principe du processus de transfert de données dans le registre à décalage via des registres intermédiaires. RI 0, 1, 2, 3 : 4 mots (0, 1, 2 et 3) dans les registres intermédiaires.

Le registre FPGA fonctionnera en mode Master série. Après chaque front montant d'horloge CCLK (horloge de configuration issue du FPGA), les données apparaissent à la sortie DATA de la PROM (fig. 4-32) ; cette sortie est connectée à l'entrée D_{IN} du FPGA. Les figures 4-34 à 4-36 représentent une série de bits servant à commander un signal optique (à l'aide d'un modulateur Mach-Zehnder) afin de délivrer une séquence des impulsions laser modulées en intensité. La clé contient proprement 128 bits ; les 2 bits de queue et 2 bits de tête servent à éviter l'influence du temps de monté et de descente du signal de modulation. Comme chaque bit a pour une durée de 100 nanosecondes (fig. 4-35), la durée du signal contenant de clé (y compris les bits de queue et de tête) est de 13,2 µs. Ce signal sera connecté au modulateur Mach-Zehnder pour moduler l'intensité du faisceau laser.

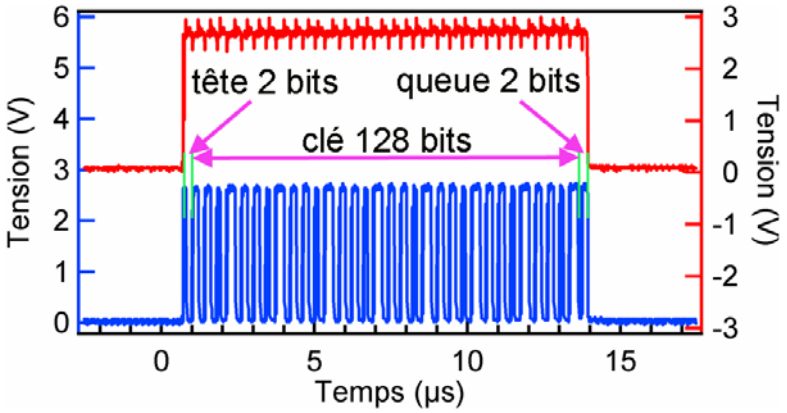


Figure 4-34. Série des clés électroniques servant à commander un signal optique (à l'aide d'un modulateur Mach-Zehnder) afin de délivrer une séquence des impulsions laser modulée en intensité.

La clé contient 128 bits ; les 2 bits de queue et 2 bits de tête servent à éviter l'influence du temps de montée et de descente du signal de modulation.
La programmation de la clé de cryptage peut être réalisée avec des logiciels courants dans les laboratoires comme Igor ou LabView. Ici, nous avons écrit un programme dans le logiciel Igor (voir annexe A).

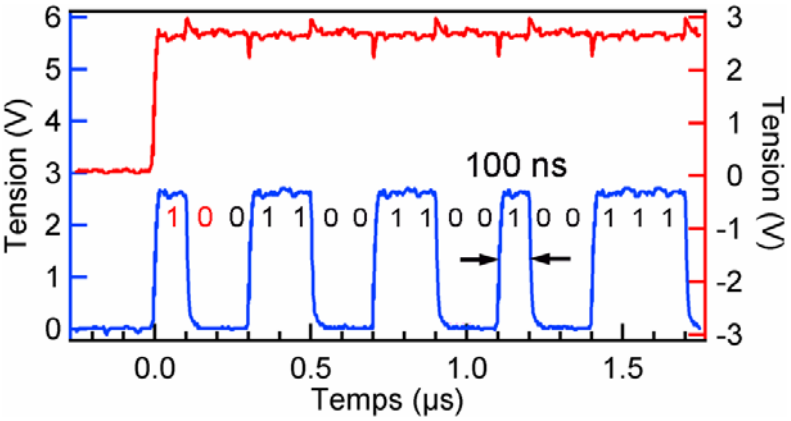


Figure 4-35. Exemple du début d'une clé électronique générée par le générateur CKG-1. La durée d'un bit est de 100 ns. Sur la figure, de gauche à droite, nous avons les 2 bits de tête '10' et une partie de la clé '011001100100111'.

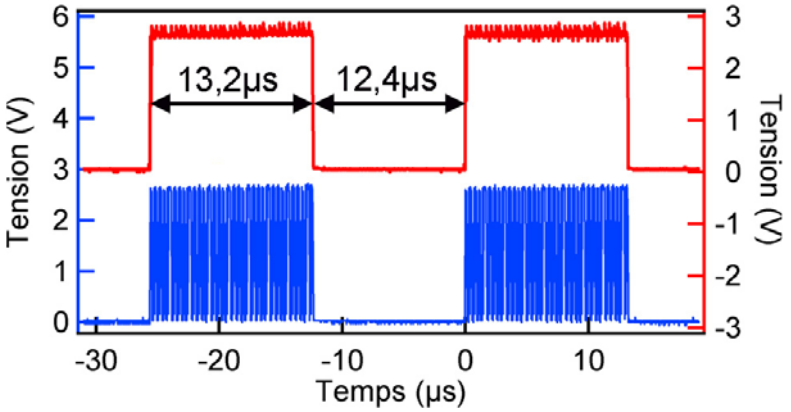


Figure 4-36. Exemple d'une clé électronique générée par le générateur CKG-1. Chaque signal de clé contiendra 132 bits dont 4 bits de queue et de tête, sa longueur est donc de 13,2 µs. Le signal de modulation est un créneau de période 2 x 128 x 100 ns = 25,6 ns (ou 39,06 kHz).

4.6.4 Nécessité de la récupération d'horloge

Dans la figure 4-5, la photodiode PIN sert à récupérer le signal horloge qui sera utilisé pour la réception et la synchronisation des clés de cryptage. Dans cette configuration-là (fig. 4-5), la fréquence d'horloge est de 10 MHz, i.e. l'inverse du temps bit de 100 ns. A la détection, la décision de la valeur **0** ou **1** d'un bit doit se faire à un moment précis du laps de temps sur lequel celui-ci est transmis. Les décisions successives doivent donc intervenir à intervalles réguliers, de longueur égale au temps bit.

On synchronise donc récepteurs et éventuellement régénérateurs à une horloge, i.e. un signal périodique (qu'il soit sinusoïdal, impulsionnel, en créneaux...) de période égale au

temps bit. Afin d'en assurer l'exactitude, cette horloge doit être extraite du signal portant les données. La fonction correspondant à cette opération est appelée récupération d'horloge, et est une fonction critique de tout système de transmission de données numériques.

5 Photodétecteurs

Sommaire

Les photodétecteurs ont pour fonction de transformer un signal optique en un signal électrique. Pour les télécommunications les qualités requises sont :

- Une détectivité importante à la longueur d'onde utilisée (de 0,8 à 1,55 μm).
  S = détectivité = photocourant / puissance optique incidente, en A/W.
- Une bande passante large. Il faut pouvoir utiliser le photodétecteur jusqu'à des débits de plusieurs dizaines de Gbit/s.
- Apporter le minimum de bruit au signal lors du processus de détection.

La longueur d'onde maximale (λ max) dépend des énergies de bande interdite (E_g) des matériaux utilisés pour photodiodes. On en cite ci-dessous quelques exemples :

Matériau	E_g (eV)	λ max (μm)
Si	1,17	1,06
Ge	0,775	1,6
GaAs	1,424	0,87
InP	1,35	0,92
$In_{0,55}Ga_{0,45}As$	0,75	1,65
$In_{1-0,45y}Ga_{0,45y}As_yP_{1-y}$	0,75 ÷ 1,35	1,65 ÷ 0,92

Tableau 5-1. Matériaux semiconducteurs utilisés pour photodiodes (voir aussi la figure 5-4).

La détection de lumière joue un rôle important dans notre système de transmission. Le photodétecteur a pour rôle de détecter des photons en petit nombre, et d'énergie très faible à 1,55 μm dans notre expérience. Nous discutons dans ce chapitre quelques types de détecteurs pour la détection de photons uniques [12], en particulier la photodiode à avalanche (APD). Le détecteur idéal pour ces applications aurait une grande rapidité, les coups d'obscurité quasiment inexistants, et une efficacité quantique très élevée à la longueur d'onde utilisée. On se limite aux photodiodes semiconductrices ou détecteurs supraconducteurs qui assurent la détection efficace des signaux optiques d'intensité extrêmement faible (l'ordre de pico watts, cf. 3.5.2).

5.1 Photodiode PIN

5.1.1 PIN au silicium

Le matériau de base pour la fabrication des photodiodes sensibles dans le domaine visible ou le proche infrarouge, est le silicium. La structure PIN est la plus répandue. Elle consiste à intercaler entre la zone N et la zone P, d'une jonction PN classique, une zone intrinsèque « I » ou très faiblement dopée. L'intérêt d'une telle structure réside, pour les fabricants, dans le fait qu'il est possible de résoudre au mieux le compromis sensibilité-rapidité en jouant sur les caractéristiques de cette zone I (fig. 5-1). Les photodiodes PIN sont polarisées en inverse. Sous l'action de cette polarisation, une partie des zones P et N est démunie de porteurs libres formant ainsi la zone de charge d'espace dans laquelle s'établit un champ électrique. Les électrons et les trous, générés par paires lors de l'absorption de photons dont l'énergie est supérieure à celle de la bande interdite, vont se déplacer en sens inverse sous l'action du champ électrique.

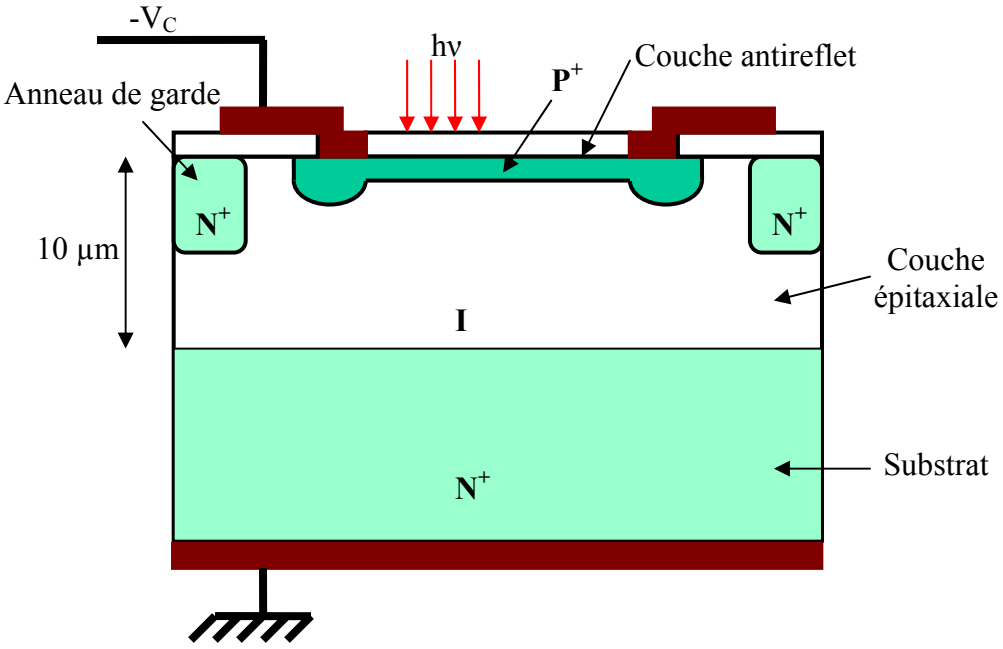


Figure 5-1. Coupe d'une photodiode PIN au silicium, obtenue par épitaxie d'une couche résistive (I) et diffusion localisée d'une mince zone fortement dopée (P^+), qui après les opérations de métallisation, est recouverte d'une couche antireflet permettant d'éliminer les pertes par réflexion.

En l'absence d'éclairement, le courant qui traverse la jonction est uniquement d'origine thermoïonique. Il est appelé courant d'obscurité I_{obs}. Sous éclairement, le bombardement photonique provoque la génération de paires électron-trou au voisinage de la jonction, qui conduise à l'accroissement du courant inverse. Ce courant est proportionnel à l'intensité du flux incident (fig. 5-2). De tels dispositifs peuvent donc être utilisés pour la mesure quantitative de la lumière.

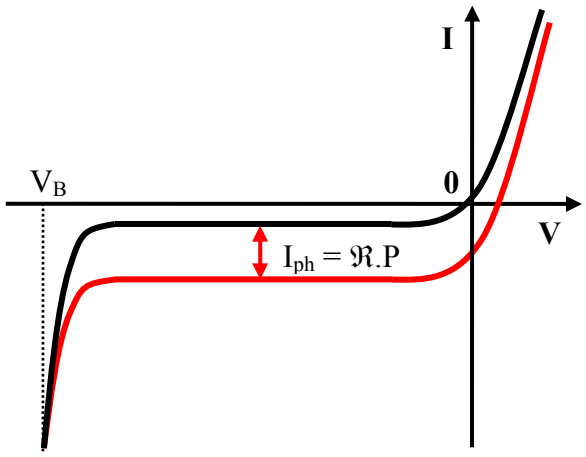


Figure 5-2. Caractéristique I-V d'une photodiode au silicium. La courbe noire (au-dessus) représente la réponse de la photodiode en obscurité. La courbe rouge (au-dessous) représente la réponse de la photodiode en présence de la puissance optique P.

La relation I-V du dispositif peut être donnée par [88] :

$$I = I_S\left(e^{qV/kT} - 1\right) - I_{\text{ph}} \tag{5-2-1}$$

où I est le courant à travers le dispositif, I_S est le courant de saturation, q est la charge de l'électron, V est la tension appliquée, k est la constante de Boltzmann, et T est la température. L'équation (5-2-1) ressemble à l'équation de diode avec le premier terme représentant le courant d'obscurité et le terme additionnel I_{ph} représentant le photocourant donné par

$$I_{ph} = \eta \frac{q}{hc} \lambda P \tag{5-2-2}$$

où η est l'efficacité quantique, h est la constante de Planck, c est la vitesse de la lumière dans le vide, λ est la longueur d'onde de lumière incidente, et P est la puissance optique incidente. En sachant la surface sensible A de la photodiode, la puissance optique peut être liée à l'intensité de la lumière I (W/m^2) par

$$P = IA \tag{5-2-3}$$

Par définition, la réponse (aussi appelée sensibilité) du détecteur $\Re$ (A/W) peut être obtenue à partir de l'équation (5-2-2) et s'exprime par

$$\Re = \frac{I_{ph}}{P} = \eta \frac{q}{hc} \lambda \tag{5-2-4}$$

Les photodiodes PIN au silicium ont des caractéristiques :

- Détection à la longueur d'onde de 0,8 µm.
- Sensibilité de l'ordre de 0,6 A/W sous une tension inverse de 5 V.
- Fréquence de coupure 140 MHz pour un diamètre de 350 µm.

Les photodiodes au germanium détectent à 1,3 et 1,55 µm.

5.1.2 PIN à hétérostructure III-V

Les photodétecteurs à base d'arséniure de gallium (AsGa) et de phosphure d'indium (InP) conçus pour détecter sur un large spectre optique ont des détectivités supérieures à 0,7 A/W de 1 à 1,55 µm. Le rendement quantique externe atteint 70% à la longueur d'onde de 1,3 µm. Les régions de type P et de type N en InP sont transparentes à 1,3 µm et 1,55 µm. La région intrinsèque (I) en InGaAs absorbe fortement dans la bande 1,3 µm - 1,55 µm.

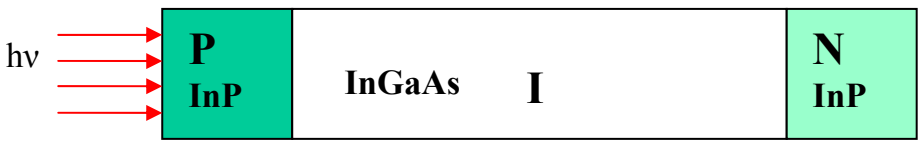


Figure 5-3. Photodiode PIN à hétérostructure III-V.

Les avantages par rapport aux photodiodes au germanium sont :

- Coefficients d'absorption plus élevés (détectivité S = 0,8 à 0,9 A/W sous tension inverse 6 V)
- Temps de réponse plus faible (capacité 0,4 à 0,9 pF, temps de réponse 0,4 ns).

5.2 Photodiode à avalanche

Les photodiodes à avalanche de silicium (Si-APD) sont les détecteurs fondamentaux pour le comptage de photons uniques dans le domaine visible [80-82], avec une efficacité de détection élevée (jusqu'à 76% à 700 nm) et les coups d'obscurité faibles (~ 100 Hz) [83]. La plus faible stabilité de synchronisation (timing jitter) annoncée est de 20 ps à la largeur à mi-hauteur (FWHM) [84], mais les valeurs typiques pour les unités commerciales sont 10 à 20 fois plus hautes. Le taux de comptage jusqu'à 5 MHz est généralement réalisé. Pour les longueurs d'onde du proche infrarouge telles que des longueurs d'onde standard de télécommunication (1310 nm et 1550 nm) la détection de photons s'effectue à l'aide des APD InGaAs [85-86]. Ces dernières nécessitent un refroidissement à 200 K, offrent une efficacité de détection réduite (20-30%), et sont limitées pour des taux de comptage vers 100 kHz. La réponse en fréquence optique des photodiodes basées sur les matériaux semiconducteurs les plus courants est montrée dans la figure 5-4 ci-dessous.

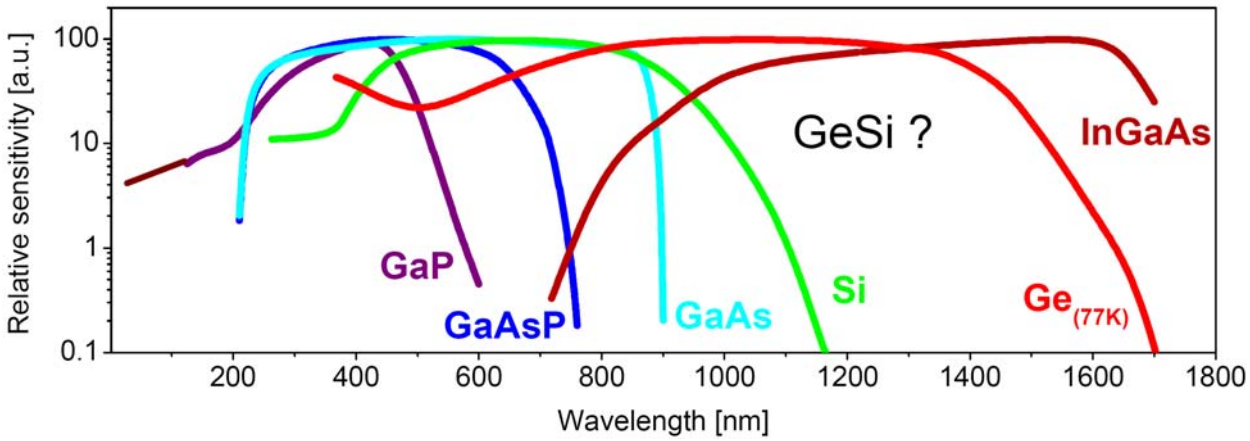


Figure 5-4. Dépendance de la sensibilité en longueur d'onde des photodétecteurs basés sur les matériaux semiconducteurs le plus courants [Fujitsu]. On prévoit l'apparition des photodétecteurs qui seraient basés sur un nouveau matériau GeSi. Il semble que les photodétecteurs actuels couvrent toutes les longueurs d'onde possibles de 0,2 µm à 1,7 µm.

5.2.1 Structure et théorie d'opération

La photodiode à avalanche est généralement utilisée pour des applications concernant des signaux optiques faibles grâce à son gain interne. Elle est basée sur une structure séparée des régions d'absorption et de multiplication. La figure 5-5 ci-dessous donne un exemple de structure pour une diode fonctionnant à 1550 nm. Le principe de fonctionnement est le suivant.

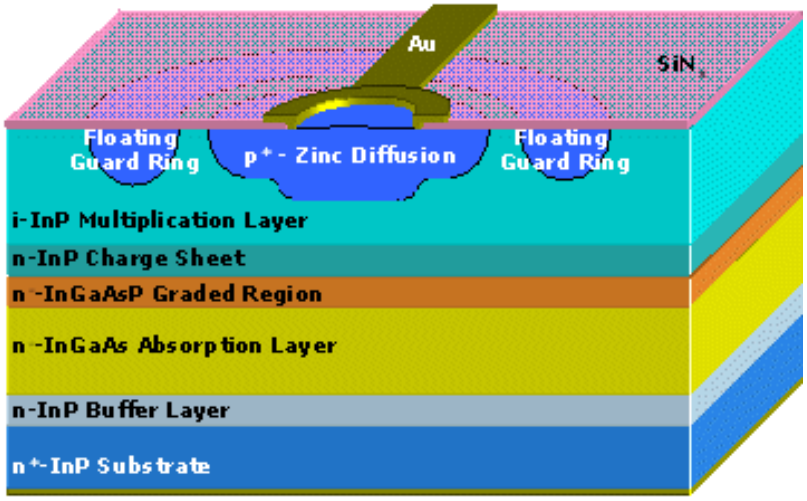


Figure 5-5. Schéma de la coupe transversale d'une APD InGaAs/InP développée à l'université Heriot-Watt - Royaume-Uni [87]. Elle possède d'un anneau de garde flottant, une couche p en haut pour zone active et une couche n pour substrat. La zone active se trouve du côté de dessus (p+ InP).

Les photodiodes à avalanche (APD) sont polarisées. Quand un photon est absorbé dans la couche InGaAs, une paire d'électron-trou est produite. Sous l'action du champ électrique, l'électron est accéléré vers le contact arrière (en bas de la figure 5-5), alors que le trou dérive dans la couche InGaAs appauvrie vers la région de multiplication InP où il subirait l'ionisation par choc. En effet, si au cours de ce déplacement, les porteurs de charge acquièrent, grâce au champ électrique, suffisamment d'énergie, ils peuvent être à l'origine de la formation d'une nouvelle paire électron/trou produite par une collision ionisante avec le réseau cristallin. Les paires secondaires ainsi créées peuvent à leur tour produire de nouvelles paires et générer un phénomène d'avalanche, permettant l'obtention d'une multiplication du nombre de porteurs libres et, par conséquent, celle d'un gain sur le signal électrique mesurable aux bornes de l'APD (fig. 5-6).

La bande interdite intermédiaire InGaAsP est introduite entre InGaAs et InP pour assurer le transfert efficace des trous à travers la grande discontinuité de bande de valence. L'anneau de garde est destiné à réduire le courant de fuite entre l'électrode collectrice et les autres électrodes d'une chambre d'ionisation et à définir les gradients de potentiel et le volume utile.

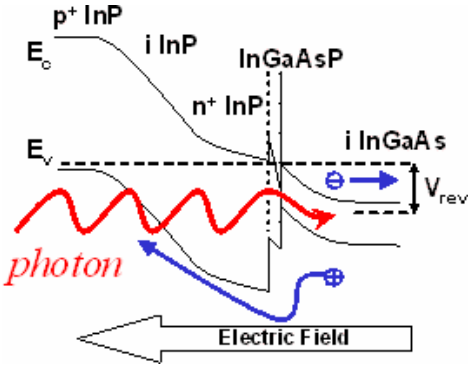


Figure 5-6. Diagramme de bande d'énergie d'une APD InGaAs/InP en présence de la polarisation électrique [87]. L'électron se déplace vers le contact arrière (à droite) et le trou en sens inverse. La bande InGaAsP intermédiaire a pour but d'assurer le transfert efficace des trous.

On distingue les photodétecteurs de type PIN et à avalanche. Une photodiode à avalanche est une diode PIN dans laquelle est réalisée une amplification du courant dans la zone de charge d'espace. Pour la photodiode PIN, un photon incident crée au mieux un photoélectron. Pour le photodétecteur à avalanche, le photoélectron créé engendre à son tour des photoélectrons secondaires en nombre aléatoire. Cela permet d'extraire un signal électrique fort même pour un signal lumineux faible.

5.2.2 Caractéristiques I-V de l'APD et circuit appliqué

Une APD en absence de la lumière incidente a les caractéristiques I-V similaires à celles qui sont représenté théoriquement sur la figure 5-7. Cependant, quand le dispositif absorbe des photons dus à la lumière incidente, les caractéristiques seront décalées en bas. Heureusement, ce décalage est fortement linéaire avec l'intensité de la lumière absorbée. En outre, les nouvelles courbes décalées sont parallèles avec les courbes originales.

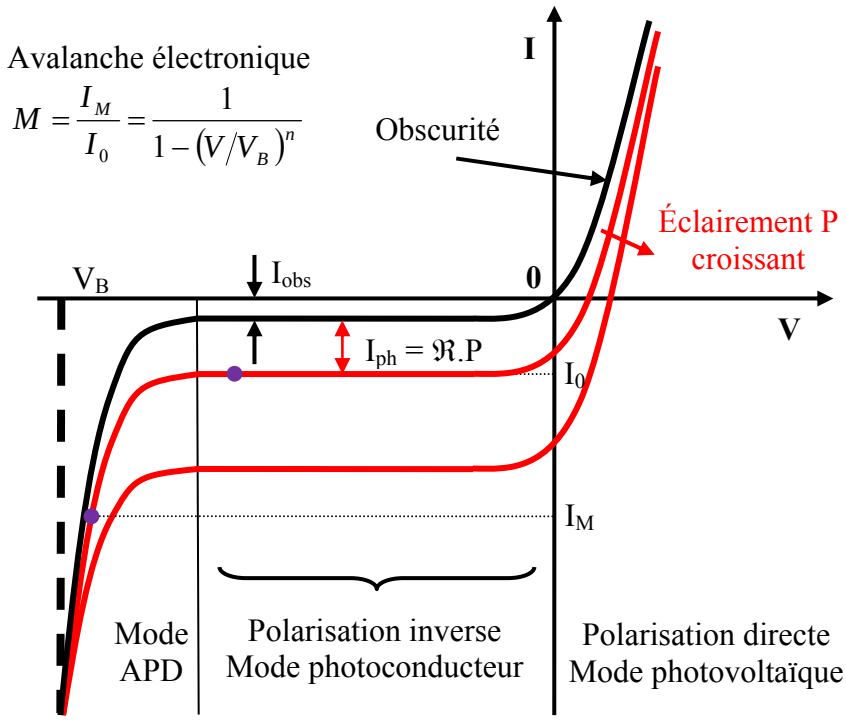


Figure 5-7. Caractéristique I-V d'une photodiode en modes photovoltaïque, photoconducteur et à avalanche.

Sur le système ci-dessus, la photodiode est représentée conventionnellement en direct, le fonctionnement inverse étant obtenu avec une tension de polarisation négative. Dans la pratique, la photodiode est le plus souvent montrée en inverse avec une polarisation positive (fig. 5-8).

Le photocourant à travers de l'APD est donné par

$$I_{ph} = \eta M \frac{q}{hc} \lambda P \qquad (5\text{-}2\text{-}5)$$

où η est l'efficacité quantique, M est le gain interne de l'APD, h est la constante de Planck, c est la vitesse de la lumière dans le vide, λ est la longueur d'onde de lumière incidente, et P est la puissance optique incidente.

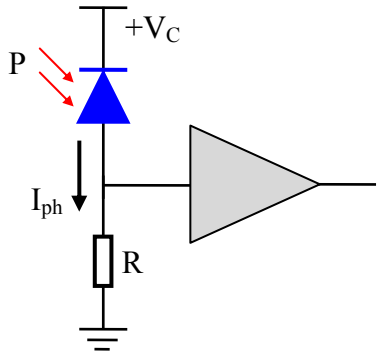


Figure 5-8. Représentation de la photodiode en inverse avec une tension de polarisation positive.

En sachant la surface sensible A de l'APD, la puissance optique peut être liée à l'intensité de la lumière I (W/m^2) par

$$P = IA \tag{5-2-6}$$

Par définition, la réponse du détecteur $\Re$ (A/W) peut être obtenue à partir de l'équation (5-2-5) et s'exprime par

$$\Re = \frac{I_{ph}}{P} = \eta M \frac{q}{hc}\lambda \tag{5-2-7}$$

Ainsi, dans la plupart des applications, une polarisation inverse importante est appliquée à l'APD, de l'ordre de la tension de claquage V_B. La variation de courant de l'APD, représentant le changement de l'intensité lumineuse, est ensuite convertie en variation de tension par un convertisseur de courant-tension ou un montage de type amplificateur de transimpédance. Cette configuration est montrée dans la figure 5-9 où R_f est la résistance de rétroaction de l'amplificateur, et R et C jouent le rôle d'un filtre passe-bas qui élimine tout bruit d'ondulation de la polarisation. Parmi les inconvénients de cette technique citons le bruit additionnel lié à l'amplificateur ainsi que la limitation dans la réponse fréquentielle.

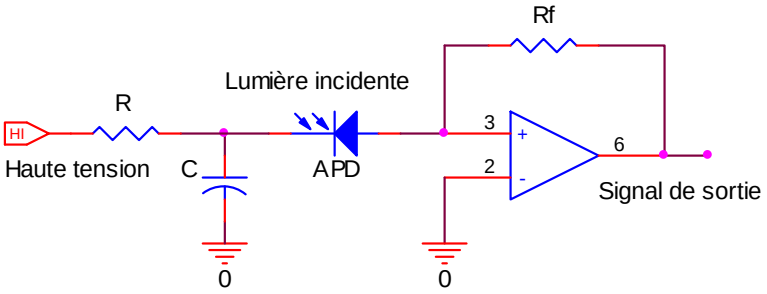


Figure 5-9. Circuit électrique utilisant l'APD. R et C éliminent le bruit de la polarisation (filtre passe-bas) ; R_f est la résistance de rétroaction ; montage de type amplificateur de transimpédance.

5.2.3 Bande passante de l'APD

L'intérêt des photodiodes à avalanche est leur grand gain, ce qui permet de détecter des signaux de très faible intensité. En revanche le prix à payer est en termes de bande passante, car ces composants ont une bande passante plus faible que celle des photodiodes PIN classiques. La bande passante des photodiodes à avalanche est limitée par trois facteurs :

a) Le temps de transit des électrons à travers la zone absorbante de la jonction :

$$\tau_{\text{transit}} = \frac{W_{\text{zone absorbante}}}{v_{\text{électrons}}} \tag{5-2-8}$$

b) Le temps nécessaire à l'installation du phénomène d'avalanche : $\tau_{\text{avalanche}}$

c) Le temps de transit des trous générés lors du phénomène d'avalanche nécessaire pour rejoindre la zone P en traversant la zone d'absorption et la zone d'avalanche :

$$\tau_{\text{trous}} = \frac{W_{\text{zone absorbante}} + W_{\text{zone d'avalanche}}}{v_{\text{trous}}} \tag{5-2-9}$$

Le retard temporel lié à $\tau_{\text{avalanche}}$ dépend du gain M. Si M électrons sont générés, il faut attendre qu'il soit tous sortis de la zone d'avalanche, soit approximativement M fois le temps de transit d'un seul électron. $\tau_{\text{avalanche}}$ dépend aussi de la différence entre le taux de génération des électrons et le taux de génération des trous (on comprend que si les trous sont générés moins vites que les électrons cela ralenti le processus), mais en première approximation on les considérera égaux. On considérera donc également que leur vitesse de transit est égale ($v_{électrons} = v_{trous}$). D'où

$$\tau_{\text{avalanche}} = \frac{MW_{\text{zone d'avalanche}}}{v_{\text{électrons}}} \tag{5-2-10}$$

Le temps total de réponse est donc :

$$\tau_{total} = \frac{W_{\text{zone absorbante}} + MW_{\text{zone d'avalanche}}}{v_{\text{électrons}}} + \frac{W_{\text{zone absorbante}} + W_{\text{zone d'avalanche}}}{v_{\text{trous}}} \tag{5-2-11}$$

Le facteur de multiplication d'avalanche est défini :

$$M = \frac{\text{photocourant multiplié}}{\text{photocourant miltiplié primaire}} \text{ et } M = \frac{1}{1-\left(\frac{V}{V_B}\right)^n} \tag{5-2-12}$$

où V_B est la tension de claquage, V est la tension appliquée à l'APD et n est un index caractéristique dépendant de la température. Il est important de noter que pour les larges valeurs de gain, la grandeur M/τ est constante. Ainsi pour les photodiodes à avalanche avec un grand gain le produit gain bande reste constant.

5.2.4 Caractéristiques de l'APD utilisée

Dans notre système de détection optique nous avons utilisé la photodiode à avalanche Fujitsu InGaAs-FPD5W1KS dont la photo est dans la figure 5-10. Le FPD5W1KS est une photodiode d'avalanche InGaAs de large bande et de haute sensibilité, optimisée pour l'opération à 1,55 μm.

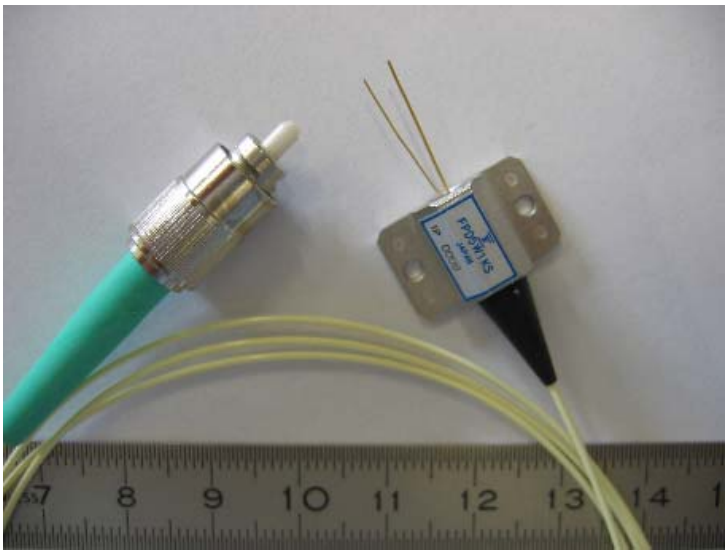


Figure 5-10. Photodiode à avalanche Fujitsu FPD5W1KS, à 1550 nm.

Cette APD est conçue pour l'usage dans les systèmes optiques de transmission fonctionnant à la gamme de gigabit, au-dessus de 2,4 Gb/s, et pour de longues distances de transmission. Le chip d'APD a une zone active de diamètre de 30 μm.

Ses caractéristiques [89] :

- Atténuation de réflexion optique (ORL) = 30 dB (1550 nm et 1310 nm)
- Zone active de l'APD est de diamètre de 30 μm
- Courant direct = 10 mA,
- Courant inverse = 1 mA
- Sensibilité $\Re$ = 0,88 A/W (à 1550 nm et M = 1)
- Tension de claquage = 47 V
- Le courant d'obscurité : I_{obs} = 10 nA (25 °C, M = 1)
- Fréquence de coupure ($M \leq 10$, -3 dB, 50Ω) : f_C = 2,5 GHz
- Capacité terminale (f = 1 MHz) : C_t = 0,5 pF
- Puissance équivalente de bruit NEP = 2.10^{-15} W/Hz$^{1/2}$
- Facteur de l'excès de bruit : F = 6,3 (1550 nm, M = 10, f = 30 MHz)

5.3 Photodétecteurs supraconducteurs

5.3.1 Généralités

Un autre détecteur potentiel pour le comptage de photons individuels est basé sur le supraconducteur. La capacité de comptage de photons de ces deux technologies de détecteurs de photons uniques supraconducteurs (SSPD – Superconducting Single Photon Detectors) se prolonge bien dans l'infrarouge. Les SSPD [90-92] ont une efficacité de détection inférieure (jusqu'à 20% dans le visible) [91] et les coups d'obscurité finis, mais ils sont potentiellement extrêmement rapide (près de la fréquences d'horloge de télécommunication ~ 1 GHz) [90] ; la largeur FWHM est de 20 ps [92], température de service est d'environ 4 K.

5.3.2 Description du dispositif

Les couches supraconductrices fabriquées en 2004 par G. Goltsman *et al.*, [93] utilisées pour la détection de photons uniques se composent de pistes de supraconducteur de nitrite de niobium (NbN possédant une température de transition de l'ordre de 10 K) d'une longueur de quelques microns, de largeur 100-150 nm et d'épaisseur 3,5-10 nm déposées sur un substrat de saphir. Ces pistes sont traversées par un courant légèrement inférieur au courant critique à une température de l'ordre de 4 K.

5.3.3 Principe de fonctionnement

Le dispositif fonctionne à une température au-dessous de la température critique T_C du matériel, dans un régime où le courant de polarisation I est près de la valeur du courant critique I_C.

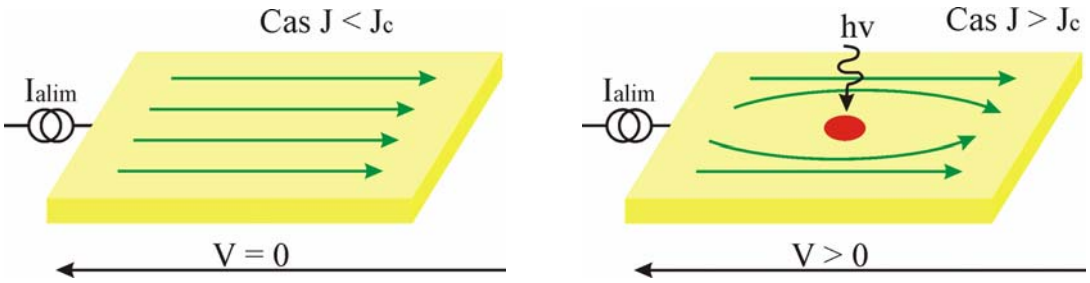


Figure 5-11a) Figure 5-11b)

Figure 5-11. Schémas de la formation du point chaud et d'une barrière résistive dans une piste supraconductrice ultra-mince maintenus à une température au-dessous T_C. Les flèches indiquent le sens d'écoulement d'un super courant polarisant la piste [98]. La piste est composée par une couche ultramince (< 10 nm) de NbN à condition $T < T_C$. a) Régime supraconducteur ; b) Régime de détection de photon : l'énergie déposée par le photon supprime la supraconductivité (thermalisation en 20 ps).

L'absorption d'un quantum $h\nu$ de lumière par une paire de Cooper crée un électron fortement excité dont l'énergie est proche de l'énergie du photon incident, et mène à la formation d'un « point chaud » (hot spot) [94] où la supraconductivité est supprimée ou

même détruite. L'électron excité perdra son énergie par la dispersion électron-électron et électron-phonon, et crée donc des électrons excités secondaires (des quasi-particules) alors que les électrons chauds répandent hors du noyau de point chaud. Quand l'énergie moyenne des quasi-particules dans la cascade diminue vers la 2Δ (qui est la bande interdite des paires de Cooper et est en général deux à trois ordres de grandeur inférieure à la bande interdite de la plupart des semi-conducteurs), leur nombre augmente, atteignant idéalement $h\nu/2\Delta$, et leur température effective T_e dépasse la température critique T_C. Le super courant, qui polarise le dispositif, est expulsé du volume résistif de point chaud et est concentré dans les « trottoirs » près des bords de la couche (fig. 5-11). Si la densité de courant après cette redistribution dépasse la valeur critique en dehors du point chaud, la supraconductivité est détruite, et la barrière résistive est formée à travers la largeur entière du dispositif, qui, à son tour, provoque un signal de tension avec l'amplitude proportionnelle à *I*. Après la croissance, le point chaud diminue de taille (extinction), ce qui est dû à la relaxation et refroidissement des électrons excités et de leur diffusion. Ainsi, après un temps de relaxation des quasi-particules d'environ 30 ps [95], le point chaud s'effondre, la supraconductivité (état nul de tension) est rétablie, et le détecteur est prêt à enregistrer un autre photon [93, 96-97].

5.3.4 Propriétés

Suivant l'écart au courant critique, l'apparition d'une tension peut nécessiter l'impact de un ou plusieurs photons. On peut alors choisir de réaliser un compteur de photon linéaire, quadratique ou cubique sensible respectivement à un, deux ou trois photons [93]. Cette possibilité de comptage de photon non-linéaire offre des possibilités très intéressantes pour des expériences d'optique quantique originales utilisant des interférences à plusieurs photons permettant de mettre en évidence la longueur d'onde lambda/N d'un état de Fock à N photons. Ces effets peuvent avoir des applications pour améliorer la résolution de processus de lithographie optique.

De plus, il apparaît que la forme de l'impulsion électrique générée en régime linéaire dépend de l'énergie lumineuse déposée et donc du nombre de photons absorbés [93]. Cette possibilité de résoudre le nombre de photons n'a encore jamais été démontrée, et constitue un point capital dans les propositions de portes logiques quantiques utilisant des interférences à plusieurs photons [40].

5.4 Modes fonctionnement de l'APD

On discute spécifiquement dans cette partie le mode comptage de photons et le régime d'extinction des APD pour la détection de photons uniques.

5.4.1 Mode linéaire de l'APD

Dans ce cas l'APD est inversement polarisée au-dessous de sa tension de claquage V_B. Chaque photon absorbé crée en moyenne un nombre fini M de paires d'électron-trou. Le gain interne M vaut typiquement des dizaines ou centaines. Puisque le photocourant moyen est strictement proportionnel au flux optique incident, ce mode de fonctionnement est connu en tant que mode linéaire.

5.4.2 Mode Geiger ou mode comptage de photons

Dans le mode Geiger [99-102], une APD est inversement polarisée au-dessus de sa tension de claquage ($V > V_B$) pour avoir un gain d'opération très élevé (10^5 à 10^6). Considérons ce qui se passe quand l'APD est inversement polarisée au-dessus de V_B en utilisant une alimentation électrique. Quand la polarisation inverse est supérieure à V_B, les électrons et les trous se multiplient par ionisation par choc plus rapidement, en moyenne, qu'ils ne peuvent être extraits. Ce critère est en fait la meilleure définition de la tension de claquage V_B de l'avalanche. Le diagramme d'espace-temps sur la figure 5-12 illustre ce concept.

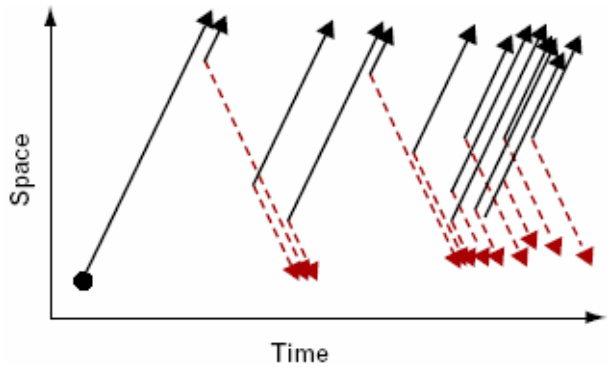


Figure 5-12. Concept de tension de claquage de l'avalanche. En mode Geiger, l'APD est alimentée au-dessus de la tension de claquage de l'avalanche. Quand la croissance de la population des électrons et des trous dus à l'ionisation par choc dépasse le taux auquel ils peuvent être extraits, il y aura la croissance exponentielle du courant.

La population des électrons et des trous dans la région de champ fort et le photocourant associé croissent exponentiellement dans le temps. Plus l'APD est polarisée au-dessus de V_B, plus la constante temporelle de croissance est grande. Par conséquent, une avalanche amorcée par l'absorption d'un seul photon provoque un courant croissant dans certaine résistance de valeur limite. Le temps d'établissement de ce courant est court, typiquement des dizaines de picosecondes.

Cependant, une simple connexion d'une APD avec une alimentation de basse impédance, ne donne aucune manière à mesurer le temps de mise en service ni éteindre l'avalanche pour que l'APD soit prête à détecter d'autres photons. L'arrêt de l'avalanche s'appelle *extinction* (quenching), et est accompli par deux types de circuit : *extinction passive* (passive quenching – PQC) et *extinction active* (active quenching – AQC).

5.4.3 Mode d'extinction passive

Le principe de fonctionnement d'une APD en mode de comptage de photons (dit également mode Geiger) avec l'extinction passive a été discuté ailleurs [81, 103-104]. Le circuit qui éteint l'avalanche et remet à zéro la tension de polarisation joue un rôle principal dans la performance du détecteur de photons uniques SPAD (Single Photon Avalanche Diode). Une analyse et une discussion complètes de ce sujet peuvent être trouvées dans [103] et les résultats principaux seront résumés ici. Les premières études sur des diodes d'avalanche

en mode Geiger ont utilisé le circuit d'extinction passive (PQC) simple, décrit sur la figure 5-13 suivante :

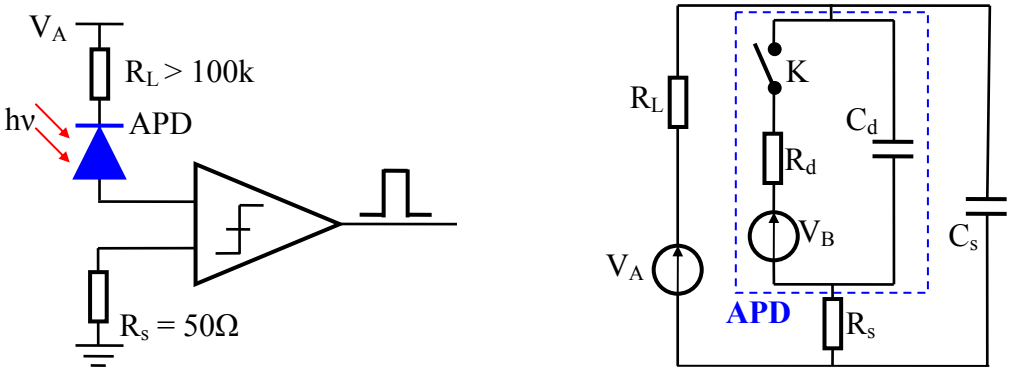


Figure 5-13. Le circuit d'extinction passive et son schéma équivalent [103]. V_A : polarisation inverse, V_B : tension de claquage ; R_d : résistance interne de l'APD ; C_d : capacité de l'APD ; C_s : capacité parasite par rapport à la masse. La diode est polarisée au-dessus de la tension de claquage et reste là jusqu'au moment où un événement de photodétection ou un bruit crée une paire électron-trou dans la région d'avalanche. Ces porteurs de charge se déplacent dans la diode. Ils sont accélérés par la tension appliquée et peuvent atteindre une énergie suffisante pour libérer d'autres électrons et trous par l'excitation de collision.

Dans ce circuit, le courant d'avalanche est simplement éteint par une tension appliquée sur une haute impédance R_L de valeur 33k [104] ou 100k [103] ou plus [81].

La polarisation est appliquée à travers d'une résistance de stabilisation R_L dont la valeur est grande ; une petite résistance R_S est reliée à l'autre borne de l'APD pour observer l'impulsion de courant. Le courant d'avalanche décharge la capacité totale C_T sur la borne de la diode, où C_T est la somme de la capacité de jonction C_J et la capacité parasite C_S. La tension sur la diode diminue vers V_B et le courant d'avalanche diminue également. Quand la tension approche V_B alors le taux de diminution ralentit ; pratiquement, tout le courant d'avalanche traverse R_L et est réduit à la valeur $(V_A - V_B)/R_L$. Si R_L est assez grande pour ramener le courant à environ 20 µA, le nombre de porteur d'avalanche est petit, la probabilité de l'interruption de la chaîne de multiplication est élevée et finalement l'avalanche est éteinte. La tension commence donc à se retrouver lentement vers la polarisation V_A pendant un temps constant $R_L C_T$.

Les inconvénients de l'extinction passive peuvent être réduits, bien que non éliminés, avec les technologies de circuit modernes qui réduisent de manière significative la capacité parasite C_S et rendent plus rapide le rétablissement. Avec les techniques du montage en surface et des composants miniatures, la C_S peut être réduite à quelques picofarads. L'intégration monolithique du détecteur et de la résistance de stabilisation, possible à nos jours au moins pour le SPAD basant sur le silicium, peut réduire le C_S bien au-dessous de 1 pF.

L'avalanche déclenchée correspond à la fermeture de l'interrupteur K dans le circuit équivalent (fig. 5-13). La chute de tension sur R_L pendant la durée de l'avalanche diminuera la tension aux bords de l'APD à une valeur inférieure à la tension de claquage V_B, L'effet d'avalanche est donc éteint. La figure 5-14 nous montre les courbes du courant I_d et de la tension V_d ou la tension d'excès $V_{ex} = V_d - V_B$ de la diode.

$$I_d(t) = \frac{V_d(t) - V_B}{R_d} = \frac{V_{ex}(t)}{R_d} \tag{5-4-1}$$

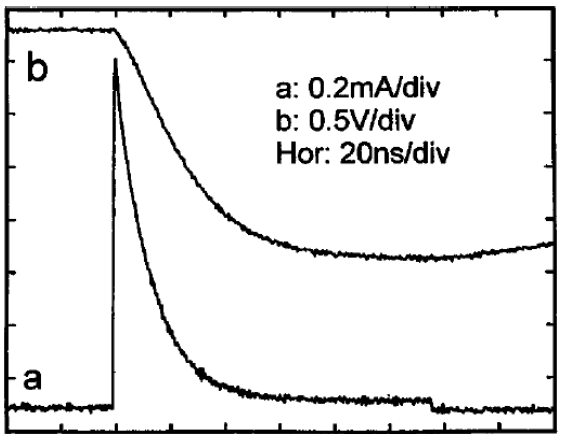


Figure 5-14. a) le courant d'avalanche I_d et b) la tension V_d de la diode [103].

a) Transition d'extinction

Le courant d'avalanche décharge les condensateurs C_d et C_S, donc V_d et I_d diminuent en fonction exponentielle à la valeur V_f et I_f.

$$I_f = \frac{V_A - V_B}{R_d + R_L} \cong \frac{V_E}{R_L} \tag{5-4-2}$$

et

$$V_f = V_B + R_d I_f \text{ car } R_L >> R_d \tag{5-4-3}$$

Le temps d'extinction T_q est constant et s'exprime comme :

$$T_q = (C_d + C_S)\frac{R_d R_L}{R_d + R_L} \cong (C_d + C_S)R_d \tag{5-4-4}$$

Si I_f est très petit, V_f est approximativement égal à V_B. Quand $V_d(t)$ s'approche à la valeur de V_B, l'intensité $I_d(t)$ devient petite et le nombre de porteurs qui peuvent passer dans la région d'avalanche est aussi petit, le processus d'avalanche est donc faible. Comme le processus de l'avalanche est statistique et il peut-être donc n'y a pas de porteur qui a assez

d'énergie pour pouvoir ioniser par choc. Quand le courant est inférieur à I_q (le courant éteint, I_q < 100 µA, I_q n'est pas défini exactement), il se passe qu'il n'y a plus assez de porteurs passant à travers la région au champ électrique élevé qui puissent avoir assez d'énergie pour ioniser les autres par choc. Alors I_d va diminuer rapidement et l'avalanche va être éteinte. La valeur de la tension V_q (qui est équivalant au courant I_q) est :

$$V_q = V_B + I_q R_d \tag{5-4-5}$$

Le total de la charge Q_{pc} pendant la durée d'impulsion d'avalanche est :

$$Q_{pc} = (V_A - V_q)(C_d + C_s) \cong V_E(C_d + C_s) \cong I_f T_r \tag{5-4-6}$$

avec :

$$T_r = R_L(C_d + C_s) \tag{5-4-7}$$

T_r est le temps de décharge. Donc, le temps mort du circuit d'extinction passive est :

$$T_{mort} = T_q + T_r = (R_L + R_d)(C_d + C_s) \tag{5-4-8}$$

Il faut remarquer que :

- V_B est la tension de seuil de la polarisation pour détecter de photons arrivés ; elle est aussi le seuil de la tension pour accélérer des porteurs à un niveau, qui peuvent ioniser les autres par choc.
- V_q est le seuil de la tension équivalente au courant I_q qui est le courant d'éteindre l'effet d'avalanche. En réalité, $V_q - V_B \geq 0$.

b) Impulsion à la sortie

On peut obtenir les impulsions à la sortie du circuit PQC via R_s (fig. 5-13). La valeur convenable de R_s est de 50 Ω. Le signe d'impulsion (moins ou plus) à la sortie peut être changé par le montage de la photodiode. L'impulsion est une copie déjà atténuée de la forme d'onde de la tension de photodiode. Donc, on dit que l'on a une sortie en mode tension, avec pour tension pic V_u :

$$V_u = (V_A - V_B - I_q R_d)\frac{R_s}{R_L + R_s} \cong V_E \frac{R_s}{R_L} \cong I_f R_s \tag{5-4-9}$$

Comme I_f est très petit, quand R_s ~ 50 Ω alors $V_u \cong$ 1 mV et on ne peut pas se connecter à un comparateur externe en utilisant un câble coaxial. Il faut diminuer le seuil détecté de la tension [103].

5.4.4 Mode d'extinction active

Une solution qui a complètement évité les inconvénients de l'extinction passive était le circuit d'extinction active (AQC), conçu d'abord en 1975. Le principe est simple : pour détecter la montée de l'impulsion d'avalanche et réagir sur le Single Photon Avalanche Diode (SPAD), on impose l'extinction avec une source de polarisation commandée et remet les transitions d'extinction dans temps courts.

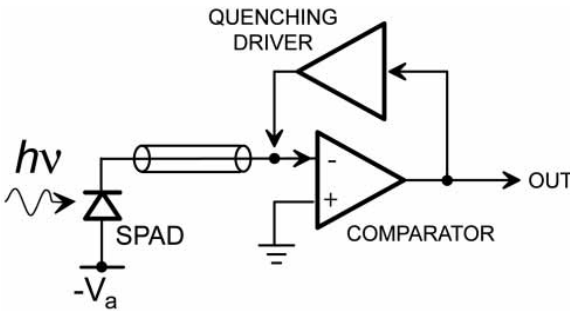


Figure 5-15. Circuit d'extinction active de la photodiode à avalanche [105].

Comme la figure 5-15 a montré, le comparateur de détection envoie une commande à un pilote de tension, qui commute la polarisation au-dessous de la tension de claquage V_B. Après une durée de retenue exactement commandée, la polarisation est commutée de nouveau au niveau de fonctionnement V_A. Une impulsion standard synchrone à la montée de l'avalanche provenant de la sortie du comparateur est utilisée pour le comptage de photons et synchronisation. La proposition est assez simple et soutient une certaine similitude à une approche utilisée dans le passé pour travailler avec de véritables détecteurs de gaz de Geiger-Müller des radiations d'ionisation. Cependant, les problèmes complètement nouveaux surviennent avec SPAD, à cause de l'échelle de temps beaucoup plus rapide et du rôle joué par des capacités, comme discuté dans [103]. Les avantages fondamentaux offerts par l'approche d'AQC sont les transitions rapides de l'état éteint au niveau de fonctionnement et réciproquement, la durée courte et bien définie du courant d'avalanche et du temps mort.

Plusieurs travaux ont réalisé avec l'AQC la synchronisation photonique de haute résolution [84] et le déclenchement rapide du détecteur [106] et, en examinant les caractéristiques essentielles des circuits, Cova *et al.* [84] ont présenté la terminologie des circuits d'extinction active et d'extinction passive maintenant universellement adoptés.

Afin de réaliser la haute résolution en photon synchronisation, le circuit devrait extraire l'information de temps à partir de la première partie de la montée de l'avalanche. Cette condition peut être en conflit avec d'autres contraintes réglées sur la conception d'un AQC. En fait de diverses AQC ne peuvent pas exploiter la performance de synchronisation démontrée pour le détecteur SPAD à faible taux de comptage avec un PQC simple [107]. Une approche simple a été conçue pour surmonter cette limite et faire breveter [108].

5.4.5 Un modèle typique d'extinction active

Le but d'un circuit d'extinction est de contrôler la polarisation de la diode en fonction du courant qui la traverse. Le circuit abaisse la polarisation après la montée du courant d'avalanche et réapplique la polarisation originale après un retard fixé ou avant l'arrivée du

photon d'intérêt (en mode à déclenchements périodiques : gated mode). Le circuit d'extinction le plus simple est celui d'extinction passive.

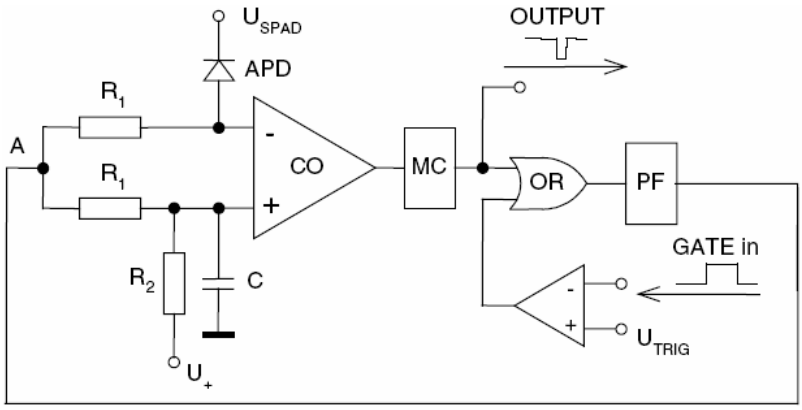


Figure 5-16. Schéma d'un circuit d'extinction active et de déclenchement. Des abréviations sont définies dans le texte. Les résistances R1 sont les charges d'entrée du comparateur [109].

Prochazka *et al.* [109] ont développé un nouveau circuit d'extinction active et de déclenchements périodiques spécifiquement design pour les structures de la diode SAM InGaAs/InP (SAM – Multiplication par absorption séparée). Le circuit a été optimisé du point de vue de la sensibilité avalanche-courant et de la charge totale traversant la diode après le claquage. Le schéma bloc du circuit est montré dans la figure 5-16. Le courant d'avalanche de l'APD est détecté par le comparateur (CO), sa sortie est prolongée par le circuit monostable (MC) et sa sortie est combinée dans le OU logique avec le signal de porte logique. La sortie de la porte logique OU commande un circuit de mise en forme d'impulsions (PF), qui contrôle la polarisation de l'APD. Le circuit de mise en forme d'impulsions permet l'ajustement du slew-rate auquel la diode est polarisée au-dessus du claquage pour réduire au minimum l'effet transitoire – cross talk – de la porte logique en commutation. Le seuil de déclenchement est très bien accordé par une résistance (R2) ; la capacité de l'APD est compensée par un condensateur réglable (C). Le circuit est élaboré sur une carte de circuit imprimé de la taille de 20 mm x 40 mm par la technique du montage en surface. La topologie du circuit et l'utilisation des composants actifs ultra-rapides sont essentielles.

Pour vérifier la rapidité du circuit d'extinction active, on peut remplacer l'APD par un condensateur de 100 pF. Le signal de déclenchement sera fourni par un générateur d'impulsion. Le condensateur a simulé l'APD comme une réponse à la porte logique selon signaux.

5.5 Bruit dans la détection photonique et les détecteurs

Le mot « bruit » désigne les signaux parasites de tous ordres, qui viennent se superposer au signal utile, issu d'un montage électronique. Le bruit existe également à l'intérieur de chaque composant du montage ou du système de détection de signaux optique et électronique.

5.5.1 Circuit d'amplification

Le circuit d'amplification de l'APD utilisant deux amplificateurs OPA846 est montré dans la figure 5-17 ci-dessous. La photo de ce circuit avec l'APD se trouve dans la figure 5-23 (p. 116).

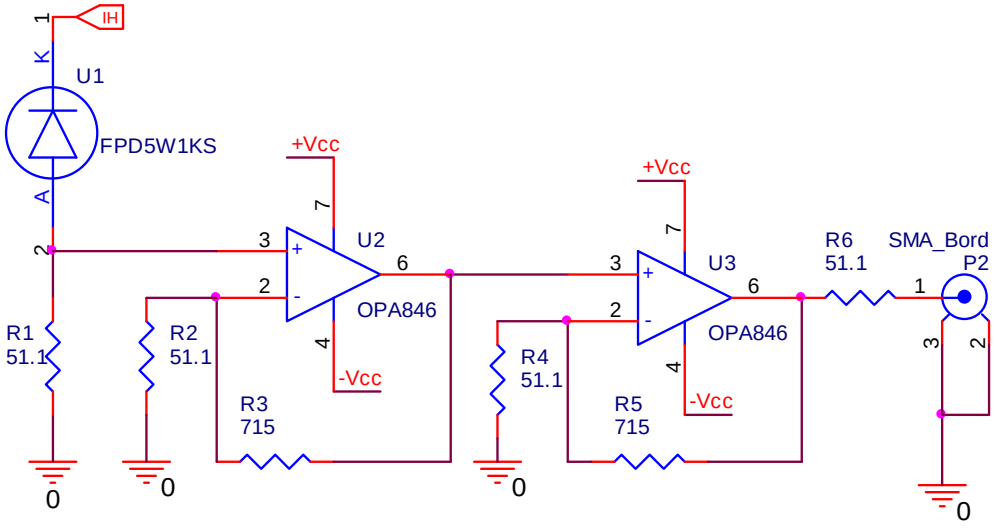


Figure 5-17. Circuit d'amplification électronique de la photodiode à avalanche utilisant OPA846.

Les amplificateurs OPA846 ont des caractéristiques suivantes :

- Bande passante = 400 MHz (pour un gain de 10).
- Produit gain-bande = 1750 MHz (pour un gain ≥ 40)
- Bruit d'entrée de tension V_{amp} = 1,2 $nV/\sqrt{Hz}$ à f > 1 MHz.
- Bruit d'entrée de courant I_{amp} = 2,8 $pA/\sqrt{Hz}$ à f > 1 MHz.
- Slew-rate = 625 V/µs.
- Courant d'alimentation = 12,6 mA.

L'ensemble (APD et son amplification) nous donne la capacité de détecter de faibles signaux de moins de 100 nW avec une bande passante de 110 MHz (fig. 5-25). La tension de sortie Vs du circuit ci-dessus a pour expression :

$$V_s = I_{ph} R_1 \left(1 + \frac{R_3}{R_2}\right)\left(1 + \frac{R_5}{R_4}\right) \qquad (5\text{-}5\text{-}0)$$

5.5.2 Principe de mesure

Le principe des systèmes de mesures de bruit du champ électromagnétique repose sur la détection d'intensité du champ et l'analyse spectrale des fluctuations de courant produites par le photodétecteur utilisé.

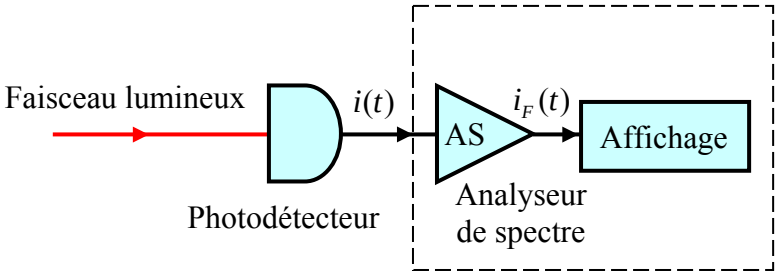


Figure 5-18. Un montage de détection simple. C'est une détection directe (mesure d'intensité) traitée par un analyseur de spectre.

Considérons un photodétecteur supposé parfait, c'est-à-dire de rendement quantique égal à l'unité. Supposons que tombe sur ce détecteur un mode transverse unique du champ, c'est-à-dire un champ de polarisation et de direction de propagation unique et fixée. Le détecteur est supposé suffisamment grand pour qu'il ne soit pas nécessaire de tenir compte de la structure transverse de ce mode. Ce qu'on obtient à la sortie de l'amplificateur est le photocourant $i(t)$ moyenné dans le temps.

$$\overline{i(t)} = \frac{1}{T}\int_{t-T}^{t} i(t')dt' \tag{5-5-1}$$

La variance du photocourant a pour expression :

$$(\Delta i)^2 = \overline{i^2} - \bar{i}^2 \tag{5-5-2}$$

La fonction de corrélation s'écrit :

$$C_i(t,t') = \overline{i(t).i(t')} - \overline{i(t)}.\overline{i(t')} \tag{5-5-3}$$

En régime stationnaire, la fonction de corrélation ne dépend que de la différence de temps $\tau = t' - t$. Par conséquent, on a

$$C_i(\tau) = C_i(t,t+\tau) = \overline{i(t).i(t+\tau)} - \overline{i(t)}.\overline{i(t+\tau)} \tag{5-5-4}$$

Le spectre de bruit du signal est la transformée de Fourier (TF) de la fonction d'auto-corrélation :

$$S_i[\Omega] = \int_{-\infty}^{+\infty} e^{i\Omega\tau} C_i(\tau)d\tau \tag{5-5-5}$$

Dans ce texte, on note Ω la fréquence de Fourier et ω, ω_0 … les fréquences optiques.
Les fluctuations du photocourant s'expriment par

$$\delta i(t) = i(t) - \overline{i(t)} \tag{5-5-6}$$

La TF nous donne

$$\delta i[\Omega] = \int_{-\infty}^{+\infty} e^{i\Omega t}\delta i(t)dt \tag{5-5-7}$$

En conséquence, le spectre de bruit se trouve lié à la transformée de Fourier des fluctuations par la relation suivante :

$$\overline{\delta i[\Omega]\delta i[\Omega']} = 2\pi\delta(\Omega - \Omega')S_i[\Omega] \tag{5-5-8}$$

Intuitivement, ceci traduit le fait que $S_i[\Omega]$ est proportionnel au carré des composantes de Fourier (énergie) des fluctuations à la fréquence Ω de bruit. On en déduit donc la variance du bruit :

$$(\Delta i)^2 = C_i(\tau = 0) = \frac{1}{2\pi}\int_{-\infty}^{+\infty} S_i[\Omega]d\Omega \tag{5-5-9}$$

Comme $S_i[\Omega]$ est souvent indépendant de Ω, l'expression de $C_i[\tau = 0]$ est une intégrale divergente. La fonction de transfert $H[\Omega]$ du filtre de l'amplificateur est définie par :

$$\delta i_F[\Omega] = H[\Omega]\delta i[\Omega] \tag{5-5-10}$$

Ainsi, la variance

$$(\Delta i_F)^2 = \frac{1}{2\pi}\int_{-\infty}^{+\infty} |H[\Omega]|^2 S_i[\Omega]d\Omega \tag{5-5-11}$$

n'est pas divergente. Cette variance (le bruit) est donc mesurable par l'analyseur de spectre électronique.

5.5.3 Mesure de bruit par analyseur de spectre

Expérimentalement, il est possible de tracer un spectre de bruit des fluctuations de l'amplitude du champ grâce à un analyseur de spectre. En effet, cet analyseur de spectre mesure la variance Δv_F des fluctuations, dans une bande de fréquence étroite, de la tension $v(t)$ produite par le passage du photocourant $i(t)$ dans une résistance de charge *R*. La bande de fréquence étroite mentionnée ci-dessus est déterminée par un filtre électronique *F* de largeur δf centré autour d'une fréquence d'analyse Ω_0 (fig. 5-19).
Alors, le calcul du spectre de bruit nous donne

$$(\Delta i_F)^2 = 2S_i[\Omega_0]\delta f \tag{5-5-12}$$

Donc,

$$S_i[\Omega_0] = \frac{(\Delta i_F)^2}{2\delta f} = \frac{(\Delta v_F)^2}{2R^2\delta f} \tag{5-5-13}$$

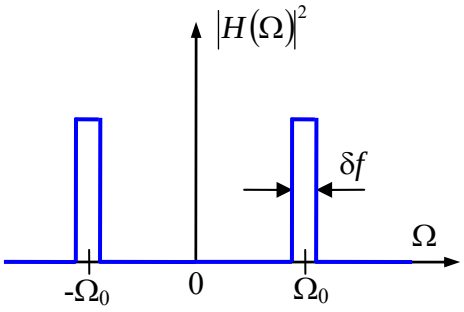


Figure 5-19. Fonction de transfert d'un filtre passe-bande.

Ici,

- δf *est connue sous nom de la bande de fréquence d'analyse (RBW).*
- F est un filtre passe-bande balayable.
- $S_i[\Omega]$ est exprimé en A^2/Hz .
- $\sqrt{S_i[\Omega]}$ est souvent utilisé (« amplitude » de bruit) et exprimé en $A/\sqrt{Hz}$.

Dans une expérience réelle, le bruit (et le signal) n'est pas en régime stationnaire : ses variances et densités spectrales de bruit varient au cours du temps. On effectue une deuxième moyenne VBW (Video Bandwidth) afin d'obtenir une valeur stable du bruit.

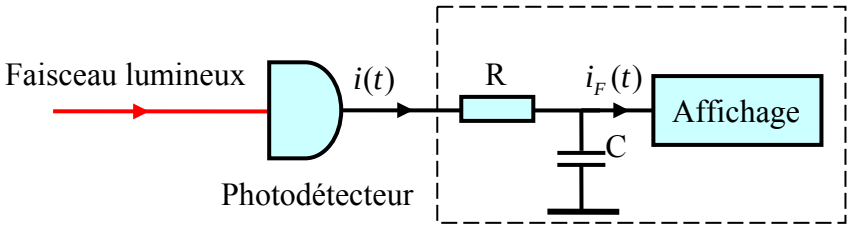


Figure 5-20. Photodétecteur suivie par un filtre passe-bas RC.

Pour la moyenne VBW, on utilise en principe un filtre passe-bas (fig. 5-20), on a :

$$i_F = \frac{1}{1+ jRC\Omega} i \tag{5-5-14}$$

et $H[\Omega] = \frac{1}{1+ j\Omega T}$ où $T = RC$. On va calculer :

$$(\Delta i_F)^2 = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \frac{S_i[\Omega]}{1+\Omega^2 T^2} d\Omega \tag{5-5-15}$$

Si $S_i[\Omega]$ varie peu avec le temps aux basses fréquences alors

$$\left(\Delta i_F\right)^2 = \frac{1}{2T} S_i\left[\Omega = 0\right] \tag{5-5-16}$$

De la même façon, si le signal est moyenné pendant un temps fini T

$$i_F(t) = \frac{1}{T} \int_{t-T}^{t} i(t')dt' \tag{5-5-17}$$

on a :

$$\left(\Delta i_F\right)^2 = \frac{1}{T} S_i\left[\Omega = 0\right] \tag{5-5-18}$$

La bande passante et l'inverse du temps de mesure sont à peu près équivalentes.

5.5.4 Calcul quantique de la densité spectrale de bruit

La fonction de corrélation s'exprime :

$$C_i(t,t') = \left\langle \hat{i}(t)\hat{i}(t') \right\rangle - \left\langle \hat{i}(t) \right\rangle \left\langle \hat{i}(t') \right\rangle \tag{5-5-19}$$

(moyenne quantique au lieu de la moyenne d'ensemble) ou plus de précision :

$$C_i(t,t') = \frac{1}{2}\left\langle \hat{i}(t)\hat{i}(t') + \hat{i}(t')\hat{i}(t) \right\rangle - \left\langle \hat{i}(t) \right\rangle \left\langle \hat{i}(t') \right\rangle \tag{5-5-20}$$

La densité spectrale de bruit a pour expression (5-5-5) : $S_i\left[\Omega\right] = \int_{-\infty}^{+\infty} e^{i\Omega\tau} C_i(\tau) d\tau$

Cas de lumière cohérente :

Un l'état cohérent du faisceau est défini par

$$\hat{\mathbf{E}}_k \left| \psi_{coh} \right\rangle = \left\langle \hat{\mathbf{E}}_k \right\rangle \left| \psi_{coh} \right\rangle \tag{5-5-21}$$

On trouve que

$$C_i(t,t') = q\left\langle \hat{i}(t) \right\rangle \delta(t-t') \tag{5-5-22}$$

et on en déduit

$$S_i\left[\Omega\right] = q\left\langle \hat{i} \right\rangle \tag{5-5-23}$$

Cela signifie qu'un faisceau des états cohérents est composé des photons de distributions aléatoires dans le temps et dans l'espace.

5.5.5 Bruit d'excès

Toutes les photodiodes à avalanche produisent du bruit d'excès dû à la nature statistique du processus d'avalanche. Le facteur de bruit d'excès est généralement dénoté comme F. Le facteur du bruit d'excès est une fonction du rapport d'ionisation de porteur, k, où k est habituellement défini comme rapport de probabilités d'ionisation des trous sur celle des électrons (k < 1). Le facteur du bruit d'excès peut être calculé en utilisant le modèle de [McIntyre] qui considère la nature statistique de la multiplication d'avalanche. Il est donné par :

$$F = k_{eff} M + \left(1 - k_{eff}\right)\left(2 - \frac{1}{M}\right) \tag{5-5-24}$$

Par conséquent, plus les valeurs de k et de M sont petites, plus le facteur du bruit d'excès est faible. Le facteur k efficace, k_{eff}, pour une APD peut être mesuré expérimentalement en adaptant la formule de McIntyre (5-5-24) à la dépendance du facteur de bruit d'excès du gain. C'est meilleur fait dans des conditions lumineuses. Il peut également théoriquement calculer à partir des coefficients d'ionisation de porteur et du profil de champ électrique de la structure d'APD.

5.5.6 Bruit dans la détection utilisant les APD et PIN

a) La puissance équivalente de bruit

Pour mesurer le bruit de détecteur, une bonne méthode est d'employer la NEP, la puissance équivalente de bruit, en unité watts$/\sqrt{\text{Hz}}$. La NEP est définie comme puissance incidente minimale exigée pour produire un photocourant égal au courant de bruit $I_{n(D)}$ du photodétecteur à la fréquence indiquée (f) et dans une largeur de bande spécifique Δf. La NEP pour un détecteur PIN et APD est calculée par la formule suivante :

$$NEP(\lambda, f, \Delta f) = \frac{I_{n(D)}}{R(\lambda)} \tag{5-5-25}$$

où $R(\lambda)$ est la sensibilité du photodétecteur (en A/W) et $I_{n(D)}$ est le courant total de bruit du photodétecteur. Les valeurs de la NEP peuvent varier de 10^{-11} W$/\sqrt{\text{Hz}}$ pour des photodiodes avec une grande surface active jusqu'à 10^{-15} W$/\sqrt{\text{Hz}}$ pour des photodiodes avec de petites surfaces actives. On a utilisé l'APD Fujitsu FPD5W1KS dont la NEP = quelques aW$/\sqrt{\text{Hz}}$ et la PIN G8376-03 dont le diamètre de la zone active = 0,3 mm et la NEP = 4 aW$/\sqrt{\text{Hz}}$.

Le bruit dans la combinaison de la figure 5-21 comprendra les composants de bruit suivants :

- bruit du détecteur : $I_{n(D)}$
- bruit thermique provenant de R_F et $I_{n(\text{rétroaction})}$
- bruit de l'amplificateur $I_{n(\text{ampli})}$

Le bruit généré par une photodiode planar fonctionnant en alimentation inverse est une somme de bruit de grenaille et bruit thermique.

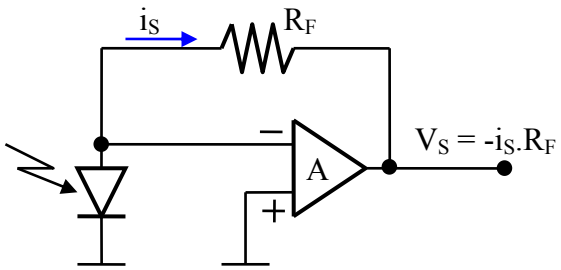


Figure 5-21. Combinaison photodétecteur-amplificateur (montage transimpédance).

b) Le bruit de grenaille

Ce bruit de grenaille (ou shot noise) est lié aux fluctuations statistiques à la fois du photocourant et du courant d'obscurité. L'amplitude du bruit grenaille est donné par la racine carré (rms) du bruit de courant :

$$I_{n(\text{shot noise})} = \sqrt{2q(I_p + I_d)\Delta f} \quad (\text{en } A/\sqrt{\text{Hz}}) \qquad (5\text{-}5\text{-}26)$$

où q = 1,6.10^{-19} C, I_p est le photocourant en ampères, I_d est le courant d'obscurité du photo-détecteur en ampères et Δf est la largeur spectrale du bruit en Hertz. Le bruit de grenaille est la source de bruit dominante pour le mode photoconductif (polarisation inverse).

c) Le bruit thermique

A chaque résistance shunt ou de rétroaction d'un photodétecteur est associé un bruit Johnson. En effet l'augmentation de température générée par effet Joule, peut provoquer par génération thermique de nouveaux porteurs. L'amplitude du bruit de courant ainsi généré est :

$$I_{n(\text{rétroaction})} = \sqrt{\frac{4k_B T\Delta f}{R_{SH}}} \quad (\text{en } A/\sqrt{\text{Hz}}) \qquad (5\text{-}5\text{-}27)$$

où k_B = 1,38.10^{-34} J/K est la constante de Boltzmann, T est la température absolue en degré Kelvin (273 K = 0 °C), Δf est la largeur spectrale du bruit et R_{SH} est la résistance shunt ou de rétroaction de la photodiode. Ce type de bruit est le bruit de courant dominant en mode photovoltaïque (non polarisé).

Note : Toute résistance est associée à un bruit Johnson, y compris la résistance de charge. Ce courant supplémentaire de bruit est grand et s'ajoute au bruit de courant Johnson provoqué par la résistance R_{SH} du photodétecteur. La résistance R_{SH} est aussi une fonction de la température dans les détecteur basés sur InGaAS, Ge et Si. Typiquement, quand la température diminue alors R_{SH} augmente et donc, d'après éq. 5-5-27, on voit que le bruit du détecteur diminue.

d) Le bruit de l'amplificateur

La dernière contribution du bruit total est le bruit de l'amplificateur. Ce bruit dépend évidemment du type de l'amplificateur utilisé et est une fonction de la fréquence. Il a pour expression :

$$I_{\text{n(ampli)}} = \sqrt{\left\langle I_{amp} \right\rangle^2 + \left\langle V_{amp} \omega C_T \right\rangle^2} \quad (\text{en } \text{A}/\sqrt{\text{Hz}}) \tag{5-5-28}$$

où I_{amp} est le courant de fuite d'entrée de l'amplificateur, V_{amp} est la tension de bruit d'entrée de l'amplificateur, $\omega = 2\pi f$ où f est la fréquence, C_T est la capacité d'entrée vue par l'amplificateur. Tous les deux I_{amp} et V_{amp} dépendent du type de l'amplificateur opérationnel utilisé. Leurs valeurs sont fournies par le fabriquant.

e) Le bruit total

Le bruit total de courant du système photométrique, c'est-à-dire, la photodiode + la résistance de rétroaction + amplificateur opérationnel, est donné par (en $\text{A}/\sqrt{\text{Hz}}$) :

$$I_{\text{bruit total}} = \sqrt{\left\langle I_{n(D)} \right\rangle^2 + \left\langle I_{n(\text{rétroaction})} \right\rangle^2 + \left\langle I_{n(ampli)} \right\rangle^2} \tag{5-5-29}$$

Le bruit total du système photométrique dépend du détecteur, de la résistance et de l'ampli opérationnel utilisé. Le refroidissement du système diminuera le bruit et augmenter donc la stabilité. On s'aperçoit clairement (d'après éq. 5-5-28) que le bruit de l'amplificateur dépend de la fréquence de fonctionnement.

f) Origine des coups d'obscurité

Dans les détecteurs d'avalanche, les coups d'obscurité (dark counts) résultent de l'injection des porteurs de charge dans la jonction par trois différents phénomènes :

- Excitation thermique.
- Pénétration par effet tunnel en travers la zone de déplétion.
- Emission par centres pièges.

Le dernier phénomène donne naissance des après-impulsions (after-pulses) dans lequel la réémission des charges piégées au cours d'une avalanche se produit durant l'impulsion suivante et donne un coup. Cela entraîne une surestimation dans le taux de comptage. En mesurant l'intervalle de temps des événements de détection, Yoshizawa [110] est arrivé à baisser le taux d'erreur des après-impulsions à 2%.

5.5.7 Optimisation du montage de détection

Dans les applications comme dans la figure 5-17, on demande un système de bande passante minimum de 10 MHz et de faible bruit. Dans ce cas-là, la tension de bruit d'entrée de l'ampli OPA846 est très faible, sa fréquence de coupure est suffisante (cf. 5.5.9). De plus, le bruit de l'amplificateur croît comme carré de la capacité vue par l'amplificateur où capacité terminale (éq. 5-5-28). Par conséquent, si l'on désire un système de faible bruit, il faudrait une petite capacité terminale.

Minimiser le bruit de système consiste à :

- minimiser la température du détecteur et de la résistance de rétroaction.
- maximiser la résistance de shunt et de rétroaction du détecteur.
- minimiser le courant et la tension de bruit du préamplificateur.

Minimiser la température du détecteur et de la résistance de rétroaction peut être réalisé par le refroidissement thermoélectrique. Ceci devrait être fait si la réduction du bruit thermique réduira le bruit total du système. De l'équation 5-5-29, on le voit que le bruit total ne sera pas réduit si le bruit d'amplificateur est la contribution principale du bruit total. Par exemple, si le bruit d'amplificateur est un ordre de grandeur plus important que celui du détecteur et de la résistance de rétroaction alors la diminution de température pour abaisser le bruit du détecteur et de la résistance de rétroaction par un ordre de grandeur, aura seulement comme conséquence une amélioration de 1% du bruit total. Maximiser la résistance shunt et de rétroaction du détecteur abaissera le bruit du détecteur comme vu dans l'équation 5-5-27, mais la grande résistance augmentera le temps de réponse du système photométrique. Par conséquent, cette méthode n'est utile que dans le cas où les applications du système photométrique n'exigent pas un temps de réponse rapide. Minimiser le courant et la tension de bruit sera une solution coûteuse mais ceci devrait être fait si le bruit d'amplificateur est la contribution principale du bruit total. Si le bruit de détecteur est beaucoup plus grand que le bruit d'amplificateur, alors la réduction du bruit d'amplificateur n'aura aucun impact sur le bruit total (voir 5-5-29).

En résumé, des photodiodes d'avalanche (APD) sont bien appropriées aux applications à haute fréquence même si le bruit d'excès de l'APD (cf. 5.5.5) augmentera le bruit du détecteur. C'est parce que le bruit d'amplificateur, dans beaucoup d'applications, est beaucoup plus élevé que le bruit d'un détecteur PIN, et l'utilisation d'une APD donne une sensibilité accrue pour gains jusqu'au point où le bruit de l'APD est comparable à celui de l'amplificateur. La stabilisation de la température par refroidissement est nécessaire car elle éliminera des variations de la sortie par rapport aux changements de la température. La partie suivante présentera la méthode de refroidissement thermoélectrique pour l'APD.

5.5.8 Refroidissement thermoélectrique

Quand une APD est refroidie à de basses températures, son courant d'obscurité et le courant de bruit diminuent de manière significative [111-112], tandis que l'efficacité quantique diminue très légèrement [113]. Comme le bruit d'APD diminue aux basses températures, le bruit d'amplificateur devient le facteur dominant qui limite la performance de l'APD. En fait, dans la distribution des impulsions de sortie de l'APD pour les photons uniques, les impulsions de petite-hauteur ont plus de chance que celles de grande-hauteur [112]. Par conséquent, dans le mode de comptage de photons, diminuer le seuil du discriminateur entraîne une efficacité quantique plus élevée.

Le système de refroidissement thermoélectrique pour l'APD est représenté dans la figure 5-22. Il est composé de 2 modules Peltier montés en étage, 3 plaques de cuivre, un dissipateur et une thermistance. Le dissipateur est en aluminium ; sa résistance thermique de 1,8 °C/W assure une bonne évacuation de chaleur. Les deux modules Peltier de puissance 1,7 W et 10,5 W sont câblés en série. Les plaques de cuivre ont pour but d'optimiser la diffusion de chaleur entre les étages.

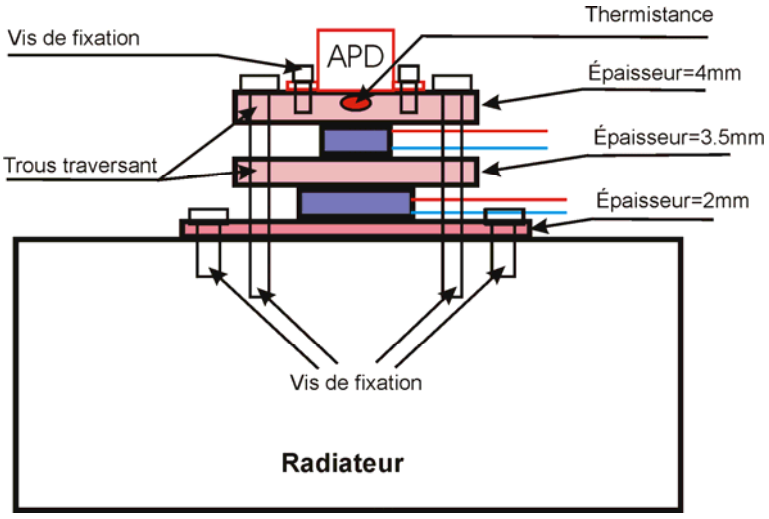


Figure 5-22. Refroidissement thermoélectrique pour l'APD. Le système est composé de 2 modules Peltier de puissance 1,7 W et 10,5 W, 3 plaques de cuivre, un dissipateur en aluminium de résistance thermique de 1,8 °C/W, la thermistance NTSA0XV103F - 10kΩ.

La thermistance 10 kΩ (ref. NTSA0XV103F) permet la température grâce à sa dépendance de sa résistance en température suivant l'expression :

$$R(T) = R_0 \exp\left\{B_{val}\left(\frac{1}{T} - \frac{1}{T_0}\right)\right\} \qquad (5\text{-}5\text{-}30)$$

où R est la résistance à la température T(K) exprimée en Kelvin, R_0 est la résistance à la température T_0(K), B_{val} est la constante d'énergie spécifique de la thermistance. Par exemple, la constante B_{val} de la thermistance NTSA0XV103F est de 3900K. La configuration montrée dans la figure 5-22 permet de maintenir facilement l'APD à la température de -10 degré ; dans ce cas-là, le système consomme un courant de 750 mA. L'asservissement de température est réalisé par le dispositif TED200 de la société Thorlabs. La figure 5-23 ci-dessous représente la photo de l'ensemble de l'APD, le circuit d'amplification utilisant l'amplificateur Burr-Brown OPA846 et le refroidissement thermoélectrique pour l'APD utilisant les deux étages de modules Peltier.

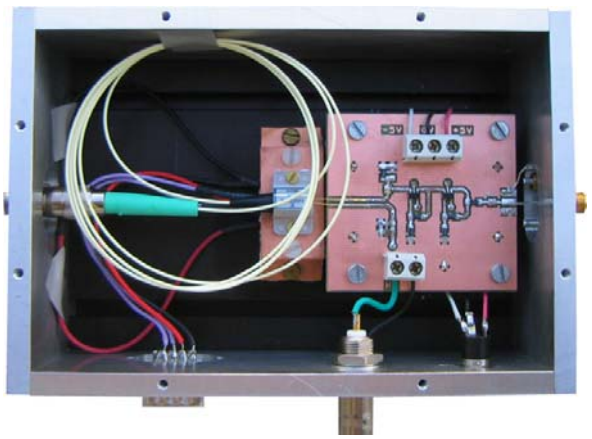


Figure 5-23. Photo du circuit d'amplification de l'APD et son système de refroidissement thermo-électrique.

5.5.9 Bande passante du circuit

a) Schéma de mesure

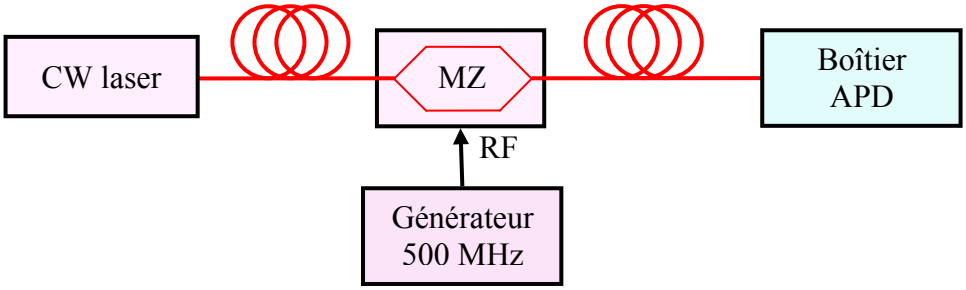


Figure 5-24. Schéma de mesure de la bande passante du boîtier contenant l'APD FPD5W1KS-1550 nm et son amplification avec OPA 846 (montage dans la figure 5-17). La tension de sortie du boîtier APD est visualisée et mesurée sur l'oscilloscope. Le signal RF est généré par le générateur de signaux HP8654A.

On utilise le montage de mesure ci-dessus (fig. 5-24) pour mesurer la bande passante du boîtier APD. Le signal optique incident de l'APD est modulé par l'intermédiaire d'un modulateur Mach-Zehnder.

b) Résultat

La bande passante du boîtier APD est donnée dans la figure 5-25. Elle correspond à ce que nous attendions (100 MHz) dans le cas où la polarisation de l'APD est supérieure à 27 V. Il semblerait que dans le cas où sa polarisation est inférieure à 27 V, l'APD subisse un effet capacitif important et sa bande passante est nettement plus faible (20 MHz à 25 V).

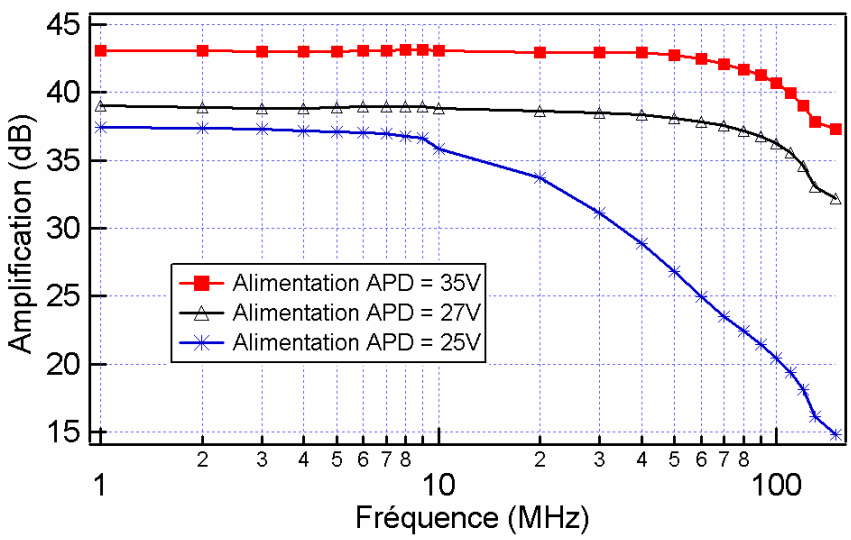


Figure 5-25. La bande passante du circuit d'amplification électronique pour l'APD FPD5W1KS-1550 nm (montage dans la figure 5-17). On gagne un gain d'environ 40 dB. La mesure est faite avec 3 valeurs différentes d'alimentation de l'APD : 25 V, 27 V et 35 V ; ce qui donne respectivement les bandes passantes (à -3 dB) de 20 MHz, 100 MHz et 110 MHz.

5.6 Détection de clés de cryptage

5.6.1 Montage de mesure

Une détection simplifiée de clés de cryptage a été mise en œuvre et est présentée dans les figures 5-26 et 5-27. Dans la partie d'émission la longueur d'onde λ_1 correspondant au premier ordre est utilisée comme la voie de clés de cryptage et modulée à l'aide d'un modulateur électro-optique. Ce dernier est commandé par une source de génération de codes binaires de 128 bits (boîtier CKG-1, cf. 4.6.3).

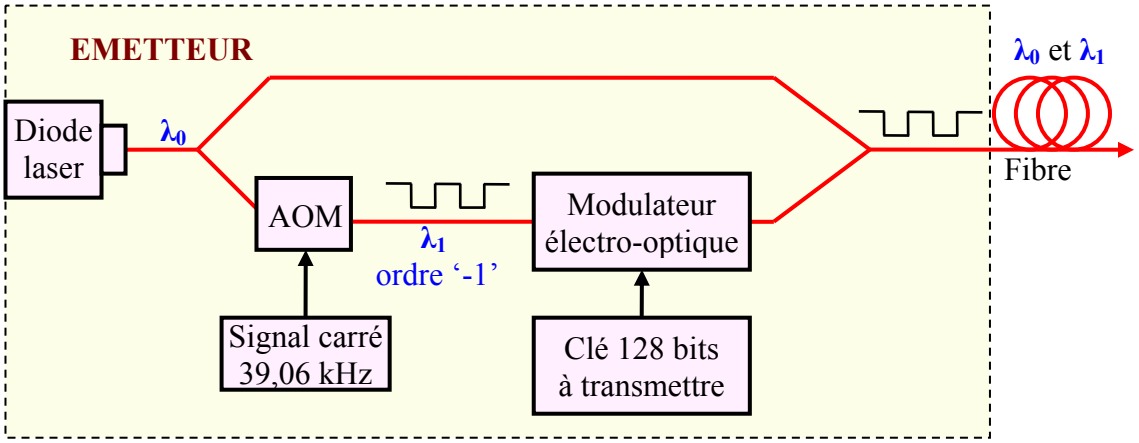


Figure 5-26. Schéma de la partie d'émission optique. Diode laser : FLD5F6CX, AOM : modulateur acousto-optique AA.MGAS. 110, modulateur électro-optique : Photline Mach-Zehnder MX-LN10, Clé de 128 bits : boîtier générateur CKG-1.

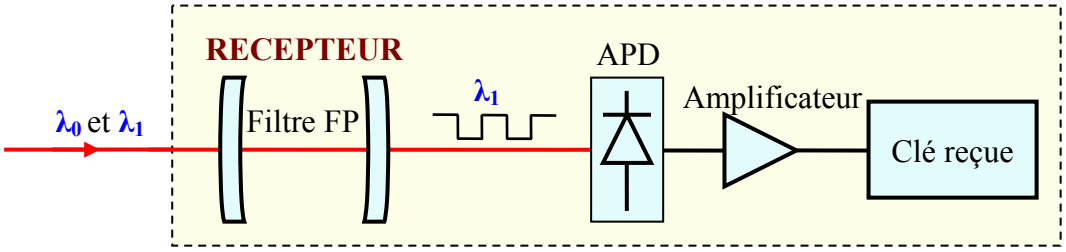


Figure 5-27. Schéma de la partie de réception. Filtre de haute résolution : cavité Fabry-Pérot confocale, APD : FPD5W1KS, amplificateur : OPA846.

La diode laser alimentée par un courant de 125 mA fournit une puissance optique de 5,53 mW. Le boîtier CKG-1 fournit à la fois un signal de type TLL pour commander l'AOM et une clé de cryptage pour moduler l'intensité optique du Mach-Zehnder. Du côté récepteur, la cavité Fabry-Pérot est sous haute tension continue qui est réglable de 0 à 900 V pour pouvoir choisir la bonne longueur d'onde. Le détecteur (APD) est maintenu à la température de zéro degré et polarisé sous 42 V près du seuil de claquage. La figure 5-28 représente la photo de l'ensemble de montage réalisé au laboratoire SATIE de l'ENS de Cachan.

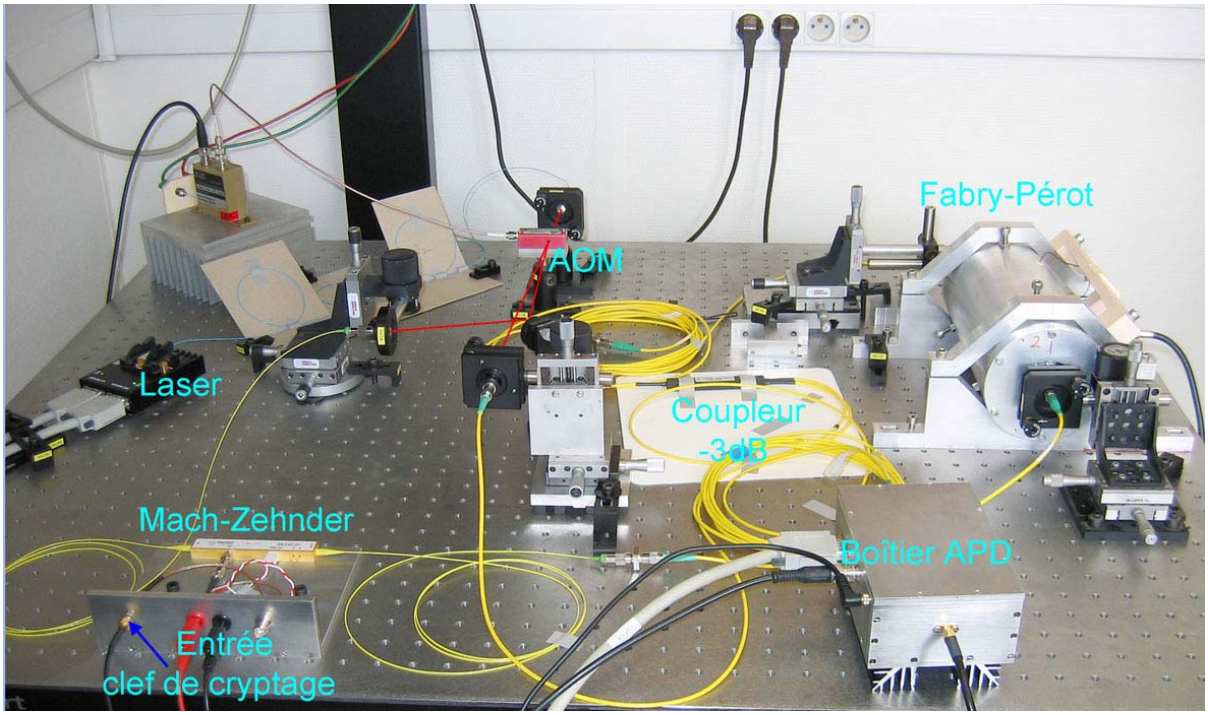


Figure 5-28. Photo de montage d'émission et de détection de clé de cryptage. La clé de cryptage est émise par le boîtier CKG-1 (cf. 4.6.3).

5.6.2 Résultats

La clé reçue est montrée dans la figure 5-29 ci-dessous. Le signal sortant du détecteur est bien stable en position temporelle (oscilloscope synchronisé sur le signal à 39,06 kHz) mais relativement instable en amplitude. Ceci peut s'expliquer par l'absence d'asservissement de la haute tension de commande du FP.

En effet, en utilisant l'équation 4-4-23, la variation de la déformation de la céramique piézoélectrique s'écrit :

$$\Delta(\Delta L) = \Delta V . d_{31} \frac{L}{e} \qquad (5\text{-}6\text{-}1)$$

L'application numérique nous donne : $\Delta(\Delta L) = 2{,}72.\Delta V$ (en nm). Par exemple, si $\Delta V = 1$ V alors $\Delta(\Delta L) = 2{,}72$ nm. Cette variation n'est pas négligeable car le FP est très sensible. Dans la figure 5-29 nous avons le signal de commande pour l'AOM (signal en haut), de fréquence de 39,06 kHz. La clé à transmettre se trouvera dans le niveau haut de la commande, correspondant à une longueur d'onde. Le niveau zéro correspond à l'existence de l'autre longueur d'onde qui portera l'horloge de 10 MHz. L'agrandissement d'une partie de la clé détectée est montré dans la figure 5-30. Il existe un retard d'environ 100 ns dû au système électronique et de transmission optique.

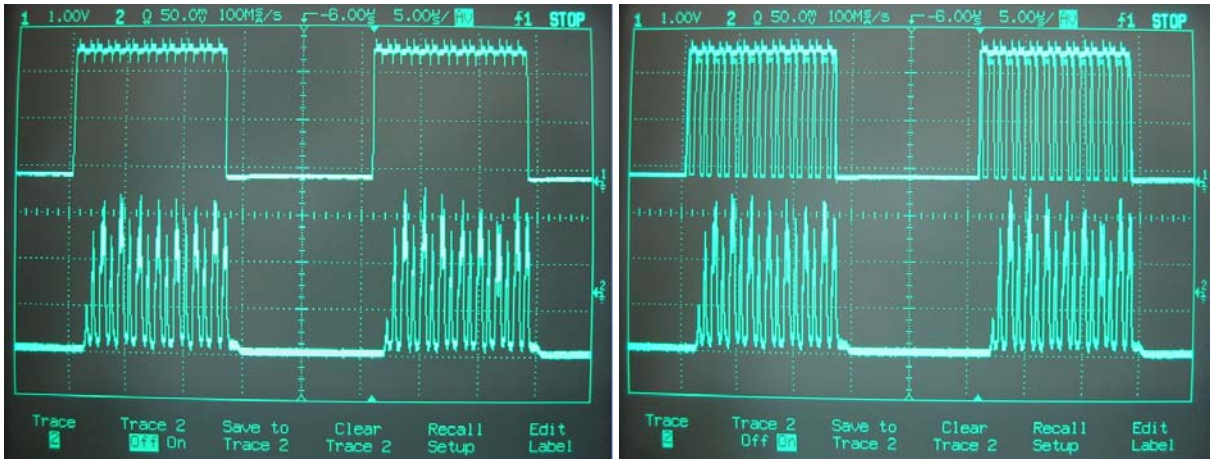


Figure 5-29. Image photographiée de l'oscilloscope. En haut (gauche) : signal de commande de l'AOM, de fréquence de 39,06 kHz ; en haut (droite) : la commande et la clé de cryptage ; en bas : clé détectée. La clé apparaît dans le niveau haut de commande correspondant à une longueur d'onde.

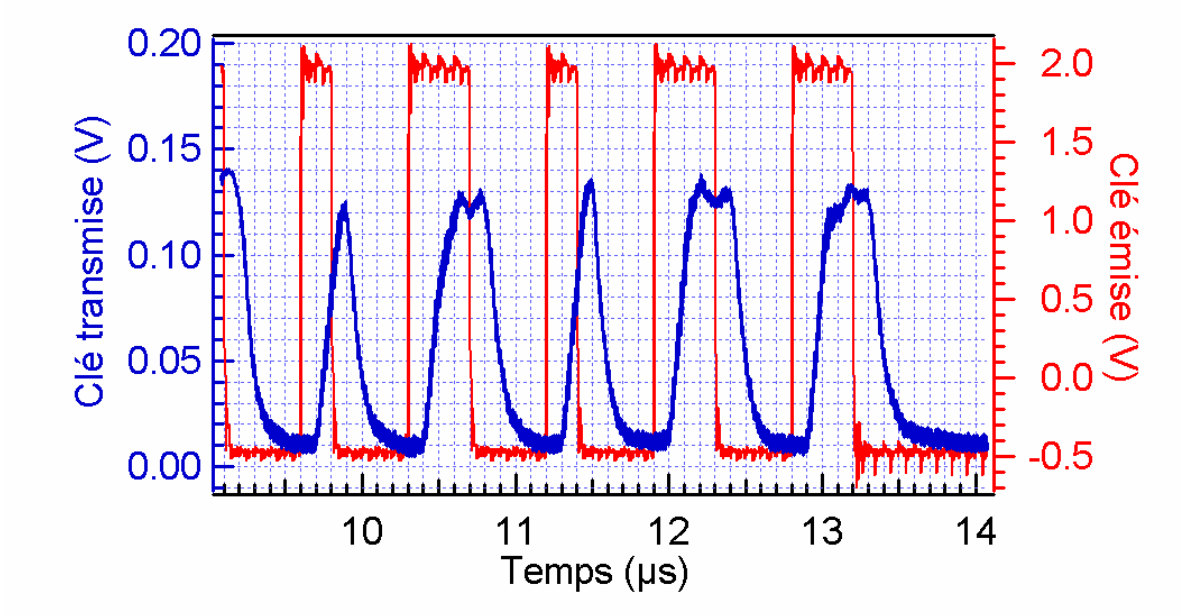


Figure 5-30. Clé émise (courbe rouge) et clé détectée après transmission (courbe bleue) du système (montage fig. 5-26 et 5-27). Le retard dans le temps est d'environ 100 ns.

Ainsi, nous avons transmis une clé de 128 bits pendant l'ouverture de 13,2 µs de l'AOM qui est considéré comme une porte optique. Cette clé de cryptage a été transformée en signal optique (en train de photons) de longueur d'onde λ_1, puis filtrée par le Fabry-Pérot et détectée par l'APD.

5.7 Conclusion

Dans le montage mis en œuvre ici nous n'avons pas transmis l'horloge par l'intermédiaire du faisceau à la longueur d'onde λ_0 faute d'un deuxième modulateur MZ. Mais nous avons néanmoins montré qu'il est possible d'extraire le signal à la longueur d'onde λ_1 à partir de la superposition des deux faisceaux et cela grâce à l'interféromètre de Fabry-Pérot. Comme indiqué sur la figure 4-5, le signal horloge à 10 MHz devrait servir à moduler le faisceau à la longueur d'onde λ_0. Ce signal optique modulé serait injecté directement (sans passer par l'AOM fig. 5-26) par un coupleur optique dans la fibre optique de transmission (longueur plus ou moins grande).

Le faisceau optique contenant les deux longueurs d'onde est séparé en deux parties à la réception, l'une vers le Fabry-Pérot donnant la clé de cryptage après filtrage et détection, l'autre va sur une photodiode PIN qui détecterait l'horloge uniquement car la puissance optique de λ_1 est très faible par rapport à celle de λ_0. Notons que la clé n'est transmise que sur une demi-période du signal à 39,06 kHz.

Néanmoins il ne s'agit que d'une toute première étape. Les impulsions optiques représentant chaque bit de la clé ne sont pas encore suffisamment atténuées pour simuler des photons uniques. Avant de pouvoir le faire, il faut améliorer les couplages au niveau du modulateur acousto-optique ou bien sûr utiliser un modulateur acousto-optique fibré, et réaliser un détecteur travaillant à plus basse température et en mode Geiger.

6 Conclusions

Nous avons présenté dans ce mémoire plusieurs expériences, qui font partie de la recherche et des applications de la physique aux transmissions optiques sécurisées. La cryptographie quantique expérimentale, qui utilise des photons uniques obéissant aux lois quantiques, est un domaine de recherche très important dès maintenant et particulièrement prometteur pour l'avenir. Dans le cadre des travaux de cette thèse, nous avons fait un certain nombre d'expériences mettant en œuvre des phénomènes du domaine de l'optique et du domaine de l'électronique. Nous avons établi les points listés ci-après.

- En utilisant les impulsions laser fortement atténuées, il est possible de préparer une source de 0,1 photon par impulsion. Ces photons sont aléatoires et sa distribution est sensiblement de type poissonien. On vérifie cette distribution par la mesure du paramètre de Mandel Q_M en utilisant la méthode des coïncidences à l'aide de deux détecteurs à photodiode à avalanche (APD). En tenant compte du temps mort de détection dans le système de deux APD et son électronique, nous avons obtenu un paramètre $Q_M = -0{,}05 < 0$ (théoriquement, $Q_M = 0$). On a donc une probabilité de 9,28% d'avoir un seul photon et de 0,24% d'avoir plus d'un photon, soit de 40 fois moins. Cela nous permet pratiquement de considérer une source laser fortement atténuée comme une source de photons uniques.

- Dans la mesure de bruit d'une diode laser, il apparaît que pour des courants de polarisation supérieurs à environ 2,8 fois le courant de seuil, le bruit d'intensité de la diode laser est limité par le bruit de photon.

- En ce qui concerne le système de transmission optique, nous avons réalisé un montage de transmission simultanée d'une clé de cryptage et d'un signal horloge de synchronisation en utilisant de deux longueurs d'onde extrêmement proches couplées à une seule fibre optique. Ainsi nous pouvons fortement diminuer les effets de la dispersion chromatique. Les fibres optiques étant de type monomode nous évitons aussi la dispersion intermodale. Pour cela, nous utilisons un modulateur acousto-optique servant à créer ces deux longueurs d'onde, de modulateurs électro-optiques pour obtenir les signaux « clé » ou « horloge », et enfin un filtre Fabry-Pérot de haute résolution pour les séparer les deux signaux au niveau de la détection et en particulier récupérer le signal correspondant aux clés de cryptage non noyé par le signal horloge.

- Nous avons créé un générateur électronique de clés de cryptage de longueur de 128 bits, qui commandera un modulateur électro-optique Mach-Zehnder pour reproduire les codes de cryptage en signal optique.

- Un filtre optique de très haute résolution a été conçu et réalisé pour ces travaux de thèse. Ce filtre de type Fabry-Pérot fonctionne à la longueur d'onde 1,55 µm. Sa résolution mesurée est de 5 MHz.

- Du côté réception, nous avons réalisé un détecteur à base de photodiode à avalanche de bande passante supérieure à 110 MHz pour une polarisation supérieure à 27 V de la photodiode. Nous avons inclus un refroidissement de la photodiode par un double étage de Peltier permettant de fonctionner à environ 0 °C. Les aspects théoriques des modes de comptage de photons des photodétecteurs ont été abordés mais pas mis en œuvre.

Au delà de ces diverses expériences, il reste bien sûr beaucoup à faire pour approfondir le système de transmissions optiques sécurisées tels que nous l'avons conçu au départ. La longueur d'onde de 1550 nm est maintenant bien fixée, mais cela reste un problème au niveau des détecteurs de photons qui n'ont pas encore une très bonne efficacité à cette longueur d'onde (photodiodes en GaAs). La première amélioration consistera bien sûr à adopter un modulateur acousto-optique fibré ce qui simplifiera les problèmes de couplage que nous avons rencontrés. La structure du système d'émission et de codage des signaux clés de cryptage et horloge est bien définie et nécessite donc deux modulateurs électro-optiques. Le travail essentiel concerne bien évidemment la détection des signaux. Le filtre optique de Fabry-Pérot doit être encore amélioré en particulier vis-à-vis du couplage avec les fibres optiques et grâce à l'introduction d'un contrôle de la température et d'une stabilisation de la haute tension. Au niveau des détecteurs il reste à exploiter pleinement le fait de disposer de l'horloge de synchronisation pour améliorer notre détecteur en travaillant en mode de comptage de photons ou mode Geiger. Il faudra si l'on veut effectivement introduire une sécurité dans la transmission des clés de cryptage régler le niveau de puissance des impulsions optiques « clés » de façon à ce que l'on ne puisse pas trouver ces photons là au sein du signal horloge, le signal en sortie du Fabry-Pérot étant alors extrêmement faible. Il faudra travailler au niveau du détecteur à une température encore plus faible, si possible la température de l'azote liquide, mais il faut donc concevoir un cryostat pour l'APD en travaillant en atmosphère inerte ou bien mieux encore sous vide.

Ce travail a un caractère pluridisciplinaire caractéristique de l'instrumentation. Nous avons pu et dû travailler dans des domaines très variés, tels que l'optique instrumentale (interféromètre de Fabry-Pérot), les détecteurs optiques (mise en œuvre de photodétecteurs à APD, contrôle de la température), la modulation de faisceau optique (modulateurs AOM et Mach-Zehnder) afin de concevoir et réaliser le système de transmission optique de clés de cryptage. Le principe de fonctionnement de ce système a été validé. Le travail d'amélioration de chaque partie peut donc commencer à partir de cette base.

Annexe A.
Programmation sous IGOR pour la boîte CKG-1

Utilisation du logiciel IGOR version 4.09A et plus.

```
#pragma rtGlobals=1          // Use modern global access method.


Function SendCommand(b7,b6,b5,b4,b3,b2,b1,b0) // Pour envoyer des séquences
                                                binaires
variable b7,b6,b5,b4,b3,b2,b1,b0
variable num
Nvar V_VDT
string cmdStr                 // commande ‘string’ pour exécuter "VDTWriteBinary"

        num = b7*2^7 + b6*2^6 + b5*2^5 +b4*2^4 +b3*2^3 +b2*2^2 +b1*2^1 + b0

        sprintf cmdStr, "VDTWriteBinary/O=5/L = 8 %g", num  // décalage à gauche
                par 4 digits, envoyer uniquement les 4 bits supérieurs.
        Execute cmdStr

        // utiliser V_VDT pour confirmer si l’opération est faite ou non.
        if (V_VDT == 1)
                        return 0
        else
                return -1
        endif

End


Function FillRegI()    // Pour charger les registres intermédiaires

SendCommand(0,0,0,0,1,1,1,0)            // Charger RI0
SendCommand(0,0,0,1,0,1,0,0)            // Charger RI1
SendCommand(0,0,1,0,0,1,1,0)            // Charger RI2
SendCommand(0,0,1,1,0,1,1,0)            // Charger RI3
SendCommand(0,1,0,0,1,1,1,0)            // Charger Tête et Queue

End


Function FillSR(a3,a2,a1,a0)          // Pour charger le registre à décalage.

variable a3,a2,a1,a0
variable n

n = a3*2^3+a2*2^2+a1*2^1+a0
```

```
SendCommand(0,1,1,1,1,0,1,0)  // on lance le CEC
FillRegI()
SendCommand(0,1,1,1,0,1,0,1)  // on arête le CEC

string cmdStr            // commande ‘string’ pour exécuter "VDTWriteBinary"
        sprintf cmdStr, "VDTWriteBinary/O=5/L = 8 %g", n + (0*2^7+1*2^6+1*2^5+0*2^4)
        // décalage à gauche par 4 digits, envoyer
        uniquement les 4 bits supérieurs.
        Execute cmdStr

End


Function Operation()

FillSR(0,0,0,0)
FillSR(0,0,0,1)
FillSR(0,0,1,0)
FillSR(0,0,1,1)
FillSR(0,1,0,0)
FillSR(0,1,0,1)
FillSR(0,1,1,0)
FillSR(0,1,1,1)

SendCommand(0,1,0,1,0,0,0,0)
SendCommand(1,0,0,0,0,0,0,0)  // Chargement de ME0 à 3
SendCommand(0,1,1,1,0,1,0,1)  // on coupe CEC pour le chargement de M4 et 5
SendCommand(1,0,0,1,0,0,0,0)  // Chargement de ME4 et 5
SendCommand(0,1,1,1,1,0,1,0)  // on lance CEC

End
```

Opération	**CEC**	**bits**	**B7**	**B6**	**B5**	**B4**		**B3**	**B2**	**B1**	**B0**	**Fonction**
1	dc	0	0	0	0	0		m3	m2	m1	m0	Chargement RI0
2	dc	16	0	0	0	1		m7	m6	m5	m3	Chargement RI1
3	dc	32	0	0	1	0		m11	m10	m9	m8	Chargement RI2
4	dc	48	0	0	1	1		m15	m14	m13	m12	Chargement RI3
5	dc	64	0	1	0	0		T1	T0	Q1	Q0	Chargement RI Ext
6	0	80	0	1	0	1		dc	dc	dc	dc	Transfert de RI Ext dans le SR
7	0	96	0	1	1	0		P3	P2	P1	P0	Transfert de RIn dans le mot pointé de SR
8	dc	112	0	1	1	1	122	1	0	1	0	On lance CEC - Marche
9	dc	112	0	1	1	1	117	0	1	0	1	On arrête CEC - Stop
10	dc	128	1	0	0	0		ME3	ME2	ME1	ME0	Chargement de ME 0 à 3
11	0	144	1	0	0	1		dc	dc	ME5	ME4	Chargement de ME 4 et 5

m0 à m15 : mot de 16 bits composé par les 4 RI
SR : shift register
RI : registre intermédiaire
RI Ext : registre de la tête et la queue
dc : don’t care
P0 à P3 : pointeur du mot dans lequel on transfert le RI
P3 : si P3 = 1, on transfert dans tous les mots à la fois
ME : mot d’état du système
ME0 : inverse F10MHz
ME1 : inverse 10MHzQB
ME2 : inverse la clé
ME3 : inverse FBP4
ME4 : inverse CEC
ME5 : place in inverseur dans la boucle SR
Note : les opérations 6, 7 et 11 ne doivent se faire que quand CEC = 0.

Annexe B.
Démonstration du théorème de Shannon

Théorème de Shannon :

Supposons que (P, C, K, $e_k(.)$,$e_k(.)$) est le système de cryptage avec #P = #C = #K. Le système de cryptage offre un secret parfait si et seulement si toutes les clefs sont utilisées avec la même probabilité 1/#K, et pour chaque $c \in C$ et $m \in P$, il y a une clef unique k telle que $e_k(m) = c$.

Démonstration :

a) Supposons que le système offre un secret parfait.

Il vérifie

$$p(P = m \mid C = c) = p(P = m)$$

Ce qui est équivalent à

$$p(C = c \mid P = m) = p(C = c)$$

Supposons que $p(C = c) > 0$ pour tout le $c \in C$ (si on n'enlève pas c de **C**). Alors, pour tout m fixe, $m \in P$, nous avons

$$p(C = c \mid P = m) = p(C = c) > 0$$

Cela signifie que pour tout le c il doit y avoir au moins une clef k telle que $e_k(m) = c$ et donc, #C ≤ #K. Comme #C = #K nous avons #C = $\#\{e_k(m) : k \in K\}$ = #K. Ça veut dire qu'il n'existe pas deux clefs k_1 et k_2 telles que : $\{e_{k1}(m) = e_{k2}(m) = c\}$.

Conclusion :
Pour tout le $m \in P$ et $c \in C$, il y a une unique clef $k \in K$ telle que $e_k(m) = c$.

Il nous faut démontrer l'équiprobabilité des clefs utilisées, c'est-à-dire

$$p(K = k) = 1/\#K \text{ pour tout le } k \in K$$

Soit n = #K et P = $\{m_i : 1 \le i \le n\}$ et une valeur fixe $c \in C$.
Noter $k_1,k_2,\ldots k_n$ tels que $e_{k_i}(m_i) = c$ pour $1 \le i \le n$.
La propriété de secret parfait du système nous donne :

$$p(P = m_i \mid C = c) = p(P = m_i)$$

et donc,

$$\mathrm{p}(\mathrm{P}=m_i)=\mathrm{p}(\mathrm{P}=m_i\mid\mathrm{C}=c)=\frac{\mathrm{p}(\mathrm{C}=c\mid\mathrm{P}=m_i).\mathrm{p}(\mathrm{P}=m_i)}{\mathrm{p}(\mathrm{C}=c)}=\frac{\mathrm{p}(\mathrm{K}=k_i).\mathrm{p}(\mathrm{P}=m_i)}{\mathrm{p}(\mathrm{C}=c)}$$

On en déduit : $\mathrm{p}(\mathrm{C}=c)=\mathrm{p}(\mathrm{K}=k_i)$ pour $1\le i\le n$. Comme $\sum_{\mathrm{i}=1}^{\mathrm{n}}\mathrm{p}(\mathrm{K}=k_i)=1$, nous avons

$$n.\mathrm{p}(\mathrm{C}=c)=1\ \Rightarrow\ \mathrm{p}(\mathrm{C}=c)=\mathrm{p}(\mathrm{K}=k_i)=1/\mathrm{n}$$

Conclusion :

$$\mathrm{p}(\mathrm{K}=k)=1/\#\mathrm{K}\ \text{ pour tout le }\ k\in K$$

Alors, toutes les clefs sont utilisées avec la même probabilité de 1/#K

b) Maintenant nous devons prouver le résultat dans l'autre sens. À savoir si

- #K = #C = #P
- Chaque clef est employée avec l'équiprobabilité égale 1/#K
- Pour chaque $m\in P$ et $c\in C$, il y a une clef unique k avec $e_k(m)=c$

alors nous devons prouver que le système est parfaitement sécurisé, c'est-à-dire :

$$\mathrm{p}(\mathrm{P}=m\mid\mathrm{C}=c)=\mathrm{p}(\mathrm{P}=m)$$

Comme toutes les clefs sont utilisées avec la même probabilité, pour un c fixe, nous avons

$$p(C=c)=\sum_{\{k:c\in C(k)\}}p(K=k).p(P=d_k(c))=\frac{1}{\#\mathrm{K}}\sum_{\{k:c\in C(k)\}}p(P=d_k(c))$$

Comme pour chaque m et c il y a une clef unique k avec $e_k(m)=c$, nous avons

$$\sum_{\{k:c\in C(k)\}}p(P=d_k(c))=\sum_{m\in P}p(P=m)=1$$

Conclusion :

$$\mathrm{p}(\mathrm{C}=c)=1/\#\mathrm{K}$$

En outre, si $c=e_k(m)$ alors $\mathrm{p}(\mathrm{C}=c\mid\mathrm{P}=m)=\mathrm{p}(\mathrm{K}=k)=1/\#\mathrm{K}$. En utilisant le théorème de Bayes[(1)], nous avons

$$\mathrm{p}(\mathrm{P}=m\mid\mathrm{C}=c)=\frac{\mathrm{p}(\mathrm{C}=c\mid\mathrm{P}=m).\mathrm{p}(\mathrm{P}=m)}{\mathrm{p}(\mathrm{C}=c)}$$

$$p(P = m \mid C = c) = \frac{1/\#K.p(P = m)}{1/\#K} = p(P = m) \text{ (CQFD)}$$

****

(1) : **Théorème de Bayes**

Si $p(Y = y) > 0$ alors

$$p(X = x \mid Y = y) = \frac{p(X = x, Y = y)}{p(Y = y)} = \frac{p(Y = y \mid X = x).p(X = x)}{p(Y = y)}$$

X et Y sont indépendants si $p(X = x \mid Y = y) = p(X = x)$, cela signifie que X ne dépend pas de Y.

Publications

[p1] Liantuan Xiao, Romain Alléaume, Quyên Đinh Xuân, François Treussart, Bernard Journet, Jean-François Roch - "Measurement of photon distribution in attenuated diode laser pulses". *Proceedings of the SPIE Physics and Simulation of Optoelectronic Devices XI*, OPTO 2003, Vol. 4986, pp 463-468, San Jose, CA, USA, Jan. 25-31, **2003**.

[p2] Romain Alléaume, Lian-Tuan Xiao, Đinh Xuân Quyên, Vu Van Luc, François Treussart, Bernard Journet, Jean-François Roch - "Etude expérimentale de la statistique de photons dans des impulsions de diode laser fortement atténuées" - *3ème Colloque Interdisciplinaire en Instrumentation (C2I)*, ENS Cachan, 29-30 Janvier **2004**.

[p3] Đinh Xuân Quyên, Nguyên Chi Thành, Xiao Liantuan, Vu Doan Miên, Vu Van Luc, Bernard Journet - "Simultaneous transmission of faint laser pulses and clock synchronization signal applied to secured optical transmissions at 1.55 µm" (Invited paper) - *9th Asia Pacific Physics Conference (APPC)*, Hà Nôi, Viêt Nam, Oct. 25-31, **2004**.

[p4] Bernard Journet, Nguyên Chi Thành, Đinh Xuân Quyên, Xiao Liantuan, Vu Doan Miên, Vu Van Luc - "Simultaneous transmission of faint laser pulses and of synchronization signal at 1.55 µm for secured optical transmissions" - *Proceedings of the SPIE Semiconductor Photodetectors II*, OPTO 2005, Vol. 5726, San Jose, CA, USA, Jan. 22-27, **2005**.

[p5] Bernard Journet, Đinh Xuân Quyên, Xiao Liantuan, Nguyên Chi Thành, Vu Van Luc, Luong Vu Hai Nam - "Transmission system of faint laser pulses at λ=1550nm based on optical modules and dedicated to secured optical telecommunications" - *6th National Physics Conference*, Hà Nôi, Viêt Nam, Nov. 23-25, **2005**.

[p6] Vu Van Luc, Bernard Journet, Đinh Xuân Quyên, Luong Vu Hai Nam - "High frequency characteristics of a travelling wave SOA module based on combining tilted facets (about 7°) with an antireflection at 1550 nm" - *6th National Physics Conference*, Hà Nôi, Viêt Nam, Nov. 23-25, **2005**.

[p7] Quyên Dinh Xuân, Romain Alléaume, Liantuan Xiao, François Treussart, Bernard Journet, and Jean-François Roch - "Intensity noise measurement of strongly attenuated laser diode pulses in the time domain" - *The European Physical Journal - Applied Physics*, Vol. 35, No. 2, 117-121, **2006**.

Références

[1] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28, 656 (1949).

[2] W. K. Wooters et W. H. Zurek, "A single quantum cannot be cloned", *Nature* **299**, 802 (1982).

[3] C. Cohen-Tannoudji, "Mécanique quantique", Edition *Paris Hermann* (1973).

[4] R. P. Feynman, "Quantum mechanics", Edition *Massachusetts Addison Wesley* (1965).

[5] P. Dirac, "The principles of quantum mechanics", Edition *Oxford Clarendon Press* (1988)

[6] Gilbert S. Vernam, "Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications", *Journal of the IEEE*, **55**, 109 (1926).

[7] Paul D. Townsend et I. Thompson, "A quantum key distribution channel based on optical fibre", *J. Mod. Opt.* **41**, 2425 (1994).

[8] C. Gobby, Z. L. Yuan et A. J. Shields, "Unconditionally secure quantum key distribution over 50 km of standard telecom fibre", *Electron. Lett.* **40**, 1603 (2004).

[9] S. Fasel, N. Gisin, G. Ribordy et H. Zbinden, "Quantum key distribution over 30 km standard fiber using energy-time entangled photon pairs", **Eur. Phys. J. D** 30, 143 (2004).

[10] B. C. Jacobs et D. Franson, "Quantum cryptography in free space", *Opt. Lett.* **21**, 1854 (1996).

[11] J. D. Franson et H. Ilves, "Quantum cryptography using polarization feedback", *J. Mod. Opt.* **41**, 2391 (1994).

[12] N. Gisin, G. Ribordy, W. Tittel et H. Zbinden, "Quantum cryptography", *Rev. Mod. Phys.* **74**, 145 (2002).

[13] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett.* **68**, 3121 (1992).

[14] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden et N. Gisin, "Plug and play systems for quantum cryptography", *Appl. Phys. Lett.* **70**, 793 (1997).

[15] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt et C. G. Peterson, "Free-space quantum key distributiono in daylight", *J. Mod. Opt.* **47**, 549 (2000).

[16] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson et C. M. Simmons, "Practical free-space quantum key distribution over 1 km", *Phys. Rev. Lett.* **81**, 3283 (1998).

[17] Thomas Durt, "Comment on *Practical free-space quantum key distribution over 1 km*", *Phys. Rev. Lett.* **83**, 2476 (1999).

[18] G. Brassard, N. Lütkenhaus, T. Mor et B. C. Sanders, "Security aspects of practical quantum cryptography", *Quant-ph/9911054* (1999).

[19] G. Brassard, T. Mor et B. C. Sanders, "Quantum cryptography via parametric downconversion", *Quant-ph/9906074* (1999).

[20] N. Lütkenhaus, "Estimates for practical quantum cryptography", *Phys. Rev. A* **59**, 3301 (1999).

[21] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller et J. E. Nordholt, "Long-distance quantum key distribution in optical fibre", *New J. Phys.* **8**, 193 (2006).

[22] H. Takesue, E. Diamanti, T. Honjo, C. Langrock, M. M. Fejer, K. Inoue1 et Y. Yamamoto, "Differential phase shift quantum key distribution experiment over 105km fibre", *New J. Phys.* **7**, 232 (2005).

[23] D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund et P. G. Kwiat, "Entangled state quantum cryptography: eavesdropping on the Ekert protocol", *Phys. Rev. Lett.* **84**, 4733 (2000).

[24] A. K. Ekert, "Quantum cryptography based on Bell's theorem", *Phys. Rev. Lett.* **67**, 661 (1991).

[25] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", in *Proc. of IEEE Inter. Conf. on Computers and Signal Processing*, Bangalore, India (Institute of Electrical and Electronics Engineers, New York), pp. 175 (1984).

[26] F. Treussart, R. Alléaume, V. Le Floc'h et J.-F. Roch, "Single photon emission from a single molecule", *C. R. Physique* **3**, 501 (2002).

[27] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, "Quantum key distribution over 67 km with a plug & play system", *New J. Phys.* **4**, 41.1 (2002).

[28] H. J. Briegel, W. Dur, J. I. Cirac et P. Zoller, "Quantum repeaters: the role of imperfect local operation in quantum communication", *Phys. Rev. Lett.* **81**, 5932 (1998).

[29] Philip A. Hiskett, G. Bonfrate, G. S. Buller et P. D. Townsend, "Eighty kilometer transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 μm", *J. Mod. Opt.* **48**, 1957 (2001).

[30] O. L. Guerreau, F. J. Malassenet, S. W. McLaughlin et J.-M. Merolla, "Quantum key distribution without a single-photon source using a strong reference", *IEEE Photon. Techno. Lett.* **17**, 1755 (2005).

[31] B. Lounis et W. E. Moerner, "Single photons on demand from a single molecule at room temperature", *Nature*, **407**, 191 (2000).

[32] R. Brouri, A. Beveratos, J.-P. Poizat, P. Grangier, "Photon antibunching in the fluorescence of individual color centers in diamond", *Opt. Lett.*, **25**, 1294 (2000).

[33] T. Gaebel, I. Popa, A. Gruber, M. Domhan, F. Jelezko et J. Wrachtrup, "Stable single-photon source in the near infrared", *New J. Phys.* **6**, 98 (2004).

[34] A. Kuhn, M. Hennrich et G. Rempe, "Deterministic single-photon source for distributed quantum networking", *Phys. Rev. Lett.* **89**, 067901 (2002).

[35] J. McKeever, A. Boca, A. D. Boozer, J. R. Buck et H. J. Kimble, "Experimental realization of a one-atom laser in the regime of strong coupling", *Nature*, **425**, 268 (2003).

[36] T. Aichele1, V. Zwiller et O. Benson, "Visible single-photon generation from semiconductor quantum dots", *New J. Phys.* **6**, 90 (2004).

[37] C. Santori, D. Fattal, J. Vuckovic, G. S. Solomon et Y. Yamamoto, "Single-photon generation with InAs quantum dots", *New J. Phys.* **6**, 89 (2004).

[38] C. Kurtsiefer, S. Mayer, P. Zarda et H. Weinfurter, "Stable solid-state source of single photons", *Phys. Rev. Lett.* **85**, 290 (2000).

[39] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat et P. Grangier, "Single photon quantum cryptography", *Phys. Rev. Lett.* **89**, 187901 (2002).

[40] E. Knill, R. Laflamme et G. J. Milburn, "A scheme for efficient quantum computation with linear optics", *Nature* **409**, 46 (2001).

[41] C. K. Law et H. J. Kimble, "Deterministic generation of a bit-stream of single-photon pulses", *J. Mod. Opt.* **44**, 2067 (1997).

[42] F. De Martini, O. Jedrkiewicz et P. Mataloni, "Generation of quantum photon states in an active microcavity trap", *J. Mod. Opt.* **44**, 2053 (1997).

[43] M. Pelton, C. Santori, J. Vuckovic, B. Zhang, G. S. Solomon, J. Plant et Y. Yamamotof, "Efficient source of single photons: a single quantum dot in a micropost microcavity", *Phys. Rev. Lett.* **89**, 233602 (2002).

[44] J. Vuckovic, D. Fattal, C. Santori, G. S. Solomon et Y. Yamamotod, "Enhanced single-photon emission from a quantum dot in a micropost microcavity", *Appl. Phys. Lett.* **82**, 3596 (2003).

[45] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard et H. Zbinden, "Fast and user-friendly quantum key distribution", *J. Mod. Opt.*, **47**, 517 (2000).

[46] G. Brassard, N. Lütkenhaus, T. Mor et B. C. Sanders, "Limitations on practical quantum cryptography", *Phys. Rev. Lett.* **85**, 1330 (2000).

[47] T. B. Pittman, B. C. Jacobs et J. D. Franson, "Heralding single photons from pulsed parametric down-conversion", Preprint quant-ph/0408093 (2004).

[48] O. Alibart, D. B. Ostrowsky et P. Baldi, "High performance heralded single photon source", Preprint quant-ph/0405075 (2004).

[49] C. K. Hong et L. Mandel, "Experimental realization of a localized one-photon state", *Phys. Rev. Lett.* **56**, 58 (1986).

[50] G. Ribordy, J. Brendel, J.-D Gautier, N. Gisin et H. Zbinden, "Long-distance entanglement-based quantum key distribution", *Phys. Rev. A* **63**, 012309 (2001).

[51] Thèse Beveratos, "Réalisation expérimentale d'une source de photons uniques par fluorescence de centres colorés dans le diamant : application à la cryptographie quantique", Université Paris XI, page 14 (2002).

[52] Mandel, "Optical coherence and quantum optics", Cambridge University press, (1995).

[53] Gardiner, "Quantum Noise", Springer-Verlag, (1991), p.153

[54] Cohen-Tannoudji, "Processus d'interaction entre photons et atomes", InterEditions CNRS (1988).

[55] P. Grangier, "Etude expérimentale de propriétés non-classiques de la lumière : interférence à un seul photon", Thèse de doctorat, Université de Paris XI, (1986).

[56] E. Hanbury Brown et R. Q. Twiss, *Nature*, **177**, 27 (1957)

[57] H. J. Kimble, M. Dagenais, et L. Mandel, "Photon antibunching in resonance fluorescence", *Phys. Rev. Lett.* **39**, 691 (1977).

[58] R. Short et L. Mandel, "Observation of sub-Poissionian photon statistics", *Phys. Rev. Lett.* **51**, 384 (1983).

[59] H. P. Yuen et V. W. S. Chan, "Noise in homodyne detection", *Opt.Lett.* **8**, 177 (1983).

[60] L. Mandel, "Sub-Poissonian photon statistics in resonance fluorescence", *Opt.Lett.* **4**, 205 (1979).

[61] R. Short et L. Mandel, "Observation of sub-Poissonian photon statistics", *Phys. Rev. Lett.* **51**, 384 (1983).

[62] P. L. Kelley et W. H. Kleiner, "Theory of electromagnetic field measurement and photoelectron counting", *Phys. Rev.* **136**, A316 (1964).

[63] L. Mandel, "Fluctuation of photon beams: the distribution of the photoelectrons", *Proc. Phys. Soc.* (London) **74**, 233 (1959).

[64] P. Grangier, B. C. Sanders et J. Vuckovic, "Focus on single photons on demand", *New J. Phys.* **6**, (2004).

[65] H. Zbinden, N. Gisin, B. Huttner, A. Muller et W. Tittel, "Practical aspects of Quantum cryptographic key distribution", *J. Cryptology* **13**, 207 (2000).

[66] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J.-F. Roch, A. Beveratos, R. Brouri-Tualle, J.-P. Poizat et P. Grangier, "Experimental open-air quantum key distribution with a single-photon source", *New J. Phys.* **6**, 92 (2004).

[67] C. Gobby, Z. L. Yuan et A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber", *Appl. Phys. Lett.* **84**, 3762 (2004).

[68] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution", *Phys. Rev. A* **61**, 052304 (2000).

[69] C. Kurtsiefer, P. Zarda, S. Mayer et H. Weinfurter, "The breakdown flash of silicon avalanche photodiodes – backdoor for eavesdropper attacks?", *J. Mod. Opt.* **48**, 2039 (2001).

[70] C. Brunel, B. Lounis, P. Tamarat et M. Orrit, "Triggered source of single photons based on controlled single molecule fluorescence", *Phys. Rev. Lett.* **83**, 2722 (1999).

[71] R. Loudon, "The quantum theory of light", Oxford University Press (2000).

[72] L. Fleury, J.-M. Segura, G. Zumofen, B. Hecht et U. P. Wild, "Nonclassical photon statistics in single-molecule fluorescence at room temperature", *Phys. Rev. Lett.* **84**, 1148 (2000).

[73] J. A. Abate, H. J. Kimble et L. Mandel, "Photon statistics of a dye laser", *Phys. Rev. A* **14**, 788 (1976).

[74] F. Treussart, R. Alléaume, V. Le Floc'h, L. T. Xiao, J.-M. Courty et J.-F. Roch, "Direct measurement of th photon statistics of a triggered single photon source", *Phys. Rev. Lett.* **89**, 093601 (2002).

[75] H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. I. Lvovsky, J. Mlynek et S. Schiller, "Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements", *Opt.Lett.* **26**, 1714 (2001).

[76] D. S. Bethune et W. P. Risk, "An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light", *IEEE J. Quant. Elect.* **36**, 340 (2000).

[77] N. Namekata, Y. Makino et S. Inoue, "Single-photon detector for long-distance fiber-optic quantum key distribution", *Opt. Lett.* **27**, 954 (2002).

[78] FTDI, La documentation d'utilisation du composant FTDI USB FIFO FT8U245AM.

[79] Xilinx, La documentation d'utilisation des registres XC3042A et XC1736EPC.

[80] T. E. Ingerson, R. J. Kearney et R. L. Coulter, "Photon counting with photodiodes", *Appl. Opt.* **22**, 2013 (1983).

[81] R. G. W. Brown, K. D. Ridley et J. G. Rarity, "Characterization of silicon avalanche photo-diodes for photon correlation measurements. 1: Passive quenching", *Appl. Opt.* **25**, 4122 (1986).

[82] R. G. W. Brown, R. Jones, J. G. Rarity et K. D. Ridley, "Characterization of silicon avalanche photodiodes for photon correlation measurements. 2: Active quenching", *Appl. Opt.* **26**, 2383 (1987).

[83] P. G. Kwiat, A. M. Steinberg, R. Y. Chiao, P. H. Eberhard et M. D. Petroff, "High-efficiency single-photon detectors", *Phys. Rev. A* **48**, R867 (1993).

[84] S. Cova, A. Longoni et A. Andreoni, "Towards picosecond resolution with single-photon avalanche diodes", *Rev. Sci. Instrum.* **52**, 408 (1981).

[85] F. Zappa, A. Lacaita, S. Cova et P. Webb, "Nanosecond single-photon timing with InGaAs/InP photodiodes", *Opt. Lett.* **19**, 846 (1994).

[86] Y. Kang, P. Mages, A. R. Clawson, P. K. L. Yu, M. Bitter, Z. Pan, A. Pauchard, S. Hummel et Y. H. Lo, "Fused InGaAs-Si avalanche photodiodes with low-noise performances", *IEEE Photon. Tech. Lett.* **14**, 1593 (2002).

[87] http://www.phy.hw.ac.uk/resrev/photoncounting/projects/spads.html

[88] E. L. Dereniak et D. G. Crowe, "Optical radiation detectors", Wiley (1984).

[89] Fujitsu, Ltd., "InGaAs avalanche photodiodes data sheet, model FPD5W1KS" Fujitsu FPD5W-1KS Application Notes (1998).

[90] G. N. Goltsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smimov, B. Voronov, A. Dzardanov, C. Williams et R. Sobolewski, "Picosecond superconducting single-photon optical detector", *Appl. Phys. Lett.* **79**, 705 (2001).

[91] A. Verevkin, J. Zhang, R. Sobolewski, A. Lipatov, O. Okunev, G. Chulkova, A. Korneev, K. Smimov, G. N. Goltsman et A. Semenov, "Detection efficiency of large-active-area NbN single-

photon superconducting detectors in the ultraviolet to near-infrared range", *Appl. Phys. Lett.* **80**, 4687 (2002).

[92] A. Korneev, P. Kouminov, V. Matvienko, G. Chulkova, K. Smimov, M. Currie, W. Lo, K. Wilsher, J. Zhang, W. Slysz, A. Pearlman, A. Verevkin et R. Sobolewski, "Sensitivity and gigahertz counting performance of NbN superconducting single-photon detectors", *Appl. Phys. Lett.* **84**, 5338 (2004).

[93] G. N. Goltsman, A; Korneev, V. Izbenko, K. Smirnov, P. Kouminov, B. Voronov, N. Kaurova, A. Verevkin, J. Zhang, A. Pearlman, W. Slysz et R. Sobolewski, "Nano-structured superconducting single-photon detectors", *Nucl. Instrum. Meth. Phys. Resear. A* **520**, 527 (2004).

[94] A. M. Kadin et M. W. Johnson, "Nonequilibrium photon-induced hotspot: A new mechanism for photodetection on ultrathin metallic films", *Appl. Phys. Lett.* **69**, 3938 (1996).

[95] K. S. Il'in, M. Lindgren, M. Currie, A. D. Semenov, G. N. Goltsman, R. Sobolewski, S. I. Cherednichenko et E. M. Gershenzon, "Picosecond hot-electron energy relaxation in NbN superconducting photodetectors", *Appl. Phys. Lett.* **76**, 2752 (2000).

[96] R. H. Hadfield, M. J. Stevens, S. S. Gruber, A. J. Miller, R. E. Schwall, R. P. Mirin et S. W. Nam, "Single photon source characterization with a superconducting single photon detector", *Opt. Expr.* **13**, 10846 (2005).

[97] A. Engel, A. Semenov, H.-W. Hübers, K. Il'in et M. Siegel, "Superconducting single photon detector for the visible and infrared spectral range", *J. Mod. Opt.* **51**, 1459 (2004).

[98] A. Lipatov, O. Okunev, K. Smirnov, G. Chulkova, A. Korneev, P. Kouminov, G. N. Goltsman, J. Zhang, W. Slysz, A. Verevkin et R. Sobolewski, "An ultrafast NbN hot-electron single-photon detector for electronic applications", *Supercond. Sci. Technol.* **15**, 1689 (2002).

[99] H. Dautet, P. Deschamps, B. Dion, A. D. MacGregor, D. MacSween, R. J. McIntyre, C. Trottier et P. P. Webb, "Photon counting technique with silicon avalanche photodiodes", *Appl. Opt.* **32**, 3894 (1993).

[100] P. A. Hiskett, J. M. Smith, G. S. Buller and P. D. Townsend, "Low-noise single-photon detection at wavelength 1.55 μm", *Electron. Lett.* **37**, 1081 (2001).

[101] M. Bourennane, A. Karlsson, J. P. Ciscar and M. Mathes, "Single-photon counters in the telecommunication wavelength region of 1550 nm for quantum information processing", *J. Mod. Opt.* **48**, 1983 (2001).

[102] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J. G. Rarity and T. Wall, "Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APDs", *J. Mod. Opt.* **48**, 1967 (2001).

[103] S. Cova, M. Ghioni, A. Lacaita, C. Samori et F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection", *Appl. Opt.* **35**, 1956 (1996).

[104] P. C. M. Owens, J. G. Rarity, P. R. Tapster, D. Knight et P. D. Townsend, "Photon counting with passively quenched germanium avalanche", *Appl. Opt.* **33**, 6895 (1994).

[105] S. Cova, M. Ghioni, A. Lotito, I. Rech et F. Zappa, "Evolution and prospects for single-photon avalanche diodes and quenching circuits", *J. Mod. Opt.* **51**, 1267 (2004).

[106] S. Cova, A. Longoni et G. Ripamonti, "Active-quenching and gating circuits for single-photon avalanche diodes", *IEEE Trans. Nucl. Sci.* **29**, 599 (1982).

[107] A. Spinelli, L. M. Davis et H. Dautet, "Actively quenched single-photon avalanche diode for high repetition rate time-gated photon counting", *Rev. Sci. Instrum.* **67**, 55 (1996).

[108] F. Zappa, M. Ghioni, S. Cova, C. Samori et A. C. Giudice, "An integrated active-quenching circuit for single-photon avalanche diodes", *IEEE Trans. Instrum. Meas.* **49**, 1167 (2000).

[109] I. Prochazka, "Peltier-cooled and actively quenched operation of InGaAs/InP avalanche photodiodes as photon counters at a 1.55 μm wavelength", *Appl. Opt.* **40**, 6012 (2001).

[110] A. Yoshizawa, R. Kaji et H. Tsuchida, "After-pulse-discarding in single-photon detection to reduce bit errors in quantum key distribution", *Opt. Expr.* **11**, 1303 (2003).

[111] J. J. Fox, N. Woodard et G. P. Lafyatisa, "Characterization of cooled large-area silicon avalanche photodiodes", Rev. Sci. Instrum. 70, 1951 (1999).

[112] N. G. Woodard, E. G. Hufstedler et G. P. Lafyatis, "Photon counting using a large area avalanche photodiode cooled to 108 K", *Appl. Phys. Lett.* **64**, 1177 (1994).

[113] L. Yang, S. N. Dzhosyuk, J. M. Gabrielse, P. R. Huffman, C. E. H. Mattoni, S. E. Maxwell, D. N. McKinsey and J. M. Doyle, "Performance of a large-area avalanche photodiode at low temperature for scintillation detection", *Nucl. Instrum. & Methods A* **508,** 388 (2003).

[114] J. I. Cirac, P. Zoller, H. J. Kimble et H. Mabuchi, "Quantum state transfer and entanglement distribution among distant nodes in a quantum network", Phys. Rev. Lett. 78, 3221 (1997).

[115] H. A. Bachor, "A guide to experiments in quantum optics", Edition *Wiley-VCH* (2004).

[116] D. F. Walls, "Quantum optics", Springer-Verlag Berlin Heidenberg (1994), p. 40.

[117] P. L. Knight et L. Allen, "Concepts of quantum optics", Pergamon Press (1983), p. 67.

[118] J. M. Liu, "Photonic devices", Cambridge University Press (2005), chapitre 8.

Résumé

Les travaux de cette thèse s'inscrivent dans le cadre de la cryptographie, et plus précisément de la cryptographie quantique. Le but est de concevoir un système permettant de transmettre simultanément une clé de cryptage et un signal horloge dans une même fibre optique (à la longueur d'onde des télécommunications soit 1550 nm) en essayant d'éviter les effets de la dispersion chromatique. En effet le signal représentant la clé de cryptage doit être réalisé sous forme d'impulsions fortement atténuées simulant des photons uniques et dans ces conditions il est nécessaire de disposer au niveau du détecteur d'un signal horloge donnant l'instant d'arrivée des impulsions. Nous fabriquons deux signaux de longueurs d'onde très proches (écart de 0,88 pm) grâce à un modulateur acousto-optique, chacune servant de porteuse à un des deux signaux. A la réception il est nécessaire de séparer ces deux longueurs d'ondes et pour cela un filtre basé sur un interféromètre de Fabry-Pérot a été conçu, réalisé, testé et mis en œuvre au laboratoire. Puis nous avons aussi réalisé un photodétecteur basé sur une photodiode à avalanche, dont nous pouvons abaisser la température de fonctionnement jusqu'à environ 0°C. Le système a été entièrement réalisé et nous avons pu montrer la faisabilité de cette technique. Des améliorations restent à apporter en particulier sur la stabilité du filtre optique et sur le fonctionnement du détecteur en mode comptage de photons.

Mots clés : cryptographie quantique – photons uniques – modulateur acousto-optique – cavité Fabry Pérot – photodiode à avalanche – contrôle de température – comptage de photons.

Abstract

The works presented here belongs to the field of cryptography and more precisely to the quantum cryptography. The goal is to design a system for transmitting simultaneously a key for encoding and a signal clock in the same optical fibre (at the classical wavelength of telecommunications 1550 nm) in order to avoid the effects of chromatic dispersion. Indeed the signal representing the key of encoding must be carried out in the form of strongly attenuated pulses simulating single photons; under these conditions it is necessary for improving the detection to know thanks to a clock signal the arrival time of the pulses. We achieve two signals with very close wavelengths (variation of 0.88 pm) thanks to an acousto-optic modulator, each one serving as carrier for one the two signals. At the reception stage it is necessary to separate these two wavelengths and for this reason a filter based on a Fabry-Pérot interferometer has been designed, produced, tested and implemented at the laboratory. Then we also produced a photodetector based on an avalanche photodiode, with the possibility to lower the operating temperature until approximately 0°C. The system was entirely carried out and we have shown the feasibility of this technique. Improvements remain to be brought in particular on the stability of the optical filter and the operation of the detector in counting mode of photons.

Key words: quantum cryptography – single photon – modulator acousto-optics – cavity Fabry Pérot – photodiode with avalanche – controls temperature – counting of photons.