# Contribution à l'étude et à la réalisation d'un système de distribution quantique de clef par codage en phase

Sébastien Agnolini

UNIVERSITE PIERRE & MARIE CURIE
LA SCIENCE A PARIS

École Doctorale d'Informatique, Télécommunications et Électronique de Paris

# Thèse

présentée pour obtenir le grade de Docteur
de l'Université Pierre et Marie Curie

Spécialité : Informatique, Télécommunications et Electronique


## Sébastien AGNOLINI


## Contribution à l'étude et à la réalisation d'un système de distribution quantique de clef par codage en phase

Soutenue le 23 avril 2007 devant le jury composé de

| | |
|---|---|
| Georges Alquié | Président |
| Henri Porte | Rapporteur |
| Jean-Marc Merolla | Rapporteur |
| Francisco J. Mendieta | Examinateur |
| Philippe Gallion | Directeur de thèse |

# Remerciements

Cette thèse est le fruit d'un peu plus de « trois ans » de travail au sein du groupe optique du département Communication et Electronique de l'Ecole Nationale Supérieure des Télécommunications, à Paris.

J'adresse dans un premier temps, tous mes remerciements à M. Georges Alquié du Laboratoire des Instruments et Systèmes d'Ile de France à l'Université Pierre et Marie Curie, qui m'a fait l'honneur de présider mon jury de thèse ; et à mes deux rapporteurs qui ont accepté de lire mon manuscrit en des temps extrêmement courts : M. Jean-Marc Mérolla du département d'optique PM Duffieux de Besançon et M. Henri Porte de Photline Technologies.

Je tiens également à remercier M. Francisco J. Mendieta du CICESE au Mexique, examinateur, pour ses conseils lors des répétitions de soutenance, et sa préparation à la fameuse séance des questions. Enfin, je remercie mon directeur de thèse, M. Philippe Gallion, de m'avoir accepté en thèse et encadré durant ces « un peu plus de trois ans ».

Je remercie M. Bernard Robinet, président de l'Ecole Doctorale d'Informatique Télécommunication et Electronique de Paris.

Je remercie également Marcia B. Costa E Silva pour son aide et sa bonne humeur quotidienne, et Qing Xu qui poursuit mes travaux.

La vie d'un thésard débute par son arrivée au laboratoire et s'achève par le traditionnel pot de thèse. Au cours de ce cycle, j'ai eu le privilège de côtoyer de nombreux thésards. Je tiens à les saluer et à les remercier en les citant : Alireza, Amira, Anne-Claire, Axel, Bruno, Cédric, Christophe, David, Désiré, Elena, Fabien, Fausto, Ghaya, Hedi, Iannis, Malek, Marcia, Mariam, Mohamad, Mounia, Philippe, Qing, Shifeng, Sophie, Stefan, Sylvain, Vincent, ainsi que tous les autres thésards du laboratoire.

Un grand merci aux amis que j'ai honteusement classifié :
- les *plongeurs* ; Ben, Bruno, Caroline, Claire, Clara, Coralie, David, François, Frank, Greg, Gwen, Johny, Karine, Laurie, Manon, Marielle, Michel, Myriam, Philippe, Romain, Sabine, Violaine, Virgile, …
- les *forçats du GR20* ; Bruno, Clara, Xavier
- le groupe *fac* ; Adelaïde, Anne-Laure, Damien, Filipe, Fix, Gwladys, Laurence
- le groupe *DD* ; Fabrice, Fanny, François, Koug, Raph, Steph
- et enfin, les *inclassables* ; Diane, Sab, Yiol.

Pour finir, je remercie mes parents, ma grand-mère, Bernard et Brigitte, pour m'avoir soutenu et encouragé par leur présence durant, notamment, la journée du 23 avril 2007, ainsi que tous les autres membres de ma famille.

# Résumé

La sécurisation des systèmes de communication passe par des techniques de cryptographie à clef. Les communications, sur un canal non protégé, imposent l'échange d'une clef entre Alice et Bob qui sont avec Eve, tentant d'obtenir cette clef à leur insu, les acteurs incontournables de tout scénario cryptographique. 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. Les erreurs résultent d'observations incompatibles d'un même objet quantique, comme la mesure de la phase d'un photon unique sur deux bases différentes. Un faible taux d'erreur garantit la confidentialité de la clef. Le protocole BB84 autorise l'élaboration et l'échange de clef entre Alice et Bob. Il nécessite quatre états quantiques constituant deux bases, notées $A_1$ et $A_2$ contenant chacune deux symboles notés *0* et *1*. Les bases $A_1$ et $A_2$ sont dites conjuguées.

Cette thèse propose une étude et une réalisation expérimentale d'un système de distribution quantique de clef utilisant le protocole BB84 par codage en phase sur un photon unique ($\lambda$ = 1,5µm). La génération des photons uniques est assurée par un laser de type *ILM* dont les impulsions optiques sont fortement atténuées. La modulation *QPSK* satisfaisant à des choix de base et de symbole indépendants est assurée par l'utilisation de modulateurs Mach-Zehnder à deux électrodes. Trois systèmes de détection cohérente sont proposées et comparées. Les évolutions successives de notre système nous amènent à proposer aujourd'hui un système de cryptographie quantique à une voie optique par codage *DQPSK*.

# Abstract

The security of communication systems is based on key cryptography techniques. Communications on a protected channel impose the exchange of a key between Alice and Bob. Eve, a third actor in the scene tries to obtain this key without making her presence notorious to the others. The quantum security results from the impossibility to Eve to duplicate successfully signals or to extract a significant part of them without giving evidence of her intervention. Since her intervention introduces important changes in the error rate of the signals received by Bob. These errors result from incompatible observations of the same quantum object, as well as phase measurements of a single photon coded on two different basis. A weak rate of error guarantees confidentiality of the key. The protocol BB84 authorizes the elaboration and the exchange of key between Alice and Bob, it requires four quantum states forming two basis, called $A_1$ and $A_2$ containing two symbols, named *0* and *1*, each. The $A_1$ and $A_2$ bases are conjugated.

This thesis presents for consideration a research and an experimental realization of a quantum key distribution system using the protocol BB84 by coding in phase on a single photon at $\lambda$ = 1,5 µm. The generation of this single photon is assured by an *ILM* laser. The optical pulses are strongly attenuated. The *QPSK* modulation satisfies independent choices of base and symbol assured by dual-electrode Mach-Zehnder modulators. Three coherent detection schemes are proposed and compared. The successive modifications to our system take to propose a one optical way quantum key distribution scheme by *DQPSK* coding.

# Table des matières

# Liste des figures

# Liste des tableaux

# Notations et abréviations

| | |
|---|---|
| $\|u\rangle$, $\|v\rangle$ | Vecteurs d'états de l'espace $E$ |
| $\phi_1$ | Premier signal de commande du modulateur d'Alice |
| $\phi_2$ | Second signal de commande du modulateur d'Alice |
| $\phi_3$ | Signal de commande du modulateur de Bob |
| $\mu$ | Nombre moyen de photon contenu dans une impulsion optique |
| $A_1$, $A_2$ | Choix de bases d'Alice |
| *Add* | Coupleur radiofréquence |
| Alice | Nom donné à l'émetteur dans le domaine de la cryptologie |
| $B_1$, $B_2$ | Choix de bases de Bob |
| BB84 | Protocole de distribution quantique de clef |
| Bob | Nom donné au récepteur dans le domaine de la cryptologie |
| $C$ | Contraste de l'interféromètre (aussi appelé visibilité) |
| *dark count* | Courant d'obscurité |
| DFB | *Distributed Feed Back* |
| *DPSK* | Modulation différentielle par saut de phase (*Differential Phase Shift Keying*) |
| Eve | Nom donné aux espions dans le domaine de la cryptologie |
| FPGA | Field Programmable Gate Array |
| $h$ | Constante de Planck = 6.62606876 E-34 $J.s^{-1}$ |
| $I_{Alice \rightarrow Bob}$ | Information mutuelle entre Alice et Bob |
| $I_{Alice \rightarrow Eve}$ | Information mutuelle entre Alice et Eve |
| $I_{Eve \rightarrow Bob}$ | Information mutuelle entre Eve et Bob |
| *ILM* | Integrated Electro-absorption Modulator |
| MAO | Modulateur acousto-optique |
| MZ | Modulateur Mach-Zehnder à doubles électrodes |
| PC | Contrôleur de polarisation |
| *QBER* | Taux d'erreur quantique (*Quantum Bit Error Rate*) |
| Qbit | Bit quantique |
| QKD | Quantum Key Distribution |
| *QPSK* | Modulation par saut de phase à 4 états (*Quadrature Phase Shift Keying*) |
| *rms* | *root mean square* : racine carrée du carré moyen |
| *SMF* | Fibre standard monomode |

# Introduction

Les premiers moyens de communication mis en place par l'Homme s'accompagnent d'une nécessité de confidentialité dans la transmission des informations.

Les premiers systèmes de cryptographie apparaissent vers 200 avant JC. Les outils mis en place n'avaient alors pour tache que de rendre difficile la lecture des informations et seule la complexité des mécanismes de cryptage était garante de la confidentialité des messages. Cette complexité, reposant essentiellement sur des systèmes physiques et mécaniques à ses débuts, a évolué au cours du XX$^{ième}$ siècle, vers une complexité mathématique.

Aujourd'hui, la plus part des systèmes de cryptographie classique repose sur des algorithmes mathématiques dont la sécurité et la robustesse au craquage n'ont pas été formellement démontrées. La complexité calculatoire n'oppose que très peu de résistance face à l'augmentation de la puissance de calcul des systèmes informatiques.

Pour obtenir des communications *parfaitement* sécurisées, la théorie de l'information de Shannon impose qu'une clef de cryptage à usage unique soit utilisée dans la transmission d'information, ce qui suppose que les interlocuteurs se seraient préalablement partagés secrètement cette clef. Les communications classiques ne pouvant théoriquement pas générer de secret à distance, il est nécessaire que les interlocuteurs se rencontrent physiquement pour s'échanger des clefs. Cette unique solution contraignante souligne la nécessité de trouver un moyen physique de partager un secret à distance.

Dans les années 60, Stephen Wiesner présente l'importance du principe d'incertitude de Heisenberg, propriété fondamentale de la physique quantique, pour garantir la confidentialité d'une information. Brassard et Bennett élaborent alors en 1984 le « protocole BB84 » autorisant la distribution de clef cryptographique en utilisant un canal quantique. La cryptographie quantique propose une solution simple et sûre au problème de distribution de clef.

La cryptographie quantique est véritablement née en 1992 lorsque Brassard et Bennett ont élaboré un système expérimental permettant la distribution quantique de clef, autorisant une transmission sécurisée en espace libre sur une distance de 30 cm.

Le professeur Philippe Gallion du laboratoire d'optique du département Communications et Electronique à l'Ecole Nationale Supérieure des Télécommunications m'a permis d'effectuer mes travaux portant sur l'élaboration et l'étude d'un système de distribution quantique de clef utilisant le protocole BB84 par codage de phase. La présente thèse se compose de sept chapitres.

Dans un premier temps, le Chapitre 1 définit les systèmes de cryptographie classique et rappelle la nécessité d'utiliser des clefs de cryptage à usage unique pour garantir la confidentialité d'une transmission. Il présente également les bases de la mécanique quantique sur lesquelles repose la cryptographie quantique, solution au problème de distribution de clef entre deux interlocuteurs distants.

Le Chapitre 2 présente le protocole BB84, protocole de distribution quantique de clef utilisé pour générer une information secrète en codant des informations binaires sur une variable physique d'un photon unique. Cette partie met en évidence la sécurité inconditionnelle d'une transmission parfaite reposant sur le protocole BB84.

Un système de distribution quantique de clef se compose de trois sous-modules présentés dans le Chapitre 3 ; la source de photon unique, la chaîne de modulation et le système de détection cohérent. Il n'existe pas encore de source parfaite de photon unique. Une solution palliative et transitoire est d'utiliser une source laser émettant des impulsions très fortement atténuées. La chaîne de modulation permet quant à elle, de transposer des informations binaires sur un paramètre physique, à savoir la phase d'un photon. Dans ce chapitre, un système de détection cohérent est étudié afin de détecter et mesurer la phase des photons uniques.

Le Chapitre 4 décrit les principaux composants utilisés pour l'élaboration d'un système expérimental permettant la distribution quantique de clef par codage de phase. Il présente également leurs caractéristiques essentielles.

Le Chapitre 5 décrit les montages expérimentaux préliminaires nécessaires à la mise en place finale d'un système de cryptographie quantique. Les résultats observés ont été obtenus en régime classique et sans composante aléatoire dans les choix des symboles et des bases. Il est possible, sous certaines conditions, de passer en régime quantique.

Le Chapitre 6 présente notre système de distribution quantique de clef fonctionnant avec un codage *DQPSK* utilisant une voie optique.

Le dernier chapitre, Chapitre 7, présente une étude de la sécurité potentielle du dispositif expérimental proposé. De plus il définit les conditions et les limites d'utilisation de notre dispositif.

# Chapitre 1.
# Introduction à la cryptographie

## 1.1 Cryptographie classique

L'Histoire nous prouve que l'Homme s'est toujours appliqué à cacher l'information des messages qu'il ne souhaitait pas voir interceptée par autrui. Il n'a eu de cesse de développer cette science appelée *cryptographie*. Parallèlement, l'Homme a mis en place l'art de percer le secret des messages qui ne lui étaient pas destinés en développant la *cryptanalyse*. Ces deux sciences constituent la *cryptologie*.

### 1.1.1 L'Histoire des Codes et des Chiffres

Depuis les premières civilisations, les Hommes ont recherché à se doter de moyens de communications efficaces pour gouverner leurs territoires et commander leurs armées.

Ces besoins s'accompagnent d'une nécessité de confidentialité avec la mise en place de services secrets, chargés d'assurer la sécurité des communications par l'invention et la mise en œuvre de codes et de chiffres. Parallèlement, ces services sont chargés d'espionner et de briser les codes des autres services. L'Histoire des Codes et des Chiffres n'est qu'une bataille ininterrompue jusqu'à aujourd'hui entre les codeurs et les briseurs de codes.

Certes les premières civilisations n'utilisaient pas à proprement parler des codes, mais plutôt des techniques pour cacher l'existence même du message.

Au V$^{ième}$ siècle avant JC, Hérodote rapporte dans ses écrits comment Demaratus, grec expulsé en Perse, transmit aux Spartiates le plan d'invasion de la Grèce par le perse Xerxès. Sa ruse consistait à enlever la cire sur une tablette de bois pliante, puis de graver le message sur le bois et enfin de couvrir à nouveau de cire le message. La tablette de cire apparaissait alors vierge.

Ce mode de communication secrète obtenu en dissimulant l'existence d'un message est appelé *stéganographie* (du grec *steganos* signifiant *couvert* et *graphein* signifiant *écriture*).

Parallèlement, la cryptographie (du grec *kryptos* signifiant *caché*) se développe. Cette fois, il ne s'agit plus de dissimuler le message, mais de masquer son sens. L'un des premiers cryptage fut utilisé au temps de l'Egypte Ancienne. Il consistait à établir une correspondance entre un alphabet clair (lettres qui composent le message originel) et un alphabet chiffré (lettres substituées au message d'origine). Ce procédé de substitution alphabétique fut complété au fil du temps avec des procédés de transposition, de combinaison, de substitutions monoalphabétiques et polyalphabétiques… Ce n'est qu'à partir de la Renaissance que l'usage de la cryptographie supplante celui de la stéganographie dans les correspondances militaires et diplomatiques.

En 1830, l'invention du télégraphe révolutionne le monde des communications. Pour réduire la taille des messages, des livres de codes étaient distribués à chaque opérateur. Ils permettaient d'établir une correspondance entre un symbole de code et un mot, voir une phrase, du message à transmettre. Le principe des livres de codes fut utilisé par la suite pour transmettre secrètement des messages. L'expéditeur et le destinataire devaient alors être les seuls à posséder le même livre de code.

En 1883, Auguste Kerckhoffs établit une liste de critères garantissant à l'époque, la confidentialité d'un système de cryptographie. Aujourd'hui, la plupart de ces critères restent valables malgré les avancés technologiques et théoriques. L'un de ces critères impose l'utilisation de clefs de chiffrement et c'est en 1917 que Vernam propose le seul code utilisant une clef inconditionnellement sûre, pour peu que la clef ne soit utilisée qu'une seule fois et qu'elle soit aussi longue que le message à transmettre. Le téléphone rouge reliant Moscou et Washington repose sur ce code.

Se pose alors le problème de distribution de clef entre l'émetteur et le destinataire…

### 1.1.2 Les principes de Kerckhoffs

En 1883, Auguste Kerckhoffs publie dans le Journal des sciences militaires un article dans lequel il expose six principes que doit remplir un système cryptographique opérationnel [1]. Aujourd'hui encore, les trois premiers critères sont à la base de tout nouveau système de cryptographie. Quant aux trois derniers, ils sont considérés comme obsolètes ou non essentiels.

*1 - Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;*
*2 - Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;*
*3 - La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;*
*4 - Il faut qu'il soit applicable à la correspondance télégraphique ;*
*5 - Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;*
*6 - Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.*

Tableau 1 Principes de Kerckhoffs.

Ces six principes étaient destinés à un usage militaire et concernaient un système de cryptographie à l'usage de l'ensemble d'un corps armé.

### 1.1.3 Le code de Vernam

En 1917, le major Joseph Mauborgne et Gilbert Vernam élaborent un cryptosystème appelé *masque jetable* ou *code de Vernam* [2].

Dans sa forme classique, le masque jetable n'est qu'une longue suite non répétitive et aléatoire de lettres qu'utilisera Alice (Figure 1), pour chiffrer le message, et Bob, pour le déchiffrer.

L'algorithme de chiffrement est simple, puisqu'il suffit d'ajouter le rang de la lettre à chiffrer au rang de la lettre correspondant au masque. Le résultat modulo 26 donne le rang de la lettre du texte chiffré. Le déchiffrement est obtenu en suivant le même algorithme.

L'idée du masque jetable peut être étendue au chiffrement de données binaires. Dans ce cas, le texte chiffré est obtenu en utilisant l'opérateur logique *ou exclusif* sur le texte à chiffrer et le masque jetable.

Le code de Vernam est reconnu comme inviolable mathématiquement puisque c'est le seul, à ce jour, qui obéit aux critères de Shannon. En effet, Shannon a démontré [3] que la sécurité d'un message chiffré ne peut être absolue que si chaque message échangé entre deux personnes est chiffré avec une clef aussi longue que celui-ci et que cette clef doit être différente pour chaque message chiffré échangé.

### 1.1.4 Les crypto-systèmes

Le processus de chiffrement consiste à transformer un texte lisible par tous en texte chiffré, incompréhensible pour tout individu qui n'est pas le destinataire. Cette opération est réalisée avant toute communication entre deux entités ; l'expéditeur nommé Alice et le destinataire, Bob. Le processus inverse est appelé déchiffrement. Un crypto-système peut être schématisé par la Figure 1. En notant :

- $k_i$ la clef $i$ utilisée lors de l'encodage ou du décodage $\in \boldsymbol{K}$, ensemble des clefs,
- $x$ le message originel,
- $y$ le message chiffré,
- $c_{k1}( )$ l'opération de chiffrement avec la clef $k_1$,
- $d_{k2}( )$ l'opération de déchiffrement avec la clef $k_2$,

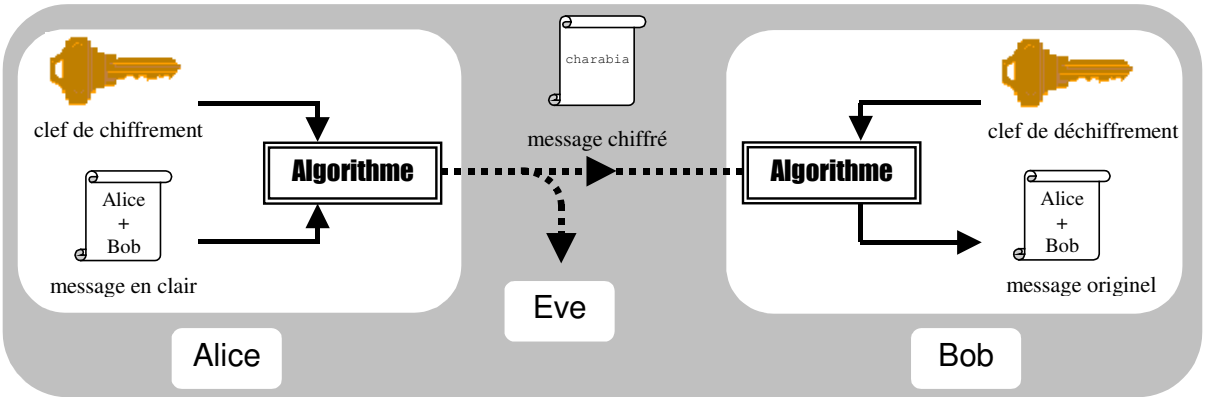



Figure 1 Synoptique d'une transmission sécurisée.

Un crypto-système doit obéir mathématiquement aux opérations

$$\begin{cases} y = c_{k_1}(x) \\ x = d_{k_2}(y) = d_{k_2}\left(c_{k_1}(x)\right) \end{cases} \quad (1)$$

Le chiffrement et le déchiffrement utilisent des algorithmes, souvent mathématiques, appelés *crypto-systèmes*. Deux types peuvent être distingués.

- Les algorithmes restreints, dont la sécurité repose sur le fait qu'ils sont tenus secrets.
- Les algorithmes à clef qui peut être privée ou publique.

#### 1.1.4.1 Les algorithmes restreints

Les algorithmes restreints basent leur sécurité sur le fait qu'ils sont tenus secrets. Ainsi connaître un algorithme restreint qui a servi à coder des messages, permet à posteriori de décoder l'ensemble de ces messages.

Un groupe d'individu désirant communiquer confidentiellement, ne peut utiliser de tels algorithmes. En effet, chaque fois qu'un membre quitte le groupe, un nouvel algorithme doit être créé sous peine que l'individu exclu n'ait la possibilité de continuer à lire les messages.

La cryptographie moderne résout ce problème par l'utilisation de clefs. Ces clefs prennent des valeurs parmi un grand nombre de valeurs possibles. L'ensemble de ces clefs est appelé espace des clefs.

Avec les algorithmes à clefs, toute la sécurité repose sur les clefs, et non plus sur la connaissance de l'algorithme ou celle du matériel. Ceux-ci peuvent même être connus de tous.

#### 1.1.4.2 Les algorithmes à clef secrète

Les algorithmes à clef secrète sont aussi appelés algorithmes symétriques. Ce sont des algorithmes où la clef de déchiffrement peut être calculée à partir de la clef de chiffrement (ou vice versa). Dans la plupart des cas, les clefs sont identiques. Dans l'équation (1), $k_1=k_2$. Il y a donc nécessité d'entente préalable entre Alice et Bob sur le choix de clefs communes, et ceci avant toute communication sécurisée. Pour ces algorithmes, la confidentialité des communications est directement liée au fait que les clefs doivent demeurer secrètes. Le DES (*Data Encryption Standard*) est un exemple de protocole de cryptographie à clef secrète.

Le code de Vernam est un algorithme symétrique inconditionnellement sûr, mais il pose des problèmes de distribution de clefs.

#### 1.1.4.3 Les algorithmes à clef publique

Les algorithmes à clef publique sont encore appelés cryptosystèmes asymétriques. Ils sont conçus de façon à ce que la clef de déchiffrement ne puisse pas être calculée, dans des temps raisonnables, à partir de la clef de chiffrement. Du coup, la clef de chiffrement peut être rendue publique, d'où le nom de ces algorithmes. La clef de déchiffrement est aussi appelée clef privée. Le RSA (du nom des inventeurs R. Rivest, A. Shamir et L. Adleman) est le plus connu et le plus utilisé comme cryptosystème à clef publique [4].

### 1.1.5 Sécurité des algorithmes

Les différents algorithmes ont des niveaux de sécurité divers, c'est-à-dire plus ou moins difficiles à casser. Cependant leur sécurité ne se réduit pas au simple fait qu'ils soient cassables ou non, c'est plutôt un rapport entre le coût nécessaire pour les casser et la valeur de l'information chiffrée.

Ainsi, si le temps nécessaire pour casser l'algorithme est plus long que le temps durant lequel l'information chiffrée doit rester secrète, alors l'algorithme est considéré comme sûr.

Et s'il faut plus d'information pour casser un algorithme qu'il n'en a été chiffré avec la même clef, alors l'algorithme est sûr.

Il est plus juste d'utiliser le terme probablement, car il est toujours possible qu'une nouvelle avancée soit faite en cryptanalyse. D'un autre coté, une information perd de sa valeur avec le temps. Il est important que la valeur d'une information reste toujours inférieure au coût nécessaire pour briser la protection qui l'entoure.

Un algorithme est inconditionnellement sûr si, quelle que soit la quantité de texte chiffré dont le cryptanaliste dispose, il n'y a pas d'information suffisante pour retrouver le texte en clair. De fait, seul le code de Vernam est invulnérable. Tous les autres cryptosystèmes sont vulnérables à une attaque à texte chiffré seulement, simplement en essayant toutes les clefs possibles une par une et en regardant si le texte en clair résultant a un sens.

La cryptographie se préoccupe plus particulièrement de cryptosystèmes invulnérables par calcul. Un algorithme est considéré invulnérable par calcul, s'il ne peut être cassé avec les ressources disponibles actuellement et dans le futur. Ce qui constitue ces « ressources disponibles » est ouvert à interprétation.

Depuis une trentaine d'années, la puissance de calcul des ordinateurs augmente de façon exponentielle et il n'y a pas de raison de penser que cela s'arrête de si tôt. Nombre d'attaques cryptanalytiques sont très bien adaptées aux machines fonctionnant en parallèles : la tâche peut être morcelée en milliards de petites tâches et aucun des processeurs ne doivent interagir avec les autres. Annoncer qu'un algorithme est sûr simplement parce qu'on ne peut pas le casser avec la technologie d'aujourd'hui est hasardeux. Les bons cryptosystèmes sont conçus pour être invulnérables même avec les puissances de calcul prévues d'ici à de nombreuses années dans le futur.

### 1.1.6 Distribution publique de clef

La confidentialité d'un message repose donc uniquement sur deux critères :

- la taille de la clef doit être aussi longue que celle du message à chiffrer
- la clef ne doit être utilisée qu'une seule fois.

Se pose alors le problème de distribution des clefs. Comment attribuer à chaque membre d'un réseau de communication des clefs secrètes ?

La première solution à cet épineux problème serait que chaque membre se rencontre et qu'ils échangent une clef secrète. Ils peuvent également se servir d'une tierce personne. Mais ces deux solutions sont lentes et ne sont pas forcement sûres (surtout si un intermédiaire est utilisé), d'où la nécessité d'élaborer un système de distribution publique de clef.

Le but d'un tel système est de permettre à deux personnes d'obtenir une clef secrète en communiquant sur un canal public (c'est-à-dire susceptible d'être espionné), de manière qu'un espion ne puisse reconstituer la clef, même si celui-ci écoute toute la communication.

Le canal étant public, la discussion entre Alice et Bob est publique, d'où distribution publique.

Soulignons que Eve (l'espion) peut écouter la discussion, mais en aucun cas, ne peut corrompre la communication entre Alice et Bob sur ce canal public en se faisant passer pour l'un d'eux. En effet, il est possible de vérifier l'identité de chaque intervenant en utilisant des protocoles d'authentification. De plus, Eve est supposée écouter la communication et non l'interrompre.

## 1.2 Cryptographie quantique

La *cryptographie quantique* n'est pas en soi un nouveau procédé de cryptographie. En effet, la cryptographie quantique ne permet pas directement la communication de messages intelligibles, mais autorise (principalement) la distribution de clef cryptographique, ce qui conduit souvent à désigner la *distribution quantique de clef* (Quantum Key Distribution) par le terme plus général de *cryptographie quantique*. Elle apparaît donc comme un complément de la cryptographie classique, puisqu'elle répond à son besoin de distribution de clef privée. La sécurité de cette méthode repose sur les lois de la mécanique quantique et est considérée comme inconditionnellement sûre.

### 1.2.1 De la mécanique quantique à la cryptographie quantique

Au début du XX$^{ième}$ siècle, le monde scientifique cherche à unifier les phénomènes physiques macroscopiques et microscopiques en étudiant les interactions lumière-matière.

En 1900, avec la théorie des quanta, Planck postule que l'émission et l'absorption de lumière par un corps ne peut se faire que par paquets entiers d'énergie. Il définit ainsi la constante *h* nommée constante de Planck. Cette théorie permet de quantifier les échanges d'énergie entre lumière et matière. De là, Bohr construit en 1916 le modèle de l'atome d'hydrogène en modélisant le noyau à une planète et l'électron à son satellite.

C'est Einstein qui introduit le premier, en 1905, la quantification de l'énergie rayonnante en décrivant la lumière comme des grains, ce qui lui permet d'expliquer l'effet photo-électrique. Gilbert Newton Lewis proposera en 1926 le terme photon. Ce nouveau concept est vérifié en 1923 par l'observation de l'effet Compton. Cependant cette vision corpusculaire de la lumière est en contradiction avec les phénomènes d'interférences qui avaient conduit à consolider à la fin du XIX$^{ième}$ le caractère ondulatoire de la lumière.

Dès lors, la lumière est considérée soit comme une onde, soit comme une particule en fonction des phénomènes observés. Mais en 1923, De Broglie réussit à allier sous certaines conditions, ces deux caractères paradoxaux en l'étendant aux électrons et en associant une onde à chaque corps matériel.

Cependant, toutes ces approches reposaient sur des suppositions arbitraires sans grandes cohérences entre elles. Heisenberg, en 1925, unifie mathématiquement les diverses approches en proposant un formalisme matriciel, appelé Mécanique des Matrices, fondé sur l'analyse harmonique du mouvement classique revisité à la lumière des conditions de quantification de Bohr.

La mécanique des matrices fonde les bases de la mécanique quantique qui s'enrichit en 1926 de l'approche de Schrödinger, dont l'objet central est une fonction d'onde, à valeurs complexes, satisfaisant à l'équation qui porte désormais son nom [4].

Les prémices de cryptographie quantique sont apparues à la fin des années 60 dans un article non-publié à l'époque, de Stephen Wiesner [6]. Il y explique l'importance du principe d'incertitude de Heisenberg dans le codage de billet de banque garantissant leur infalsification. De plus, il propose l'utilisation d'un canal quantique multiplexeur permettant d'entremêler deux messages de telle façon que lire l'un d'eux rend l'autre illisible.

En 1979, Charles H. Bennett et Gilles Brassard reprirent ses travaux et conçurent un système de distribution de clefs secrètes reposant sur la mécanique quantique [7]. Peu de

temps après, en 1983, l'article de Wiesner fut publié [6]. Désormais, le photon serait utilisé pour le transport de l'information, et non pour le stockage.

En 1984, C. H. Bennett et G. Brassard définissent le protocole de distribution de clés ; le BB84. Mais c'est seulement en 1991 que la fiction devient réalité, lorsqu'ils parviennent à implémenter le premier protocole de distribution quantique de clefs.

Depuis, la cryptographie quantique apparaît comme le successeur de celle basée sur les mathématiques et son principe est décrit dans de nombreux magazines de vulgarisation.

### 1.2.2 Notions de mécanique quantique

La mécanique quantique est connue pour ne pas être une science intuitive. Dans cette partie, nous présenterons succinctement les notions de mécanique quantique sur lesquelles repose la cryptographie quantique.

#### 1.2.2.1 Etat d'un système

La mécanique quantique permet de décrire l'état d'un système quantique par l'étude de sa fonction d'onde (solution de l'équation de Schrödinger (2)) qui a, fondamentalement, une interprétation statistique et ne prétend donc pas décrire l'état du système en particulier au sens classique. La description de l'état d'un système quantique consiste donc en l'énoncé des lois de probabilités permettant d'en décrire les propriétés et de fournir une explication du monde à l'échelle atomique.

La connaissance de l'état d'un système à un instant *t* donné est complètement contenue dans un vecteur appelé *vecteur d'état*, noté $|\psi(t)\rangle$, solution de l'équation (2). L'espace vectoriel auquel appartient ce vecteur est appelé *espace d'états* $\varepsilon$ défini sur le corps des complexes.

$$i\hbar\frac{\partial}{\partial t}\psi(\vec{r},t)=\left[-\frac{\hbar^2}{2m}\vec{\nabla}^2+V(\vec{r})\right]\psi(\vec{r},t) \tag{2}$$

où $\vec{r}$ est le vecteur repérant la particule dans l'espace ; $V(\vec{r})$ est l'énergie potentielle de la particule étudiée, $\vec{\nabla}$ est le vecteur gradient.

La cryptographie quantique utilise des particules quantiques pour transmettre de l'information portée par la valeur de l'une de ses variables d'état. Une variable d'un système quantique peut être modélisée dans un espace hermitien ***E***. Un état particulier est alors décrit par un vecteur d'état appelé *ket* et noté $|\psi(t)\rangle \in \boldsymbol{E}$ . Cet espace ***E*** est muni d'un produit scalaire $\langle\varphi|\psi\rangle$ où $|\psi\rangle \in \boldsymbol{E}$ et $\langle\varphi| \in \boldsymbol{E}^*$, l'espace dual de *E*, est appelé *bra*. Le produit scalaire est quant à lui appelé *braket*. Il suit les propriétés suivantes,

$$\begin{aligned}
&\forall \lambda_1, \lambda_2 \in C,\\
&\forall \varphi, \varphi_1, \varphi_2, \psi, \psi_1, \psi_2 \in \boldsymbol{E},\\
&\bullet \langle \lambda_1\varphi_1 + \lambda_2\varphi_2 | \psi\rangle = \lambda_1^* \langle\varphi_1|\psi\rangle + \lambda_2^* \langle\varphi_2|\psi\rangle\\
&\bullet \langle \lambda\varphi | \lambda_1\psi_1 + \lambda_2\psi_2\rangle = \lambda_1 \langle\varphi|\psi_1\rangle + \lambda_2 \langle\varphi|\psi_2\rangle\\
&\bullet \langle\psi|\psi\rangle \in R^+
\end{aligned} \tag{3}$$

#### 1.2.2.2 Mesure d'un état quantique

A chaque grandeur physique susceptible d'être mesurée est associée un opérateur linéaire auto-adjoint $\hat{A}$ agissant dans $\boldsymbol{E}$ et appelé observable. Les résultats possibles de la mesure de $A$ sont les valeurs propres de l'observable $\hat{A}$. La mesure est dite projective car le résultat est une valeur propre de l'observable et l'état devient un état propre de l'observable. La probabilité de trouver la valeur $|\alpha(t)\rangle$ lors d'une mesure de $A$ effectuée sur un système dans l'état quelconque $|\psi(t)\rangle$ est alors

$$P(\alpha) = |\langle \alpha | \psi(t) \rangle|^2 \tag{4}$$

De plus, juste après une mesure de $A$ ayant donné $\alpha$ comme résultat, le nouvel état du système noté $|\psi_{proj}(t)\rangle$ est égal à la projection de $|\psi(t)\rangle$ sur le sous-groupe propre associé à $\alpha$

$$|\psi_{proj}(t)\rangle = \frac{\langle \alpha | \psi(t) \rangle}{|\langle \alpha | \psi(t) \rangle|} |\alpha\rangle \tag{5}$$

Si une seconde mesure est effectuée sur $|\psi(t)\rangle$, la probabilité de trouver $\alpha$ est de 1. La première mesure de $|\psi(t)\rangle$ a donc perturbé l'état du système.

#### 1.2.2.3 Le principe d'incertitude de Heisenberg

Le principe d'incertitude montre qu'il est impossible d'attribuer à un corpuscule, à un instant donné, par exemple une position et une quantité de mouvement parfaitement déterminées. Il est impossible de mesurer simultanément, avec une précision absolue, la position $p$ et la vitesse $q$ d'une particule dans le domaine de l'atome, car la mesure perturbe le système. En effet, il faut utiliser des ondes très courtes afin de saisir la position de la particule. Or ces ondes sont, par exemple, des photons qui communiquent une énergie à la particule et change du même coup sa position. L'imprécision résultante a été évaluée par Heisenberg. Le produit des valeurs *rms* des variables considérées est borné par la constante de Planck.

$$\Delta p . \Delta q \geq h \tag{6}$$

#### 1.2.2.4 Le clonage des photons

En 1982, W. K. Wooters et W. H. Zurek ont démontré qu'il était impossible de cloner un état quantique arbitraire et inconnu [8].

Pour preuve, supposons qu'Eve ait réalisé une photocopieuse quantique. Par définition, la photocopieuse réalise l'opération

$$|blanc\rangle|\psi\rangle \Rightarrow |\psi\rangle|\psi\rangle \tag{7}$$

avec $|blanc\rangle$ l'état initial du photon qui servira de « feuille blanche ».

Si $|\psi\rangle$ représente une polarisation horizontale notée $|H\rangle$, alors

$$|blanc\rangle|H\rangle \Rightarrow |H\rangle|H\rangle \tag{8}$$

Si $|\psi\rangle$ représente une polarisation verticale notée $|V\rangle$, alors

$$|blanc\rangle|V\rangle \Rightarrow |V\rangle|V\rangle \tag{9}$$

Si $|\psi\rangle$ est une combinaison linéaire des états $|H\rangle$ et $|V\rangle$, alors l'état initial de la photocopieuse s'écrit également

$$|blanc\rangle(\alpha|H\rangle + \beta|V\rangle) = \alpha|blanc\rangle|H\rangle + \beta|blanc\rangle|V\rangle \tag{10}$$

Des équations (8) et (9), l'opération de copie d'un état résultant d'une superposition d'états propres est alors

$$|blanc\rangle(\alpha|H\rangle + \beta|V\rangle) \Rightarrow \alpha|H\rangle|H\rangle + \beta|V\rangle|V\rangle \tag{11}$$

Le résultat représenté par l'équation (11) est, en général, différent du résultat souhaité, à savoir

$$(\alpha|H\rangle + \beta|V\rangle)(\alpha|H\rangle + \beta|V\rangle) = \alpha^2|H\rangle|H\rangle + \alpha\beta|H\rangle|V\rangle + \beta\alpha|V\rangle|H\rangle + \beta^2|V\rangle|V\rangle \tag{12}$$

L'équation (11) n'est exacte que pour les états propres.

#### 1.2.2.5 Les photons intriqués

Deux photons sont intriqués quand ils sont, par exemple, générés par la désexcitation d'un même atome et qu'ils se propagent dans deux directions opposées. Des photons intriqués présentent la propriété suivante : lorsqu'une mesure est effectuée dans une certaine base de l'un des deux photons, la mesure de l'autre photon dans la même base donne toujours un résultat entièrement déterminé par le résultat de la première mesure.

On pourrait ainsi croire que l'information du premier photon se propage instantanément (i.e. plus vite que la lumière) au deuxième. Or ceci est une violation des lois de la relativité (rien ne peut aller plus vite que la lumière). En 1935, Einstein, Podolski et Rosen sont les premiers à présenter ce paradoxe désormais connu sous le nom de paradoxe EPR [9].

Mais il n'en est rien. En effet, le photon ne porte pas d'information, puisque l'information est issue de la mesure. De plus, le résultat de la première mesure est aléatoire, ce qui signifie qu'aucune information connue et déterminée n'est transmise.

Certains protocoles de cryptographie quantique nécessitent l'utilisation de photons intriqués [10], leur sécurité reposant sur les propriétés de ces photons. La génération de photons corrélés permet également de constituer des sources à photons uniques [11].

### 1.2.2.6 Mesure d'un photon polarisé

De la lumière polarisée peut être obtenue en faisant passer un rayon de lumière à travers un polariseur. L'axe de polarisation du faisceau est déterminé par l'orientation du polariseur d'où émerge le faisceau. La production de photons polarisés isolés est théoriquement possible mais n'est, à l'heure actuelle, pas réalisable d'un point de vue technologique. Pour simplifier, nous ferons comme s'il était réaliste d'obtenir de tels photons isolés avec une polarisation définie.

Si un faisceau lumineux avec un angle de polarisation α traverse un filtre orienté selon un angle β, les photons individuels se répartissent de manière dichotomique et probabiliste, chacun étant transmis avec une probabilité $cos^2\ (\alpha\text{-}\beta)$ ou absorbé avec une probabilité complémentaire $sin^2\ (\alpha\text{-}\beta)$. Les photons se comportent de manière déterministe seulement lorsque les deux axes sont parallèles (transmission certaine) ou perpendiculaires (absorption certaine).

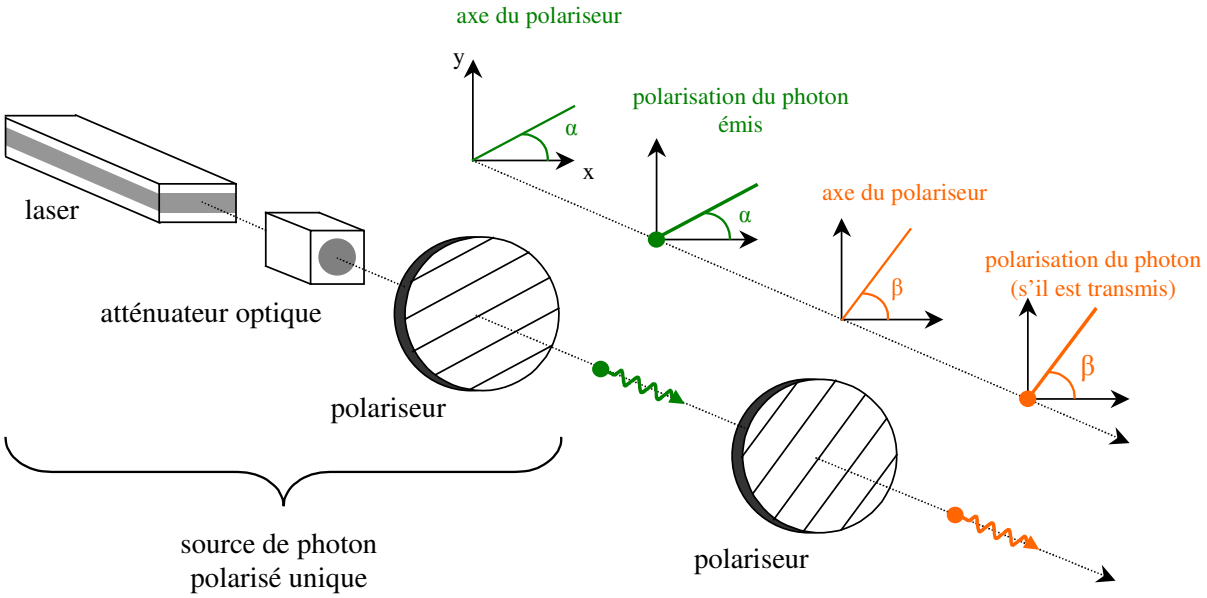



Figure 2 Mesure d'un photon polarisé linéairement.

Il est important de souligner que les photons perdent leurs polarisations initiales une fois qu'ils passent au travers d'un polariseur. A la sortie d'un polariseur orienté selon un angle α, les photons portent la polarisation α du polariseur, ce qui interdit une nouvelle mesure. Par contre, il est possible d'effectuer plusieurs mesures différentes sur des photons distincts d'un même faisceau de manière à déterminer la polarisation des photons du faisceau. Mais cela suppose que le faisceau soit constitué de plusieurs photons de polarisation identique. Cette approche ne peut donc pas aider à mesurer la polarisation d'un photon isolé.

### 1.2.3 Principe de la cryptographie quantique

La cryptographie quantique repose sur ces principales notions de mécanique quantique pour interdire à un espion de connaître des informations échangées entre deux entités, Alice et Bob.

Si Eve tente d'intercepter les signaux envoyés par Alice, elle doit effectuer une mesure sur ceux-ci, et obligatoirement les perturber. Cette perturbation peut être évaluée par Bob, ce qui lui permet de détecter la présence d'Eve.

La cryptographie quantique repose sur l'utilisation de deux canaux. L'un est obligatoirement quantique, i.e. capable de transmettre des objets régis par les lois de la mécanique quantique (par exemple un photon transmis par fibre optique), le second est un canal classique qui peut être écouté par Eve, mais qu'elle ne peut modifier.

Il est impossible d'empêcher Eve d'écouter discrètement le canal quantique, mais il est possible de le savoir. Par conséquent, la cryptographie quantique ne permet pas d'échanger directement des messages, mais permet l'échange de données aléatoires qui constituent une clef. Si la ligne n'a pas été écoutée, il est alors possible de se servir de la clef pour chiffrer classiquement le message en utilisant la technique du masque jetable appliquée à une transmission de données binaires, encore appelée *one-time pad*.

# Chapitre 2.
# Distribution quantique de clef

Dans une première partie, nous présenterons le principe du protocole BB84 codant la polarisation ou la phase de photons uniques ou de photons intriqués. Puis nous définirons la sécurité de ce protocole dans les cas idéaux d'une absence totale de bruit sur la ligne et de l'utilisation de composants parfaits. En fin, nous évaluerons la confidentialité d'une transmission utilisant ce protocole face à l'intervention d'un espion.

## 2.1 Protocole de distribution quantique de clef ; BB84

Le protocole de distribution quantique de clef, élaboré en 1984 par Charles Bennett et Gilles Brassard, permet à deux correspondants d'échanger une clef de chiffrement [12]. De nombreuses réalisations expérimentales utilisant des variables physiques à valeurs discrètes, codées sur des photons uniques, reposent sur l'utilisation de ce protocole [13][14][15][16].

Alice et Bob disposent d'un canal de transmission quantique (fibre optique, espace libre) et d'un canal public (radio, internet).

### 2.1.1 Codage sur la polarisation

Alice et Bob adoptent la même convention pour les bases et les symboles (Figure 3).

Alice transmet à Bob une série de bits choisis aléatoirement afin de constituer une clef de chiffrement unique. Chaque choix de bits est codé par modulation d'un paramètre physique, la polarisation sur un système quantique, un photon unique.

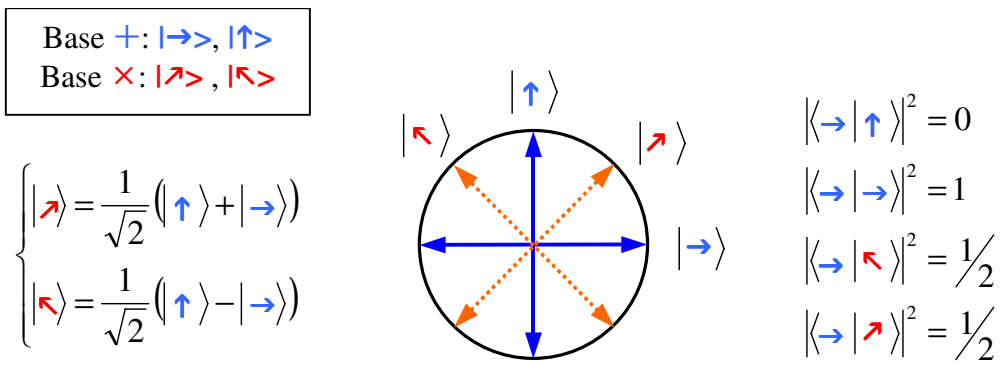



Figure 3 Représentation des 4 états de polarisation.

Bob détermine chaque bit transmis en mesurant l'état du photon. Pour assurer la sécurité de cette communication, Alice et Bob utilisent deux bases dites conjuguées, notées + et ×, dans lesquelles les vecteurs propres correspondent aux deux symboles notés 0 et 1. Par

définition, deux bases conjuguées sont telles que toute mesure d'un photon sur une des bases et codé dans l'autre donne un résultat complètement aléatoire et entraîne la perte de toute information.

Le protocole BB84 nécessite quatre états de codage qui constituent deux bases conjuguées. Chaque état est codé par une polarisation linéaire.

| **Alice** (étape 1) | | | **Bob** (étape 2) | | | **Alice et Bob** (étape 3 ) | |
|---|---|---|---|---|---|---|---|
| choix de base | choix de symbole | état du photon émis | choix de base | résultat de la mesure | clef brute | coïncidence de base | clef finale |
| + | 0 | → | × | ↖ | 1 | | |
| | | | | ↗ | 0 | | |
| | | | + | → | 0 | ✓ | 0 |
| × | 1 | ↖ | × | ↖ | 1 | ✓ | 1 |
| | | | + | → | 0 | | |
| | | | | ↑ | 1 | | |
| + | 1 | ↑ | × | ↖ | 1 | | |
| | | | | ↗ | 0 | | |
| | | | + | ↑ | 1 | ✓ | 1 |
| × | 0 | ↗ | × | ↗ | 0 | ✓ | 0 |
| | | | + | → | 0 | | |
| | | | | ↑ | 1 | | |

Tableau 2 Table de vérité du protocole BB84 (polarisation).

Ce protocole se décompose en trois étapes.

1. Alice choisit aléatoirement l'un des deux symboles (0 ou 1) et l'une des deux bases (+ et ×). Elle code ses choix sur la polarisation d'un photon et le transmet à Bob via un canal quantique.
2. Bob choisit aléatoirement une base (+ et ×) pour effectuer sa mesure.

Les étapes 1 et 2 sont reproduites plusieurs fois afin qu'Alice et Bob aient une première série de bits. Les bits de Bob étant le résultat d'une mesure effectué dans une base choisie aléatoirement, ne sont pas identiques à ceux d'Alice. Par conséquent, la série de Bob comporte en principe 25 % d'erreurs, résultant des anticoïncidence de bases et est appelée clef brute (*raw key*).

3. Sur un canal public, Bob révèle à Alice son choix de base pour chaque photon reçu. Si leurs choix de bases coïncident, Bob déduit de sa mesure le bit transmis par Alice. Sinon, Alice et Bob écartent le bit correspondant. A la fin de cette étape de réconciliation, Alice et Bob ont en commun une série de bits identiques constituant la clef de chiffrement appelée clef raffinée (*sifted key*).

Avant l'étape 3, la série de bit de Bob présente un taux d'erreur moyen de 25 % par rapport à celle d'Alice. L'étape de réconciliation (étape 3) permet de ramener en principe le taux d'erreur à 0. En contrepartie, la taille de leur série commune est réduite de moitié par rapport à la série émise par Alice.

### 2.1.2 Codage sur la phase

L'idée de coder la valeur d'un bit quantique sur la phase d'un photon a été mentionnée pour la première fois par Bennett [17] en 1992. Il utilisait alors le protocole B92 nécessitant deux états non-orthogonaux. Le codage sur la phase optique d'un photon peut être étendu au protocole BB84 à la condition d'utiliser un système de détection adapté.

A l'émission, le protocole BB84 nécessite deux bases conjuguées, notées $A_1$ et $A_2$. Les vecteurs propres de ces bases codent les deux symboles binaires (0 et 1) et adoptent, dans l'espace des phases, quatre valeurs différentes (Figure 4). A la réception, Bob se place dans l'une des deux bases (notées $B_1$ et $B_2$) pour effectuer sa mesure (Figure 5).

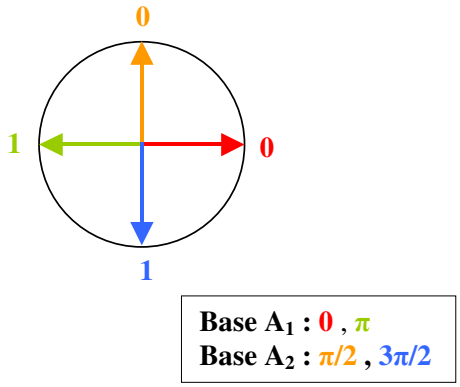



Figure 4 Valeurs des 4 états de phase à l'émission.

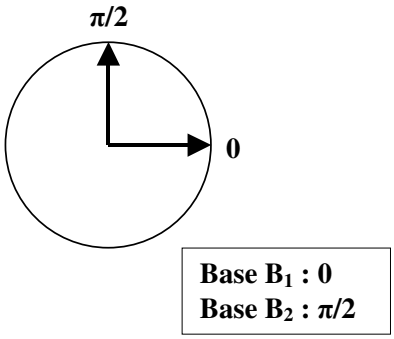



Figure 5 Valeurs des déphasages additifs représentant les bases de réception.

Le fonctionnement du protocole BB84 par codage de phase est identique à celui par codage sur la polarisation.

1. Alice transmet une séquence binaire, résultat d'une suite de choix aléatoires de la base et des symboles. Elle encode chaque bit sur la phase d'un photon.

2. Bob mesure l'état quantique du photon sur une des deux bases qu'il choisit aléatoirement.
3. Puis sur un canal classique, Alice et Bob échangent publiquement leur choix de base définitive. Lorsqu'il y a coïncidence, ils conservent alors les symboles correspondants, constituant ainsi une clef de chiffrement commune.

Le Tableau 3 présente la table de vérité relative au protocole BB84 par codage de phase.

| Alice | | | Bob | | | Alice et Bob | |
|---|---|---|---|---|---|---|---|
| choix de base | choix de symbole | $\phi_{Alice}$ | choix de base | $\phi_{Bob}$ | $\phi_{Alice+Bob}$ | coincidence | clef finale |
| $A_1$ | 0 | 0 | $B_1$ | 0 | 0 | ✓ | 0 |
| | | | $B_2$ | $\pi/2$ | $\pi/2$ | | |
| | 1 | $\pi$ | $B_1$ | 0 | $\pi$ | ✓ | 1 |
| | | | $B_2$ | $\pi/2$ | $3\pi/2$ | | |
| $A_2$ | 0 | $\pi/2$ | $B_1$ | 0 | $\pi/2$ | | |
| | | | $B_2$ | $\pi/2$ | $\pi$ | ✓ | 0 |
| | 1 | $3\pi/2$ | $B_1$ | 0 | $3\pi/2$ | | |
| | | | $B_2$ | $\pi/2$ | 0 | ✓ | 1 |

Tableau 3 Table de vérité du protocole BB84 (phase).

### 2.1.3 Codage sur la polarisation de photons intriqués

Le protocole E.P.R. (Einsten, Podolski, Rosen) est une variante du protocole BB84 par codage de polarisation. Il nécessite quatre états quantiques distincts. Le canal de transmission du photon entre Alice et Bob est remplacé par un canal ayant en son milieu une source de paires de photons intriqués. Les deux photons intriqués sont émis dans des directions différentes ; l'un vers Alice, l'autre vers Bob.

Le fonctionnement de ce protocole suit trois étapes.

1. La source émet une paire de photons intriqués codée dans l'un des quatre états qu'elle choisit aléatoirement (choix aléatoires de la base et du symbole),
2. Alice et Bob mesurent l'état du photon qu'ils reçoivent dans une des deux bases qu'ils choisissent aléatoirement et séparément,
3. Alice et Bob ne conservent leurs mesures que si leurs choix de base de mesure coïncident avec le choix de base de la source.

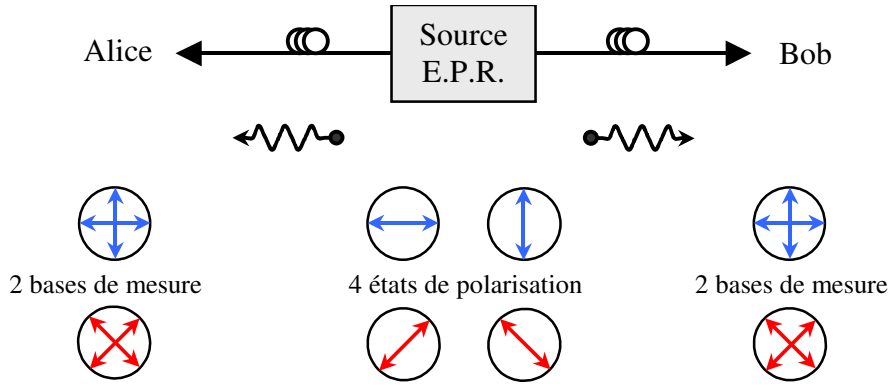



Figure 6 Synoptique du protocole EPR.

| Source EPR | | | Alice | Bob | Alice et Bob | |
|---|---|---|---|---|---|---|
| choix de base | choix de symbole | état | choix de base | choix de base | coïncidence des 3 bases | clef finale |
| + | 0 | → | + | + | ✓ | 0 |
| | | | | × | | |
| | | | × | + | | |
| | | | | × | | |
| | 1 | ↑ | + | + | ✓ | 1 |
| | | | | × | | |
| | | | × | + | | |
| | | | | × | | |
| × | 0 | ↖ | + | + | | |
| | | | | × | | |
| | | | × | + | | |
| | | | | × | ✓ | 0 |
| | 1 | ↗ | + | + | | |
| | | | | × | | |
| | | | × | + | | |
| | | | | × | ✓ | 1 |

Tableau 4 Table de vérité du protocole BB84 (EPR).

### 2.1.4 Sécurité du protocole BB84 en l'absence de bruit

L'idéal pour Eve serait de dupliquer les photons transmis par Alice pour effectuer une mesure dans chaque base. Eve connaîtrait avec certitude le bit transmis par Alice. Cependant le clonage de l'état d'un photon est interdit par la théorie de la mécanique quantique.

Eve n'a donc pas d'autre choix que d'effectuer une mesure sur les photons transmis. Elle se retrouve confronter au même dilemme que Bob, à savoir le choix de la bonne base. En moyenne, Eve choisit la mauvaise base dans un cas sur deux. Lorsqu'il n'y a pas coïncidence de sa base avec celle d'Alice, sa mesure projette le vecteur d'état du photon sur l'un des vecteurs propres de l'autre base.

Les résultats de Bob ne sont alors plus corrélés avec les émissions d'Alice et des erreurs apparaissent dans la clef de chiffrement. Pour détecter l'intervention d'Eve, donc sa présence, Alice et Bob mesurent le taux d'erreur en comparant une partie de leurs bits communs. Ces éléments sont abandonnés et ne servent plus à la constitution de la clef finale.

Pour ne pas être détectée, Eve doit choisir la même base qu'Alice à chaque fois ; événement qui ne se produit que 1 fois sur $2^n$ avec *n* nombre de bits de la clé. Pour 1000 bits échangés, Eve passe inaperçue dans seulement 1 cas sur $2^{1000}$, soit environ $10^{301}$.

En l'absence de bruit, ce protocole est donc inconditionnellement sûr pour peu que le nombre de bits échangés par Alice et Bob soit suffisamment grand.

## 2.2 Sécurité du protocole BB84

### 2.2.1 Notion de théorie de l'information

#### 2.2.1.1 Bit classique/bit quantique

Un bit est un objet mathématique qui permet de décrire l'état d'un système physique classique. A un instant donné, il prend pour valeur 0 ou 1.

Le bit quantique, appelé QBit, décrit l'état d'un système quantique. Il peut prendre les valeurs 0 et 1 comme un bit classique, mais aussi toutes les valeurs intermédiaires, combinaison linéaire des états 0 et 1. La notation de Dirac est utilisée.

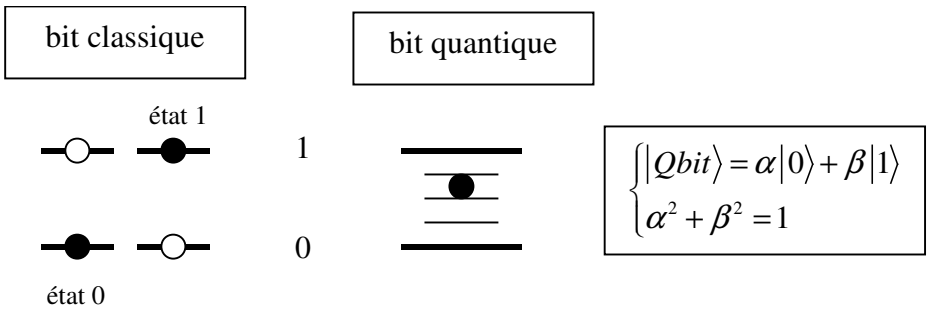



Figure 7 Comparaison d'un bit classique et d'un bit quantique.

Le résultat de la mesure d'un Qbit est une valeur déterministe, comme pour un bit classique.

Un Qbit est un système quantique à deux dimensions. Son espace de Hilbert se compose de deux états propres formant une base. Ils sont orthogonaux et sont notés $|0\rangle$ et $|1\rangle$. Tous les Qbits s'expriment dans cette base.

$$\begin{aligned} &\left|Qbit\right\rangle = \cos\theta.\left|0\right\rangle + e^{j\varphi}.\sin\theta\left|1\right\rangle \\ &\text{avec} \quad \begin{matrix} 0 \le \theta < \pi/2 \\ 0 \le \varphi < 2\pi \end{matrix} \end{aligned} \tag{13}$$

Les angles $\theta$ et $\varphi$ sont deux paramètres indépendants caractérisant un unique point sur une sphère unité de $\mathbb{R}^3$, nommée sphère de Bloch, ayant pour coordonnées cartésiennes

$$\begin{aligned} x &= \sin 2\theta.\cos\varphi \\ y &= \sin 2\theta.\sin\varphi \\ z &= \cos 2\theta \end{aligned} \tag{14}$$

Un Qbit est représenté sur cette sphère par la Figure 8. Dans cette représentation, $|0\rangle$ et $|1\rangle$ ont pour coordonnées respectives (0,0,1) et (0,0,-1).

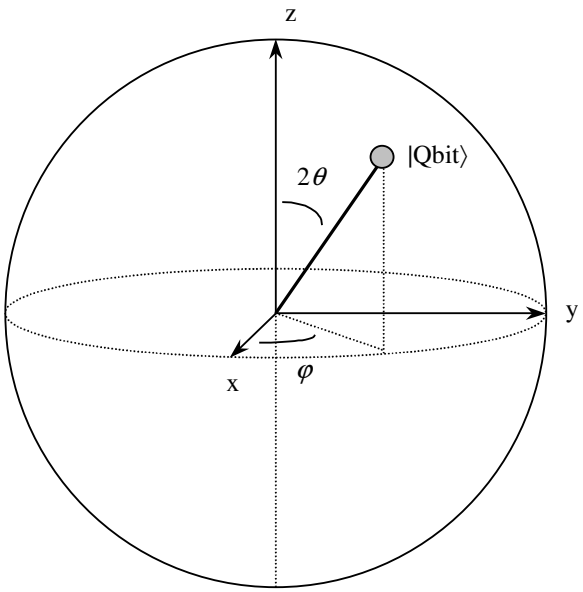



Figure 8 Sphère de Bloch.

### 2.2.1.2 Entropie

En 1948, Shannon a montré que la quantité d'information contenue dans une séquence aléatoire peut être définie par son entropie [18]. L'entropie, notée *H*, d'une variable aléatoire discrète *A* avec *n* états possibles est définie comme

$$H(A) = \sum_{i=1}^{n} p(a_i) \log_2 \left( \frac{1}{p(a_i)} \right) \tag{15}$$

où $\log_2$ désigne le logarithme en base 2, $p(a_i)$ désigne la probabilité que la variable $A$ soit égale à $a_i$.

Plus généralement, lorsque $A$ et $B$ sont deux séquences aléatoires, l'entropie conjointe $H$ s'écrit

$$H(A,B) = \sum_i \sum_j p(a_i, b_j) \log_2 \left( \frac{1}{p(a_i, b_j)} \right) \tag{16}$$

Si la variable $A$ est connue, l'entropie conditionnelle de $B$ s'écrit

$$H(B|A) = H(A,B) - H(A) \tag{17}$$

L'entropie conditionnelle représente la quantité d'information qu'il manque encore pour spécifier complètement $B$ sachant $A$.

L'information mutuelle contenue dans $A$ et $B$ reflète les informations communes de $A$ et $B$. Si les séquences $A$ et $B$ représentent, respectivement, le signal émis par Alice et la mesure de Bob, alors l'information mutuelle définit ce que Bob apprend de $A$ en observant $B$.

Elle est notée $I(A,B)$ et s'exprime

$$I(A,B) = H(A) + H(B) - H(A,B) \tag{18}$$

Des équations (17) et (18), l'information mutuelle contenue dans $A$ et $B$ s'écrit également

$$I(A,B) = H(A) - H(A|B) \tag{19}$$

De la définition de l'entropie exprimée par les équations (15) et (16), $I(A,B)$ s'écrit

$$I(A,B) = \sum_{i=A} \sum_{j=B} p(a_i, b_j) \log_2 \left( \frac{p(a_i, b_j)}{p(a_i)\, p(b_j)} \right) \tag{20}$$

La probabilité $p(a_i,b_j)$ peut s'écrire

$$p(a_i, b_j) = p(a_i)\, p(b_j / a_i) \tag{21}$$

La Figure 9 présente le diagramme de Venn, illustrant les liens entre entropie et information mutuelle.

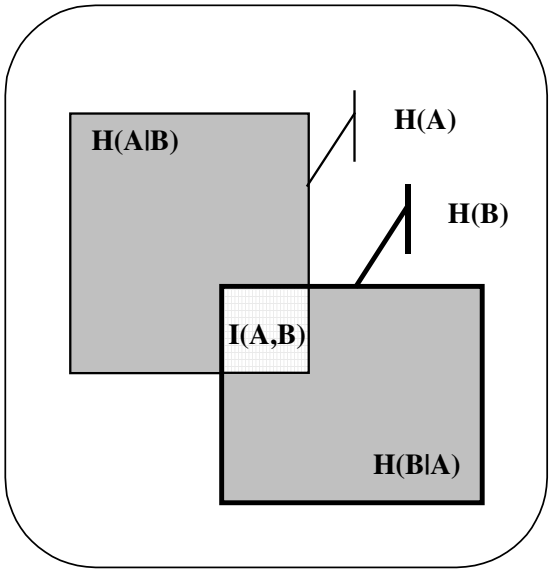



Figure 9 Diagramme de Venn

### 2.2.2 Etapes classiques et clef secrète

Une distribution quantique de clef se compose toujours d'un « protocole quantique » suivi d'étapes classiques réalisées sur un canal public authentifié, c'est-à-dire qu'Alice et Bob sont les seuls expéditeurs et destinataires. Eve ne peut jouer qu'un rôle passif en écoutant les échanges entre Alice et Bob.

La première étape de la distribution quantique de clef consiste à suivre le protocole BB84 (transmission quantique et réconciliation) afin qu'Alice et Bob partagent une série de données fortement corrélées constituant une clef raffinée (Figure 10).

Si le système de distribution est parfait technologiquement (composants sans perte…), les clefs d'Alice et Bob sont identiques en l'absence de toute intervention d'Eve. Cependant les imperfections des appareils expérimentaux introduisent des erreurs entre les deux clefs, le taux d'erreurs est alors noté *QBER* (*Quantum Bit Error Rate*). Ce taux moyen est la limite asymptotique du nombre d'erreurs rapporté au nombre de bits transmis durant une transmission :

$$QBER = \frac{N_{\text{erreur}}}{N_{\text{erreur}} + N_{\text{sans erreur}}} \tag{22}$$

où $N_{sans\ erreur}$ représente le nombre total de bits reçus conformément à ce qui a été émis par Alice et $N_{erreur}$ le nombre de bits reçus erronés.

Par comparaison d'un petit nombre de bits de leur clef raffinée, Alice et Bob évaluent un QBER, puis effectuent une correction d'erreur. A la fin de cette seconde étape, Alice et Bob connaissent exactement le taux d'erreur.

Ces erreurs sont toutes attribuées à l'écoute d'Eve qui gagne de l'information en perturbant la transmission. Si le taux d'erreur est trop élevé, Alice et Bob décident de rejeter la totalité de leur clef brute. Dans le cas contraire, il leur est nécessaire d'augmenter la confidentialité en réduisant la quantité d'information connue d'Eve. En contrepartie, Alice et

Bob sacrifient un nombre de bits, plus ou moins important en fonction du degré de sécurité recherché. A la fin de cette troisième étape, Alice et Bob partagent une clef finale secrète.

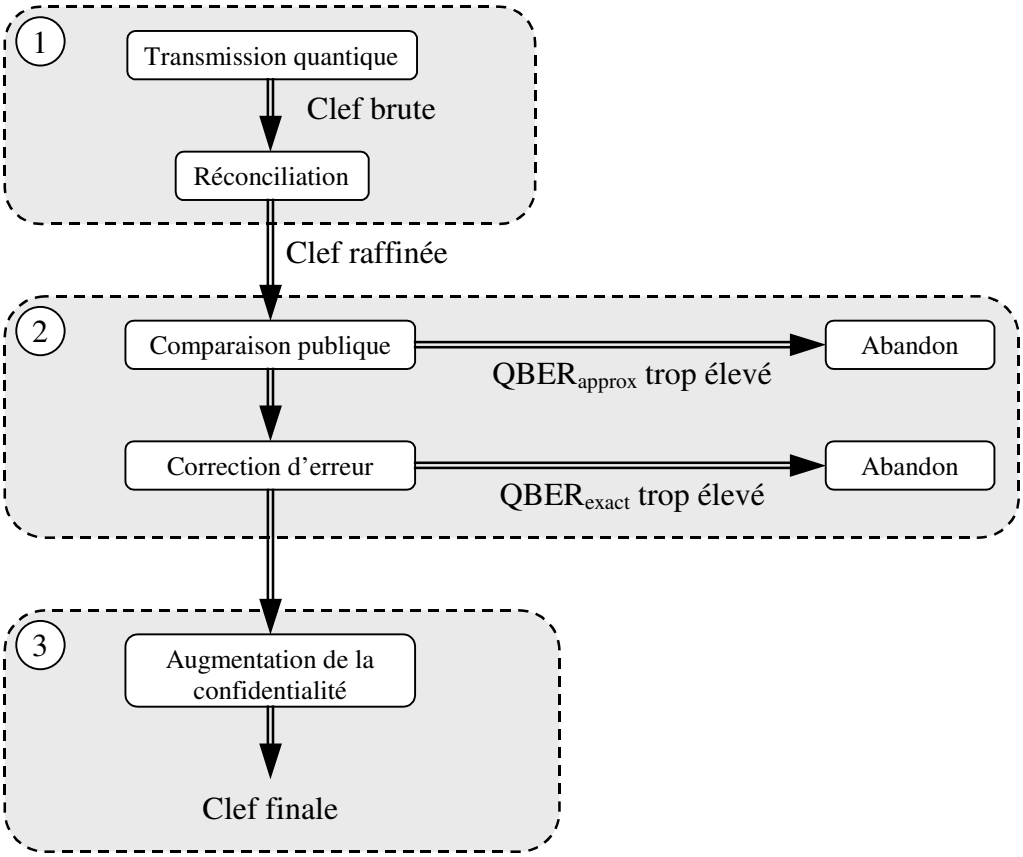



Figure 10 Synoptique d'une distribution quantique de clef.

### 2.2.3 Comparaison publique, correction d'erreur et augmentation de la confidentialité

Chaque évaluation du taux d'erreur s'accompagne d'un choix de poursuivre ou non la distribution quantique de clef. Lors de la comparaison publique, Alice et Bob sacrifient une partie de leurs bits pour obtenir une approximation du taux d'erreur. Le nombre de bits comparés doit être suffisamment important pour que le taux d'erreur soit représentatif de l'ensemble de la transmission afin d'effectuer une correction d'erreur adaptée.

De plus, le choix des bits comparés doit être aléatoire et, effectué a posteriori, par rapport à la transmission quantique.

Il existe de nombreux codes correcteurs d'erreur permettant l'obtention d'une clef identique entre Alice et Bob. Certains sont relativement simples à mettre en place, mais peu efficaces. Tous permettent de mesurer la valeur exacte du taux d'erreur initial de la clef sans avoir à la divulguer entièrement. Cependant cette clef ne peut être utilisée en l'état puisque Eve en connaît une part. Il convient alors à Alice et Bob d'évaluer la quantité d'information détenue par Eve et de la réduire en dessous d'un seuil déterminé représentatif de la sécurité recherchée. En effet Alice et Bob peuvent établir une clef secrète [19] si

$$I_{Alice \to Bob} \geq I_{Alice \to Eve} \text{ ou } I_{Alice \to Bob} \geq I_{Bob \to Eve} \quad (23)$$

où $I_{Alice \to Bob}$ représente l'information mutuelle au sens de Shannon entre Alice et Bob. Alice et Bob sont en mesure d'établir une clef secrète lorsque soit Alice soit Bob a plus d'information sur l'autre qu'Eve.

## 2.3 Stratégies d'écoute d'Eve

En l'absence de bruit, toute mesure d'Eve perturbe la transmission en introduisant des changements entre les bits émis par Alice et ceux mesurés par Bob. Ces discordances mesurables directement imputables à Eve trahissent sa présence.

Lorsque le canal est bruité, Alice et Bob ne sont pas en mesure de différencier les erreurs dues au bruit du canal des erreurs issues de l'intervention d'Eve. Il est donc envisageable qu'Eve masque sa présence en mimant les caractéristiques de bruit du canal, surtout si celui-ci est très bruité.

Eve peut choisir une stratégie d'écoute parmi deux grandes classes d'attaque :

- les attaques incohérentes,
- les attaques cohérentes.

La stratégie d'écoute choisie par Eve doit lui permettre de gagner un maximum d'information sur la transmission sans pour autant augmenter le bruit "naturel" du canal, tout en respectant les règles de la mécanique quantique. Eve, supposée omnipotente, a à sa disposition du matériel parfait technologiquement (ligne de transmission sans perte, photodétecteur sans bruit et avec une efficacité quantique de 1, …).

Lors d'une attaque cohérente, Eve utilise une sonde pour enregistrer dans une mémoire quantique chaque Qbit. En accord avec le théorème de non-clonage, les enregistrements ne sont pas des copies parfaites des Qbit. Le fait d'utiliser des mémoires quantiques permet à Eve d'attendre l'étape de réconciliation des bases entre Alice et Bob. Ce type d'attaques est donc très efficace par rapport aux attaques incohérentes, mais nécessite des composants n'existant qu'au plan théorique [20][21][22].

Les attaques incohérentes consistent en l'intervention d'Eve sur chaque photon, les uns après les autres de façon séquentielle. Ce type d'attaques peut être étudié classiquement en évaluant l'information mutuelle retirée par Eve, d'une part, et celle possédée par Bob [23].

### 2.3.1 Interception-Emission

La stratégie *Interception-Emission* est sans doute la plus intuitive. Eve, placée entre Alice et Bob, intercepte avec une probabilité $\omega$ le photon émis par Alice, mesure son état et renvoie ensuite en direction de Bob un photon préparé dans l'état dépendant du résultat de sa mesure. A la place des photons non interceptés (probabilité complémentaire $1-\omega$), Eve choisit aléatoirement le symbole constituant sa clef. L'intervention d'Eve est alors répétée pour chaque photon (Figure 11).

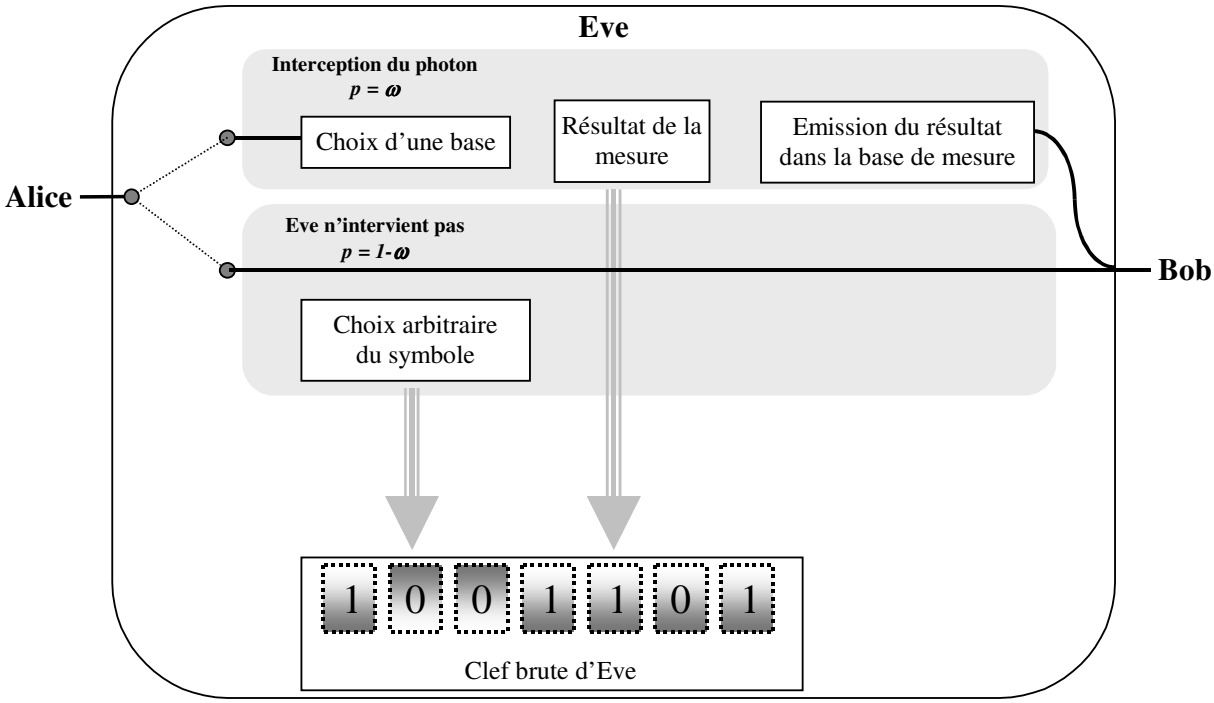



Figure 11 Synoptique de l'attaque *Interception-Emission*.

En posant *a*, *b*, *e* les états respectivement d'Alice, de Bob et d'Eve, l'information mutuelle entre Alice et Bob s'exprime

$$I_{Alice\to Bob}(A,B)=\sum_a\sum_b p(a,b)\log_2\left(\frac{p(a,b)}{p(a)\,p(b)}\right) \tag{24}$$

et l'information mutuelle entre Alice et Eve s'écrit

$$I_{Alice\to Eve}(A,E)=\sum_a\sum_e p(a,e)\log_2\left(\frac{p(a,e)}{p(a)\,p(e)}\right) \tag{25}$$

Pour évaluer ces informations mutuelles, il est nécessaire de calculer les probabilités de détection d'un symbole connaissant le symbole émis.

Si Eve commet une erreur, par exemple le symbole *0* est mesuré par Eve alors qu'Alice a émis le symbole *1*, deux cas se présentent ; soit Eve a mesuré le photon, soit elle ne l'a pas fait et a choisi aléatoirement le symbole constituant sa clef.

Si elle l'a mesuré, elle a une probabilité $\omega$ de choisir d'intercepter le photon, une probabilité ½ de choisir la bonne base. Si elle a choisi la bonne base, elle a une probabilité nulle de détecter le symbole *0*. Si au contraire elle a choisi la mauvaise base, elle a une probabilité ½ d'obtenir un 0. La probabilité d'Eve de détecter le symbole 0 alors qu'Alice a émis un 1 est

$$p_{intercepté}(1/0) = \omega\frac{1}{2}\left(0+\frac{1}{2}\right) \tag{26}$$

Si Eve n'intercepte pas le photon,

$$p_{non\text{-}intercepté}(1/0) = (1-\omega)\frac{1}{2} \tag{27}$$

De la même façon,

$$\begin{aligned} p_{intercepté}(0/0) &= \omega\frac{1}{2}\left(1+\frac{1}{2}\right) \\ p_{non\text{-}intercepté}(0/0) &= (1-\omega)\frac{1}{2} \end{aligned} \tag{28}$$

Par symétrie entre les symboles, les probabilités conditionnelles entre Alice et Eve s'écrivent

$$\begin{aligned} p(1/0) &= p(0/1) = \frac{1}{2} - \frac{\omega}{4} \\ p(1/1) &= p(0/0) = \frac{1}{2} + \frac{\omega}{4} \end{aligned} \tag{29}$$

Des équations (21),(25) et (29),

$$I_{Alice\to Eve} = \frac{1}{2}\log_2\left(1-\frac{\omega^2}{4}\right) + \frac{\omega}{4}\log_2\left(\frac{2+\omega}{2-\omega}\right) \tag{30}$$

Suivant le même raisonnement entre Alice et Bob,

$$I_{Alice\to Bob} = \log_2\left(2-\frac{\omega}{2}\right) - \frac{\omega}{4}\log_2\left(\frac{4}{\omega}-1\right) \tag{31}$$

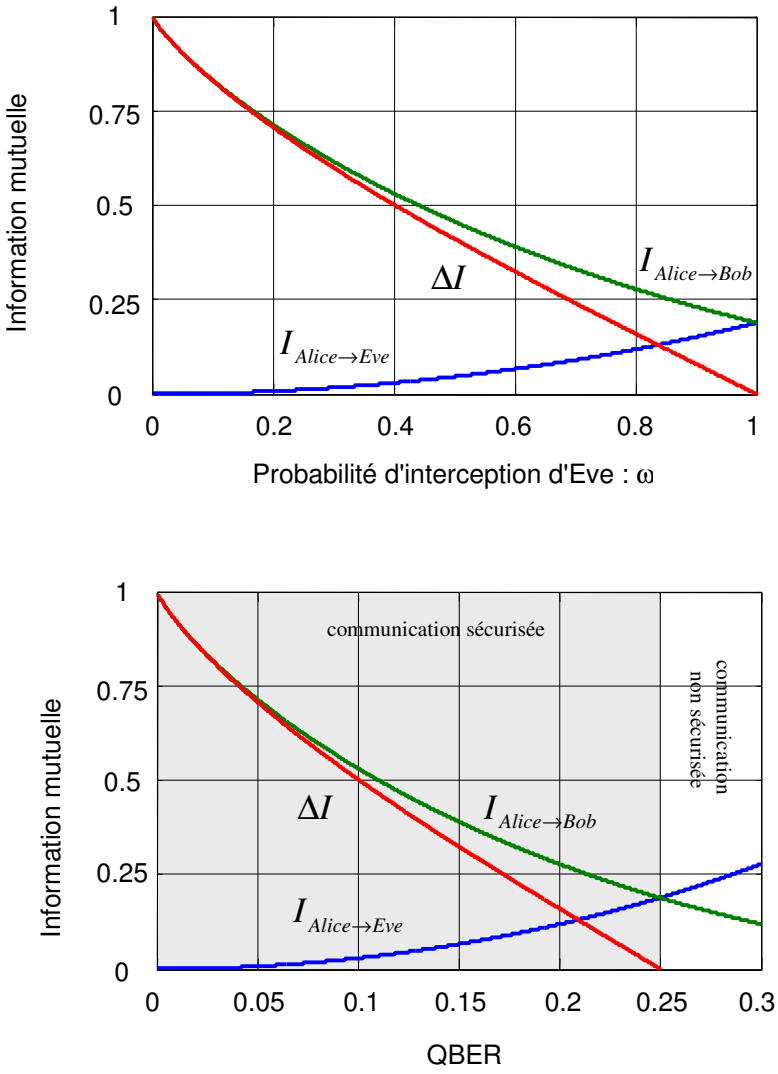



Figure 12 Information mutuelle entre Alice, Bob et Eve lors d'une attaque *Interception-Emission*.

La Figure 12 montre que si Eve n'intercepte pas tous les photons ($\omega<1$), alors l'information mutuelle entre Alice et Bob est supérieure à celle entre Alice et Eve. Par conséquent, Alice et Bob sont en mesure d'élaborer une clef. Si Eve intercepte tous les photons ($\omega = 1$), Eve a autant de connaissance que Bob sur la clef brute. Alice et Bob sont obligés d'abandonner leur clef.

Le taux d'erreur représente les perturbations dues à l'intervention d'Eve.

$$QBER = \left[ p(1,0)_{|\omega} - p(1,0)_{|\omega=0} \right] + \left[ p(0,1)_{|\omega} - p(0,1)_{|\omega=0} \right] = \frac{\omega}{4} \quad (32)$$

La stratégie d'écoute Interception-émission n'est efficace que si Eve mesure tous les photons émis par Alice. Dans ce cas, les mesures d'Eve sont correctes dans un cas sur deux en moyenne. Son gain d'information moyen est alors de 0,5. Eve génère un taux d'erreurs de 25%. Sa présence est donc facilement repérable par Alice et Bob.

### 2.3.2 Mesure dans la base de Breidbart

Au lieu d'utiliser les mêmes bases que celles de Bob, Eve peut utiliser une base unique pour récupérer de l'information sur la clef. Cette base intermédiaire a subi une rotation d'un angle $\theta$ par rapport à l'une des bases précédentes (Figure 13). Lorsque $\theta=\pi/8$, cette base est appelée *base de Breidbart* [22].

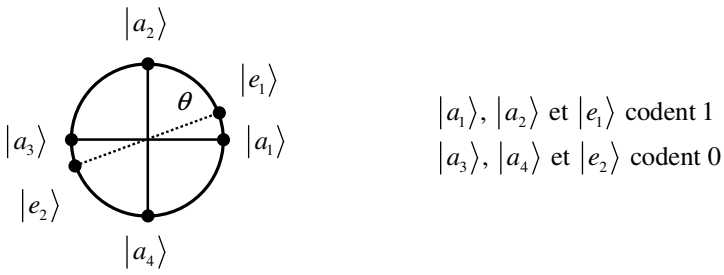



Figure 13 Mesure dans la base de Breidbart.

Il est possible de quantifier l'information mutuelle gagnée par Eve en calculant l'information mutuelle entre les signaux envoyés par Alice $A = \{0,1\}$ et les signaux détectés par Eve $E = \{|e_1\rangle, |e_2\rangle\}$.

$$\begin{aligned} I_{Alice \to Eve} &= I(A,E) \\ &= H(E) - H(E/A) \end{aligned} \tag{33}$$

Le choix des symboles émis par Alice étant aléatoire et équiprobable, l'entropie de $X$ est maximale.

$$H(X) = 1 \tag{34}$$

Pour évaluer l'entropie conditionnelle $H(E/A)$ en fonction de $\theta$, il est nécessaire de calculer la probabilité de détection d'un symbole connaissant le symbole émis.

Pour le symbole 0, Alice choisit d'envoyer l'état $|a_3\rangle, |a_4\rangle$.

$$\begin{aligned} p(|e_2\rangle/0) &= p(|a_3\rangle)\, p(|e_2\rangle/|a_3\rangle) + p(|a_4\rangle)\, p(|e_2\rangle/|a_4\rangle) \\ &= \frac{1}{2}\cos^2(\theta) + \frac{1}{2}\cos^2\left(\frac{\pi}{4} - \theta\right) \end{aligned} \tag{35}$$

De la même manière,

$$\begin{aligned}
p(|e_1\rangle/0) &= p(|a_3\rangle)\,p(|e_1\rangle/|a_3\rangle) + p(|a_4\rangle)\,p(|e_1\rangle/|a_4\rangle) \\
&= \frac{1}{2}\sin^2(\theta) + \frac{1}{2}\sin^2\left(\frac{\pi}{4}-\theta\right) \\
p(|e_1\rangle/1) &= p(|a_1\rangle)\,p(|e_1\rangle/|a_1\rangle) + p(|a_2\rangle)\,p(|e_1\rangle/|a_2\rangle) \\
&= \frac{1}{2}\sin^2(\theta) + \frac{1}{2}\sin^2\left(\frac{\pi}{4}-\theta\right) \\
p(|e_2\rangle/1) &= p(|a_1\rangle)\,p(|e_2\rangle/|a_1\rangle) + p(|a_2\rangle)\,p(|e_2\rangle/|a_2\rangle) \\
&= \frac{1}{2}\cos^2(\theta) + \frac{1}{2}\cos^2\left(\frac{\pi}{4}-\theta\right)
\end{aligned} \tag{36}$$

Ainsi, des équations (16) et (36),

$$\begin{aligned}
H(E/A) = &-p(0)\left[p(|e_1\rangle/0)\log_2\left(p(|e_1\rangle/0)\right) + p(|e_2\rangle/0)\log_2\left(p(|e_2\rangle/0)\right)\right] \\
&-p(1)\left[p(|e_1\rangle/1)\log_2\left(p(|e_1\rangle/1)\right) + p(|e_2\rangle/1)\log_2\left(p(|e_2\rangle/1)\right)\right]
\end{aligned} \tag{37}$$

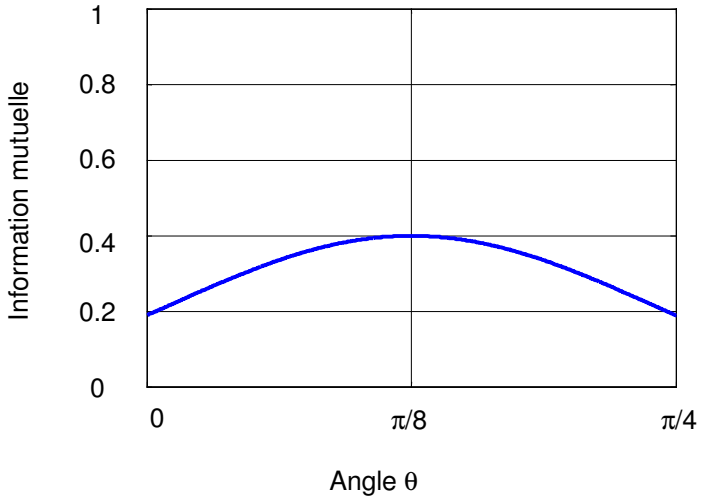



Figure 14 Information mutuelle d'Eve lors d'une écoute dans la base de Breitdbart.

L'information mutuelle entre Alice et Eve est maximale pour $\theta = \pi/8$ correspondant à l'angle définissant la base de Breidbart [22] et vaut ≈ 0,399. Cette stratégie d'écoute permet de connaître la valeur d'un bit avec une probabilité de 85%.

### 2.3.3 La cloneuse quantique

Le principe de cette attaque consiste à ce qu'Eve réalise une copie de chaque photon envoyé par Alice et effectue une mesure après l'étape de réconciliation des bases entre Alice et Bob. Elle connaît alors leur base commune.

Le théorème de non-clonage interdit à Eve d'obtenir des parfaites copies des états émis par Alice. Eve introduit des erreurs qu'Alice et Bob peuvent détecter. L'information mutuelle entre Alice et Bob [25] s'exprime

$$I_{Alice\to Bob} = (1-QBER)\log_2(2-2.QBER) + QBER.\log_2(2.QBER) \tag{38}$$

L'information mutuelle entre Alice et Eve est

$$I_{Alice\to Eve} = \frac{1}{2}.\left[\begin{array}{l}\left(1+\sqrt{1-(1-2.QBER)^2}\right).\log_2\left(1+\sqrt{1-(1-2.QBER)^2}\right)\\ +\left(1-\sqrt{1-(1-2.QBER)^2}\right).\log_2\left(1-\sqrt{1-(1-2.QBER)^2}\right)\end{array}\right] \tag{39}$$

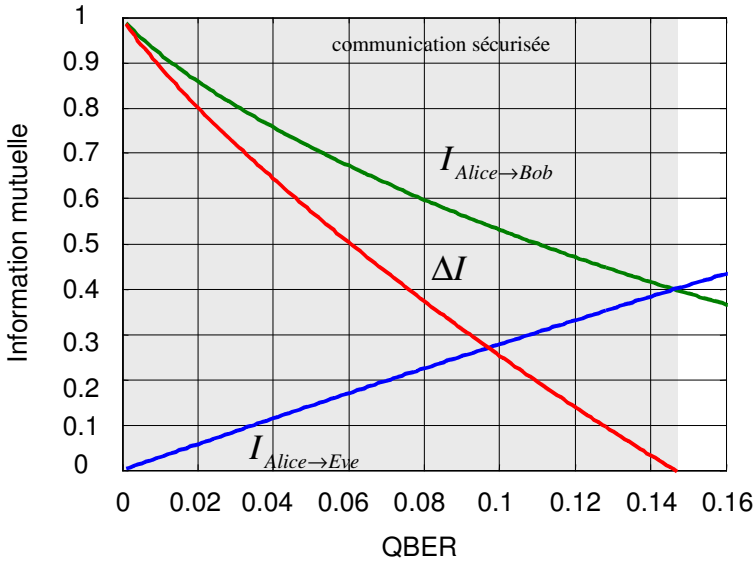



Figure 15 Informations mutuelles lors d'une écoute de type « attaque des clones ».

D'après la Figure 15, Alice et Bob ne peuvent constituer une clef que si leur système présente un QBER inférieur à 15%.

### 2.3.4 Attaque cohérente

Il existe plusieurs types d'attaques cohérentes reposant sur l'utilisation de composants n'existant aujourd'hui qu'au plan théorique.

Pour les attaques cohérentes, Eve utilise une sonde de grande dimension qu'elle intrique à chaque photon envoyé par Alice. Cette sonde est ensuite conservée dans une mémoire quantique jusqu'à l'étape de réconciliation des bases d'Alice et de Bob. Eve est alors en mesure d'effectuer sa mesure. La classe la plus générale de mesure est celle des mesures à opérateurs à valeur positive (*POVM* : *positive operator valued measurement*) [26].

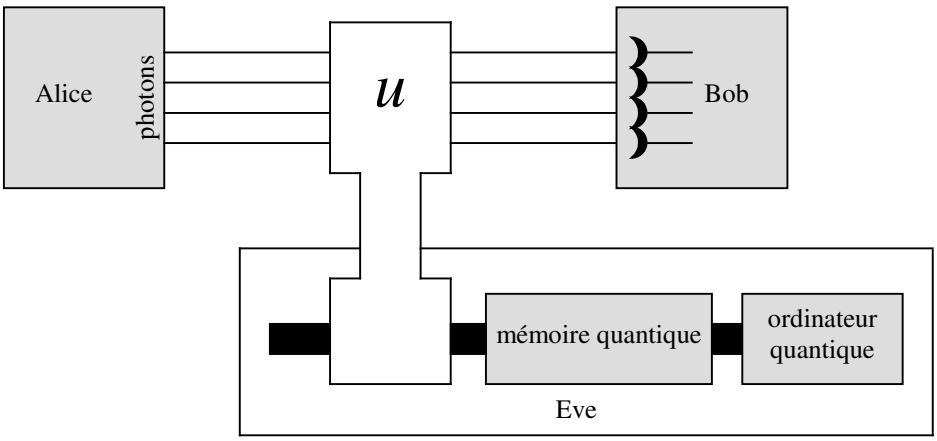



Figure 16 Synoptique d'une attaque cohérente.

Lorsque Alice envoie un nombre *n* de Qbits, Eve récupère une information mutuelle $I_{Alice \to Eve}$ , et Bob gagne une information $I_{Alice \to Bob}$.

$$I_{Alice \to Eve} + I_{Alice \to Bob} \leq 1 \tag{40}$$

La condition pour qu'une clef secrète puisse être extraite est alors

$$I_{Alice \to Bob} \geq \frac{1}{2} \tag{41}$$

L'information mutuelle entre Alice et Bob est fonction du taux d'erreur quantique [20][21].

$$QBER.\log_2(QBER) + (1 - QBER).\log_2(1 - QBER) \leq \frac{1}{2} \tag{42}$$

$$QBER \leq 11\% \tag{43}$$

En considérant que Eve possède une sonde l'autorisant à effectuer cette stratégie, Alice et Bob sont obligés d'élaborer un dispositif de distribution quantique de clef présentant un taux d'erreur quantique inférieur à 11% [27].

### 2.3.5 Conclusion

L'attaque de la machine cloneuse est la stratégie d'écoute la plus discrète parmi les attaques incohérentes. Le taux d'erreur maximal que peuvent accepter Alice et Bob est voisin de 15%. Ainsi le protocole BB84 est sécurisé contre toute attaque individuelle si $QBER < 15\%$. Il est alors possible de distiller une clef après correction des erreurs suivie d'une amplification de confidentialité.

Dans le cas d'une sécurité inconditionnelle, il est nécessaire d'envisager d'autres types d'attaque de la part des espions. Les attaques cohérentes fixent alors un nouveau critère : $QBER < 11\%$.

Cependant ce *QBER* maximal correspond à une limite fondamentale pour des protocoles de correction d'erreur et d'amplification de confidentialité unidirectionnels. Il existe des protocoles plus performants, utilisant une communication bidirectionnelle, permettant de repousser cette limite à 30% [28].

# Chapitre 3.
# Sous-ensembles d'un système de distribution quantique de clef

Un système de distribution quantique de clef se décompose en trois sous-ensembles :
- une source laser générant des impulsions optiques contenant au plus 1 photon,
- une chaîne de modulation permettant de traduire les choix d'Alice et de Bob en déphasage d'une onde optique (dans le cas d'un codage sur la phase),
- un système de détection autorisant une mesure de la phase de chaque photon.

Ce troisième chapitre propose diverses solutions pour ces trois sous-ensembles

# 3.1 Source à photon unique

Le protocole BB84 nécessite l'utilisation d'impulsion optique contenant au plus 1 photon. Ce type de signal optique est difficile à obtenir expérimentalement, puisque les sources à photon unique (encore appelé pistolet à photon) font encore l'objet d'étude [29].

La plupart des systèmes de distribution quantique de clef basés sur l'utilisation du protocole BB84 utilise des sources laser fortement atténuées régies par une distribution poissonienne [30].

Nous présenterons deux systèmes expérimentaux permettant la génération d'impulsions optiques fortement atténuées.

## 3.1.1 Statistique des sources laser atténuées

Le processus de génération des photons obéit à une statistique de Poisson. La probabilité de trouver $n$ photons par impulsion sachant que le nombre moyen, souhaité, de photons par impulsion $\mu$ est donné par la loi suivante

$$P(n,\mu) = \frac{\mu^n e^{-\mu}}{n!} \tag{44}$$

Lorsque le nombre moyen recherché de photon par impulsion est 1 (Figure 17), la probabilité d'avoir plus de deux photons par impulsion est élevée (28%). Par conséquent une telle source ne permet pas d'obtenir une sécurité suffisante pour l'implémentation d'un protocole de cryptographie.

En diminuant le nombre moyen de photon émis par impulsion $\mu = 0.1$ (Figure 18), il est possible de diminuer la probabilité d'émettre plus de 2 photons par impulsion. En contre partie, la probabilité de n'émettre aucun photon est très élevée (de l'ordre 90%).

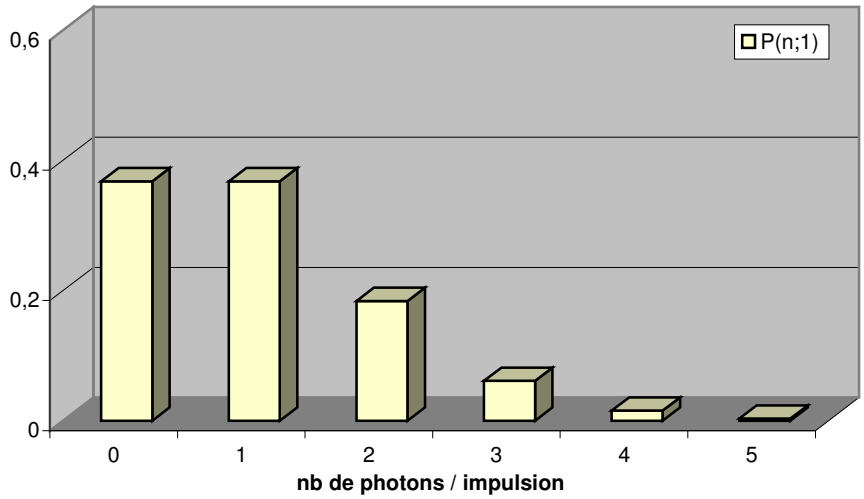



Figure 17 Distribution poissonienne pour un laser fortement atténué $\mu$=1.

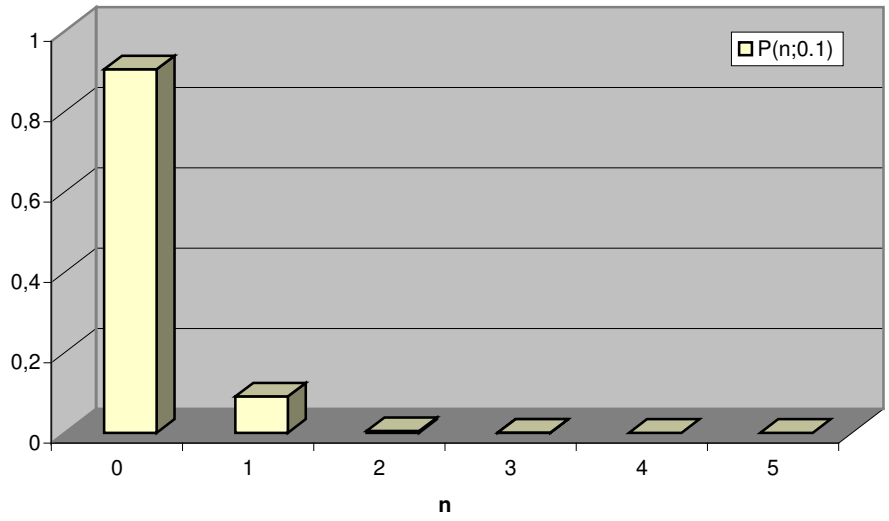



Figure 18 Distribution poissonienne pour un laser fortement atténué $\mu$=0.1.

### 3.1.2 Laser DFB

Le premier module laser utilisé délivre une puissance optique fixe de –22,8 dBm à la longueur d'onde 1553,7 nm (Figure 19). Une entrée radiofréquence permet de moduler

directement l'intensité optique de sortie du laser, ce qui autorise la génération d'impulsions optiques. Cependant, ce laser n'a pas été utilisé en mode impulsionnel.

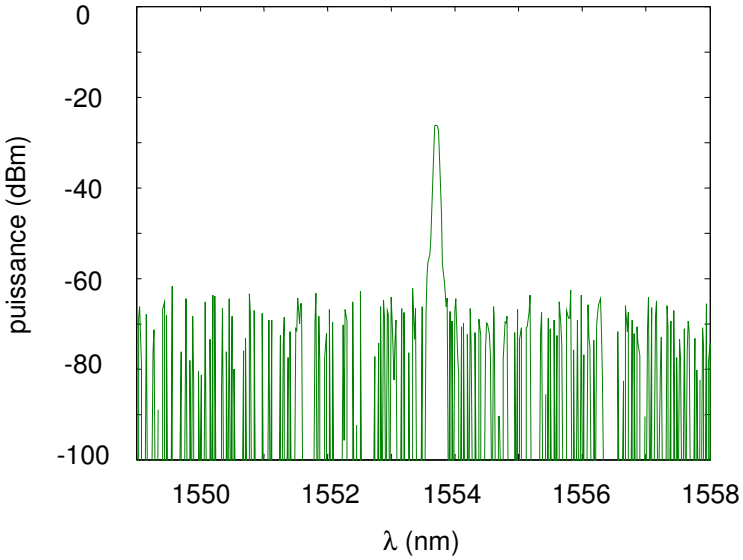



Figure 19 Spectre du laser DFB.

### 3.1.3 Source laser munie d'un modulateur d'intensité intégré

La société *Avanex* a mis, gratieusement, à notre disposition un module laser de type ILM (*Integrated Laser electro-absorption Modulator*) constitué d'un laser DFB (*Distributed FeedBack*) et d'un modulateur électro-absorbant monolitique intégré.

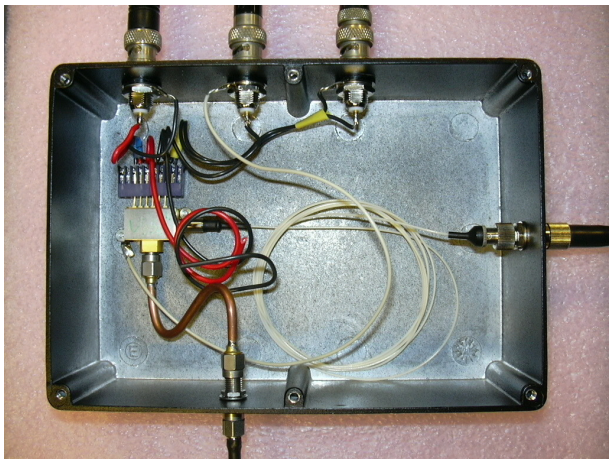


Figure 20 Laser *ILM* fourni par la société *Avanex* dans son boîtier.

Le laser et le modulateur intégré sont encapsulés dans un boîtier métallique sur lequel sont fixées les broches de contrôle du laser, le connecteur SMA de contrôle du modulateur d'intensité et la fibre optique de sortie (Figure 20).

Chaque boîtier est fixé dans une boite métallique servant de dissipateur de chaleur. Les sept broches d'entrée permettent de contrôler la température, le point d'émission du laser et la photodiode placée en face arrière du laser.

Les caractéristiques de cette source sont identiques à celles du produit d'*Avanex* référencé *PowerSource*$^{TM}$ *1915 LMM* [31], excepté pour le taux d'extinction. La puce mise à notre disposition présente un taux d'extinction minimum de 25 dB lorsque la tension du signal de modulation est inférieure à –1,5 V (Figure 23). Sa longueur d'onde d'émission est de 1543,6 nm (Figure 22).

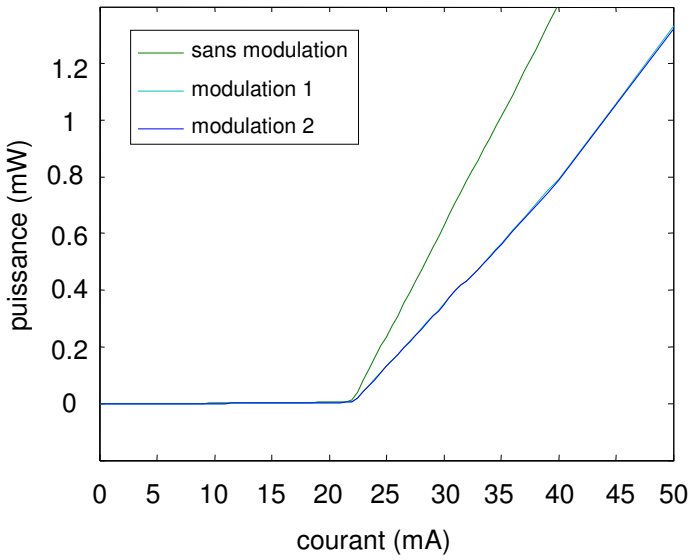



Figure 21 Réponse du laser *ILM*.

Le modulateur d'intensité intégré à l'*ILM* est transparent sans modulation (Figure 21). En fonction de l'amplitude et des niveaux en tensions du signal pilotant ce modulateur, la puissance optique en sortie d'*ILM* varie.

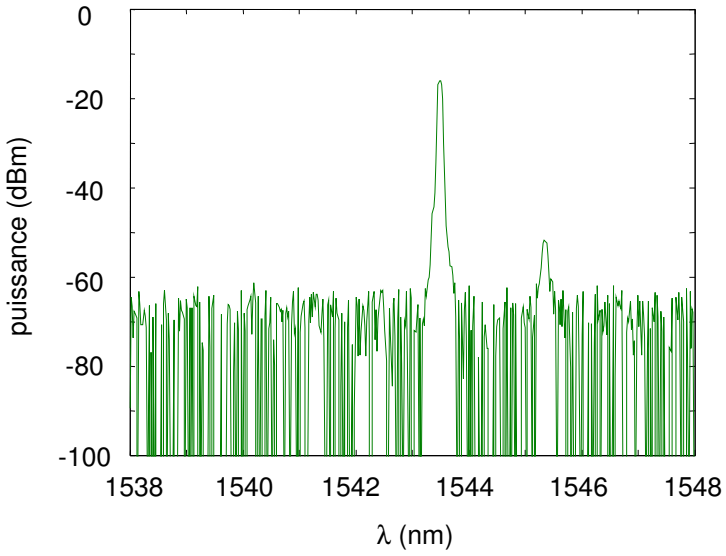



Figure 22 Spectre optique du laser *ILM*.

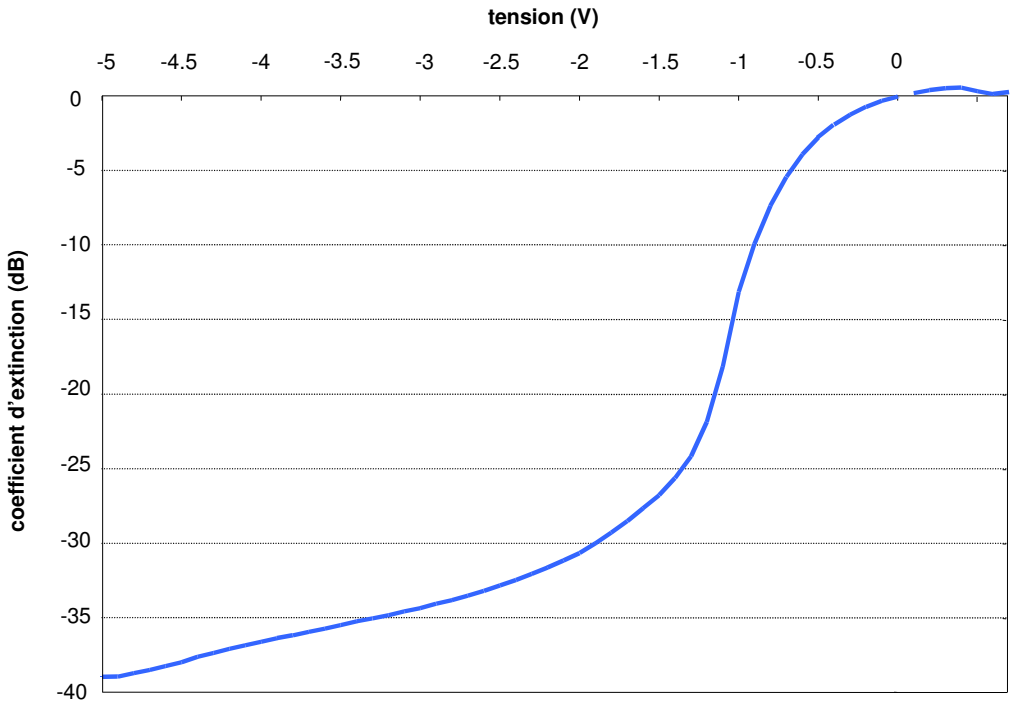



Figure 23 Taux d'extinction du laser *ILM*.

La Figure 21 présente la réponse du laser à 18°C en fonction de différentes modulations de tension du signal de commande (modulation 1 : fréquence de 500 kHz, amplitude de 2 V ; modulation 2 : fréquence de 1 MHz, amplitude de 2 V). Le courant de seuil vaut 22 mA.

Les caractéristiques sont données par le Tableau 5.

| | |
|---|---|
| Longueur d'onde d'émission | 1543,5 nm |
| Courant de seuil | 22 mA |
| Fréquence de coupure | < 8 GHz |
| Taux d'extinction (modèle de série) | > 10 dB |
| Température | 18 °C |

Tableau 5 Caractéristiques du laser *ILM*.

### 3.1.4 Réalisation d'une source de *photon unique* par atténuation d'un laser

Deux systèmes d'émission d'impulsions lumineuses ont été étudiés. Le premier repose sur l'utilisation d'un laser DFB directement modulé en intensité par un signal électrique (Figure 24 a) dont les caractéristiques sont présentées dans la section 3.1.2. La seconde option expérimentée utilise un laser ayant en sortie un modulateur intégré d'intensité, de type ELM (Figure 24 b), dont les caractéristiques principales sont données à la section 3.1.3.

Cependant ces deux solutions ne sont pas équivalentes à une véritable source à photon unique (« pistolet à photon »), puisqu'elles n'autorisent pas la génération à coup sûr d'impulsion contenant exactement 1 photon. Afin d'atteindre des puissances optiques équivalentes à celle d'une impulsion d'énergie de l'ordre de moins de 1 photon en moyenne, il est nécessaire d'ajouter à leur sortie un atténuateur optique variable calibré.

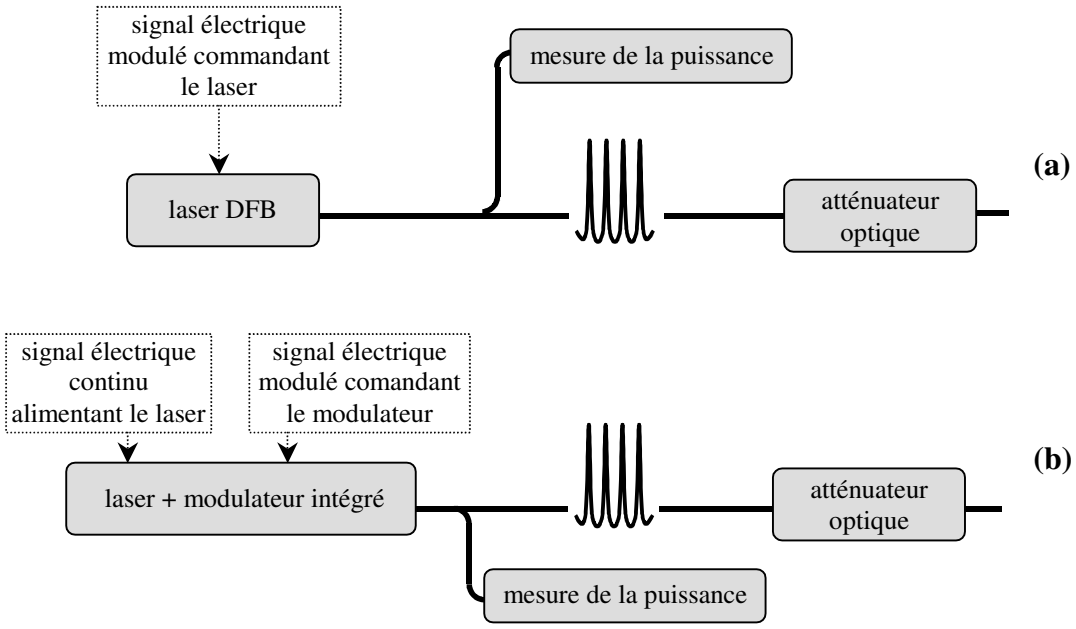



Figure 24 Synoptiques de deux sources laser fortement atténuées.

La puissance optique correspondant à *n* photons par impulsion est

$$P\left(n \text{ photons / pulse}\right) = n.h\frac{c}{\lambda}F_{impulsion} \tag{45}$$

où *h* est la constante de Planck, *c* la vitesse de la lumière dans le vide, $\lambda$ la longueur d'onde et $F_{impulsion}$ la fréquence d'émission des impulsions.

Cette puissance étant très inférieure à –70 dBm ne peut être mesurée directement. Il convient d'évaluer la puissance à la sortie du laser, puis de choisir le coefficient d'atténuation, étalonné à un niveau de puissance mesurable, adapté.

## 3.2 Chaîne de modulation d'Alice et de Bob

Le protocole BB84 nécessite le codage de quatre états de phase distincts pour l'émetteur Alice et le codage de deux états de phase pour le destinataire Bob. Ces états de phases reflètent les choix de bases et de symboles d'Alice et de Bob.

Nous présenterons dans cette section, les modules d'encodage d'Alice et de Bob permettant de traduire leurs choix de bases et symboles en déphasage d'ondes optiques [33][34].

### 3.2.1 Encodage des choix de bases et de symboles d'Alice

La Figure 25 présente le dispositif encodeur d'Alice permettant la génération de signaux QPSK (*Quadrature Phase Shift Keying*) utilisés dans l'implémentation du protocole BB84 par codage de phase. Alice émet ses choix de base et de symbole en modulant la phase d'une onde optique au moyen d'un modulateur Mach-Zehnder à deux électrodes permettant le contrôle indépendant des déphasages optiques introduits sur chaque bras.

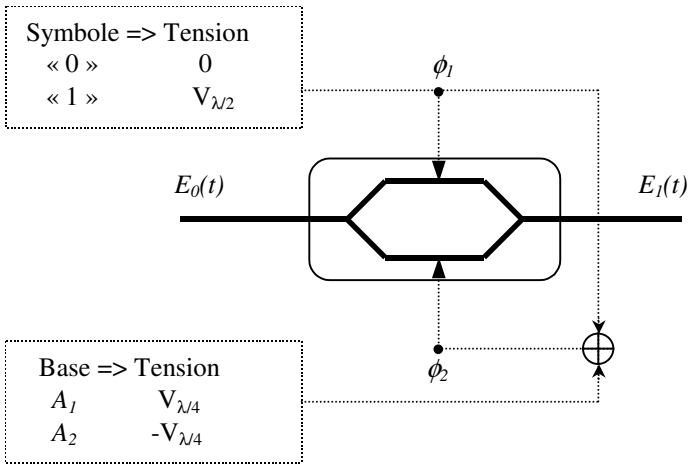



Figure 25 Module d'encodage d'Alice.

L'onde optique incidente, de fréquence angulaire $\omega_0$, est caractérisée par son champ électrique $E_0(t)$.

$$E_0(t) = E_0.\exp(j\omega_0 t) \tag{46}$$

L'onde de sortie après application des déphasages $\phi_1$ et $\phi_2$, est

$$E_1(t) = E_0(t).\underbrace{\cos\left(\frac{\phi_1-\phi_2}{2}\right)}_{\substack{\text{modulation}\\ \text{d'amplitude}}}.\underbrace{\exp\left(j\frac{\phi_1+\phi_2}{2}\right)}_{\text{modulation de phase}} \tag{47}$$

Le champ électrique $E_1(t)$ porte une modulation simultanée en amplitude et en phase. Le terme réel caractérisant une modulation d'amplitude varie en fonction des déphasages $\phi_1$ et $\phi_2$. Or toute modulation d'amplitude appliquée sur un signal fortement atténué portant une distribution aléatoire et équiprobable d'états entraîne une modification des probabilités de chaque état. Il est ainsi possible d'éteindre totalement un état si celui-ci est encodé par $\phi_1$ et $\phi_2$ tels que $\phi_1 = \phi_2$. Sa probabilité d'être détectée par Bob est alors nulle.

Il apparaît alors que chaque état encodé par Alice doit subir la même modulation d'amplitude (ou atténuation) de manière à conserver l'équiprobabilité de chaque état. Cette contrainte est réalisée lorsque

$$\frac{\phi_1-\phi_2}{2} = \text{constante} \tag{48}$$

Les valeurs des déphasages $\phi_1$ et $\phi_2$ ont été fixées dans le respect d'une enveloppe constante telle que $\phi_1 - \phi_2 = \pm\frac{\pi}{2}$.

La modulation de phase $\frac{\phi_1+\phi_2}{2} = \phi_{\text{Alice}}$ permet à elle seule l'encodage des choix de base et de symbole d'Alice.

Le protocole BB84 impose, par définition, l'existence de quatre états distincts correspondant à quatre valeurs distinctes de $\phi_{Alice}$. Le respect de ces contraintes et des choix de valeurs $\phi_1$ et $\phi_2$ permettent d'écrire

$$E_1(t) = \frac{\sqrt{2}}{2}.E_0(t).\exp\left(j\frac{\phi_1+\phi_2}{2}\right) \text{ avec } \frac{\phi_1+\phi_2}{2} \in \left\{-\frac{\pi}{4}, \frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}\right\} \tag{49}$$

correspondant à un signal numérique modulé en phase à quatre états d'équation caractéristique [35]

$$E_1(t) \propto E_0(t).\exp\left(j\frac{2\pi}{M}(m-1)\right) \text{ avec } m \in \{1,2,3,4\} \text{ et } M = 4 \tag{50}$$

Le Tableau 6 établit la correspondance entre les déphasages optiques introduits par Alice ($\phi_1$ et $\phi_2$) et ses choix de bases ($A_1$ ou $A_2$) et de symboles (0 ou 1).

L'implémentation consiste donc à encoder le choix de base par le signe de la tension quart d'onde appliquée à la première électrode (Figure 25). La seconde est commandée par le même signal auquel s'ajoute une tension demi-onde selon le symbole. L'additionneur correspond à un coupleur radiofréquence à fort isolement entre ses deux entrées. Le résultat de cette addition correspond à un signal électrique à trois niveaux.

Le modulateur de phase d'Alice est donc piloté par deux signaux électriques appliqués chacun à une électrode ; le premier correspond à un signal à deux niveaux (noté $\phi_1$), le second à un signal à trois niveaux (noté $\phi_2$).

Les correspondances entre la valeur des déphasages et les niveaux de tension de commande des modulateurs Mach-Zehnder d'Alice figurent sur le Tableau 6. Les niveaux de tensions sont directement fonction des caractéristiques de chaque modulateur.

| Alice | | | | | | |
|---|---|---|---|---|---|---|
| Base | Symbole | $\phi_{Alice}$ | $\phi_1$ | | $\phi_2$ | |
| | | | déphasage | Tension (V) | déphasage | Tension (V) |
| $A_1$ | 0 | 0 | 0 | -1,8 | π/2 | 0 |
| | 1 | π | π | 2 | 3π/2 | 3,6 |
| $A_2$ | 0 | π/2 | 0 | -1,8 | -π/2 | -3,6 |
| | 1 | 3π/2 | π | 2 | π/2 | 0 |

Tableau 6 Correspondance entre les choix d'Alice et les signaux de commandes de son modulateur Mach-Zehnder.

### 3.2.2 Encodage des choix de bases de Bob

Bob encode son propre choix de base au moyen d'un modulateur Mach-Zehnder à doubles électrodes identique à celui d'Alice, en introduisant un unique déphasage $\phi_3$ (Figure 26). En ne tenant pas compte des effets de dispersion et de biréfringence dans le canal de transmission, l'onde optique incidente au modulateur de Bob est identique à celle sortant du module d'encodage d'Alice.

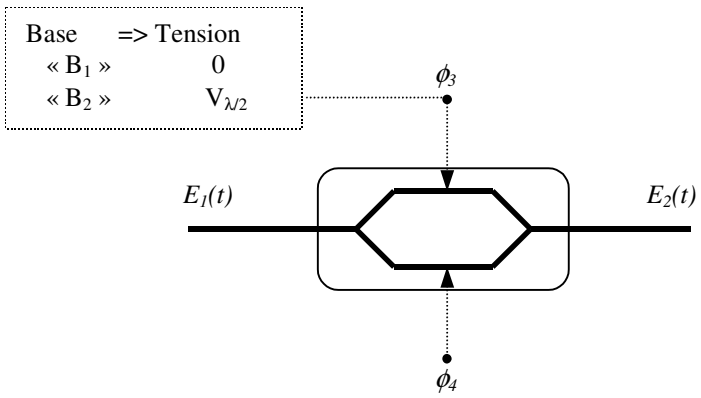



Figure 26 Module d'encodage de Bob.

L'onde optique de sortie du modulateur de Bob s'écrit

$$E_2(t) = E_1(t).\cos\left(\frac{\phi_3}{2}\right).\exp\left(j\frac{\phi_3}{2}\right) \tag{51}$$

La seconde électrode du modulateur de Bob est susceptible d'être utilisée pour l'implantation d'un asservissement en phase par contre-réaction. En posant

$$\frac{\phi_3}{2} = \phi_{Bob} \tag{52}$$

le champ électrique de l'onde de sortie de l'encodeur de Bob est

$$E_2(t) = E_0(t).\frac{\sqrt{2}}{2}.\cos(\phi_{Bob}).\exp\left(j(\phi_{Alice}+\phi_{Bob})\right) \tag{53}$$

Lorsqu'il y a coïncidence des bases, le déphasage $\phi_{Alice}+\phi_{Bob}$ prend une des deux valeurs antipodales que Bob est capable de mesurer. Dans le cas de non-coïncidence, Bob reçoit des valeurs orthogonales aux états propres de son détecteur. La mesure alors réalisée prend une valeur aléatoire correspondante aux états propres du système de détection. La mesure n'étant pas informative est écartée. Le Tableau 7 établit la correspondance entre la base de mesure, le déphasage et le niveau de tension de contrôle du modulateur.

| Bob | | |
|---|---|---|
| Base | $\phi_3$ | $V_{\phi 3}$ (V) |
| $B_1$ | -π/2 | -1,8 |
| $B_2$ | π/2 | 1,8 |

Tableau 7 Correspondance entre les choix de Bob et les signaux de commandes de son modulateur Mach-Zehnder.

### 3.2.3 Encodage des choix d'Alice et de Bob

Les encodages des choix de base et de symbole d'Alice (présentés dans la section 3.2.1), et des choix de base de Bob (présentés dans la section 3.2.2) respectent le protocole BB84 par codage de phase présenté dans la section 2.1.2.

Cependant la réalisation des modules d'encodage d'Alice et de Bob à partir de modulateurs Mach-Zehnder à deux électrodes impose des valeurs de phase différentes de celles présentées dans le Tableau 3.

| Alice | | | | | Bob | | | symbole retenu |
|---|---|---|---|---|---|---|---|---|
| base | symbole | $\phi_1$ | $\phi_2$ | $\phi_{Alice}$ | base | $\phi_3$ | $\phi_{Alice}+\phi_{Bob}$ | |
| $A_1$ | 0 | 0 | $\frac{\pi}{2}$ | $\frac{\pi}{4}$ | $B_1$ | π/2 | π/2 | 0 |
| | | | | | $B_2$ | -π/2 | 0 | ? |
| | 1 | $\pi$ | $\frac{3\pi}{2}$ | $\frac{5\pi}{4}$ | $B_1$ | π/2 | 3π/2 | 1 |
| | | | | | $B_2$ | -π/2 | π | ? |
| $A_2$ | 0 | 0 | $-\frac{\pi}{2}$ | $-\frac{\pi}{4}$ | $B_1$ | π/2 | 0 | ? |
| | | | | | $B_2$ | -π/2 | -π/2 | 0 |
| | 1 | $\pi$ | $\frac{\pi}{2}$ | $\frac{3\pi}{4}$ | $B_1$ | π/2 | π | ? |
| | | | | | $B_2$ | -π/2 | π/2 | 1 |

Tableau 8 Table de vérité du protocole BB84 par codage de phase réalisé avec des modulateurs MZ à deux électrodes.

Ces nouvelles valeurs (Tableau 8) respectent ainsi les contraintes du protocole BB84 par codage sur la phase d'une onde optique réalisé avec deux modulateurs Mach-Zehnder à deux électrodes.

### 3.2.4 Encodeurs expérimentaux d'Alice

Le module d'encodage d'Alice présenté par la Figure 25 nécessite deux signaux électriques de commande, noté $V_{\phi 1}$ et $V_{\phi 2}$.

#### 3.2.4.1 Dispositif à deux générateurs

La génération des deux signaux $V_{\phi 1}$ et $V_{\phi 2}$ est réalisée par un premier dispositif expérimental présenté dans la partie gauche de la Figure 27.

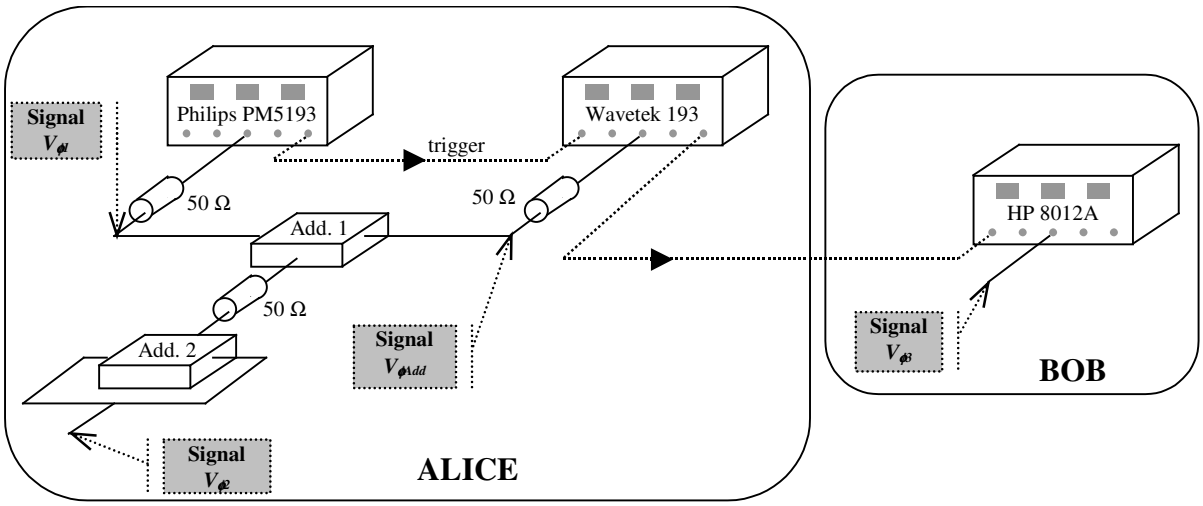



Figure 27 Premier dispositif électrique de commande des modulateurs d'Alice et Bob.

La génération de l'onde optique à trois états de phase nécessite un signal électrique à trois niveaux contrôlant le modulateur de phase d'Alice. Ce signal est le résultat d'une addition de deux signaux électriques à deux niveaux (notés $V_{\phi 1}$ et $V_{\phi Add}$ sur la Figure 27), générés par deux générateurs de signaux électriques synchronisés (*Philips PM5193* et *Wavetek 193*). L'addition s'effectue par l'intermédiaire d'un premier coupleur électrique, noté *Add1*, de type *Mini-Circuit* référencé *ZFSC-2-4*.

Pour une meilleure adaptation d'impédance entre les différents composants, des impédances de 50 Ω sont placées à l'entrée et à la sortie du coupleur électrique. Ces impédances diminuant les niveaux de tension du signal électrique et étant proche de la puissance maximale que délivre les générateurs, un second coupleur électrique, noté *Add2*, de type *Mini-Circuit* référencé *ZFSC-2-1* est utilisé afin d'augmenter les niveaux du signal. Sans ces impédances, les signaux électriques présenteraient des signaux fortement perturbés (Figure 28).

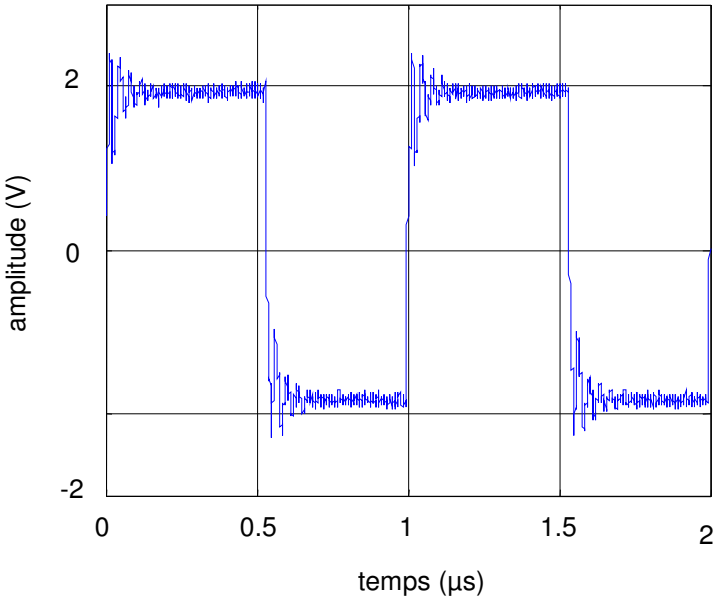



Figure 28 Signal électrique $V_{\phi 1}$ mesuré dans un dispositif sans impédance.

Ce premier dispositif permet de générer les signaux électriques $V_{\phi 1}$ (Figure 29), $V_{\phi add}$ (Figure 30) et $V_{\phi 2}$ (Figure 31).

Les signaux $V_{\phi 1}$ et $V_{\phi 2}$ présentent des transitoires d'ordre élevé entre les différents niveaux. Ces parasites électriques sont causés par une adaptation d'impédance difficile à réaliser entre les coupleurs *Add1*, *Add2*, le générateur électrique et le modulateur Mach-Zehnder sur la Figure 27.

Pour remédier à ce problème, un nouvel encodeur d'Alice, utilisant trois générateurs, est proposé en Figure 32.

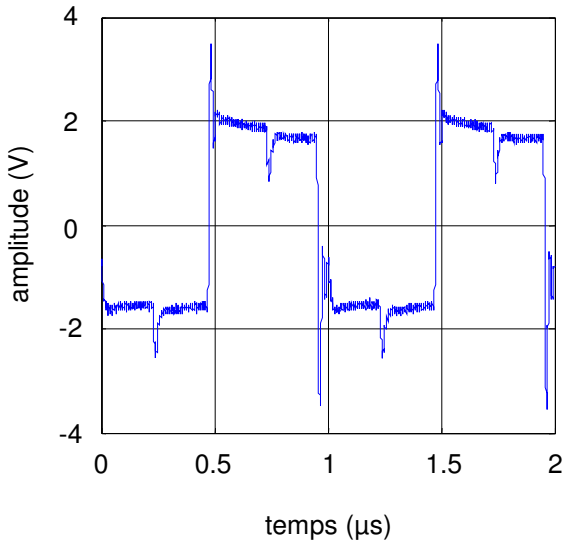



Figure 29 Signal électrique $V_{\phi 1}$ commandant la première électrode du modulateur Mach-Zehnder d'Alice.

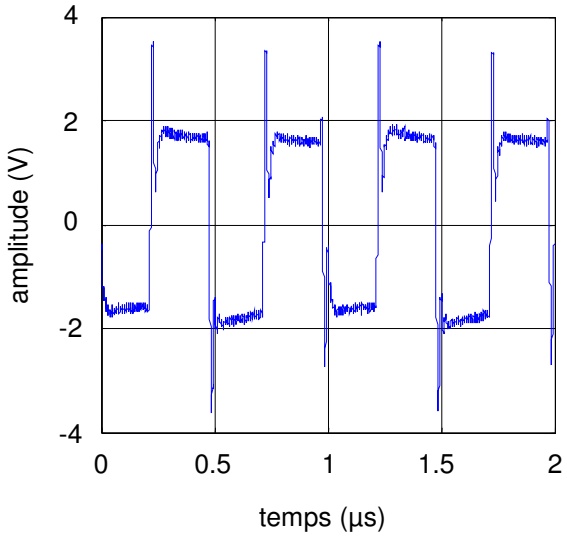



Figure 30 Signal électrique $V_{\phi add}$ servant à générer le signal $\phi_2$.

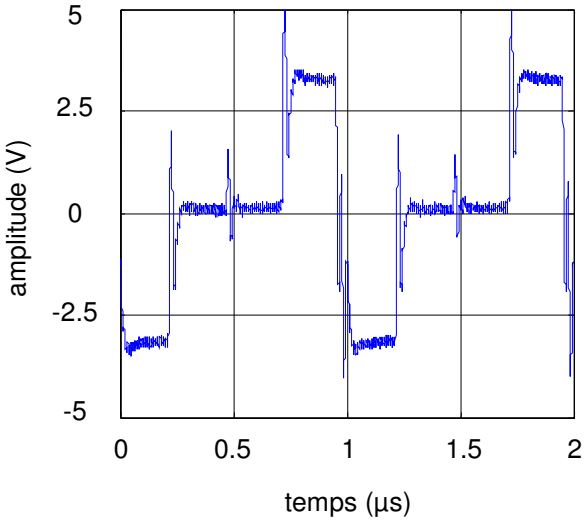



Figure 31 Signal électrique $V_{\phi 2}$ obtenu par addition des signaux $V_{\phi 1}$ et $V_{\phi add}$, commandant la seconde électrode du modulateur Mach-Zehnder d'Alice.

### 3.2.4.2 Dispositif à trois générateurs

La partie gauche de la Figure 32 présente le dispositif expérimental retenu pour générer les signaux de commande du modulateur MZ d'Alice.

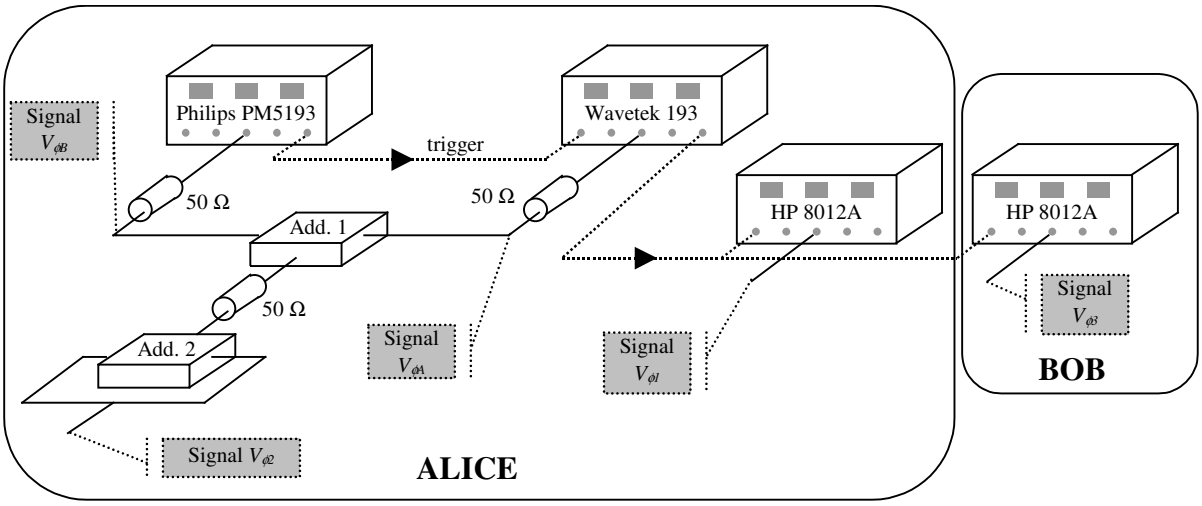



Figure 32 Second dispositif électrique de commande des modulateurs d'Alice et de Bob.

Deux générateurs électriques (*Philips PM5193* et *Wavetek 193*) sont dédiés à la génération du signal $V_{\phi 2}$ construit par addition de deux signaux électriques, notés $V_{\phi A}$ et $V_{\phi B}$

sur la Figure 32. Le signal de commande de la première électrode du modulateur Mach-Zehnder d'Alice est généré par le générateur *HP 8012A* afin de supprimer les transitoires entre les différents niveaux apparaissant dans 3.2.4.1. Les trois générateurs électriques sont synchronisés par un même signal d'horloge.

Les Figure 33 et Figure 34 présentent les mesures des signaux de commandes du modulateur MZ d'Alice.

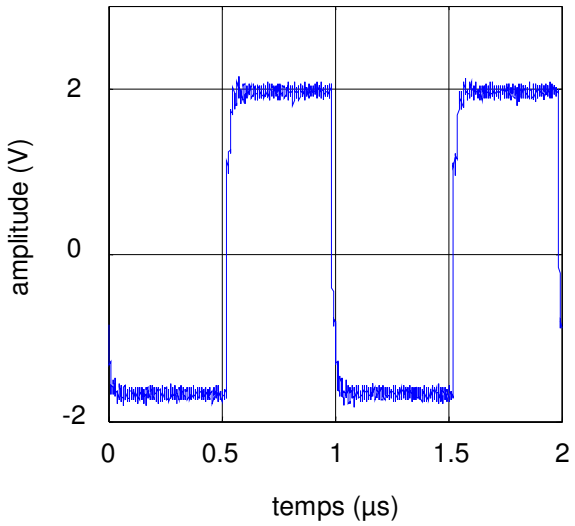



Figure 33 Signal $V_{\phi 1}$ commandant la première électrode du modulateur MZ d'Alice.

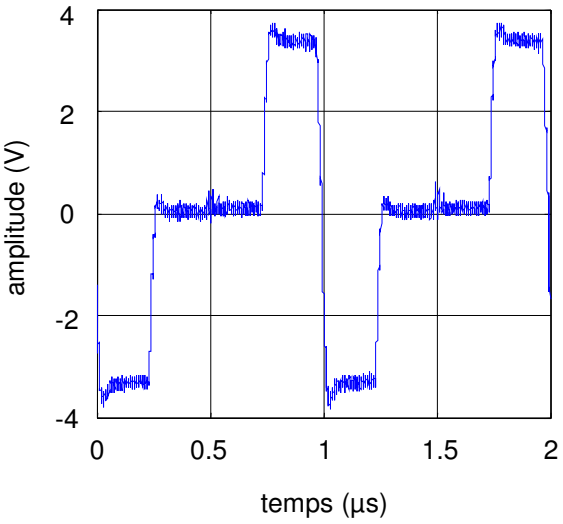



Figure 34 Signal $V_{\phi 2}$ commandant la seconde électrode du modulateur MZ d'Alice.

Les signaux $V_{\phi 1}$ et $V_{\phi 2}$ (Figure 33 et Figure 34) présentent des transitions moins perturbées par les transitoires que celles des signaux générés par le premier dispositif présenté dans la section 3.2.4.1.

### 3.2.5 Encodeur expérimental de Bob

Le signal représentant les choix de Bob n'admet que deux valeurs représentant son choix parmi les deux bases de mesure. Le signal électrique de commande du modulateur MZ de Bob, noté $V_{\phi 3}$, est représenté par la Figure 35.

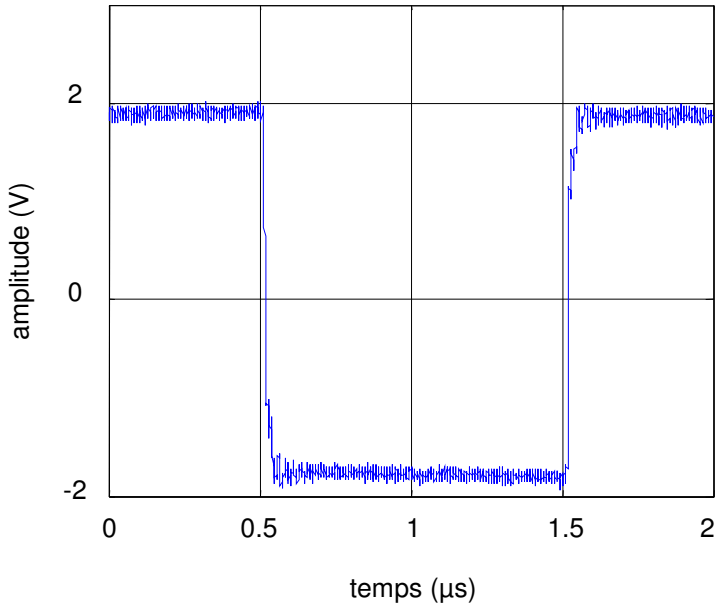



Figure 35 Signal $V_{\phi 3}$ commandant le modulateur MZ de Bob.

## 3.3 Détection cohérente

La détection cohérente présente les avantages par rapport à la détection directe d'avoir une sensibilité de détection plus importante et un accès à la phase optique dans le domaine électrique.

L'amplitude du photocourant généré par le photodétecteur à la fréquence intermédiaire est proportionnelle aux amplitudes de l'onde *signal* optique et de l'onde de l'oscillateur local optique (encore appelée onde *référence*).

La dépendance linéaire du photocourant vis-à-vis des paramètres de l'onde signal (modulation d'amplitude, de fréquence ou de phase optique) est l'élément clef des systèmes optiques cohérents [36].

### 3.3.1 Détection optique équilibrée cohérente

La détection utilisée dans notre dispositif est une détection cohérente équilibrée. Le signal optique est combiné à une onde issue d'un oscillateur local au moyen d'un coupleur 3 dB. Les ondes *signal* et *référence* sortant de ce coupleur possèdent des puissances optiques identiques (d'où le terme *équilibré*).

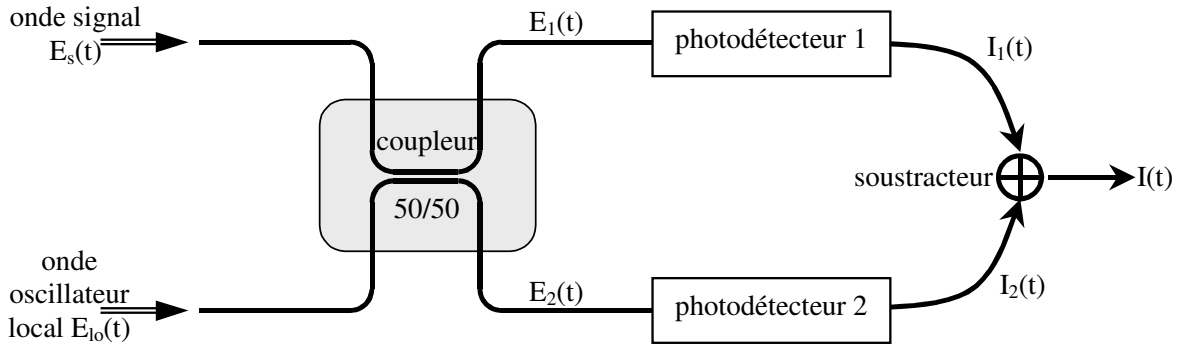



Figure 36 Synoptique d'une détection cohérente équilibrée.

Chaque onde optique en sortie, caractérisée par son champ électrique $E_1(t)$ et $E_2(t)$, est détectée par une photodiode qui génère chacune un photocourant noté $I_1(t)$ et $I_2(t)$. Un module électrique soustracteur combine les deux photocourants en un seul, noté $I(t)$ tel que $I(t) = I_1(t)-I_2(t)$, porteur de la modulation d'amplitude, de phase ou de fréquence.

#### 3.3.1.1 Hypothèses et notations

Nous supposerons :
- Les ondes optiques *signal* et *oscillateur local* ont même polarisation, donc leur champs électriques sont représentables par des scalaires.
- Les deux photodiodes présentent des caractéristiques identiques.
- La matrice de transfert du coupleur 50/50, supposé parfait, est donnée par l'équation (111).

Les ondes optiques sont caractérisées par leur champs électriques, notés :

$$E_S(t) = |E_S| \exp j(\omega_0 t + \phi_S) \tag{54}$$

$$E_{LO}(t) = |E_{LO}| \exp j(\omega_{LO} t + \varphi_{LO}) \tag{55}$$

Le module du champ $|E_{LO}|$ est proportionnel à celui de $E_S$.

$$|E_{LO}| = K|E_S| \tag{56}$$

La fréquence $\omega_{LO}$ correspond à la fréquence optique de l'oscillateur local. Le déphasage $\phi_S$ représente les modulations successives d'Alice et de Bob. Les éventuelles variations de phase entre le bras *signal* et le bras *oscillateur local* sont notées $\varphi_{LO}$.

#### 3.3.1.2 Equations

A la sortie du coupleur, les champs électriques des ondes ont pour équations :

$$E_1(t) = \frac{|E_S|}{\sqrt{2}}\left[\exp j(\omega_0 t + \phi_S) - jK \exp j(\omega_{LO} t + \varphi_{LO})\right] \tag{57}$$

$$E_2(t) = \frac{|E_S|}{\sqrt{2}}\left[K \exp j(\omega_{LO} t + \varphi_{LO}) - j \exp j(\omega_0 t + \phi_S)\right] \tag{58}$$

Chaque onde est alors détectée par une photodiode générant chacune deux photocourants électriques :

$$I_1(t) = R_1 . \frac{|E_S|^2}{2}\left[1 + K^2 + 2K \sin\left((\omega_{LO} - \omega_0)t + \varphi_{LO} - \phi_S\right)\right] \tag{59}$$

$$I_2(t) = R_2 . \frac{|E_S|^2}{2}\left[1 + K^2 - 2K \sin\left((\omega_{LO} - \omega_0)t + \varphi_{LO} - \phi_S\right)\right] \tag{60}$$

$$R_i = \frac{\eta_i e}{h\nu} . \frac{S}{2Z_0} \tag{61}$$

où $e$ représente la charge élémentaire de l'électron, $\eta$ rendement quantique de la photodiode, $h$ constante de Planck, $\nu$ fréquence optique, $S$ surface du détecteur et $Z_0$ impédance du détecteur

Un module électrique soustracteur effectue la soustraction de ces deux courants et délivre un courant $I_-(t)$ . En supposant que les photodiodes soient identiques (de même efficacité), la différence des photocourants, notée $I_-(t)$, s'écrit

$$I_-(t) = I_2(t) - I_1(t) \tag{62}$$

$$I_-(t) = \frac{\eta . e}{h\nu} \frac{S}{Z_0} K |E_S|^2 \sin\left((\omega_0 - \omega_{LO})t + \phi_S - \varphi_{LO}\right) \tag{63}$$

Le courant $I_-(t)$ est linéairement dépendant de la modulation de phase.

### 3.3.2 Détection hétérodyne / homodyne

Dans une détection hétérodyne [37], l'onde *oscillateur local* provient d'un modulateur acousto-optique. Sa fréquence est alors décalée de $\Omega$ par rapport à celle de l'onde *signal*. Soit $\omega_{IF}$ la fréquence intermédiaire, différence des fréquences de l'onde *signal* et de l'onde *référence*.

$$I_{-}(t) = \alpha K \left|E_S\right|^2 \sin\left(\omega_{IF} t + \phi_S - \varphi_{LO}\right) \tag{64}$$

avec $\alpha$ coefficient caractéristique du système de détection.

Le principe de la détection homodyne est similaire à celui de la détection hétérodyne à la différence que la fréquence de l'onde *signal* est identique à celle de l'onde de l'oscillateur local.

$$\omega_{LO} = \omega_0 \tag{65}$$

Le courant $I_{-}(t)$, réponse d'un système de détection homodyne, s'écrie

$$I_{-}(t) = \alpha K \left|E_S\right|^2 \sin\left(\phi_S - \varphi_{LO}\right) \tag{66}$$

Lorsque les amplitudes des champs des ondes *signal* et de l'oscillateur local sont égales,

$$K = 1 \tag{67}$$

L'équation (67) devient

$$I_{-}(t) = \alpha \left|E_S\right|^2 \sin\left(\phi_S - \varphi_{LO}\right) \tag{68}$$

La détection est dite *super-homodyne* pour $K>>1$ et *homodyne* pour $K=1$.

### 3.3.3 Théorie classique de la détection homodyne

Soient $A$ l'onde *signal* et $jB$ l'onde *référence* entrant dans le coupleur optique représentées sur la Figure 37. En respectant la matrice de transfert d'un coupleur 50/50 donnée en (4.1.2), les champs des ondes à la sortie du coupleur, notés $C_1$ et $C_2$, s'expriment par

$$\begin{aligned} C_1 &= \frac{1}{\sqrt{2}}\left(A - B\right) \\ C_2 &= \frac{j}{\sqrt{2}}\left(A + B\right) \end{aligned} \tag{69}$$

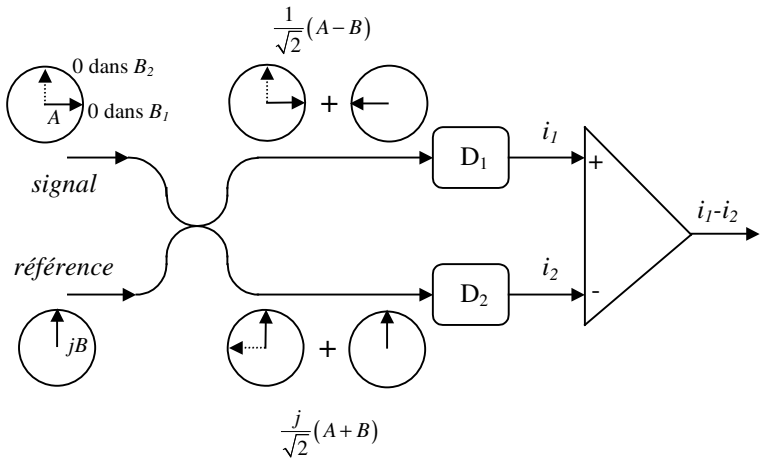



Figure 37 Schéma d'un système de détection homodyne équilibrée fonctionnant en régime classique.

Les détecteurs $D_1$ et $D_2$ génèrent deux photocourants, notés $i_1$ et $i_2$, proportionnels au module carré de l'onde les éclairant.

$$\begin{aligned} i_1 &= \frac{A^2 + B^2}{2} - AB \\ i_2 &= \frac{A^2 + B^2}{2} + AB \end{aligned} \tag{70}$$

La soustraction des deux photocourants a pour expression

$$i_2 - i_1 = 2AB \tag{71}$$

### 3.3.4 Théorie quantique de la détection homodyne

Soient $\hat{s}$ l'opérateur de l'onde *signal* et $\hat{l}$ celui représentant l'onde *référence* entrant dans le coupleur optique représentés sur la Figure 38.

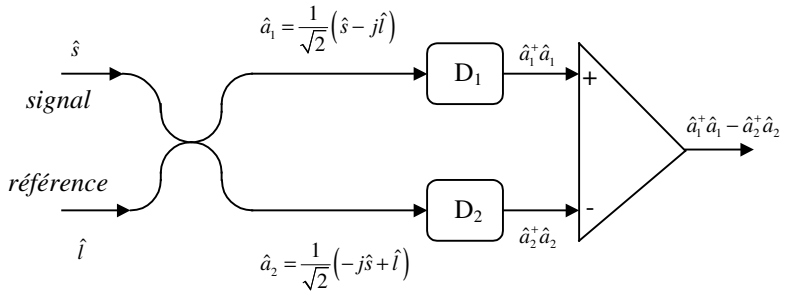



Figure 38 Schéma d'un système de détection homodyne équilibrée fonctionnant en régime quantique.

En considérant le système de détection homodyne équilibré et sans perte et un rendement quantique des détecteurs égales à 1, les opérateurs *nombre de photons* avant les détecteurs $D_1$ et $D_2$ sont respectivement

$$\begin{aligned}\hat{a}_1^+\hat{a}_1 &= \frac{1}{2}\left(\hat{s}^+\hat{s} + \hat{l}^+\hat{l} - j\left(\hat{s}^+\hat{l} - \hat{l}^+\hat{s}\right)\right)\\ \hat{a}_2^+\hat{a}_2 &= \frac{1}{2}\left(\hat{s}^+\hat{s} + \hat{l}^+\hat{l} + j\left(\hat{s}^+\hat{l} - \hat{l}^+\hat{s}\right)\right)\end{aligned} \tag{72}$$

La soustraction cohérente des deux photocourants permet de retrouver toute l'énergie du signal qui s'est propagée aux deux détecteurs via le coupleur. En considérant une efficacité quantique unitaire pour les deux détecteurs, l'opérateur *nombre d'électrons* est donné

$$\hat{N} = \hat{a}_1^+\hat{a}_1 - \hat{a}_2^+\hat{a}_2 = -j\left(\hat{s}^+\hat{l} - \hat{l}^+\hat{s}\right) \tag{73}$$

Les opérateurs *signal* et *référence* peuvent être décomposés en un terme en amplitude et un terme en phase, soit

$$\begin{aligned}\hat{s} &= \hat{s}_I + j\hat{s}_Q\\ \hat{l} &= \hat{l}_I + j\hat{l}_Q\end{aligned} \tag{74}$$

L'équation (73) devient alors

$$\hat{N} = 2\left(\hat{s}_I\hat{l}_Q - \hat{s}_Q\hat{l}_I\right) \tag{75}$$

Précisons que la description des opérateurs $\hat{s}$ et $\hat{l}$ fait référence aux champs aux entrées du coupleur optique.

Il est possible de simplifier la notation en se référant au champ de l'onde *référence* arrivant sur le détecteur $D_1$, c'est à dire en remplaçant $-j\hat{l}$ par $\hat{l}$ dans l'équation (73). L'opérateur *nombre d'électrons* s'écrit alors

$$\hat{N} = \hat{s}^{+}\hat{l} + \hat{l}^{+}\hat{s} \tag{76}$$

$$\hat{N} = 2\left(\hat{s}_I\hat{l}_I + \hat{s}_Q\hat{l}_Q\right) \tag{77}$$

$\hat{N}$ est proportionnel à la double projection de l'opérateur *signal* sur l'opérateur *référence*.

En séparant les contributions classiques et quantiques pour chaque composante des champs *signal* et *référence*, les opérateurs s'écrivent

$$\begin{aligned}
&\hat{s}_I = S_I + \Delta\hat{s}_I \quad \text{avec} \quad S_I = \left\langle \hat{s}_I \right\rangle \\
&\hat{s}_Q = S_Q + \Delta\hat{s}_Q \quad \text{avec} \quad S_Q = \left\langle \hat{s}_Q \right\rangle \\
&\hat{l}_I = L_I + \Delta\hat{l}_I \quad \text{avec} \quad L_I = \left\langle \hat{l}_I \right\rangle \\
&\hat{l}_Q = L_Q + \Delta\hat{l}_Q \quad \text{avec} \quad L_Q = \left\langle \hat{l}_Q \right\rangle
\end{aligned} \tag{78}$$

L'équation (77) s'écrit alors

$$\hat{N} = 2\left(\left(L_I + \Delta\hat{l}_I\right)\hat{s}_I + \left(L_Q + \Delta\hat{l}_Q\right)\hat{s}_Q\right) \tag{79}$$

Afin de mesurer $S_I$ (ou $S_Q$), il convient d'annuler le terme $L_Q$ (ou $L_I$). Lorsque $S_I$ doit être mesuré, l'équation (79) devient

$$\hat{N} = 2\left(\left(L_I + \Delta\hat{l}_I\right)\left(S_I + \Delta\hat{s}_I\right) + \Delta\hat{l}_Q\hat{s}_Q\right) \tag{80}$$

Le niveau de l'onde *référence* est dit fort lorsque $N_L >> N_S$. Or

$$\begin{aligned}
N_L &= L_I^2 \\
N_S &= S_I^2 + S_Q^2
\end{aligned} \tag{81}$$

Dans ce cas, le terme dominant de l'équation (80) est $\hat{s}_I\hat{l}_I$. L'équation (80) se simplifie en

$$\hat{N} = 2\left(S_I + \Delta\hat{s}_I\right)L_I \tag{82}$$

Précisons que les fluctuations quantiques de la *référence* ont été négligées devant la composante déterministe de la *référence*.

Le signal de sortie d'un système de détection homodyne équilibrée est proportionnel au signal d'entrée, somme de la composante $S_I$ et du bruit quantique $\Delta\hat{s}_I$. Ce signal d'entrée est

amplifié par la composante $L_I$ , partie déterministe de la composante en phase de la *référence*, qui joue le rôle de gain de mixage sans bruit. Cette composante est définie à l'entrée des détecteurs, et correspond donc à la composante orthogonale à l'entrée du coupleur optique (4.1.2).

Dans une détection homodyne, seule une quadrature du signal est mesurée et ceci s'opère sans ajout de bruit. Le bruit quantique du *signal* d'entrée est donc la seule contribution au bruit du signal de sortie. Il correspond aux fluctuations du vide entrant dans le coupleur optique. La soustraction des deux photocourants générés par un système de détection homodyne permet de rejeter les fluctuations classiques et quantiques de la *référence*. Il apparaît alors que la détection homodyne est seulement limitée par les fluctuations quantiques du *signal*, c'est à dire, les fluctuations du vide. Le bruit de photon de la référence dû aux fluctuations du vide entrant dans le coupleur par le port référence n'influence pas le bruit en sortie.

### 3.3.5 Rapport *signal sur bruit* dans une détection homodyne

Les imperfections réelles du *signal* et de la *référence* dégradent le battement des deux ondes et affaiblissent la détection homodyne. Ces sources de perturbations sont :

- le bruit quantique du *signal*,
- le déphasage statique de la *référence*.

#### 3.3.5.1 Bruit quantique du *signal*

Si la différence de phase entre la *référence* et le *signal* ne fluctue pas, l'opérateur *nombre de photon* est

$$\begin{aligned} \hat{N} &= 2\hat{s}_I\hat{l}_I = 2\left(S_I + \Delta\hat{s}_I\right)L_I \\ \hat{N} &= \left\langle \hat{N} \right\rangle + \Delta\hat{N} \quad \text{avec} \quad \hat{N} = 2L_I S_I \quad \text{et} \quad \Delta\hat{N} = 2L_I\Delta\hat{s}_I \end{aligned} \tag{83}$$

Le carré moyen du signal est

$$\left\langle \hat{N} \right\rangle^2 = \left\langle \hat{N}^2 \right\rangle - \left\langle \left(\Delta\hat{N}\right)^2 \right\rangle = 4L_I^2\left(S_I^2 + \frac{1}{4}\right) \tag{84}$$

En posant $N_S = \left\langle \hat{s}^+\hat{s} \right\rangle$ et $N_L = \left\langle \hat{l}^+\hat{l} \right\rangle$,

$$\left\langle \hat{N} \right\rangle^2 = 4N_L N_S + N_L \tag{85}$$

En considérant que le *signal* est un état cohérent, le bruit est donné par

$$\left\langle \left(\Delta\hat{N}\right)^2 \right\rangle = 4L_I^2\left\langle \left(\Delta\hat{s}_I\right)^2 \right\rangle = L_I^2 = N_L \tag{86}$$

Il apparaît que le bruit en sortie est égal à la moyenne du carré des fluctuations du nombre de photon.

$$\left\langle \left(\Delta \hat{N}_L\right)^2 \right\rangle = N_L \tag{87}$$

L'équation (103) correspond aux fluctuations de Poisson. En accord avec la théorie classique de la détection homodyne, la limite fondamentale du bruit correspond au *shot noise* de la *référence*.

La puissance du signal de sortie est

$$\left\langle \hat{N}^2 \right\rangle = 4N_L N_S \tag{88}$$

Des équations (87) et (104), le rapport du signal sur bruit par bit est alors

$$\frac{E_B}{N_0} = \frac{4N_L N_S}{N_L} = 4N_S \tag{89}$$

où $E_B$ est l'énergie par bit et $N_0$ la densité spectrale de bruit.

### 3.3.5.2 Déphasage statique de la *référence*

Des équations (76) et (78), l'opérateur nombre de photon s'écrit

$$\begin{aligned} \hat{N} &= \hat{s}^+ \left(L + \Delta\hat{l}\right) + \left(L^+ + \Delta\hat{l}^+\right)\hat{s} \\ &= \hat{s}^+ L + L^+ \hat{s} \end{aligned} \tag{90}$$

Soit $\theta$ le déphasage de l'onde référence, $L = |L| \exp j\theta$.

$$\hat{N} = |L|\left(\hat{s}^+ \exp j\theta + \hat{s} \exp - j\theta\right) \tag{91}$$

Soit $\hat{s}_\theta = \hat{s} \exp(-j\theta)$ tel que $\hat{s}_\theta = \hat{s}_I \cos\theta + \hat{s}_Q \sin\theta + j\left(\hat{s}_Q \cos\theta - \hat{s}_I \sin\theta\right)$.

Lorsque $\hat{s}_{\theta I}$ est mesuré à la place de $\hat{s}_\theta$, l'opérateur *nombre de photon* s'écrit

$$\hat{N} = 2|L|\hat{s}_{\theta I} = 2|L|\left(\hat{s}_I \cos\theta + \hat{s}_Q \sin\theta\right) \tag{92}$$

$$\left\langle \hat{N} \right\rangle = 2|L|\left(S_I \cos\theta + S_Q \sin\theta\right) \tag{93}$$

$$\begin{aligned} \left\langle \hat{N}^2 \right\rangle &= 4|L|\left(\left(S_I \cos\theta + S_Q \sin\theta\right)^2 + \left\langle \left(\Delta\hat{s}_I^2\right)\right\rangle \cos^2\theta + \left\langle \left(\Delta\hat{s}_Q^2\right)\right\rangle \sin^2\theta\right) \\ &= 4L^2\left(S_I^2 \cos^2\theta + \frac{1}{4}\right) \end{aligned} \tag{94}$$

Soit

$$\left\langle \hat{N}^2 \right\rangle = 4N_L N_S \cos^2\theta + N_L \tag{95}$$

La puissance du bruit en sortie est

$$\left\langle \left(\Delta\hat{N}\right)^2 \right\rangle = 4L^2 \left\langle \left(\Delta\hat{s}_I\right)^2 \right\rangle = L^2 = N_L \tag{96}$$

De l'équation (95), la puissance du signal en sortie est

$$\left\langle \hat{N} \right\rangle^2 = 4N_L N_S \cos^2\theta \tag{97}$$

Le rapport signal sur bruit par bit est alors défini par

$$\frac{E_B}{N_0} = 4N_S \cos^2\theta \tag{98}$$

## 3.4 Conclusion

Un système de Distribution Quantique de Clef nécessite trois sous-ensembles ; un émetteur de photons uniques, une chaîne de modulation et un système de détection adapté. Nous avons présenté différentes solutions permettant de réaliser ces trois fonctions.

La source de photon unique est constituée d'un laser fortement atténué, dont la distribution du nombre de photons par impulsion peut être paramétrée aisément.

Une chaîne de modulation permettant de transposer les choix d'Alice et de Bob dans le domaine optique par codage de phase réalisé à l'aide de deux modulateurs Mach-Zehnder à doubles électrodes a été proposée. Ses caractéristiques ont été mises en évidence.

Plusieurs systèmes de détection ont été proposés autorisant des mesures de la phase optique, porteuse de l'information, à faible et forte puissance (respectivement domaine quantique et domaine classique).

# Chapitre 4.

# Description des composants

Ce quatrième chapitre présente les composants nécessaires à l'implémentation du protocole BB84 par codage de phase. Il décrit leurs fonctions générales, et précise leurs caractéristiques techniques afin de fournir une base facilitant le passage des équations théoriques aux montages expérimentaux.

## 4.1 Les coupleurs, systèmes optiques à quatre ports

Un coupleur se définit comme un dispositif optique passif à deux entrées et deux sorties optiques, dont le rôle est de transmettre les signaux optiques d'entrée aux sorties suivant des relations algébriques linéaires caractérisées par une *matrice de transfert*.

Le principe de base est celui du couplage par onde évanescente entre deux fibres dont les cœurs sont très proches. Le champ électromagnétique s'étendant au-delà des cœurs, la lumière qui se propage dans un guide passe graduellement dans l'autre via la zone de transfert et la longueur de couplage est ajustée pour le coefficient de répartition en puissance choisi.

Ces systèmes optiques peuvent être réalisés par la technique du polissage-assemblage ou celle de la fusion-étirage.

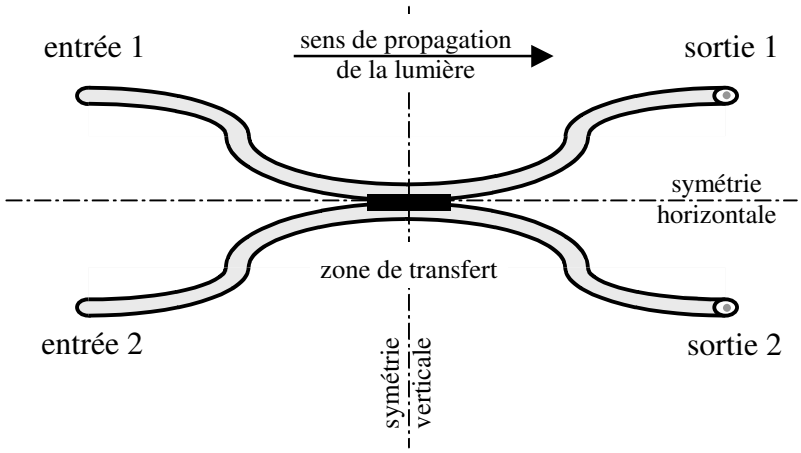



Figure 39 Coupleur optique 2x2.

Certains coupleurs, notés 1x2 ou 2x1, possèdent une entrée ou, respectivement, une sortie masquée. Cependant leurs matrices de transfert sont identiques à celle d'un coupleur 2x2.

### 4.1.1 Matrice de transfert d'un coupleur 2x2

Les ondes optiques entrantes et sortantes sont caractérisées par leurs champs électromagnétiques $E_1$, $E_2$, $S_1$ et $S_2$. Ce sont des nombres complexes. La matrice de transfert carrée $M_{2x2}$ à éléments complexes s'écrit

$$\begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} \tag{99}$$

• Le coupleur possède une symétrie hermitienne par rapport à l'axe horizontal (Figure 39) qui permet d'écrire l'invariance de $M_{2x2}$ lorsque les signaux d'entrée sont permutés, induisant une permutation des signaux de sortie.

$$\begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = M_{2x2} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} \text{ et } \begin{pmatrix} S_2 \\ S_1 \end{pmatrix} = M_{2x2} \begin{pmatrix} E_2 \\ E_1 \end{pmatrix} \tag{100}$$

Par conséquent, $M_{2x2}$ est symétrique et s'écrit

$$M_{2x2} = {}^t M_{2x2} \tag{101}$$

• Les coupleurs à fibre présentent peu de pertes intrinsèques à la zone de transfert. En ne tenant pas compte des pertes d'insertion et d'absorption dans les fibres optiques, le coupleur est sans perte. Sa matrice $M_{2x2}$ est de plus unitaire.

$$M_{2x2}^{-1} = M_{2x2}^{+} \tag{102}$$

• Le coupleur possède une symétrie hermitienne par rapport à l'axe vertical (Figure 39) induisant un changement du sens de propagation de la lumière.

$$M_{2x2}^{-1} = M_{2x2}^{*} \tag{103}$$

$$\overline{M}_{2x2} . M_{2x2} = I \tag{104}$$

La forme de $M_{2x2}$ se déduit des propriétés (101), (102) et (103). Elle s'écrit

$$M_{2x2} = \begin{pmatrix} A & B \\ B & A \end{pmatrix} \tag{105}$$

L'équation (104) s'écrit

$$\begin{cases} A^* A + B^* B = 1 \\ A^* B + B^* A = 0 \end{cases} \tag{106}$$

Soient $a$ et $b$ les modules de $A$ et de B et $\phi_A$ et $\phi_B$ les arguments de $A$ et $B$,

$$\begin{cases} a^2 + b^2 = 1 \\ ab.\cos(\phi_A - \phi_B) = 0 \end{cases} \tag{107}$$

Le système (107) admet alors quatre solutions équivalentes.

$$\begin{cases} \Delta\phi = \pm\frac{\pi}{2}[2\pi] \\ b = \pm\sqrt{1-a^2} \end{cases} \tag{108}$$

Ainsi, un coupleur 2x2 supposé sans perte, linéaire et réciproque est caractérisé par la matrice (109), solution du système (107). Cette solution particulière a été retenue pour exprimer les fonctions de transfert d'un interféromètre et d'un modulateur Mach-Zehnder.

$$M_{2x2} = \begin{pmatrix} a & -\sqrt{1-a^2}\,j \\ -\sqrt{1-a^2}\,j & a \end{pmatrix} \tag{109}$$

### 4.1.2 Matrice de transfert d'un coupleur 3 dB

Un coupleur 3 dB, encore appelé coupleur "50/50", equipartage la puissance optique de chaque entrée entre les deux sorties.

$$a^2 = b^2 \tag{110}$$

Il est caractérisé par la matrice

$$M_{3dB} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -j \\ -j & 1 \end{pmatrix} \tag{111}$$

## 4.2 Interféromètre Mach-Zehnder

Un interféromètre Mach-Zehnder est représenté par la Figure 40. Les faisceaux optiques incidents, caractérisés par leurs champs électromagnétiques $E_1$ et $E_2$, sont divisés en deux via un coupleur 3 dB, puis chacun des faisceaux résultants empruntent des chemins optiques différents sur lesquels ils subissent un retard optique $\tau$ induisant un déphasage. En fonction du déphasage, les faisceaux cohérents interfèrent de manière constructive ou destructive.

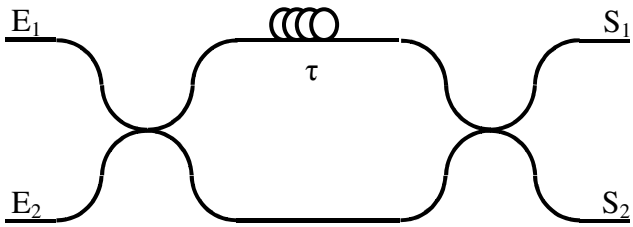



Figure 40 Interféromètre de Mach-Zehnder.

### 4.2.1 Mach-Zehnder équilibré

Dans un dispositif Mach-Zehnder équilibré, la différence de chemin optique des deux bras est nulle ($\tau = 0$). Sa matrice de transfert est alors

$$\begin{aligned} M_{MZ_{équilibré}} &= M_{3dB}.M_{3dB} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -j \\ -j & 1 \end{pmatrix} \times \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -j \\ -j & 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -j \\ -j & 0 \end{pmatrix} \end{aligned} \tag{112}$$

### 4.2.2 Mach-Zehnder déséquilibré

Dans un interféromètre Mach-Zehnder déséquilibré, l'un des faisceaux subit un retard optique $\tau$ par rapport à l'autre. Sa matrice de transfert s'écrit

$$M_{MZ_{déséquilibré}} = M_{3dB} \cdot \begin{pmatrix} \exp j\omega\tau & 0 \\ 0 & 1 \end{pmatrix} . M_{3dB} \tag{113}$$

$$M_{MZ_{déséquilibré}} = j\exp\left(\frac{j\omega\tau}{2}\right)\begin{pmatrix} \sin\left(\frac{j\omega\tau}{2}\right) & -\cos\left(\frac{j\omega\tau}{2}\right) \\ -\cos\left(\frac{j\omega\tau}{2}\right) & -\sin\left(\frac{j\omega\tau}{2}\right) \end{pmatrix} \tag{114}$$

## 4.3 Modulateur Mach-Zehnder

La modulation est une des fonctions optiques les plus importantes pour l'implémentation d'un protocole cryptographique. Elle permet d'imprimer une information (dans notre cas, une information binaire) sur un signal physique (une onde optique). La modulation est dite externe, puisqu'elle est réalisée par un système électro-optique indépendant de la source optique émettant une onde pure.

### 4.3.1 Structure d'un modulateur Mach-Zehnder

Les modulateurs de type Mach-Zehnder en $LiNbO_3$ ont tous une structure identique. Ils sont composés de deux guides d'onde, de deux embranchements en Y (coupleurs 1x2 et 2x1) et d'électrodes permettant d'injecter des signaux électriques.

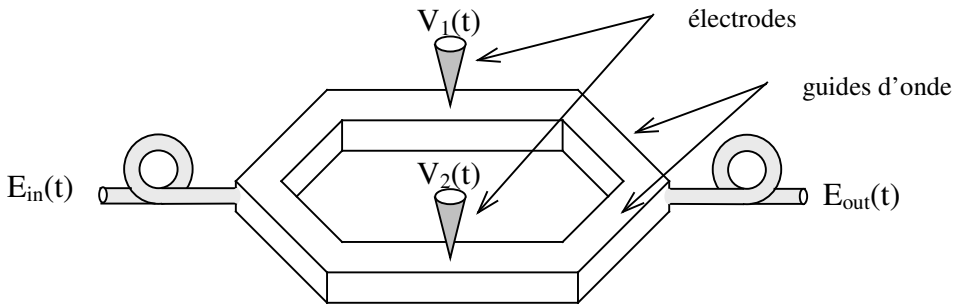



Figure 41 Structure d'un modulateur MZ
intégré à doubles électrodes.

Le signal optique d'entrée pénètre dans le modulateur au moyen d'une fibre optique à maintien de polarisation appelée fibre d'amorce. Le premier embranchement en Y sépare également les signaux pour les transmettre aux deux guides d'onde (encore appelés « bras »). L'écartement entre les deux bras est suffisant pour que le couplage par onde évanescente soit négligeable.

L'indice de réfraction du matériau électro-optique est modifié par l'application d'une tension, entraînant ainsi un déphasage entre les deux faisceaux. La seconde jonction en Y combine les deux faisceaux qui interfèrent. Il est ainsi possible d'obtenir toute la puissance optique en sortie (interférence constructive) ou au contraire, que la lumière ne soit pas injectée dans le guide de sortie (interférence destructive).

Entre ces deux extrêmes, tous les cas intermédiaires sont possibles et la modulation de la lumière reproduit celle de la tension appliquée avec une fonction de transfert sinusoïdale.

Le déphasage entre les deux faisceaux peut être introduit de trois manières :
- soit par application d'une tension électrique sur les électrodes d'un seul bras ($V_2$=0),
- soit par application de tensions électriques opposées sur les électrodes des deux bras suivant le procédé « push-pull » ($V_1$= -$V_2$),
- soit par application de tensions électriques différentes sur chaque bras.

Ce type de modulateur permet ainsi de moduler l'amplitude et/ou la phase d'un signal optique.

Les modulateurs Mach-Zehnder utilisés dans notre dispositif expérimental possèdent deux électrodes, une sur chaque bras. Les tensions électriques de contrôle $V_1$ et $V_2$ se traduisent optiquement par deux déphasages notés respectivement $\phi_1$ et $\phi_2$ (Figure 42).

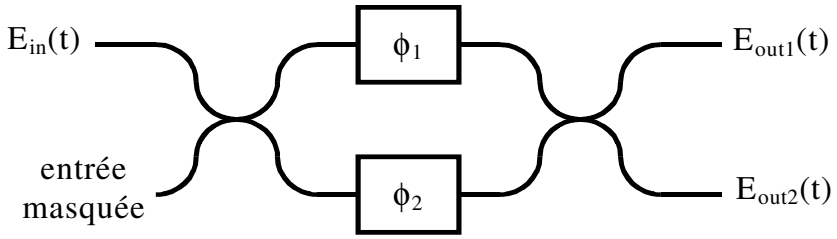



Figure 42 Modulateur MZ à deux électrodes.

D'après les Figure 41 et Figure 42, les ondes de sortie caractérisées par les champs $E_{out1}(t)$ et $E_{out2}(t)$ obéissent à

$$\begin{pmatrix} E_{out1}(t) \\ E_{out2}(t) \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -j \\ -j & 1 \end{pmatrix} \cdot \begin{pmatrix} \exp j\phi_1 & 0 \\ 0 & \exp j\phi_2 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -j \\ -j & 1 \end{pmatrix} \cdot \begin{pmatrix} E_{in}(t) \\ 0 \end{pmatrix} \tag{115}$$

Un modulateur Mach-Zehnder intégré ne possède souvent qu'une sortie optique, la seconde sortie étant cachée. L'équation de l'onde optique sortante est alors représentée par $E_{out1}(t)$ ou $E_{out2}(t)$.

$$\begin{cases} E_{out1}(t) = j.E_{in}(t).\sin\left(\frac{\phi_1 - \phi_2}{2}\right).\exp j\frac{\phi_1 + \phi_2}{2} \\ E_{out2}(t) = -j.E_{in}(t).\cos\left(\frac{\phi_1 - \phi_2}{2}\right).\exp j\frac{\phi_1 + \phi_2}{2} \end{cases} \tag{116}$$

L'expression de $E_{out1}(t)$ dans l'équation (116) présente un terme complexe $j$ ne dépendant pas des déphasages introduits. Il est possible de le supprimer en posant :

$$\begin{cases} \phi_1^{'} = \phi_1 + \dfrac{\pi}{2} \\ \phi_2^{'} = \phi_2 + \dfrac{\pi}{2} \end{cases} \tag{117}$$

Des équations (116) et (117), l'expression de $E_{out1}(t)$ s'écrit

$$E_{out1}(t) = E_{in}(t).\sin\left(\frac{\phi_1^{'} - \phi_2^{'}}{2}\right).\exp j\frac{\phi_1^{'} + \phi_2^{'}}{2} \tag{118}$$

De même, l'expression de $E_{out2}(t)$ représentée par l'équation (116) présente un terme complexe *-j* ne dépendant pas des déphasages introduits. Il est possible de le supprimer en posant :

$$\begin{cases} \phi_1^{'} = \phi_1 - \dfrac{\pi}{2} \\ \phi_2^{'} = \phi_2 - \dfrac{\pi}{2} \end{cases} \tag{119}$$

Des équations (116) et (119), l'expression de $E_{out2}(t)$ s'écrit

$$E_{out2}(t) = E_{in}(t).\cos\left(\frac{\phi_1^{'} - \phi_2^{'}}{2}\right).\exp j\frac{\phi_1^{'} + \phi_2^{'}}{2} \tag{120}$$

L'introduction d'un déphasage constant de $\pm\pi/2$ à $\phi_1$ et à $\phi_2$ est facilement réalisable expérimentalement en ajoutant à $V_1$ et à $V_2$ une tension constante $\pm V_\pi/2$.

L'équation (121) présente un terme réel correspondant à une modulation d'amplitude, et un terme complexe correspondant à une modulation de phase.

L'implémentation du protocole BB84 par l'utilisation de modulateur Mach-Zehnder à double électrode nécessite une modulation d'amplitude constante et fixée à $\sqrt{2}/2$.

L'équation du champ électromagnétique de l'onde de sortie du modulateur d'Alice est par conséquent égale à

$$E_{out}(t) = \frac{\sqrt{2}}{2}E_{in}(t).\exp j\left(\frac{\phi_1 + \phi_2}{2}\right) \tag{121}$$

### 4.3.2 Caractéristiques des modulateurs Mach-Zehnder

Les deux modulateurs Mach-Zehnder utilisés ont été fabriqués par *Sumitomo Osaka* et sont référencés : *T-DEH-1.5-5*. Leurs numéros de série sont : *MZ6-91-29-55-621* et *MZ6-91-29-55-622*. Les trois derniers chiffres permettent de les distinguer ; le 621 est attribué au dispositif d'Alice et le 622 à celui de Bob.

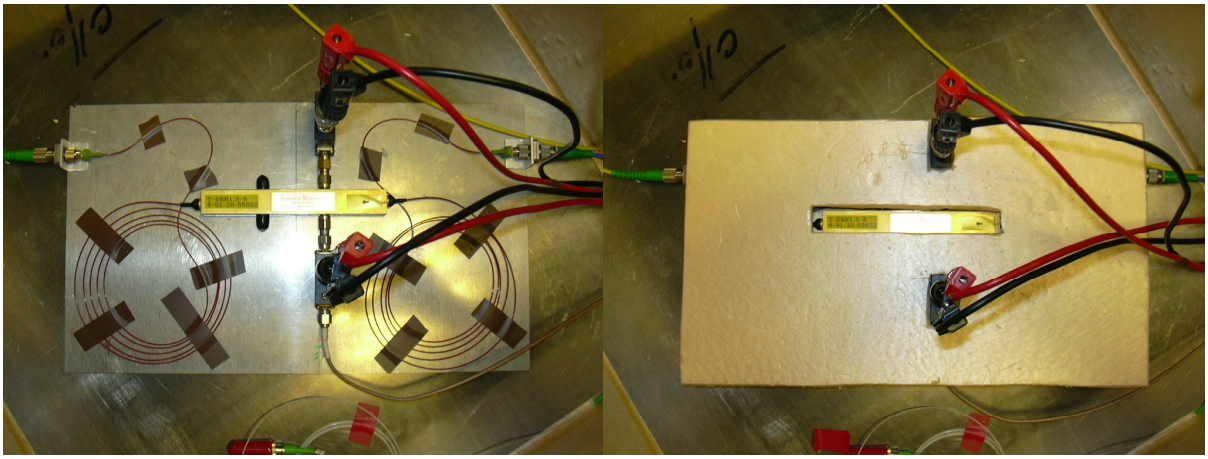


Figure 43 Modulateur Mach-Zehnder à doubles électrodes et sa protection thermique.

La tension $V_\pi$, encore appelée $V_{\lambda/2}$, correspond à la tension nécessaire à l'ouverture complète de la cellule électro-optique. En appliquant cette tension aux bornes électriques du modulateur, le déphasage introduit vaut π. Pour mesurer $V_\pi$, il est nécessaire de mesurer la puissance optique sortante en fonction de la tension appliquée sur chaque électrode (Figure 44).

Les deux modulateurs Mach-Zehnder à doubles électrodes présentent la même tension $V_\pi$. Cette caractéristique est essentielle pour la traduction des signaux électriques, représentant les choix d'Alice et de Bob, en déphasages optiques.

Le Tableau 9 présente les autres caractéristiques essentielles.

| | **Alice** | | **Bob** | | constructeur |
|---|---|---|---|---|---|
| Perte d'insertion en dB | 4,0 | | 4,5 | | ≤ 6,0 |
| | Electrode 1 | Electrode 2 | Electrode 1 | Electrode 2 | |
| $V_\pi$ en volt | 3,6 | 3,6 | 3,6 | 3,6 | ≤ 4,5 |
| Coefficient d'extinction en dB | 31,6 | 31,8 | 32,2 | 32,3 | ≥ 20,0 |
| Bande passante en GHz | 7,9 | 8,1 | 8,1 | 8,0 | ≥ 4,0 |

Tableau 9 Caractéristiques des modulateurs MZ.

La puissance optique d'entrée ne doit pas dépasser 10 mW. Les tensions électriques appliquées ne doivent pas excéder ± 15 V.

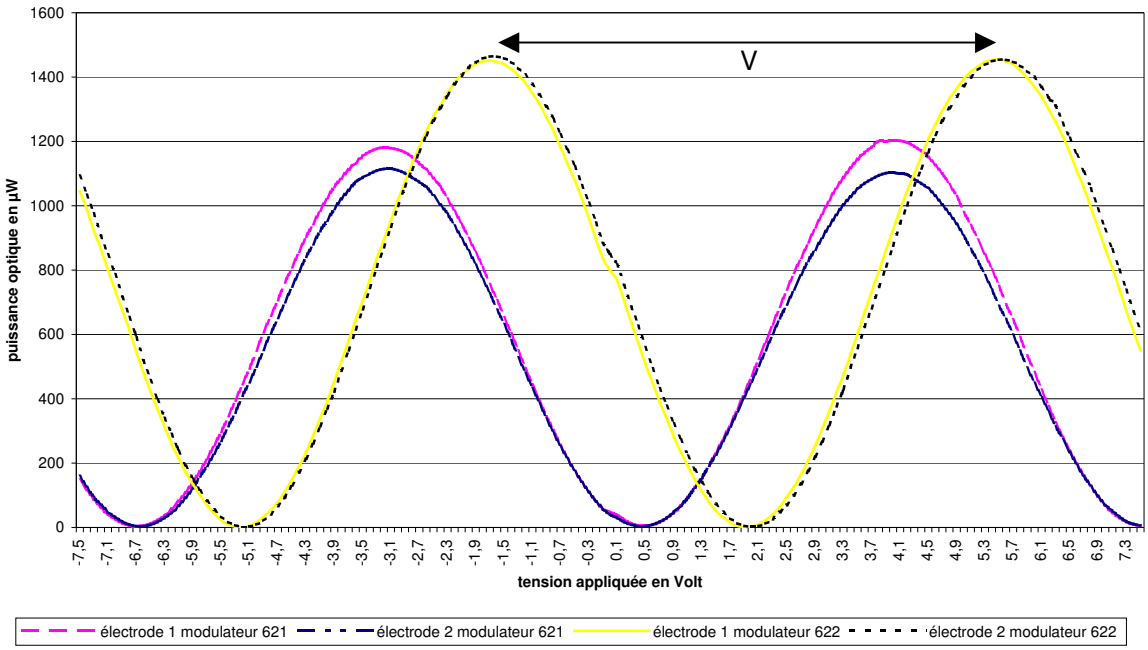



Figure 44 Tension $V_\pi$ des modulateurs Mach-Zehnder à doubles électrodes.

## 4.4 Les contrôleurs de polarisation

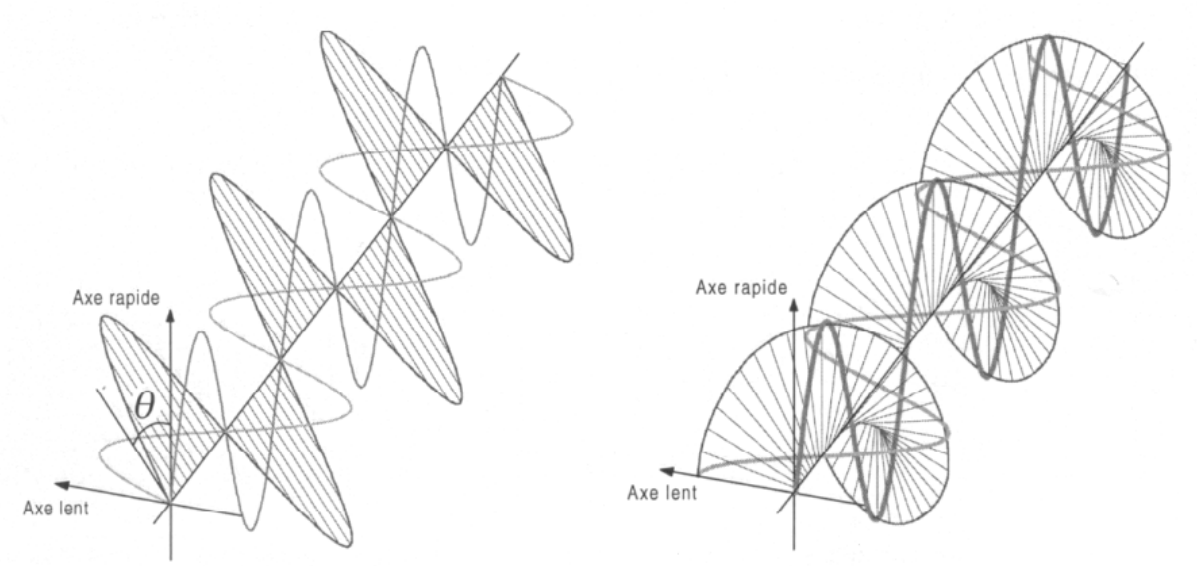
Les différents composants optiques (principalement les modulateurs Mach-Zehnder) nécessitent un ajustement de la direction de la polarisation de l'onde incidente.

Les contrôleurs de polarisation fibrés reposent tous sur le même principe ; l'utilisation d'éléments biréfringents fibrés, qui induisent des différences de trajets de $\lambda/2$ ou $\lambda/4$ entre les axes principaux de polarisation. Les éléments $\lambda/4$ permettent de convertir une polarisation linéaire en une polarisation circulaire ou elliptique, et inversement. Les éléments $\lambda/2$ sont utilisés pour effectuer des rotations de polarisation. Les contrôleurs de polarisation utilisés sont tous composés d'un élément $\lambda/4$, d'un élément $\lambda/2$ suivi d'un second élément $\lambda/4$.

### 4.4.1 Eléments $\lambda/4$

Soit un signal entrant dans un élément $\lambda/4$, ayant une polarisation linéaire, et un angle $\theta$ par rapport à l'axe de rapide. Si $\theta$ est un multiple de $\pi/2$, le signal traverse l'élément sans être affecté, car une de ses composantes de polarisation est alors nulle. Si $\theta = \pi/4$, ses deux composantes de polarisation sont en phase et d'amplitudes égales. A la sortie de l'élément $\lambda/4$, la polarisation sur l'axe lent est retardé de $\pi/2$ par rapport à l'axe rapide. La polarisation résultante est donc circulaire. Pour les autres valeurs de $\theta$, la polarisation résultante est

elliptique. Réciproquement, une polarisation circulaire ou elliptique est convertie en polarisation linéaire.




polarisation linéaire polarisation circulaire

Figure 45 Elément *λ/4*.

Les éléments *λ/4* sont donc principalement utilisés pour transformer une onde polarisée linéairement en une onde polarisée circulairement (ou inversement).

### 4.4.2 Eléments *λ/2*

Un élément *λ/2* rend la direction de polarisation de sortie symétrique à sa direction d'entrée par rapport à l'axe rapide. En notant $\theta$ l'angle formé par la direction de polarisation d'entrée et l'axe rapide (Figure 46), la direction de polarisation de l'onde subira une symétrie par rapport à l'axe rapide. A la sortie d'un élément *λ/2*, l'angle est égal à $-\theta$. La composante de polarisation sur l'axe lent prend un retard de $\pi$, ce qui correspond à un changement de signe.

$$\forall \phi \in [2\pi],\ \cos(\omega t + \phi + \pi) = -\cos(\omega t + \phi) \tag{122}$$

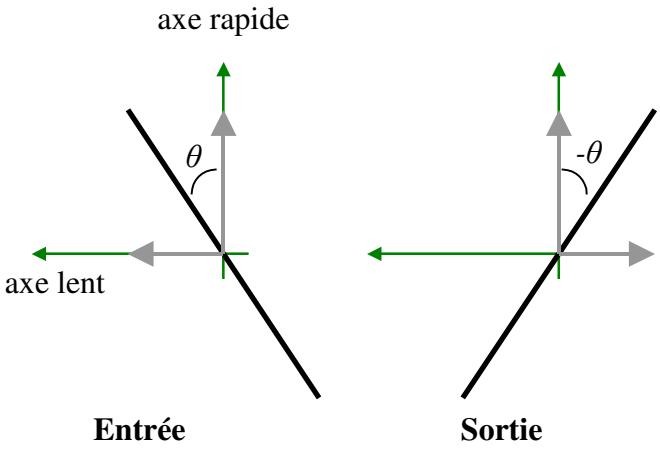



Figure 46 Elément $\lambda/2$.

## 4.5 Modulateur acousto-optique

Le modulateur acousto-optique est utilisé pour décaler la fréquence de l'onde *signal* par rapport à une onde dite de *référence*. Il permet la réalisation d'une détection de type hétérodyne.

### 4.5.1 Effets acousto-optiques

Sous l'effet d'une contrainte mécanique, un cristal subit des déformations caractérisées par un déplacement d'atomes. Ces déformations induisent des variations de la densité locale de matière qui sont à l'origine de variation de la valeur locale de l'indice de réfraction.

Dans le cas d'un modulateur acousto-optique, la contrainte mécanique correspond à la propagation d'une onde élastique résultante de l'émission d'une onde électromagnétique dans un milieu piézo-électrique.

La propagation d'une onde élastique sinusoïdale dans le cristal crée un réseau périodique de valeurs locales d'indice de réfraction. En fonction de l'angle d'incidence d'une onde optique sur ce réseau, l'un des deux effets apparaît.

L'effet Raman-Nath apparaît sous incidence quasi-normale du faisceau lumineux et pour de faibles longueurs d'interaction, notée L sur la Figure 47.

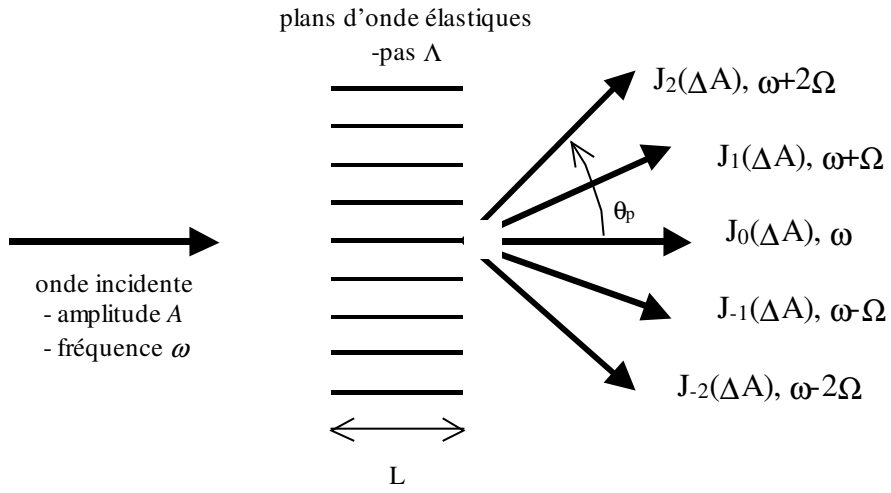



Figure 47 Effet Raman-Nath.

A la sortie du cristal, le faisceau diffracté d'ordre p fait un angle $\theta_p$ avec le faisceau lumineux incident. Cet angle est tel que

$$\sin\left(\theta_p\right) = p\frac{\lambda_0}{\Lambda} \tag{123}$$

avec $\Lambda$ pas du réseau.

Son amplitude est notée $J_p(\Delta A)$ et sa fréquence, $\omega + p\Omega$, multiple de la fréquence de l'onde élastique.

L'effet Bragg apparaît lorsque $L >> \frac{\Lambda^2}{4\lambda}$ et lorsque l'angle d'incidence $\theta_0$ du faisceau incident suit la condition de Bragg :

$$\sin\left(\theta_0\right) = \frac{\lambda_0}{2\Lambda} \tag{124}$$

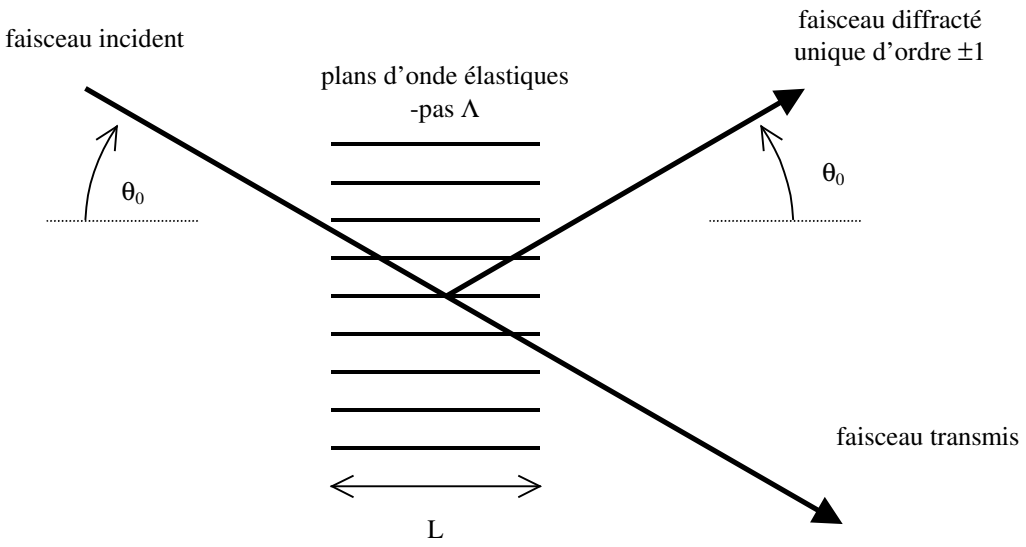



Figure 48 Effet Bragg.

### 4.5.2 Description du modulateur acousto-optique

Le modulateur acousto-optique utilisé est fabriqué par *Brimrose* et est référencé *AMF-100-1550-3FP*. Il est commandé par un générateur de signal qui délivre une onde électrique de fréquence Ω = 100 MHz. Il est référencé *FFF-100-A-FO.29-E*.

Ce modulateur a été conçu pour que le faisceau d'entrée soit diffracté sous l'effet de Bragg, et que chaque faisceau de sortie soit guidé dans une fibre optique. Par conséquent, ce modulateur ne fonctionne qu'à une unique fréquence ; 100 MHz. Le rayon diffracté est d'ordre +1.

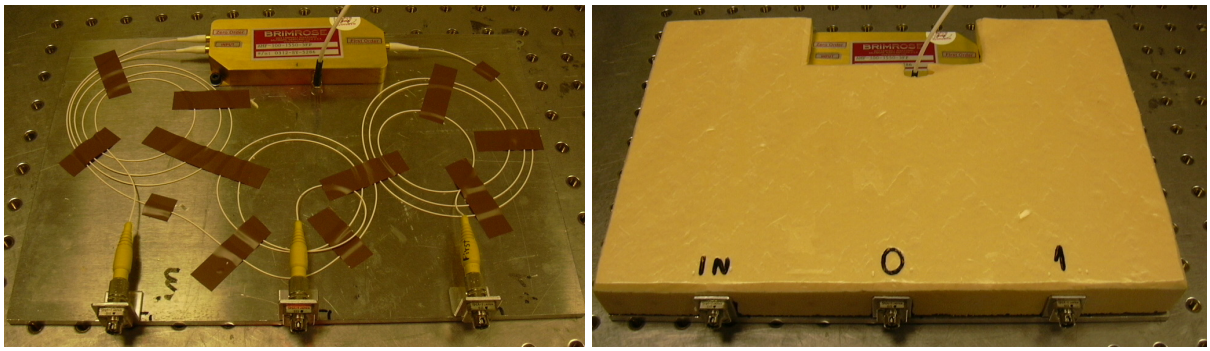



Figure 49 Modulateur AO et sa protection.

Les fibres d'entrée et de sortie ont un cœur de 9 µm et une gaine de 125 µm. Ce type de fibre est très sensible aux vibrations mécaniques et thermiques, surtout si un contrôle de la

phase est nécessaire. Il a été nécessaire de les isoler en encapsulant les fibres dans une couche d'isolant thermique.

### 4.5.3 Caractéristiques du modulateur acousto-optique

Le générateur de signaux commandant le modulateur présente les caractéristiques résumées dans le Tableau 10.

| | |
|---|---|
| Fréquence | 100.0017 MHz |
| Puissance en sortie | 24.5 dBm |

Tableau 10 Caractéristique du driver du MAO

La Figure 50 présente les harmoniques du signal de commande. La raie fondamentale est centrée à 100 MHz. La différence de puissance entre la raie fondamentale et le second ordre est de l'ordre de 44 dB.

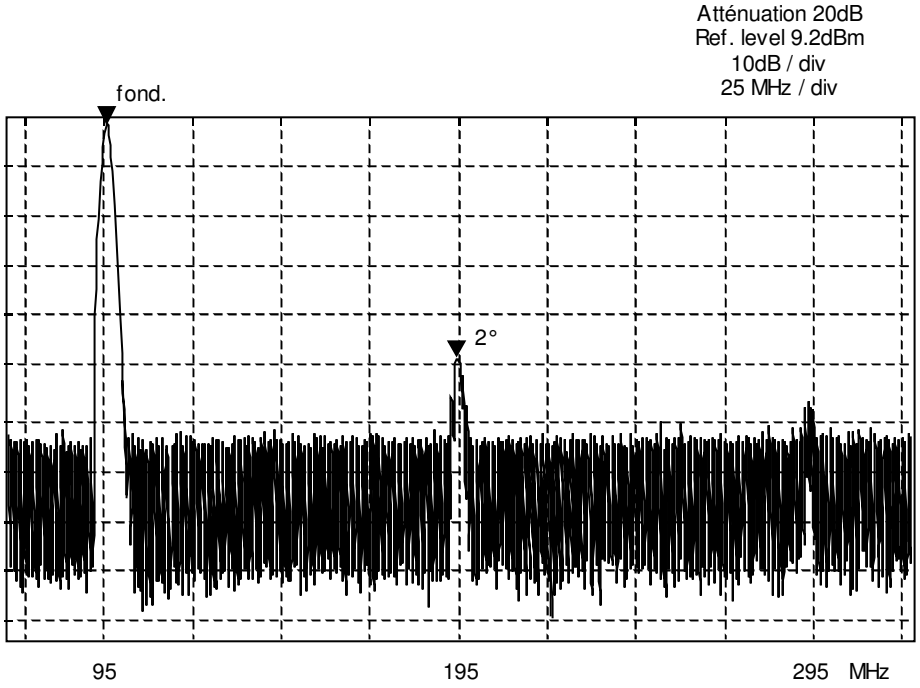



Figure 50 Spectre du MAO.

Le modulateur acousto-optique ne fonctionne que pour des longueurs d'onde comprises dans la fenêtre 1540 et 1560 nm. A une longueur d'onde de 1543 nm, les pertes d'insertion sont présentées dans le Tableau 11.

| | |
|---|---|
| ordre 0 | 2 dB |
| ordre 1 | 3.2 dB |

Tableau 11 Pertes d'insertion du MAO.

## 4.6 Les photodétecteurs

Trois types de détecteurs optiques ont été utilisés lors de l'implémentation du protocole de distribution quantique de clef. Le premier est une simple photodiode fibrée, le second est un détecteur optique intégrant un amplificateur électrique, et le troisième est un système muni d'une photodiode à avalanche permettant le comptage de photon.

### 4.6.1 Rôle d'une photodiode

Il existe de nombreuses photodiodes ayant des structures et des fonctionnements différents décrits dans de nombreux ouvrages techniques. Mais toutes répondent à cette définition ; une photodiode capte un signal optique et le traduit en un signal électrique.

Généralement, lorsqu'une photodiode est éclairée, le courant électrique généré est proportionnel à la puissance du signal reçu.

$$I = R.P \tag{125}$$

avec $I$ l'intensité du photocourant en Ampère, $P$ la puissance du signal en Watt et $R$ l'efficacité de la conversion en A/W.

Lorsque plusieurs ondes planes arrivent simultanément, il est préférable d'utiliser l'expression du champ électromagnétique décrivant chaque signal incident.

$$I(t) = R.\left|\sum_k \vec{E}_k.\exp j\left(\omega_k t + \phi_k\right)\right|^2 \tag{126}$$

où $\omega_k$ la fréquence optique du signal $k$, $\phi_k$ la phase du signal $k$ et $E_k$ l'amplitude du champ.

Physiquement, le paramètre $R$ en *A/W* représente l'efficacité de conversion des photons, ie de l'énergie, en paires d'électron-trou, ie en courant. Mais expérimentalement, il caractérise l'efficacité réelle de la photodiode en intégrant les pertes par réflexion sur la zone active du détecteur, l'absorption dans la fibre amorce, etc.

Il convient alors de définir et de caractériser les trois photodétecteurs utilisés dans l'implémentation du protocole BB84.

### 4.6.2 Photodiode PIN fibrée

Le premier photodétecteur est composé d'une photodiode PIN en InGaAs fabriquée par *PD-LD*, référencée *PDIND0555FAA-0-0-01*.

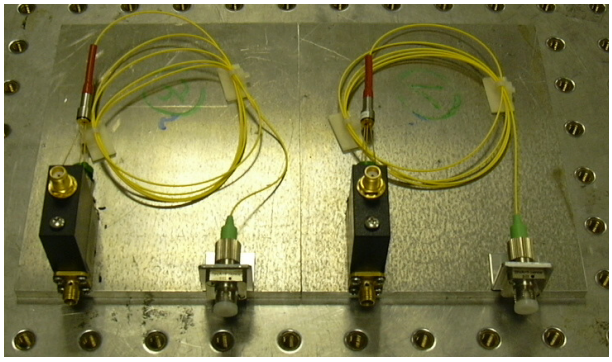


Figure 51 Photodiodes PIN fibrées.

Elle est reliée à une fibre optique standard monomode via un dispositif de couplage constitué d'une lentille boule. Lorsque la longueur d'onde est de 1550 nm, la photodiode présente une efficacité quantique théorique supérieure à 85%, or il apparaît que le dispositif de couplage dégrade fortement l'efficacité. Les Figure 54 présentent les mesures de l'efficacité des deux photodiodes utilisées, proches de 70%. La bande passante de ces photodiodes est de 3 GHz.

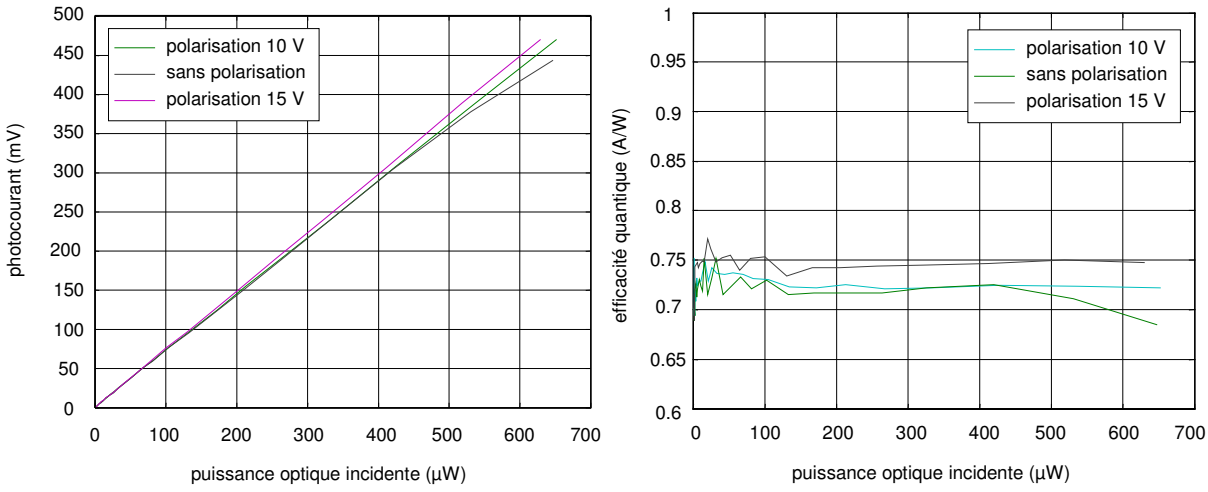



Figure 52 Caractéristiques de la photodiode 1.

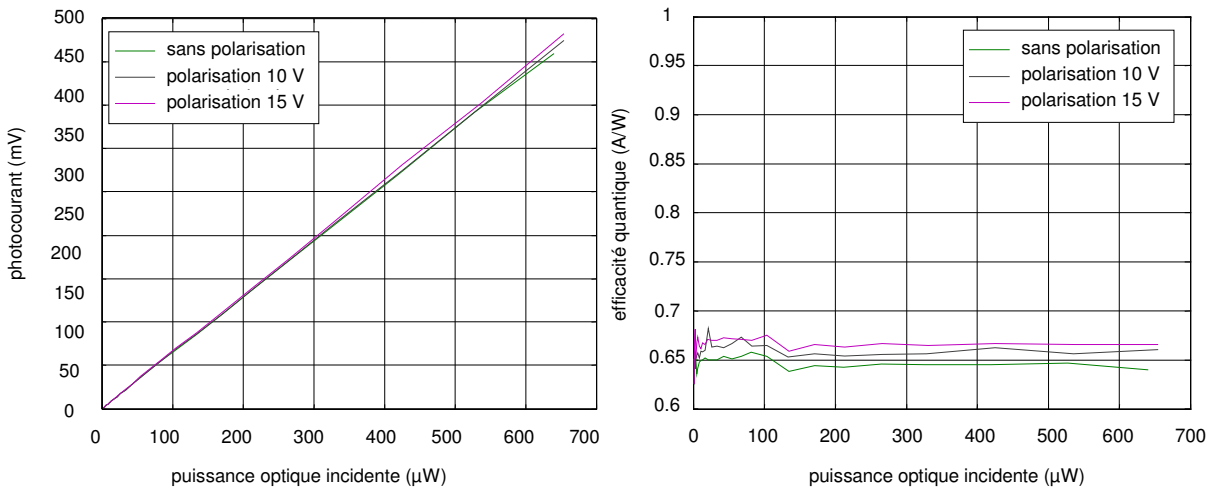



Figure 53 Caractéristiques de la photodiode 2.

Les courants de sortie de chaque détecteur sont amplifiés par deux amplificateurs électriques à faible bruit (facteur de bruit 1,6 dB) *MITEQ* de gain 40 dB et opérant sur une bande de fréquence de 1 MHz à 100 MHz. Ils sont alimentés en parallèle.

### 4.6.3 Détecteurs *New Focus*

#### 4.6.3.1 Description

Ces détecteurs fabriqués par *New Focus* et référencés *Model 1811*, intègrent une photodiode PIN en InGaAs et un système amplificateur de type transimpédance à faible bruit. Ils permettent de récupérer les composantes alternatives et continues des photocourants après amplification, sur deux sorties distinctes d'impédance 50 Ω.

Le gain transimpédance de la composante alternative est supérieur à 40 V/mA, celui de la sortie continue est supérieur à 1 V/mA (caractéristiques fournies par le constructeur). Ces détecteurs présentent une bande passante de 125 MHz.

Ils sont alimentés en parallèle par deux sources de tension –15 V et +15 V.

#### 4.6.3.2 Caractéristiques

Les deux détecteurs présentent une efficacité quantique minimale de 95% à la longueur d'onde de 1550 nm. Il est impossible de mesurer directement leurs efficacités respectives, puisqu'elles intègrent des amplificateurs électriques. Expérimentalement, le produit gain efficacité est égal à 1,19 A/W pour le premier photodétecteur et 1,21 A/W pour le second. La Figure 54 présente la réponse de chaque détecteur en fonction de la puissance optique incidente.

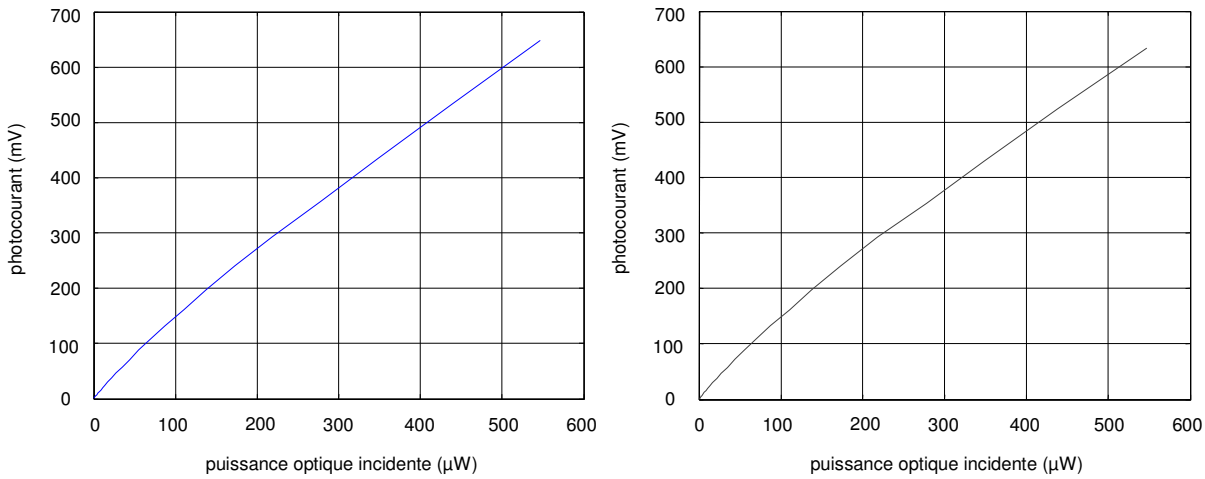



Figure 54 Réponse des deux photodétecteurs
*New Focus*.

### 4.6.4 Compteur de photon

Dans un système de distribution quantique de clef, les compteurs de photons utilisent des photodiodes à avalanche fonctionnant en mode compteur.

#### 4.6.4.1 Photodiode à avalanche

La détection d'un unique photon n'est pas possible en utilisant une simple photodiode PIN, puisque la puissance du signal détecté est très inférieure aux bruits intrinsèques d'une photodiode (bruit quantique, bruit thermique,…).

Cependant dans la zone désertée d'une structure PIN fortement polarisée en inverse, une amplification interne du photocourant peut être obtenue sous l'effet de multiplication par ionisation par chocs.

En effet, sous l'action d'un champ électrique suffisamment élevé, un porteur peut atteindre le seuil d'ionisation du matériau, et créer par collision avec un atome du réseau une paire électron-trou secondaire. Les porteurs ainsi créés peuvent à leur tour participer au processus de création de porteurs : c'est l'effet avalanche. Les valeurs du gain d'avalanche, du temps de réponse et du bruit associé à l'effet d'avalanche dépendent du matériau et des conditions d'utilisation.

Les photodiodes à avalanche peuvent détecter des puissances optiques très faibles, et sont donc utilisées dans la détection de photon unique. Celles à base de silicium présentent de bonnes caractéristiques – faible *dark count* et efficacité quantique supérieure à 50% - mais elles sont limitées aux longueurs d'onde inférieures à 1 µm. Pour les longueurs d'onde *télécom* (1,3 et 1,55 µm), les photodiodes à avalanche sont à base de semi-conducteur ayant une énergie de *gap* plus petite. Elles ont par conséquent des caractéristiques plus faibles et nécessitent des conditions d'utilisation plus contraignantes.

Les photodiodes à avalanche utilisées dans les systèmes de distribution quantique de clef par codage de photon unique fonctionne en mode compteur.

#### 4.6.4.2 Mode compteur

Afin de détecter un photon incident, le système de détection intègre une photodiode à avalanche fortement refroidie. L'incidence d'un photon sur la photodiode à avalanche produit dans celle-ci un phénomène d'avalanche créant ainsi un courant macroscopique facilement détectable.

Pour limiter les déclenchements accidentels de l'avalanche d'électrons dans la photodiode (*dark count*), la photodiode n'est armée que pendant une courte durée, appelée fenêtre active, pendant laquelle la photodiode est susceptible d'être éclairée par un photon. Armer la photodiode consiste à porter sa tension de polarisation légèrement en dessous de la tension seuil d'avalanche. Pour relaxer la photodiode en dehors de fenêtres actives et ainsi éviter un déclenchement accidentel, sa tension de polarisation est abaissée de manière à s'éloigner de la tension seuil d'avalanche.

Outre le *dark count*, un effet indésirable apparaît lors de l'utilisation de la photodiode à avalanche ; c'est l'*afterpulsing*. Ce sont des impulsions qui apparaissent lorsque la diode s'arme alors qu'elle n'a pas eu le temps de vider son matériau de tous les porteurs, créant une avalanche. Il est possible de rendre cet effet négligeable pour peu que la photodiode ait suffisamment de temps pour évacuer les électrons. La fréquence de détection et, par conséquent, le débit d'échange de clef sont donc limités.

#### 4.6.4.3 Description des compteurs de photon unique

Les compteurs de photon unique ont été fabriqués par *Id Quantique* et sont référencés *id-200 Single-Photon Detector Module*. Ils fonctionnent à la longueur d'onde de 1550 nm.

Le cœur de ces systèmes est constitué d'une photodiode à avalanche en InGaAs. Sa température de fonctionnement est stabilisée automatiquement à –50°C afin d'optimiser les performances du système.

Ils intègrent également des circuits électroniques autorisant les paramétrages:

- de la durée d'ouverture de la photodiode (2,5 ns, 5 ns, 20 ns, 50 ns, 100 ns),
- de la fréquence d'ouverture de la photodiode,
- du temps de réarmement de la photodiode (0,1 µs, 2 µs, 5 µs, 10 µs),
- de compensation du retard entre l'horloge et le signal détecté (0-25 ns).

#### 4.6.4.4 Caractéristiques

Lorsqu'une photodiode à avalanche est utilisée en mode compteur de photon, celle-ci déclenche une avalanche d'électron à l'arrivée d'un photon, avec une probabilité de déclenchement proportionnelle à son efficacité quantique. Cependant, il arrive parfois que le phénomène d'avalanche se déclenche spontanément, induisant une erreur dans le système de détection. Il est possible de quantifier cet effet parasite, nommé *dark count*. Le Tableau 12 présente les probabilités mesurées de *dark count* pour chaque détecteur. Ces mesures ont été effectuées sans *deadtime* et avec un signal de synchronisation normé TTL (signal créneaux d'amplitude 5 V et de fréquence 1 MHz). Les caractéristiques données par le constructeur ont été obtenues à une fréquence de mesure de 10 kHz et sans *deadtime*.

| Probabilité des *dark count* | | | |
|---|---|---|---|
| | Détecteur 1 | Détecteur 2 | Données constructeur |
| Durée d'ouverture = 2,5 ns | $4{,}89.10^{-5}$ | $6{,}85.\ 10^{-5}$ | $< 5.10^{-5}$ |
| Durée d'ouverture = 100 ns | 0,995 | 0,992 | $< 5.10^{-2}$ |

Tableau 12 Probabilité de *dark count* des compteurs de photon.

| Efficacité de détection à 1550 nm | |
|---|---|
| Durée d'ouverture = 2,5 ns | > 10% |

| *Timing jitter* | |
|---|---|
| Durée d'ouverture = 100 ns | < 600 ps |

Tableau 13 Caractéristiques des compteurs de photon fournies par le constructeur.

# Chapitre 5.

# Montages pour un système de distribution quantique de clef

Dans ce chapitre, nous présentons les montages expérimentaux validant l'intégration des trois sous-ensembles composant un système de distribution quantique de clef, décrits dans le Chapitre 3.

Le premier dispositif expérimental présente l'intégration de la chaîne de modulation et d'une détection hétérodyne, le second dispositif introduit la détection super-homodyne, dispositif de détection repris dans la troisième implémentation.

# 5.1 Intégration de la chaîne de modulation à deux générateurs et d'une détection hétérodyne

Ce premier dispositif expérimental a pour but de vérifier le fonctionnement de la chaîne de modulation d'Alice et de Bob.

## 5.1.1 Description de l'implémentation

Dans cette première implémentation du protocole BB84, le laser émet un signal optique continu de longueur d'onde $\lambda$=1550 nm. Son fonctionnement est d'écrit dans la section 3.1.2.

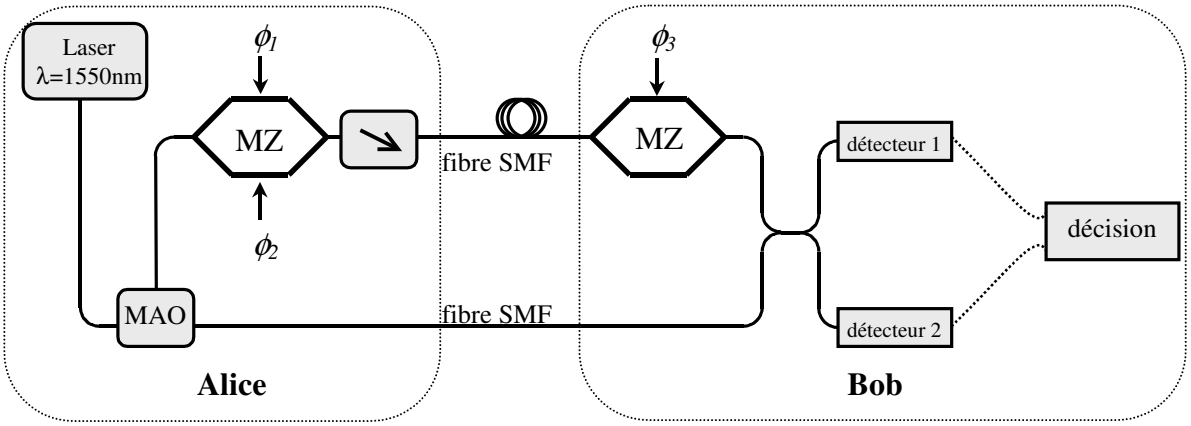



Figure 55 Synoptique du dispositif permettant une modulation QPSK en détection hétérodyne.

Le dispositif schématisé par la Figure 55 réunit la chaîne de modulation présentée dans la section 3.2.4.1. Le modulateur acousto-optique permet de diviser l'onde incidente en deux ondes ; la première servant d'onde *signal*, porteuse des informations d'Alice et de Bob, la seconde servant d'onde *référence* dont la fréquence est translatée de 100 MHz par rapport à

l'onde *signal*. Le modulateur acousto-optique permet également de diviser d'un facteur 2 environ la puissance de l'onde incidente. L'atténuateur variable placé à la sortie du modulateur d'Alice autorise un ajustement de la puissance afin d'approcher du régime quantique.

Des contrôleurs de polarisation non représentés sur la Figure 55 sont placés à l'entrée de chaque modulateur (Mach-Zehnder et acousto-optique) puisque ceux-ci sont dépendants de la polarisation de l'onde incidente.

Les canaux de transmission des ondes *référence* et *signal* correspondent à des fibres optiques standard monomode, d'une longueur de 1 mètre.

Les ondes *signal* et *référence* sont combinées par un coupleur 3 dB. A sa sortie, chaque signal est détecté par les photodiodes notés 1 et 2, correspondant aux photodétecteurs *New-Focus* présentés dans la partie 4.6.3.

Le dispositif de décision est, dans cette première implémentation, un oscilloscope *Tektronix* référencé *TDS 3044B*. La fréquence de modulation du signal électrique de commande du modulateur de Bob est de 2 MHz.

### 5.1.2 Signaux de commandes

Les choix de bases et de symboles d'Alice et de Bob sont transposés dans le domaine électrique par des générateurs de signaux, puis dans le domaine optique par les modulateurs Mach-Zehnder à doubles électrodes. Pour commander le modulateur d'Alice, deux signaux électriques sont nécessaires ; le premier reflète les choix de symbole, noté $V_{\phi 1}$, le second les choix de base, noté $V_{\phi 2}$ (Dans la section 3.2.2, il a été montré que $V_{\phi 2}$ est une combinaison de $V_{\phi 1}$ et du signal représentant le codage des choix de base d'Alice). Le signal $V_{\phi 3}$ représente les choix de base de Bob et commande son modulateur Mach-Zehnder. $V_{\phi 1}$, $V_{\phi 2}$ et $V_{\phi 3}$ sont de forme carrée et leurs niveaux en tension sont représentés sur la Figure 56.

Les signaux $V_{\phi 1}$, $V_{\phi 2}$ et $V_{\phi 3}$ représentent uniquement la composante variable de la tension de contrôle des électrodes 1 et 2 pour le modulateur d'Alice et de l'électrode 3 pour celui de Bob. En effet, il est nécessaire de polariser chaque modulateur afin d'égaliser les enveloppes des signaux optiques sortant du système d'Alice, et de s'assurer que l'encodage des choix de Bob n'affecte pas l'amplitude du signal.

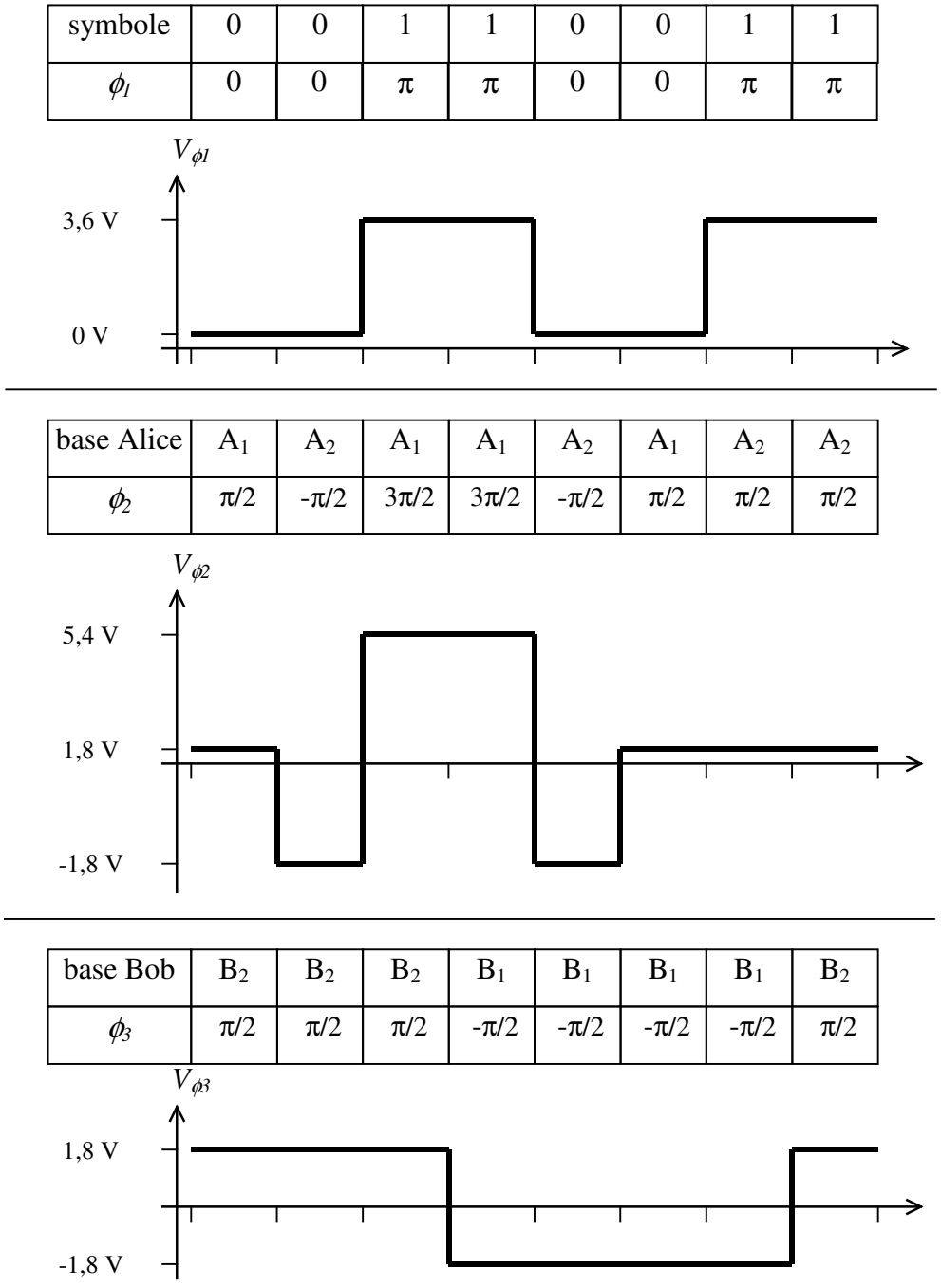



Figure 56 Chronogramme des 3 signaux de commandes dans un système utilisant une détection hétérodyne.

Les fréquences des signaux $V_{\phi 1}$ et $V_{\phi 3}$ sont respectivement de 1 et 2 MHz.

### 5.1.3 Résultats

#### 5.1.3.1 Compensation des retards électriques et optiques

La Figure 58 montre que le signal délivré par le détecteur 1 est en avance par rapport au signal du détecteur 2. Les signaux ne sont pas en opposition de phase, d'après les équations (59) et (60). Ceci s'explique par un déséquilibre des chemins optiques et électriques délimités par la sortie de la zone active du coupleur et l'entrée dans l'oscilloscope, représentés sur la Figure 59. Ce déséquilibre induit un retard évalué à 0,004 µs.

Une détection hétérodyne est dite équilibrée lorsque l'onde optique arrivant sur le détecteur 1 parcourt le même chemin que l'onde optique éclairant le détecteur 2. De même, les chemins électriques parcourus par les ondes électriques délivrées par les photodétecteurs 1 et 2 doivent être identiques.

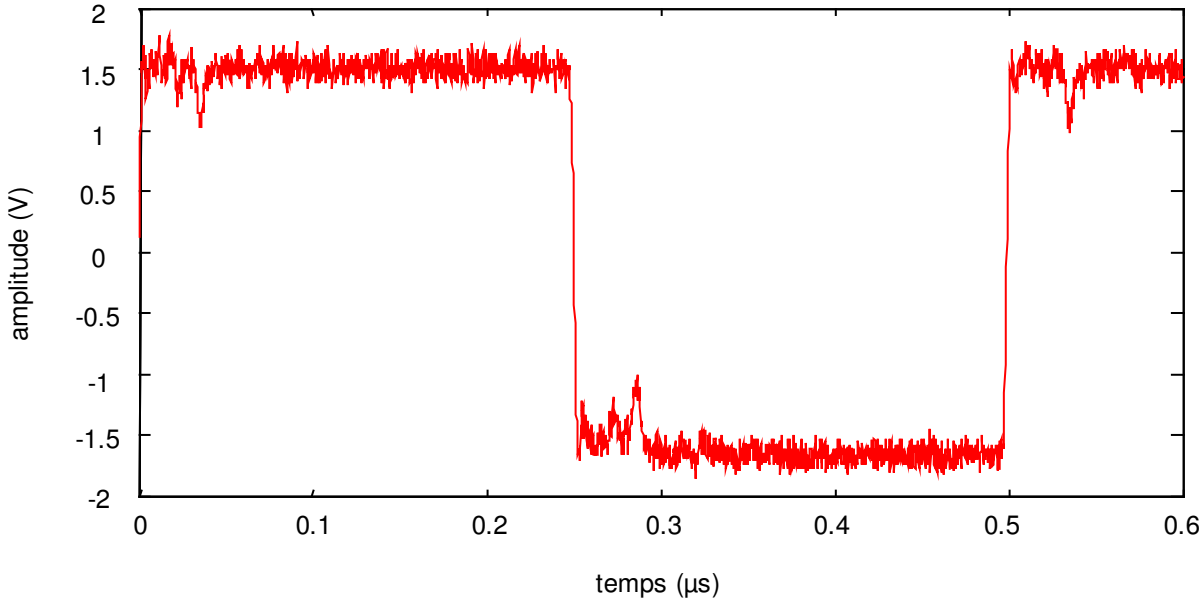



Figure 57 Mesure du signal de commande de $\phi_3$ dans une détection hétérodyne.

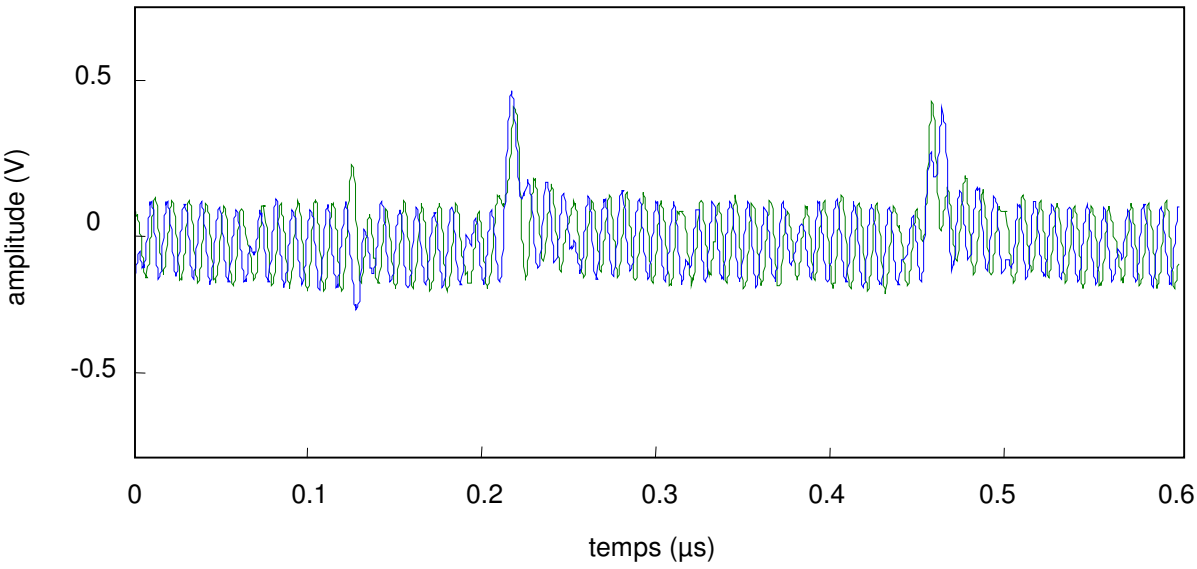



Figure 58 Mesure des photocourants délivrés par les photodétecteurs dans une détection hétérodyne.

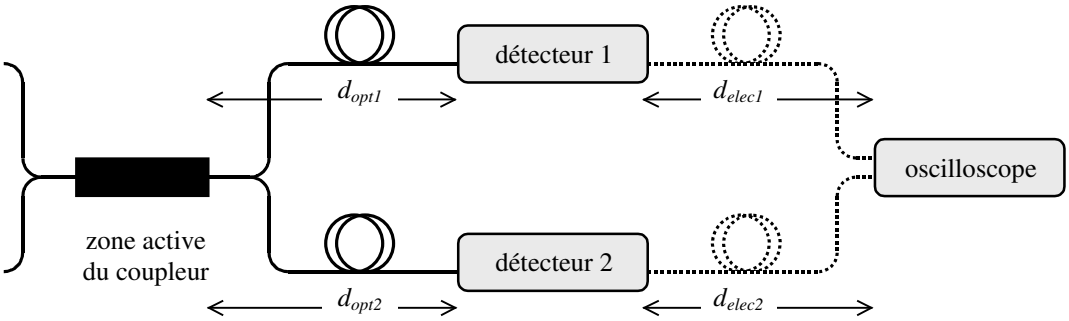



Figure 59 Représentation d'une détection équilibrée optiquement et électriquement.

Pour une détection équilibrée, les deux conditions suivantes doivent être respectées.

$$\begin{aligned} &\bullet\ d_{opt1} = d_{opt2} \\ &\bullet\ d_{elec1} = d_{elec2} \end{aligned} \qquad (127)$$

Une ligne à retard optique ajustable est placée entre le coupleur et le détecteur 2, et la longueur des câbles électriques est égalisée.

Après compensation et égalisation des retards, la Figure 60 présente les signaux délivrés par les deux photodétecteurs. Entre chaque modulation de phase, les battements de chacun d'eux sont en phase.

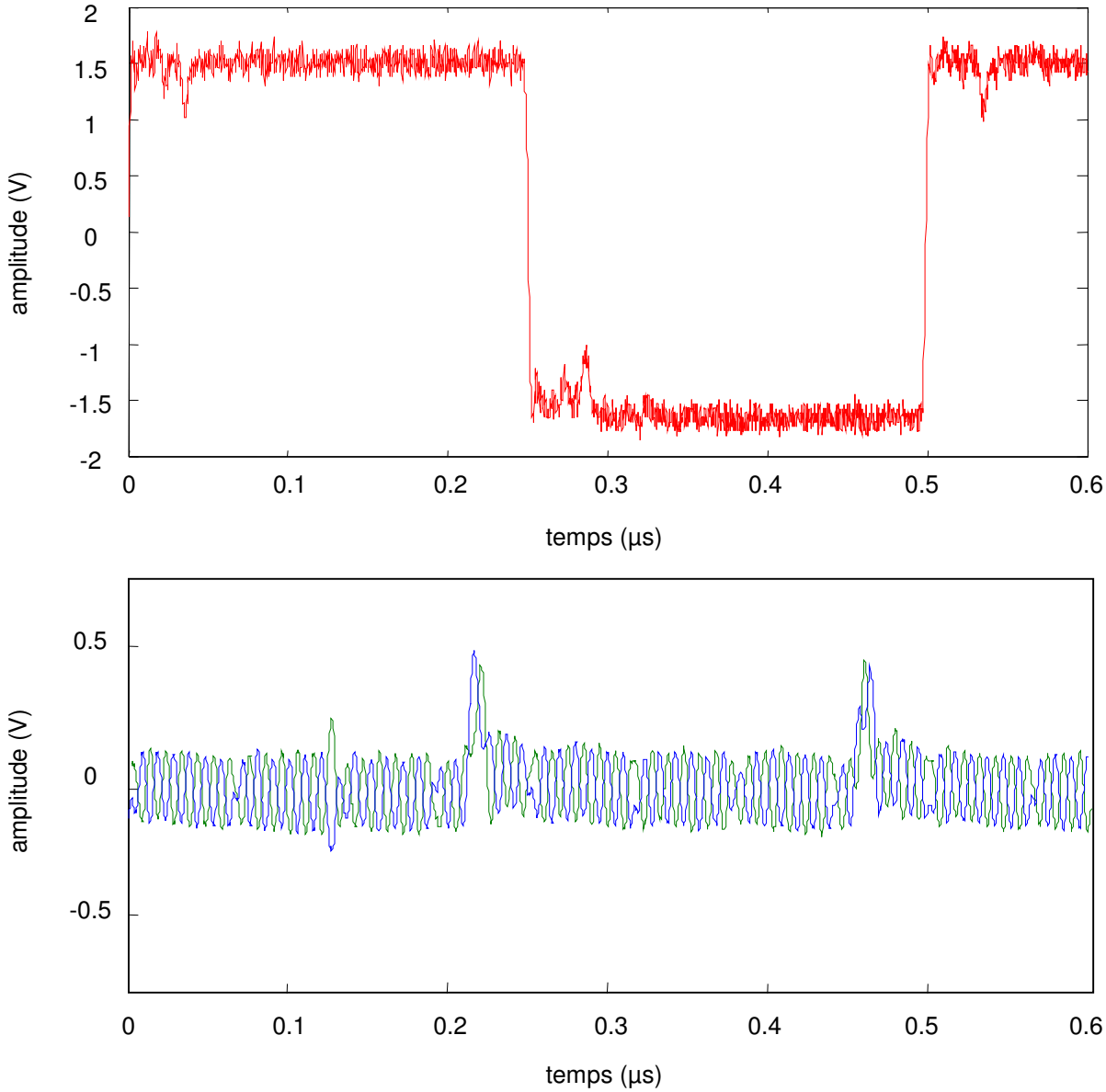



Figure 60 Mesure des photocourants et du signal de commande de $\phi_3$ après équilibre de la détection hétérodyne.

#### 5.1.3.2 Synchronisation de la chaîne de modulation et du système de détection

Les générateurs électriques des signaux de commandes des modulateurs MZ d'Alice et de Bob sont synchronisés par un même signal électrique d'horloge. Le système de décision,

dans un premier temps remplacé par un oscilloscope, utilise également ce signal d'horloge. Cependant il apparaît sur la Figure 60 un retard constant de quelques dizaines de ns entre les signaux délivrés par les photodétecteurs et le signal $V_{\phi 3}$ nécessaire pour renseigner le choix de base de Bob au système de décision. Ce retard traduit une désynchronisation entre le générateur, les photodétecteurs et l'oscilloscope composant le module de détection de Bob.

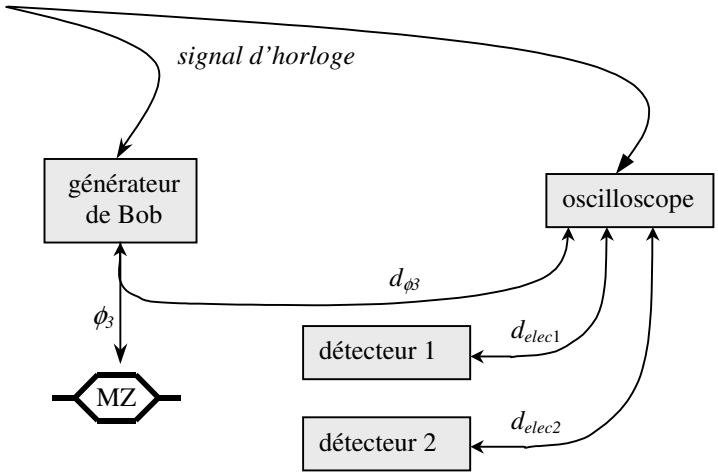



Figure 61 Branchement électrique dans le module de Bob

Il est possible de compenser ce retard en ajustant la longueur des câbles électriques reliant le générateur de Bob à l'oscilloscope de façon à respecter l'équation (128)

$$d_{elec1} = d_{elec2} = d_{\phi_3} \tag{128}$$

Pour synchroniser parfaitement les signaux $V_{\phi 1}$, $V_{\phi 2}$ et $V_{\phi 3}$ , il est également possible de retarder le signal d'horloge synchronisant chaque générateur.

La Figure 62 présente les signaux issus des deux détecteurs et du signal $V_{\phi 3}$ après compensation des retards électriques et synchronisation des composants électriques du module de Bob.

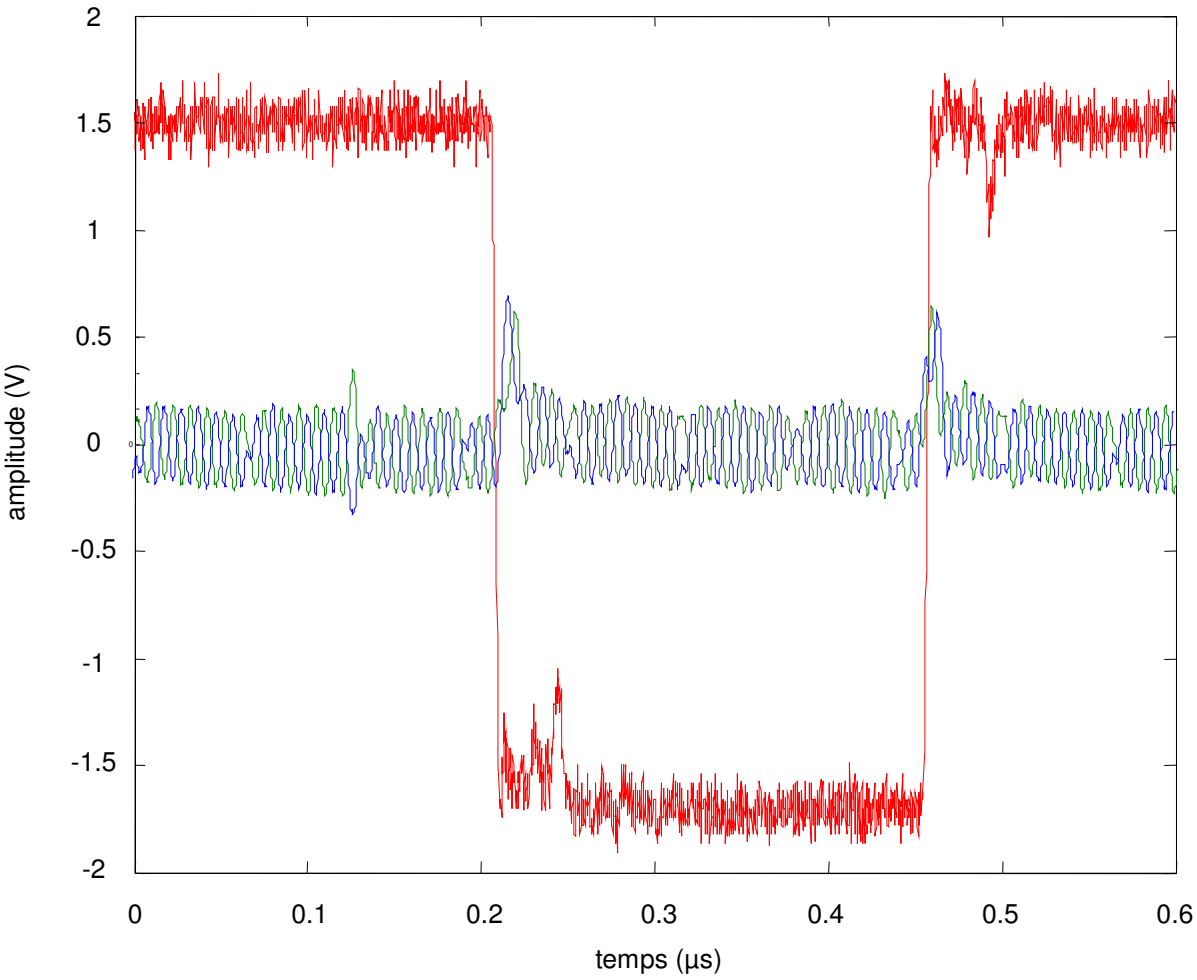



Figure 62 Mesure des photocourants et du signal $V_{\phi 3}$ après compensation des retards électriques et optiques, et synchronisation des composants électriques et optiques de Bob.

#### 5.1.3.3 Déphasages d'Alice et de Bob

Les choix d'Alice et de Bob sont dans cette phase de mise au point, déterministes et connus, et sont représentés sur le chronogramme Figure 56. Il s'agit de vérifier que les photocourants portent leurs choix.

La Figure 63 reprend uniquement les signaux des détecteurs de la Figure 62. Il est possible d'y observer les différents changements de phase correspondant aux huit combinaisons résultant des choix d'Alice et de Bob.

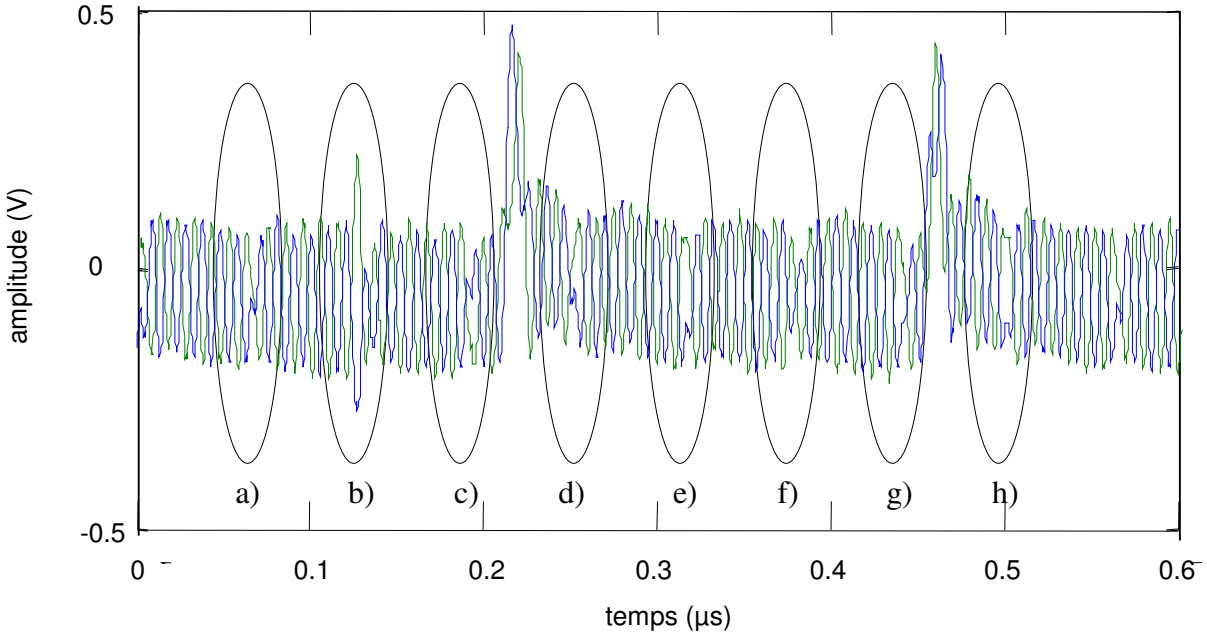



Figure 63 Visualisation des 8 déphasages

Un zoom des huit déphasages respectivement nommés a), b), … h), est présenté dans la Figure 64.

Les déphasages sont assez facilement identifiables lorsque le signal optique sortant du module d'Alice n'est pas atténué. Dès lors qu'une atténuation supérieure à 10 dB est appliquée, les déphasages correspondant à $-\frac{\pi}{2}$ et $\frac{\pi}{2}$ ne sont plus identifiables.

La principale cause résulte des générateurs électriques qui présentent des transitions entre niveaux très perturbées et déformées dès lors que la fréquence est supérieure à 1 MHz.

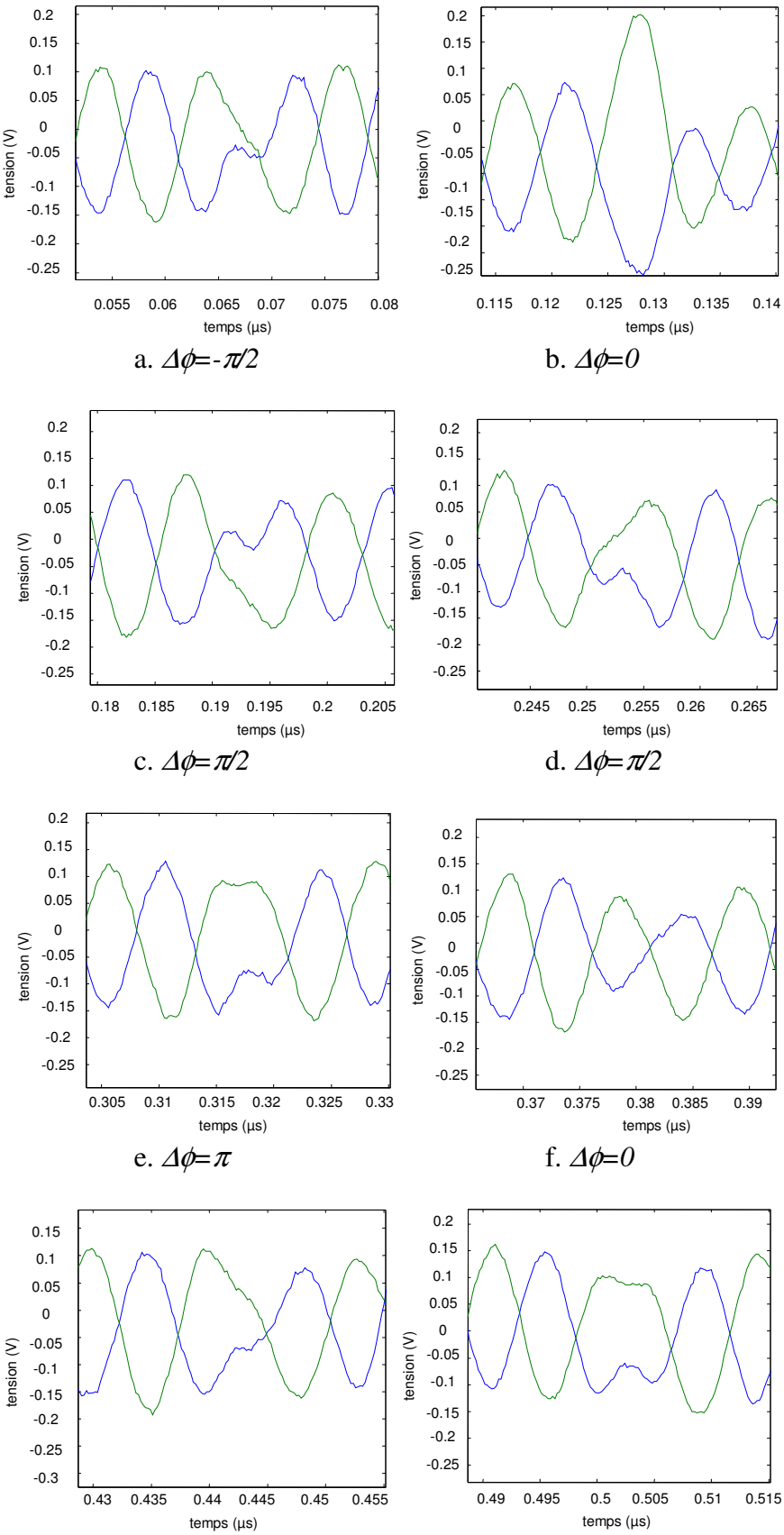



Figure 64 Mesure des 8 déphasages.

### 5.1.4 Conclusion

Dans cette première implémentation, la puissance optique des signaux émis par Alice en direction de Bob est importante, très éloignée de la puissance requise pour atteindre le régime quantique nécessaire à la sécurité du protocole BB84.

Cependant, ce premier dispositif expérimental fonctionnant en régime classique permet de valider l'intégration de la chaîne de modulation dans l'implémentation du système et autorise un ajustement très facile des tensions de polarisation du modulateur d'Alice afin d'obtenir des enveloppes de signaux constantes, quel que soit le déphasage codé par Alice [38][39].

L'équilibrage du système de détection est de plus très aisé puisqu'il suffit de superposer les signaux délivrés par chaque détecteur. Ces signaux sont sinusoïdaux, représentant le battement de l'onde *signal* et l'onde *référence* dans un système de détection hétérodyne.

Il apparaît que les perturbations des transitions entre niveaux des signaux électriques de commande des modulateurs Mach-Zehnder se répercutent sur les signaux optiques. En régime classique, il est possible de différencier chaque déphasage. Mais des lors que l'atténuation augmente, la différenciation n'est plus possible. Il est donc nécessaire d'utiliser de meilleurs générateurs de signaux pour commander les modulateurs MZ d'Alice et de Bob. Un dispositif de commande des modulateurs MZ utilisant trois générateurs de signaux électriques est proposé dans la section 3.2.4.2. Il permet de générer des signaux électriques ayant des transitions entre niveaux moins perturbées.

Un système hétérodyne présente une sensibilité théorique de détection plus faible qu'un système homodyne (-3 dB) et n'est qu'un outil de mise au point du système de modulation.

## 5.2 Intégration de la chaîne de modulation à trois générateurs et d'une détection super-homodyne

Pour améliorer la sensibilité de détection de 3 dB, une détection équilibrée homodyne est préférable à une détection hétérodyne en détection classique. Elle est indispensable pour notre application.

### 5.2.1 Description de l'implémentation

Dans ce second montage, le laser émet un signal optique continu de longueur d'onde $\lambda$=1550 nm. Son fonctionnement est décrit dans la section 3.1.2.

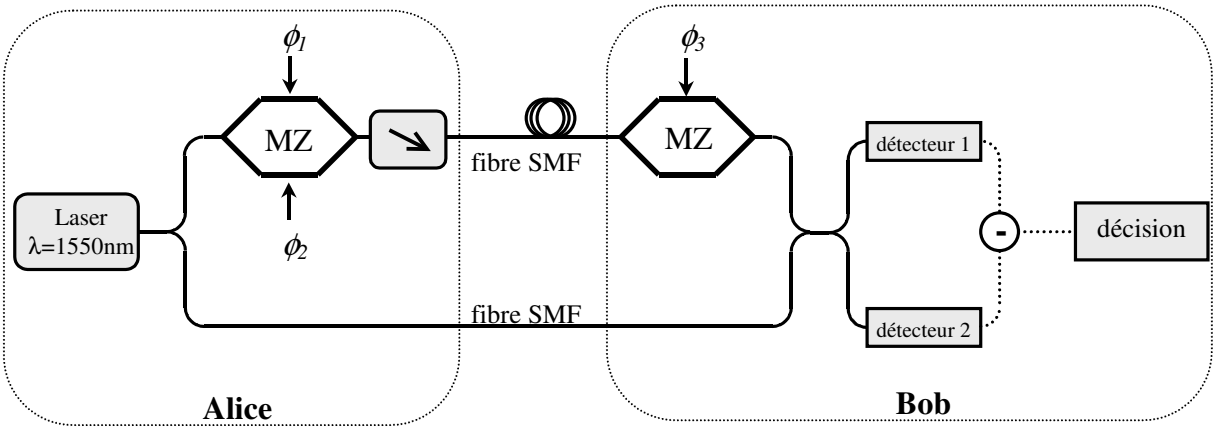



Figure 65 Synoptique de la chaîne de modulation et d'une détection homodyne.

L'onde optique délivrée par le laser est divisée par un coupleur 1x2. L'une des deux ondes de sortie sert directement de *référence* tandis que l'autre passe par la chaîne de modulation (présentée dans la section 3.2.4.2). Elle porte donc les choix d'Alice et de Bob, et sert d'onde *signal* dans la détection homodyne équilibrée.

Les photodétecteurs sont identiques à ceux du montage précédent et délivrent deux photocourants qui traversent une jonction hybride de type *Maacom H19*. Cette jonction permet de soustraire les bruits en mode commun et les composantes continues des deux photocourants.

### 5.2.2 Signaux de commandes

Les choix de symbole et de base d'Alice et de Bob sont encore ici déterministes et sont représentés par la Figure 66.

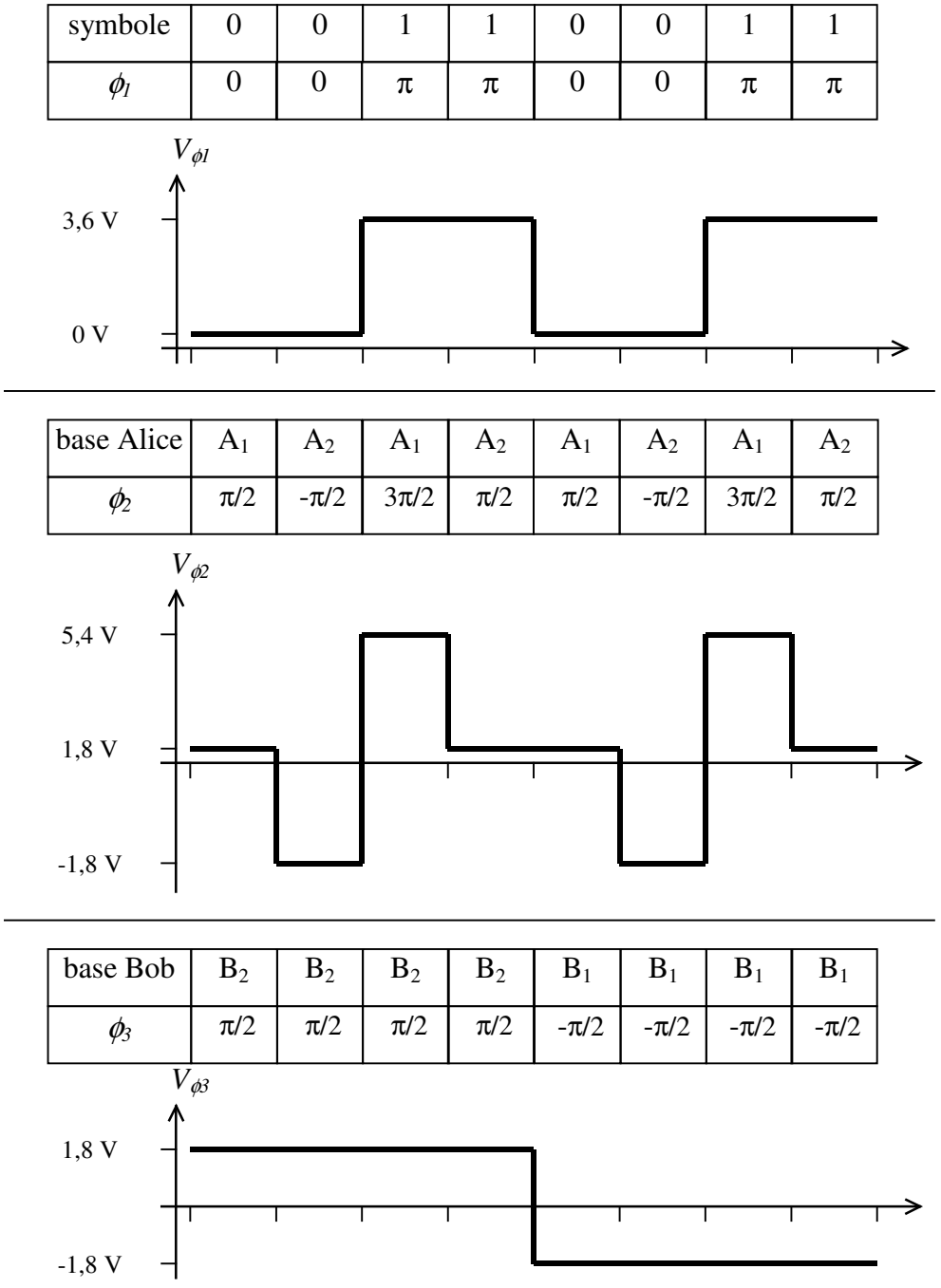



Figure 66 Chronogramme des 3 signaux de commandes dans un système utilisant une détection homodyne.

### 5.2.3 Observations des photocourants

La Figure 67 présente les deux photocourants et le signal $V_{\phi 3}$. En accord avec l'équation (66), il apparaît que les photocourants ont perdu leur caractère sinusoïdal et chaque niveau en amplitude correspond à la somme des déphasages d'Alice et de Bob.

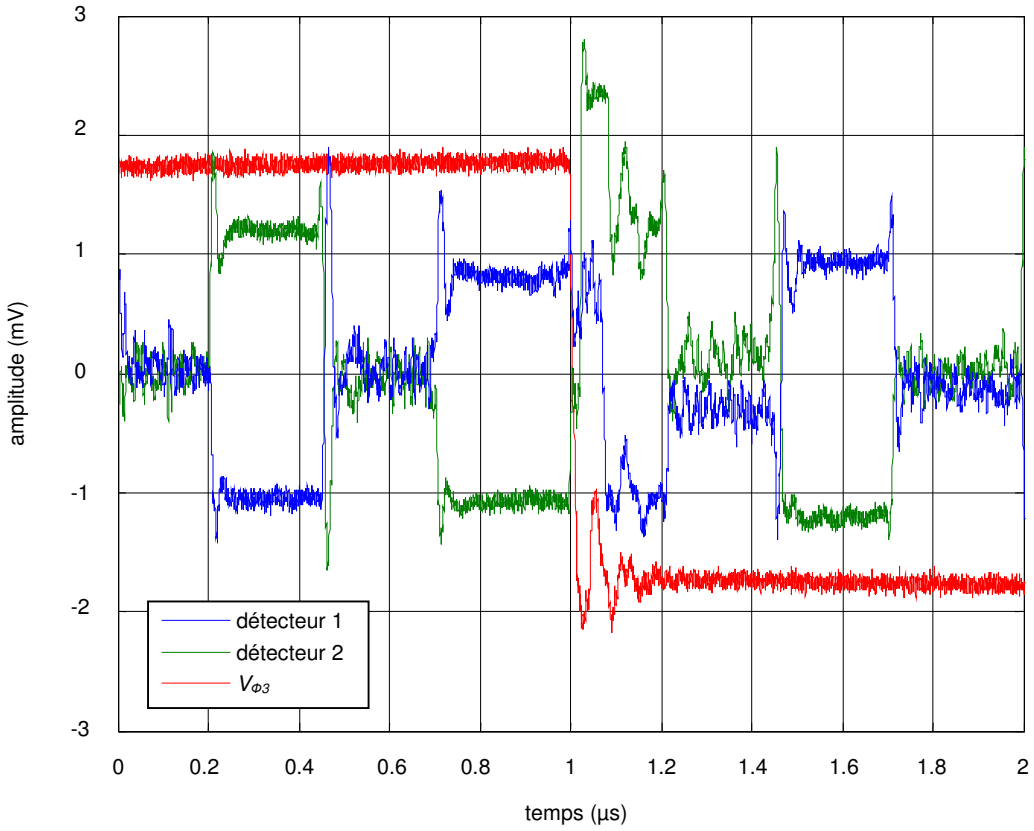



Figure 67 Mesure des photocourants et du signal $V_{\phi 3}$ dans une détection homodyne.

Bien que les puissances optiques des ondes *signal* et *référence* soient dans le domaine classique, il apparaît que les photocourants sont très perturbés, surtout dans la fenêtre [1 1,2µs] de la Figure 67. Ceci s'explique par l'accumulation des perturbations dans les transitions entre niveaux des signaux de commandes de $\phi_1$, $\phi_2$ et $\phi_3$.

Cependant le fait de réaliser une soustraction des deux photocourants permet, comme le montre la Figure 68, d'atténuer l'effet de ces parasites. En effet, le signal *I(t)* résultant de la soustraction des deux photocourants présente des niveaux en amplitude suffisamment distinguables pour identifier la somme des déphasages d'Alice et de Bob.

La mesure de *I(t)* (Figure 68) permet d'identifier les huit états de phase nécessaires au protocole BB84, notés respectivement a), b), … h). Les déphasages d) et g) correspondent au niveau 1 caractérisant une coïncidence des bases d'Alice et de Bob et codant le symbole *1*. Les déphasages b) et e) correspondent au niveau -1 caractérisant une coïncidence des bases

d'Alice et de Bob et codant le symbole *0*. Les quatre autres états correspondent à des non-coïncidences de base et ne seront, par conséquent, pas identifiables.

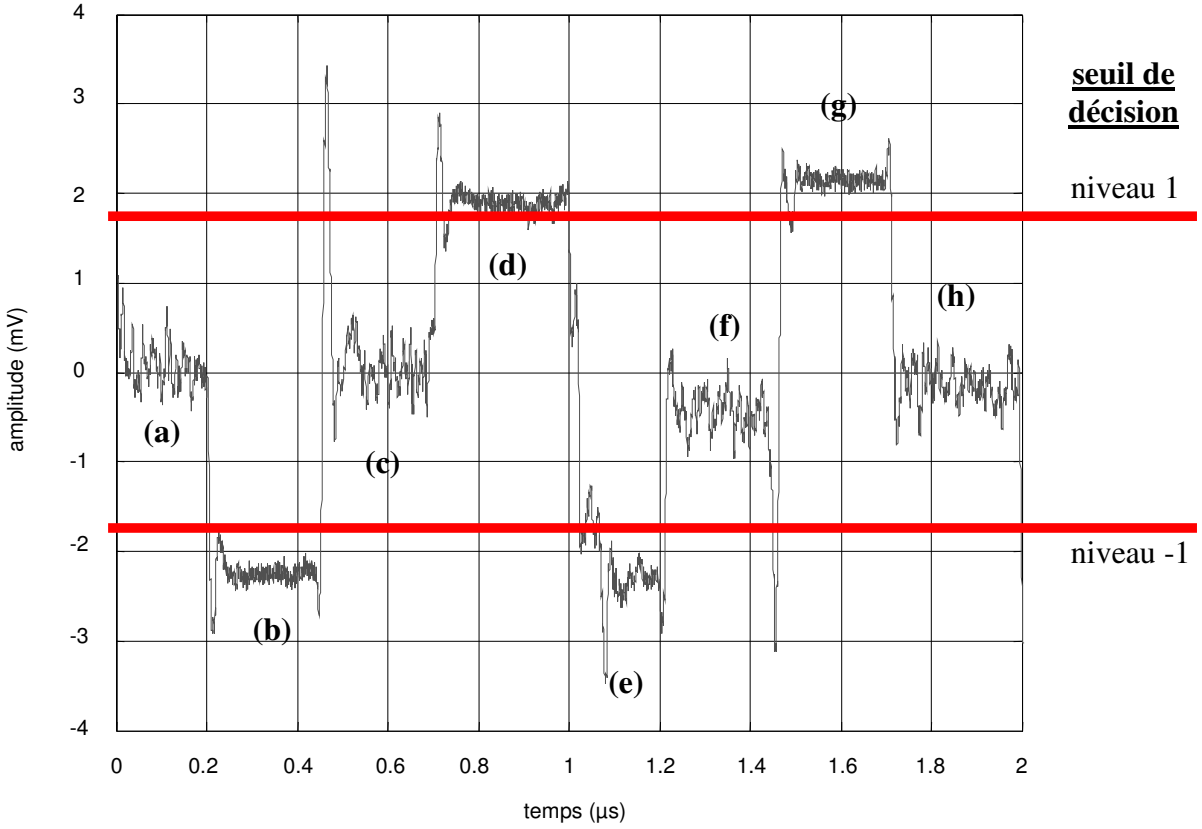



Figure 68 Mesure de *I(t)*, résultant de la soustraction des deux photocourants.

Le Tableau 14 présente les déphasages d'Alice ($\phi_{Alice}$), de Bob ($\phi_{Bob}$) représentant leurs choix respectifs de base et de symbole. Les déphasages $\phi_{Alice}+\phi_{Bob}$ caractérisent la somme de leurs deux déphasages. Les déphasages attendus correspondent bien aux états observés.

Lorsqu'il y a coïncidence des bases d'Alice et de Bob, les déphasages sont parfaitement identifiables (états b, d, e, g). Alors que dans le cas d'anti-coïncidence des bases, le photocourant résultant ne permet pas d'identifier le déphasage (états a, c, f, h).

| $\phi_{Alice}$ | π/4 | -π/4 | 5π/4 | 3π/4 | π/4 | -π/4 | 5π/4 | 3π/4 |
|---|---|---|---|---|---|---|---|---|
| $\phi_{Bob}$ | π/4 | π/4 | π/4 | π/4 | -π/4 | -π/4 | -π/4 | -π/4 |
| $\phi_{Alice} + \phi_{Bob} + cst$ | 0 | -π/2 | π | π/2 | -π/2 | π | π/2 | 0 |
| état observé | (a) | (b) | (c) | (d) | (e) | (f) | (g) | (h) |

Tableau 14 Déphasages attendus et observés dans un système utilisant une détection homodyne.

### 5.2.4 Conclusion

L'implémentation proposée dans cette section 5.2 a permis de mettre en évidence la plus grande sensibilité attendue d'une détection homodyne par rapport à une détection hétérodyne. De plus la prise de décision après une détection homodyne est plus aisée, puisque les déphasages se traduisent par une variation d'amplitude et non plus par des déphasages entre les photocourants [40][41].

Cependant si la puissance de l'onde signal était très faible, ce montage génèrerait des erreurs puisque la mesure de *I(t)* présente des pics parasites dont l'amplitude dépasse les seuils de décision. Par exemple, la Figure 68 présente un pic entre les états b et c dont l'amplitude est supérieure à 3 V. Le seuil de décision du niveau 1 étant de 1,8 V, ce pic parasite aurait déclenché la détection d'un symbole correspondant au niveau 1.

Pour remédier à ce problème, il suffit d'effectuer une détection par fenêtre temporelle et non plus une détection continue. Les fenêtres de détection sont alors placées de façon à éviter les transitions entre les niveaux.

## 5.3 Intégration de la chaîne de modulation à deux générateurs programmables et d'une détection super-homodyne

Les chaînes de modulation présentées dans la section 3.2 et utilisées dans les précédentes implémentations généraient des parasites lors des changements de phase introduits par Alice et Bob. La génération des signaux électriques commandant les modulateurs MZ à doubles électrodes d'Alice et de Bob est désormais assurée par deux générateurs programmables de signaux électriques.

### 5.3.1 Signaux de commandes

La chaîne de modulation décrite en section 3.2.4.2 a été simplifiée par deux générateurs programmables de signaux électriques *Tektronix* référencés *AFG 3252*. Ils délivrent directement les signaux de commandes de $\phi_1$, $\phi_2$ (Figure 69) et de $\phi_3$ (Figure 70).

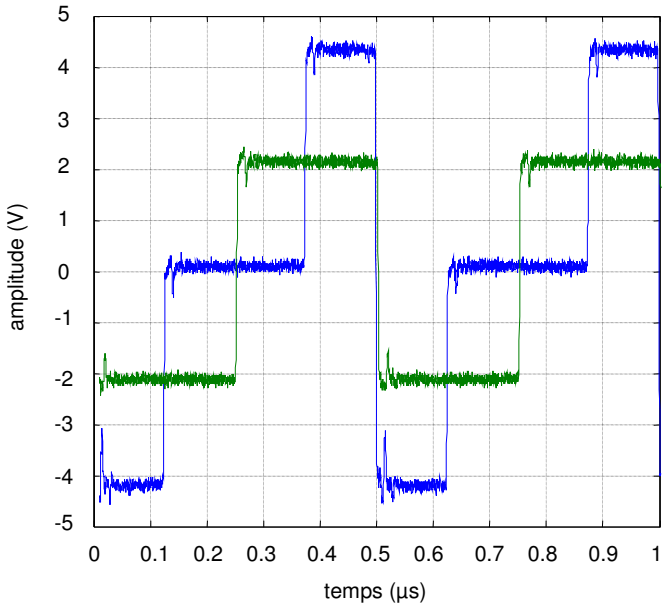



Figure 69 Mesure des signaux $V_{\phi 1}$ et $V_{\phi 2}$ commandant le modulateur d'Alice.

L'utilisation de ces générateurs programmables permet de s'affranchir des pics de transitions entre les niveaux des signaux $V_{\phi 1}$, $V_{\phi 2}$ et $V_{\phi 3}$ présents lors de l'utilisation de la chaîne de modulation à trois générateurs présentée dans la section 3.2.4.2.

Les signaux $V_{\phi 1}$, $V_{\phi 2}$ et $V_{\phi 3}$ présentés dans les Figure 69 et Figure 70 codent les choix d'Alice et de Bob représentés dans le Tableau 15.

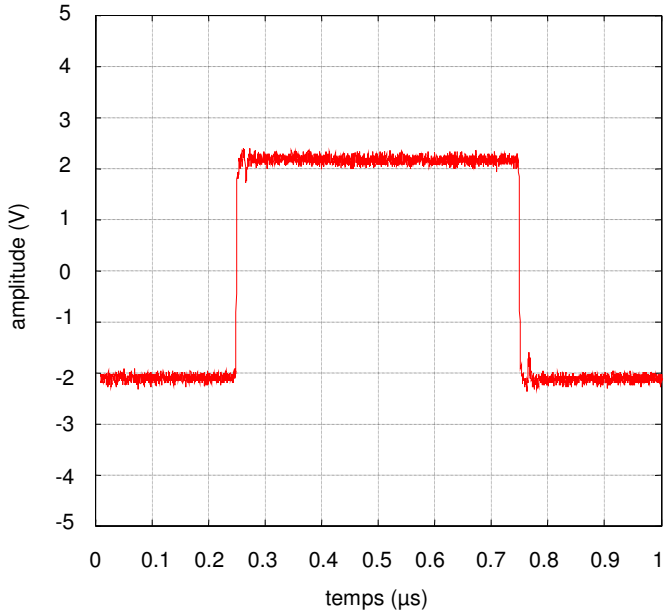



Figure 70 Mesure des signaux $V_{\phi 3}$ commandant le modulateur de Bob.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ***ALICE*** | *Base* | $A_2$ | $A_1$ | $A_2$ | $A_1$ | $A_2$ | $A_1$ | $A_2$ | $A_1$ |
| | *Symbole* | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| | $\phi_1$ | 0 | 0 | $\pi$ | $\pi$ | 0 | 0 | $\pi$ | $\pi$ |
| | $\phi_2$ | $-\pi/2$ | $\pi/2$ | $\pi/2$ | $3\pi/2$ | $-\pi/2$ | $\pi/2$ | $\pi/2$ | $3\pi/2$ |
| ***BOB*** | *Base* | $B_2$ | $B_2$ | $B_1$ | $B_1$ | $B_1$ | $B_1$ | $B_2$ | $B_2$ |
| | $\phi_3$ | $-\pi/2$ | $-\pi/2$ | $\pi/2$ | $\pi/2$ | $\pi/2$ | $\pi/2$ | $-\pi/2$ | $-\pi/2$ |

Tableau 15 Correspondance entre les choix d'Alice et de Bob, et les signaux de commande de leurs modulateurs MZ.

### 5.3.2 Observations

La Figure 71 présente la soustraction des deux photocourants en l'absence d'atténuation optique. Dans ce cas et en plaçant les seuils de décision à 1,9 V pour le niveau 1 et -1,9 V pour le niveau –1, il est aisé d'identifier les états correspondants aux coïncidences de bases

entre Alice et Bob. Par déduction, les états représentés par des amplitudes de tension comprises ]-1,9V 1,9V[ correspondent aux non-coïncidences de bases.

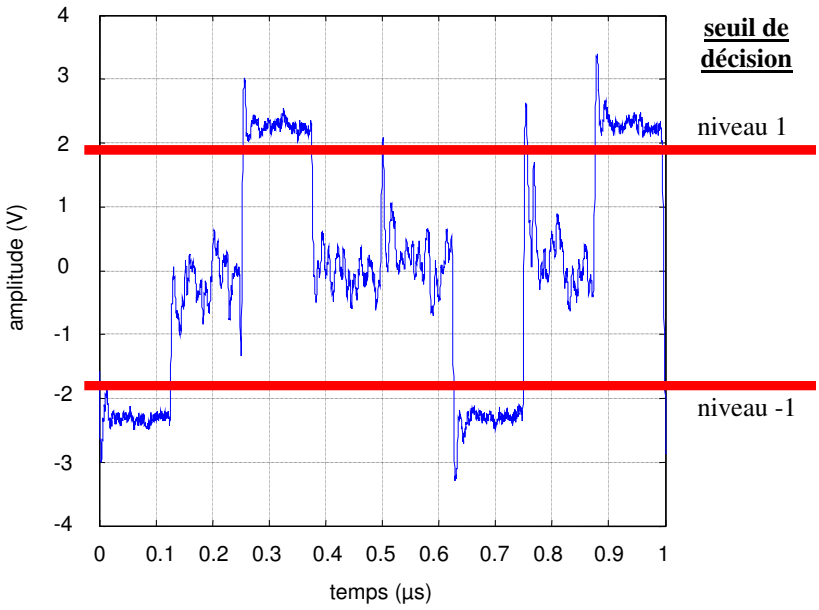



Figure 71 Mesure de *I(t)* sans atténuation.

### 5.3.2.1 Rôle des générateurs programmables

L'utilisation de deux générateurs programmables de signaux électriques à la place de la chaîne de modulation à trois générateurs (présentée dans la section 3.2.4.2) permet de supprimer la majeure partie des perturbations électriques. En effet, d'après la Figure 71, seule la perturbation apparaissant à 0,75 µs aurait introduit une erreur, alors que dans le précédent dispositif expérimental (section 5.2), plusieurs perturbations auraient été synonymes d'erreurs.

D'autre part, l'emploi des générateurs programmables a permis d'obtenir des amplitudes constantes pour les niveaux correspondants aux coïncidences de bases, ce qui n'était pas le cas dans le précédent montage (section 5.2).

### 5.3.2.2 Atténuation

Après mise au point à un niveau d'impulsion classique, il est possible de se rapprocher du domaine quantique en diminuant le nombre de photons par bit. D'après l'équation (45) de la section 3.1, il suffit d'augmenter le coefficient d'atténuation par l'intermédiaire d'atténuateurs optiques placés dans le modulateur d'Alice (Figure 65).

La Figure 72 présente la soustraction des photocourants lorsque l'atténuation atteint 40 dB. Les états correspondants aux coïncidences de bases restent très facilement identifiables.

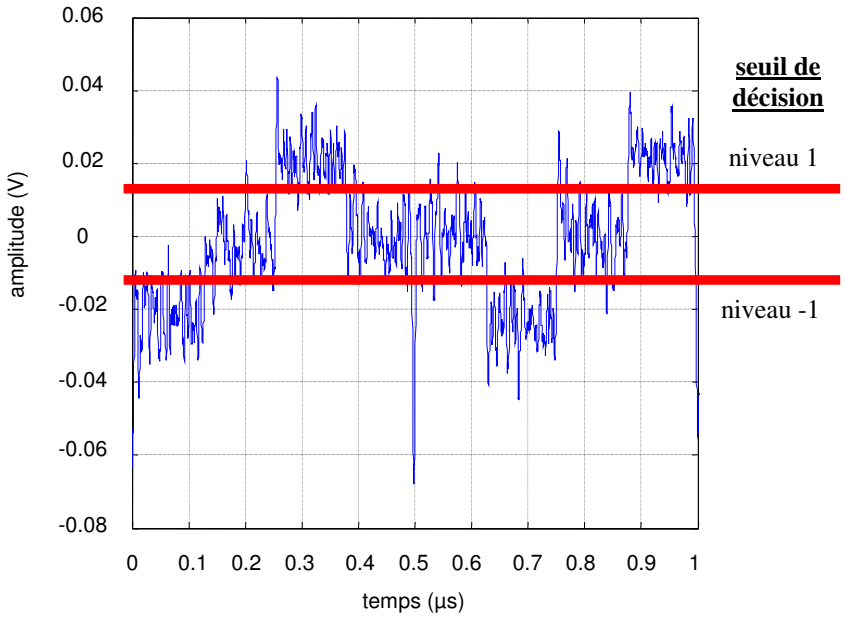



Figure 72 Mesure de *I(t)* avec une atténuation de 40 dB.

Les Figure 73 et Figure 74 présentent le courant *I(t)*, résultat de la soustraction des deux photocourants mesurés lorsque le coefficient d'atténuation vaut respectivement 45 dB et 50 dB.

L'observation des différents états est encore possible. Cependant le courant *I(t)* atteint des niveaux très proches des limites de mesures de l'oscilloscope empêchant une distinction aisée des différents niveaux. Les fluctuations observées sur les Figure 73 et Figure 74 correspondent aux bruits électriques de l'oscilloscope et des amplificateurs électriques intégrés aux photodiodes.

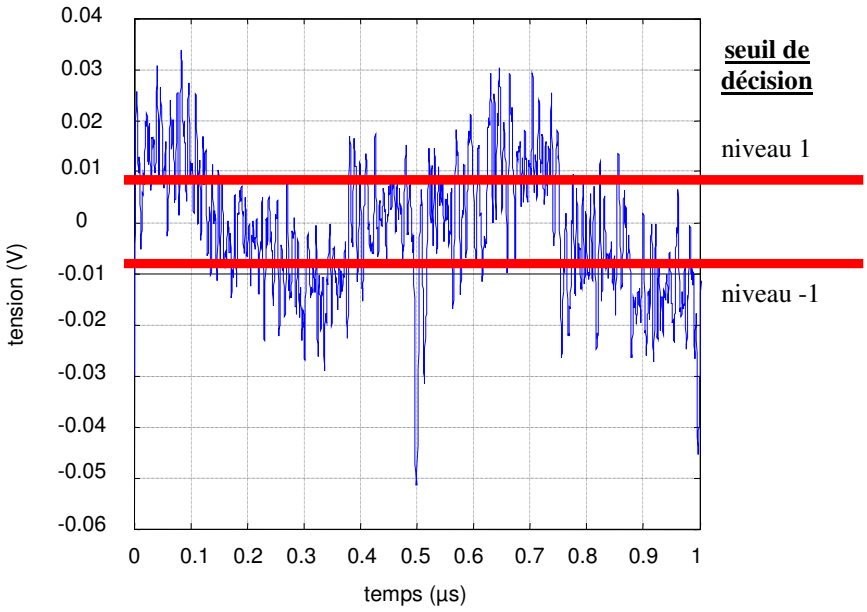



Figure 73 Mesure de *I(t)* avec une atténuation de 45 dB.

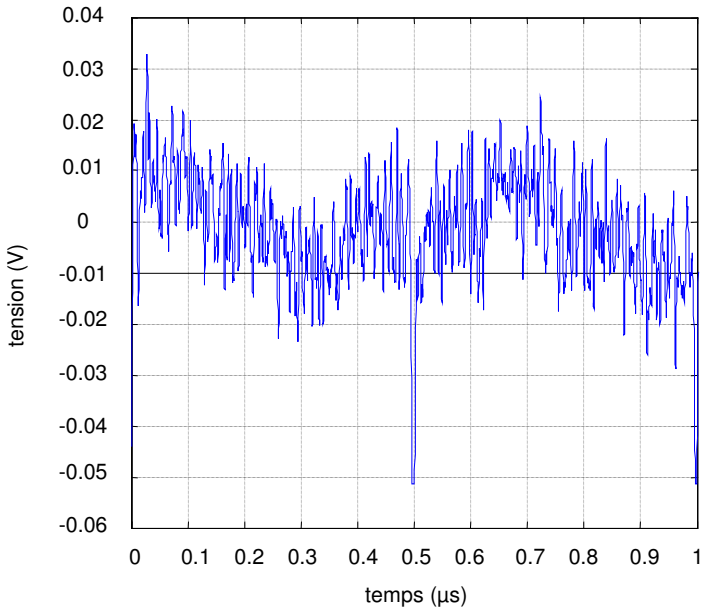



Figure 74 Mesure de *I(t)* avec une atténuation de 50 dB.

Un coefficient d'atténuation de 50 dB correspond à un nombre moyen de photons par temps de mesure égal à 483, le temps d'un bit valant 125 ns.

## 5.4 Conclusion

L'implémentation proposée dans cette section 5.3 a permis d'améliorer la qualité des signaux électriques commandant les modulateurs Mach-Zehnder à doubles électrodes d'Alice et de Bob [42]. Ainsi, les signaux optiques détectés porteurs des déphasages introduits par Alice et Bob en fonction de leurs choix respectifs ne présentent plus de transitoires parasites en régime classique, synonymes d'erreurs dans le domaine quantique.

Cette amélioration permet d'atténuer fortement les signaux optiques et de se rapprocher de la puissance optique minimale pouvant être détectée par des photodétecteurs classiques. Cependant, pour atteindre le régime quantique et ainsi pouvoir transmettre une clef, il est nécessaire de coder les choix d'Alice sur des courtes impulsions optiques afin de minimiser le nombre de photons contenu dans une impulsion représentant un bit.

Ce chapitre souligne l'importance que jouent les trois sous-ensembles d'un système de cryptographie quantique, à savoir une chaîne de modulation, une détection de phase et une source laser d'impulsions optiques.

Trois chaînes de modulation ont été présentées. Elles génèrent les signaux électriques commandant les modulateurs Mach-Zehnder à doubles électrodes d'Alice et de Bob. Les deux premières chaînes sont composées de générateurs de signaux électriques classiques délivrant des signaux fortement parasités sous forme de pics lors des transitions entre chaque niveau caractérisant les déphasages. De plus, les signaux électriques générés par ces deux premières chaînes ne permettent pas de stabiliser les niveaux de tension caractérisant un déphasage.

La troisième chaîne de modulation se compose de deux générateurs programmables autorisant la génération de signaux électriques non-parasités et stables.

# Chapitre 6.
# Implémentations d'un système de distribution quantique de clef

Dans ce sixième chapitre, nous présentons deux implémentations d'un système de distribution quantique de clef, basées sur le protocole BB84 par codage *QPSK*, fonctionnant, pour l'instant, en régime classique (plusieurs photons par bit).

Travailler avec plusieurs photons par bit ne garantit évidemment pas la confidentialité de la transmission, mais autorise la description du comportement des systèmes et ainsi d'identifier les avantages et inconvénients des différentes implémentations.

En régime classique, la détection des déphasages d'Alice et de Bob est réalisée par une détection homodyne, utilisant de simples photodiodes PIN (décrites dans les sections 4.6.2 et 4.6.3).

Afin d'atteindre la puissance correspondant au régime quantique, il est nécessaire de coder chaque bit sur une impulsion optique, puis d'atténuer fortement l'impulsion porteuse de l'information. Les implémentations décrites dans ce chapitre, introduisent et valident la génération et la modulation d'impulsions optiques.

Nous présentons, en fin, un système de distribution quantique de clef à un canal optique, reposant sur un codage *DQPSK* utilisant une référence forte.

## 6.1 Implémentation à deux voies optiques utilisant la génération d'impulsions optiques et une détection homodyne

Pour atteindre une puissance inférieure correspondant à 1 photon par bit et garantissant la confidentialité de l'information, il convient de coder chacun des choix d'Alice sur une impulsion optique de faible largeur spectrale fortement atténuée.

### 6.1.1 Description

Le module laser utilisé pour générer des impulsions optiques est composé d'un laser *DFB* et d'un modulateur d'intensité intégré décrit dans la section 3.1.3. Les impulsions sont générées à la fréquence de 4 MHz et ont une largeur de 50 ns.

Le train d'impulsions ainsi généré se propage dans un interféromètre de type Mach-Zehnder (section 4.2) représenté sur la Figure 75.

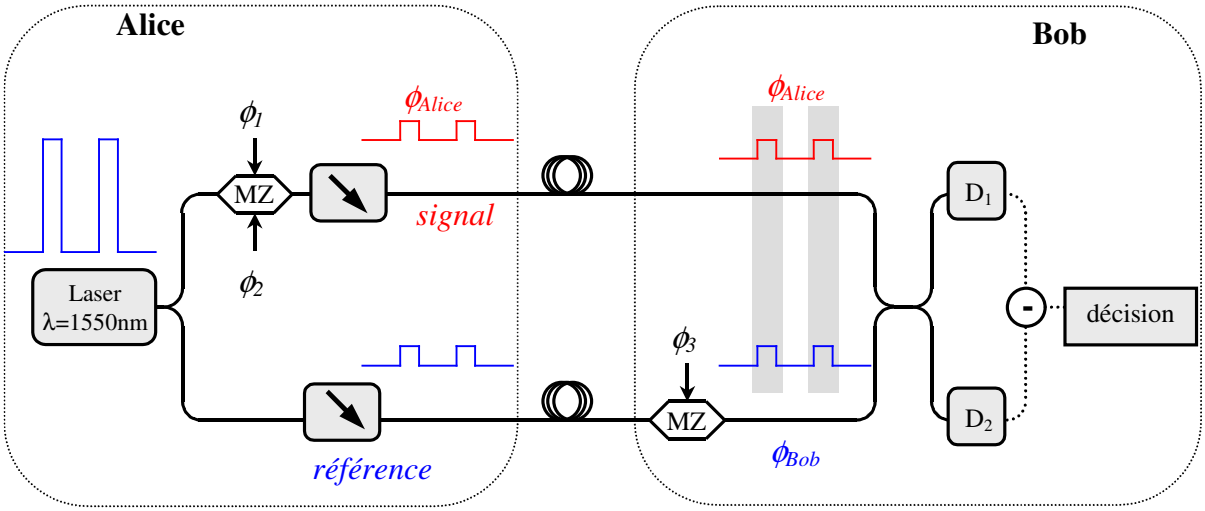



Figure 75 Synoptique d'un système de QKD composé d'une source laser impulsionnelle, de la chaîne de modulation de phase et d'une détection homodyne.

L'un des bras de l'interféromètre porte le modulateur MZ à doubles électrodes d'Alice suivi d'un atténuateur optique calibré. Ce bras correspond au canal quantique, et est appelé bras *signal*. Le second bras de l'interféromètre intègre un atténuateur optique et le modulateur MZ de Bob. L'onde qui s'y propage est appelée onde *référence*. La chaîne de modulation est décrite dans la section 3.2.4.2. Les puissances des ondes optiques *signal* et *référence* sont identiques. La détection est qualifiée de homodyne, le terme super-homodyne étant réservé aux références très intenses.

A la sortie de l'interféromètre, deux photodétecteurs *New-Focus* (section 4.6.3) recueillent le battement des deux ondes.

### 6.1.2 Résultats

A la sortie du module laser, les impulsions optiques contiennent $4{,}8 \times 10^7$ photons. Après atténuation, leur puissance correspond à $3{,}8 \times 10^4$ photons par bit. La Figure 76 présente la mesure de *I(t)* résultant de la soustraction des deux courants générés par les photodétecteurs.

Lorsque la base d'Alice coïncide avec celle de Bob, l'impulsion porteuse de l'information est détectée. Si son amplitude est positive (respectivement négative), alors le symbole transmis par Alice correspond à un bit 1 (respectivement, bit 0).

Lorsque les bases ne sont pas identiques, la somme des déphasages prend une des deux valeurs antipodales (0 ou π) qui annulent le courant *I(t)*. Dans ce cas, il ne reste plus que le bruit du dispositif (essentiellement le bruit des photodétecteurs). Sur la Figure 76, les non-coïncidences des bases sont notées *AC*.

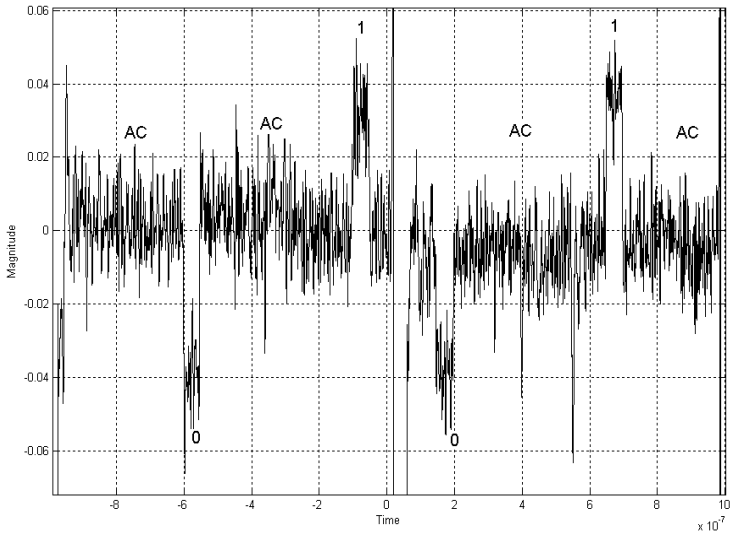



Figure 76 Mesure de *I(t)*.

### 6.1.3 Compteur de photon

Il est possible d'atténuer plus fortement la puissance de chaque impulsion pour atteindre le régime quantique (moins de 1 photon par bit, en moyenne), mais dans ce cas, les détecteurs sont remplacés par les compteurs de photon présentés dans la section 4.6.4.

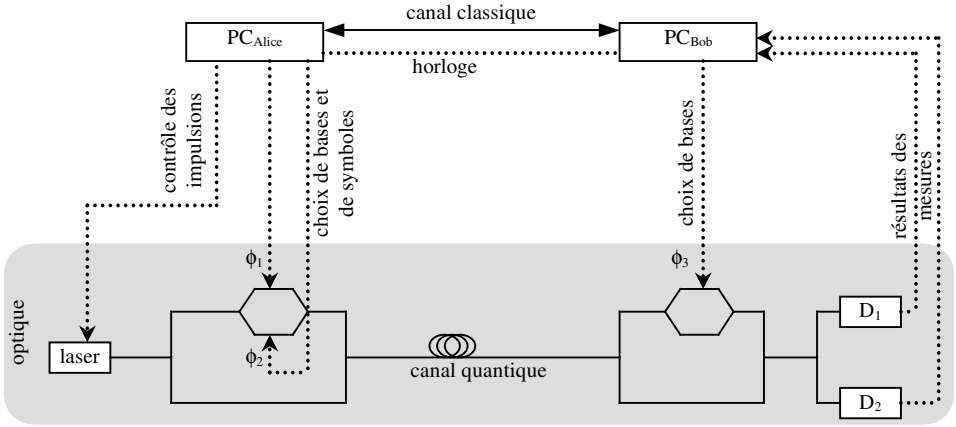



Figure 77 Synoptique du système de contrôle et d'acquisition électronique.

L'utilisation de ce type de détecteur nécessite un système informatique d'acquisition et d'enregistrement de données afin de comparer les choix de symboles et de bases d'Alice, aux choix de bases de Bob et aux résultats de ses mesures. Ce système est en cours de test, il est représenté par la Figure 77, et décrit dans la section 6.2.

### 6.1.4 Mode compteur

Les détecteurs $D_1$ et $D_2$ sont des photodiodes à avalanche opérant en mode compteur (Geiger mode) (voir 4.6.4). Un photon détecté déclenche une avalanche d'électrons créant un courant macroscopique.

L'ouverture des fenêtres temporelles d'observation des détecteurs est cadencée afin d'éviter les déclenchements intempestifs d'avalanche, ce qui permet de diminuer les effets de *dark count*.

Les photodiodes à avalanche utilisées dans cette implémentation sont intégrées dans des modules « compteurs de photons » conçus et fabriqués par *ID Quantique* et sont caractérisés dans la section 4.6.4.4.

Dans ce type de montage, la fréquence est de 1 MHz, la durée d'observation est de 2,5 ns. Lorsque la phase optique est stable, un taux moyen d'erreur a été mesuré et évalué à 30 %.

Les performances de notre système est alors limitée par :

- le taux d'extinction des impulsions *référence*, celles-ci n'étant pas forcement vides entre deux impulsions,
- les imperfections de polarisation du laser affectant le mélange des impulsions *référence* et *signal*,
- la dérive des signaux de modulation,
- les perturbations mécaniques et thermiques s'exerçant sur les interféromètres dans les modules d'Alice et de Bob,
- le *dark count* des photodiodes à avalanche.

### 6.1.5 Conclusion

Cette implémentation valide l'intégration de la source laser impulsionnelle, de la chaîne de modulation de phase et d'une détection homodyne.

Le bruit des détecteurs nous empêche d'atténuer plus fortement la puissance des impulsions pour atteindre le régime quantique. Cependant il est possible de travailler en régime quantique en les remplaçant par les compteurs de photons.

## 6.2 Interface électro-optique

Le cœur d'un système de distribution quantique de clef est constitué d'un dispositif optique permettant l'émission, la modulation et la détection, ainsi que son électronique de contrôle. Il nécessite également un système de décision et d'enregistrement des résultats des mesures de Bob. Des cartes électroniques conçues à l'ENST sont en cours de test. Elles intègrent également un circuit générant des variables aléatoires représentant les choix respectifs d'Alice et de Bob [46].

### 6.2.1 Description des cartes

La carte d'Alice délivre deux signaux électriques commandant chacun une électrodes du modulateur Mach-Zehnder d'Alice. Les valeurs de tension correspondant à $V_{\phi 1}$ et $V_{\phi 2}$ dépendent de deux variables aléatoires générées par la carte électronique représentant les choix de bases et de symboles d'Alice.

| base | symbole | $V_{\phi 1}$ (en V) | $V_{\phi 2}$ (en V) | $\phi_{Alice}$ |
|---|---|---|---|---|
| $A_1$ | 0 | $X$ | X | $\pi/4$ |
| $A_1$ | 1 | X + 3,6 | X + 3,6 | $3\pi/4$ |
| $A_2$ | 0 | X + 3,6 | X | $-3\pi/4$ |
| $A_2$ | 1 | X + 7,2 | X + 3,6 | $-\pi/4$ |
| | | X : tension de polarisation du modulateur | | |

Tableau 16 Correspondance entre les choix d'Alice, $V_{\phi 1}$ et $V_{\phi 2}$.

Le Tableau 16 établit la correspondance entre les choix d'Alice, les signaux électriques commandant le modulateur MZ et le déphasage optique qui en résulte.

La carte commande également le laser qui émet les impulsions optiques. Dans cette première version, un signal d'horloge permet de synchroniser les cartes d'Alice et de Bob.

La carte de Bob délivre un signal $TRIG_{optique}$ commandant les deux compteurs de photon en armant les photodiodes à avalanche. Un signal $V_{\phi 3}$ représente le choix de base de Bob, variable aléatoire générée par le *FPGA*. Les signaux délivrés par les détecteurs, notés $D_1$ et $D_2$ sur la Figure 78, sont acquis par la carte.

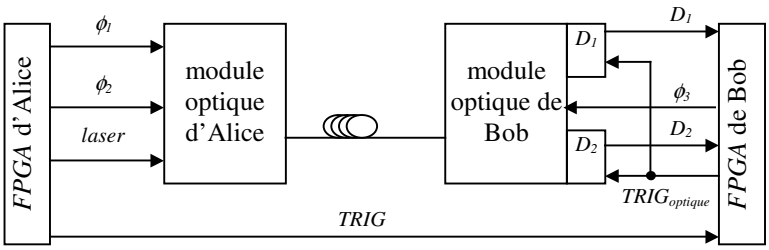



Figure 78 Synoptique des signaux électriques commandant les modules optiques

### 6.2.2 Architecture des cartes

La réconciliation des bases entre Alice et Bob se fait sur une liaison éthernet. La Figure 79 présente l'architecture électronique du système de distribution quantique de clef.

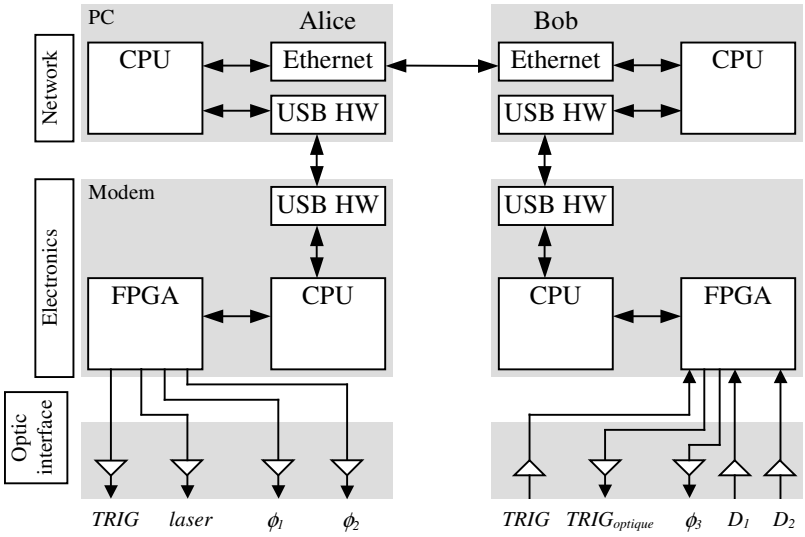



Figure 79 Architecture du système

### 6.2.3 Caractéristiques techniques

Cette première version de carte permet de générer les signaux électriques représentés sur la Figure 80, commandant les modules optiques d'Alice et de Bob. Le temps et les tensions sont ajustés directement par le *FPGA*.

Sur la Figure 80, *c* correspond à la célérité de la lumière et *l* à la longueur de la fibre optique (canal quantique).

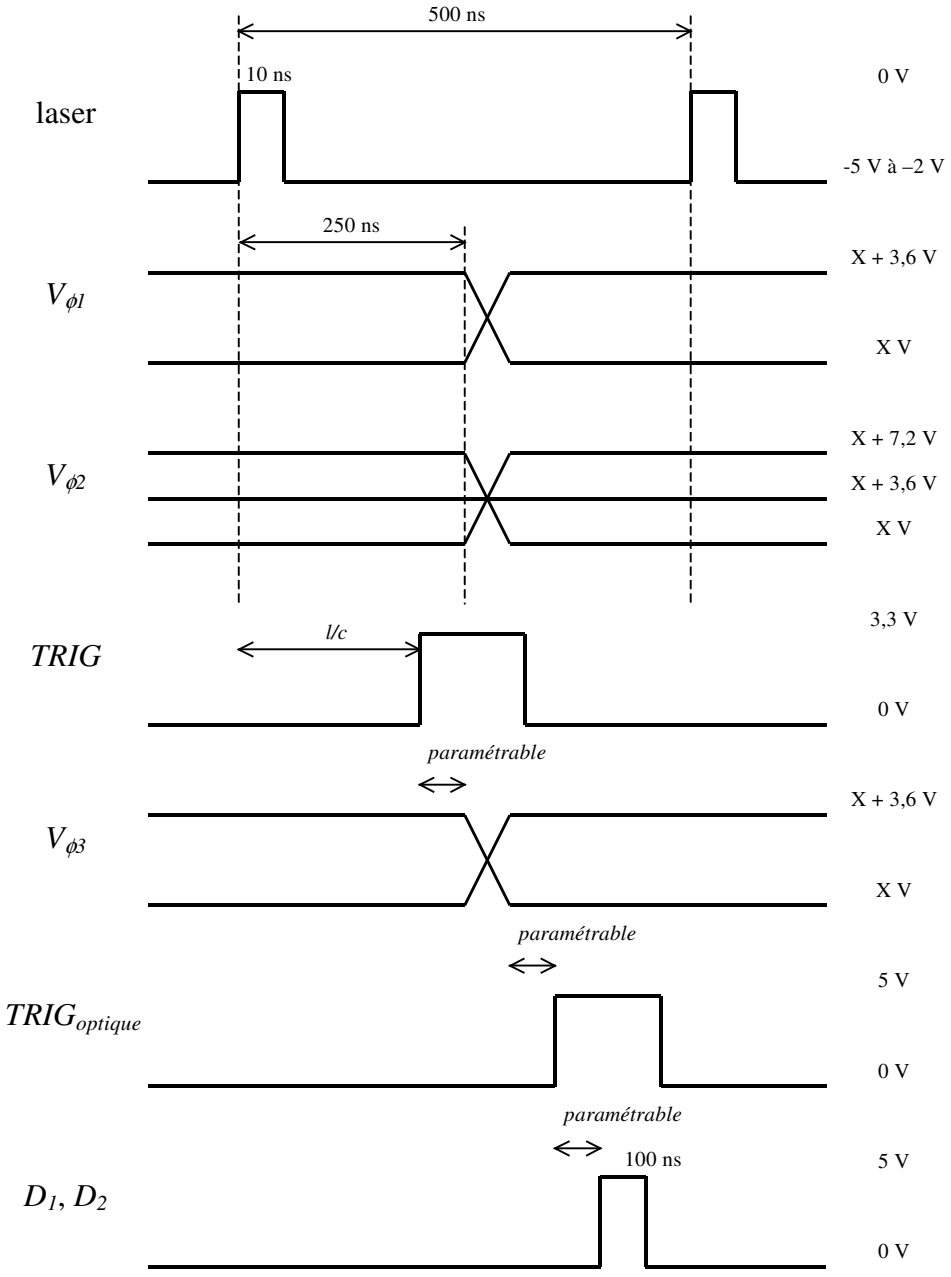



Figure 80 Chronogramme des signaux électriques entre les *FPGA* et les modules optiques d'Alice et de Bob.

Cet interface permet de piloter la partie optique, d'acquérir les résultats de mesures de Bob et de réconcilier les bases choisies par Alice et Bob.

# 6.3 Implémentation à une voie optique utilisant un multiplexage temporel et une détection super-homodyne

La section 6.1 a permis de valider l'intégration des trois sous-ensembles d'un système de distribution quantique de clef. Cependant ces trois premiers montages expérimentaux reposent sur un dispositif interféromètrique de type Mach-Zehnder (section 4.2) dont l'un des deux bras transmet l'onde *signal*, porteuse de la modulation de phase, et l'autre sert à transmettre la *référence* de phase.

Dans ce type d'interféromètre, l'absence de contraintes mécaniques, thermiques et phoniques exercées sur les deux bras est indispensable pour maintenir la stabilité des déphasages entre l'onde *signal* et l'onde *référence*. Or, dans nos précédents montages expérimentaux, il apparaît évidemment une instabilité de la phase d'autant plus importante que la longueur des bras reliant Alice et Bob est grande. Même en l'absence d'expérimentateur dans le laboratoire et pour une longueur des fibres reliant Alice et Bob de quelques mètres, la phase ne reste stable que quelques dizaines de secondes. Au-delà de 10 km, la durée de stabilité n'excède pas quelques secondes.

Afin d'atténuer la sensibilité de l'interféromètre, chaque composant optique a été enrobé d'isolant thermique (Figure 43, Figure 49) et les modules d'Alice et de Bob ont été placés dans des boîtes isolantes. Cependant les fibres *signal* et *référence* restent exposées aux perturbations environnementales.

Dans une détection homodyne, les variations de phase entre le bras *signal* et le bras *référence* sont notées $\varphi_{LO}(t)$ dans l'équation (66). Elles sont aléatoires.

L'utilisation d'un multiplexage temporel entre une onde *signal* ayant une puissance moyenne inférieure à 1 photon par bit et une onde *référence* ayant une puissance forte permet de s'affranchir de compteurs de photon [43][44].

## 6.3.1 Description de l'implémentation

Les précédentes implémentations nécessitent une stabilité de phase sur toute la longueur des deux bras. Il est possible de réduire la sensibilité en faisant transiter les ondes *signal* et *référence* dans un unique canal reliant Alice à Bob. Il est alors nécessaire de les décaler temporellement lors de la transmission entre Alice et Bob.

Les Figure 81 et Figure 82 présentent les modules expérimentaux d'Alice et de Bob autorisant une distribution quantique de clef par codage *DQPSK* (*Differential Quadrature Phase Shift Keying*) [41].

Ce montage consiste à envoyer sur un même canal, des impulsions optiques très fortement atténuées, vectrices des choix d'Alice, décalées temporellement par rapport à des impulsions optiques dont la puissance optique n'est pas atténuée. Ces dernières servent de *référence* de phase dans une configuration super-homodyne [1].

### 6.3.1.1 Module expérimental d'Alice

Le module d'Alice est composé du laser DFB muni d'un modulateur intégré décrit dans la section 3.1.3. Il permet de générer des impulsions optiques cohérentes, dont la fréquence d'émission et la largeur des impulsions sont paramétrables.

Chaque impulsion entre dans un interféromètre Mach-Zehnder assymétrique où la puissance de chaque impulsion est séparée en deux composantes égales. La première composante traverse un bras de l'interféromètre sur lequel elle subit la modulation *QPSK* par l'intermédiaire d'un modulateur MZ à doubles électrodes et sa puissance est fortement atténuée. La seconde composante est transmise sur le second bras de l'interféromètre dont la longueur est plus courte. A la sortie de l'interféromètre, l'impulsion *signal* est ainsi retardée d'un temps $\tau$ par rapport à l'impulsion *référence*.

La Figure 81 présente le module expérimental d'Alice.

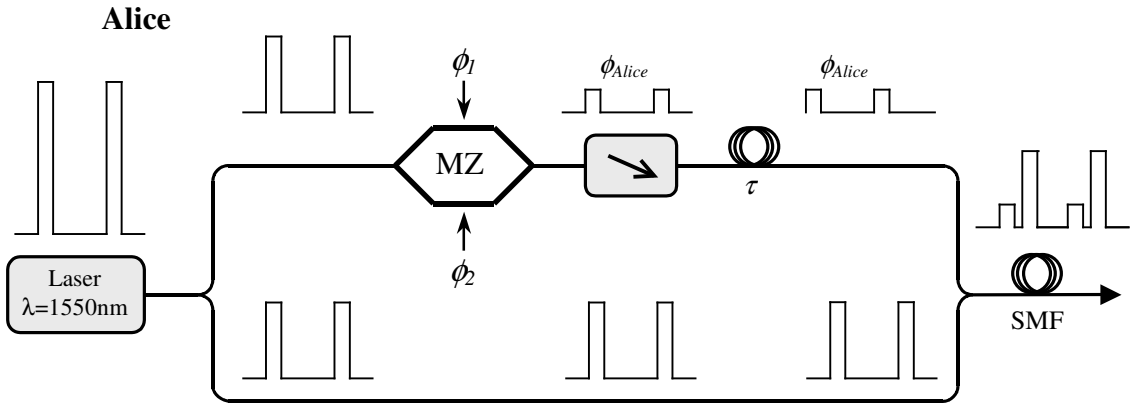



Figure 81 Synoptique du module d'Alice.

### 6.3.1.2 Module expérimental de Bob

Après transmission des impulsions sur l'unique canal (une fibre monomode standard d'une longueur de 11 km), chaque impulsion traverse au travers d'un interféromètre Mach-Zehnder assymétrique composant le module de Bob.

Sur l'un des bras de cet interféromètre, le modulateur MZ introduit une modulation de phase sur les impulsions qui servaient de référence (impulsions dont la puissance est la plus forte). Ce bras, plus long que l'autre, introduit un retard dans la propagation des impulsions. A la sortie de l'interféromètre, les impulsions des deux bras interfèrent.

Les retards introduits dans les modules d'Alice et de Bob autorisent le battement des impulsions de plus faible puissance avec celles de plus forte puissance. Cependant, seul le battement entre les impulsions de forte puissance, porteuses du choix de Bob, et des impulsions de faible puissance, porteuse des choix d'Alice, est pris en compte dans la réconciliation des bases, étape suivante du protocole BB84 permettant la distribution quantique de clef.

La détection équilibrée est assurée par les photodiodes décrites dans la section 4.6.3. Elles délivrent deux photocourants qui passent au travers d'une jonction hybride de type *Maacom H19*. Cette jonction permet de soustraire les bruits en mode commun aux deux photocourants.

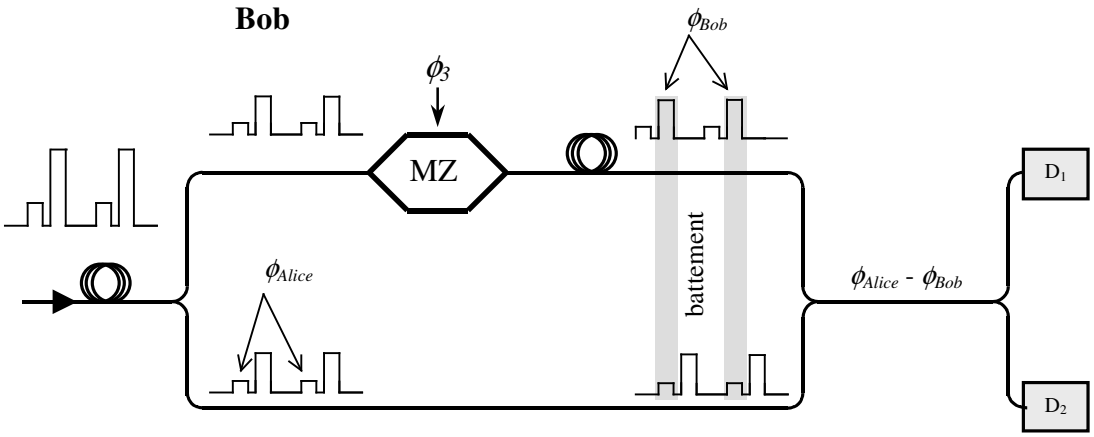



Figure 82 Synoptique du module de Bob.

### 6.3.2 Signaux de commandes

La Figure 83 présente les signaux électriques commandant une électrode du modulateur Mach-Zehnder à doubles électrodes d'Alice. Ces signaux délivrés par les générateurs de signaux programmables, ne présentent pas de transitoires entre chaque transition de niveaux de tension représentant les trois déphasages $\phi_1$. De plus les niveaux sont parfaitement constants au cours des 0,5 µs, contrairement aux signaux obtenus par les précédents montages composés de plusieurs générateurs de signaux présentés dans les sections 3.2.4.1 et 3.2.4.2.

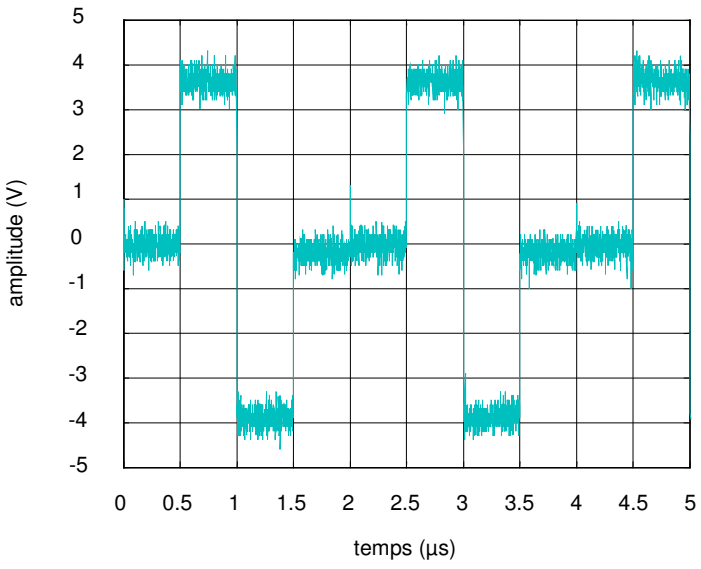



Figure 83 Mesure de $V_{\phi 1}$.

La Figure 84 présente le signal commandant la seconde électrode du modulateur MZ d'Alice.

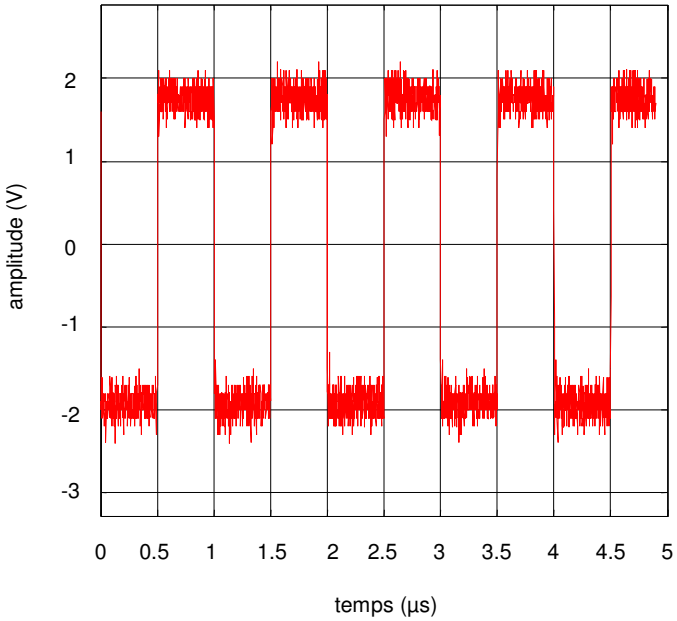



Figure 84 Mesure de $V_{\phi 2}$.

La Figure 85 présente le signal électrique commandant le modulateur MZ de Bob. Il traduit ses choix de bases.

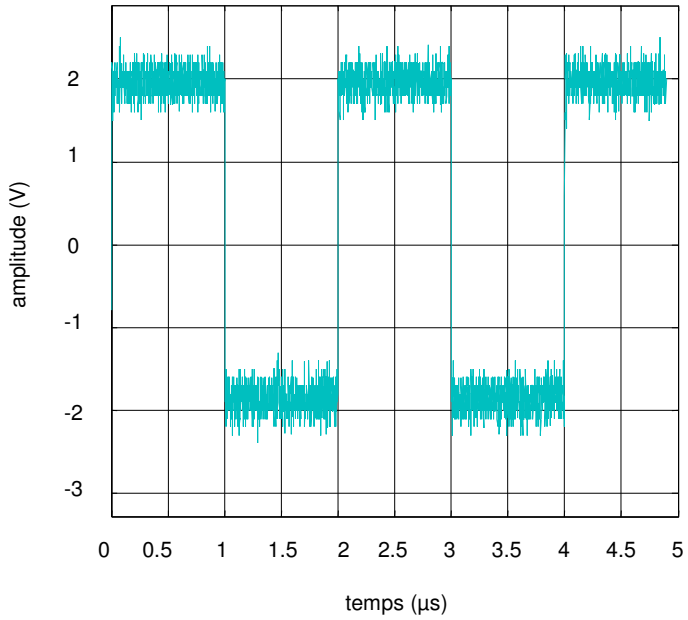



Figure 85 Mesure de $V_{\phi 3}$.

Les Figure 83, Figure 84 et Figure 85 présentent la composante alternative des signaux électriques de commande de $\phi_1$, $\phi_2$ et $\phi_3$ aux quels il faut ajouter des tensions continues servant à polariser les modulateurs MZ d'Alice et de Bob.

### 6.3.3 Taux d'extinction

Le taux d'extinction est un élément déterminant dans ce dispositif. En effet, les impulsions vectrices des choix d'Alice doivent contenir un nombre moyen de photon de l'ordre de 0,1. Il est par conséquent crucial que le taux d'extinction du module laser soit le plus élevé possible afin d'éviter toute émission d'un photon en dehors des impulsions prévues.

Afin d'obtenir un meilleur taux, il est possible de cumuler le taux d'extinction du modulateur MZ d'Alice à celui de la source laser. Il est alors nécessaire d'isoler le modulateur entre chaque impulsion optique afin de le rendre opaque. Pour se faire, les signaux électriques commandant le modulateur ne sont délivrés que lorsqu'une impulsion optique entre dans le modulateur. La synchronisation est très simple à réaliser avec les générateurs programmables.

La Figure 86 présente le signal électrique $V_{\phi 1}$. Les cercles noirs représentent les valeurs de la tension du signal de commande de $\phi_1$ lorsqu'une impulsion pénètre dans le modulateur. En l'absence d'impulsion, les signaux $V_{\phi 1}$ (Figure 86) et $V_{\phi 2}$ (Figure 84) éteignent le modulateur. Ainsi, il est possible d'obtenir un taux d'extinction de l'ordre de 20 dB, caractéristique propre au laser *ILM* fourni gracieusement par *Avanex*.

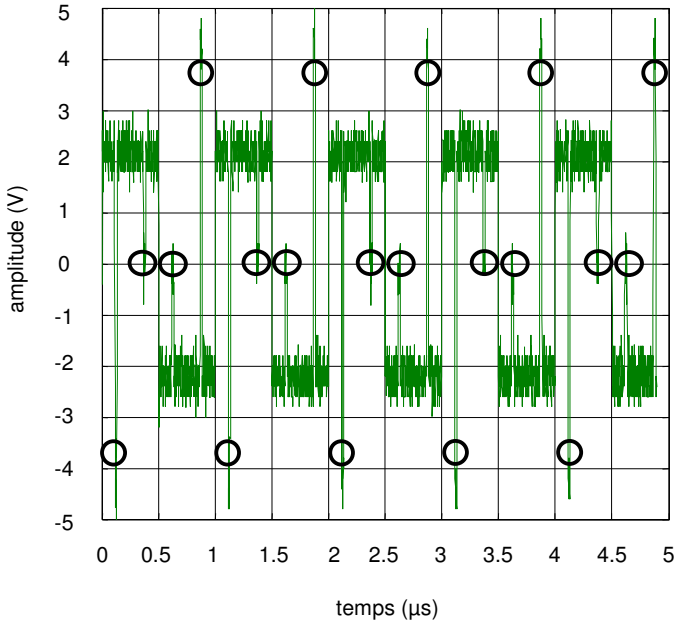



Figure 86 Mesure du signal $V_{\phi 1}$ éteignant le modulateur d'Alice.

### 6.3.4 Résultats

#### 6.3.4.1 Détection super-homodyne

La Figure 87 présente le courant *I(t)* résultant de la soustraction des deux photocourants générés par les deux photodiodes. Sur cette figure, il est aisé d'identifier les états correspondants aux coïncidences de bases.

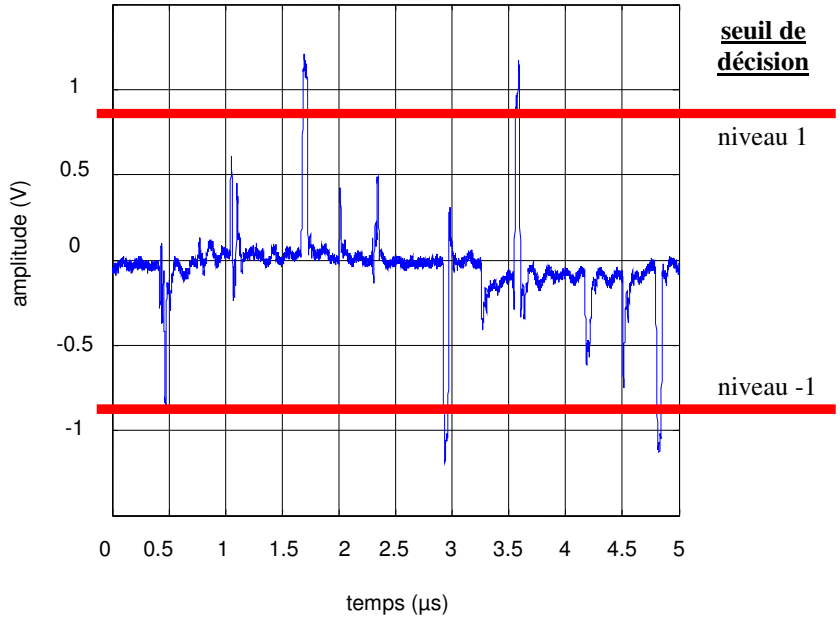



Figure 87 Mesure de *I(t)* sans atténuation.

Les pics dont l'amplitude est comprise entre les seuils de décision [-0,8 0,8] caractérisent les impulsions ne résultant pas du battement des impulsions porteuses des modulations de phase d'Alice et de Bob.

Les Figure 88, Figure 89 et Figure 90 présentent des mesures de *I(t)* réalisées aléatoirement, pour différentes valeurs d'atténuation (respectivement 20 dB, 30 dB et 40 dB).

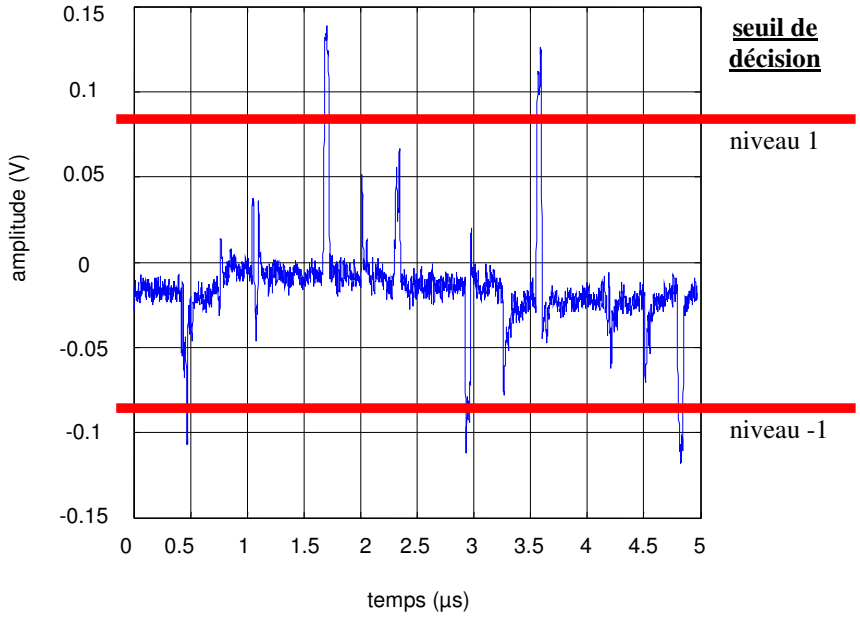



Figure 88 Mesure de *I(t)* avec une atténuation de 20 dB.

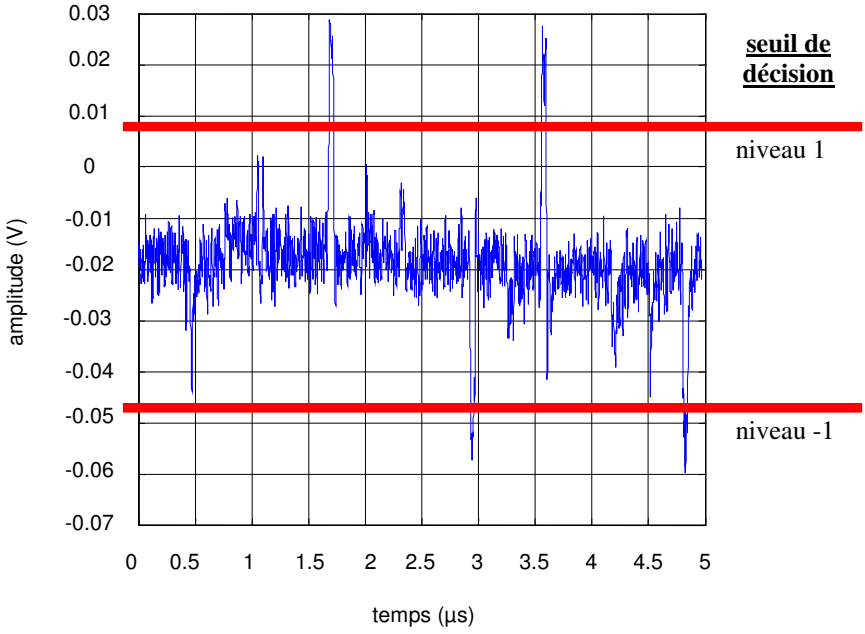



Figure 89 Mesure de *I(t)* avec une atténuation de 30 dB.

Lorsque le coefficient d'atténuation reste inférieur à 30 dB, la différenciation entre les états correspondants aux coïncidences de bases et les pics de bruits est très facile. Par contre,

à partir de 40 dB, l'amplitude des pics est trop proche des niveaux de bruits générés par les photodétecteurs. Il devient difficile alors de détecter et d'identifier un pic porteur d'information d'un pic résultant du bruit. Cependant en ouvrant une fenêtre temporelle de détection lors de l'arrivée d'une impulsion fortement atténuée, il est possible d'identifier les pics correspondants aux coïncidences de bases.

Les fenêtres de détection ayant servi à détecter l'arrivée de pics correspondants aux coïncidences de bases sont représentées sur la Figure 90.

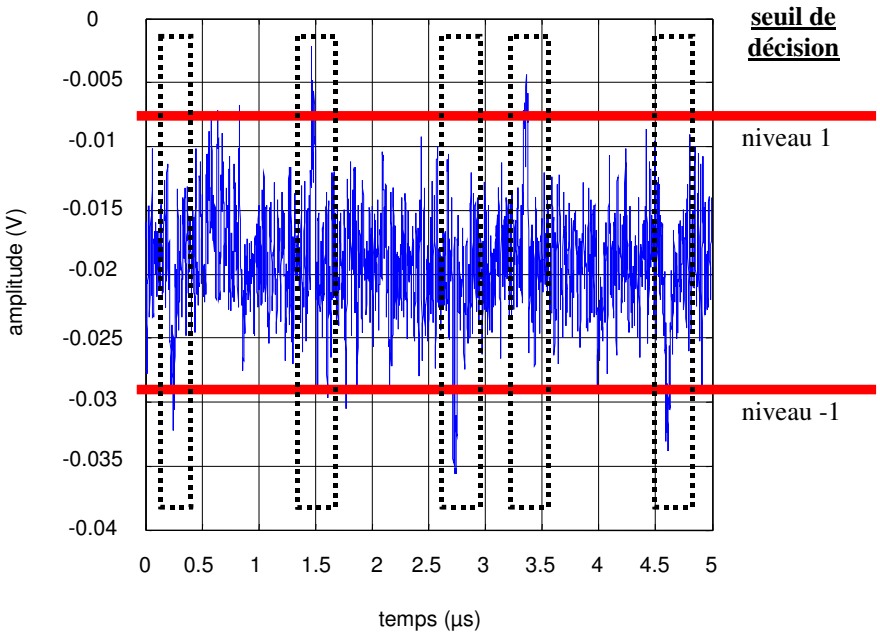



Figure 90 Mesure de *I(t)* avec une atténuation de 40 dB.

### 6.3.4.2 Comparaison des deux modes de détection

Une détection équilibrée super-homodyne présente plusieurs avantages par rapport à une détection de type « compteur de photon » :

- l'efficacité quantique des photodiodes PIN est proche de 95 %, largement supérieure à l'efficacité des photodiodes à avalanche d'efficacité inférieure à 10 %,
- une détection équilibrée permet de supprimer fortement le bruit en mode commun des signaux et double la sensibilité de détection,
- le débit de transmission est plus élevé avec une détection homodyne dés lors que les photodiodes PIN ne requièrent pas de réarmement entre l'arrivée de deux impulsions.

## 6.4 Conclusion

Cette implémentation valide l'intégration d'une modulation de type *DQPSK* et d'une détection homodyne équilibrée. L'utilisation d'une référence de phase transmise à travers le même canal servant à transmettre l'onde signal permet d'obtenir une plus grande stabilité de phase. De plus, le battement de l'onde *signal* fortement atténuée avec une onde *référence* forte améliore la sensibilité de détection de notre dispositif.

Pour atteindre le régime quantique, soit moins de 1 photon en moyenne par bit, il est possible d'atténuer plus fortement les impulsions optiques et de réduire la largeur des impulsions.

Dans ce sixième chapitre, deux dispositifs expérimentaux ont été présentés et étudiés permettant la conception d'un système autorisant, à terme, la transmission quantique d'une clef de cryptage utilisant le protocole BB84 basé sur une détection différentielle par saut de phase (*DQPSK*).

Ce chapitre présente le fonctionnement de ces dispositifs en régime classique. Afin d'atteindre le régime quantique, une source laser d'impulsions paramétrables a été réalisée et intégrée dans le dispositif expérimental présentée dans la section 6.3.

L'étude des dispositifs expérimentaux présentés dans le Chapitre 4 et l'évolution du matériel expérimental disponible au laboratoire a permis de proposer, dans la section 6.3, un système de distribution quantique de clef pour peu que la puissance de l'onde *signal* soit inférieure, en moyenne, à la puissance d'un photon par bit.

Ce dispositif de distribution quantique de clef utilisant le protocole BB84 par codage *DQPSK* a fait l'objet de plusieurs publications [47][48][49].

# Chapitre 7.
# Evaluation de la sécurité potentielle

Dans le Chapitre 6, le fonctionnement en régime classique de notre système de distribution quantique de clef a été présenté. Ce dernier chapitre a pour but de vérifier qu'il présente les potentialités pour fonctionner en régime quantique et qu'il vérifie les critères de sécurité décrit dans la section 2.3.4.

Dans un premier temps, nous vérifierons qu'il est possible de transposer notre système fonctionnant en régime semi-classique dans le domaine quantique. Puis dans une seconde partie, nous évaluerons la sécurité d'une transmission en calculant le taux d'erreur quantique potentiel. En fin, nous comparerons les performances théoriques de notre dispositif expérimental aux autres systèmes dans la littérature.

## 7.1 Interprétation quantique

Lorsque la puissance des impulsions est fortement atténuée, le fonctionnement du système présenté en section 6.3 n'est pas modifié. Les impulsions optiques fortement atténuées sont modélisées par des états cohérents. La description classique de la chaîne de modulation reste donc valide pour les états quantiques.

En régime quantique, la probabilité de détecter un photon est proportionnelle à la puissance du signal incident à une fréquence déterminée. Lorsque $\phi_{Alice}-\phi_{Bob} = 0$ ou $\pi$, le photon incident porteur de cette modulation de phase ne peut être détecté, en principe, que par l'un des détecteurs, soit $D_1$, soit $D_2$. De même lorsque $\phi_{Alice}-\phi_{Bob} = \pm\pi/2$, le photon incident est détecté de manière aléatoire par l'un ou l'autre des détecteurs.

Le déphasage introduit par Alice, noté $\phi_{Alice}$, correspond à son choix de l'état quantique à envoyer. La phase $\phi_{Bob}$ représente le choix de Bob pour la mesure quantique. La projection quantique sur cette base est alors assurée par la détection.

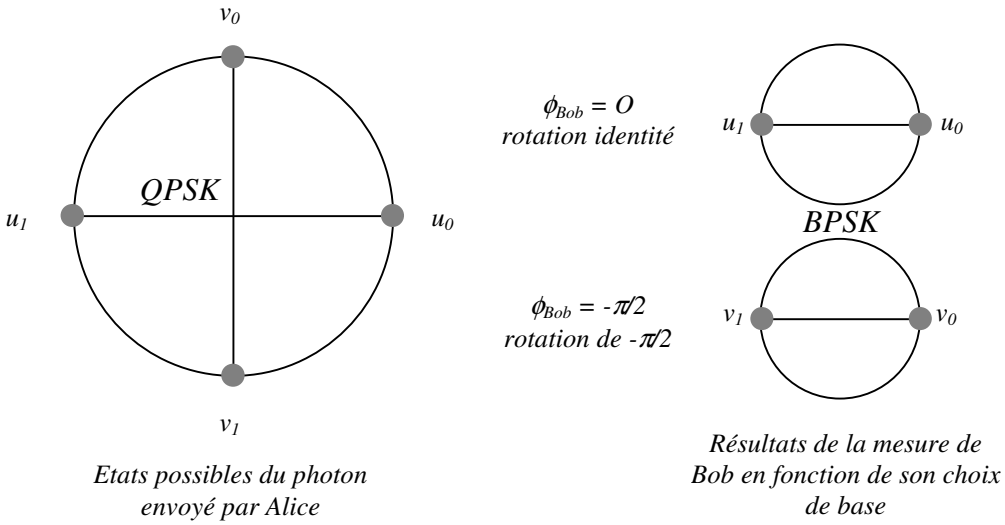
Les états de la base $A_1$, $|u_0\rangle$ et $|u_1\rangle$, correspondent aux déphasages d'Alice valant $0$ et $\pi$. Les états de la base $A_2$, $|v_0\rangle$ et $|v_1\rangle$, correspondent à ceux de valeur $-\pi/2$ et $+\pi/2$.

$$\begin{array}{ll} \phi_{Alice} = 0 \mapsto |u_0\rangle & \phi_{Alice} = \pi/2 \mapsto |v_0\rangle \\ \phi_{Alice} = \underbrace{\pi \mapsto |u_1\rangle}_{A_1} & \phi_{Alice} = \underbrace{-\pi/2 \mapsto |v_1\rangle}_{A_2} \end{array} \tag{129}$$

La mesure de Bob suivant la base qu'il a choisie peut être reliée au déphasage de Bob. La mesure est alors une rotation de l'état envoyé par Alice suivant la matrice

$$M_{\phi_{Bob}} = \begin{pmatrix} \cos\left(\phi_{Bob}/2\right) & \sin\left(\phi_{Bob}/2\right) \\ -\sin\left(\phi_{Bob}/2\right) & \cos\left(\phi_{Bob}/2\right) \end{pmatrix} \tag{130}$$

Finalement, la détection est une projection sur les vecteurs de base, $|u_0\rangle$ et $|u_1\rangle$.




*Etats possibles du photon envoyé par Alice*

*Résultats de la mesure de Bob en fonction de son choix de base*

Figure 91 Projection des états du photon envoyé par Alice sur la base de détection.

$$\begin{aligned} |u_0\rangle &= \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |u_1\rangle &= \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{aligned} \tag{131}$$

Le résultat des projections est caractérisé par les « clics » des compteurs de photons $D_1$ et $D_2$ et correspond à la notation

$$\begin{aligned} D_1 &\mapsto \langle u_0 | \\ D_2 &\mapsto \langle u_1 | \end{aligned} \tag{132}$$

Le dispositif présenté dans la section 6.3 peut donc utiliser le protocole BB84. Son fonctionnement en régime quantique est alors en correspondance avec son fonctionnement décrit en mode classique.

## 7.2 Calcul du *QBER* dans une transmission à un canal quantique

La performance (détectabilité, confidentialité, etc) d'un système de distribution quantique de clef s'évalue en calculant le taux d'erreur de bit quantique (*QBER*). Ce taux est défini comme le rapport entre le nombre de bits erronés détectés par Bob, noté $N_{erroné}$, et le nombre total de bits détectés par Bob, noté $N_{total}$. Le nombre total de bits détectés est le nombre de bits utilisés par la clef, noté $N_{clef}$, et le nombre de bits erronés [50].

$$QBER = \frac{N_{erroné}}{N_{total}} = \frac{N_{erroné}}{N_{erroné} + N_{clef}} \tag{133}$$

Le nombre de bits erronés et le nombre total détecté peuvent s'exprimer en fonction du débit de la transmission.

$$QBER = \frac{R_{erroné}}{R_{erroné} + R_{clef}} \tag{134}$$

Un système de distribution quantique de clef à un canal quantique est représenté par la Figure 92.

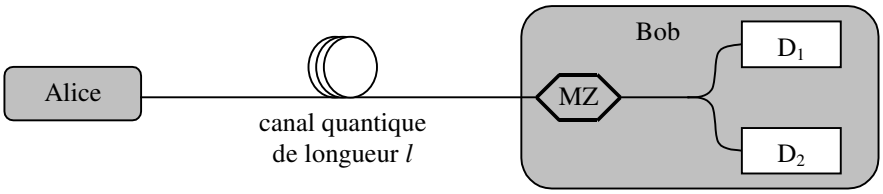



Figure 92 Schéma d'un système de *QKD* servant à l'évaluation du *QBER*.

### 7.2.1 Pertes du canal quantique

La probabilité qu'un photon émis par Alice soit détecté par Bob, est fonction des pertes du canal quantique de transmission et pertes optiques du module de Bob. Plus ces pertes sont importantes, plus la probabilité que le photon soit absorbé avant d'arriver aux détecteurs de photon est grande. Si les pertes de la fibre entre Alice et Bob sont exprimées en dB, alors la probabilité d'absorption du photon par la fibre est

$$\eta_{fibre} = 10^{-\frac{l.\alpha_{fibre}}{10}} \tag{135}$$

avec $l$ la longueur de la fibre constituant le canal quantique et $\alpha_{fibre}$ son coefficient de perte par unité de longueur.

Le module de Bob réunit plusieurs composants optiques ayant des pertes d'insertion et chacun d'eux augmente la probabilité que le photon soit absorbé avant d'arriver sur les détecteurs. Cependant seul le modulateur Mach-Zehnder de Bob présente une perte suffisante pour être prise en compte. Soit $\eta_{Bob}$ la probabilité d'absorption du photon par le module de Bob.

$$\eta_{Bob} = 10^{-\frac{\alpha_{MZBob}}{10}} \tag{136}$$

Ainsi le débit des photons détectés par Bob avant réconciliation des bases s'exprime

$$R_{clef\ brute} = f_{impulsion} \mu \eta_{fibre} \eta_{Bob} \eta_{détecteur} \tag{137}$$

où $f_{impulsion}$ correspond à la fréquence de génération des impulsions optiques contenant en moyenne $\mu$ photon, et $\eta_{détecteur}$ est l'efficacité quantique des détecteurs.

Par définition, le débit de constitution de la clef après réconciliation correspond à la moitié du débit de constitution de la clef brute.

$$R_{clef\ après\ réconciliation} = \frac{1}{2} R_{clef\ brute} \tag{138}$$

### 7.2.2 Contributions au QBER

Trois facteurs d'erreur contribuent au QBER.

a. le dark count des détecteurs,
b. le contraste de l'interféromètre,
c. l'afterpulsing des détecteurs.

**a.** La première contribution provient des compteurs de photon qui peuvent se déclencher sans qu'un photon ne soit présent. Ce phénomène est appelé *dark count* et caractérise la qualité d'un photodétecteur constitué d'une photodiode à avalanche. Le taux de génération d'erreur due au *dark count* s'exprime

$$R_{dark} = \frac{1}{2}\frac{1}{2} f_{impulsion} . P_{dark} . n \tag{139}$$

avec $n$ le nombre de détecteur, $P_{dark}$ la probabilité de *dark count* des détecteurs durant le temps d'observation. Le premier facteur ½ exprime le fait qu'un *dark count* puisse se produire lorsqu'il y a anticoïncidence des bases (le bit est alors éliminé lors de la réconciliation des bases). Le second facteur ½ exprime le fait qu'un détecteur puisse se déclencher sous l'effet d'un *dark* count, et non par l'arrivée d'un photon, lorsqu'il y a coïncidence des bases (le bit est comptabilisé pour la constitution de la clef raffinée).

**b.** La seconde contribution reflète le fait qu'un photon ayant une valeur de phase donnée ne soit pas détecté par le détecteur ayant la valeur propre correspondante. Lorsqu'il y a coïncidence des bases, les valeurs de phase des interférences ne coïncidant pas exactement

aux valeurs propres du système de détection engendrent alors des erreurs. Le débit de cette contribution est

$$\begin{aligned} R_{contraste} &= R_{clef\ raffinée}.P_{contraste} \\ &= \frac{1}{2} f_{impulsion} \mu \eta_{fibre} \eta_{MZ_{Bob}} \eta_{détecteur} . \frac{1-C}{2} \end{aligned} \tag{140}$$

où $C$ représente le contraste de l'interféromètre.

**c.** Le phénomène d'*afterpulsing* est un déclenchement accidentel d'une avalanche lors de la phase de réarmement de la photodiode à avalanche. Cependant si le temps de réarmement de la photodiode est suffisamment long, la probabilité d'apparition de ce phénomène est négligeable. Il existe alors un compromis avec la fréquence de détection.

### 7.2.3 Expression du QBER

Des équations (139) et (140), le débit d'erreurs s'exprime

$$\begin{aligned} R_{erroné} &= R_{contraste} + R_{dark} \\ &= \frac{1}{2} f_{impulsion} \mu \eta_{fibre} \eta_{MZ_{Bob}} \eta_{détecteur} . \left( \frac{1-C}{2} \right) + \frac{1}{2} f_{impulsion} P_{dark} . n \end{aligned} \tag{141}$$

Le *QBER* dans une transmission à un canal quantique se déduit des équations (134), (138) et (141),

$$QBER = \frac{\frac{1}{2} f_{impulsion} \mu \eta_{fibre} \eta_{MZ_{Bob}} \eta_{détecteur} . \left( \frac{1-C}{2} \right) + \frac{1}{2} f_{impulsion} P_{dark} . n}{\frac{1}{2} f_{impulsion} \mu \eta_{fibre} \eta_{Bob} \eta_{détecteur} + \frac{1}{2} f_{impulsion} \mu \eta_{fibre} \eta_{MZ_{Bob}} \eta_{détecteur} . \left( \frac{1-C}{2} \right) + \frac{1}{2} f_{impulsion} P_{dark} . n} \tag{142}$$

Soit

$$QBER = \frac{\mu \eta_{fibre} \eta_{MZ_{Bob}} \eta_{détecteur} . \left( \frac{1-C}{2} \right) + \frac{1}{2} P_{dark} . n}{\mu \eta_{fibre} \eta_{MZ_{Bob}} \eta_{détecteur} . \left( \frac{3-C}{2} \right) + \frac{1}{2} P_{dark} . n} \tag{143}$$

### 7.2.4 Evaluation du *QBER*

D'après l'expression (143), le taux d'erreur quantique est fonction du nombre moyen $\mu$ de photon dans une impulsion et du contraste $C$ de l'interféromètre. Nous évaluerons l'expression du *QBER* pour différentes valeurs de $\mu$.

#### *7.2.4.1 QBER (μ=0.1)*

Les Figure 93 et Figure 94 présentent, pour différentes valeurs du contraste *C* de l'interféromètre, une estimation du taux d'erreur en l'absence d'espion sur le canal en fonction de sa longueur. En effet, le dispositif de détection présenté dans la section 6.3 étant entièrement fibré, il est difficile de contrôler les fluctuations de phase dans les fibres optiques reliant chaque détecteur. La conséquence directe de ces fluctuations est une variation du contraste de l'interféromètre.

Plusieurs mesures ont été effectuées et donnent une valeur du contraste oscillant entre [0,7 0.9].

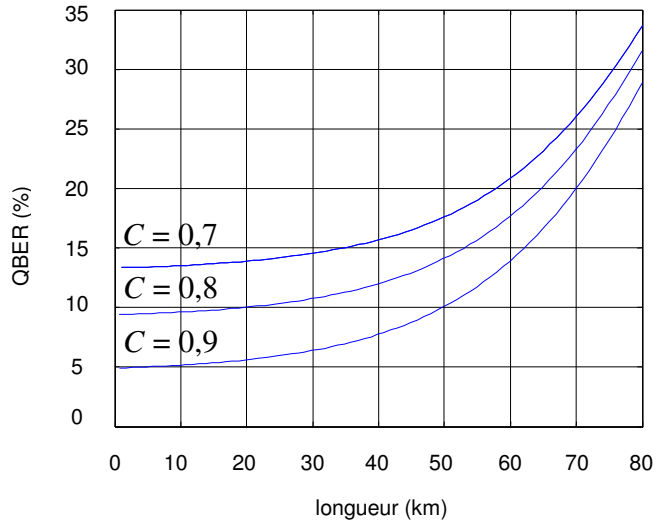



Figure 93 Taux d'erreur en fonction du contraste *C*.

Dans le pire des cas, la valeur du contraste est de 0,7. Dans ce cas, le taux d'erreur est supérieur à 13% quelque soit la longueur du canal, ce qui ne garantit pas une sécurité inconditionnelle (se référer à 2.3.4).

La valeur moyenne du contraste de notre système de détection est 0,8. La Figure 93 présente l'évaluation du taux d'erreur dans ce cas.

La confidentialité d'une transmission est alors garantie puisque le taux d'erreur est inférieur à 11% lorsque la longueur du canal n'excède pas plus de 30 km.

Dans le meilleur des cas, la valeur du contraste vaut 0,9. Une transmission ayant pour but de constituer une clef de cryptage peut être considérée comme confidentielle tant que la longueur du canal n'excède pas 50 km.

En modifiant le dispositif interférométrique afin d'affiner son contraste à l'aide d'une boucle d'asservissement en phase, il est possible de s'approcher des valeurs habituelles pour un système de distribution quantique de clef. Ces valeurs de contraste sont supérieures à 0.95. La Figure 94 présente une estimation du taux d'erreur quantique pour les valeurs de contraste appartenant à {0.95, 0.96, 0.97, 0.98, 0.99}.

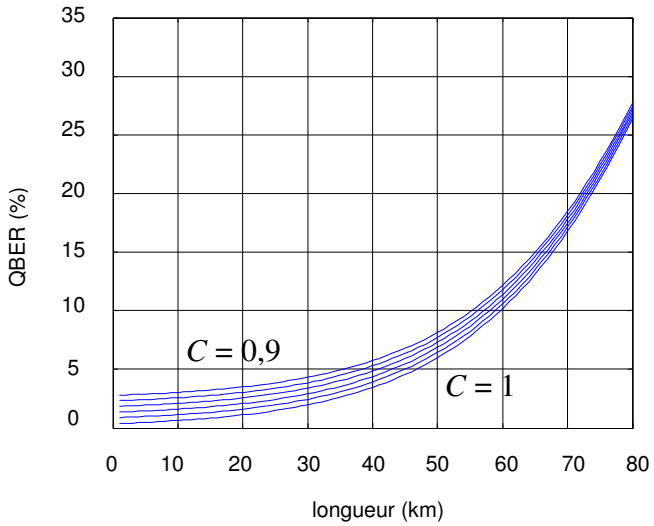



Figure 94 Taux d'erreur (contraste compris entre 0,95 et 1).

La confidentialité d'une transmission est alors garantie pour un canal ayant une longueur maximale de 60 km.

#### *7.2.4.2 QBER (μ=0.5)*

En augmentant le nombre moyen de photon par impulsion, le débit d'arrivée des photons sur les détecteurs augmente. Le nombre de fenêtres vides de photon étant plus faible, l'effet *dark count* diminue. La conséquence est une amélioration du taux d'erreur.

La Figure 95 présente l'estimation du taux d'erreur quantique pour différentes valeurs de contraste compris entre [0.95 1].

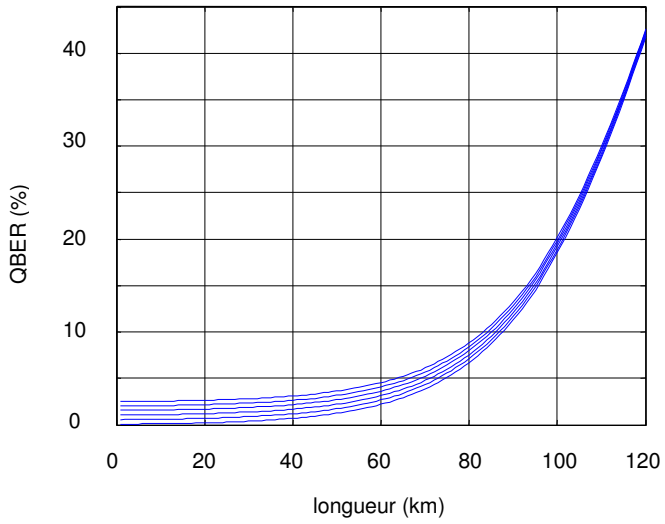



Figure 95 Taux d'erreur (contraste compris entre 0,95 et 1).

Une sécurité inconditionnelle est garantie lorsque la longueur du canal quantique de notre dispositif n'excède pas 83 km.

### 7.2.5 Comparaison avec des systèmes existants

Le premier dispositif de distribution quantique de clef a été élaboré en 1992 et utilisait un canal quantique à l'air dont la longueur ne dépassait pas 32 cm [51].

Aujourd'hui, plusieurs équipes de recherche ont développé des systèmes expérimentaux par fibre dont la longueur du canal de transmission dépasse 100 km :

- Le groupe de *British Telecom* a développé un système de cryptographie quantique reposant sur un codage différentiel à saut de phase Ce système est très sensible aux perturbations externes mécaniques et de température [51].
- Le groupe de Los Alamos présente un système semblable reposant sur un codage de phase utilisant un canal quantique de longueur valant 48 km [53].
- Le groupe de Genève a développé un système *Plug&Play* basé sur le protocole BB84 par codage de phase utilisant un canal de 67 km [54].
- Le système développé par le groupe de *NEC Lab* repose sur des interférence de photon unique en utilisant un détecteur équilibré en mode d'*active gating* et un système *Plug&Play*. Le contraste avec 0,1 photon par impulsion est supérieur à 80% après une transmission de 100 km [55].
- Le groupe de *Toshiba UK* utilise un système à modulation de phase réalisé par un interféromètre Mach-Zehnder. La longueur du canal quantique est de 101 km [56].
- Le système développé au laboratoire *GTL-CNRS Telecom* utilise la phase relative entre la porteuse et les bandes latérales d'un signal modulé. Le schéma de modulation permet la détection d'une simple bande latérale de modulation (principe *SSB* : *Single Side Band*) [57].

| Equipe de recherche | $\lambda$ (nm) | $l$ (km) | μ | Freq (kHz) | *QBER* (%) |
|---|---|---|---|---|---|
| British Telecom | 1300 | 25 | 0,15 | 1000 | 2 |
| Los Alamos | 1300 | 48 | 0,63 | 100 | 9,3 |
| Genève | 1550 | 67 | 0,2 | 5000 | 5,6 |
| Nec Lab. | 1550 | 100 | 0,2 | 500 | 10 |
| Toshiba | 1550 | 101 | 0,1 | 500 | 7,1 |
| G.T.L. | 1550 | 120 | 1 | 1000 | 8 |
| ENST | 1550 | 83 | 0,5 | 4000 | 11 |

Tableau 17 Comparaison du *QBER*.

## 7.3 Conclusion

Les performances potentielles de notre système, bien qu'en état de *proof of concept* en terme de taux d'erreur peuvent être comparées assez favorablement avec celles d'autres systèmes de distribution quantique de clef par codage de phase lorsque le contraste de l'interféromètre sera stabilisé à 0,95.

Bien que le système de détection soit parfaitement équilibré, il apparaît un contraste dont la valeur oscille autour de 0,8. En optique classique, il est courant d'obtenir des valeurs de contraste supérieures à 0,95. Pour cette valeur de contraste, la longueur maximale du canal quantique est de 57 km pour un nombre moyen de photon par impulsion de 0,1. Lorsque $\mu$ = 0,5, la longueur maximale est de 84 km.

| $\mu = 0.1$ | |
|---|---|
| C | $l_{max}$ (km) |
| 0.7 | x |
| 0.8 | 30 |
| 0.9 | 53 |
| 0.95 | 57 |
| 0.97 | 60 |
| 0.99 | 63 |

| $\mu = 0.5$ | |
|---|---|
| C | $l_{max}$ (km) |
| 0.95 | 84 |
| 0.97 | 85 |
| 0.99 | 86 |

Tableau 18 Longueur maximale $l_{max}$ du canal en fonction du contraste $C$.

En améliorant cette caractéristique de notre dispositif, il est possible d'obtenir un taux d'erreur garantissant une sécurité inconditionnelle pour des longueurs de canal quantique représentées dans le Tableau 18.

# Conclusion générale et perspectives

Le protocole de distribution quantique de clef utilisé dans notre étude a été élaboré en 1984 par C. H. Bennett et G. Brassard. Il repose sur l'utilisation de variables physiques ayant des valeurs discrètes.

Les variables utilisées et étudiées pour encoder l'information sur les photons sont principalement la polarisation et la phase. Cependant, les derniers systèmes étudiés reposent sur la différence de phase relative entre deux impulsions séparées temporellement. Ces systèmes se comportent comme un très long interféromètre et sont, par conséquent, très sensibles aux perturbations environnementales. Le système de distribution quantique de clef développé au laboratoire d'optique du département Communication et Electronique à l'ENST repose sur le principe de deux impulsions séparées temporellement transmises sur un canal quantique unique. L'utilisation d'un unique canal permet d'obtenir une plus grande stabilité de la phase optique, puisqu'il est nécessaire de maintenir la phase stable pendant un temps bit, ie la durée entre deux impulsions optiques.

Notre système utilise le protocole BB84 par codage de phase à quatre états, résultant de la différence relative de phase entre deux impulsions séparées temporellement (*DQPSK*). Ce système mis en place est l'aboutissement à ce jour de l'évolution successive des précédents dispositifs de cryptographie quantique étudiés au sein du laboratoire.

Nous avons montré dans le Chapitre 3, deux solutions pour émettre des impulsions optiques fortement atténuées, palliant l'absence de source à photon unique, et différentes chaînes de modulations, transposant les signaux électriques d'Alice et de Bob caractérisant leurs choix respectifs, au domaine optique. Les précédents dispositifs expérimentaux de cryptographie quantique reposaient sur l'utilisation de différents modes de détection cohérente.

Le premier montage utilise une détection hétérodyne. Il nous a permis d'établir une série de critères expérimentaux afin d'équilibrer la détection et de synchroniser l'ensemble des composants électriques. Cependant ce type de détection ne présente pas une sensibilité suffisante pour atteindre le domaine quantique.

Le second montage repose sur une détection homodyne. Il nous a permis de mettre en évidence l'importance de la chaîne modulation servant à transposer les choix d'Alice et de Bob dans le domaine électrique, sous forme de signaux contrôlant leurs modulateurs Mach-Zehnder à doubles électrodes, puis dans le domaine optique.

Le troisième dispositif expérimental utilisant une détection super-homodyne est formé d'un interféromètre Mach-Zehnder ; l'un de ses bras transmettant l'onde *signal*, et l'autre l'onde *référence*. Les contraintes mécaniques et thermiques exercées sur ces deux canaux perturbent les déphasages introduits par Alice. La stabilité de phase est d'autant plus difficile à obtenir que la longueur des canaux est grande.

Le dernier montage expérimental présenté valide, dans le domaine classique, le fonctionnement de la modulation de phase de type *DQPSK* et du système de détection cohérente associé. Ce montage expérimental permet de s'affranchir du canal optique dédié à la transmission de l'onde *référence*, en faisant transiter cette onde sur le même canal que l'onde *signal*. Ainsi, le contrôle sur la stabilité de la phase optique n'est nécessaire que pendant un temps bit, alors que dans un montage à deux voies optiques, il est nécessaire de stabiliser la phase sur toute la longueur du canal de transmission.

La sécurité d'un système de distribution quantique de clef s'évalue en calculant son taux d'erreur quantique. Il a été démontré qu'un taux d'erreur inférieur à 11% est nécessaire afin de garantir la confidentialité d'une transmission de clef. Le taux d'erreur dépend des caractéristiques des composants utilisés et est fonction de la longueur du canal quantique. Notre système de cryptographie quantique de clef utilisant le protocole BB84 par codage *DQPSK* présente un taux d'erreur inférieur à cette limite pour une longueur de 83 km et un nombre moyen de photon par impulsion évalué à 0,5. Cependant ce résultat est obtenu en posant l'hypothèse que le contraste de l'interféromètre vaut 0,95. En pratique, il a une valeur moyenne de 0,8.

Il convient d'étudier le contraste de notre dispositif fibré et de l'améliorer afin d'atteindre une valeur usuelle supérieure à 0,95.

Le point faible actuel repose sur la détection de photon unique. Les compteurs de photons à notre disposition fonctionnant à 1550 nm sont des photodiodes à avalanche dont l'efficacité quantique ne dépasse pas 10%. Une amélioration de cette caractéristique permettrait de diminuer le taux d'erreur et d'augmenter le débit de la transmission.

Ces premiers résultats nous permettent d'envisager l'automatisation de la distribution quantique de clef en intégrant des systèmes informatiques aux modules d'Alice et de Bob.

# Annexe sur la modulation de phase

## 1. Modulation *PSK*

Une modulation *PSK* (*Phase Shif Keying*) est une modulation par saut de phase d'une porteuse appliquée à un signal binaire.

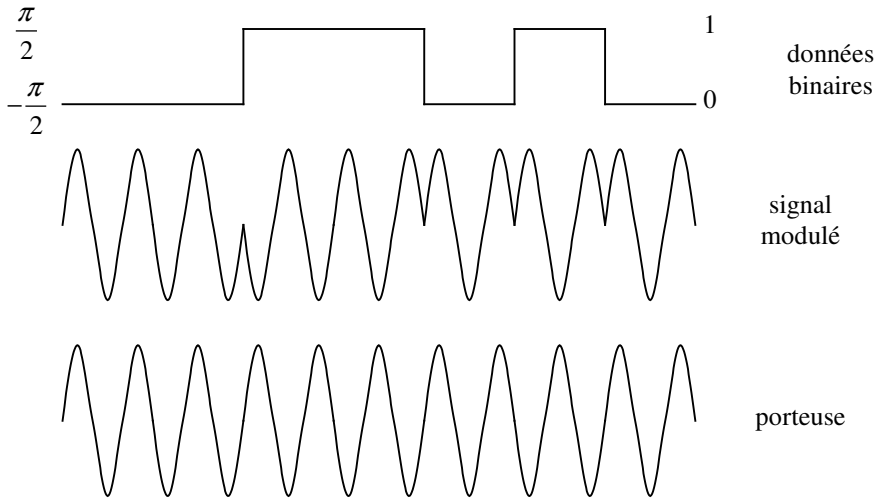



Figure 96 Modulation *PSK*.

Comme le montre la Figure 96, les *1* logiques sont encodés par des déphasages de $\pi/2$ et les *0* logiques par des déphasages de $-\pi/2$. Le signal modulé a pour équation caractéristique

$$m(t) = E.\sin\left(\omega t + \phi(t)\right) \tag{144}$$

avec $E$ l'amplitude du champ électromagnétique, $\omega$ la pulsation de la porteuse et $\phi(t)$ la phase de la porteuse.

## 2- Modulation *QPSK*

La modulation *QPSK* (*Quadrature Phase Shift Keying*) est une modulation par saut de phase à 4 états. Son équation caractéristique s'écrit

$$m(t) = E.\sin\left(\omega t + \phi_i\right) \text{ avec } \phi_i = \left\{\frac{-\pi}{2}; 0; \frac{\pi}{2}; \pi\right\} \tag{145}$$

## 3- Modulation *DPSK*

Dans le cas d'une transmission *PSK*, il est nécessaire au récepteur de retrouver la fréquence et la phase de la porteuse afin d'obtenir une référence. La restauration de la fréquence ne pose pas de réel problème à la différence de la récupération de la phase. En effet, dans une transmission codée en *PSK* sur un canal de longueur *l*, la phase fluctue aléatoirement en fonction des contraintes mécaniques et thermiques exercées sur le canal.
L'utilisation d'une modulation différentielle *DPSK* permet d'atténuer les perturbations engendrées par les fluctuations de phase en utilisant, comme référence, la phase de la donnée précédente. Dans une transmission *DPSK*, il est alors nécessaire de maintenir une stabilité de phase pendant un temps bit, alors que dans une transmission *PSK*, la phase doit être maintenue stable pendant toute la durée de la transmission.

# Annexe sur les matrices

## Notation

Soit A une matrice à éléments complexes.
Nous appelons :
$A^{-1}$ la matrice inverse de $A$.
$A^{+}$ la matrice adjointe de $A$.
$A^{*}$ la matrice conjuguée de $A$.
${}^{t}A$ la matrice transposée de $A$.

## Propriété

${}^{t}A^{*} = A^{+}$

La matrice $A$ est unitaire si et seulement si elle vérifie $A^{-1} = A^{+}$.
La matrice $A$ est hermitienne si et seulement si elle vérifie $A = A^{+}$.
La matrice $A$ est symétrique si et seulement si elle vérifie $A={}^{t}A$.

# Annexe sur les opérateurs

Une onde optique de fréquence $\nu$ est caractérisée par l'expression de son champ électromagnétique *E(t)*. Sa puissance optique est alors

$$P(t) = h\nu \left| E(t) \right|^2 \tag{146}$$

où *h* correspond à la constante de Planck.

Pour une description quantique de cette onde, le champ classique est remplacé par un opérateur $\hat{E}(t)$ (appelé opérateur *annihilation de photon*). Son adjoint est noté $\hat{E}^+(t)$ et est appelé opérateur *création de photon*.

$$\hat{E}(t) = \frac{\hat{a}}{\sqrt{T}} \exp(j\omega t) \tag{147}$$

où $T$ est le temps d'observation

La puissance optique *P(t)* s'exprime en fonction du nombre de photon *N(t)* et le temps *T*, soit

$$P(t) = h\nu N(t) \text{ avec } N(t) = \left\langle \hat{a}^+ \hat{a} \right\rangle \tag{148}$$

$\left\langle \hat{X} \right\rangle$ correspond à la valeur moyenne de l'état quantique $|\psi\rangle$ auquel est associé l'observable $\hat{X}$, tel que

$$\left\langle \hat{X} \right\rangle = \left\langle \psi \left| \hat{X} \right| \psi \right\rangle \tag{149}$$

$\hat{a}$ et son adjoint $\hat{a}^+$ obéissent à la relation de commutation

$$\left[ \hat{a}\hat{a}^+ \right] \equiv \hat{a}\hat{a}^+ - \hat{a}^+\hat{a} = 1 \tag{150}$$

$\hat{a}$ et $\hat{a}^+$ se composent d'un terme en phase et d'un terme en amplitude. Ainsi $\hat{a}$ et $\hat{a}^+$ s'écrivent

$$\hat{a} = \hat{a}_I + j\hat{a}_Q \quad \hat{a}^+ = \hat{a}_I^+ - j\hat{a}_Q^+ \tag{151}$$

$$\hat{a}_I = \frac{\hat{a} + \hat{a}^+}{2} \quad \hat{a}_Q = \frac{\hat{a} - \hat{a}^+}{2j}$$

$$\left[\hat{a}_I \hat{a}_Q\right] = \frac{j}{2} \tag{152}$$

En séparant $\hat{a}$ en une partie classique regroupant le signal et le bruit classique, notée $A = \langle \hat{a} \rangle$, et une partie quantique représentant les fluctuations quantique, notée $\Delta\hat{a}$, $\hat{a}$ s'écrit

$$\hat{a} = A + \Delta\hat{a} \tag{153}$$

$$\left[\Delta\hat{a}\Delta\hat{a}^+\right] = 1 \quad \left[\Delta\hat{a}_I \Delta\hat{a}_Q\right] = \frac{j}{2} \tag{154}$$

# Bibliographie


[1] A. Kerckhoffs. “La cryptographie militaire”, *Journal des sciences militaires*, vol. IX, pp. 5-38, Janvier 1883.

[2] G. Vernam, “Cipher printing telegraph systems for secret wire and radio telegramphic communications”, *Journal of the American Institute of Electrical Engineers*, vol.45, pp. 109-115, 1926.

[3] C. E. Shannon, “Communication Theory of secrecy Systems”, *The Bell System Technological Journal*, vol. 28, pp. 656-715, Oct. 1949.

[4] R. L. Rivest, A. Shamir, and L. M. Adleman, “A method for obtaining digital signatures and public-key cryptosystems”, *Communications of the ACM*, vol. 21, pp. 120-126, Februray 1978.

[5] J. Gabay, Mémoire sur la mécanique ondulatoire, Paris, 1988.

[6] S. Wiesner, “Conjugate Coding”, *SIGACT News*, vol. 15, no. 1, pp. 78-88, 1983.

[7] C. H. Bennett, G. Brassard, “Quantum Cryptography : public key distribution and coin tossing”, *Proceding IEEE International Conference Computers*, *Systems and Signal Processing*, Bangalore, India, pp. 175-179, IEEE, New-York, 1984.

[8] W. K. Wooters, W. H. Zurek. “A single quantum cannot be cloned”, *Nature*, vol. 299, pp. 802, 28 october 1982.

[9] A. Einstein, B. Podolsky, N. Rosen, “Can quantum-mechanical description of physical reality be considered complete ?”, *Physical Review Letters,* vol. 47, pp. 777-780, 1935.

[10] A. K. Ekert, “Quantum cryptography based on Bell’s theorem”, *Physical Review Letters*, vol. 67, pp. 661-663.

[11] O. Alibart, S. Tanzilli, D. B. Ostrowsky, P. Baldi,“Source de photons uniques annoncés à 1,55 µm en optique intégrée”, *Journée Nationales d’Optique Guidée*, Octobre 2004, Paris.

[12] C. H. Bennett, G. Brassard, “Quantum Cryptography : public key distribution and coin tossing”, Proceding IEEE International Conference Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179, IEEE, New-York, 1984.

[13] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, N. Gisin, “Plug and play systems for quantum cryptography”, Appl. Phys. Lett., pp. 793, 17 février 1997.

[14] J.-M. Mérolla, Y. Mazurenko , J-P. Goedgebuer, H. Porte, W. T. Rhodes, “Phase-modulation transmission system for quantum cryptography”, Optics Letters, vol. 24, n° 2, pp. 104, 1999.

[15] D. S. Bethune, W. P. Risk, “An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light”, IEEE Journal of Quantum Electronics, vol. 36, n° 3, 2000.

[16] L. Duraffourg, J.-M. Merolla, J-P. Goedgebuer, Y. Mazurenko, W. T. Rhodes, “Compact transmission system using single-sideband modulation of light for quantum cryptography”, Optics Letters, vol. 26, n° 18, pp. 1427, September 2001.

[17] C. H. Bennett, “Quantum Cryptography using any two nonorthogonal states”, Physical Review Letters, vol. 68, pp. 3121-3124, 1992.

[18] C. E. Shannon, “A mathematical theory of communication”, Bell System Technical Journal, vol. 27, pp.379-423 and pp. 623-656, July and October 1948.

[19] I. Csiszar and J. Körner, “Broadcast channels with confidential messages”, IEEE Transactions on Information Theory, vol. IT-24, no. 3, pp. 339-348, May 1978.

[20] D. Mayers, “Unconditional security in quantum cryptography”, Journal of the ACM, vol. 48, pp. 351-406, May 2001.

[21] P. W. Shor and J. Preskill, “Simple proof of security of the BB84 quantum key distribution protocol”, Physical Review Letters, vol. 85, pp. 441-444, July 2000.

[22] E. Biham and T. Mor, “Security of quantum cryptography against collective attacks”, Physical Review Letters, vol. 78, pp. 2256-2259, 1997.

[23] V. Lena, J. Guitton, “Cryptographie quantique”, Projet de 3ième année, ENST, juillet 2003.

[24] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, “Experimental Quantum Cryptography”, Journal Cryptology, vol. 5, pp. 3-28, 1992.

[25] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography”, Rev. Mod. Phys., vol. 74, pp 145-195, Jan 2002.

[26] A. Peres, Quantum Theory : Concepts and methods, Kluwer Academic Publisher, 1995.

[27] J. I. Cirac and N. Gisin, “Coherent eavesdropping strategies for the four state quantum cryptography protocol”, Physical Review Letters A, vol. 229, pp. 1-7, April 1997.

[28] N. Gisin and S. Wolf, “Quantum Cryptography and noisy channels : Quantum versus classical key-agreement protocols”, Physical Review Letters, vol. 83, n°20, pp.4200-4203, 1999.

[29] O. Alibart, S. Tanzilli, D. B. Ostrowsky, P. Baldi,“Source de photons uniques annoncés à 1,55 µm en optique intégrée”, *Journée Nationales d’Optique Guidée*, *JNOG 2004*, Paris, octobre 2004.

[30] D. Fattal, K. Inoue, J. Vuckovic, C. Santori, G. S. Solomon, and Y. Yamamoto, “Entanglement formation and violation of Bell’s inequality with a semiconductor single photon source”, *Physical Review Letters*, vol. 92, pp. 037903-1/037903-4, Jan. 2004.

[31] B. Huttner, N. Imoto, N. Gisin and T. Mor, "Quantum cryptography with coherent states", *Physical Review Letters*, vol. A51, pp. 1863-1869, 1995.

[32] http://www.avanex.com/products/datasheets/transmission/pwrsource.1915lmm.1600.pdf

[33] S. Agnolini, P. Gallion, ,"De la modulation QPSK à la cryptographie quantique", *Workshop of the IEEE Lasers and Electro-Optics Society (LEOS) French Chapter*, 5 décembre 2003.

[34] S. Agnolini, P. Gallion, "Implémentation du protocole de cryptographie quantique BB84 par modulation QPSK utilisant des modulateurs Mach-Zehnder à deux électrodes", *23èmes Journées Nationales d'Optique Guidée*, *JNOG 2003*, Valence (France), novembre 2003.

[35] J. G. Proakis, "Digital Communications", 4 ed., p. 266-272, McGraw-Hill, 2001.

[36] I. Joindot, M. Joindot, "Les Télécommunications par fibres optiques", p. 544-545, Collection Technique et Scientifiques des Télécommunications, Dunod, 1996.

[37] G. L. Abbas, V. W. S. Chan et T. K. Yee, "A dual-detector optical heterodyne receiver for local oscillator noise suppression", *Journal of Lightwave Technology*, vol. LT-3, n. 5, octobre 1985.

[38] S. Agnolini, P. Gallion, "Implémentation du protocole de cryptographie quantique BB84 par modulation QPSK utilisant des modulateurs Mach-Zehnder à deux électrodes", *23èmes Journées Nationales d'Optique Guidée JNOG 2003*, Valence (France), novembre 2003.

[39] S. Agnolini, P. Gallion, "De la modulation QPSK à la cryptographie quantique", *Workshop of the IEEE Lasers and Electro-Optics Society (LEOS) French Chapter*, 5 décembre 2003.

[40] S. Agnolini, P. Gallion, "Implementation of BB84 Protocol by QPSK Modulation using Dual-Electrode Mach-Zehnder Modulators", *IEEE International Conference on Industrial technology ICIT'2004*, Paper 4149, Hammamet (Tunisia), December 2004.

[41] S. Agnolini, P. Gallion, "Implementation of BB84 Protocol by QPSK Modulation using Dual-Electrode Mach-Zehnder Modulators", *IEEE International Conference on Industrial Technology ICIT'2004*, Paper 4149, vol. 1, 8-10, pp. 250-253, Hammamet (Tunisia), December 2004.

[42] S. Agnolini, P. Gallion, "Quantum Key Distribution Implementations by QPSK Modulation Using a Single Dual-Electrode Mach-Zehnder Modulator", *Symposium on Technology Fusion of Optoelectronics and Communications SFTO'05*, Paper 21S11, Taipei (ROC), May 2005.

[43] O. L. Guerreau, F. J. Malassenet, S. W. McLaughlin, J-M. Merolla, "Quantum Key without a Single-Photon Source Using a Strong Reference", *IEEE Photonics Technology Letters*, vol. 17, n. 8, pp. 1755, August 2005.

[44] T. Hirano, "Quantum cryptography using pulsed homodyne detection", *Physical Review Letters*, vol. A68, pp. 042331-1 – 042331-7, 2003.

[45] M. Koashi, "Unconditional Security of Coherent State Quantum Key Distribution with a Strong Reference Phase Pulse", *Physical Review Letters*, vol. 93, pp. 120501-1 – 120501-4, 2004.

[46] M. B. Costa e Silva, Q. Xu, S. Agnolini, S. Guilley, J-L. Danger, P. Gallion, F. J. Mendieta, "Integrating a QPSK Quantum Key Distribution Link", *European Conference on Optical Communication ECOC'06, CLEO Focus Meeting on Nonlinear, Quantum and Chaotic Optics: New Directions in Photonics and Optical Communications*, Paper Tu4.1.2, Cannes (France), September 2006.

[47] M. B. Costa e Silva, Q. Xu, S. Agnolini, P. Gallion, and F. J. Mendieta, "Homodyne Detection for Quantum Key Distribution : an Alternative to Photon Counting", *International Conference On Applications of Photonic Technology, Photonics North 2006*, Quebec City, (Canada), June 2006.

[48] M. B. Costa e Silva, Q. Xu, S. Agnolini, P. Gallion, and F. J. Mendieta, "Homodyne QPSK Detection for Quantum Key Distribution", *Coherent Optical Technologies and Applications (COTA) Topical Meeting. of the OAA*, Paper CFA2, Whistler B.C. (Canada), June 2006.

[49] Q. Xu, M. B. Costa e Silva, S. Agnolini, P. Gallion, and F. J. Mendieta, "Photon Counting and Super Homodyne Detection of Weak QPSK Signals for Quantum Key Distribution Applications", Accepted paper *EOS Annual Meeting 2006, Topical Meeting on Extreme Optics (QEOD/EPS and EOS)*, Paris, October 2006.

[50] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography", arXiv:quant-ph/0101098v2, pp. 22, September 2001.

[51] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and Smolin, "Experimental quantum cryptography", *J. Crypto.*, vol. 5, n° 1 ,pp. 3-28, 1992.

[52] P. D. Townsend, J. G. Rarity, and P. R. Tapster, "Enhanced single photon fringe visisbility in 10 km-long prototype quantum cryptography channel", *Electronics Letters*, vol. 29, pp. 1291-1293, July 1993.

[53] R. J. Hughes, G. L. Morgan, and C. G. Peterson, "Quantum key distribution over a 48 km optical fiber network", *Journal of Modern Optics*, vol. 47, pp. 533-547, February 2000.

[54] D. Stücki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a Plug&Play system", *New Journal of Physic*, vol. 4, pp. 41.1-41.9, July 2002.

[55] H. Kosaka, A. Tomita, Y. Nambu, and K. Nakamura, "Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector", *Electronics Letters*, vol. 39, pp. 1199-1201, August 2003.

[56] Z. Yuan, C. Gobby, and A. J. Shields, "Quantum key distribution over distances as long as 101 km", *CLEO / QELS 2003*, 2003.

[57] O. L. Guerreau, J.-M. Merolla, A. Soujaeff, F. Patois, J.6P. Goedgebuer, and F. J. Malassenet, "Long-distance QKD transmission using single sideband detection scheme with WDM synchronization", *IEEE J. Select. Topics Quantum Electron.*, vol. 9, pp. 1533-1540, November / December 2003.

# Liste des publications

- S. AGNOLINI, P. GALLION, “Implémentation du protocole de cryptographie quantique BB84 par modulation QPSK utilisant des modulateurs Mach-Zehnder à deux électrodes”, *23èmes Journées Nationales d’Optique Guidée JNOG 2003*, Valence (France), novembre 2003.

- S. AGNOLINI, P. GALLION, “De la modulation QPSK à la cryptographie quantique”, *Workshop of the IEEE Lasers and Electro-Optics Society (LEOS) French Chapter*, 5 décembre 2003.

- S. AGNOLINI, P. GALLION, “Implementation of BB84 Protocol by QPSK Modulation using Dual-Electrode Mach-Zehnder Modulators”, *IEEE International Conference on Industrial technology ICIT’2004*, Paper 4149, Hammamet (Tunisia), December 2004.

- S. AGNOLINI, P. GALLION, “Implementation of BB84 Protocol by QPSK Modulation using Dual-Electrode Mach-Zehnder Modulators”, *IEEE International Conference on Industrial Technology ICIT'2004*, Paper 4149, vol. 1, 8-10, pp. 250-253, Hammamet (Tunisia), December 2004.

- S. AGNOLINI, P. GALLION, “Quantum Key Distribution Implementations by QPSK Modulation Using a Single Dual-Electrode Mach-Zehnder Modulator”, *Symposium on Technology Fusion of Optoelectronics and Communications SFTO’05*, Paper 21S11, Taipei (ROC), May 2005.

- M. B. COSTA E SILVA, Q. XU, S. AGNOLINI, P. GALLION, and F. J. MENDIETA, “Homodyne Detection for Quantum Key Distribution : an Alternative to Photon Counting”, *International Conference On Applications of Photonic Technology, Photonics North 2006*, Paper XXXX-XX, Quebec City, (Canada), June 2006

- M. B. COSTA E SILVA, Q. XU, S. AGNOLINI, P. GALLION, and F. J. MENDIETA, “Homodyne QPSK Detection for Quantum Key Distribution”, *Coherent Optical Technologies and Applications (COTA) Topical Meeting. of the OAA*, Paper CFA2, Whistler B.C. (Canada), June 2006.

- M. B. COSTA E SILVA, Q. XU, S. AGNOLINI, S. GUILLEY, J.-L. DANGER, P. GALLION, and F. J. MENDIETA, “Integrating a QPSK Quantum Key Distribution Link”, *European Conference on Optical Communication ECOC’06, CLEO Focus Meeting on Nonlinear, Quantum and Chaotic Optics: New Directions in Photonics and Optical Communications*, Paper Tu4.1.2, Cannes (France), September 2006.

- Q. XU, M. B. COSTA E SILVA, S. AGNOLINI, P. GALLION, and F. J. MENDIETA, “Photon Counting and Super Homodyne Detection of Weak QPSK Signals for Quantum Key Distribution Applications”, Accepted paper *EOS Annual Meeting 2006, Topical Meeting on Extreme Optics (QEOD/EPS and EOS)*, Paris, October 2006.

- M. B. COSTA E SILVA, Q. XU, S. AGNOLINI, P. GALLION, and F. J. MENDIETA, “Homodyne QPSK Detection for Quantum Key Distribution”, Submitted paper.