Université de Montréal

Cryptographie quantique à plusieurs participants par multiplexage en longueur d'onde

par

Félix Bussières

Département de Physique
Faculté des Arts et des Sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès Sciences (M.Sc.)
en Physique

Juillet 2003

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

Cryptographie quantique à plusieurs participants par multiplexage en longueur d'onde

présenté par :
Félix Bussières

a été évalué par un jury composé des personnes suivantes :

Louis-André Hamel
Président-rapporteur

Gilles Brassard
Directeur de recherche

Nicolas Godbout
Codirecteur de recherche

Suzanne Lacroix
Codirectrice de recherche

Romain Maciejko
Membre du jury

Mémoire accepté le 24 octobre 2003

Résumé

La cryptographie étudie la confidentialité de l'information et la mécanique quantique est la description de la matière au niveau microscopique. La cryptographie quantique est la fusion de ces deux disciplines et offre un moyen de communiquer avec confidentialité garantie sur grande distance. La cryptographie quantique a été réalisée avec succès à plusieurs reprises par l'utilisation de photons guidés dans la fibre optique et à l'air libre. Or, la plupart de ces démonstrations ne font intervenir que deux participants.

Dans ce mémoire, nous étudions, à l'aide d'une démonstration de principe, la possibilité d'utiliser le multiplexage en longueur d'onde dans le but d'élaborer un réseau optique permettant à n'importe quelle paire de participants de communiquer de façon parfaitement confidentielle.

Au premier chapitre, nous révisons les concepts généraux de la cryptographie quantique et des outils d'analyse de sa sécurité. Au second chapitre, nous décrivons d'abord le fonctionnement du montage utilisé dans cette expérience. Par la suite, nous proposons une architecture de réseau optique sur laquelle la cryptographie quantique est implantable sans compromis sur la sécurité. Au troisième chapitre, nous décrivons le développement et la caractérisation d'un détecteur de photon à 1550 nm et nous étudions l'impact de ses propriétés sur la faisabilité de la cryptographie quantique. Au quatrième chapitre, nous décrivons d'abord le développement et la caractérisation du réseau optique proposé à l'aide du détecteur de photon. Nous discutons ensuite des limitations du réseau en utilisant les outils d'analyse développés au chapitre 1.

Mots clés : Cryptographie quantique, optique quantique, fibre optique, multiplexage en longueur d'onde, réseaux quantiques, détection de photons dans l'infrarouge proche.

Abstract

Cryptology is the science of confidentiality while quantum mechanics is the description of nature at the microscopic level. Quantum cryptography is the fusion of these two fields and offers a provably secure way to guarantee absolute confidentiality in communications. Quantum cryptography has been successfully demonstrated by many groups using optical fibre and photons. However, most of these experiments were designed for two users only.

In this thesis, we show how wavelength division multiplexing can be used to realize an all optical network that uses quantum cryptographic protocols to allow any two user pairs to communicate in a provably secure fashion.

The first chapter consists in a review of the main concepts behind quantum cryptography and its security. In the second chapter, we first describe the principle of operation of the optical link that we built, and then we propose a secure optical network architecture on which quantum cryptographic protocols are implementable. In the third chapter we report the construction and the characterization of a single photon detector at 1550 nm and we study the impact of the measured performances on the feasibility of quantum cryptography. Finally, in the fourth chapter, we first describe the development and characterization of the proposed multi-user architecture using the single photon detector and, secondly, we study its efficiency and security level.

Keywords : Quantum cryptography, quantum optics, optical fibre, wavelength division multiplexing, quantum networks, single-photon detection in the near infrared.

Table des matières

Liste des tableaux

Table des figures

Notations

$\hat{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	Opérateur identité dans $\mathcal{H}_2$
$\hat{\sigma}_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	Matrice de Pauli x
$\hat{\sigma}_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	Matrice de Pauli y
$\hat{\sigma}_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	Matrice de Pauli z
$\mathbf{v} = (v_x, v_y, v_z)$	Vecteur dans $\mathbb{R}^3$
$\binom{n}{l} = \frac{n!}{l!(n-l)!}$	Binôme de Newton
$\oplus$	Addition modulo 2
$\otimes$	Produit tensoriel
$\in_A$	Choisi aléatoirement parmi
$\hat{U}$	Opérateur quantique
$\mathcal{H}_2$	Espace d'Hilbert de dimension 2
μ	Nombre moyen de photons par impulsion (équ. A.9)
WDM	Multiplexage en longueur d'onde
PDA	Photodiode à avalanche
$\mathcal{V}$	Visibilité d'interférence (équ. 2.15)
$\mathcal{V}_{\text{dB}}$	Visibilité d'interférence en dB (équ. 4.5)
V_p	Amplitude de l'impulsion d'activation du détecteur
T_p	Durée de l'impulsion d'activation du détecteur
τ	Durée de l'impulsion optique
T_r,f_r	Temps et fréquence d'activation du détecteur
V_B	Tension d'avalanche
V_{RT}	Tension de pénétration
V_{DC}	Tension de polarisation continue du détecteur
V_E	Tension en excès. $V_E = V_{DC} + V_p - V_B$

T_l	Transmission du lien
T_B	Transmission de l'appareil de Bob
v_d	Vitesse de dérive des porteurs de charges
η	Rendement du détecteur de photon
p_{co}	Probabilité de compte obscur
p_c	Probabilité de compte simple (réel ou obscur) (équ. 3.12, 3.20, 4.10)
p_{cr}	Probabilité de compte réel (équ. 3.11, 3.18)
f_c	Facteur de réduction de la clé par la correction des erreurs (équ. 1.22)
f_{ds}	Facteur de réduction de la clé par la distillation de secret (équ. 1.24)
R_p	Taux d'extraction de la clé finale par impulsion (équ. 4.6)

Remerciements

Premièrement, je tiens à remercier mon directeur de recherche, Gilles Brassard, tout d'abord pour avoir co-inventé la cryptographie quantique, un sujet passionnant qui a alimenté mon intérêt durant ces deux années, et ensuite pour la confiance qu'il m'a accordée, pour sa perspicacité, sa rigueur et sa curiosité insatiable. Je remercie ensuite mon codirecteur Nicolas Godbout pour avoir investi son indispensable expertise au profit de ce projet. Sa curiosité et sa polyvalence ont sans contredit contribué au succès de l'expérience. Merci enfin à ma codirectrice, Suzanne Lacroix, qui a su à maintes reprises me donner la motivation nécessaire pour faire avancer le projet. Sans elle, les résultats ne seraient pas là. Je remercie conjointement mes trois superviseurs pour avoir investi leurs fonds de recherche dans ce projet.

Je tiens ensuite à remercier tous les étudiants que j'ai côtoyés durant mes études au LITQ et au LFO. Ces moments agréables passés en votre compagnie resteront d'heureux souvenirs impérissables. En particulier, je remercie Yannick Lizé qui a accepté de partager le montage et qui, pour cette raison, a contribué à l'aboutissement de ce projet.

Sans l'excellent travail technique de Bertrand Gauvreau, ce projet n'aurait jamais pu être réalisé et je le remercie chaleureusement. Je remercie également Jonathan Robin et Guillaume Leblanc pour leur expertise technique très appréciée.

Je tiens à souligner la contribution du Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG), le fond EMPOWR, la compagnie *ITF Technologies optiques* et l'Institut canadien pour les innovations en photonique (ICIP) pour leur soutien financier.

Un remerciement spécial à mon père qui m'a toujours encouragé et prodigué les meilleurs conseils qu'un père puisse donner. Merci à ma mère et à ma grand-mère pour m'avoir donné autant d'amour. Finalement, merci à Jacynthe pour m'avoir montré ce qui est essentiel dans la vie et pour avoir su me rendre heureux.

1 — Préliminaires

Dans ce chapitre, nous commençons par faire un bref survol de la cryptographie classique dans le but de motiver les efforts mis dans le développement de la cryptographie quantique. Par la suite, nous introduisons le concept de qubit ainsi que les outils nécessaires à la compréhension des deux principaux protocoles de cryptographie quantique, soit les protocoles BB84 et EPR. Finalement, nous exposons les outils nécessaires à l'analyse de la sécurité et de la performance de ces protocoles. Ces outils seront utilisés au chapitre quatre.

Une excellent revue du domaine de la cryptographie quantique est faite dans la référence [36].

1.1. Cryptographie classique

L'objectif traditionnel de la cryptographie est de développer et d'étudier des méthodes permettant la transmission confidentielle d'information entre participants légitimes. Bien que le chiffrement des messages soit utilisé depuis fort longtemps, la première véritable formalisation mathématique de la sécurité cryptographique fut développée en 1949. En effet, c'est le célèbre informaticien Claude E. Shannon qui appliqua le premier la théorie de l'information (qu'il a inventée) au problème de la cryptographie à clé privée [67]. Vinrent en 1976 les premiers travaux qui menèrent à l'invention de la cryptographie à clé publique par Ralf Merkle [58], Whitfield Diffie et Martin Hellman [29], ce qui donna un véritable essor au domaine. Aujourd'hui, le champ d'application de la cryptographie s'est considérablement étendu, tant du côté classique que quantique, et on traite désormais de problèmes comme la mise-en-gage de bit (*Bit Commitment*), le tirage à pile ou face (*Coin Tossing*), l'authentification de messages quantiques, entre

autres. Dans les sous-sections qui suivent, nous décrivons brièvement la cryptographie à clé privée et à clé publique en mettant l'emphase sur les inconvénients qui sont surmontés par la cryptographie quantique.

1.1.1. Cryptographie à clé privée

Un protocole de cryptographie à clé privée peut être décrit de la façon suivante : Alice veut envoyer un message m à Bob en utilisant une chaîne de bits aléatoires et secrets qui constituent la clé k. Le protocole est équivalent à utiliser un coffre-fort : Alice cache le message dans le coffre en utilisant la clé, et seul Bob peut l'ouvrir car il est le seul autre à posséder la même clé. L'exemple le plus simple de protocole à clé privée est probablement le masque jetable (*one-time-pad*) inventé par Gilbert Vernam en 1926 [81] et qui est défini comme suit ; Alice veut communiquer à Bob le message m. Elle possède une clé k, de même longueur que m, qui est secrète et partagée avec Bob. Alice obtient le cryptogramme $C_k(m)$ en additionnant bit à bit modulo 2 le message et la clé, c'est-à-dire $C_k(m) = m \oplus k$. Sur réception du cryptogramme, Bob obtient le message en faisant la même opération, soit $C_k(m) \oplus k = m \oplus k \oplus k = m$. Comme la clé est complètement aléatoire, chaque bit du cryptogramme l'est aussi. Il est alors facile de montrer que ce système est inconditionnellement sécuritaire au sens donné par Shannon [67], ce qui implique que la connaissance du cryptogramme ne révèle aucune information supplémentaire sur le message. Quoique parfaitement sécuritaire, ce système fait face à deux problèmes sérieux. Premièrement, la clé ne peut être réutilisée avec un message différent sans pénaliser sérieusement la sécurité du protocole puisque deux cryptogrammes chiffrés avec la même clé permettent d'obtenir la somme des deux messages ; $C_k(m_1) \oplus C_k(m_2) = m_1 \oplus m_2$. Un bit secret est donc nécessaire pour chiffrer chaque bit du message. Deuxièmement, la génération de la clé secrète ne peut être réalisée de façon sécuritaire autrement que par des moyens conventionnels comme une rencontre préalable entre Alice et Bob, ou encore, par l'utilisation d'un messager honnête. Dans les deux cas, l'implantation sur grande distance et pour un grand nombre de participants demande trop de ressources et la sécurité serait difficile à garantir. Nous verrons dans la section 1.3 que cette

difficulté est surmontée par la cryptographie quantique qui permet, par une utilisation astucieuse de la mécanique quantique, de générer à distance une clé secrète avec une sécurité garantie, d'où l'intérêt de cette discipline.

1.1.2. Cryptographie à clé publique

La cryptographie à clé publique diffère de celle à clé privée par le fait qu'elle utilise une clé publiquement connue pour le chiffrement et une clé secrète pour le déchiffrement. L'analogie est une boîte postale ; tout le monde peut y déposer une lettre avec la clé publique, mais uniquement le facteur possédant la clé privée peut l'ouvrir. Ce type de protocole est facilement implantable à grande échelle puisqu'il ne nécessite pas d'échange de clé secrète. Illustrons le principe avec le protocole RSA, inventé par R. Rivest, A. Shamir et L. Adleman en 1978 [64]. Il s'agit du premier véritable protocole à clé publique et qui est, notons-le, grandement utilisé sur le réseau Internet. Dans RSA, Alice choisit au hasard deux entiers premiers, impairs, distincts et secrets, p et q. Ces deux nombres servent à obtenir la clé publique de chiffrement en calculant le produit $n = pq$. Sans s'intéresser au fonctionnement précis du protocole, notons que le fait de factoriser n en ses deux facteurs premiers (cette décomposition étant unique) permet de briser le chiffrement. La sécurité du protocole repose sur la conviction que la factorisation d'un nombre en ses facteurs premiers ne peut se faire qu'en temps exponentiel en terme de la taille binaire du nombre à factoriser [74]. Inversement, nous savons que si p et q sont connus, le calcul du produit $pq = n$ se fait en temps polynomial. Il est donc facile de calculer la clé publique à partir de la clé secrète, mais l'inverse prendrait un temps qui atteint rapidement l'âge connu de l'Univers à mesure que n grandit ! Donc, contrairement à la cryptographie à clé privée, la sécurité des protocoles à clé publique est basée sur la théorie de la complexité du calcul et non pas sur la théorie de l'information.

Malheureusement, l'absence d'une preuve que le factorisation peut se faire en temps exponentiel rend le protocole non garanti d'être sécuritaire. Tous les protocoles basés sur la complexité du calcul sont également sans garantie de sécurité. Compte tenu de la nature imprévisible des découvertes scientifiques, cela s'impose

comme une grande menace envers la sécurité des protocoles. Cependant, cette menace n'est pas aussi importante que celle découverte par Peter Shor en 1994. En effet, il a montré qu'avec l'aide d'un ordinateur quantique il est possible de calculer en temps polynomial les facteurs premiers d'un entier, permettant ainsi de briser facilement RSA [68] quelle que soit la taille de la clé secrète. Avec cette découverte, on pourrait penser qu'un protocole de chiffrement qui est à la fois sécuritaire et implantable sur un réseau de communication à grande échelle semble impossible à réaliser. Heureusement, cela n'est pas le cas si on se dote du même outil que Shor. En effet, nous verrons dans ce mémoire que la cryptographie quantique apporte une solution à ce problème.

1.1.3. Authentification

Pour assurer la confidentialité et l'intégrité du message, ce dernier doit également être authentifié par un protocole approprié. Un protocole d'authentification permet au récepteur d'être convaincu que, d'une part, le message a été envoyé par l'émetteur légitime, et d'autre part, qu'il n'a pas été modifié en chemin par un espion potentiel. L'absence d'authentification permet une attaque du type « usurpation » où l'espion n'a qu'à intercepter et modifier à son avantage toutes les communications entre Alice et Bob. Par exemple, cette attaque permet facilement de briser un protocole de chiffrement à clé publique car la clé aurait pu être générée par l'espion. Heureusement, l'authentification classique est possible si Alice et Bob partagent une clé secrète de longueur $\log m$, où m est la longueur du message à authentifier. Plusieurs protocoles inconditionnellement sécuritaires et quasi optimaux existent [25]. En cryptographie quantique, l'authentification de la partie classique de la communication est également obligatoire si on désire obtenir un protocole parfaitement sécuritaire. Notons finalement que l'authentification de messages quantiques (qubits) est également possible [7], mais qu'il n'est pas nécessaire d'authentifier la partie quantique de la communication pour faire de la cryptographie quantique.

Introduisons ici un outil qui nous sera très utile, le canal public. Un canal public est une idéalisation d'un canal où toutes les communications qui y transitent ne

peuvent être modifiées. Par exemple, le journal ou la télévision seraient des canaux publics. Notons que, dans ce mémoire, nous ne traitons pas d'authentification, malgré son importance cruciale.

1.2. Quelques propriétés de l'information quantique

Dans le but d'obtenir un protocole sécuritaire de génération de clé, un changement de paradigme s'impose. Dans cette section, nous énonçons d'abord trois des postulats de la mécanique quantique dans le cas particulier du qubit et nous discutons de leur importance en cryptographie quantique (CQ).[1] Nous étudions ensuite les conséquences de l'encodage quantique de l'information, ce que nous appelons l'information quantique. Nous discutons finalement des propriétés surprenantes de l'information quantique qui lui permettent de réaliser ce qui est impossible classiquement.

1.2.1. Le qubit

État

La génération inconditionnellement sécuritaire de clés secrètes à grande distance n'est pas possible par l'échange de bits classiques, mais l'est par l'échange de *bits quantiques* (communément appelé *qubit*). Mais qu'est-ce qu'un qubit ? Un qubit est une description générique d'un système quantique dont une observable (au sens donné par la mécanique quantique [27]) possède deux niveaux accessibles (et nécessairement orthogonaux) que nous désignons par $|0\rangle$ et $|1\rangle$. Ces deux niveaux font partie d'une base orthonormée. En général, la dimension de cette base peut être supérieure à deux, voire même infinie. Cependant, les conditions expérimentales sont telles que seuls ces deux états sont accessibles. Par exemple, l'état du spin de l'électron dans un champ magnétique aligné selon z pourrait constituer un qubit avec les états de base $|\uparrow\rangle_z \equiv |0\rangle$ et $|\downarrow\rangle_z \equiv |1\rangle$. Parfois, il faut ignorer certains degrés de liberté. C'est le cas du photon, où l'on peut encoder un qubit dans sa polarisation en ignorant le nombre d'onde. Dans ce chapitre, nous

[1] Nous ne discutons pas des autres postulats et nous les supposons connus par le lecteur.

ne nous soucierons pas de l'observable associée à l'état, nous nous concentrerons plutôt sur l'état lui-même. Par conséquent, la phrase « mesurer l'état $|\psi\rangle$ » signifiera « mesurer l'observable représentée par l'état $|\psi\rangle$ ». L'espace de Hilbert d'un qubit est donc de dimension deux (que nous notons $\mathcal{H}_2$) et l'état du qubit correspond à un vecteur dans cet espace. L'état le plus général d'un qubit est décrit mathématiquement par une matrice densité, qui est présentée à la section 1.2.3. Un cas particulier de la matrice densité est un *état pur* qui s'exprime comme une superposition linéaire des états de la base générique $\{|0\rangle, |1\rangle\}$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{1.1}$$

où α, β sont complexes et satisfont à la condition de normalisation suivante :

$$|\alpha|^2 + |\beta|^2 = 1. \tag{1.2}$$

Cet énoncé est une reformulation, pour un qubit, du premier postulat de la mécanique quantique telle que décrit dans l'interprétation de Copenhague [27]. La première différence fondamentale avec le bit est donc la *superposition des états de base*. C'est le premier ingrédient nécessaire à la cryptographie quantique.

L'information quantique est évidemment un concept plus élaboré que ce que nous venons d'énoncer. Il est en effet possible d'étudier formellement les propriétés du codage de l'information dans un qubit et de définir l'entropie informationnelle associée à ce codage [82]. Cela permet, pour ne citer qu'un exemple, d'étudier ses propriétés lors de la transmission sur un canal quantique bruyant [65]. Ce concept est à la base de la théorie de l'information quantique qui est devenue aujourd'hui un domaine d'étude très vaste englobant la cryptographie quantique [61].

Dynamique

Une deuxième différence importante est la dynamique. Tel que le dicte le postulat d'évolution [27], la dynamique temporelle de l'état d'un qubit isolé $|\psi(t)\rangle$ est définie par l'observable associée à l'énergie du système, l'hamiltonien $\hat{H}(t)$, et par l'équation de Schrödinger :

$$i\hbar\frac{\mathrm{d}|\psi(t)\rangle}{\mathrm{d}t} = \hat{H}(t)|\psi(t)\rangle. \tag{1.3}$$

Étant donné l'état du qubit au temps $t = 0$, $|\psi(0)\rangle$, la solution formelle de l'équation 1.3, lorsque $\hat{H}$ ne dépend pas du temps, est donnée par :

$$|\psi(t)\rangle = \exp\left(-\frac{i}{\hbar}\hat{H}t\right)|\psi(0)\rangle \equiv \hat{U}(t,0)|\psi(0)\rangle, \tag{1.4}$$

où nous avons défini l'opérateur d'évolution temporelle $\hat{U}(t,0)$. Sachant que $\hat{H}$ est hermitique, on peut montrer que $\hat{U}$ doit être unitaire, c'est-à-dire que $\hat{U}\hat{U}^\dagger = \hat{U}^\dagger\hat{U} = \hat{I}$, où $\hat{I}$ est l'opérateur identité. Cela est nécessaire car $\hat{U}$ doit conserver la norme de $|\psi\rangle$. Dans toute base orthonormée de $\mathcal{H}_2$, et en particulier dans la base générique, la matrice unitaire associée à l'opérateur $\hat{U}$ peut toujours s'exprimer comme une combinaison linéaire des matrices de Pauli, $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$, et de la matrice identité $\hat{I}$:

$$\hat{U} = \hat{I}\cos\frac{\alpha}{2} - i\mathbf{n}\cdot\vec{\sigma}\sin\frac{\alpha}{2} = \exp(-i\alpha\mathbf{n}\cdot\vec{\sigma}/2), \tag{1.5}$$

où α est un angle réel. Le terme $\mathbf{n}\cdot\vec{\sigma}$ correspond à la matrice $n_x\hat{\sigma}_x + n_y\hat{\sigma}_y + n_z\hat{\sigma}_z$, où la norme du vecteur $\mathbf{n} = (n_x, n_y, n_z)$ est égale à un pour assurer l'unitarité. L'intérêt de ce développement est qu'en paramétrisant $|\psi\rangle$ de la façon suivante

$$|\psi\rangle \equiv |\psi(\theta,\varphi)\rangle = \mathrm{e}^{-i\varphi/2}\cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{i\varphi/2}\sin\frac{\theta}{2}|1\rangle, \tag{1.6}$$

on peut donner une représentation visuelle de l'effet de $\hat{U}$ sur $|\psi(\theta,\varphi)\rangle$. À $|\psi(\theta,\varphi)\rangle$ on associe un vecteur unitaire $\mathbf{s} = (s_x, s_y, s_z)$ faisant un angle longitudinal θ par rapport à l'axe z, ainsi qu'un angle azimutal φ par rapport à l'axe x dans le plan xy. Avec cette représentation, la transformation $\hat{U}$ appliquée à $|\psi(\theta,\varphi)\rangle$ correspond à une rotation de $\mathbf{s}$ d'un angle α autour du vecteur $\mathbf{n}$ (voir la figure 1.1). Pour cette raison, nous utiliserons la notation $\hat{U} = \mathcal{R}(\mathbf{n},\alpha)$ lorsque ce sera utile. Pour vérifier cette propriété, il suffit de constater que

$$\mathcal{R}(\hat{z},\alpha)|\psi(\theta,\varphi)\rangle = |\psi(\theta,\varphi+\alpha)\rangle \tag{1.7}$$

et que, par symétrie, ce doit aussi être vrai quels que soient les vecteurs $\mathbf{n}$ et $\mathbf{s}$. La sphère sur laquelle se déplace l'extrémité de $\mathbf{s}$ est nommée la *sphère de Bloch* et elle est formellement équivalente à la *sphère de Poincaré* utilisée pour représenter la polarisation de la lumière [23]. Notons au passage que l'équivalence entre $\hat{U}$ et une rotation dans $\mathbb{R}^3$ est une conséquence de l'homomorphisme des groupes SU(2) et O(3) [3].

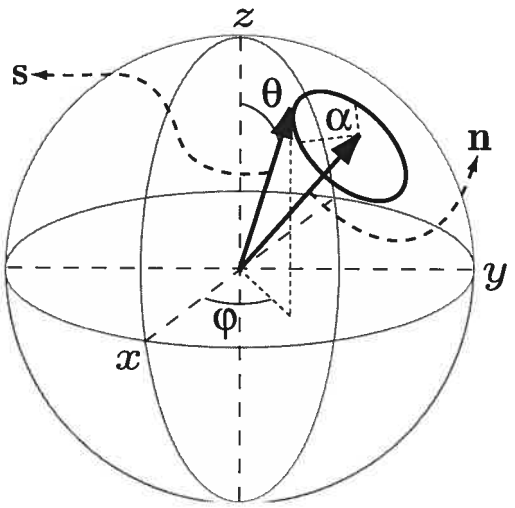

FIG. 1.1 – Sphère de Bloch. Les vecteurs **s** et **n** sont dessinés en rouge et vert respectivement.

Mesure

La description du processus de mesure de l'état d'un qubit nécessite l'ajout du postulat de la mesure [27]. La difficulté conceptuelle de ce postulat est qu'il décrit une dynamique non-unitaire probabiliste du vecteur d'état lorsque le qubit interagit avec un appareil de mesure « classique » mais qui, au fond, n'est qu'un assemblage d'un grand nombre de sous-systèmes quantiques. En effet, le postulat stipule que lorsqu'un appareil de mesure « classique » interagit avec le système quantique, il force ce dernier à être projeté sur un des états de base possibles avec la probabilité associée. Formellement, pour un état général $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, la mesure donnera le vecteur $|0\rangle$ avec une probabilité $|\alpha|^2$ ou bien $|1\rangle$ avec une probabilité $|\beta|^2$. L'effet de la mesure sur l'état est de le projeter sur le vecteur propre associé :

$$|\psi\rangle \rightarrow |\psi'\rangle = \frac{\hat{P}_n|\psi\rangle}{\sqrt{\langle\psi|\hat{P}_n|\psi\rangle}} \tag{1.8}$$

où $\hat{P}_n = |n\rangle\langle n|$ est le projecteur sur l'état $|n\rangle$, avec $n = 0$ ou 1. C'est ce qu'on appelle la *réduction du paquet d'onde.*

Lors d'une mesure, la dynamique est probabiliste et non-unitaire et il y a contradiction avec le postulat d'évolution. Discuter correctement de l'interaction entre l'appareil de mesure classique et le système quantique nécessite une modélisation. Comme nous l'avons mentionné, un appareil classique n'existe pas, il n'y a que des systèmes quantiques. Ce problème est étudié dans le cadre de la *décohérence* qui a été développée principalement par W. Zurek [85, 86]. Sans pouvoir expliquer pourquoi il y a réduction du paquet d'onde, la décohérence montre que l'interaction appareil-système détruit la superposition cohérente des états de base du système quantique. De plus, on y montre pourquoi la destruction de la superposition se fait exactement dans la base propre de l'observable en question, expliquant pourquoi nous n'observons pas de superposition quantique dans le monde classique. La décohérence nous montre aussi que l'information quantique est très fragile car le couplage inévitable avec l'environnement détruit l'encodage.

Finalement, en plus d'être étrange, le postulat de la mesure est le deuxième ingrédient nécessaire à la réalisation de la cryptographie quantique.

1.2.2. Intrication

Considérons maintenant l'état quantique de deux qubits. L'état du système conjoint s'écrit, d'une façon générale, comme un développement sur la base produit tensoriel des bases propres des deux qubits, soit $\{|b\rangle_1 \otimes |b'\rangle_2 \equiv |bb'\rangle\}$, où $b, b' \in \{0, 1\}$ et où l'indice est relatif au qubit respectif. On peut donc écrire l'état global $|\psi\rangle$ comme

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle, \tag{1.9}$$

où les coefficients complexes satisfont à la condition de normalisation. On montre sans trop de difficultés que si l'égalité $\alpha\delta = \beta\gamma$ n'est pas respectée, alors l'état global ne peut se factoriser en produit tensoriel des états individuels des deux qubits, $|\psi\rangle \neq |\psi_1\rangle|\psi_2\rangle$, auquel cas on dit que les deux qubits sont intriqués. Sinon, on dit que l'état est *séparable*. Par exemple, l'état $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ est un état intriqué. Physiquement, un tel état est obtenu en faisant interagir deux qubits indépendants via une certaine transformation unitaire $\hat{U}$ non-séparable agissant sur l'espace conjoint des qubits. L'état final est intriqué et constitue en quelque

sorte une signature du passé commun des qubits. Ce type d'état entraîne des corrélations qui peuvent paraître étranges *a priori*. Par exemple, toujours pour l'état $|\Phi^+\rangle$, la mesure de l'état du premier qubit projette l'état global sur $|bb\rangle$, où b est le résultat de la mesure. Nous avons donc projeté l'état du deuxième qubit sur celui du premier après la mesure sans l'avoir fait interagir directement avec l'appareil de mesure. C'est comme si le premier qubit avait communiqué le résultat de la mesure au deuxième, et ce, instantanément et indépendamment de la distance entre les deux qubits. Heureusement, cela ne viole pas le principe de relativité restreinte car le résultat de la mesure est aléatoire. On ne peut que réaliser la mesure sans décider de son résultat, ce qui est inutile pour communiquer de l'information. L'intrication permet plutôt de créer des mesures parfaitement corrélées, ce qui est d'une grande utilité pour la cryptographie quantique.

L'étrangeté de l'intrication a toujours dérangé Albert Einstein qui, dans un travail conjoint avec Boris Podolsky et Nathan Rosen, utilisa ce type d'état pour argumenter que la description quantique d'une réalité physique était incomplète, ce qui donna naissance aux théories quantiques locales à variables cachées et au paradoxe EPR [32].[2] Ce ne fut qu'en 1964 qu'une façon de trancher expérimentalement la question fut proposée avec les inégalités de Bell [8]. Le but de ces dernières est de démontrer que pour une certaine catégorie d'expériences, les prédictions faites par la mécanique quantique diffèrent de celles de toutes les théories locales à variables cachées. Dix-sept années plus tard, A. Aspect, P. Grangier et G. Roger ont réalisé l'expérience avec des photons intriqués et les prédictions de la mécanique quantique furent vérifiées [5]. On en conclut que la mécanique quantique est complète mais non-locale.

La notion d'intrication se généralise naturellement à plus de deux systèmes et ne se limite pas aux qubits. La classification et la mesure du niveau d'intrication constituent un champ d'étude du traitement de l'information quantique [39, 77].

[2]Une paire de particules intriquées est parfois nommée *paire EPR* pour cette raison.

1.2.3. Mélange statistique et matrice densité

L'état décrit par le premier postulat de la mécanique quantique n'est pas la description la plus générale possible. En effet, supposons que nous ayons en notre possession un qubit intriqué avec un autre qui nous est inaccessible. L'état intriqué est non-séparable, alors comment pouvons nous décrire l'état du qubit seul ? Cette description nécessite le concept de *mélange statistique*, que nous présentons ici sans motivation physique mais dont la signification est simple à comprendre. L'état le plus général d'un qubit est décrit par une *matrice densité* ρ qui peut s'écrire comme

$$\rho = \sum_{i=1}^{r} p_i |\psi_i\rangle\langle\psi_i| \quad \text{où} \quad 0 < p_i \leq 1 \quad \text{et} \quad \sum_{i=1}^{r} p_i = 1 \tag{1.10}$$

où les $|\psi_i\rangle$ correspondent à des vecteurs de $\mathcal{H}_2$ et r est le rang de la matrice. À la limite $r = 1$ on retrouve un *état pur* $\rho = |\psi\rangle\langle\psi|$ qui nous est déjà familier. On montre facilement que ρ est une matrice positive, $\langle\varphi|\rho|\varphi\rangle \geq 0 \ \forall |\varphi\rangle$, et que sa trace est égale à 1, $\mathrm{Tr}\{\rho\} = \sum_{i=0}^{1}\langle i|\rho|i\rangle = 1$.

Physiquement, un qubit dans l'état ρ signifie qu'il se trouve dans l'état $|\psi_i\rangle$ avec probabilité p_i. Par exemple, si Alice envoie à Bob un qubit dans l'état $|0\rangle$ avec probabilité p_0 ou dans l'état $|1\rangle$ avec probabilité p_1, mais ne dit pas à Bob quel est l'état envoyé, alors la meilleure description du qubit que Bob peut donner est $p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1|$. Supposons maintenant que le qubit envoyé soit intriqué avec un autre auquel Bob n'a pas accès et dont l'état conjoint s'écrit $\alpha_0|00\rangle + \alpha_1|11\rangle$ avec $|\alpha_i|^2 = p_i$. Si Alice mesure le qubit caché et envoie l'autre à Bob, alors la description de Bob est toujours $p_0|0\rangle\langle 0| + p_1|1\rangle\langle 1|$. Cela reste vrai même si Alice ne mesure pas la particule car les deux situations sont physiquement indiscernables pour Bob, à condition bien sûr que Bob n'ait pas d'information sur le qubit caché.

Formellement, pour un état pur à deux qubits possiblement intriqués $|\Psi\rangle$, la description du premier qubit s'obtient en appliquant une trace partielle sur l'espace du deuxième qubit, $\rho_1 = \mathrm{Tr}_2\{|\Psi\rangle\langle\Psi|\}$. En guise d'exemple, si $|\Psi\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, alors $\rho_1 = \frac{1}{2}\hat{I}_1$. Il s'agit d'un état maximalement mélangé.

Avec cette description générale, une adaptation des postulats est nécessaire. Se référer à [48, 62, 82] pour plus de détails.

1.2.4. Non-clonage, distinguabilité et perturbation

Rolf Landauer affirmait que l'information est physique. En fait, l'information est fondamentalement quantique, mais pour des systèmes macroscopiques, elle est équivalente à l'information classique en raison de la décohérence. Dans le monde classique, nous savons que l'information peut être copiée librement d'un système à un autre. Quantiquement, ce n'est plus le cas, comme l'ont montré en 1982 W.K. Wootters et W.H. Zurek [84] ainsi que D. Dieks [30]. Voyons comment cela est possible (ou impossible !). Soit $|\psi\rangle$ l'état arbitraire à copier, $|0\rangle$ l'état « blanc » sur lequel on veut copier $|\psi\rangle$, et $|S\rangle$ l'état des qubits supplémentaires de la machine servant à copier. On cherche une opération unitaire $\hat{U}_c$ réalisant la transformation suivante :

$$\hat{U}_c(|\psi\rangle|0\rangle|S\rangle) = |\psi\rangle|\psi\rangle|S_\psi\rangle, \tag{1.11}$$

où $|S_\psi\rangle$ est l'état global des qubits supplémentaires après la transformation, qui dépend de $|\psi\rangle$. Autrement dit, on aimerait que, pour tout état d'entrée $|\psi\rangle$, la sortie consiste en deux copies identiques du même état. La preuve d'impossibilité est simple. Lorsqu'on applique $\hat{U}_c$ sur les états de base, nous avons par définition

$$\hat{U}_c\left[|a\rangle|0\rangle|S\rangle\right] = |a\rangle|a\rangle|S_a\rangle \tag{1.12}$$

où $a = 0, 1$. Un tel opérateur existe et est unitaire. Maintenant, si on applique $\hat{U}_c$ à un état général $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, on obtient

$$\hat{U}_c|\psi\rangle|0\rangle|S\rangle = \alpha|0\rangle|0\rangle|S_0\rangle + \beta|1\rangle|1\rangle|S_1\rangle \tag{1.13}$$

$$\neq (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)|S_\psi\rangle, \tag{1.14}$$

ce qui montre qu'une machine à copier $\hat{U}_c$ ne peut être universelle car si elle peut copier les états de base, alors elle ne peut copier les superpositions de ces états. Ce résultat est l'essentiel du théorème de *non-clonage*. La preuve montrée ici n'est pas générale car elle ne permet pas à la machine d'utiliser des mesures, c'est-à-dire d'être non-unitaire. Ce problème est étudié dans la référence [19] où l'on montre que le théorème de non-clonage tient toujours.

Une autre propriété de l'information quantique nécessaire à la sécurité de la cryptographie quantique est l'impossibilité de distinguer parfaitement des états

non-orthogonaux. Prenons deux états non-orthogonaux $|\psi_1\rangle$ et $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\psi_1^\perp\rangle$, où $\langle\psi_1|\psi_1^\perp\rangle = 0$ et $|\beta| < 1$. Pour distinguer à coup sûr ces deux états, il faudrait que deux projecteurs $\hat{P}_1$ et $\hat{P}_2$ tels que $\hat{P}_i|\psi_j\rangle = \delta_{ij}|\psi_j\rangle$ puissent exister. Or, par définition, $\hat{P}_2|\psi_2\rangle = \beta\hat{P}_2|\psi_1^\perp\rangle$, d'où

$$\langle\psi_2|\hat{P}_2|\psi_2\rangle = |\beta|^2\langle\psi_1^\perp|\hat{P}_2|\psi_1^\perp\rangle \leq |\beta|^2 < 1, \tag{1.15}$$

ce qui contredit l'hypothèse de départ. Il est donc impossible de distinguer à coup sûr deux (ou plusieurs) états non-orthogonaux. Cependant, il est toujours possible de distinguer des états orthogonaux, auquel cas l'information est équivalente à l'information classique.

En 1992, C.H. Bennett, G. Brassard et N.D. Mermin ont poussé encore plus loin le résultat d'indiscernabilité que nous venons de voir en montrant qu'il est impossible de distinguer des états non-orthogonaux sans encourir une probabilité non nulle de les perturber [17]. Pour illustrer ce principe, considérons la situation où une observatrice Ève reçoit un qubit Q qui est soit dans l'état $|\psi_1\rangle$ avec probabilité $0 < p_1 < 1$, soit dans l'état $|\psi_2\rangle$ non-orthogonal à $|\psi_1\rangle$ avec la probabilité complémentaire. Ève possède un système quantique E dans l'état initial $|E\rangle$ et elle désire faire interagir E avec Q à l'aide de la transformation $\hat{U}$ de façon à distinguer le mieux possible $|\psi_1\rangle$ de $|\psi_2\rangle$ mais sans perturber l'état de Q. Concrètement, $\hat{U}$ doit agir de la façon suivante sur le système conjoint QE :

$$\hat{U}\left(|\psi_1\rangle|E\rangle\right) = |\psi_1\rangle|E'\rangle, \quad \hat{U}\left(|\psi_2\rangle|E\rangle\right) = |\psi_2\rangle|E''\rangle. \tag{1.16}$$

Pour distinguer à coup sûr les états $|\psi_1\rangle$ et $|\psi_2\rangle$, $|E'\rangle$ et $|E''\rangle$ doivent être orthogonaux, comme nous venons juste de le montrer. Cela n'est cependant pas nécessaire car il suffit seulement que $|E'\rangle$ et $|E''\rangle$ soit non parallèles pour donner de l'information partielle permettant de discerner $|\psi_1\rangle$ de $|\psi_2\rangle$. Comme $\hat{U}$ est unitaire, on a nécessairement

$$\begin{aligned}
\langle\psi_1|\psi_2\rangle\langle E'|E''\rangle &= \langle\psi_1, E'|\psi_2, E''\rangle && (1.17)\\
&= \langle\psi_1, E|\hat{U}^\dagger\hat{U}|\psi_2, E\rangle && (1.18)\\
&= \langle\psi_1|\psi_2\rangle\langle E|E\rangle, && (1.19)
\end{aligned}$$

d'où $|E'\rangle = |E''\rangle$, ce qui contredit l'hypothèse de départ car $\langle\psi_1|\psi_2\rangle \neq 0$. Ève n'obtient aucune information sur l'état du qubit Q car elle ne peut distinguer les deux états de son système E. Cela implique que toute stratégie permettant de distinguer l'état de Q choisi parmi un ensemble d'états non-orthogonaux perturbe inévitablement cet état avec une probabilité non nulle. Pour quantifier la sécurité de la cryptographie quantique, nous devons donc connaître la quantité maximale d'information qu'il est possible d'obtenir pour une perturbation minimale de l'état. La section 1.4 se penche sur ce problème.

La perturbation associée à l'obtention d'information est directement reliée au principe d'incertitude de Heisenberg. En effet, considérons deux observables de $\mathcal{H}_2$, $\hat{O}_1$ et $\hat{O}_2$, dont les vecteurs propres forment deux bases orthonormées. Si le produit scalaire de n'importe quel vecteur de la première base avec tout autre de la deuxième est égal à $1/\sqrt{2}$, alors ces deux bases sont linéairement dépendantes et sont dites *maximalement conjuguées*. Cette dépendance linéaire a pour conséquence que le commutateur de $\hat{O}_1$ avec $\hat{O}_2$ est non nul et que, par conséquent, on peut définir une relation d'incertitude entre les deux observables ; $\Delta\hat{O}_1\Delta\hat{O}_2 \geqslant \frac{|\langle[\hat{O}_1,\hat{O}_2]\rangle|}{2}$. Autrement dit, mesurer $\hat{O}_1$ perturbe les fluctuations statistiques de la valeur moyenne de $\hat{O}_2$, et vice-versa. La conclusion est que toute paire d'observables qui ne commutent pas peut être utilisée pour réaliser un protocole de cryptographie quantique.

En résumé, l'information quantique est équivalente à l'information classique lorsqu'on l'encode dans des états orthogonaux, auquel cas on peut librement distinguer et copier les différents états. Sinon, lorsque l'encodage est fait avec des états non orthogonaux, les propriétés classiques disparaissent, ce qui permet entre autres de faire de la cryptographie parfaitement confidentielle.

1.3. Protocoles quantiques de génération de clés

Dans cette section, nous décrivons en détail et de façon générique deux des principaux protocoles quantiques de génération de clé et discutons de leurs similitudes. Nous ne nous soucions pas du système physique sur lequel ces protocoles sont implantés.

La cryptographie quantique est née à la fin des années soixante avec les travaux de Stephen Wiesner qui restèrent, malheureusement, non publiés jusqu'en 1983 [83]. Wiesner avait trouvé comment la mécanique quantique permettait, en principe, de fabriquer une monnaie impossible à contrefaire. Le véritable coup d'envoi de la cryptographie quantique fut donné en 1979 lorsque Charles Bennett rencontra Gilles Brassard et le mit au courant des travaux de Wiesner. Cinq années plus tard, leurs travaux conjoints sur la génération quantique de clé cryptographique furent présentés à Bangalore à l'occasion d'une conférence [10]. C'était la naissance du protocole BB84.

Donnons tout d'abord un aperçu général de tout protocole de génération de clé secrète. Nous allons voir qu'il s'agit bien de protocoles de *génération* et non pas de *distribution* de clé. En effet, la clé est créée par le protocole car elle n'existe pas avant. Chaque protocole contient trois phases énumérées ci-dessous :

1. Transmission des qubits et réconciliation des bases.
2. Réconciliation des clés.
3. Distillation de secret.

Dans les deux sous-sections suivantes, nous détaillons la première phase pour les protocoles BB84 et EPR. Nous exposons ensuite les deux autres phases.

1.3.1. Protocole BB84

Le protocole BB84 tire profit du principe de superposition quantique en utilisant deux bases maximalement conjuguées que nous nommerons base rectilinéaire $B_+ = \{|0_+\rangle, |1_+\rangle\}$, et base diagonale $B_\times = \{|0_\times\rangle, |1_\times\rangle\}$. En fonction des états génériques $|0\rangle$ et $|1\rangle$, les états de B_+ et $B_\times$ s'écrivent comme suit :

$$\begin{aligned} |0_+\rangle = |0\rangle \quad , \quad |1_+\rangle = |1\rangle \\ |0_\times\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad , \quad |1_\times\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,. \end{aligned}$$

Le protocole débute avec Alice qui envoie un qubit dont l'état est choisi de façon aléatoire et secrète parmi les quatre états $|0_+\rangle, |1_+\rangle, |0_\times\rangle, |1_\times\rangle$. Sur réception du qubit, Bob désire identifier l'état, mais comme il ne connaît pas la base de

préparation, il choisit la base de mesure au hasard entre B_+ ou $B_\times$. Avec une probabilité 1/2, la base de mesure est compatible avec l'état envoyé, auquel cas le résultat de la mesure est déterministe. Sinon, le résultat de la mesure est complètement aléatoire. Après la mesure, Bob annonce publiquement[3] son choix de base. Si l'état envoyé fait partie de la base de mesure, alors Alice connaît nécessairement le résultat de Bob et lui dit de conserver ce résultat comme bit de clé en utilisant la convention $|b_+\rangle \rightarrow b$ et $|b_\times\rangle \rightarrow b'$, où b et $b' = 0$ ou 1. Sinon, elle dit à Bob de rejeter le résultat. Dans une situation sans erreurs expérimentales et sans espion, il faudra donc, en moyenne, transmettre $2N$ qubits pour générer une clé de N bits. La clé obtenue après la procédure décrite se nomme la *clé tamisée.*

1.3.2. Protocole EPR

En 1991, Artur Ekert proposa un protocole de génération de clé quantique qui, *a priori*, semblait différent de BB84 [33]. L'idée est d'utiliser des particules ou photons intriqués dans l'état $|\Phi^+\rangle$ pour générer à distance des mesures corrélées chez Alice et Bob. Initialement, Ekert proposa de tester la présence de l'espion en vérifiant que les corrélations des résultats violent les inégalités de Bell, s'assurant ainsi que les particules sont bien intriquées. L'année suivante, C.H. Bennett, G. Brassard et N.D. Mermin montrèrent que le protocole de Ekert, que nous appellerons *protocole EPR*, peut se réduire au protocole BB84 et que, par conséquent, la sécurité de l'un implique la sécurité de l'autre. Voici donc le protocole. Alice génère d'abord une paire de qubits intriqués dans l'état suivant :

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}\left([|0_+0_+\rangle + |1_+1_+\rangle\right] \\ &= \frac{1}{\sqrt{2}}\left[|0_\times 0_\times\rangle + |1_\times 1_\times\rangle\right]. \end{aligned} \tag{1.20}$$

Elle garde le premier qubit et envoie l'autre à Bob. Après la réception, Alice et Bob mesurent leur qubit respectif dans B_+ ou $B_\times$, en choisissant la base aléatoirement et indépendamment. Si les bases d'Alice et Bob sont les mêmes, alors ils ont obtenu le même résultat, sinon, les résultats sont statistiquement indépendants.

[3]Publiquement signifie « en utilisant un canal public ».

En comparant publiquement les bases de mesure, ils conservent le bit associé au résultat de la mesure si les bases sont les mêmes et le rejettent sinon.

Pour l'espion Ève, le qubit envoyé par Alice dans le protocole EPR est dans le même état que celui envoyé dans BB84, soit

$$\rho = \frac{1}{4}\left[|0_+\rangle\langle 0_+| + |1_+\rangle\langle 1_+| + |0_\times\rangle\langle 0_\times| + |1_\times\rangle\langle 1_\times|\right]. \tag{1.21}$$

Les deux protocoles sont donc physiquement indiscernables. Cependant, Alice n'est pas nécessairement la source des qubits reçus par Bob. En effet, Ève pourrait très bien être la source mais sans pour autant augmenter son information sur la clé. En effet, si les photons envoyés par Ève ne sont pas intriquées mais dans un état séparable, cela se détecte facilement dans les clés tamisées. Par exemple, si Ève envoie $|0_+0_+\rangle = \frac{1}{2}\left(|0_\times 0_\times\rangle + |0_\times 1_\times\rangle + |1_\times 0_\times\rangle + |1_\times 1_\times\rangle\right)$ et qu'Alice et Bob mesurent dans la base $B_\times$, alors les résultats des mesures ne sont pas corrélés. Une autre stratégie possible pour Ève serait d'intriquer les qubits envoyés avec un troisième qubit qu'elle conserverait et qui servirait de « sonde » (l'état $\frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right)$ serait un exemple). Or, on montre facilement que cela n'est pas possible sans se faire détecter [17]. Si Ève désire s'insérer comme étant la source des qubits, elle doit envoyer $|\Phi^+\rangle$, sinon sa présence sera révélée mais alors elle ne pourra rien apprendre sur la clé tamisée d'Alice et de Bob.

1.3.3. Réconciliation des clés

En raison des imperfections du montage ou de la présence éventuelle de l'espion, la clé tamisée obtenue par Bob sera différente de la clé d'Alice, ce qui la rend inutilisable. Une phase de *réconciliation des clés* (ou correction d'erreur) est donc nécessaire. En 1992, Bennett *et al.* [11] proposèrent un protocole simple de correction d'erreur que nous exposons ici. Tout d'abord, le taux d'erreur sur la clé tamisée est estimé en comparant publiquement une partie de celle-ci, les bits comparés sont ensuite jetés. Si la probabilité d'erreur par bit de clé tamisée est E, alors pour n bits sacrifiés, l'erreur relative sur l'estimation de E est $\sqrt{(1-E)/n}$. Il faut donc choisir n suffisamment grand pour estimer E avec un bon niveau de confiance. Décrivons maintenant l'algorithme. Brièvement, il consiste à comparer

les parités de sous-ensembles de bits et à chercher les erreurs lorsque ces parités diffèrent. Les étapes sont les suivantes :

1. Une permutation choisie aléatoirement est appliquée à la chaîne de bits de façon à uniformiser la distribution des erreurs.
2. Les clés sont divisées en sous-ensembles de p bits chacun et la parité de chaque sous-ensemble est publiquement comparée. S'il y a égalité, Alice et Bob rejettent un bit du sous-ensemble et passent au sous-ensemble suivant. Sinon, une recherche bisective est entreprise dans laquelle le sous-ensemble est divisé en deux nouveaux sous-ensembles de même dimension. La parité de la première moitié est comparée, et s'il y a égalité, un bit est rejeté et ils passent à la deuxième. Sinon, le bloc est de nouveau séparé en deux et la recherche continue jusqu'à ce que le bloc ne contienne que deux bits, auquel cas l'erreur est trouvée et les deux bits sont jetés.
3. Lorsque tous les sous-ensembles ont été examinés, ils recommencent les étapes 1 et 2 mais avec des sous-ensembles de p' bits, où p' n'est pas nécessairement égal à p.
4. Après avoir appliqué plusieurs fois les étapes 1, 2 et 3 de sorte que la probabilité qu'il reste plus de deux erreurs soit très faible, ils appliquent à répétition les étapes 1 et 2 en prenant p égal à la moitié de la taille de la chaîne restante. Cela leur permet de se convaincre que toutes les erreurs ont été éliminées.

Chaque comparaison de parité révèle à Ève un bit d'information sur la chaîne, ce qui nécessite le rejet d'un bit par Alice et Bob. En 1994, ce protocole a été modifié quelque peu et ses performances ont été analysées dans la référence [22]. Pour les besoins de ce mémoire, nous utilisons les résultats de la référence [76] où est présentée une analyse de la performance de *Cascade*. Sous quelques approximations valides lorsque la clé est suffisamment longue et que le taux d'erreur E est inférieur à 10%, les auteurs ont trouvé une borne inférieure au facteur de réduction moyen de la clé après correction d'erreur. Pour une clé tamisée de N bits avec un

taux d'erreur E, la taille de la clé réconciliée est donnée par $N' = f_c N$, où

$$f_c(E) = 1 + E\log_2 E - \frac{7}{2}E \tag{1.22}$$

est le facteur de réduction. La quantité de bits éliminés augmente très rapidement en fonction de E. Par exemple, on a $f_c(5\%) = 0{,}61$ et $f_c(10\%) = 0{,}32$.

Il est utile de comprendre l'effet de la correction d'erreur à l'aide de la théorie de l'information (voir l'annexe C). Soient A et B les variables aléatoires associées aux bits de clé d'Alice et de Bob lorsque la préparation et la mesure ont été faites dans la même base. Ces variables prennent les valeurs $a, b \in \{0, 1\}$ et sont liées par la distribution de probabilité P_{AB}. Avant la correction d'erreur, l'information mutuelle entre A et B est donnée par

$$I(A;B) = 1 + E\log_2 E + (1-E)\log_2(1-E). \tag{1.23}$$

Après la correction d'erreur, on a $I(A;B) = 1$ avec une très grande probabilité. En principe, si Alice et Bob pouvaient comparer leurs clés de façon confidentielle, alors le facteur de réduction de clé serait donné (dans la limite des très grandes clés) par l'équation 1.23. En pratique cela est impossible car la correction d'erreur est une discussion publique qui révèle de l'information à Ève. Néanmoins, on peut considérer l'équation 1.23 comme une borne supérieure à f_c.

Maintenant, supposons que la stratégie de l'espion lui permette d'obtenir l bits d'information de la clé de N bits d'Alice ou de Bob.[4] En moyenne, le processus de correction d'erreur diminue cette information par le facteur f_c lorsque les bits qu'Ève connaît sont éliminés. Cependant, nous adoptons ici une attitude conservatrice et supposons que l'information de l'espion n'est pas diminuée par le processus de correction d'erreur. Cette approximation est valide lorsque le taux d'erreur est faible.

1.3.4. Distillation de secret

L'information sur la clé corrigée que possède Ève est nuisible pour Alice et Bob car elle augmente ses chances de briser le chiffrement à clé privée utilisé avec

[4]Nous supposons, pour simplifier, que ces l bits sont déterministes et correspondent à la connaissance de l bits individuels, et non l bits de parité (voir [11]).

la clé obtenue. Pour régler ce problème, les auteurs de BB84, en collaboration avec Jean-Marc Robert, développèrent une technique permettant de diminuer à un niveau arbitrairement faible l'information de l'espion [15, 18]. Cette technique se nomme *distillation de secret* (*privacy amplification* en anglais) et nous allons la décrire brièvement en commençant par énoncer le théorème :

Théorème 1. *Soit k la clé corrigée, n sa longueur, et $l < n$ le nombre de bits individuels de k connus par l'espion. Si $h(k)$ est une fonction de hachage choisie uniformément parmi une classe appropriée de fonctions de n vers $n - l - s$ bits, $h : \{0,1\}^n \rightarrow \{0,1\}^{n-l-s}$, alors l'information espérée de l'espion sur $h(k)$ est réduite à $2^{-s}/\ln 2$ bit, où $0 < s < n - l$ est un facteur de sécurité arbitrairement choisi.*

Une fonction de hachage h est une fonction définie par $h : \{0,1\}^n \rightarrow \{0,1\}^{n'}$, où $n' < n$, et qui a la propriété que, pour un couple (x, y) de chaînes de n bits, la probabilité que $h(x) = h(y)$ est au plus $1/2^{n'}$ lorsque h est choisie aléatoirement. Pour le problème qui nous occupe, cette fonction de hachage est réalisée de la façon suivante : Alice et Bob choisissent publiquement et aléatoirement $n - l - s$ sous-ensembles de la clé corrigée et calculent leurs parités sans toutefois les révéler. Les parités constituent la nouvelle clé secrète. On peut alors définir le facteur de réduction causé par la distillation de secret, f_{ds}, comme suit :

$$f_{ds} = \frac{n - l - s}{n}. \tag{1.24}$$

Il est évident à ce point que si $l = n$, il est impossible d'obtenir une clé secrète car Ève possède autant d'information sur la clé d'Alice que Bob, auquel cas on a $f_{ds} = 0$. Notons cependant qu'il existe un technique nommée, en anglais, *advantage distillation*, et qui permet à Alice et Bob de s'en sortir quand même [54], mais nous n'en discuterons pas ici.

Pour s'assurer que l'information de l'espion est réduite à un niveau négligeable, Alice et Bob doivent être en mesure d'estimer correctement l en fonction du taux d'erreur E. Cela n'est pas un mince problème et nous allons en discuter à la section 1.4. De plus, le taux d'erreur sur la clé est attribuable en partie aux imperfections du montage et cette fraction est relativement facile à calculer. Par

contre, ne connaissant pas la stratégie de l'espion, il est nécessaire pour Alice et Bob de considérer que toute erreur sur la clé est causée par Ève et doivent appliquer la distillation de secret en prenant en considération le taux d'erreur total.

1.3.5. Réconciliation, distillation et authentification

Nous pouvons maintenant mettre en évidence le rôle de l'authentification. Comme nous l'avons mentionné, elle sert à prévenir des attaques du type « usurpation » lors de la transmission de qubits ou de messages classiques. Pour BB84, l'authentification des qubits n'est pas nécessaire. Cependant, toute communication classique associée à la correction d'erreur et à la distillation de secret doit être authentifiée. Donc, si Alice et Bob sont deux nouveaux utilisateurs de la cryptographie quantique, ils doivent authentifier les premières communications classiques, ce qui nécessite une clé secrète préalablement partagée. Une partie de la clé générée quantiquement est ensuite réinvestie dans l'authentification future. Par conséquent, la génération quantique de clé est en réalité un protocole de génération de clé arbitrairement longue à partir d'une clé de longueur finie [11].

1.4. Sécurité des protocoles de génération de clé

Dans cette section, nous montrons comment le protocole BB84 est sécuritaire contre deux types d'attaque.

1.4.1. Modèle de l'espion

En principe, on aimerait montrer que BB84 est sécuritaire contre un espion qui n'est limité que par les lois de la physique telles qu'on les connaît aujourd'hui. En pratique, on peut s'en tenir à des situations plus réalistes où l'espion est limité technologiquement, bien que l'intérêt d'une telle supposition soit discutable. En effet, si on désire remplacer RSA par BB84, alors il faut supposer que l'espion peut briser RSA, et donc qu'il a accès à une connaissance ou à une technologie très avancée comme un ordinateur quantique par exemple. Par conséquent, on

doit appliquer les mêmes conditions pour BB84.

1.4.2. Attaque Interception-renvoi *(I-R)*

Dans l'attaque *Interception-Renvoi*, ou I-R, Ève intercepte une fraction des qubits à la sortie du laboratoire d'Alice et tente de déterminer leur état en choisissant judicieusement sa mesure. Elle communique ensuite son résultat à son complice, Fred, lequel renvoie l'état correspondant directement dans le laboratoire de Bob (voir la figure 1.2).

FIG. 1.2 – Attaque Interception-Renvoi

Définissons la base de mesure d'Ève par les deux états orthogonaux $\{|e_0\rangle, |e_1\rangle\}$, où $|e_0\rangle = \alpha|0\rangle + \beta|1\rangle$ et $|e_1\rangle = \beta|0\rangle - \alpha|1\rangle$. Nous avons pris $\alpha, \beta \in \mathbb{R}$ sans perte de généralité. On désire calculer le gain d'information d'Ève ainsi que la probabilité que sa mesure cause une erreur dans la clé tamisée. Nous supposons que le montage d'Alice et de Bob est parfait et que la préparation et la mesure ont été faites dans la même base. Soient B et R les variables aléatoires correspondant respectivement au bit codé dans l'état envoyé par Alice et au résultat de la mesure d'Ève. La variable B prend les valeurs $b \in \{0, 1\}$ et R les valeurs $r \in \{|e_0\rangle, |e_1\rangle\}$. On calcule premièrement l'entropie sur B, $H(B)$, selon la formule suivante :

$$H(B) = \sum_r P[r] H(B|R = r), \tag{1.25}$$

où $P[r]$ est la probabilité d'obtenir l'état r, et $H(B|R = r)$ est l'entropie conditionnelle sur B ayant obtenu l'état r, qui est définie par

$$H(B|R = r) = -\sum_b P[b|r] \log_2 P[b|r]. \tag{1.26}$$

Les probabilités $P[b|r]$ se calculent en utilisant la règle de Bayes ([37]) :

$$P[b|r] = P[r|b] \frac{P[b]}{P[r]}. \tag{1.27}$$

En moyenne, Alice prépare aussi souvent des 0 que des 1, d'où $P[b] = 1/2$. Pour la même raison, $P[r] = 1/2$, d'où $P[b|r] = P[r|b]$. La probabilité $P[r|b]$ est facile à calculer si on fixe la base. Par exemple, si l'état envoyé est dans la base B_+, alors la probabilité de mesurer l'état $|e_0\rangle$ est donnée par le produit scalaire $P_+[|e_0\rangle|b] = |\langle b_+|e_0\rangle|^2$. Le calcul permet de trouver l'entropie en fonction de la base de préparation :

$$H_+(B) = -\alpha^2 \log_2 \alpha^2 - (1-\alpha^2)\log_2(1-\alpha^2) \tag{1.28}$$

$$H_\times(B) = -\frac{(\alpha+\beta)^2}{2}\log_2\frac{(\alpha+\beta)^2}{2} - \frac{(\alpha-\beta)^2}{2}\log_2\frac{(\alpha-\beta)^2}{2} \tag{1.29}$$

Le gain d'information I dans une base précise est donné par la différence entre l'entropie sur B avant la mesure, c'est-à-dire 1, et celle après la mesure, que nous venons de calculer. Donc, $I_+ = 1 - H_+(B)$ et $I_\times = 1 - H_\times(B)$. Comme Alice choisit la base de préparation au hasard avec une probabilité 1/2, le gain moyen d'information est donné par

$$I = \frac{I_+}{2} + \frac{I_\times}{2} \tag{1.30}$$

$$= 1 - \frac{H_+(B)}{2} - \frac{H_\times(B)}{2} \tag{1.31}$$

On montre facilement que I est maximisé à 0,5 bit pour $\alpha = 0$ et $1/\sqrt{2}$, ce qui correspond à espionner dans les bases B_+ et $B_\times$, respectivement. Dans cette situation, Ève réussit à identifier correctement l'état une fois sur deux et n'obtient aucune information le reste du temps. Si Fred renvoie toujours l'état identifié par Ève, elle se trompe 1 fois sur 2, auquel cas l'état cause une erreur chez Bob avec une probabilité 1/2. La probabilité que cette stratégie cause une erreur dans la clé tamisée est donc de 25% par tentative. Bien entendu, Fred ne devrait pas toujours renvoyer l'état dans une seule base, car Bob pourrait facilement s'en rendre compte.

Une autre stratégie, dont l'intérêt sera expliqué plus loin, est de minimiser I. On montre facilement que cela est possible pour $\alpha = \cos(\pi/8)$, ce qui correspond à un gain $I \approx 0{,}399$ bit, mais toujours avec une probabilité d'erreur induite de 25% par tentative. Cette base d'espionnage, appelée la base de *Breidbart* [12],

est située à mi-chemin entre les bases B_+ et $B_\times$. Dans cette base, l'information d'Ève est probabiliste, car elle identifie le bit avec une probabilité $\cos^2(\pi/8) \approx 85\%$ à chaque mesure. *A priori*, maximiser I sur la clé tamisée semble être la meilleure stratégie. Cependant, Ève désire plutôt maximiser son information sur la clé finale, après la distillation de secret. Ce point est très subtil car le théorème de distillation de secret tel que nous l'avons décrit s'applique lorsque l'information d'Ève est déterministe et non probabiliste. Pour régler ce problème, Bennett *et al.* on montré qu'en tenant compte de la distillation de secret, connaître un bit de la clé tamisée avec une probabilité de 85% (résultat obtenu en espionnant dans la base de Briedbart) est équivalent à posséder une information déterministe de $1/\sqrt{2}$ bit (par bit de clé tamisée), comparativement à 0,5 bit avec l'autre stratégie [11]. Par conséquent, pour un taux d'erreur E, l'information moyenne obtenue par l'adversaire est donnée par

$$\tilde{I}_{\mathrm{IR}} = \frac{4E}{\sqrt{2}}, \tag{1.32}$$

où le tilde nous rappelle qu'il s'agit d'une moyenne, valide dans la limite des grandes clés. Pour une petite clé tamisée, il faudrait tenir compte des fluctuations statistiques de I_{IR} [11], ce que nous ne ferons pas ici.

1.4.3. Attaque Séparation du nombre de photons *(SNP)*

Cette attaque n'est possible que pour un système utilisant les photons, ce qui nécessite le rappel de quelques notions préalables sur les sources laser. À l'annexe A, on affirme qu'une source de lumière cohérente a une statistique de photons poissonnienne. Ces sources laser sont fiables, disponibles commercialement et peuvent êtres utilisées pour réaliser BB84 comme nous le verrons au chapitre 2. Cependant, l'utilisation de ces sources cause une brèche dans la sécurité qui, selon les capacités technologiques de l'espion, peut être sévère ou non. L'attaque *séparation du nombre de photons* (SNP) [21] profite directement de cette brèche. Une étude plus complète que celle présentée ici est faite dans la référence [51].

Rappelons d'abord (voir l'annexe A) que la distribution du nombre de photons

dans une impulsion, n, est poissonnienne :

$$\mathcal{P}_\mu(n) = \frac{\mu^n \mathrm{e}^{-\mu}}{n!}, \tag{1.33}$$

où μ est le nombre moyen de photons par impulsion.

Dans l'attaque SNP, on suppose qu'Ève n'est limitée que par les lois de la physique. En particulier, on lui donne la possibilité de réaliser une mesure dite *non destructive*[5] du nombre de photons dans l'impulsion, sans toutefois modifier l'observable dans laquelle le qubit de BB84 est codé. Ce type de mesure est possible en principe [66], mais nécessite une interaction non-linéaire de type Kerr ou un processus paramétrique de second-ordre ayant une efficacité de 100% au niveau du photon individuel, ce qui est loin d'être possible actuellement. Ce n'est pas tout ! Ève doit également être capable de réaliser une interaction dite « séparation du nombre de photons », (SNP), qui consiste à séparer de façon déterministe un des photons de l'impulsion [50]. Elle doit aussi posséder un canal de transmission sans pertes. Un tel canal pourrait être réalisé, par exemple, par la téléportation quantique [14]. La dernière condition, et non la moindre, est qu'Ève possède une mémoire quantique de durée arbitrairement longue. Encore une fois, cela est actuellement hors de portée, mais les lois de la physique ne l'interdisent pas !

Dotée de ces outils, l'attaque suivante devient possible :

1. À la sortie du laboratoire d'Alice, Ève détermine le nombre de photons dans l'impulsion à l'aide d'une mesure non-destructive.
2. Si le nombre de photons est supérieur à 1, elle en conserve un à l'aide de l'interaction SNP et téléporte les autres à l'entrée du laboratoire de Bob. Sinon, elle a deux possibilités. Soit qu'elle téléporte simplement le photon à l'entrée de Bob, soit qu'elle applique l'attaque I-R et passe ensuite à l'impulsion suivante.
3. Ève conserve le photon séparé dans sa mémoire quantique jusqu'à l'annonce publique de la base de préparation.
4. Connaissant la base de préparation du photon, Ève mesure son état et découvre la valeur du bit d'Alice à coup sûr.

[5] *Quantum non-demolition measurement*, en anglais.

Donc, lorsque l'impulsion contient deux photons ou plus, le gain d'information est de 1 bit pour une probabilité d'erreur induite égale à 0. Sinon, le gain est celui de l'attaque I-R, avec une probabilité d'erreur induite de 1/4. Faisons ici une analyse approximative dans le but de trouver l'information que cette attaque peut donner. À la sortie d'Alice, Ève applique l'attaque SNP sur toutes les impulsions de deux photons et ne laisse passer qu'une fraction f des impulsions à 1 photon, où f est à déterminer. Cela est possible car la transmission du lien entre Alice et Bob n'est pas parfaite, ce qui donne la liberté à Ève de choisir quelles impulsions atteindront le laboratoire de Bob. Pour simplifier l'analyse, nous négligeons les impulsions à trois photons ou plus, ce qui est valide dans la limite où $\mu \ll 1$. Pour acheminer les photons vers Bob, Ève possède un canal sans pertes. Un tel canal pourrait être réalisé, par exemple, par la téléportation quantique [14]. Les impulsions à un photon ainsi obtenues sont injectées dans le laboratoire de Bob. Notons que Bob ne reçoit aucune impulsion contenant plus de un photon, mais en supposant que ses détecteurs sont incapables de résoudre le nombre de photons, comme c'est souvent le cas, alors il ne s'en rendra jamais compte.

Pour assurer le succès de l'attaque, Ève ne doit pas modifier la probabilité que Bob mesure un compte réel, ce qui nécessite une analyse poussée. À cette fin, introduisons η, le rendement des détecteurs de Bob, ainsi T_B, la transmission de son appareil d'analyse qui correspond aux pertes des composants optiques de son système. Lorsque Ève applique l'attaque SNP, la probabilité d'obtenir un compte chez Bob est donnée par

$$p_c^{(\mathrm{SNP})} = \eta T_B \left[f\mathcal{P}_\mu(1) + \mathcal{P}_\mu(2)\right] \tag{1.34}$$

$$= \eta T_B \mu \mathrm{e}^{-\mu} \left[f + \frac{\mu}{2}\right], \tag{1.35}$$

Si Ève n'applique aucune attaque, en tenant compte de la transmission T_l du lien optique entre Alice et Bob et en négligeant les impulsions à plus de trois photons, cette même probabilité est donnée par

$$p_c = \mathcal{P}_\mu(1)\eta T_B T_l + \mathcal{P}_\mu(2)\left[1 - (1 - \eta T_B T_l)^2\right] \tag{1.36}$$

$$= \eta T_B T_l \mu \mathrm{e}^{-\mu} + \frac{\mu^2}{2}\mathrm{e}^{-\mu}\left[1 - (1 - \eta T_B T_l)^2\right]. \tag{1.37}$$

En posant $p_c^{(\mathrm{SNP})} = p_c$, on trouve la valeur de f :

$$f = T\left(1 + \mu - \frac{\mu\eta T_B T_l}{2}\right) - \frac{\mu}{2} \tag{1.38}$$

Si $f = 0$, tous les photons reçus chez Bob proviennent d'impulsions multi-photons et Ève obtient toute l'information. La transmission minimale $T_{\min}$ où cette condition est atteinte est :

$$T_{\min} = \frac{1 + \mu - \sqrt{1 + 2\mu + (1 - T_B\eta)\mu^2}}{\eta\mu T_B}. \tag{1.39}$$

En écrivant $T_l = 10^{-(\alpha l + c)/10}$, où α est l'atténuation du lien en dB/km, l sa longueur en km et c les pertes constantes en dB, alors on peut trouver la distance maximale $l_{\max}$ sur laquelle le système est sécuritaire contre l'attaque SNP :

$$l_{\max} = \frac{-10}{\alpha}\log T_{\min} - \frac{c}{\alpha}. \tag{1.40}$$

Pour $\mu = 0{,}1$, $\eta = 0{,}1$, $\alpha = 0{,}22$ dB/km, $c = 0{,}5$ dB et $T_B = -3{,}5$ dB, qui sont des valeurs typiques pour notre montage, on trouve $l_{\max} \approx 56$ km. Cette distance est, notons-le, indépendante du taux de bruit des détecteurs.

Maintenant, pour une valeur de $f \geq 0$ fixée par les paramètres du montage, Ève espionne chaque impulsion avec l'attaque SNP avec une probabilité $\mu/2$ et avec l'attaque I-R avec une probabilité f. Le nombre d'impulsions reçues chez Bob est donné par $\mu/2 + f$. En tenant compte de ces valeurs, on trouve que l'information moyenne obtenue $\tilde{I}_{\mathrm{SNP}}$ pour chaque impulsion non-vide est

$$\tilde{I}_{\mathrm{SNP}} = \frac{1}{f + \mu/2}\left(\frac{\mu}{2} + \frac{f}{\sqrt{2}}\right), \tag{1.41}$$

pour un taux d'erreur induit E_{SNP} de

$$E_{\mathrm{SNP}} = \frac{1}{4}\frac{f}{f + \mu/2}. \tag{1.42}$$

Ce dernier diminue à mesure que f diminue, car la proportion d'impulsions sur lesquelles l'attaque I-R est appliquée diminue. Dans la limite où $f = 0$, le système est brisé.

Finalement, remarquons que si la statistique de photons n'est pas modifiée par l'attaque SNP lorsque Alice et Bob utilisent la même base, cela n'est pas

vrai dans le cas contraire. En effet, comme Ève n'envoie pas d'impulsions à deux photons, la probabilité de mesurer une coïncidence aux deux détecteurs de Bob est diminuée, et cette diminution dépend directement du taux de bruit du détecteur. Une analyse plus poussée est nécessaire pour déterminer l'impact de cet effet secondaire. Néanmoins, cela nous rappelle que dans un système de cryptographie quantique complet, il est impératif de mesurer la statistique de photons chez Bob, d'où l'urgence de créer des détecteurs efficaces et capables de faire la résolution du nombre de photons.

1.4.4. Information en fonction du taux d'erreur

Les deux attaques présentées ne tiennent pas compte du bruit des détecteurs. En principe, le bruit aide l'espion, car il camoufle les erreurs qu'il introduit. Un calcul plus complet permettrait d'en tenir compte, ce que nous n'avons pas fait ici. Cependant, l'effet le plus néfaste du bruit est que les erreurs qu'il induit doivent être considérées comme des erreurs causées par l'espion, ce qui a pour effet de diminuer grandement le taux de génération de clé. En tenant compte de cela, nous allons considérer que pour un taux d'erreur moyen E, l'information moyenne par bit de clé tamisée obtenue par l'espion est donnée par

$$\tilde{I} = 4E/\sqrt{2} + \frac{\mu}{2f + \mu}, \tag{1.43}$$

où le premier terme correspond à l'attaque I-R, et le deuxième terme (qui est constant) correspond à l'attaque SNP. Notons que ce gain d'information peut être supérieur au résultat de l'équation 1.41 si le bruit des détecteurs est très grand.

1.4.5. Tolérance du taux d'erreur

Armé de ces outils, nous sommes en mesure de déterminer le taux d'erreur maximalement tolérable en supposant que les protocoles de correction d'erreur et de distillation de secret sont parfaits. Selon le théorème de distillation de secret énoncé à la section 1.3, la génération de clé devient impossible si Ève possède autant ou plus d'information sur la clé tamisée d'Alice que Bob. Soient $I(\alpha;\beta)$ et $I(\alpha;\epsilon)$, l'information mutuelle sur chaque bit de clé tamisée entre Alice et Bob

et entre Alice et Ève, respectivement. Ces quantités permettent de définir une condition simple permettant d'assurer la sécurité de l'implémentation :

$$I(\alpha;\beta) > I(\alpha;\epsilon) \Longrightarrow \text{Implémentation sécuritaire} \tag{1.44}$$

Comme l'information mutuelle entre Alice et Bob est donnée par l'équation 1.23 et celle d'Ève par l'équation 1.43, alors on peut trouver le taux d'erreur maximalement tolérable en posant l'égalité des deux expressions. En particulier, on peut trouver une borne maximale en posant $f = 1$, signifiant qu'Ève renvoie toutes les impulsions à 1 photon qu'elle intercepte. En utilisant les mêmes valeurs que pour le calcul de $l_{\max}$ (équ. 1.40), on calcule que $E_{\max} = 13{,}5\%$.

1.4.6. Preuve complète de sécurité

Les deux attaques que nous avons décrites n'ont pas la prétention d'être optimales et ne constituent pas une démonstration générale de la sécurité de BB84. Elles font partie d'une catégorie d'attaques dites « individuelles » où l'on permet à l'espion de manipuler les qubits individuellement uniquement. Les attaques dites « cohérentes » correspondent à la situation où l'espion manipule simultanément un grand nombre de qubits de façon cohérente. Des preuves tentant d'inclure cette possibilité existent, mais il est hors de notre portée de les présenter ici. Contentons-nous simplement de mentionner que, depuis 1998, plusieurs preuves ont été proposées [56, 49, 13, 69]. En particulier, la preuve de H. Inamori, N. Lütkenhaus et D. Mayers (2001) affirme qu'il est possible d'implanter BB84 de façon sécuritaire même si le montage comporte certaines imperfections, en l'occurrence une transmission inférieure à 1, des détecteurs inefficaces et bruyants et une source émettant des impulsions multi-photons [42]. Ils supposent cependant qu'Alice est en parfait contrôle de la source mais que les détecteurs de Bob ont un bruit et un rendement inconnus et possiblement sous le contrôle de l'espion. En 2003, M. Koashi et J. Preskill ont démontré que dans la situation où la source n'est pas caractérisée mais que les détecteurs sont parfaits, alors BB84 est toujours réalisable de façon sécuritaire [44]. Une preuve englobant les deux situations n'est, au meilleur de notre connaissance, toujours pas connue.

2 — Cryptographie quantique expérimentale sur fibre optique

La lumière est présentement la meilleure façon d'encoder les qubits dans le but de réaliser un protocole de cryptographie quantique (CQ). Dans ce chapitre, nous discutons d'abord de la faisabilité de la CQ sur fibre optique. Nous exposons ensuite le principe d'encodage en phase des qubits et discutons du montage *Plug&Play* utilisant ce principe. Finalement, nous montrons comment le multiplexage en longueur d'onde permet de réaliser un réseau optique à plusieurs utilisateurs supportant la CQ.

2.1. Fibre optique, composants optiques et cryptographie quantique

Dans cette section, nous survolons brièvement les principales propriétés de la fibre optique et discutons de leur influence sur la faisabilité de la cryptographie quantique. Nous ne discutons que de la fibre unimodale à 1550 nm avec cœur en silice (SiO_2).

Atténuation et guidage

La propriété de la fibre optique qui a le plus d'impact sur la faisabilité de la cryptographie quantique sur grande distance est son atténuation. L'atténuation provient de deux sources ; l'absorption et la diffusion. L'absorption est principalement causée par les modes de vibration des dipôles électriques de la silice et elle domine complètement le spectre d'atténuation en longueur d'onde à plus de 1600 nm. À moins de 1500 nm, c'est la diffusion Rayleigh qui varie selon λ^{-4} qui est la principale source d'atténuation. La zone d'atténuation minimale entre 1500 et 1600 nm est donc la plage de longueur d'onde de prédilection pour la CQ. L'atténuation minimale de la fibre SMF-28 (*Corning*) est de 0,19 dB/km à 1550 nm, ce qui est très près de la limite théorique de 0,18 dB/km [26]. Cette limite

théorique intrinsèque est fixée par la diffusion Rayleigh qui est une conséquence de l'inhomogénéité de l'indice de réfraction à l'échelle microscopique en raison de la nature moléculaire de la silice [70]. Elle est donc inévitable dans la silice.

L'autre propriété clé de la fibre est le guidage de la lumière [70]. Rappelons brièvement la structure de la fibre optique. Le cœur de silice, d'indice de réfraction n_c, est entouré de la gaine optique, d'indice $n_g < n_c$, avec $\Delta n = n_c - n_g \approx 5 \times 10^{-3}$ pour la fibre unimodale standard. La lumière est conduite dans le cœur par réflexion totale interne. Il est intéressant ici de noter l'analogie entre le puits

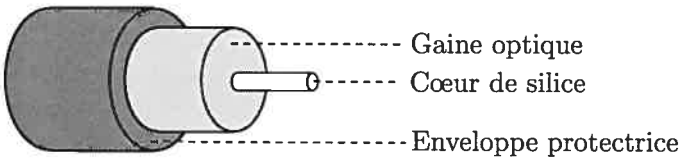

FIG. 2.1 – Structure de la fibre optique à saut d'indice.

de potentiel en mécanique quantique et le cœur de la fibre. En effet, il est possible de montrer que l'équation de propagation des ondes optiques dans la fibre est formellement identique à l'équation de Schrödinger pour une particule, mais avec un potentiel $V(r,\theta) = -\frac{n^2(r,\theta)}{2}$, où $n(r,\theta)$ est l'indice sur une section de la fibre [70]. Pour une fibre à saut d'indice (fig. 2.1), il y a quantification du vecteur d'onde, ce qui correspond aux différents modes de propagation ayant chacun leur propre distribution de champ électrique. Si Δn est suffisamment faible et si le diamètre du coeur est assez petit, un seul mode guidé existe et on dit que la fibre est unimodale. Dans ce cas, le vecteur d'onde est unique, la direction du champ électrique est perpendiculaire à la direction de propagation. De plus, la phase de l'onde entre le début et la fin de la fibre est proportionnelle à la distance entre les deux. Ces conditions sont nécessaires pour définir correctement la notion de qubit de polarisation et de phase dans la fibre (section 2.2) et elles permettent également de construire des interféromètres tout-fibre. Elles sont donc essentielles pour faire de la CQ sur fibre optique et seule la fibre unimodale peut-être utilisée.

Dispersion chromatique

Une impulsion optique limitée dans le temps est constituée d'une gamme de longueurs d'onde comme le stipule la relation d'incertitude $\Delta\nu\Delta t \geq 1/2$ qui découle du théorème de décomposition spectrale de Fourier (l'égalité est atteinte pour une impulsion gaussienne en prenant la définition de la variance pour $\Delta\nu$ et Δt). La dispersion chromatique est liée à la variation de la vitesse de phase résultant de la variation de l'indice de réfraction en fonction de la longueur d'onde. Son effet net est la modification de la largeur temporelle de l'impulsion optique avec la propagation. Or, cet effet est négligeable si la largeur spectrale de la source utilisée est suffisamment faible ou si la durée des impulsions est suffisamment longue, ce qui est le cas dans notre expérience.

Effets reliés à la polarisation

Premièrement, discutons des *pertes dépendantes de la polarisation* (nous utilisons l'acronyme PDL, dérivé de l'anglais). L'effet de la PDL sur un qubit de polarisation ne peut être décrit par une transformation unitaire mais plutôt par un superopérateur (voir [62]) car elle correspond à une absorption sélective [41]. Si elle fluctue, elle ne peut être compensée et doit être évitée. Heureusement, les fibres à symétrie circulaire ne souffrent généralement pas de PDL sauf dans le cas particulier où elles sont soumises à des pressions ou déformations mécaniques importantes. Notons cependant que certains composants comme les modulateurs de phase ont une PDL intrinsèque ce qui nécessite un contrôle de polarisation lors de leur utilisation.

Deuxièmement, la variation de la vitesse de phase en fonction de l'état de polarisation est ce qu'on appelle la *biréfringence*. Elle est causée par l'asymétrie de la fibre et par les contraintes résiduelles à l'intérieur et à l'extérieur du cœur. Pour les systèmes à fibre optique, elle est inévitable et fluctue statistiquement sur courte et sur grande distance en raison des perturbations mécaniques et thermiques [43]. Son effet sur la polarisation est équivalent à une transformation unitaire et peut donc être compensée.

Troisièmement, la dispersion du mode de polarisation (PMD) est causée par la différence de vitesse de groupe entre deux états de polarisation du mode fonda-

mental. Pour la fibre optique, les différences de vitesse de phase et de groupe sont approximativement égales, et tant que le délai introduit entre les deux modes de polarisation est inférieur au temps de cohérence de la source, la PMD est équivalente à la biréfringence. Si le délai est trop grand, alors les deux modes de polarisation sont découplés, et en terme de qubit de polarisation, il y a décohérence. Sous ces conditions, l'état de polarisation d'un photon passe d'un état pur à un mélange statistique. Heureusement, les sources utilisées dans cette expérience ont un temps de cohérence suffisamment long pour éviter cet effet.

Effets non-linéaires

La fibre optique possède une non-linéarité de troisième ordre non-nulle, ce qui induit plusieurs effets comme l'auto-modulation de phase, la modulation de phase mutuelle entre deux fréquences, les processus Raman de diffusion et de conversion de fréquence, la diffusion Brillouin ainsi que le mélange à quatre ondes [1]. Fort heureusement (ou malheureusement, selon le point de vue), ces effets sont très inefficaces et sont inexistants au niveau du photon individuel.

2.2. Cryptographie quantique par encodage en phase

Dans cette section, nous montrons d'abord comment il est possible d'encoder les états de BB84 en utilisant la phase de la lumière. Par la suite, nous expliquons les détails du montage *Plug&Play* que nous avons utilisé dans les expériences présentées dans ce mémoire, tout en mettant l'emphase sur ses avantages et ses inconvénients.

2.2.1. Encodage en phase

À sa publication, BB84 était décrit en utilisant la polarisation de photons individuels [10]. La toute première démonstration du principe (1989) fut d'ailleurs réalisée avec la polarisation et sur une distance de 30 cm à l'air libre [11]. Dans la fibre, ce choix d'encodage entraîne cependant des difficultés reliées aux fluctuations aléatoires de la biréfringence. Un système actif de compensation est nécessaire, ce qui réduit inévitablement le taux de génération de clé. Plusieurs groupes ont

démontré le principe d'encodage en polarisation dans la fibre [35, 59, 80].

La polarisation n'étant pas stable dans les fibres, il est naturel de se tourner vers la phase. Il y a cependant une subtilité. La phase absolue de la lumière (tout comme la phase absolue d'un état quantique quelconque) n'est pas une observable, ou du moins, la définir comme une observable entraîne des inconsistances (voir la section 10.7 de [53]). La phase est toujours relative à celle d'un autre faisceau et c'est de cette façon qu'il faut procéder. En 1992, C.H. Bennett proposa d'encoder les états de BB84 dans la phase relative des bras d'un interféromètre Mach-Zehnder [9]. Ce type d'interféromètre se fabrique facilement dans la fibre, mais nous verrons qu'il est difficile à stabiliser.

Pour illustrer le principe, considérons l'interféromètre Mach-Zehnder illustré à la figure 2.2. Alice possède une source produisant l'état à un photon $|1\rangle_0|0\rangle_1$,

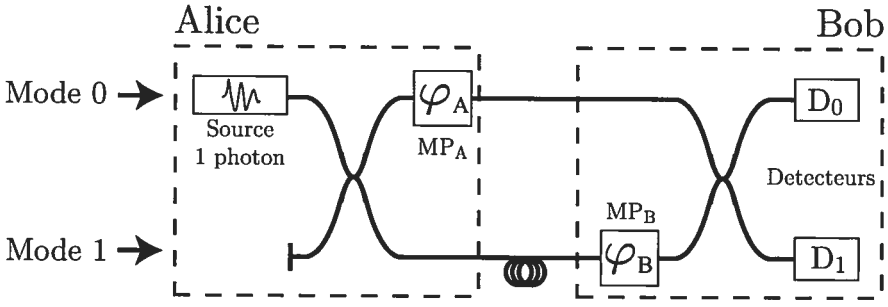

FIG. 2.2 – Interféromètre Mach-Zehnder pour encodage en phase de BB84.

écrit ici dans la base de Fock, où l'indice 0 se réfère au bras supérieur et l'indice 1 se réfère au bras inférieur (voir l'annexe A). On suppose que la polarisation est conservée du début à la fin et que la fibre est sans pertes.

Il faut trouver la transformation du coupleur sur l'état incident.[1] Pour ce faire, rappelons d'abord la transformation du coupleur sur l'amplitude complexe du champ électrique classique. Soit α_0 et α_1, les amplitudes complexes de vecteur d'onde k dans les modes 0 et 1 du coupleur d'entrée (voir la figure 2.2), ainsi que $\psi = (\alpha_0, \alpha_1)$, le vecteur colonne associé au champ total. L'effet du coupleur est

[1] Un coupleur est l'équivalent tout-fibre d'une lame séparatrice de faisceau.

défini par $\psi' = \underline{C}\psi$, où $\underline{C}$ est la matrice unitaire suivante ([53], section 10.9) :

$$\underline{C} = \begin{pmatrix} a\mathrm{e}^{i\varphi_0} & b\mathrm{e}^{i\varphi_1} \\ -b\mathrm{e}^{-i\varphi_1} & a\mathrm{e}^{-i\varphi_0} \end{pmatrix}, \tag{2.1}$$

avec $a, b, \varphi_0, \varphi_1 \in \mathbb{R}$, $0 \leq a \leq 1$ et $b = \sqrt{1-a^2}$. Les constantes a^2 et b^2 représentent le taux de couplage, et φ_0, φ_1 sont les phases acquises par la transmission dans les deux modes de sortie du coupleur. La quantification du problème se fait par la méthode usuelle, $\alpha_0 \rightarrow \hat{a}_0$ et $\alpha_1 \rightarrow \hat{a}_1$, ce qui nous permet, après un calcul un peu laborieux, de trouver l'opérateur d'évolution du coupleur, $\hat{C}$, dans la représentation de Schrödinger [48]. Nous énonçons ici le résultat dans le cas particulier d'un coupleur 50/50 ($a = b = 1/\sqrt{2}$) avec $\varphi_0 = \varphi_1 = 0$. Dans la base des états de Fock des deux modes, $\{|n_0, n_1\rangle\}$ ($n_0, n_1 = 0, \ldots, \infty$), on montre que

$$\begin{aligned} \hat{C}|n_0, n_1\rangle \;=\; & \left(\frac{1}{\sqrt{2}}\right)^{n_0+n_1} \frac{1}{\sqrt{n_0!n_1!}} \sum_{l_0}^{n_0} \sum_{l_1}^{n_1} \binom{n_0}{l_0} \binom{n_1}{l_1} (-1)^{n_0-l_0} \\ & \times \sqrt{(l_0+l_1)!(n_0+n_1-(l_0+l_1))!} \\ & \times |l_0+l_1, n_0+n_1-(l_0+l_1)\rangle. \end{aligned} \tag{2.2}$$

Si on applique cette transformation à l'état $|1\rangle_0|0\rangle_1 \equiv |1,0\rangle$, on obtient, à la sortie du premier coupleur de l'interféromètre (figure 2.2), l'état suivant :

$$|\psi'\rangle = \hat{C}|1,0\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle - |0,1\rangle\right) \tag{2.3}$$

Vient ensuite le modulateur de phase $\mathrm{MP_A}$ situé sur le mode 0 et qui est décrit par l'opérateur $\hat{P}(\varphi_a) = \mathrm{e}^{i\varphi_a\hat{n}_0}$, où $\hat{n}_0 = \hat{a}_0^\dagger\hat{a}_0$ est l'opérateur nombre de photons. Juste après $\mathrm{MP_A}$, on a, à un facteur de phase global près, l'état suivant :

$$|\psi''\rangle = (\hat{P}(\varphi_a) \otimes \hat{I})|\psi'\rangle = \frac{1}{\sqrt{2}}\left(|1,0\rangle - \mathrm{e}^{-i\varphi_a}|0,1\rangle\right). \tag{2.4}$$

À ce point, on peut établir la correspondance formelle avec les états de BB84, en choisissant $\varphi_a \in \{0, \pi/2, \pi, 3\pi/2\}$:

$$\varphi_a = 0 \;\rightarrow\; |1,0\rangle - |0,1\rangle \equiv |0_+\rangle, \tag{2.5}$$

$$\varphi_a = \pi/2 \;\rightarrow\; |1,0\rangle + i|0,1\rangle \equiv |0_\times\rangle, \tag{2.6}$$

$$\varphi_a = \pi \;\rightarrow\; |1,0\rangle + |0,1\rangle \equiv |1_+\rangle, \tag{2.7}$$

$$\varphi_a = 3\pi/2 \;\rightarrow\; |1,0\rangle - i|0,1\rangle \equiv |1_\times\rangle, \tag{2.8}$$

où nous avons omis d'écrire le facteur de normalisation.

Si on poursuit les calculs en tenant compte du modulateur de phase $\mathrm{MP_B}$, du coupleur de Bob, et en supposant que la différence de longueur entre les deux bras est ΔL, on obtient l'état $|\psi_f\rangle$ suivant à la sortie de l'interféromètre :

$$|\psi_f\rangle = \sin\left(\frac{\Delta\varphi + k\Delta L}{2}\right)|1,0\rangle + i\cos\left(\frac{\Delta\varphi + k\Delta L}{2}\right)|0,1\rangle, \qquad (2.9)$$

où $\Delta\varphi = \varphi_a - \varphi_b$. La probabilité d'observer le photon dans les détecteurs D_0 et D_1 est donc donnée par

$$\mathcal{P}(D_0) = \eta\sin^2\left(\frac{\Delta\varphi + k\Delta L}{2}\right), \qquad \mathcal{P}(D_1) = \eta\cos^2\left(\frac{\Delta\varphi + k\Delta L}{2}\right), \qquad (2.10)$$

où η est le rendement, supposée égale pour les deux détecteurs.

Les choix de phase $\varphi_a \in_A \{0, \pi/2, \pi, 3\pi/2\}$ et $\varphi_b + k\Delta L \in_A \{0, \pi/2\}$, où $\in_A$ signifie « choisi aléatoirement parmi... », permettent à Alice et à Bob de préparer et mesurer les quatre états de BB84, les bases étant compatibles lorsque $\Delta\varphi + k\Delta L = 0$ ou π, et incompatibles lorsque $\Delta\varphi + k\Delta L = \pi/2$ ou $3\pi/2$.

Les équations 2.10 montrent qu'une variation d'une fraction de longueur d'onde de la différence de marche ΔL est suffisante pour rendre l'interféromètre inutilisable. Sur grande distance, un tel interféromètre est impossible à stabiliser.

Signalons finalement que si l'impulsion optique est dans un état cohérent au lieu d'un état à un photon, alors les équations 2.10 représentent la probabilité de détection de chaque photon de l'impulsion.

2.2.2. Montage Plug&Play

Devant les difficultés occasionnées par l'instabilité du principe interférometrique, le groupe du professeur Nicolas Gisin (Université de Genève) trouva un moyen ingénieux d'auto-compenser les fluctuations de la biréfringence et de la différence de marche ΔL leur permettant ainsi de réaliser un interféromètre ne nécessitant aucun alignement ni stabilisation en température. Pour cette raison, les inventeurs ont nommé le montage « *Plug&Play* ».

Auto-compensation par le miroir de Faraday

Avant d'explorer les détails du montage *Plug&Play*, nous avons besoin d'expliquer comment il est possible de compenser automatiquement les fluctuations de biréfringence sur le lien. En supposant que les pertes dépendantes de la polarisation (PDL) sont négligeables, la biréfringence d'une fibre optique peut être vue comme une succession de N petits éléments ayant chacun leur biréfringence propre caractérisée par une transformation unitaire $\hat{B}_i$, $i = 1, \ldots, N$ (figure 2.3). La biréfringence totale, $\hat{B}$, est également une transformation unitaire sur l'état de polarisation et s'écrit comme $\hat{B} = \hat{B}_N \ldots \hat{B}_i \ldots \hat{B}_1$.

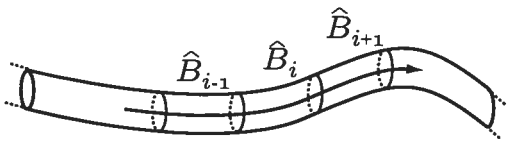

FIG. 2.3 – Succession d'éléments biréfringents d'un bout de fibre.

On peut donc représenter $\hat{B}$ par une rotation sur la sphère de Poincaré, $\hat{B} = \mathcal{R}(\mathbf{n}, \alpha)$ (équ. 1.5). Lorsque la lumière emprunte le chemin inverse, la biréfringence est $\hat{B}^{-1} = \hat{B}^\dagger$. Comme on le montre à l'annexe B, la transformation $\hat{M}_F$ associée au miroir de Faraday commute avec la transformation induite par la biréfringence, ce qui donne

$$\hat{B}^\dagger \hat{M}_F \hat{B} = \hat{B}^\dagger \hat{B} \hat{M}_F \tag{2.11}$$

$$= \hat{M}_F \tag{2.12}$$

Par conséquent, le miroir de Faraday permet de compenser automatiquement la biréfringence. Évidemment, les fluctuations de la biréfringence doivent être plus lentes que le temps d'aller-retour, autrement l'auto-compensation est affectée.

Auto-compensation et encodage en phase

Le truc à la base de la cryptographie auto-compensée est d'utiliser deux fois le même interféromètre. Un schéma est présenté à la figure 2.4. Examinons en détail son fonctionnement. La génération d'un bit de clé débute par l'envoi, par le

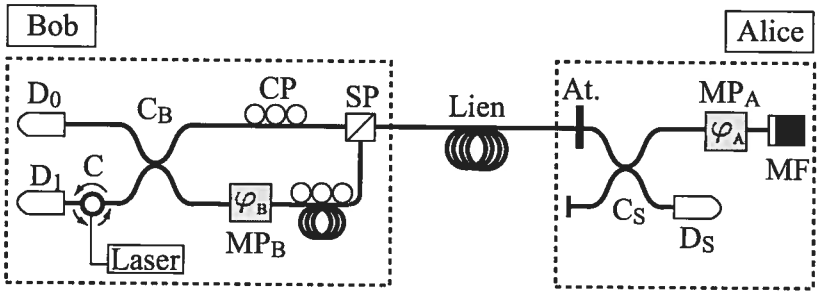

FIG. 2.4 – Montage *Plug&Play*.

laser de Bob, d'une impulsion cohérente intense et de durée limitée. L'impulsion passe par le circulateur optique **C** et est séparée en deux au coupleur 50/50 $\mathbf{C_B}$. L'impulsion P_c emprunte le bras court, et l'impulsion P_l le bras long, où elle est retardée d'un délai Δt qui est supérieur à la durée des impulsions. Le modulateur de phase $\mathbf{MP_B}$ n'est pas activé au premier passage. La polarisation dans chaque bras est modifiée par les contrôleurs **CP** de façon à maximiser la transmission dans le cube séparateur en polarisation **SP**. À la sortie du laboratoire de Bob, les polarisations de P_c et P_l sont, respectivement, horizontales et verticales. À l'arrivée chez Alice, les deux impulsions sont tour à tour réfléchies sur le miroir de Faraday (**MF**) et atténuées au retour par l'atténuateur **At.**. La puissance totale à la sortie correspond à un nombre moyen de photons par impulsion typiquement égal à $1/10 = 0{,}1$. La préparation de l'état de BB84 est effectuée durant le passage chez Alice en appliquant un déphasage $\varphi_A \in_A \{0, \pi/2, \pi, 3\pi/2\}$ sur l'impulsion P_l uniquement. La synchronisation du modulateur de phase d'Alice ($\mathbf{MP_A}$) est obtenue en captant une fraction de la puissance d'entrée des impulsions avec le détecteur $\mathbf{D_S}$, via le coupleur $\mathbf{C_S}$. De retour à l'entrée du laboratoire de Bob, grâce au miroir de Faraday, les polarisations des impulsions P_c et P_l sont échangées. P_c est donc transmis dans le bras long et P_l dans le bras court. Bob choisit la base de mesure en appliquant la phase $\varphi_B \in_A \{0, \pi/2\}$ sur l'impulsion P_c. Le délai entre les deux impulsions est exactement compensé et, juste avant $\mathbf{C_B}$, les polarisations sont remises à leur état initial. Cela permet d'obtenir une interférence quasi parfaite dans le coupleur.

L'auto-compensation n'est assurée que si l'interféromètre de Bob est stable durant le temps d'aller-retour de l'impulsion. Pour une distance de 100 km entre Alice et Bob, donc une distance d'aller-retour de 200 km, ce temps est de l'ordre $\Delta t = 1$ msec. Supposons que les bras court et long de l'interféromètre de Bob soient respectivement de longueur $l_c = 20$ et $l_l = 50$ m. Il faut d'abord vérifier qu'une variation de l'indice de réfraction des fibres causée par un changement de température ne peut modifier significativement le délai introduit par les deux bras de l'interféromètre. Pour cela, on utilise l'expression du déphasage optique $\Delta\varphi$ introduit par une variation de l'indice de réfraction Δn donnée :

$$\Delta\varphi = kl\frac{\Delta n}{\Delta t}\frac{\Delta t}{\Delta T}, \tag{2.13}$$

où $k = 2\pi/\lambda$, $\Delta n/\Delta T = 10^{-5}$ K^{-1} est le coefficient thermo-optique et $\lambda = 1550$ nm. Supposons que $\Delta T/\Delta t = 100$ K/heure. Le calcul donne un déphasage de 0,022 radians pour le bras court et de 0,056 radians pour le bras long. La différence des deux déphasage est approximativement égale à $\pi/92$, soit un centième de frange d'interférence, ce qui est négligeable. Une autre difficulté pourrait être occasionnée par des vibrations mécaniques de l'interféromètre dont la fréquence serait de l'ordre de $1/\Delta t = 1$ kHz. Finalement, le délai d entre les deux impulsions durant le trajet pourrait varier en raison de la dilatation thermique de la fibre du lien entre Alice et Bob. Pour une différence de 30 m entre les deux bras de l'interféromètre, ce délai est égal à $d = 148$ ns. La variation de la longueur du lien, Δl, s'exprime comme

$$\Delta l = l\tau\frac{\Delta T}{\Delta t}d. \tag{2.14}$$

Avec $\tau = 10^{-5}$ K^{-1} et $l = 100$ km, on trouve $\Delta l = 0{,}4$ nm, ce qui est négligeable devant la longueur d'onde.

Les causes d'erreurs discutées plus haut affectent le contraste d'interférence qui est maximal si les parcours des impulsions P_c et P_l sont indiscernables. Pour quantifier ce contraste on utilise la visibilité V d'interférence définie comme

$$\mathcal{V} = \frac{\mathcal{P}_{\text{bon}} - \mathcal{P}_{\text{mauvais}}}{\mathcal{P}_{\text{bon}} + \mathcal{P}_{\text{mauvais}}}, \tag{2.15}$$

où $\mathcal{P}_{\text{bon}}$ et $\mathcal{P}_{\text{mauvais}}$ sont les probabilités de détecter le photon dans le bon et le mauvais détecteur lorsque la préparation et la mesure ont été faites dans la

même base. Ces probabilités sont proportionnelles à la puissance mesurée dans les branches respectives, indiquant que la mesure peut être faite à haute puissance. Pour une visibilité $\mathcal{V}$ donnée, la probabilité que le photon cause une erreur est égale à

$$\mathcal{P}_{\text{mauvais}} = \frac{1-\mathcal{V}}{2}. \tag{2.16}$$

Le principe d'auto-compensation à été démontré pour la première fois en 1997 [60]. Récemment, les concepteurs ont testé le système avec succès sur plusieurs distances et sur différents types de câbles de transmission optique. En particulier, il a été testé sur une distance de 67 km sur une fibre souterraine et sur un câble aérien de 2,5 km [73]. Dans les deux cas la visibilité mesurée était supérieure à 99,6%.

D'autres groupes ont rapporté la construction de systèmes auto-compensés en phase basés sur le système *Plug&Play* [20, 36]. Récemment, un groupe japonais a réussi à observer une visibilité d'interférence égale à 90% avec un nombre moyen de photon $\mu = 0{,}1$ sur une distance de 100 km [45]. Or, comme nous l'avons montré à la section 1.4, l'attaque SNP permet de briser ce système car la distance est supérieure à 56 km. Ce système est sécuritaire uniquement si on exclut l'attaque SNP.

Problèmes

Le système *Plug&Play* souffre de quatre problèmes qui ont une cause commune, l'utilisation du miroir de Faraday. Nous en discutons ici brièvement.

Le premier problème est l'impossibilité d'utiliser une source à un photon avec ce système. En effet, le système est incompatible avec l'utilisation d'une source à un photon en raison de la nécessité de synchroniser le modulateur de phase d'Alice avec une impulsion intense. Autrement dit, l'impulsion envoyée par Bob doit être cohérente, ce qui augmente la probabilité d'impulsions multi-photons au retour et diminue la sécurité du système en raison de l'attaque SNP (section 1.4). Cependant, suivant les arguments de M. Matsuoka et T. Hirato [55], l'utilisation d'une source cohérente intense et comprimée en amplitude pourrait possiblement

diminuer cet effet en réduisant la probabilité d'impulsions multi-photons.[2] Cela est une bonne question à étudier.

Le deuxième problème est que l'introduction du miroir permet un nouveau type d'attaque dit de « Cheval de Troie ». Voyons de quoi il s'agit. Pour détecter la phase appliquée par Alice, Ève pourrait injecter dans le laboratoire d'Alice une impulsion de durée Δt_e légèrement décalée en fréquence qui serait réfléchie sur le miroir et modulée en phase par φ_a. Pour cette raison, Alice doit activer son modulateur de phase $\mathbf{MP_A}$ (voir la figure 2.4, page 38) uniquement pendant la durée Δt de l'impulsion envoyée par Bob, ce qui force Ève à faire de même avec son impulsion sonde. Comme l'atténuateur **At.** atténue à un nombre de photons par impulsion typiquement égal à 0,1, alors Ève doit utiliser une puissance 10 fois supérieure à l'entrée pour obtenir en moyenne 1 photon à la sortie et espérer mesurer la phase à tout coup. Si $\Delta t_e \approx \Delta t$, alors Alice détecte facilement la présence de l'impulsion sonde à l'aide son détecteur $\mathbf{D_S}$. Cependant, si $\Delta t_e \ll \Delta t$, et en particulier, si le temps de réponse de $\mathbf{D_S}$ est plus long que Δt_e, alors Ève n'est plus détectable. Pour contrer cela, Alice peut utiliser un filtre dont la largeur spectrale correspond à celle des impulsions et choisir un détecteur $\mathbf{D_S}$ ayant un temps de réponse beaucoup plus court que Δt. Par conséquent, Ève devra diminuer encore plus la durée de son impulsion, et donc utiliser une puissance encore plus grande. Il n'est pas du tout clair ici s'il est possible pour Ève de rester non détectable, car cela dépend des propriétés de $\mathbf{D_S}$. La sécurité contre ce type d'attaque repose donc sur des considérations technologiques, et non uniquement sur les lois de la physique, comme on le souhaiterait. Une étude plus poussée est nécessaire.

Le troisième problème est causée par la rétro-diffusion Rayleigh de la fibre [1]. En principe, rien n'empêche d'envoyer sur le lien des photons dans les deux directions simultanément. En pratique, les impulsions voyageant vers Alice sont rétro-diffusées vers Bob et elles peuvent se superposer aux impulsions réfléchies

[2]Une source comprimée en amplitude (amplitude squeezed, en anglais) est caractérisée par des fluctuations réduites en intensité, au détriment d'une diminution du temps de cohérence. Voir [66].

sur le miroir de Faraday, ce qui cause des erreurs. La rétro-diffusion est cependant négligeable si l'intensité de Bob est suffisamment faible, mais dans ce cas il devient difficile de contrer une attaque Cheval de Troie. Il est donc impossible d'opérer le système avec des photons circulant dans les deux sens simultanément, ce qui réduit le taux de génération de clé.

Le quatrième et dernier problème est beaucoup plus subtil.[3] Nous avons vu qu'il existe des preuves de sécurité lorsque le système est imparfait 1.4. Cependant, ces preuves supposent toutes que la source est dans le laboratoire d'Alice ce qui n'est pas le cas avec le système *Plug&Play*. En effet, Ève pourrait très bien manipuler à son avantage les photons envoyés par Bob avant leur arrivée chez Alice, ou encore les remplacer par ses propres photons qui pourraient, par exemple, être intriqués avec d'autres photons qu'elle conserve dans son laboratoire. Il s'agit d'un problème important qui reste à explorer. Pour cette raison, et au meilleur de notre connaissance, la sécurité du *Plug&Play* n'est toujours pas démontrée.

2.3. Cryptographie quantique à plusieurs participants

Pour aspirer un jour à devenir utilisable à grande échelle, on doit penser dès aujourd'hui à intégrer la cryptographie quantique sur des structures de réseaux de communication optique. Or, la faisabilité de la CQ sur un réseau optique à plusieurs participants dépend entièrement de sa structure. Nous n'avons ici pas la prétention de couvrir tous les types de réseau optique actuels, ni de faire une étude complète de faisabilité. Nous verrons plutôt comment le multiplexage en longueur d'onde peut être utilisé pour réaliser un type précis de réseau capable de supporter les protocoles BB84 et EPR. Nous discuterons également de façons d'utiliser le multiplexage pour améliorer d'autres aspects de la CQ.

2.3.1. Propriétés recherchées

Définissons d'abord une liste de quatre propriétés qu'un réseau supportant la CQ devrait posséder :

[3] Je remercie David Poulin pour m'en avoir fait part.

Universalité	N'importe quelle paire d'utilisateurs est en mesure d'établir un clé secrète.
Stabilité	Le taux de génération de clé par utilisateur est indépendant du nombre d'utilisateurs du réseau.
Adaptation	Le coût technologique associé à l'ajout d'un utilisateur au réseau n'est pas prohibitif (cette propriété dépend directement de la façon dont le protocole de CQ est implanté).
Confidentialité	Le réseau n'utilise pas de relais sécurisés (ce concept est défini dans la prochaine section).

Armé de ces propriétés, nous sommes en mesure d'évaluer et de comparer les différentes architectures.

2.3.2. Cryptographie quantique et réseaux actuels

Commençons d'abord par énumérer les composants qui ne peuvent pas être utilisés sur un réseau optique voué à la CQ. Tout d'abord, toute amplification optique est inutile, en raison du théorème de non-clonage. Qui plus est, elle peut être néfaste, comme c'est le cas avec les amplificateurs à fibre dopée à l'erbium (et avec la plupart des amplificateurs optiques) qui introduisent un signal parasite non polarisé causé par l'émission spontanée, et ce, même sans signal à amplifier [2]. Une autre difficulté, toujours en raison du théorème de non-clonage, est que le signal ne peut être mesuré et régénéré, comme cela est nécessaire actuellement sur le réseau Internet pour établir la communication entre deux points arbitraires du réseau. Par conséquent, on ne peut pas battre la limite de la distance maximale sans utiliser des *relais sécurisés*. Un relais sécurisé est un intermédiaire entre Alice et Bob, appelons-le Robin, qui établit de façon sécuritaire une clé secrète k_a avec Alice et une autre clé k_b avec Bob. Cela permet à Alice et Bob de communiquer secrètement en utilisant une des deux façons suivantes :

1. Alice chiffre son message avec k_a, l'envoie à Robin qui le déchiffre et le chiffre à nouveau avec k_b et l'envoie à Bob.
2. Robin, qui connaît les deux clés, indique à Bob quels bits de k_b doivent être

inversés (c'est-à-dire changer un 0 pour un 1 et vice-versa) pour obtenir k_a, ce qui ne révèle aucune information supplémentaire. Cela permet à Alice et Bob de communiquer via le canal de leur choix, et pas nécessairement celui passant par Robin.

Bien entendu, Robin doit être honnête, ce qui impose une restriction supplémentaire mais inévitable en utilisant cette façon de procéder. Sur un vaste réseau optique, de tels relais sécurisés seraient difficiles à implanter sur tous les points d'accès. Une infrastructure privée et contrôlée est donc nécessaire pour couvrir une très grande distance. Sur ce point, un groupe de chercheurs de l'entreprise BBN Technologies développe actuellement un protocole de communication réseau (semblable à TCP/IP) capable de supporter BB84 en utilisant des relais sécurisés [31]. Un tel travail est intéressant, mais pour économiser des ressources, il est impératif de trouver des façons de maximiser le nombre de participants par relais sécurisé.

La solution simple pour satisfaire cette condition est de construire un *réseau en étoile* autour d'un relais. Dans ce type de réseau, chaque utilisateur est relié physiquement au relais par un canal unique. Un tel réseau peut ensuite faire partie d'une structure plus élaborée avec plusieurs unités du même genre, comme illustré à la figure 2.5. Cette architecture permet à deux utilisateurs du même réseau R_i

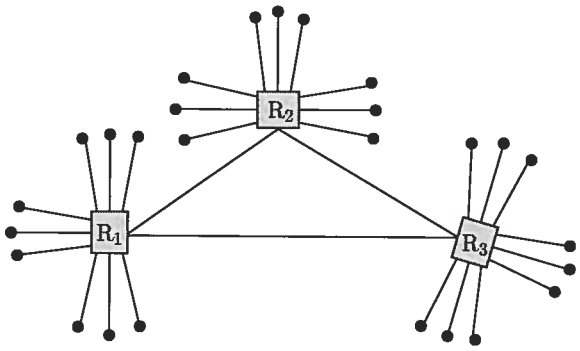

FIG. 2.5 – Réseau en étoile dans un réseau global. Les carrés R_i représentent les relais sécurisés, et les points les utilisateurs du réseau. Les lignes représentent les canaux de communications passibles d'espionnage.

ou de réseaux différents R_i et R_k de communiquer de façon sécuritaire. Comparons

cette architecture avec la solution triviale où chaque utilisateur est relié à tous les autres avec un lien dédié. Dans la deuxième solution, $(N+1)N/2 \propto N^2$ canaux sont nécessaires, tandis que seulement N canaux sont suffisants à l'intérieur d'un réseau R_i. De plus, le nombre de relais sécurisés est grandement réduit car le même relais est disponible pour plusieurs utilisateurs.

La première démonstration de la faisabilité de la CQ sur un réseau optique en étoile fut réalisée en 1997 par P. Townsend (*British Telecom*, maintenant devenue *Corning*). L'idée était d'utiliser un coupleur diviseur de puissance pour partager la communication optique du relais vers les utilisateurs. Un coupleur diviseur de puissance est un coupleur optique à N entrées et N sorties, mais dont $N-1$ entrées sont inutilisées. Au niveau du photon individuel, l'effet du coupleur sur l'état à un photon incident $|1,0,...,0\rangle$, où chaque entrée représente un mode du coupleur, est de créer une superposition égale de tous les modes de sortie :

$$\hat{C}|1,0,\ldots,0\rangle = \frac{1}{\sqrt{N}} \sum_{k=1}^{N} \mathrm{e}^{i\varphi_k} |\delta_{1k}, \delta_{2k}, \ldots, \delta_{Nk}\rangle, \tag{2.17}$$

où δ_{ij} est le symbole de Kronecker. Le photon a donc une chance égale d'être détecté dans chaque mode, et le choix est aléatoire. Dans la direction inverse, pour un seul photon incident, l'état du premier mode est donné par un mélange statistique de 0 et 1 photon :

$$\rho = \frac{N-1}{N}|0\rangle\langle 0| + \frac{1}{N}|1\rangle\langle 1|. \tag{2.18}$$

Autrement dit, le photon sort en moyenne par le premier mode une fois sur N et est perdu le reste du temps. À l'aide d'un tel coupleur, il est simple de réaliser un réseau en étoile avec un relais sécurisé. Il suffit de placer Robin à l'entrée simple et les N utilisateurs aux N sorties.

P. Townsend a démontré la faisabilité d'un tel réseau avec un coupleur 1×3 [79] comme illustré à la figure 2.6. Le relais (Robin) est relié aux trois utilisateurs U_1, U_2 et U_3 et le but de la démonstration est de générer les clés k_1, k_2 et k_3 en utilisant BB84 avec un encodage en polarisation, donc avec une communication quantique uni-directionnelle. La longueur du lien est d'environ 10 km pour chaque utilisateur. Physiquement, rien n'empêche un tel réseau de fonctionner, pourvu que la fibre et

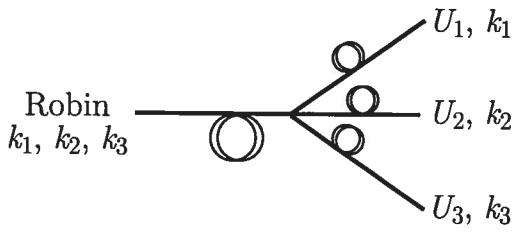

FIG. 2.6 – Réseau en étoile avec un coupleur 1×3.

le coupleur n'aient qu'un seul mode de propagation avec une polarisation définie, un vecteur d'onde et une phase uniques et bien définis, ce qui est le cas ici.

Le réseau de Townsend souffre de deux inconvénients. Premièrement, le chemin emprunté par le photon est aléatoire, ce qui empêche le relais de choisir l'utilisateur avec qui il communique. Cela implique que pour la partie classique du protocole (réconciliation et distillation), le taux de transfert par utilisateur est divisé par un facteur N. De plus, si pour une raison quelconque un des utilisateurs suspend sa communication avec le relais, il reçoit tout de même les photons de BB84, ce qui est un gaspillage de ressources. Deuxièmement, la communication quantique dans la direction inverse subit également une perte d'un facteur $1/N$. Pour ces deux raisons, cette architecture ne satisfait que la propriété d'universalité, énoncée à la section 2.3.1.

2.3.3. Réseau avec multiplexage en longueur d'onde

Réseau avec BB84

Une solution simple permettant d'améliorer le réseau de Townsend est d'utiliser le *multiplexage en longueur d'onde* (WDM, de l'anglais *Wavelength division multiplexing*). En principe, une fibre optique peut guider une large bande de longueurs d'onde qui peuvent toutes véhiculer indépendamment de l'information. Chaque longueur d'onde représente un canal de communication. Un multiplexeur est un composant qui possède N entrées physiques à N longueurs d'onde différentes, et une seule sortie physique guidant tous les canaux. Donc, un seul canal physique (la fibre) permet de guider N canaux de communication. L'extraction des longueurs

d'onde se fait par la technique inverse, le démultiplexage. Au cours de ce mémoire, nous utiliserons le terme multiplexeur uniquement pour identifier un composant capable de réaliser le multiplexage et le démultiplexage des longueurs d'onde. Revenons maintenant au réseau. Si on remplace le coupleur par un démultiplexeur en longueur d'onde, alors Robin peut communiquer directement avec l'utilisateur de son choix en utilisant la bonne longueur d'onde (figure 2.7). Le chapitre 4 est consacré à la démonstration expérimentale de ce principe. Cette architecture

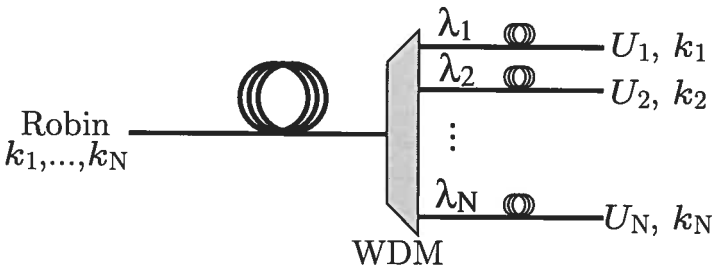

FIG. 2.7 – Réseau en étoile avec WDM.

possède plusieurs avantages. Premièrement, elle permet au relais de communiquer avec tous les utilisateurs de façon simultanée ou séquentielle. Deuxièmement, les pertes sont minimisées dans les deux directions. Finalement, chaque canal peut supporter autant la communication classique que quantique ce qui permet d'implanter les procédures de réconciliation et d'amplification sur le réseau même et ce indépendamment de l'utilisation des autres canaux en fréquence. En principe, elle permet donc de satisfaire la propriété de stabilité. La situation serait probablement différente si la fibre, par multiplexage en longueur d'onde, comportait à la fois une communication quantique (photons individuels) et classique (possiblement à grande puissance). Il faut alors s'assurer que les effets non-linéaires induits par la communication classique ne détruisent pas l'information quantique codée dans les photons des autres canaux. En particulier, le canal classique à grande puissance pourrait très bien, par modulation de phase mutuelle, détruire l'encodage en phase d'un canal quantique adjacent. Pour un signal quantique à 1550 nm et un signal classique à 1300 nm, une démonstration concluante à déjà été faite [78]. Or, avec

les techniques actuelles, il est possible de multiplexer des longueurs d'onde séparées par 0,4 nm. Avec un espacement aussi faible, les effets non-linéaires mutuels sont plus importants et une étude plus poussée est nécessaire [1]. En particulier, il serait intéressant de déterminer la puissance maximale admissible dans le canal classique en présence du signal quantique.

Réseau avec le protocole EPR

Selon nous, le plus grand avantage de l'utilisation du multiplexage est le fait qu'avec une source de photons intriqués en fréquence (voir plus loin), le réseau satisfait la propriété de confidentialité en utilisant le protocole EPR. Pour comprendre cette affirmation, expliquons d'abord le concept d'intrication en fréquence de photons. Soit $|n_1, \nu_1; n_2, \nu_2\rangle$, un état de Fock avec n_1 et n_2 photons aux fréquences ν_1 et ν_2, respectivement. Un état du type

$$|\Psi\rangle = \alpha|0, \nu_1; 0, \nu_2\rangle + \beta|1, \nu_1; 1, \nu_2\rangle \tag{2.19}$$

correspond à deux photons intriqués en fréquence. Ils sont intriqués au sens où la mesure de la présence (non-présence) d'un photon à ν_1 implique la présence (non-présence) de l'autre à ν_2, et vice-versa. L'optique non-linéaire offre plusieurs façons de de créer un tel état. En particulier, la faisabilité d'une telle source à été démontrée par le mélange à quatre ondes dans les fibres [46, 53, 66] ainsi que par la conversion paramétrique par génération de différence de fréquences [66]. Pour implanter le protocole EPR, le relais émet deux photons intriqués aux fréquences ν_i et ν_j. Grâce au démultiplexeur optique, les photons émis sont guidés vers les utilisateurs i et j respectifs. Pour générer la clé, les utilisateurs pourraient utiliser un interféromètre de Franson tout-fibre qui est l'équivalent EPR de l'encodage en phase avec BB84 [34]. Ce principe à été démontré pour la première fois par Ribordy *et al.* [63]. Encore une fois, il s'agit d'un sujet intéressant à étudier.

Le multiplexage en longueur d'onde permet donc, en principe, de créer un réseau qui satisfait la propriété de de confidentialité, car même si le relais distribue les photons intriqués en fréquence, il ne peut acquérir d'information sur la clé créée sans se faire détecter (section 1.3).

3 — Détection de photons dans l'infrarouge proche

La détection de photons uniques dans les longueurs d'onde allant du visible jusqu'à 1100 nm est, depuis plusieurs années, possible grace à l'existence de détecteurs efficaces, peu bruyants et commercialement disponibles. Ce n'est pas le cas à plus de 1100 nm et en particulier dans les longueurs d'onde utilisées pour la cryptographie quantique. Depuis l'essor fulgurant de cette discipline et de celle du traitement optique de l'information quantique, le besoin de détecteurs à ces longueurs d'onde est maintenant bien réel, ce qui a motivé (et motive encore) plusieurs groupes à développer de nouvelles techniques.

Dans ce chapitre, nous rapportons le travail de construction et de caractérisation d'un détecteur de photons en utilisant une photodiode à avalanche opérée en mode Geiger. Cette technique en soi à été utilisée dans le passée par d'autres groupes et le travail rapporté ici n'apporte pas d'éléments nouveaux. Son élaboration était tout de même nécessaire à la réalisation du système de cryptographie à plusieurs participants (chapitre 4). Soulignons également que notre but n'était pas de caractériser la photodiode dans toutes les conditions possibles mais uniquement dans celles qui sont pertinentes à la caractérisation du réseau à plusieurs participants. Si notre désir avait été d'optimiser les performances du détecteur, alors une étude plus poussée aurait été nécessaire. Les points à améliorer sont mis en évidence dans ce chapitre.

Le chapitre est divisé comme suit. Dans la première section, nous discutons du principe de fonctionnement du détecteur et des ses propriétés. Ensuite, nous décrivons le montage et présentons les résultats de la caractérisation. Finalement, nous discutons de l'impact de la performance du détecteur sur la faisabilité de la cryptographie quantique (CQ).

3.1. Détection de photons dans l'infrarouge proche : un aperçu

Faisons d'abord un bref survol des techniques actuelles de détection de photons uniques pour comprendre pourquoi elles ne sont pas satisfaisantes pour les besoins de la CQ.

Premièrement, dans le visible, les tubes photomultiplicateurs, lorsqu'ils sont suffisamment refroidis, sont très efficaces, ont un fort gain et sont peu bruyants dans le visible. Cependant, un matériau ayant un rendement supérieur à 1% à 1550 nm et pouvant faire office de cathode et dynode reste à découvrir.

Pour les longueurs d'onde inférieures à 1100 nm, les photodiodes au silicium à structure PIN (utilisés avec un circuit d'amplification approprié) et à structure à avalanche offrent de très bonnes performance en mode comptage de photons. Cependant, l'énergie de la bande interdite (gap) du silicium (1,12 eV à 300 K) est supérieure à l'énergie d'un photon à 1550 nm (0,8 eV), ces photodiodes sont donc insensibles aux longueurs d'onde désirées. Il en est de même pour les photodiodes à avalanche au germanium qui ont une longueur d'onde de coupure de 1480 nm.

Présentement, les meilleures photodiodes à avalanche (PDA) commercialement disponibles ayant une sensibilité non négligeable à 1550 nm sont celles à hétérojonction InGaAs/InP. Quoique moins performantes que les PDA au silicium, nous verrons qu'elles offrent actuellement la solution la plus abordable au problème de détection de photons uniques. Notons également que, en principe, rien n'empêche les PDA InGaAs/InP d'êtres aussi performantes que celles au silicium. En pratique, les techniques de fabrication sont moins perfectionnées et les PDA ne sont pas conçues pour fonctionner comme détecteur de photons uniques, ce qui affecte leur performance.

En guise de comparaison, énumérons les propriétés évidentes qu'un détecteur de photons parfait devrait posséder :

- Rendement de 1.
- Bruit nul.
- Temps de réponse instantané.
- Fréquence d'activation illimitée.
- Fonctionnement en mode continu.

– Capacité de résolution du nombre de photons.

3.2. Fonctionnement des photodiodes à avalanche

Dans cette section nous décrivons la structure de la PDA au InGaAs/InP et nous discutons du mécanisme de gain permettant d'obtenir rendement suffisant à la détection de photons individuels.

3.2.1. Structure de la PDA

La photodiode est, comme son nom l'indique, une diode dont la capacité de détection optique est basée sur la création de charges libres par absorption de photons dans la structure. En polarisation inverse, le champ électrique présent au niveau de la jonction accélère les charges vers les contacts électriques, ce qui crée un courant mesurable. La photodiode à avalanche, pour sa part, se distingue de la photodiode simple du fait que sa structure comporte une région d'absorption et une région d'avalanche.

Examinons d'abord la structure de la PDA que nous utilisons dans cette expérience. La figure 3.1 montre l'empilement des couches semi-conductrices, la structure des bandes d'énergie résultantes ainsi que le profil du champ électrique. Les références [4, 52] sont un bon point de départ pour comprendre comment ces profils sont calculés. Cette structure est dite à « pénétration » car les régions d'absorption et d'avalanche sont séparées. La jonction *p-n* est formée à l'interface p+InP/n-InP, d'où s'étend de part et d'autre la région d'appauvrissement. La largeur de cette dernière, W, augmente avec la tension de polarisation V selon $W = W_0(1 + V/a)^{1/2}$, où W_0 et a sont des constantes. En augmentant V, la région d'appauvrissement s'étend progressivement dans la couche n-InP pour atteindre la région d'absorption à la *tension de pénétration*, V_{RT} (*reach-through voltage* en anglais). Ce n'est qu'à partir de cette tension qu'apparaît un champ électrique non nul dans la région d'absorption, ce qui permet aux charges libres créées par absorption de dériver et d'être injectées dans la région d'avalanche. Lorsqu'elles sont injectées, le fort champ électrique les accélère suffisamment pour causer une multiplication des charges par ionisation par impact. Cette multipli-

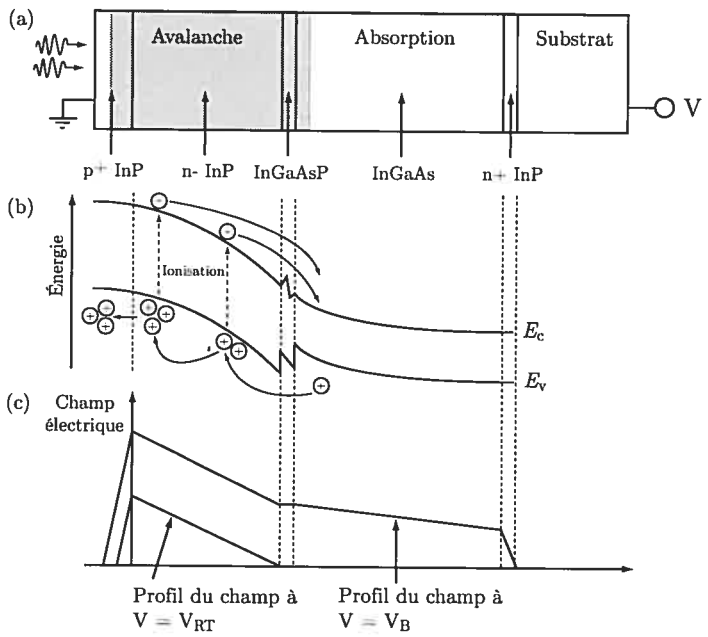

FIG. 3.1 – Structure d'une PDA InGaAs/InP. (a) Empilement des couches. (b) Structure des bandes de valence et de conduction, où E_c et E_v représentent l'énergie des bandes de conduction et de valence. (c) Profil du champ électrique. La zone ombrée représente la région d'appauvrissement. Tiré de [38].

cation est équivalente à un effet d'amplification, ce qui permet de détecter des signaux optiques de faible puissance. Comme le processus d'avalanche est stochastique, il crée un bruit intrinsèque et il a été montré que c'est le porteur de charge qui a le coefficient d'ionisation le plus élevé qui devrait initier le processus d'avalanche. Dans l'InP, ce sont les trous qui remplissent ce rôle et la structure est conçue en conséquence. D'ailleurs, la couche intermédiaire d'InGaAsP sert justement à adoucir la jonction entre l'InP (E_{gap} = 1,35 eV à 300K) et l'InGaAs (E_{gap} = 0,73 eV à 300K) pour ainsi favoriser la capture des trous dans la région d'avalanche.

3.2.2. Gain d'avalanche

Un explication détaillée du processus d'avalanche est nécessaire pour comprendre le mécanisme permettant de détecter un photon unique. Nous allons considérer que les électrons autant que les trous participent au processus d'ionisation, qui est illustré à la figure 3.2. Un trou est tout d'abord injecté en $x = 0$, il est ensuite accéléré par le fort champ électrique pour atteindre rapidement sa vitesse de dérive $v_d = \mu_t E$, où μ_t est la mobilité des trous et E la grandeur du champ électrique local. La vitesse de dérive est suffisante pour créer d'autres paires électron-trou qui sont également accélérées pour créer d'autres paires, et ainsi de suite. Pour caractériser l'ampleur du processus d'avalanche on utilise le

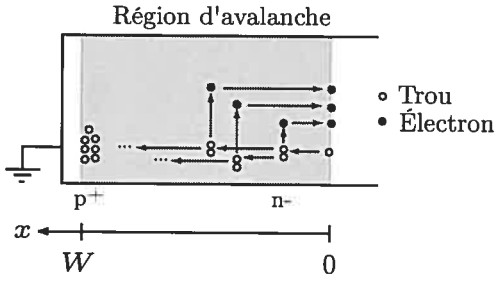

FIG. 3.2 – Processus d'avalanche par ionisation par impact dans la région d'avalanche de la photodiode. Par souci de clarté, seule la multiplication par les trous est illustrée.

facteur de multiplication des charges, M, défini comme étant le nombre moyen de paires électron-trou accumulées lorsqu'un trou est injecté en $x = 0$. Le calcul de M fait intervenir les coefficients d'ionisation des électrons et des trous, α et β, qui correspondent à la probabilité par unité de longueur que le porteur de charge crée un nouvelle paire par ionisation par impact. Il est inutile de faire le calcul de M au complet, il suffit de mentionner le résultat [57] :

$$M = \frac{1}{1 - G} \tag{3.1}$$

où G est donné par

$$G = \int_0^W \mathrm{d}x\, \alpha \exp\left[- \int_0^x (\alpha - \beta)\, \mathrm{d}x' \right]. \tag{3.2}$$

G est le gain d'avalanche. Mathématiquement, on a $0 \leq G \leq 1$. Ce n'est pas écrit explicitement ici, mais tous les paramètres expérimentaux comme la valeur du champ électrique dans la région d'avalanche, la température, la mobilité des porteurs ainsi que la tension de polarisation sont inclus dans les valeurs de α et de β.

Lorsque $G = 1$, alors $M \to \infty$. Autrement dit, un nombre quasi-infini de paires est créé. C'est le régime d'*avalanche complète* (*avalanche breakdown* en anglais) qui signifie qu'un seul trou injecté en $x = 0$ a une probabilité unité de créer un nombre infini de charges libres dans la région d'avalanche. À température fixée, la tension à laquelle cela se produit se nomme la *tension d'avalanche* que l'on note V_B. Pour $V < V_B$, le gain est trop faible pour obtenir une avalanche significative lorsqu'un seul trou est injecté dans le région d'avalanche et, comme un photon ne peut créer qu'une seule paire, seule l'opération en régime d'avalanche complète permet d'obtenir un courant macroscopique détectable.

En pratique, le nombre de paires créées lorsque $V > V_B$ n'est pas infini. Il est plutôt donné par le courant circulant dans la jonction lors de l'avalanche. Le courant d'avalanche, I_A, est égal à [47]

$$I_A = \frac{V - V_B}{R_S(V)}, \tag{3.3}$$

où $R_S(V)$ est la résistance de la région d'appauvrissement, qui est donnée par [47]

$$R_S(V) = \frac{W^2(V)}{2\epsilon v_d A(V)}, \tag{3.4}$$

où ϵ est la constante diélectrique de la région d'appauvrissement, et $A(V)$ l'aire de la section d'avalanche, dépendante de V. Le courant d'avalanche est donc indépendant du nombre de trous injectés dans la région d'avalanche. Par conséquent, ce type de détecteur ne permet pas de résoudre le nombre de photons contenus dans l'impulsion.

Dans cette expérience, le courant d'avalanche est de l'ordre de 10 µA, ce qui donne environ 62 400 paires électron-trou créées par nanoseconde.

3.2.3. Courant de fuite et dépendance en température

L'absorption n'est pas la seule source d'injection de trous libres. La génération thermique d'un trou suffisamment près de la région d'avalanche peut aussi causer une avalanche. Pour $V_{\mathrm{RT}} < V < V_B$, on peut montrer que la densité de courant de trous J_t (c'est-à-dire le nombre de trous par unité de surface par unité de temps) collectés à la borne négative de la photodiode dépend faiblement de V et est donnée par [4]

$$J_t = J_0 T^3 \exp\left(-\frac{E_g}{k_{\mathrm{B}} T}\right), \tag{3.5}$$

où J_0 est une constante de proportionnalité, k_{B} est la constante de Boltzmann et T la température. Pour $V > V_B$, on peut s'attendre au même comportement en température. Le nombre de trous thermiques injectés (et donc le taux de bruit) diminue exponentiellement avec l'inverse de la température. On a donc intérêt, *a priori*, à diminuer le plus possible la température.

Cependant, en diminuant la température, la mobilité des porteurs augmente. À 100 K et plus, cette mobilité est dominée par les collisions avec les phonons, et varie selon $1/T$ [4]. Par conséquent, l'augmentation de la vitesse de dérive v_d lorsque la température diminue fait augmenter la probabilité d'ionisation par unité de longueur (le coefficient d'ionisation), et donc la tension nécessaire pour atteindre le régime d'avalanche complet (V_B) est moins grande. Comme la tension de pénétration ne dépend que du profil de dopage et de l'empilement des couches du dispositif, il existe une température de coupure à partir de laquelle $V_B \leq V_{\mathrm{RT}}$, auquel cas aucune charge ne peut être injectée dans la région d'avalanche et le dispositif cesse de fonctionner.

Un autre phénomène important influence le courant de fuite. Les trous présents dans la bande de valence de la région d'absorption ont une certaine probabilité d'être injectés par effet tunnel dans la bande de valence de la région d'avalanche, auquel cas ils sont accélérés et peuvent déclencher une avalanche. Cette probabilité augmente avec la chute de potentiel de la région d'appauvrissement et avec la valeur champ électrique à l'interface InP/InGaAs [38].

3.3. Opération et montage

3.3.1. Mode d'opération

Nous opérons la PDA en mode « Geiger » par analogie au compteur de radiation. Ce mode d'opération est possible lorsque le temps d'arrivée de l'impulsion optique est localisé dans une fenêtre temporelle de durée τ bien définie. Durant cette période, on polarise la PDA au-delà de la tension d'avalanche V_B. Si un ou plusieurs photons sont absorbés, l'avalanche est enclenchée et elle dure jusqu'à ce que le circuit d'opération abaisse la tension au-dessous de V_B. Pour obtenir ce mode d'opération, on polarise en continu la PDA avec une tension $V_{DC} < V_B$, et durant la période de temps $T_p \geq \tau$ on lui superpose une impulsion carrée de tension d'amplitude V_p. On contrôle également le temps de répétition des impulsions optiques, que nous noterons T_r (voir la figure 3.3). Remarquons ici qu'en raison de la nature poissonnienne de la probabilité de génération thermique des trous, la probabilité d'obtenir un compte obscur est directement proportionnelle à la durée d'activation T_p, que l'on désire donc garder la plus courte possible.

Avec ce mode d'opération on peut mesurer les deux quantités définissant la performance du détecteur, soit le rendement η et la probabilité p_{co} qu'un *compte obscur* survienne durant la période d'activation. Par *compte obscur*, on entend une avalanche causée par un porteur généré thermiquement ou par toute cause autre que l'absorption d'un photon de l'impulsion optique.

Pour mesurer p_{co}, il suffit d'activer à répétition le détecteur en coupant le signal optique. On trouve alors N_{co} comptes obscurs pour N_a activations. On estime p_{co} par

$$\bar{p}_{co} = \frac{N_{co}}{N_a}. \tag{3.6}$$

La barre au-dessus de p_{co} indique qu'il s'agit d'une estimation de la véritable probabilité p_{co}. On rappelle que la probabilité $\mathcal{P}(N_{co})$ de mesurer N_{co} comptes parmi N_a activations est donnée par une distribution binomiale :

$$\mathcal{P}(N_{co}) = \binom{N_a}{N_{co}} p_{co}^{N_{co}} (1 - p_{co})^{N_a - N_{co}}, \tag{3.7}$$

de valeur moyenne $N_a p_{co}$ et de variance $N_a p_{co}(1 - p_{co})$. Dans le cas où N_a est très

grand, alors la distribution binomiale devient une distribution de Poisson. C'est le cas ici, car on s'attend à $p_{co} \sim 10^{-4}$, ce qui nécessite un très grand nombre d'activations pour accumuler un nombre suffisant de comptes. L'espérance de N_{co} est notée ν et elle est égale à $N_a p_{co}$. La probabilité de mesurer N_{co} s'écrit alors comme

$$\mathcal{P}(N_{co}) = \frac{\nu^{N_{co}} \mathrm{e}^{-\nu}}{N_{co}!}. \tag{3.8}$$

Puisque qu'il s'agit d'une distribution poissonnienne, la variance est également ν. L'incertitude absolue sur $\bar{p}_{co}$ est donnée par

$$\Delta \bar{p}_{co} = \frac{\sqrt{\nu}}{N_a} \tag{3.9}$$

$$\approx \frac{\sqrt{N_{co}}}{N_a}. \tag{3.10}$$

La dernière égalité est obtenue en remplaçant l'espérance ν par la valeur mesurée N_{co}. L'erreur relative sur l'estimation de p_{co} est donc égale à $1/\sqrt{N_{co}}$. Pour $N_{co} =$ 100 et 1 000, on obtient une erreur relative de 10% et 3,2% respectivement.

Pour mesurer le rendement, il faut répéter l'expérience avec le signal optique présent. Nous ne cherchons pas à mesurer rendement quantique, mais seulement la probabilité qu'un photon incident sur la photodiode cause une avalanche détectable. La valeur du rendement inclut donc les pertes aux connecteurs et toute autre perte à l'intérieur du dispositif. Un calcul plus élaboré que pour p_{co} est nécessaire car il faut tenir compte de la statistique de photons et des comptes obscurs. Définissons p_{cr} (pour compte réel) comme la probabilité qu'une impulsion cohérente contenant en moyenne μ photons cause une avalanche. Lorsque l'impulsion contient k photons, la probabilité d'avalanche est $[1 - (1 - \eta)^k]$, d'où

$$p_{cr} = \sum_{k=1}^{\infty} \mathcal{P}_\mu(k)[1 - (1 - \eta)^k], \tag{3.11}$$

où, comme d'habitude, $\mathcal{P}_\mu(k) = \mu^k \mathrm{e}^{-\mu}/k!$. Définissons ensuite la probabilité p_c qu'il y ait un compte simple causé par un photon ou un compte obscur. Cette probabilité est directement mesurable lorsque le signal optique est activé, il suffit de diviser le nombre de comptes N_c par le nombre d'activations N_a, et, par le

même raisonnement que pour p_{co}, on trouve

$$\bar{p}_c = \frac{N_c}{N_a} \pm \frac{\sqrt{N_c}}{N_a}. \tag{3.12}$$

En supposant que les comptes obscurs et réels sont statistiquement indépendants, on a

$$\begin{aligned} p_c &= p_{cr}(1-p_{co}) + (1-p_{cr})p_{co} + p_{cr}p_{co} && (3.13)\\ &= p_{cr} + p_{co} - p_{cr}p_{co}, && (3.14) \end{aligned}$$

d'où on peut isoler p_{cr}

$$p_{cr} = \frac{p_c - p_{co}}{1-p_{co}}, \tag{3.15}$$

et finalement trouver η en posant l'égalité des équations 3.11 et 3.15 :

$$\frac{p_c - p_{co}}{1-p_{co}} = \sum_{k=1}^{\infty} \mathcal{P}_\mu(k)[1-(1-\eta)^k]. \tag{3.16}$$

3.3.2. Rendement

Le rendement dépend des deux facteurs suivants : (1) la probabilité qu'un photon soit absorbé, (2) la probabilité que le trou généré par absorption déclenche une avalanche. Seules la température et la tension de polarisation influencent le coefficient d'absorption et donc la probabilité d'absorption. Cependant, la probabilité de déclenchement est proportionnelle, en première approximation, à la tension en excès V_E [38] définie comme la différence entre la tension appliquée lors de l'activation et la tension d'avalanche, $V_E = V_{DC} + V_p - V_B$.

L'avantage d'opérer la photodiode en mode Geiger est que cela permet de réduire la probabilité de compte obscur en diminuant le temps d'activation. Par contre, le principal désavantage est que l'on doit connaître le temps d'arrivée du photon. Un autre inconvénient est que l'amplitude de l'avalanche ne dépend pas du nombre de porteurs qui l'ont déclenchée, ce qui rend le détecteur inapte à résoudre le nombre de photons dans l'impulsion.

3.3.3. Re-déclenchement

Un problème propre à l'opération en mode Geiger est un effet secondaire que nous nommons le *re-déclenchement* (*afterpulsing* en anglais) que nous expliquons ici. Lors du processus de fabrication des PDA, des impuretés sont inévitablement introduites dans les couches. Ces impuretés n'ont pas le même nombre de valence que les autres atomes du réseau et forment alors des centres d'attraction (que nous appelons « pièges ») attirant par force électrostatique les charges libres. Les pièges peuvent d'ailleurs capturer les charges libres durant un temps de vie bien défini qui dépend du champ électrique local et de la température [75]. Comme la probabilité de capture par unité de temps de ces pièges augmente avec la densité de charges libres, elles se remplissent durant une avalanche. Si le temps entre deux activations est inférieur au temps de vie des pièges, ces derniers peuvent libérer leur charge libre à l'activation suivante ce qui causera une autre avalanche, et ainsi de suite, jusqu'à ce que les pièges se vident complètement. Cela impose une sévère limite au nombre d'activations du détecteur par unité de temps. Comme le temps de vie des pièges augmente avec la diminution de la température, il y a un compromis à faire entre fréquence d'activation et taux de comptes obscurs. Pour limiter cet effet le plus possible, il faut minimiser le temps d'activation de la PDA, ce qui diminue le nombre de pièges remplis. Choisir V_{DC} le plus près de V_B possible peut également aider, comme cela est suggéré dans la référence [47].

3.3.4. Résolution temporelle

En mode Geiger, le temps de réponse (ou résolution temporelle) non-nul est causé par trois facteurs : (1) la variation de la profondeur d'absorption du photon, (2) le temps de traversée des trous à travers l'hétérojonction InGaAs/InP, et (3) la nature stochastique du processus de multiplication. Les causes (2) et (3) peuvent êtres minimisées en augmentant la tension en excès V_E. Cette propriété est cruciale car elle nous indique le temps minimal d'activation et par conséquent la probabilité minimale de compte obscur par activation qu'il est possible d'atteindre.

3.3.5. Montage

Le circuit d'opération en mode Geiger est illustré à la figure 3.3. Le condensateur C_1 a une capacité de 100 pF de sorte que son impédance à la fréquence de l'impulsion $1/T_p \approx 125$ MHz, en l'occurrence $T_p/2\pi C_1 \approx 12\ \Omega$, soit très faible, permettant ainsi de découpler la tension V_{DC} du générateur d'impulsion. De même, l'inductance $L \approx 100$ mH lui donne une très grande impédance à la fréquence de l'impulsion, soit environ 800 MΩ, mais une résistance nulle à tension continue. Cela permet donc de superposer l'impulsion au niveau V_{DC}. La résistance choisie pour R (50 kΩ) nous assure que le courant d'avalanche ne dépasse pas 2 mA, la limite fixée par le fabriquant.

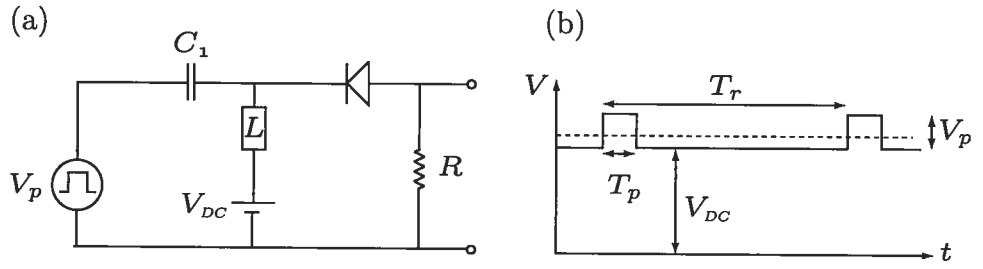

FIG. 3.3 – (a) Circuit d'opération de la PDA, (b) tension appliquée à l'anode de la PDA. La ligne pointillée correspond à V_B.

Les deux photodiodes caractérisées proviennent de *JDS Uniphase*, modèle *EPM 239 AA SS* et sont fibrées. Ce modèle à été choisi car il présentait les meilleures caractéristiques pour la détection de photons selon la littérature [72]. Précisons ici que cette photodiode n'est pas conçue spécifiquement pour être opérée en mode Geiger à basse température. Elle est plutôt conçue pour être opérée à une tension $V < V_B$ avec un courant de fuite minimisé et un facteur de multiplication maximisé à la température de la pièce, des conditions souhaitables pour des applications de télécommunication à faible intensité.

Les PDA sont placées en contact thermique avec un bloc de cuivre (figure 3.4). La chaleur du bloc est pompée par un élément Peltier à trois étages (*Melcor*) dont le côté chaud est en contact avec un dissipateur en cuivre refroidi à l'eau à

7°C. L'eau provient du circuit d'eau du système de climatisation du bâtiment. La température du bloc (et des PDA) est mesurée à l'aide d'une résistance variable en platine (RTD) mise en contact thermique avec ce dernier et dont la résistance est directement proportionnelle à la température. Le tout est placé dans une boîte avec parois en acrylique et partiellement scellée. Un flux constant d'argon est injecté pour éviter la condensation. Avec ce système, nous avons pu atteindre une température minimale de -65°C avec une stabilité de l'ordre de 0,1°C par heure.

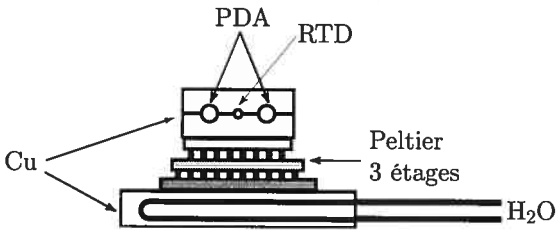

FIG. 3.4 – Système de refroidissement de la PDA.

Le montage complet est schématisé à la figure 3.5. Le laser utilisé est un laser de télécommunication à fréquence accordable sur la bande C (191,0 à 195,5 THz) de *Agilent (modèle 81689A)* ayant une largeur spectrale $\Delta\nu$ de 100 kHz. Selon la relation d'incertitude fréquence-temps $\Delta\nu\Delta t \geq 1/2$, on trouve que la longueur de cohérence du laser est donnée par $L_c = c/2\Delta\nu$, ce qui donne 1500 m dans ce cas-ci. Le laser est d'abord atténué par un atténuateur optique calibré (*JDS Uniphase, HA9*) et ensuite modulé en intensité à l'aide du modulateur électro-optique (**MZ**, *Corning*) basé sur la structure Mach-Zehnder. Le guide d'onde du modulateur est fait de niobate de lithium ($LiNbO_3$) indiffusé au titane et possède un taux d'extinction de 15 dB. La bande passante du modulateur est de 10 Gbit/s, ce qui permet de générer des impulsions optiques de 100 ps ou plus. Comme l'atténuation du modulateur varie en fonction de la température, le modulateur possède une entrée où l'on applique une tension continue et asservie permettant de compenser ce décalage. Nous n'avions pas accès à un tel circuit, si bien que la tension continue était fixée par la source de tension **DC-MZ** à 6,6 V. Malgré cela, nous avons observé que l'intensité maximale ne variait que de 5% ou moins sur une heure, ce

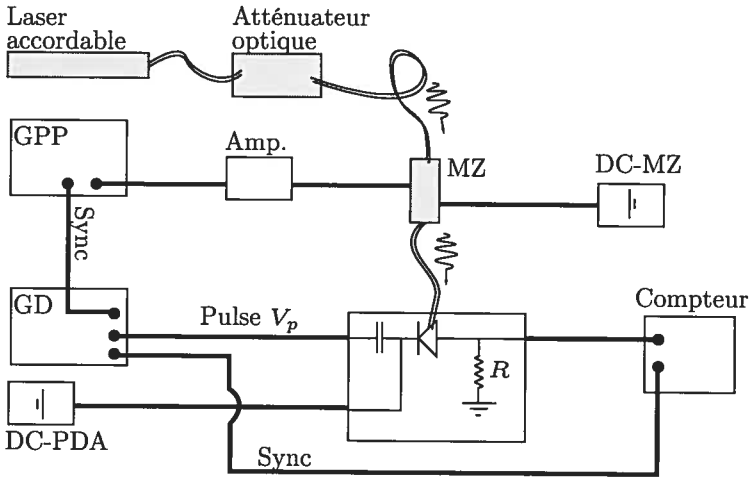

FIG. 3.5 – Montage de caractérisation des PDA. Les traits gras représentent des cables coaxiaux 50 Ω et les traits doubles des fibres optiques SMF28. L'expression « Sync » signifie qu'il s'agit d'un signal logique de synchronisation.

qui était suffisamment stable. Le signal électrique de modulation est produit par le générateur d'impulsions programmable (**GPP**, *Anritsu MP1763C*), dont la sortie est amplifiée par un amplificateur RF (**Amp.**). Ce même **GPP** sert également à synchroniser le générateur de délai (**GD**, *Stanford Research Systems DG-535*) fournissant l'impulsion d'activation d'amplitude V_p à la photodiode. Finalement, le compteur (*Stanford research systems, SR-400*) prend deux signaux en entrées, un provenant du **GD** permettant de compter le nombre d'activations, et un autre de la photodiode permettant de compter le nombre d'avalanches. Les deux entrées en question possèdent un discriminateur programmable et une bande passante de 300 MHz, ce qui permet de compter des impulsions d'avalanche de durée égale à 3 ns ou plus.

3.4. Résultats et discussion

3.4.1. Caractérisation à tension continue

Nous avons caractérisé deux photodiodes que nous avons nommées PDA « 1 » et « 2 ». Elles ont été achetées en février 2003 et mars 2002, respectivement.

Tout d'abord, pour s'assurer que les photodiodes étaient refroidies à la température désirée, nous avons mesuré la tension d'avalanche V_B en fonction de la température. Pour mesurer V_B, il suffit d'augmenter la tension de polarisation jusqu'à la mesure d'un courant de 10 µA, tel que prescrit par le fabriquant. On peut voir la courbe à la figure 3.6 pour la photodiode « 2 », les résultats pour la photodiode « 1 » étant similaires. La courbe est linéaire avec une pente de 0,11 V/°C et une ordonnée à l'origine de 51,1 V.

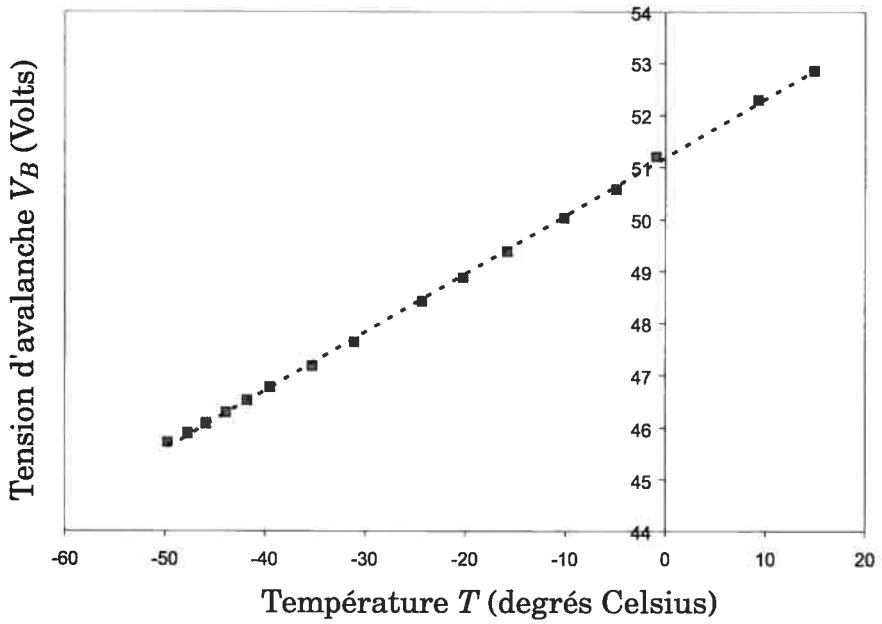

FIG. 3.6 – Tension d'avalanche V_B en fonction de la température pour la photodiode « 2 ». La droite représente la régression linéaire d'équation $V_B(T) = 0{,}11T + 51{,}1$.

Afin de trouver la température minimale d'opération, nous avons mesuré la

tension de pénétration V_{RT} de la photodiode « 2 » à −22, −40 et −52°C. Pour observer l'effet de la tension V_{RT}, nous avons éclairé la photodiode avec une puissance continue de 1 µW à 1550 nm. La courbe est présentée à la figure 3.7. On

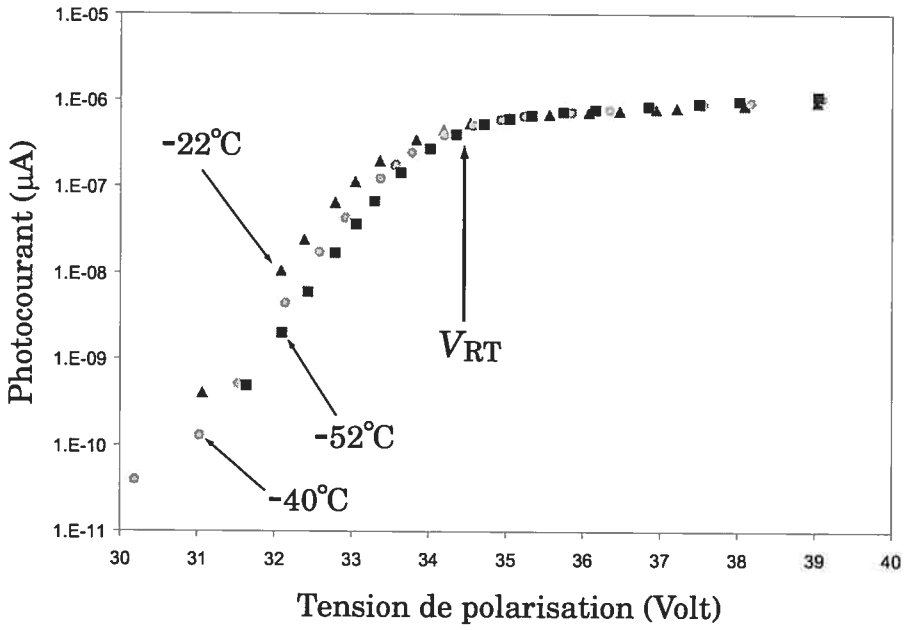

FIG. 3.7 – Photocourant à 1 µW en fonction de la tension de polarisation dans le but de déterminer V_{RT} à −22, −40 et −52°C (photodiode « 2 »).

voit que le photocourant augmente rapidement jusqu'à l'atteinte d'un plateau à 34,5 V indiquant que la région de multiplication a atteint la région d'absorption et que tous les trous sont captés. On voit aussi que cette tension ne dépend pas de la température dans l'intervalle utilisé. En supposant que la variation de V_B continue d'être linéaire à des températures inférieures à −50°C, comme sur la figure 3.7, alors V_B devrait atteindre V_{RT} à −150°C. Notons cependant que cette hypothèse n'est pas justifiée *a priori*. Une étude plus complète serait nécessaire, mais en raison du re-déclenchement, diminuer la température en-deçà de −60°C limite sévèrement la fréquence d'activation de la PDA.

3.4.2. Analyse de l'impulsion d'avalanche

Nous avons débuté la caractérisation en mode Geiger par une analyse de l'impulsion d'avalanche. Pour obtenir les courbes, nous avons branché la résistance R sur un oscilloscope à échantillonnage *Agilent Infinium DCA*.

Premièrement, l'impulsion d'activation V_p fournie par le générateur de délai (GD) avait une largeur à mi-hauteur de 8 ns et un amplitude variable de 0,1 à 4 V. Elle est illustrée à la figure 3.8. On voit que le temps de montée de l'impulsion est d'environ 3 ns, le temps de descente de 2 ns, et la largeur du plateau d'environ 5 ns. Les temps de montée et de descente influencent beaucoup la forme de l'impulsion d'avalanche. En effet, la capacité de la région de déplétion de la photodiode combinée à la résistance de la jonction forment un circuit de charge RC qui produit des impulsions de transition au début et à la fin de l'impulsion d'avalanche, comme illustré à la figure 3.9. Par conséquent, si le temps de montée de l'impulsion d'activation était plus court, cela produirait un effet capacitif de plus grande amplitude qui, à la limite, pourrait masquer complètement l'impulsion d'avalanche. Nous n'avons pas rencontré ce problème ici.

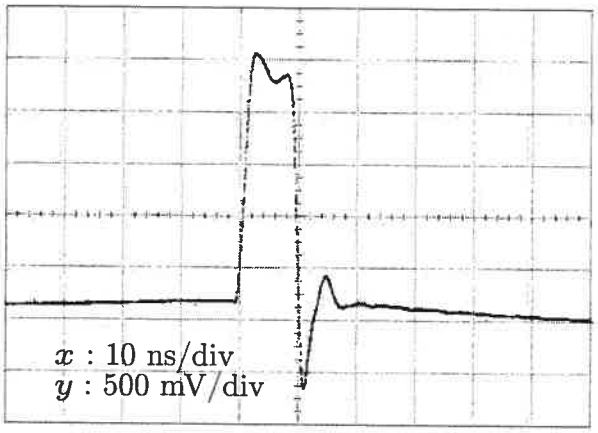

FIG. 3.8 – Forme de l'impulsion d'activation V_p.

Toujours à la figure 3.9, on voit l'impulsion d'avalanche (obtenue avec T_p = 8 ns et $V_p = 2$ V) en opposition au signal sans avalanche. L'amplitude maximale (170 mV) est nettement supérieure à celle de l'effet capacitif ($\approx$ 25 mV), ce qui,

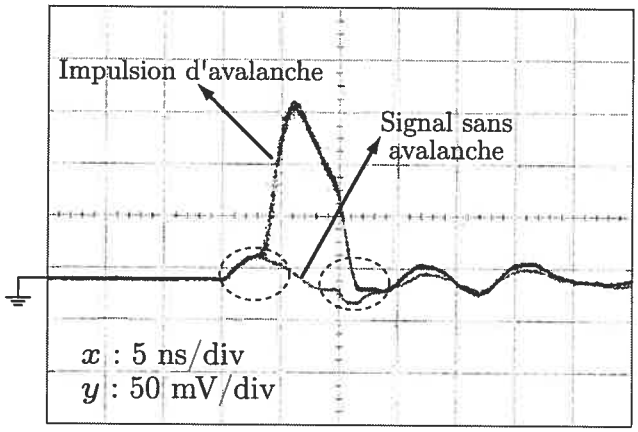

FIG. 3.9 – Forme de l'impulsion d'avalanche pour $T_p = 8$ ns. Les ovales pointillés montrent les lobes causés par la charge et la décharge de la capacité de la photodiode. La courbe supérieure correspond à l'impulsion d'avalanche, tandis que la courbe inférieure correspond au signal sans avalanche.

en fixant le niveau du discriminateur du compteur à 40 mV, permet de compter correctement les avalanches. Notons que l'amplitude de l'impulsion d'avalanche pourrait être plus grande car elle est directement proportionnelle à la tension en excès V_E.

3.4.3. Temps de réponse

Le temps de montée de l'avalanche observée à la figure 3.9 est égal à celui de l'impulsion d'activation, soit de 3 ns. Nous n'étions donc pas en mesure de déterminer le temps de montée de l'avalanche. Cependant, Stucki *et al.* ont rapporté avoir observé un temps de réponse de l'ordre de 400 ps pour le même type de photodiode à une température de -50°C [72] avec une tension en excès de 6 V. La bande passante associée à ce temps de réponse est donnée par $1/2\pi t_r$, où t_r est le temps de réponse. Avec $t_r = 400$ ps, la bande passante est de 400 MHz, et le temps minimal d'activation est de $1/(400\text{ MHz}) = 2$ ns. Ce résultat est décevant comparativement aux temps de réponse typiques obtenus avec les PDA au silicium et germanium en mode Geiger, qui sont de l'ordre de 20 et 85 ps. Il y a

certainement place à l'amélioration.

3.4.4. Rendement et comptes obscurs

Avant de présenter les résultats, mentionnons que toutes les mesures de comptes obscurs et de rendement ont été faites avec $T_p = \tau = 8$ ns, $f_r \equiv 1/T_r = 10$ kHz et $\mu = 0{,}1$ et nous faisions varier V_{DC} et V_p. De plus, la température était ajustée à -50 ou -60°C uniquement. Ce choix à été fait en se basant sur les résultats de [72] montrant que les performances étaient optimales dans cet intervalle de température. Pour déterminer le rendement ainsi que son incertitude, nous faisions une résolution numérique de l'équation 3.16 en tenant compte des trois premiers termes de la somme, les autres étant négligeables en raison du faible μ.

Mentionnons qu'une étude complète du processus de détection nécessiterait de mesurer les dépendances de η et p_{co} envers V_E mais il sera plus simple et visuel d'observer seulement la dépendance de p_{co} envers η, sans se soucier de V_E.

Nous voulions d'abord vérifier que l'amplitude de l'impulsion d'activation n'avait pas d'effet notable sur la courbe de p_{co} en fonction de η. Pour obtenir cette courbe, nous avons fixé $V_p = 2$, 3 ou 4 V, avons fait varier V_{DC} et avons mesuré les valeurs de p_{co} et η correspondantes. Les courbes sont présentées à la figure 3.10 pour la PDA « 2 » à -50°C. Tout d'abord, on voit que p_{co} augmente exponentiellement en fonction de η. La théorie exposée n'est pas suffisante pour expliquer ce résultat et une étude plus poussée doit être accomplie, quoique cela ne soit pas nécessaire ici. On remarque également que les trois courbes sont superposées et donc indépendantes de V_p. Or, seule $V_p = 4$ V permet d'atteindre $\eta \geq 15\%$, ce qui supporte l'hypothèse que $\eta \propto V_E$ (section 3.3.3).

Nous avons ensuite mesuré p_{co} en fonction de η pour les deux photodiodes avec $V_p = 4$ V (fig. 3.11). On voit que le rendement varie entre 2 et 30% pour un taux de compte obscur allant de $1{,}1 \times 10^{-5}$ à $4{,}8 \times 10^{-3}$. Sur l'intervalle de température et de rendement exploré, la figure 3.11 suggère la paramétrisation suivante pour p_{co} :

$$p_{co}(T, \eta) = A(T, \eta)\mathrm{e}^{b\eta}. \tag{3.17}$$

Pour la PDA « 2 », on trouve que $A(-50\text{°C},\eta) \approx 2A(-60\text{°C},\eta)$ (p_{co} double en

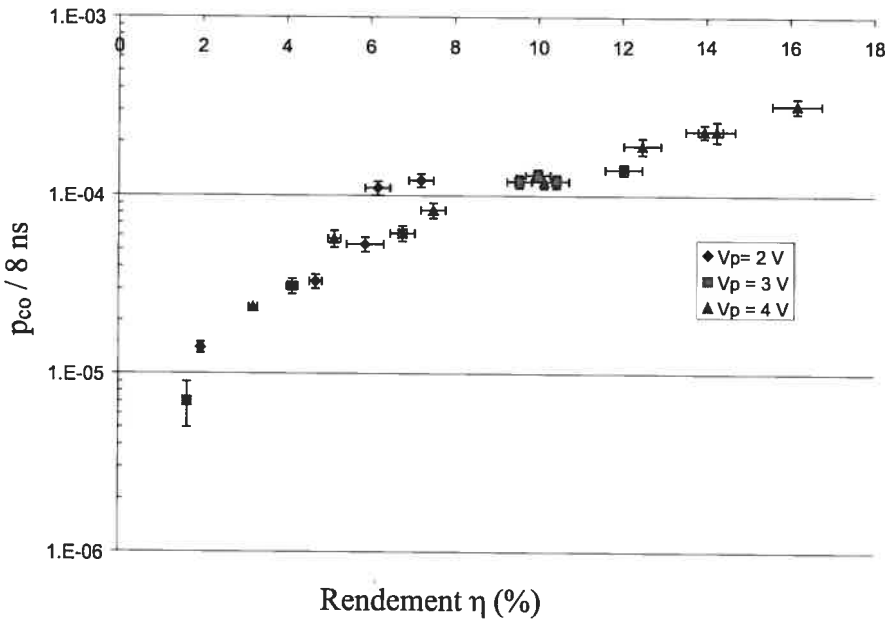

FIG. 3.10 – Effet de l'amplitude V_p de l'impulsion d'activation sur le rendement η.

passant de -50 à -60°C). Plus de points seraient nécessaires pour trouver la forme exacte de $A(T)$, mais on peut supposer qu'elle ressemble à $T^3 \exp(-cT)$ (équ. 3.5). Pour la PDA « 1 », on observe le contraire pour $A(T)$, soit que que $A(-50°C) < A(-60°C)$. Une explication possible de ce comportement est une diminution non-intentionnelle de l'intensité optique causée par l'instabilité du modulateur d'intensité, ce qui aurait entraîné une sous-estimation du rendement. Indépendamment de cela, on remarque qu'à un rendement de 15%, le préfacteur $A(T)$ est environ 8 fois plus que celui de la PDA « 1 », et nous verrons à la section 3.5 que dans ces conditions, ce détecteur est inutilisable pour la CQ.

En guise de comparaison, les meilleurs résultats actuels de la littérature pour le même modèle de détecteur donnent un rendement de 10% pour une probabilité de compte obscur de $2{,}3 \times 10^{-5}$ par 2 ns à une température de -60°C [72]. Dans les mêmes conditions, nous obtenons les valeurs $(1{,}6 \pm 0{,}1) \times 10^{-4}$ (PDA « 1 ») et $(1{,}5 \pm 0{,}2) \times 10^{-5}$ (PDA « 2 »). Les valeurs sont résumées au tableau 3.1. La

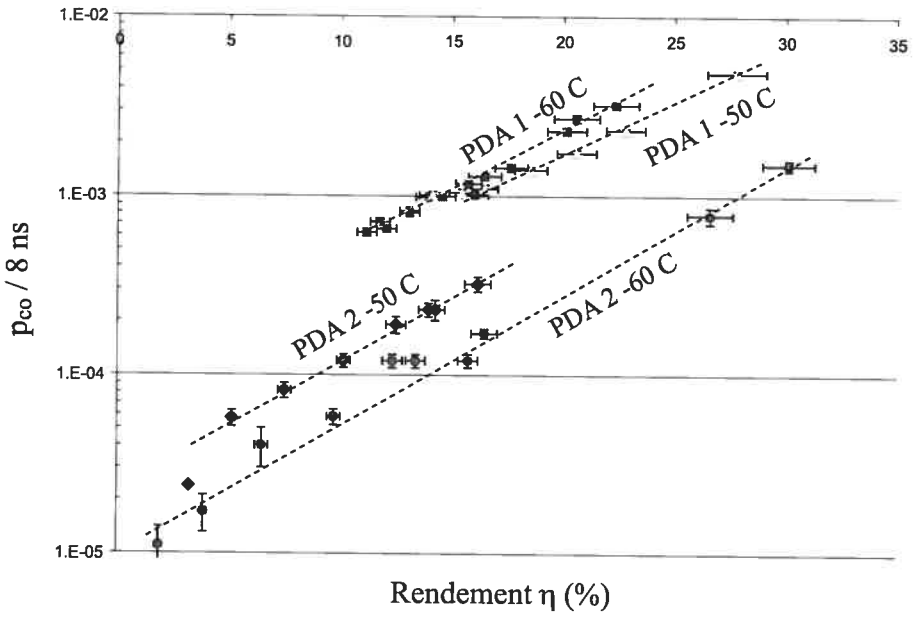

FIG. 3.11 – Probabilité de compte obscur p_{co} par 8 ns en fonction du rendement η pour les deux photodiodes à -50 et -60°C. Les droites pointillées servent différencier les courbes. Elles ne représentent pas des courbes de lissage.

PDA « 2 » offre donc une performance similaire.

Pour compléter l'étude, il faudra vérifier explicitement que l'erreur absolue sur l'estimation de p_{co} et de p_c varie comme $\sqrt{N_{co}}/N_A$ et $\sqrt{N_c}/N_A$. De plus, il faudra caractériser la stabilité de p_{co} et de η en fonction du temps, ce qui dépend de la stabilité en température et de la tension de polarisation V_{DC}. Une telle caractérisation est nécessaire dans le but d'opérer le système pendant une longue période sans interruption.

3.4.5. Re-déclenchement et fréquence d'opération

Dans les mesures de probabilité de compte obscur que nous avons présentées, nous avons supposé que la contribution du re-déclenchement était négligeable. Nous allons maintenant justifier cette supposition. Une étude complète consisterait à déterminer la probabilité $\mathcal{P}_{rd}(nT_r)$ qu'il y ait un re-déclenchement à

	PDA « 1 »	PDA « 2 »	Stucki *et al.*
p_{co}/8 ns ($\eta = 10\%$)	$(6{,}4 \pm 0{,}3) \times 10^{-4}$	$(5{,}9 \pm 0{,}6) \times 10^{-5}$	$9{,}3 \times 10^{-5}$
p_{co}/2 ns ($\eta = 10\%$)	$(1{,}6 \pm 0{,}1) \times 10^{-4}$	$(1{,}5 \pm 0{,}2) \times 10^{-5}$	$2{,}3 \times 10^{-5}$

TAB. 3.1 – Résumé des valeurs de p_{co} mesurées comparées à celles publiées dans la littérature. Ces valeurs sont données pour un temps d'activation de 8 ns (valeur utilisée ici) et de 2 ns (temps minimal d'activation, section 3.4.3).

un temps nT_r suivant une avalanche, et ce pour plusieurs n (entiers positifs) et différents temps de répétition T_r. Cela n'est pas nécessaire car nous ne cherchons pas à maximiser la fréquence d'activation. Au lieu de cela nous avons plutôt mesuré l'augmentation de p_{co} à $\eta = 10\%$ en fonction de la fréquence d'activation $f_r = 1/T_r$ pour les deux PDA. Les résultats sont présentés à la figure 3.12. Les

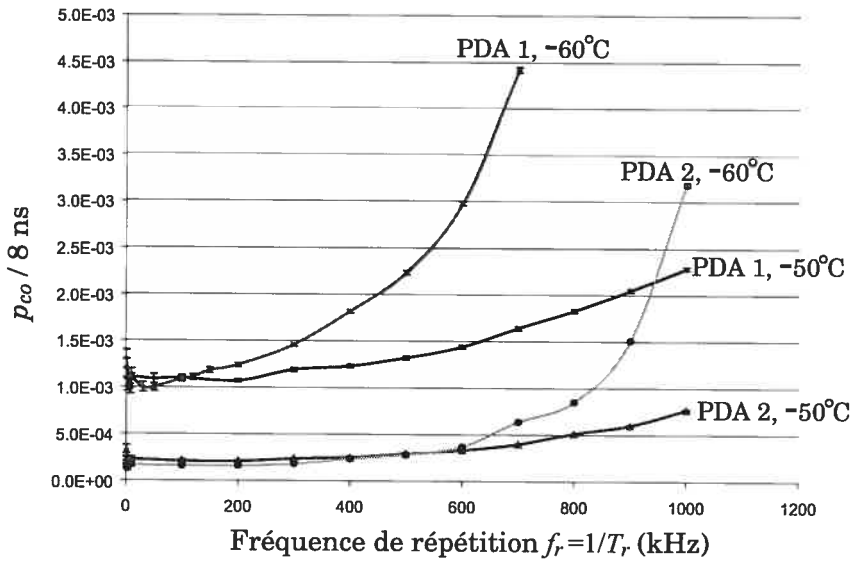

FIG. 3.12 – Augmentation de p_{co} causée par le re-déclenchement en fonction de la fréquence d'activation $f_r = 1/T_r$. $V_p = 4$ V et $\eta = 10\%$.

deux PDA subissent une augmentation de la probabilité de compte obscur avec l'accroissement de la fréquence d'activation. On remarque aussi que la hausse est plus rapide à -60°C, une conséquence de l'augmentation du temps de vie des

pièges lorsque la température diminue (section 3.3.3). Pour se fixer un repère, calculons la fréquence à laquelle p_{co} a doublé par rapport à sa valeur à 10 kHz. À cette fréquence, chaque avalanche cause en moyenne un re-déclenchement. Ce calcul donne 900 kHz (−50°C) et 500 kHz (−60°C) pour la PDA « 1 », et 700 kHz (−50°C) et 600 kHz (−60°C) pour la PDA « 2 ». Ces résultats justifient donc notre supposition de re-déclenchement négligeable à 10 kHz et indique que dans ces conditions d'opérations, la fréquence d'activation doit être inférieure à 500 kHz pour les deux PDA pour éviter le re-déclenchement.

Il serait intéressant d'évaluer la fréquence d'opération maximale à des températures inférieures à −60°C, ce qui n'était malheureusement pas possible avec notre système de refroidissement.

3.5. Application à la cryptographie quantique

Dans cette section, nous calculons le taux d'erreur sur la clé tamisée causé par le bruit des détecteurs et mettons en évidence qu'il s'agit du facteur qui limite grandement la faisabilité de la CQ sur grande distance.

3.5.1. Expression du taux d'erreur

Notons E_d le taux d'erreur induit par le bruit des détecteurs. On considère le montage *Plug&Play* avec deux détecteurs de rendement η et de probabilité de compte obscur par activation p_{co}. Lorsque les bases de préparation et de mesure sont les mêmes, et en supposant que la visibilité d'interférence est de 1, alors une erreur survient lorsque le ou les photons incidents sur le bon détecteur ne sont pas détectés et que, au même moment, un compte obscur survient dans le mauvais détecteur.

On définit d'abord la probabilité qu'il y ait un compte réel dans le bon détecteur comme :

$$p_{cr} = \sum_{k=1}^{\infty} \frac{\mu^k \mathrm{e}^{-\mu}}{k!} [1 - (1 - \eta T_B T_l)^k]. \tag{3.18}$$

$T_l = 10^{-(\alpha l + c)/10}$ est la transmission du lien, α l'atténuation en dB/km, l sa longueur en km et c les pertes constantes en dB (fusions, composants). T_B est la

transmission de l'appareil de Bob.

La probabilité d'obtenir une détection simple (un seul compte) causée par un photon ou un compte obscur dans le bon ou le mauvais détecteur est

$$\begin{aligned} p_c &= [p_{cr}(1-p_{co}) + (1-p_{cr})p_{co} + p_{cr}p_{co}](1-p_{co}) \\ &\quad +(1-p_{cr})(1-p_{co})p_{co} \qquad (3.19) \\ &= p_{cr}(1-p_{co}) + 2(1-p_{cr})(1-p_{co})p_{co}. \qquad (3.20) \end{aligned}$$

La probabilité p_e qu'il y ait un compte obscur dans le mauvais détecteur et aucune détection dans le bon est donnée par

$$p_e = (1-p_{cr})(1-p_{co})p_{co}. \qquad (3.21)$$

Cela nous permet de calculer la probabilité d'erreur sur la clé tamisée par détection E_d :

$$E_d = \frac{p_e}{p_c} = \frac{1}{\frac{p_{cr}}{(1-p_{cr})p_{co}} + 2}. \qquad (3.22)$$

À la limite où $T_l = 0$, on a $p_{cr} = 0$ et alors $E_d = 1/2$, signifiant que seuls les comptes obscurs contribuent à la création de la clé, et que chaque compte survient dans le mauvais détecteur une fois sur deux. À l'aide cette formule, on peut aussi trouver le taux de bruit maximal que l'on peut tolérer sur une distance donnée. Il suffit de fixer E_d et l et d'isoler p_{co} :

$$p_{co} = \frac{E_d p_{cr}}{(1-p_{cr})(1-2E_d)} \qquad (3.23)$$

Si les détecteurs ont des probabilités p_{co} différentes mais un rendement identique, comme c'est le cas des PDA « 1 » et « 2 », le calcul est différent. Soient p_{co1} et p_{co2} ces probabilités, et E_{d1} et E_{d2} les probabilités d'erreur lorsque les détecteurs 1 et 2 correspondent au bon détecteur. Par le même raisonnement fait plus haut, on calcule facilement

$$E_{d1} = \frac{1}{1 + \frac{(1-p_{co2})(p_{cr}+p_{co1}-p_{cr}p_{co1})}{p_{co2}(1-p_{cr})(1-p_{co2})}} \qquad (3.24)$$

et

$$E_{d2} = \frac{1}{1 + \frac{(1-p_{co1})(p_{cr}+p_{co2}-p_{cr}p_{co2})}{p_{co1}(1-p_{cr})(1-p_{co1})}}. \qquad (3.25)$$

Lorsque le taux de bruit n'est pas le même dans les deux détecteurs, cela induit un « biais » dans la clé tamisée car un des détecteurs s'activera plus souvent que l'autre. Pour éliminer ce biais, Bob peut utiliser la stratégie suivante : avant chaque échange de photon, Bob choisit secrètement et au hasard quel détecteur servira à produire un 0 dans la clé tamisée. Cela est très facile à réaliser avec le système *Plug&Play*. Pour le voir, rappelons d'abord que les probabilités de détecter le photon dans les détecteurs D_1 et D_2 sont données par

$$\mathcal{P}(D_1) \propto \cos^2\left(\frac{\Delta\varphi}{2}\right), \qquad \mathcal{P}(D_2) \propto \sin^2\left(\frac{\Delta\varphi}{2}\right), \tag{3.26}$$

où $\Delta\varphi = |\varphi_a - \varphi_b|$, avec $\varphi_a \in_A \{0, \pi/2, \pi, 3\pi/2\}$ et $\varphi_b \in_A \{0, \pi/2\}$. Avec ce choix de phase, un 0 est toujours produit dans le détecteur D_1 ($\varphi_a = 0$ ou $\pi/2$) et un 1 dans le détecteur D_2 ($\varphi_a = \pi$ ou $3\pi/2$). Pour avoir le contraire, il suffit que Bob utilise les phases π et $3\pi/2$, auquel cas les 0 seront produits par D_2 et les 1 par D_1. Bob n'a pas besoin de divulguer ce choix à Alice. Il lui suffit donc de choisir avec une probabilité 1/2 quel ensemble de phase il utilisera, ce qui permet d'éliminer le biais sur la clé. Ainsi, le taux d'erreur moyen $\tilde{E}_d$ est donné par

$$\tilde{E}_d = \frac{E_{d1} + E_{d2}}{2}. \tag{3.27}$$

3.5.2. Taux d'erreur en fonction de la distance

Nous allons maintenant appliquer les formules 3.22 et 3.27 au cas de nos deux détecteurs. Nous utilisons les paramètres suivants dans les calculs : $\alpha =$ 0,22 dB/km, $c = 0{,}5$ dB, $T_B = 3{,}5$ dB et $\mu = 0{,}1$.

Nous considérons dans un premier temps que les deux détecteurs sont identiques et nous prendrons les valeurs du tableau 3.1. Les courbes sont présentées à la figure 3.13. On remarque premièrement que toutes les courbes ont la même allure et que l'effet de la diminution de p_{co} est de décaler les courbes vers la droite. Nous avons vu à la section 1.4.5 qu'un p_{co} supérieur à 13,5% rend impossible l'échange de clé. À la figure 3.13, on voit que le taux d'erreur pour la PDA « 2 » sur 2 ns n'atteint 13,5% qu'à 80 km environ, ce qui est plus grand que la distance maximale de 56 km fixée par l'attaque SNP (section 1.4.3). C'est donc l'attaque

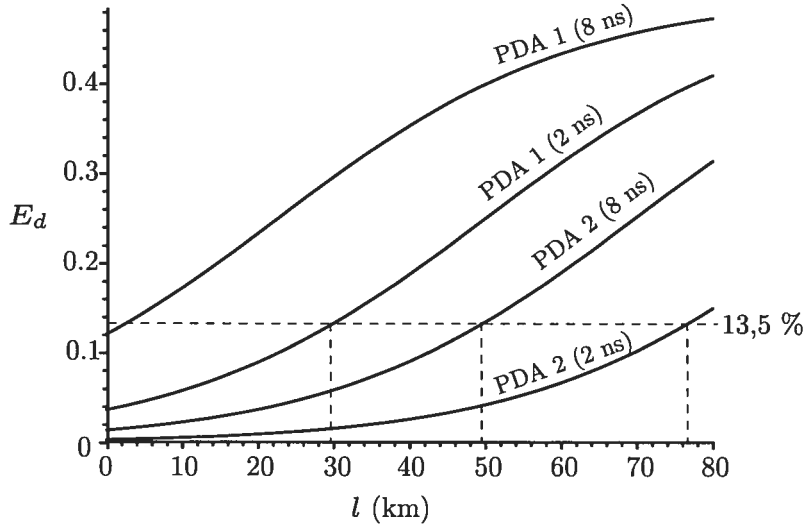

FIG. 3.13 – Taux d'erreur sur la clé tamisée en fonction de la distance causé par le bruit des détecteurs ; cas où les deux détecteurs sont identiques. Voir le tableau 3.1 pour les choix de valeurs de p_{co}.

SNP qui limite la distance maximale dans ce cas. Si on ne tient pas compte de l'attaque SNP, alors cette distance est la distance maximale sur laquelle on peut réaliser le protocole de façon sécuritaire avec ce détecteur.

En fixant $E_d = 13{,}5\%$ dans l'équation 3.23 on peut trouver le p_{co} maximal tolérable en fonction de la distance (voir la figure 3.14). On voit que ce p_{co} maximal diminue exponentiellement avec la distance l. De plus, l'ordonnée à l'origine indique que si $p_{co} > 7{,}4 \times 10^{-4}$ ($l = 0$), alors le détecteur ne peut mener à un échange de clé et ce même à 0 km. Avec un taux de bruit de $6{,}4 \times 10^{-4}$ (PDA « 1 » sur 8 ns), le taux d'erreur induit à $l = 0$ est de 13% indiquant que ce détecteur seul est inutilisable. Dans ce cas, c'est le bruit du détecteur qui fixe la distance maximale.

Si les détecteurs utilisés sont différents, on obtient les courbes présentées à la figure 3.15. On voit que pour une activation sur 8 ns, alors le faible bruit de la PDA « 2 » compense le bruit de l'autre PDA, ce qui rend possible l'échange de clé sur une distance maximale d'environ 20 km. Comme il s'agit des conditions

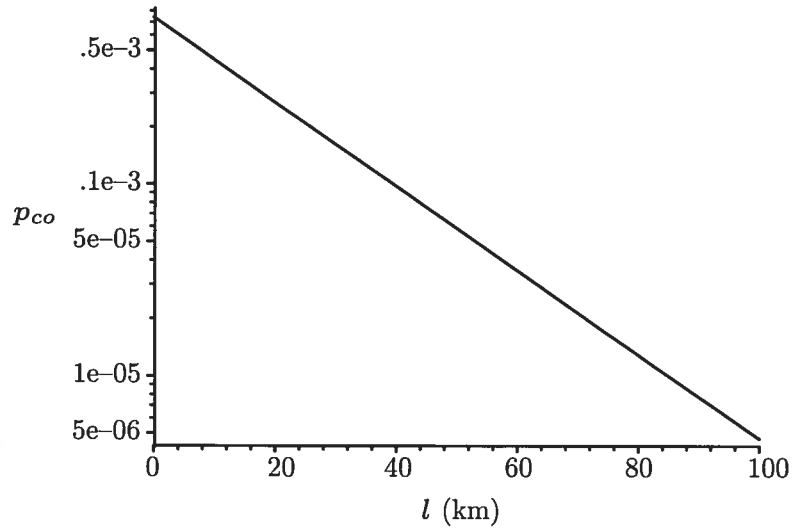

FIG. 3.14 – Taux de bruit maximal tolérable en fonction de la distance.

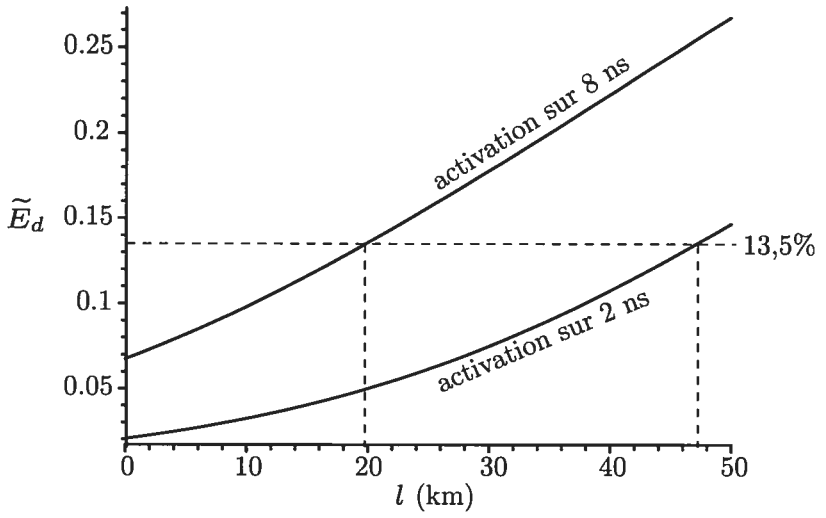

FIG. 3.15 – Taux d'erreur sur la clé tamisée en fonction de la distance causé par le bruit des détecteurs ; cas où les deux détecteurs sont différents.

réelles d'opération, c'est une indication que l'échange de clé sécuritaire est possible avec notre système. Un calcul plus précis de la distance maximale sera fait à la section 4.2.

3.6. Discussion

Quatre points retiennent notre attention.

Premièrement, la détection de photons par utilisation de PDA InGaAs/InP opérée en mode Geiger est, actuellement, la solution la plus simple, la plus rapide et la moins coûteuse à réaliser. Malgré cela, le bruit inévitable qu'elle génère est le facteur le plus important limitant la distance maximale sur laquelle on peut réaliser BB84. Cependant, pour un taux de bruit suffisamment faible ($< 10^{-5}$), ce qui correspond à l'opération de la PDA « 2 » activée sur 2 ns, alors ce n'est plus le cas, ce qui est encourageant. L'amélioration des techniques de microfabrication de dispositifs au InGaAs et InP, ainsi que l'optimisation de la structure des PDA dans le but précis de les opérer en mode Geiger, pourraient probablement mener à l'amélioration du rendement, à la diminution du niveau de bruit et à la réduction du temps de réponse de ces détecteurs.

Deuxièmement, le re-déclenchement est un facteur limitant fortement le taux de génération de clé. Bien que l'ont puisse limiter son effet sur le taux d'erreur, comme l'ont montré Stucki *et al.* [73], on ne peut atteindre une fréquence d'activation supérieure à $\approx$ 10 MHz.

Troisièmement, les bornes sur la distance maximale que nous avons trouvées sont pour un rendement égal à 10%. Si ce rendement augmente, alors il est clair que la limite de distance imposée par l'attaque SNP est repoussée. En principe, avec un détecteur quasi-parfait, la CQ est possible sur des distances supérieures à 100 km.

Quatrièmement, la non-résolution du nombre de photons des détecteurs est également un facteur limitant car il donne plus de liberté à l'espion dans le type d'attaques qu'il peut réaliser [24, 51]. Il s'agit encore une fois d'un aspect à améliorer. Notons que l'utilisation de coupleurs optiques et de boucles de retardement en fibre permet de donner un certain pouvoir de résolution du nombre de photons aux PDA, comme cela a été proposé dans la référence [6].

Actuellement, plusieurs groupes travaillent sur l'élaboration de meilleurs détecteurs. On peut donc s'attendre à ce que prochainement, des détecteurs ultra-rapides, peu bruyants et très efficaces soient construits.

4 — Caractérisation du système de cryptographie quantique à plusieurs participants par multiplexage en longueur d'onde

Dans ce chapitre, nous décrivons d'abord l'architecture d'un réseau en étoile avec multiplexage en longueur d'onde en utilisant le système *Plug&Play*. Nous décrivons ensuite les résultats de la caractérisation du réseau que nous avons construit. Finalement, en prenant en considération les résultats de cette caractérisation, nous calculons le taux d'extraction de la clé prévu en fonction de la distance.

4.1. Réseau en étoile et montage *Plug&Play*

4.1.1. Principe

Dans le but de démontrer que le réseau en étoile avec multiplexage en longueur d'onde proposé peut supporter BB84 (section 2.3.3), nous avons choisi d'utiliser le système *Plug&Play* pour la génération de clé entre le relais et les utilisateurs, comme illustré à la figure 4.1. Le principal avantage découlant de l'utilisation du système *Plug&Play* est qu'il permet de regrouper la génération et la détection des impulsions optiques dans le laboratoire du relais sécurisé. Un atténuateur optique, un détecteur de synchronisation, un modulateur de phase et un miroir de Faraday seulement sont requis pour chaque utilisateur. Cela nous assure que le coût technologique associé à l'ajout d'un nouvel utilisateur n'est pas prohibitif, ce qui permet au réseau de satisfaire la condition d'adaptation énoncée à la section 2.3.1.

Dans le but de conserver le taux de création de clé indépendant du nombre d'utilisateurs, il est possible de modifier le montage du relais de façon à lui permettre de communiquer simultanément avec chaque utilisateur. Pour ce faire, il suffit de multiplexer autant de sources laser que d'utilisateurs et de démultiplexer

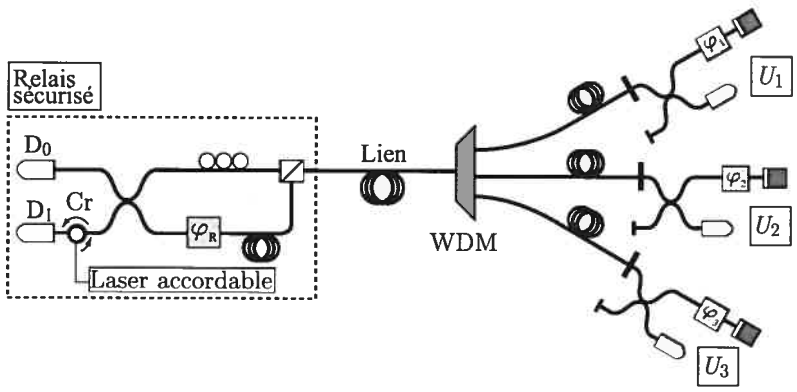

FIG. 4.1 – Réseau en étoile avec WDM et le montage *Plug&Play*.

le signal aux endroits où chaque longueur d'onde doit être modulée ou détectée indépendamment. Le montage présenté à la figure 4.2 illustre le principe pour trois longueurs d'onde différentes. Comparativement au montage de la figure 4.1, trois sources lasers correspondant à trois longueurs d'onde différentes sont multiplexées à l'entrée de l'interféromètre. Elles sont ensuite démultiplexées dans le bras long dans le but de moduler indépendamment leurs phases. Finalement, elles sont démultiplexées à la sortie pour détecter indépendamment les signaux. Ce montage permet de remplir toutes les propriétés recherchées d'un réseau sauf celle de la confidentialité car le relais connaît toutes les clés (section 2.3.1). En particulier, la condition d'adaptation est remplie car seuls un modulateur de phase, un atténuateur optique et un miroir de Faraday sont nécessaires pour chaque utilisateur supplémentaire. La détection, qui présente actuellement le plus grand défi technologique, est concentrée uniquement au relais sécurisé, ce qui facilite s l'ajout d'un nouvel utilisateur.

4.1.2. Description du montage

Rappelons que le montage réalisé ici est une démonstration de principe de la faisabilité de l'utilisation du multiplexage en longueur d'onde avec la cryptographie quantique. L'élaboration d'un système permettant d'implanter toutes les étapes de BB84 nécessite le développement d'électronique de synchronisation et

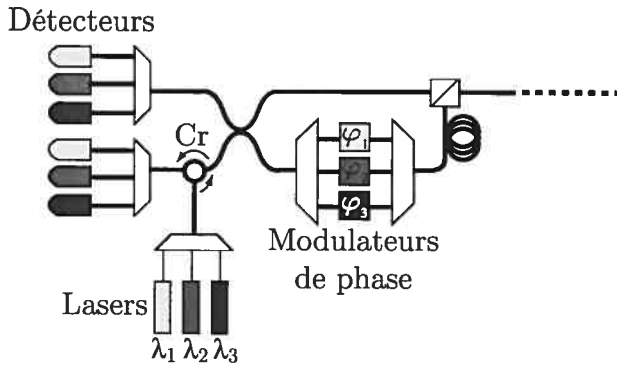

FIG. 4.2 – Montage du relais sécurisé lui permettant de communiquer simultanément avec tous les utilisateurs. Les trois teintes de gris correspondent à trois longueurs d'onde différentes.

d'acquisition qui sont indépendants de l'optique du système. Nous nous sommes concentré sur cette partie optique et nous avons démontré que le lien construit possède une visibilité d'interférence suffisante permettant de réaliser BB84 si nous avions développé l'électronique nécessaire.

Commençons par décrire les appareils du relais sécurisé, qui est illustré à la figure 4.3. Le montage est semblable à celui utilisé pour la caractérisation des détecteurs. En particulier, le générateur d'impulsion programmable (**GPP**) agit toujours en tant qu'horloge de synchronisation des appareils. Les détecteurs D_0 et D_1 pourraient correspondre aux PDA « 1 » et « 2 », mais en réalité, nous n'avons utilisé que la PDA « 2 » en la branchant dans la branche de sortie supérieure ou inférieure. Elle était opérée à -60°C avec une impulsion d'activation d'amplitude V_p égale à 4 V et une durée T_p de 8 ns. Nous sélectionnions la tension d'opération, mesurions le taux de compte obscur et déterminions le rendement en utilisant la courbe de caractérisation obtenue au chapitre 3 (figure 3.11).

Avant de continuer, signalons que tous les composants utilisés possèdent des entrées et sorties fibrées et que l'interféromètre est fait de fibre unimodale *SMF28* de *Corning*. Le circulateur optique **Cr** (*New Focus*) possède une perte d'insertion d'environ 0,6 dB et 65 dB dans les directions de circulation (indiquées par les

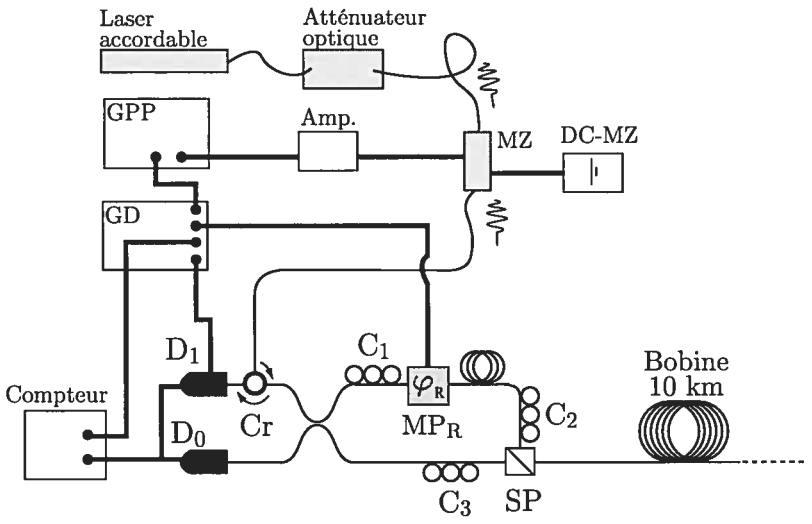

FIG. 4.3 – Montage du relais sécurisé. Les traits gras représentent les cables coaxiaux (50 Ω) et les traits fins représentent des les fibres optiques.

flèche) et de non circulation (directions contraires aux flèches), ainsi qu'une très faible perte dépendante de la polarisation (PDL). Au retour de l'impulsion, la phase est modulée par le modulateur de phase électro-optique ($LiNbO_3$) $\mathbf{MP_R}$ (*JDS Uniphase*). La phase appliquée est proportionnelle à l'amplitude de l'impulsion électrique fournie par le générateur de délai **GD**. Sa bande passante est de 10 GHz, sa perte constante est de 3,5 dB et sa tension $V_\pi \approx 5$ V à 1550 nm.[1] Notons que, contrairement au modulateur d'intensité **MZ**, le modulateur de phase est stable en température. Finalement, de par sa nature, le guide d'onde du modulateur agit comme un polariseur, d'où la nécessité d'utiliser le contrôleur de polarisation $\mathbf{C_1}$. Ce dernier, ainsi que les deux autres contrôleurs $\mathbf{C_2}$ et $\mathbf{C_3}$ (*Thorlabs*) présentent une perte d'insertion inférieure à 0,1 dB et permettent de transformer n'importe quelle polarisation en n'importe quelle autre. Cela permet de maximiser la transmission dans le cube séparateur en polarisation **SP** (*OZ Optics*) qui possède une perte d'insertion de 1 dB. Le lien utilisé est une bobine de fibre d'une longueur de 10 km et une perte constante de 2,28 ± 0,1 dB (0,228 dB/km) à

[1] V_π est la tension nécessaire pour appliquer une phase de π sur l'impulsion optique.

1550 nm, ce qui correspond bien à la perte de 0,22 dB/km utilisée dans les calculs faits aux sections 1.4 et 3.5. La différence de marche entre les deux bras de l'interféromètre est de l'ordre de 20 m, ce qui est inférieur à la longueur de cohérence du laser ($\approx$ 1500 m).

La transmission du système (T_B) est calculée en comparant la puissance continue à l'entrée du circulateur avec celle à la sortie du montage du relais lorsque cette dernière est maximisée en ajustant successivement les trois contrôleurs de polarisation. Typiquement, nous obtenions une perte de 3,8 dB. En réalité, la véritable transmission T_B correspond à cette mesure divisée par la transmission du circulateur, ce qui donne une transmission corrigée correspondant à une perte de $3{,}8-0{,}6 = 3{,}2$ dB. Or, il faut tenir compte de la perte du circulateur car lorsque le photon ressort par cette branche, il est atténué, ce qui diminue la probabilité de le détecter en D_1. Cela induit alors un « biais » vers le bit associé à D_1 dans la clé tamisée. Pour éliminer ce biais, il suffit à Bob de choisir aléatoirement le bit associé à chaque détecteur, comme cela a été suggéré à la section 3.5. Ce détail ne doit pas être pris à la légère, car un biais sur la clé correspond à une fuite d'information vers l'espion. En utilisant cette stratégie, on obtient une transmission correspondant à une perte de $3{,}2 + 0{,}6/2 = 3{,}5$ dB.

Nous passons maintenant au montage des utilisateurs, illustré à la figure 4.4. Nous avons fait la démonstration pour deux utilisateurs et un relais sécurisé. Nous

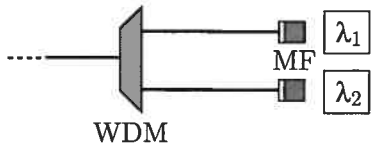

FIG. 4.4 – Montage des utilisateurs. MF = Miroir de Faraday.

n'avions pas de modulateur de phase pour les utilisateurs, mais cela ne change en rien la validité de la démonstration car la puissance dans les branches de sortie ne dépend que de la différence entre les phases appliquées au relais et à l'utilisateur. Cette situation correspond donc à $\Delta\varphi = |\varphi_R|$, où φ_R est la phase appliquée par le relais. Les deux miroirs de Faraday **MF** (*OZ Optics*) comportent une perte d'in-

sertion de 1 dB et possèdent une incertitude de $\pm$ 3° sur la polarisation de sortie, ce qui n'influence pas significativement la visibilité d'interférence. On remarque aussi qu'il n'y pas d'atténuateur. En effet, ils ne sont pas nécessaires car il n'y a pas de modulateur de phase, éliminant alors le besoin d'un détecteur de synchronisation (comme sur la figure 4.1). Par conséquent, il suffit d'ajuster la puissance à la sortie du relais de sorte qu'après la réflexion sur le miroir de Faraday, la puissance corresponde à $\mu = 0{,}1$ photon/impulsion. La distance entre le multiplexeur et les miroirs est de l'ordre de 1 m. Dans le futur, il sera intéressant de recommencer l'expérience avec une plus grande distance entre les deux utilisateurs (qui sont ici côte-à-côte ...) et avec plusieurs étages de multiplexage.

Quant au multiplexeur (**WDM**), nous avons d'abord utilisé un coupleur optique 2×2 (*ITF Technologies optiques*) dont la transmission dans les deux branches de sortie varie en fonction de la fréquence ν du signal optique. Nommons ces branches de sortie 1 et 2. Lorsque la lumière de longueur d'onde λ (dans le vide) est injectée dans la branche d'entrée (branche 0, l'autre branche d'entrée n'est pas utilisée), alors la puissance dans les branches 1 et 2 est donnée approximativement par

$$P_1(\lambda) = P_0 A \sin^2(\alpha\lambda + \beta), \tag{4.1}$$

$$P_2(\lambda) = P_0 A \cos^2(\alpha\lambda + \beta), \tag{4.2}$$

où P_0 est la puissance incidente, A la transmission d'insertion (indépendante de la longueur d'onde λ), et α et β des constantes. La figure 4.5 résume ce comportement. On définit l'espacement entre les canaux comme la différence en longueur d'onde entre le maximum de la branche 1 e le minimum de la branche 2. En tenant compte des formules pour P_1 et P_2, cet espacement est donné par $\pi/2\alpha$. Dans le cas de notre coupleur, l'espacement est de 8 nm et nous avons choisi de l'opérer aux longueurs d'ondes suivantes : $\lambda_1 = 1\,542{,}54$ et $\lambda_2 = 1\,550{,}52$ nm. Il est courant d'exprimer l'espacement en fréquence en utilisant la formule $c(1/\lambda_1 - 1/\lambda_2)$, ce qui donne 1 THz dans ce cas-ci. En pratique, la puissance minimale dans chaque branche n'est pas nulle mais est plutôt donnée par P_{min}. L'isolation en dB entre les canaux correspond au rapport $10\log(P_1(\lambda_1)/P_{\text{min}})$ et est égale à 25 dB pour notre

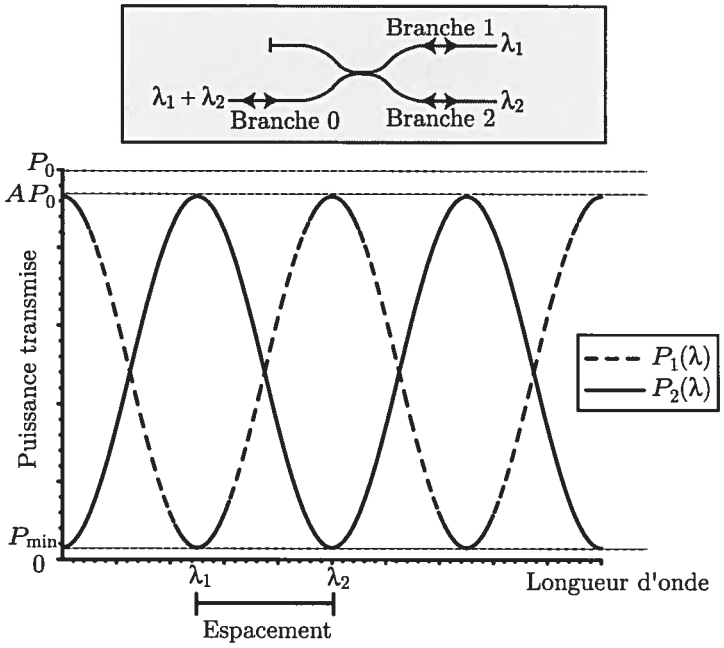

FIG. 4.5 – Transmission en fonction de la longueur d'onde dans un coupleur WDM.

coupleur. Mentionnons également que le coupleur comporte une PDL et une perte d'insertion négligeables ($A \approx 1$), que sa réponse ne dépend pas de la température et qu'il fonctionne dans les deux directions, signifiant par exemple qu'un signal injecté dans la branche 1 avec une longueur d'onde λ_1 sera complètement couplé dans la branche 0 avec la même perte d'insertion que dans l'autre direction.

Dans le but de démontrer le principe avec un composant utilisant le multiplexage dense (DWDM), nous avons également utilisé un multiplexeur 1×4 (*JDS Uniphase*). Contrairement au coupleur WDM, ce composant possède une entrée et quatre sorties. Le spectre de transmission est illustré à la figure 4.6. Pour une puissance P_0 injectée dans l'entrée commune, la puissance dans les quatre branches de sortie est notée $P_i(\lambda)$ ($i = 1, 2, 3, 4$). Ce composant est fait avec un agencement de couches minces dont la transmission dépend de la longueur d'onde. Pour cette raison la dépendance en longueur d'onde des $P_i(\lambda)$ ne varie pas selon $\sin^2(\alpha\lambda)$ comme pour le coupleur WDM. La transmission maximale dans chaque branche est donnée par AP_0 et dans le cas de notre composant, cela correspond à une perte

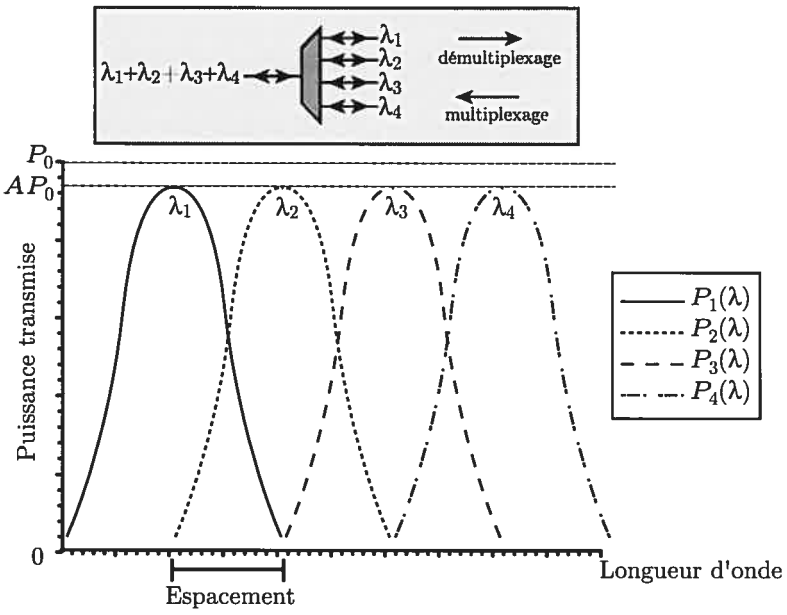

FIG. 4.6 – Transmission en fonction de la longueur d'onde dans le multiplexeur 1×4.

d'insertion de 1 dB et cette perte est stable en température. Les quatre canaux sont alignés sur les longueurs d'onde (fréquence) suivantes :

- λ_1 = 1 548,51 nm (193,6 THz)
- λ_2 = 1 549,32 nm (193,5 THz)
- λ_1 = 1 550,12 nm (193,4 THz)
- λ_1 = 1 550,92 nm (193,3 THz)

L'espacement entre les canaux est de 0,8 nm (100 GHz). L'isolation entre deux canaux adjacents est de 34 dB et de 52 dB entre deux canaux non-adjacents. L'intérêt de démontrer le principe avec ce composant est qu'avec un aussi faible espacement, il serait possible de multiplexer 45 canaux entre les fréquence de 191 à 195,9 THz, ce qui correspondrait à 45 utilisateurs pour un réseau en étoile. Bien entendu, dans le cas précis de ce composant, le réseau serait limité à quatre utilisateurs.

L'introduction du multiplexeur doit se faire avec précautions. En effet, si l'isolation entre deux canaux voisins n'est pas suffisamment grande, alors une fraction

de l'impulsion est dirigée vers le mauvais canal. Si la longueur du lien entre le multiplexeur et les deux utilisateurs est égale à la longueur de l'impulsion optique près (1,6 m dans le cas d'une impulsion de 8 ns), alors les deux impulsions interfèrent au multiplexeur à leur retour mais avec une phase relative aléatoire, ce qui réduit la visibilité d'interférence. Heureusement, avec une isolation de 25 dB entre les canaux, alors la fraction de l'amplitude dirigée vers le mauvais canal est inférieure à 0,3%, ce qui ne peut influencer significativement la visibilité.

Le temps d'aller-retour des photons sur 10 km est de 100 µs environ. La fréquence de répétition est fixée à 5 kHz (200 µs entre les impulsions) nous assurant qu'une seule impulsion était présente dans le lien à la fois pour éviter des erreurs possibles causées par la rétro-diffusion Rayleigh (section 2.2.2). Bien entendu, si notre désir avait été de maximiser la fréquence d'opération, nous n'aurions pas procédé ainsi.

4.1.3. Mesure de visibilité

Impulsions non atténuées

En utilisant le coupleur WDM, nous avons mesuré la visibilité d'interférence avec une impulsion optique non atténuée de 8 ns ayant une puissance maximale à l'entrée du circulateur égale à 1 mW, ce qui donnait une puissance de l'ordre de 20 µW aux détecteurs après avoir parcouru le trajet aller-retour. Pour détecter cette puissance, nous avons utilisé la PDA « 1 » opérée en continu ($V < V_B$) à une température de 6°C et dont la réponse en puissance à été caractérisée précisément. Pour visualiser l'effet d'interférence obtenu, nous avons tracé la puissance mesurée en dB dans les deux branches de sortie de l'interféromètre (correspondant aux détecteurs D_0 et D_1 sur la figure 4.3) en fonction de la phase appliquée au relais et ce pour les deux canaux du coupleur. La puissance de référence utilisée est de 29 µW, soit la puissance maximale mesurée à 1 542,52 nm. Pour une des deux branches de sortie, l'amplitude est maximale pour un déphasage nul (qui est obtenu en n'activant pas le modulateur de phase) et minimale pour un déphasage de π (qui est obtenu en appliquant V_π au modulateur). Cela nous a permis d'étalonner la phase en fonction de la tension appliquée au modulateur.

Les courbes sont présentées à la figure 4.7. On voit que la phase varie de -2 à π

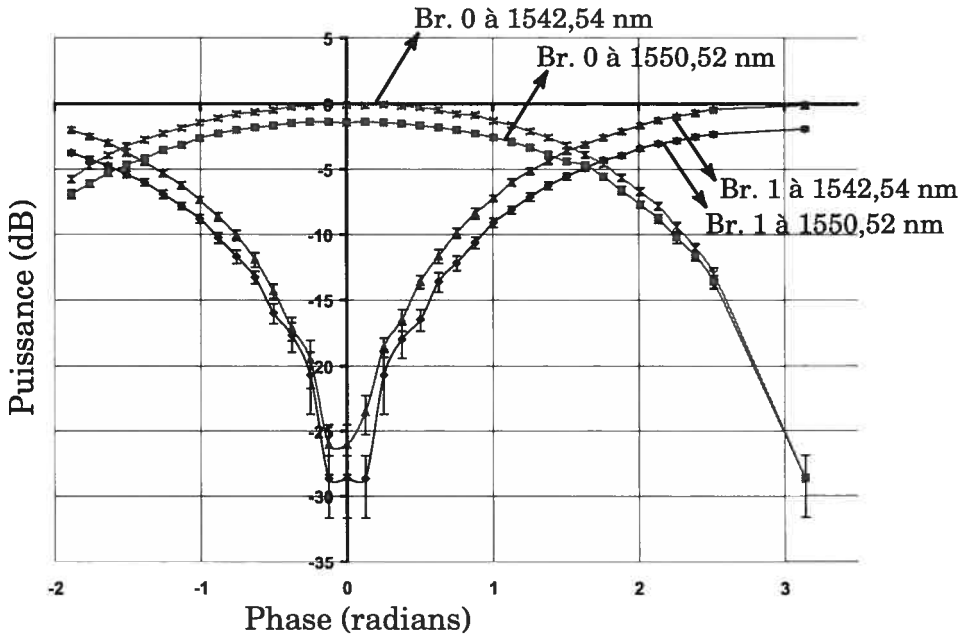

FIG. 4.7 – Puissance de sortie (en dB) dans les deux branches de l'interféromètre à 1 542,54 et 1 550,52 nm. « Br. 0 » signifie branche 0. La puissance de référence utilisée est de 29 µW.

radians. Cela est dû aux limitations du générateur de délai fournissant des impulsions dont l'amplitude varie entre -3 et 4 V. Pour atteindre 5 V (V_π), nous avons utilisé un amplificateur identique à celui utilisé pour moduler l'intensité des impulsions.

On remarque premièrement que la puissance maximale à 1 550,52 nm est inférieure à celle à 1 542,54 nm. Cela est dû au fait que l'atténuation totale, de l'entrée du circulateur jusqu'aux détecteurs, était d'environ 15,2 dB à 1 542,54 nm et de 16,5 dB à 1 550,52 nm. La perte introduite par le circulateur est apparente sur la courbe à 1 550,52 nm lorsqu'on compare l'intensité maximale de la branche 0 avec celle de la branche 1. Selon cette mesure, la perte du circulateur est de l'ordre de 0,52 dB, ce qui correspond à la perte de 0,6 dB mesurée directement.

Deuxièmement, on remarque que la puissance minimale aux deux longueurs

d'onde est constante aux alentours de 0 degré. Ce plateau est causé par le courant d'obscurité du détecteur.

Pour s'assurer que la puissance normalisée dans chaque branche suit bien la loi de Malus, c'est-à-dire

$$\hat{P}_0 = \cos^2\frac{\theta}{2} \quad \text{et} \quad \hat{P}_1 = \sin^2\frac{\theta}{2}, \tag{4.3}$$

où $\hat{P}_0$ ($\hat{P}_1$) est la puissance normalisée dans la branche 0 (branche 1) et θ la phase appliquée, nous avons fait une régression linéaire par la méthode des moindres carrés de la fonction linéaire en θ suivante : $y = \arcsin\hat{P}_0 = a\theta$. Pour la branche 0 à 1 550,52 nm, le calcul donne $a = 0{,}508$ avec un résidu carré moyen égal à 0,003 8, indiquant que la régression est bonne.

Finalement, nous avons calculé la visibilité selon la formule suivante, qui est équivalente à l'équation 2.15,

$$\mathcal{V} = \frac{P_{\text{max}} - P_{\text{min}}}{P_{\text{max}} + P_{\text{min}}} \tag{4.4}$$

et ce pour chaque branche et longueur d'onde. Il est également instructif de mesurer la visibilité en dB à l'aide de la formule suivante :

$$\mathcal{V}_{\text{dB}} = 10\log\frac{P_{\text{max}}}{P_{\text{min}}}. \tag{4.5}$$

Les résultats sont résumés au tableau 4.1. On trouve que les visibilités $\mathcal{V}$ et $\mathcal{V}_{\text{dB}}$ moyennes sont égales à 99,6 $\pm$ 0,2 % et 27 $\pm$ 2 dB respectivement. Le taux d'erreur sur la clé tamisée induit par une telle visibilité est de 0,2 $\pm$ 0,1 % (équ. 2.16), ce qui est négligeable comparativement au taux d'erreur induit par le bruit des détecteurs.

Un point important est à noter. Le fait que la puissance mesurée à l'extinction maximale soit limitée par le bruit des détecteurs, et non par l'interférence, indique que les valeurs rassemblées au tableau 4.1 représentent une borne inférieure à la visibilité. Par conséquent, la visibilité d'interférence est supérieure ou égale à 99,6%.

Impulsions atténuées au niveau du photon individuel

Dans le but de montrer que le système peut être utilisé avec des impulsions ne contenant qu'une fraction de photons, nous avons répété l'expérience mais en

	1 542,54 nm	1 550,52 nm
Branche 0 (%)	99,5 ± 0,2 %	99,6 ± 0,2 %
Branche 0 (dB)	26 ± 2 dB	28 ± 2 dB
Branche 1 (%)	99,7 ± 0,2 %	99,6 ± 0,2 %
Branche 1 (dB)	27 ± 2 dB	27 ± 2 dB

TAB. 4.1 – Visibilités $\mathcal{V}$ et $\mathcal{V}_{\mathrm{dB}}$ mesurées avec des impulsions non-atténuées et le coupleur WDM.

atténuant les impulsions à l'entrée de l'interféromètre du relais de sorte qu'après la réflexion sur le miroir de Faraday, leur puissance corresponde à $\mu = 0{,}1$ sur 8 ns. Pour ajuster la synchronisation entre l'activation de la PDA et l'arrivée du photon, nous faisions varier le délai de l'impulsion d'activation par pas de 1 ns et nous calculions le rapport entre le nombre comptes accumulés (N_c) et le nombre d'activation de la photodiode (N_A). La synchronisation était optimale lorsque la probabilité d'obtenir un compte, $p_c = N_c/N_A$, était maximisée.

Lors de ces mesures, nous avons rencontré une difficulté technique. L'amplificateur utilisé pour atteindre la tension V_π lors des mesures avec impulsions non-atténuées était défectueux. Le déphasage maximal que nous pouvions appliquer au modulateur de phase n'était plus que de 2,5 rad au lieu de π rad. Par conséquent, une mesure précise de la visibilité à l'aide d'impulsions atténuées au niveau du photon individuel n'a pu être réalisée. Cependant, les mesures faites nous montrent que la visibilité est très près de 100%. La figure 4.7 montre que la puissance dans la branche 1 est minimale pour une phase égale à 0 rad. Après avoir correctement synchronisé l'impulsion optique et l'activation du détecteur dans cette branche, nous avons mesuré la valeur de p_c pour une phase égale à 0. En comparant cette valeur au taux de compte obscur lorsque le signal optique est coupé, la différence entre les deux nous donne une indication de la visibilité. En effet, si $p_c \approx p_{co}$, alors l'interférence est destructive et la visibilité est près de 100%. Nous avons effectué cette mesure avec le coupleur WDM et le multiplexeur 1×4. Les résultats sont présentés au tableau 4.2. On voit qu'en tenant compte de l'incertitude absolue, toutes les valeurs sont égales. Cela nous indique deux choses. La première est que

	1 542,54 nm	1 550,52 nm	193,5 THz	193,6 THz
p_c ($\times 10^{-4}$)	0,9 ± 0,1	1,1 ± 0,1	1,1 ± 0,1	1,2 ± 0,1
p_{co} ($\times 10^{-4}$)	1,0 ± 0,1	1,1 ± 0,1	1,0 ± 0,1	1,2 ± 0,1

TAB. 4.2 – Probabilité p_c et taux de compte obscur dans la branche 1 de l'interféromètre avec le coupleur WDM (canaux écrits en longueur d'onde) et le multiplexeur 1×4 à espacement de 100 GHz (canaux écrits en fréquence) avec une phase appliquée de 0 rad.

la visibilité est très près de 100%, et la deuxième est que nos mesures ne sont pas assez précises pour le déterminer correctement. Dans les mesures futures, il faudra accumuler plus de comptes pour diminuer l'incertitude et espérer discerner p_c de p_{co}.

Bien que nous ayons démontré que l'interférence est observable avec $\mu = 0{,}1$, la caractérisation n'est pas complète. En particulier, il faut tracer la variation de p_c en fonction de la phase appliquée pour $\varphi = 0$ à π. Ensuite, nous devons mesurer précisément le « biais » sur la clé introduite par le circulateur. Finalement, nous devons nous assurer que la quantité de photons reçus correspond bien aux pertes du lien.

4.1.4. Stabilité

Un inconvénient de notre système est que l'ajustement des contrôleurs de polarisation dépend de la longueur d'onde. En pratique, nous avons observé que cette dépendance est faible, mais elle rend tout de même nécessaire le ré-ajustement des contrôleurs lorsque la longueur d'onde est changée de quelques nm ou plus. De plus, cet ajustement dépend de la température et doit être refait au bout d'un certain temps. Une solution simple à ces deux problèmes consiste à utiliser de la fibre à maintien de polarisation pour le montage du relais. Une autre amélioration consisterait à remplacer le cube séparateur en polarisation (voir la figure 4.3) par un coupleur séparateur en polarisation qui possède typiquement une très faible perte d'insertion.

4.2. Taux d'extraction de la clé

Maintenant que nous avons montré que la visibilité de notre système influence de façon négligeable le taux d'erreur sur la clé tamisée sur 10 km, nous supposons que cela est vrai à plus grande distance et nous procédons au calcul du taux d'extraction de la clé finale. Cette supposition est justifiée par les résultats obtenus par d'autres groupes qui ont mesuré une visibilité de 99% sur une distance de 67 km avec un montage similaire [73]. Le but est d'évaluer la probabilité $R_p(l)$ qu'une impulsion à la sortie du laboratoire du relais produise un bit de la clé finale, après correction des erreurs et distillation de secret, où l est la distance entre le relais et l'utilisateur. Cette probabilité est donnée par l'expression suivante :

$$R_p(l) = \frac{1}{2} p_c(l) f_c(l) f_{ds}(l). \tag{4.6}$$

Le facteur $1/2$ correspond à la probabilité que les bases de préparation et de mesure soient compatibles, $p_c(l)$ est la probabilité d'enregistrer un compte simple (réel ou obscur) chez l'utilisateur, et $f_c(l)$ et $f_{ds}(l)$ sont les facteurs de réduction de la clé tamisée associés à la correction d'erreur et à la distillation de secret.

Nous ferons un calcul dans la limite asymptotique où la clé tamisée est de longueur $n = 10^9$. Dans cette situation, on peut modifier le facteur $f_{ds}(l)$ de la façon suivante (équation 1.24) :

$$f_{ds} = \frac{n-k-s}{n} = 1 - \frac{k}{n} - \frac{s}{n} \to 1 - I(l) - \gamma, \tag{4.7}$$

où n est la longueur de la clé tamisée, k le nombre de bits connus par l'espion, s le facteur de sécurité arbitraire et $\gamma = s/n$. Nous avons utilisé l'égalité $k/n = I(l)$ valable dans la limite asymptotique. $I(l)$ est l'information de Shannon sur chaque bit de la clé tamisée de l'espion en fonction de la distance. En effet, si l'espion connaît avec certitude la valeur de k bits sur n, et qu'il n'a aucune idée de la valeur des autres bits, alors son information moyenne par bit est k/n. Pour obtenir l'expression de $I(l)$, il suffit de combiner les équations 1.43, 3.27 et 3.18.

Rappelons également que l'information de l'espion sur chaque bit de la clé finale, après distillation de secret, est donnée par :

$$I_f = \frac{2^{-s}}{(n-k-s)\ln 2} \to \frac{2^{-\gamma n}}{n f_{ds} \ln 2}, \tag{4.8}$$

où la flèche indique le résultat dans la limite asymptotique. On remarque que comme n est très grand, alors on peut poser $\gamma = 0$, ce qui correspond à un facteur de sécurité égal à 0. Nous obtenons quand même $I_f \sim 1/n = 10^{-9}$ bit, ce qui est négligeable. Cette approximation permet de simplifier les calculs.

Il faut maintenant évaluer la probabilité d'obtenir un compte simple $p_c(l)$ en fonction de la distance. Nous considérons trois cas. Dans un premier temps nous supposons que les deux détecteurs utilisés sont les PDA « 1 » et « 2 » activées sur 8 ns. Dans un deuxième temps nous prenons les mêmes photodiodes mais avec une activation de 2 ns dans le but de réduire le bruit. Dans un troisième et dernier temps nous supposons que les deux détecteurs ont un p_{co} égal à celui de la PDA « 2 » activée sur 2 ns. Le calcul de $p_c(l)$ à déjà été fait pour le troisième cas ; il correspond à l'équation 3.20 et on peut l'utiliser directement dans l'équation du taux d'extraction (4.6). Cependant, dans les deux premiers cas, les taux de comptes obscurs sont différents pour les deux détecteurs, ce qui nécessite d'utiliser la stratégie d'assignation aléatoire de la valeur des bits (section 3.5). La probabilité d'obtenir un compte simple est donc la moyenne de celle pour chaque détecteur, et selon le même raisonnement utilisé pour obtenir l'équation 3.20, on trouve que

$$\tilde{p_c}(l) = \frac{p_{c1}(l) + p_{c2}(l)}{2} \tag{4.9}$$

$$= \frac{1}{2} p_{cr}(2 - p_{co1} - p_{co2}) + (1 - p_{cr})(p_{co1} + p_{co2} - 2p_{co1}p_{co2}). \tag{4.10}$$

Nous prenons toujours les valeurs suivantes pour les paramètres de l'expérience : $\alpha = 0{,}22$ dB/km, $c = 0{,}5$ dB, $T_B = 3{,}5$ dB et $\mu = 0{,}1$. Le résultat du calcul du taux d'extraction $R_p(l)$ en fonction de la distance l est présenté à la figure 4.8.

On remarque que la diminution du taux d'extraction est d'abord exponentielle en raison de l'absorption de la fibre. Ensuite, elle devient surexponentielle à l'approche de la distance limite qui est fixée soit par le bruit des détecteurs, comme c'est le cas pour la courbe 1, ou soit par l'attaque SNP, ce que est le cas de la courbe 3. Avec $\mu = 0{,}1$ et un rendement de 10%, la courbe 3 représente la limite maximale du taux d'extraction. Les limites approximatives de distance sont de 26, 46 et 54 km pour les courbes 1, 2 et 3 respectivement. Si on ne tient pas compte de l'attaque SNP, alors la limite maximale est repoussée à 80 km approximativement

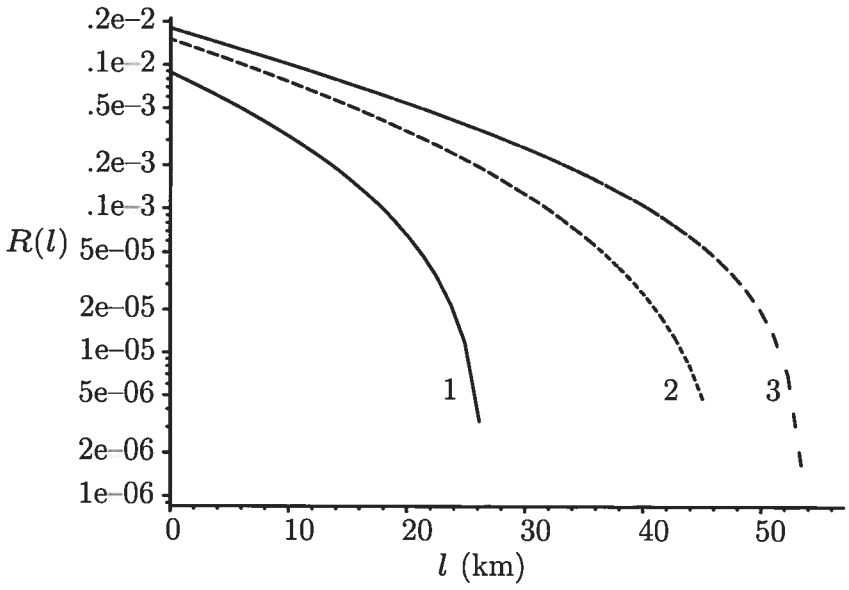

FIG. 4.8 – Taux d'extraction de la clé en fonction de la distance. Les trois courbes correspondent aux trois cas expliqués dans le texte (les valeurs sont prises au tableau 3.1). En particulier, la courbe 1 correspond à $p_{co1} = 6{,}4 \times 10^{-4}$ et $p_{co2} = 5{,}9 \times 10^{-5}$, la courbe 2 à $p_{co1} = 1{,}6 \times 10^{-4}$ et $p_{co2} = 1{,}5 \times 10^{-5}$, et la courbe 3 à $p_{co} = 1{,}5 \times 10^{-5}$.

(section 3.5).

Pour trois raisons que nous énumérons ici, ces courbes représentent une borne supérieure au taux d'extraction. Premièrement, les attaques proposées ne sont pas optimales. Deuxièmement, le facteur de réduction de la clé par la correction d'erreur, $f_c(l)$ est lui-même une borne inférieure au facteur réel lorsque le taux d'erreur est de l'ordre de 10%. Finalement, le traitement de l'attaque SNP que nous avons fait n'est qu'approximatif car il ne tient pas compte des impulsions à trois photons et plus qui permettent à l'espion d'obtenir plus d'information que ce nous avons trouvé en les négligeant.

Maintenant, en supposant que le taux de répétition de l'expérience est de 1 MHz, alors sur une distance de 20 km le système permet de créer 50, 350 et 600 bits de clé finale par seconde dans les trois cas explorés. Pour un réseau en

étoile comme celui que nous avons construit, on doit diviser ce taux de création par le nombre d'utilisateurs.

Un taux de 600 bits par seconde est très bon, mais bien entendu, le développement futur de détecteurs moins bruyants et ayant un rendement supérieur à 10% permettra de faire grimper ce taux ainsi que la distance maximale d'application.

Terminons ce chapitre en mentionnant qu'il est possible, en principe, d'optimiser les conditions d'opération du détecteur de façon à maximiser la distance et le taux d'extraction de la clé finale. Les paramètres à optimiser sont le nombre de photons par impulsion (μ), le rendement (η), le taux de bruit des détecteurs (p_{co}) ainsi que la fréquence de répétition des impulsions optiques (f_r). Comme le rendement ne dépend que de p_{co}, et que ce dernier est fixé par la tension en excès du détecteur et la fréquence de répétition, alors cela se ramène à une optimisation à trois paramètres, soit V_E, f_r et μ.

Conclusion

Dans ce mémoire nous avons tout d'abord introduit les concepts à la base de la cryptographie quantique et présenté les protocoles BB84 et EPR. Par la suite, nous avons décrit les outils nécessaires à l'analyse de la sécurité de BB84 en considérant les attaques « interception-renvoi » (I-R) et « séparation du nombre de photons » (SNP). En particulier, pour les conditions de cette expérience, nous avons montré que si la probabilité de compte obscur par activation des détecteurs, p_{co}, est inférieure à 10^{-5}, et que si le rendement est de 10%, alors la distance maximale sur laquelle BB84 peut être réalisé est fixée non pas par le bruit des détecteurs mais par l'attaque SNP. Cette limite est égale à 56 km.

Forts de ces explications, nous avons décrit le montage *Plug&Play* permettant d'implanter BB84 sur fibre optique et nous avons proposé une architecture optique de réseau en étoile utilisant le multiplexage en longueur d'onde. Cette architecture peut être utilisée avec BB84, ce qui nécessite l'utilisation de relais sécurisés. On peut s'affranchir de cette difficulté en utilisant le protocole EPR avec des photons intriqués en fréquence. Il s'agit, au meilleur de notre connaissance, de la première proposition de ce genre.[2] Nous avons ensuite discuté du multiplexage dense de canaux classiques et quantiques et noté que les effets non-linéaires induits par le canal classique pourraient être néfastes à l'encodage de l'information quantique dans la fibre.

Nous avons ensuite décrit les travaux de développement et de caractérisation d'un détecteur de photons réalisé avec une photodiode à avalanche InGaAs/InP refroidie à -60°C et opérée en mode Geiger. Le taux de bruit obtenu est comparable aux résultats publiés dans la littérature. En tenant compte de ces perfor-

[2]Un projet visant à démontrer ce principe est d'ailleurs en cours au Laboratoire des fibres optiques de l'École Polytechnique de Montréal.

mances, nous avons calculé le taux d'erreur sur la clé tamisée induit par le bruit des détecteurs en fonction de la distance. Nous avons déduit que dans les conditions d'opération de cette expérience, une probabilité p_{co} supérieure à 7×10^{-4} rend impossible l'extraction de clé et ce même sur une distance de 0 km.

Finalement, nous avons construit un réseau en étoile avec multiplexage en longueur d'onde. Le réseau comporte deux utilisateurs reliés au relais sécurisé par 10 km de fibre optique. Le système *Plug&Play* a été utilisé ainsi que deux multiplexeurs ayant un espacement de 8 et 0,8 nm respectivement. Cela a permis de montrer que, en principe, la cryptographie quantique peut être implantée sur des réseaux optiques utilisant le multiplexage dense qui pourraient supporter plusieurs utilisateurs. La visibilité d'interférence mesurée à l'aide d'impulsions non atténuées est de l'ordre de 99,6%. Nous avons également montré que la visibilité d'interférence obtenue avec des impulsions atténuées à une fraction de photon est très près de 100%. Cela nous a permis de négliger le taux d'erreur induit par l'imperfection de l'interférence et de calculer le taux d'extraction de la clé finale en fonction de la distance. Nous avons montré qu'avec les conditions d'opération actuelles des détecteurs, nous pourrions extraire un maximum de 50 bits de clé par seconde sur une distance de 20 km. Pour un réseau à N utilisateurs, ce taux doit être divisé par N.

Beaucoup de travail reste à faire. Premièrement, au niveau du détecteur de photons, il faut caractériser la probabilité de re-déclenchement en fonction de la fréquence d'activation dans le but d'augmenter le taux de génération de clé. Il faut également mesurer son temps de réponse et déterminer son temps minimal d'activation. La PDA « 1 » devra être remplacée car l'important taux de bruit qu'elle comporte limite grandement la distance maximale de sécurité, comme nous l'avons vu au chapitre 3. Deuxièmement, le réseau en étoile construit doit être complété pour permettre une véritable génération sécuritaire de clé avec BB84. Plusieurs étages de multiplexage pourraient êtres ajoutés dans le but de démontrer le principe avec un nombre d'utilisateurs supérieur à quatre. Les conditions d'opération devront également être optimisées dans le but de maximiser le taux d'extraction de la clé en fonction de la distance. Troisièmement, nous allons tenter de démontrer

expérimentalement que la génération de clé avec photons intriqués en fréquence (en utilisant le protocole EPR) est possible sur le réseau en étoile avec multiplexage en longueur d'onde, comme nous l'avons proposé au chapitre 2. Quatrièmement, comme nous l'avons mentionné au chapitre 2, une étude de la faisabilité de la cryptographie quantique sur un réseau optique où sont multiplexés simultanément des signaux à un photon et des signaux à haute puissance devra être faite.

Le travail de ce mémoire à mené à une publication scientifique [16].

Bibliographie

[1] G.P. Agrawal. *Nonlinear Fiber Optics, Third Edition*, Academic Press (2001).

[2] G.P. Agrawal. *Fiber-Optic Communication Systems, Third Edition*, Wiley Interscience (2002).

[3] G.B. Arfken et H.J. Weber. *Mathematical Methods for Physicists, Fourth Edition*, Academic Press (1995).

[4] N.W. Ashcroft et N.D. Mermin. *Solid State Physics*, Saunders College Publishing (1976).

[5] A. Aspect, P. Grangier et G. Roger. Experimental tests of realistic local theories via Bell's theorem, *Phys. Rev. Lett.* **47**, 460-463 (1981).

[6] K. Banaszek et I.A. Walmsley. Photon counting with a loop detector, *Optics Letters* **28**, 52–54 (2003).

[7] H. Barnum, C. Crépeau, D. Gottesman, A. Smith et A. Tapp. Authentication of quantum messages, arXiv : quant-ph/0205128, (2002).

[8] J.S. Bell. On the problem of hidden variables in quantum mechanics, *Rev. of Modern Physics* **38**, 447–452 (1964).

[9] C.H. Bennett. Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett.* **68**, 3121–3124 (1992).

[10] C.H. Bennett et G. Brassard. Quantum cryptography : public key distribution and coin tossing, *Int. Conf. Computers, Systems & Signal Processing, Bangalore, India* (IEEE New York), 175–179 (1984).

[11] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail et J. Smolin. Experimental quantum cryptography, *Journal of Cryptology* **5**, 3–28 (1992).

[12] C.H. Bennett, G. Brassard, S. Breidbart et S. Wiesner. Quantum cryptography, or unforgeable subway tokens, *Advances in Cryptology : Proc. of Crypto '82*, 267–275 (1982).

[13] E. Biham, M. Boyer, P.O. Boykin, T. Mor et V. Roy-chowdurry. A proof of the security of quantum key distribution, *Proc. of the 32nd Annual ACM Symposium on Theory of Computing* (ACM Press, New York), 715–724 (2000).

[14] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres et W. Wootters. Teleporting an unknown quantum state via dual EPR and classical channels, *Phys. Rev. Lett.* **70**, 1895–1898 (1993).

[15] C.H. Bennett, G. Brassard, C. Crépeau et U.M. Maurer. Generalized privacy amplification, *IEEE Transactions on Information Theory* **41**, 1915–1923 (1995).

[16] G. Brassard, F. Bussières, N. Godbout et S. Lacroix. Multi-user quantum key distribution using wavelength division multiplexing, *Proc. of Photonics North 2003* (SPIE), à paraître (2003).

[17] C.H. Bennett, G. Brassard et N.D. Mermin. Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* **68**, 557–559 (1992).

[18] C.H. Bennett, G. Brassard et J.-M. Robert. Privacy amplification by public discussion, *SIAM Jour. of Computing* **17**, 210–229 (1988).

[19] H. Barnum, C.M. Caves, C.A. Fuchs, R. Jozsa et B. Schumacher. Noncommuting mixed states cannot be broadcast, *Phys. Rev. Lett.* **76** 2818–2821 (1996).

[20] D.S. Bethune et W.P. Risk. Autocompensating quantum cryptography, *New Journal of Physics* **4**, 42.1–42.15 (2002).

[21] G. Brassard, N. Lütkenhaus, T. Mor et B.C. Sanders. Limitations on practical quantum cryptography, *Phys. Rev. Lett.* **85**, 1330–1333 (2000).

[22] G. Brassard et L. Salvail. Secret-key reconciliation by public discussion, *Lecture Notes in Computer Science* **765** (Springer-Verlag, New York) 410–423 (1994).

[23] M. Born et E. Wolf. *Principles of Optics, Seventh Edition*, Cambridge University Press (1999).

[24] J. Calsamiglia, S,M. Barnett et N. Lütkenhaus. Conditional beam-splitting attack on quantum key distribution, *Phys. Rev. A* **65**, 012312 (2002).

[25] J. L. Carter et M. N. Wegman. New hash functions and their use in authentication et set equality, *IEEE Trans. Inform. Theory* **44**, 265–279, (1981).

[26] Spécification prise sur le site de Corning, `http://www.corning.com`.

[27] C. Cohen-Tannoudji, B. Diu et F. Laloë. *Mécanique Quantique, Tome 1*, Hermann (1996)

[28] T. Cover et J. Thomas. *Elements of Information Theory*, Wiley & Sons, New York (1991).

[29] W. Diffie et M. E. Hellman. New directions in cryptography, *IEEE Transactions on Information Theory* **IT-22**, 644–654 (1976).

[30] D. Dieks. Communication by EPR devices, *Phys. Lett. A* **92**, 271-272 (1982).

[31] C. Elliott. Building the quantum network, *New Journal of Physics* **4**, 41.6–41.12 (2002).

[32] A. Einstein, B. Podolsky et N. Rosen. Can quantum-mechanical description of physical reality be considered complete?, *Phys. Rev.* **47**, 777-780 (1935).

[33] A. Ekert. Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661–663 (1991).

[34] J.D. Franson. Bell inequality for position and time, *Phys. Rev. Lett.* **62**, 2205–2208 (1989).

[35] J.D. Franson et B.C. Jacobs. Operational system for quantum cryptography, *Elect. Lett.* **31**, 232–234 (1995).

[36] N. Gisin, G. Ribordy, W. Tittel et H. Zbinden. Quantum cryptography, *Rev. of Mod. Phys.* **74** 145–195 (2002).

[37] G.R. Grimmett et D.R. Stirzaker. *Probability and Random Processes*, Clarendon Press, Oxford (1992).

[38] P. Hiskett, G. Buller, A. Loudon, J. Smith, I. Gontjio, A. Walker, P. Townsend et M. Roberston. Performance and design of InGaAs/InP photodiodes for single-photon counting at 1.55 μm, *Applied Optics* **39**, 6818–6829 (2000).

[39] M. Horodecki. Entanglement measures, *Quantum Information and Computation* **1**, 3–26 (2001).

[40] R. Hughes, G. Morgan et C. Peterson. Quantum key distribution over a 48 km optical fibre network, *J. Modern Optics* **47**, 533–547 (2000).

[41] B. Huttner, J.-D. Gauthier, A. Muller, H. Zbinden et N. Gisin. Unambiguous quantum measurement of non-orthogonal states, *Phys. Rev. A* **54**, 3783–3789 (1996).

[42] H. Inamori, N. Lütkenhaus et D. Mayers. Unconditional security of practical quantum key distribution, `http://arxiv.org/abs/quant-ph/0107017` (2001).

[43] I.P. Kaminow et T.L. Koch. (Éditeurs) *Optical Fiber Telecommunications IIIA*, Academic Press (1997).

[44] M. Koashi et J. Preskill. Secure quantum key distribution with an uncharacterized source, *Phys. Rev. Lett.* **90**, 057902 (2003).

[45] H. Kosaka, A. Tomita, Y. Nambu, T. Kimura et K. Nakamura. Single-photon interference experiment over 100 km for quantum cryptography system using a balanced gated-mode photon detector, Soumis à *Elec. Letters.* `http://arxiv.org/abs/quant-ph/0306066` (2003).

[46] P. Kumar, X. Li, M. Fiorentino, P.V. Loss, J.E. Sharping et G. Balbosa. Fiber-optic sources of quantum entanglement, *Proc. of 6th Intern. Conf. on Quantum Communication, Measurement and Computing, Ed. J.H. Shapiro et O. Hirota*, Rinton Press, 522–527 (2002).

[47] A. Lacaita, F. Zappa, C. Cova et P. Lovati. Single-photon detection beyond 1 µm : performance of commercially available InGaAs/InP detectors, *Applied Optics* **35**, 2986–2996 (1996).

[48] U. Leonhardt. *Measuring the Quantum State of Light*, Cambridge University Press, (1993).

[49] H.-K. Lo et H.F. Chau. Unconditional security of quantum key distribution over arbitrary long distances, *Science* **283**, 2050–2056 (1999).

[50] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution, *Phys. Rev. A* **61**, 052304 (2000).

[51] N. Lütkenhaus et M. Jahma. Quantum key distribution with realistic states : photon-number statistics in the photon-number splitting attack, *New J. of Physics* **4**, 44.1–44.9 (2002).

[52] R. Maciejko. *Optoélectronique*, Presses internationales Polytechnique (2002).

[53] L. Mandel et E. Wolf. *Optical Coherence and Quantum Optics*, Cambridge University Press, (1995).

[54] U.M. Maurer. Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory* **39**, 733–742 (1993).

[55] M. Matsuoka et T. Hirano. Quantum key distribution with a single photon from a squeezed coherent state, *Phys. Rev. A* **67**, 042307 (2003).

[56] D. Mayers. Unconditional security in quantum cryptography, `http://arxiv.org/abs/quant-ph/9809039` (1998).

[57] R.J. McIntyre. Multiplication noise in uniform avalanche photodiodes, *IEEE Trans. Electron Devices* **ED-13**, 164–168 (1966).

[58] R. Merkle. Secure communications ovec insecure channels, *Comm. of the ACM* **21**, 294–299 (1978).

[59] A. Muller, H. Zbinden et N. Gisin. Quantum crptography over 23 km in installed under-lake telecom fibre, *Europhysics Letters* **33**, 335–339 (1996).

[60] A. Muller, T. Herzog, W. Tittel, H. Zbinden et N. Gisin. Plug&Play systems for quantum cryptography, *Applied Phys. Lett.* **70**, 793–795 (1997).

[61] M. Nielsen et I. Chuang. *Quantum Computation and Quantum Information*, Cambridge University Press (2000).

[62] J. Preskill. *Lecture Notes for Physics 219 : Quantum Information and Computation*, disponible à l'adresse suivante : `http://www.theory.caltech.edu/people/preskill/ph229/` (2002).

[63] G. Ribordy, J. Brendel, J.D. Gauthier, N. Gisin et H. Zbinden. Long distance entanglement based quantum key distribution, *Phys. Rev. A* **63**, 012309 (2001).

[64] R.L. Rivest, A. Shamir et L. Adleman. A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM* **21**, 120–126 (1978).

[65] B. Schumacher. Quantum coding, *Phys. Rev. A* **51**, 2738–2747, (1995).

[66] M.O. Scully et M.S. Zubairy, *Quantum Optics*, Cambridge University Press, (1997).

[67] C. E. Shannon. Communication theory of secrecy systems, *Bell System Technical Journal* **28**, 656–715, (1949).

[68] P. W. Shor. Algorithms for quantum computation : discrete logarithm and factoring, *Proceedings of the 35th Symposium on Foundations of Computer Science*, Los Alamitos (IEEE Computer Society Press), 124–134 (1994).

[69] P.W. Shor et J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol, *Phys. Rev. Lett.* **85**, 441–444 (2000).

[70] A.W. Snyder. *Optical Waveguide Theory*, Chapman & Hall, Londres (1983).

[71] D. Stinson. *Cryptography - Theory and Practice*, CRC press Inc. (2000).

[72] D. Stucki, G. Ribordy, A. Stefanov, H. Zbinden, J.G. Rarity et T. Wall. Photon counting for quantum key distribution with Peltier cooled InGaAs/InP APDs, *J. of Modern Optics* **48**, 1967–1981 (2001).

[73] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy et H. Zbinden. Quantum key distribution over 67 km with a plug&play system, *New. Jour. of Phys.* **4**, 41.1–41.8 (2002).

[74] T. A. Sudkamp. *Languages and Machines. An Introduction to the Theory of Computer Science, 2nd edition*, Addison-Wesley (1997).

[75] S.M. Sze. *Semiconductor Devices : Physics and Technology. 2nd edition*, Wiley Press, New York (2002).

[76] L. Tancevski, B. Slutsky, R. Rao et S. Fainman. Evaluation of the cost of error-correction protocol in quantum cryptographic transmission, *Proc. of SPIE* **3228**, 322–332 (1997).

[77] B. Terhal, M.M. Wolf et A.C. Doherty. Quantum entanglement : A modern perspective, *Physics Today* **56**, 46–52 (2003).

[78] P. Townsend. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using WDM, *Electronics Lett.* **33**, 188–190 (1997).

[79] P. Townsend. Quantum cryptography on multiuser optical fiber networks, *Nature* **385**, 47–49 (1997).

[80] P. Townsend. Experimental investigation of the performance limits for first telecommunications window quantum cryptography systems, *IEEE Photonics Tech. Lett.* **10**, 1048–1050 (1998).

[81] G. Vernam. Cypher printing telegraph systems for secret wire and radio telegraphic communications, *J. Am. Institute of Electrical Engineers Vol. XLV*, 109–115 (1926).

[82] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*, Princeton University Press (1955)

[83] S. Wiesner. Conjugate coding, *Sigact News* **15**, 78–88 (1983).

[84] W.K. Wootters et W.H. Zurek. A single quantum cannot be cloned, *Nature* **299**, 802–803 (1982).

[85] W.H. Zurek. Pointer-basis of quantum apparatus: Into what mixtures does the wave packet collapse?, *Phys. Rev. D* **24**, 1516–1525 (1981).

[86] W.H. Zurek. Environment-induced superselection-rules, *Phys. Rev. D* **26**, 1862–1880 (1982).

Annexe A — Description quantique de la lumière cohérente

Nous exposons ici quelques résultats issus de la procédure de quantification du champ électromagnétique. Sans dériver ces résultats, nous mentionnons d'où ils proviennent. Pour une excellente introduction, consulter l'ouvrage de L. Mandel et E. Wolf [53].

Pour quantifier le champ électromagnétique, on exprime d'abord le champ électrique dans une boîte cubique de coté L avec les conditions de frontières périodiques sur le nombre d'onde $k_\alpha = 2\pi n_\alpha L$, $n = 0, \pm 1, \pm 2, \ldots$ avec $\alpha = x, y, z$, ce qui donne

$$\mathbf{E}(\mathbf{r}, t) = \frac{1}{L^{3/2}} \sum_{\mathbf{k}} \sum_{s=1}^{2} \left(\frac{\hbar\omega}{2\varepsilon_0} \right)^{1/2} \left[i\alpha_{\mathbf{k}s}(0)\varepsilon_{\mathbf{k}s} \mathrm{e}^{i(\mathbf{k}\cdot\mathbf{r}-\omega t)} + \text{c.c.} \right] \tag{A.1}$$

où s est l'état de polarisation, $\varepsilon_{\mathbf{k}s}$ le vecteur unitaire de polarisation du mode, $\alpha_{\mathbf{k}s}$ l'amplitude complexe du mode à $t = 0$ et c.c. est le complexe conjugué. Cette expansion nous permet d'écrire l'énergie totale du champ électromagnétique comme suit

$$H = \sum_{\mathbf{k}} \sum_{s=1}^{2} \hbar\omega \left[\alpha^\dagger_{\mathbf{k}s}(t)\alpha_{\mathbf{k}s}(t) + \frac{1}{2} \right]. \tag{A.2}$$

avec $\alpha_{\mathbf{k}s}(t) = \alpha_{\mathbf{k}s}(0)\mathrm{e}^{-i\omega t}$. On reconnaît l'expression de l'énergie d'un ensemble d'oscillateurs harmoniques, ce qui nous permet de procéder directement à la quantification dans la représentation de Heisenberg par analogie en faisant $\alpha_{\mathbf{k}s}(t) \longrightarrow \hat{a}_{\mathbf{k}s}(t)$ et en posant les commutateurs suivants :

$$\left[\hat{a}_{\mathbf{k}s}(t), \hat{a}^\dagger_{\mathbf{k}'s'}(t) \right] = \delta^3_{\mathbf{k}\mathbf{k}'}\delta_{ss'} \tag{A.3}$$

$$\left[\hat{a}_{\mathbf{k}s}(t), \hat{a}_{\mathbf{k}'s'}(t) \right] = 0 \tag{A.4}$$

$$\left[\hat{a}^\dagger_{\mathbf{k}s}(t), \hat{a}^\dagger_{\mathbf{k}'s'}(t) \right] = 0. \tag{A.5}$$

L'énergie totale correspond alors à l'hamiltonien du système

$$\hat{H} = \sum_{\mathbf{k}} \sum_{s} \hbar\omega \left[\hat{n}_{\mathbf{k}s} + 1/2\right], \tag{A.6}$$

où $\hat{n}_{\mathbf{k}s}$ est l'opérateur nombre de photons dans le mode $\mathbf{k}$ de polarisation s. Les états propres de $\hat{n}_{\mathbf{k}s}$ sont les états de Fock et on montre facilement que ses valeurs propres sont entières positives :

$$\hat{n}_{\mathbf{k}s}|n_{\mathbf{k}s}\rangle = n_{\mathbf{k}s}|n_{\mathbf{k}s}\rangle \tag{A.7}$$

avec $n_{\mathbf{k}s} = 0, 1, 2, \ldots$ Les états de Fock forment une base orthonormée sur laquelle on peut exprimer l'état quantique du champ électromagnétique.

Considérons maintenant un seul mode $\mathbf{k}$ de polarisation fixée et cherchons l'état propre de l'opérateur $\hat{a}$. Comme $\hat{a}$ n'est pas hermitique, la valeur propre correspondant au vecteur propre $|\alpha\rangle$, que nous noterons α, est un nombre complexe. En développant $|\alpha\rangle$ sur la base de Fock, on montre que

$$|\alpha\rangle = \mathrm{e}^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{A.8}$$

Cet état correspond à celui de la lumière parfaitement cohérente et monochromatique. À l'aide de la définition de $\hat{n}$ on montre facilement que le paramètre $|\alpha|^2/2$ est égal au nombre moyen μ de photons par intervalle de temps Δt du faisceau. Sa puissance P s'exprime en fonction de μ selon

$$P = \frac{\mu\hbar\omega}{\Delta t}. \tag{A.9}$$

La phase absolue du faisceau, θ, est donnée par l'argument de $\alpha = |\alpha|\mathrm{e}^{i\theta}$. En cryptographie quantique, la phase des impulsions envoyées par Alice est inconnue d'Ève et de Bob. L'état du faisceau correspond alors à un mélange statistique des états de Fock dont la matrice densité s'écrit comme

$$|\alpha\rangle \to \rho = \int_0^{2\pi} \frac{\mathrm{d}\theta}{2\pi} |\alpha\rangle\langle\alpha| \tag{A.10}$$

$$= \mathrm{e}^{-\mu} \sum_{m,n=0}^{\infty} \frac{|\alpha|^{m+n}}{\sqrt{m!n!}} \int_0^{2\pi} \frac{\mathrm{d}\theta}{2\pi} \mathrm{e}^{i\theta(m-n)} |m\rangle\langle n| \tag{A.11}$$

$$= \sum_{n=0}^{\infty} \frac{\mu^n \mathrm{e}^{-\mu}}{n!} |n\rangle\langle n|. \tag{A.12}$$

Chaque impulsion contient alors un nombre défini (mais *a priori* inconnu de Ève) de photons. La probabilité d'en observer n pour une durée d'impulsion Δt, $\mathcal{P}_\mu(n)$, est donc

$$\mathcal{P}_\mu(n) = \frac{\mu^n \mathrm{e}^{-\mu}}{n!}. \tag{A.13}$$

La probabilité que l'impulsion contienne plus de un photon est donnée par

$$\begin{aligned} \mathcal{P}_\mu(n>1) &= 1 - \mathcal{P}_\mu(0) - \mathcal{P}_\mu(1) && \text{(A.14)} \\ &= 1 - \mathrm{e}^{-\mu} - \mu \mathrm{e}^{-\mu} && \text{(A.15)} \\ &\approx \frac{\mu^2}{2}, && \text{(A.16)} \end{aligned}$$

où l'approximation est valide pour $\mu \ll 1$.

Pour réaliser BB84, on choisit $\mu \ll 1$, de façon à minimiser la probabilité que l'impulsion contienne plus d'un photon. Cependant, cela augmente également la probabilité que l'impulsion soit vide ce qui diminue le taux de génération de clé. Typiquement, les expériences sont faites avec $\mu = 0{,}1$ ce qui est un bon compromis compte tenu du bruit des détecteurs de photons disponibles. Avec un tel μ, 90,4% des impulsions sont vides, 9,04% contiennent 1 photon, 0,45% contiennent deux photons et 0,015% contiennent trois photons ou plus.

Annexe B — Miroir de Faraday

Nous expliquons ici en détail le fonctionnement du miroir de Faraday. Pour ce faire, on utilise la sphère de Poincaré pour décrire l'état de polarisation [23]. Cette dernière est équivalente à la sphère de Bloch (section 1.2.1) en posant $|0\rangle = |\circlearrowright\rangle$ (polarisation circulaire droite) et $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |\updownarrow\rangle$ (polarisation verticale). L'état de polarisation $|\psi\rangle$ s'écrit comme

$$|\psi\rangle \equiv |\psi(\theta,\varphi)\rangle = \mathrm{e}^{-i\varphi/2}\cos\frac{\theta}{2}|\circlearrowright\rangle + \mathrm{e}^{i\varphi/2}\sin\frac{\theta}{2}|\circlearrowleft\rangle. \tag{B.1}$$

Les états correspondant aux axes x, y et z sont montrés à la figure B.1.

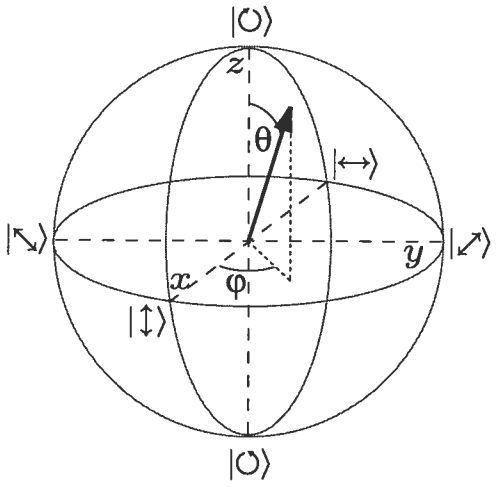

FIG. B.1 – Sphère de Poincaré : $|\leftrightarrow\rangle$ = pol. horizontale, $|\updownarrow\rangle$ = pol. verticale, $|\nearrow\swarrow\rangle$ = pol. +45°, $|\nwarrow\searrow\rangle$ = pol. −45°, $|\circlearrowright\rangle$ = pol. circ. droite, $|\circlearrowleft\rangle$ = pol. circ. gauche.

Un miroir de Faraday est composé d'un rotateur de Faraday suivi d'un miroir normal, comme illustré à la figure B.2. Sur la figure nous avons défini les

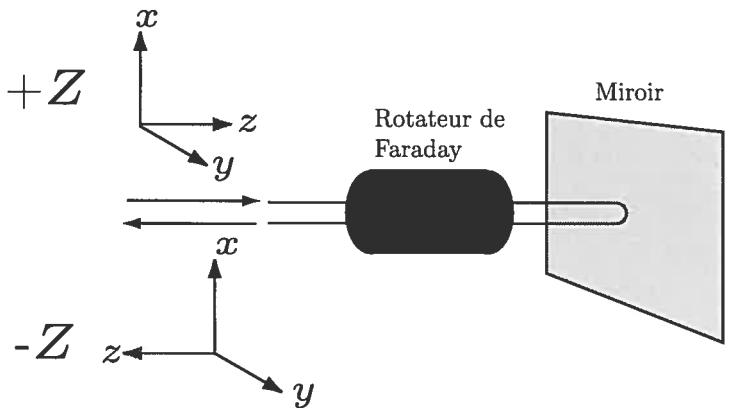

FIG. B.2 – Miroir de Faraday. Les référentiels $+Z$ et $-Z$ servent à décrire la polarisation avant et après la réflexion sur le miroir.

référentiels $+Z$ et $-Z$ permettant de décrire la polarisation de la lumière avant et après la réflexion. On remarque que $-Z$ est un référentiel gauche.

Décrivons tout d'abord l'effet du miroir seul, que nous notons $\hat{M}$. Il est clair que le miroir laisse inchangés tous les états de polarisation linéaire. Cependant, après la réflexion, les polarisations circulaires droite et gauche sont échangées entres elles car la direction d'observation de la polarisation, obtenue par définition en observant la polarisation dans la direction opposée à sa propagation, passe de $+z$ à $-z$. Par conséquent, l'effet du miroir sur la sphère de Poincaré correspond à une réflexion par rapport au plan x-y. Remarquons que cette opération n'est pas unitaire, mais la mécanique quantique n'est pas violée pour autant. Cela est une conséquence du fait que notre description de la polarisation avant et après passe d'un référentiel droit à un référentiel gauche. Si nous avions utilisé un référentiel droit pour décrire la polarisation au retour, la transformation du miroir serait unitaire.

Le rotateur de Faraday utilise l'effet Faraday[1] pour effectuer une rotation des polarisations linéaires d'un angle de $\pi/4$ autour de l'axe de propagation, mais

[1]L'effet Faraday correspond à l'apparition d'une biréfringence dans un matériau en présence d'un champ magnétique.

laissant les polarisations circulaires inchangées. Par conséquent, sur la sphère de Poincaré, la transformation associée au rotateur, que l'on note $\hat{R}_F$, correspond à une rotation de $\pi/2$ autour du vecteur unitaire $\mathbf{z}$:

$$\hat{R}_F = \mathcal{R}(\pi/2, \mathbf{z}), \tag{B.2}$$

où nous avons utilisé la notation définie à la section 1.2.1. Une particularité de l'effet Faraday est qu'il est non-réciproque, signifiant que la direction de rotation de la polarisation est indépendante de la direction de propagation. Autrement dit, $\hat{R}_F$ est identique dans les deux référentiels, ce qui n'est pas le cas notamment de la biréfringence induite par des contraintes dans la fibre.

L'effet global du miroir de Faraday, $\hat{M}_F$, est donné par

$$\hat{M}_F = \hat{R}_F \hat{M} \hat{R}_F \tag{B.3}$$

et une représentation visuelle de cet effet est donnée à la figure B.3. On voit

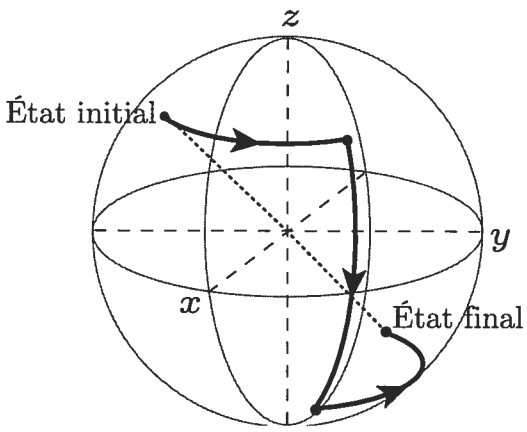

FIG. B.3 – Effet du miroir de Faraday sur la sphère de Poincaré pour un état arbitraire.

alors qu'en utilisant les référentiels $+Z$ et $-Z$ pour décrire la transformation, la polarisation sortante est diamétralement opposée à la polarisation entrante.

Maintenant, si on tient compte de la biréfringence de la fibre $\hat{U}_B$ juste avant la réflexion sur le miroir de Faraday, alors la transformation de l'état de polarisation

est donnée par

$$\hat{U}_B^{-1}\hat{M}_F\hat{U}_B. \tag{B.4}$$

Il est facile de voir que $\hat{U}_B$ commute avec $\hat{M}_F$. En effet, $\hat{M}_F$ correspond à une rotation sur la sphère de Poincaré dans le même plan que celle associée à $\hat{U}_B$, ce qui assure leur commutation. Par conséquent :

$$\hat{U}_B^{-1}\hat{M}_F\hat{U}_B = \hat{M}_F. \tag{B.5}$$

Annexe C — Notions de théorie de l'information

L'ouvrage de T. Cover et J. Thomas est une excellente référence sur la théorie de l'information [28].

Commençons par rappeler quelques éléments de la théorie des probabilités. Soit X une variable aléatoire prenant ses valeurs dans un ensemble $\mathcal{X}$ que l'on nomme le domaine de X, et soit $P_X(x)$, la distribution de probabilité de X associant à une valeur $x \in \mathcal{X}$ un nombre réel compris entre 0 et 1. On a alors

$$\sum_{x \in \mathcal{X}} P_X(x) = 1, \tag{C.1}$$

signifiant que la probabilité totale est égale à 1. On peut généraliser la définition de distribution de probabilité à plusieurs variables aléatoires $X_1, X_2, \ldots, X_N$, ce qui nous donne une distribution de *probabilité conjointe* :

$$P_{X_1,X_2,\ldots,X_N}(x_1, x_2, \ldots, x_N) \tag{C.2}$$

Si les variables sont statistiquement indépendantes, alors on peut écrire

$$P_{X_1,X_2,\ldots,X_N}(x_1, x_2, \ldots, x_N) = P_{X_1}(x_1)P_{X_2}(x_2)\ldots P_{X_N}(x_N). \tag{C.3}$$

On peut également définir la *probabilité conditionnelle* d'une variable X sur le résultat d'une autre Y. Cette distribution correspond à la probabilité que $X = x$ survienne sachant que le résultat de la mesure de Y ait donné la valeur y. On note cette probabilité comme

$$P[X = x|Y = y] = P_{X|Y=y}(x) \tag{C.4}$$

Maintenant, pour une variable aléatoire donnée X, on aimerait quantifier l'incertitude sur le résultat de la mesure de X en fonction de sa distribution de

probabilité P_X. Nous nommons cette mesure l'entropie de Shannon sur X, que nous notons $H(X)$. Essayons de donner une interprétation intuitive de l'entropie. Soit $\mathcal{X} = \{x_0, x_1, \ldots, x_N\}$, le domaine de X. Si on a $P_X(x_0) = 1$, alors chaque mesure de X donnera x_0, et on peut prédire le résultat de la mesure avant même de l'avoir faite. On aimerait alors que $H(X) = 0$, signifiant que l'incertitude sur X est nulle. Au contraire, si on a $P_X(x_i) = 1/N$, alors chaque résultat de la mesure est équiprobable, et on aimerait alors que $H(X)$ soit maximisée pour cette distribution uniquement. On peut montrer que la fonction suivante remplit ces conditions :

$$H(X) = -\sum_{x \in \mathcal{X}} P_X(x) \log_2 P_X(x) \tag{C.5}$$

Dans le cas où $\mathcal{X} = \{0, 1\}$ (X est une variable binaire) avec $P_X(0) = p$ et $P_X(1) = 1 - p$, alors on peut écrire

$$H(X) = -p \log_2 p - (1 - p) \log_2 (1 - p) \tag{C.6}$$

et on montre facilement que $H(X) \to 0$ pour $p \to 0$ et 1 et que $H(X) = 1$ pour $p = 1/2$.

On peut également définir l'entropie conjointe de X et Y comme

$$H(XY) = \sum_{(x,y) \in (\mathcal{X} \times \mathcal{Y})} -P_{XY}(x, y) \log_2 P_{XY}(x, y), \tag{C.7}$$

qui satisfait l'inégalité suivante :

$$H(XY) \leqslant H(X) + H(Y), \tag{C.8}$$

où l'égalité est obtenue lorsque X et Y sont statistiquement indépendantes.

Toujours en utilisant la définition de l'entropie, nous pouvons définir l'entropie conditionnelle sur X étant donné la valeur y pour Y. Cette entropie est donnée par

$$H(X|Y = y) = -\sum_{x \in \mathcal{X}} P_{X|Y=y}(x) \log_2 P_{X|Y=y}(x). \tag{C.9}$$

Si la valeur de Y n'est pas spécifiée, on peut tout de même définir l'entropie

conditionnelle sur X en fonction de Y

$$H(X|Y) = H(XY) - H(Y) \tag{C.10}$$
$$= \sum_{y \in \mathcal{Y}} P_Y(y) H(X|Y = y) \tag{C.11}$$

qui correspond à l'incertitude moyenne sur X par rapport à Y. À l'aide de ces définitions, nous pouvons maintenant définir l'information mutuelle entre X et Y

$$I(X;Y) = H(X) + H(Y) - H(XY) \geq 0. \tag{C.12}$$

Intuitivement, $I(X;Y)$ correspond au gain moyen d'information sur X lorsqu'on nous donne la valeur de Y uniquement. L'inverse est également vrai car $I(X;Y) = I(Y;X)$. D'après l'équation C.8, il est clair que $I(X;Y) = 0$ lorsque X et Y sont indépendantes. Au contraire, si la valeur de $I(X;Y)$ est maximale (cette valeur dépend de la taille des domaines de X et Y), alors la connaissance de la valeur de X nous donne toute l'information sur Y avec certitude.