Titre: Title:	Interféromètre tout-fibre stabilisé pour encodage en phase d'information quantique
Auteur: Author:	Daniel Summers-Lépine
Date:	2007
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Summers-Lépine, D. (2007). Interféromètre tout-fibre stabilisé pour encodage en phase d'information quantique [Mémoire de maîtrise, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/8112/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/8112/
Directeurs de recherche: Advisors:	Nicolas Godbout
Programme: Program:	Non spécifié

UNIVERSITÉ DE MONTRÉAL

Interféromètre tout-fibre stabilisé pour encodage en phase d'information quantique

DANIEL SUMMERS-LÉPINE
DÉPARTEMENT DE GÉNIE PHYSIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE PHYSIQUE)
DÉCEMBRE 2007

Your file Votre référence
ISBN: 978-0-494-36943-2
Our file Notre référence
ISBN: 978-0-494-36943-2

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé:

Interféromètre tout-fibre stabilisé pour encodage en phase d'information quantique

présenté par: SUMMERS-LÉPINE Daniel,

en vue de l'obtention du diplôme de: Maîtrise ès sciences appliquées

a été dûment accepté par le jury d'examen constitué de:

Mme LACROIX Suzanne, D.Sc., présidente

M. GODBOUT Nicolas, Ph.D., directeur de recherche

M. AZANA, Jose, Ph.D., membre

Résumé

Dans ce mémoire, on présente un interféromètre à très long délai conçu et fabriqué pour application en cryptographie quantique par DPSK à 100 Mbit/sec. Il est également conçu pour une stabilité thermique sur la plage de 22,5°C à 23,5°C et une insensibilité totale à la polarisation. La stabilité thermique est fondée sur l'utilisation d'une fibre dopée au phosphore dans l'une des branches de l'interféromètre afin de compenser l'effet thermo-optique de l'autre branche, fabriquée de fibre SMF-28. On montre que pour un interféromètre de 100 Mbit/sec ($\Delta L = 2{,}042$ m), on doit utiliser 20,419 m de fibre dopée au phosphore pour compenser 18,377 m de fibre SMF-28. Ceci mène à l'enroulement des branches et donc à une sensibilité à la polarisation. Afin d'éliminer cette dépendance, on propose une géométrie d'enroulement telle que la différence de longueur des branches corresponde à un multiple entier de la longueur de battement de polarisation.

À cause de la très longue différence de marche de l'interféromètre, sa caractérisation a nécessité l'élaboration d'une technique fondée sur une petite modulation de phase pour explorer la pente locale de la réponse de l'interféromètre. En appliquant cette technique, on a obtenu un interféromètre *temporairement stable* autour de 22,6°C. L'hypothèse est que l'aspect temporaire de cette stabilité soit relié à l'absorption d'humidité par la gaine polymérique des fibres. De plus, les résultats obtenus montrent une insensibilité en polarisation, mais montrent également que le modèle utilisé pour la détermination de la forme de l'enroulement n'est que qualitativement précis et doit donc être étalonné.

Abstract

In this Masters thesis, we present an all-fibre interferometer designed and built for use in DPSK based quantum key distribution at a rate of 100 Mbit/sec. As well, the interferometer is designed for thermal stability over the range of 22.5°C to 23.5°C and for polarisation insensitive visibility. Thermal stability is based on the use of a phosphorus doped fibre in one branch of the device in order to compensate the thermo-optic effect of the other branch, made of SMF-28. We show that for a 100 Mbit/sec interferometer ($\Delta L = 2.042$ m), this requires 20.419 m of phosphor doped fibre to compensate for 18.377 m of SMF-28 fibre. This leads to the winding of the branches, and thus to a polarisation dependence. To eliminate this dependence, a winding geometry is proposed such that the branch length difference is a multiple of the polarisation beat length.

Conventionnal characterisation methods cannot be used to test an interferometer of such long delay. Thus, a method based on the use of a small phase modulation was elaborated to locally measure the slope of the interferometer response function. Using this technique, we obtained an interferometer *temporarily stable* near 22.6°C. We hypothesize that the loss of stability is related to the absobtion of humidity in the fibre protective polymer coating. As well, results obtained show that polarisation insensitivity is acheived, but also that the model used to determine the winding geometry is merely qualitatively accurate and must be calibrated.

Table des matières

Liste des figures

Liste des tableaux

Liste des annexes

Liste des sigles et abréviations

a = coefficient équivalent de transmission [n/a]

$B_{+,\times} = \{|0_{+,\times}\rangle, |1_{+,\times}\rangle\}$ = bases d'états quantiques maximalement conjugés [n/a]

c = 299 792 458 [m/s], vitesse de la lumière dans le vide

C = matrice de transfert d'un coupleur [n/a]

c, c' = coefficients de couplage en amplitude des coupleurs [n/a]

C_s = coefficient élasto-optique [n/a]

d_B = taux de production de comptes au détecteur en absence de signal [n/a]

dL = segment de fibre [m]

D_{eq} = diamètre équivalent de l'enroulement [m]

E = champ électrique [V/m]

E = module d'Young [Pa]

E_x = projection du champ électrique selon l'axe de polarisation x [V/m]

E_y = projection du champ électrique selon l'axe de polarisation y [V/m]

f_r = taux de répétition [bit/s]

h = paramètre caractérisant la forme de l'enroulement [m]

I_{max} = intensité correspondant au maximum de transmission de l'interféromètre [cd]

I_{min} = intensité correspondant au minimum de transmission de l'interféromètre [cd]

I = moment d'inertie [kg/m^2]

$j = \sqrt{-1}$, nombre imaginaire

k_0 = vecteur d'onde dans le vide [rad/m]

L = longueur de branche [m]

L_{tol} = tolérance sur la longueur des branches de l'interféromètre [m]

L_e = longueur enroulée [m]

L_{ne} = longueur non enroulée [m]

$L_{ne,E}$ Longueur non enroulée à l'entrée [m]

$L_{ne,S}$ Longueur non enroulée à la sortie [m]

$L_{c,E}$ = Longueur des branches du coupleur d'entrée [m]

$L_{c,S}$ = Longueur des branches du coupleur de sortie [m]

ℓ = distance de transmission [km]

m = entier constant [n/a]

M = moment de force [N.m]

n = indice de réfraction (matériel) de la fibre [n/a]

n_g = indice de groupe du monde fondamental [n/a]

N = nombre de tours d'enroulement [n/a]

N = force normale [N]

$\bar{n}$ = nombre moyen de photons par impulsion [n/a]

p_{11}, p_{12} = éléments de matrice élasto-optique [n/a]

r = rayon de la section transversale de la fibre [μm]

R = taux de génération de clef sécurisée [bit/s]

s_T = sensibilité en température de l'interféromètre [m/K]

T = température [K]

T_0 = température de référence [K]

T = tension [N]

t', t'' = coefficients de transmission des épissures [n/a]

t = coefficient de transmission combiné [n/a]

V = visibilité de l'interféromètre [n/a]

x_r = distance entre les poteaux d'enroulement [m]

X, Y = signaux de quadrature [V]

Symboles grecs

$\alpha_n = \frac{dn}{dT}$ = coefficients thermo-optique [K^{-1}]

α_L = coefficient de dilatation thermique [n/a]

β_b = biréfringence de courbure [m^{-1}]

β_τ = biréfringence de torsion [m^{-1}]

Δt_{imp} = délai entre impulsions [s]

ΔL = différence de marche de l'interféromètre [m]

$\Delta\phi = \phi_1 - \phi_2$ = différence de phase de l'interféromètre [rad]

$\Delta\phi_{tol}$ = tolérance sur la différence de phase de l'interféromètre [rad]

ΔT_{tol} = tolérance sur la stabilité de la température [K]

ΔN = différence de nombre de tours d'enroulement [n/a]

$\Delta\lambda_{laser}$ = largeur spectrale du laser [m]

$\Delta\lambda_0$ = stabilité en longueur d'onde du laser [m]

η_T = efficacité de transmission du canal quantique [n/a]

η_B = efficacité quantique du détecteur [n/a]

Γ_ℓ = pertes de la fibre [dB]

Γ_c = pertes de transmission constantes [dB]

λ = longueur d'onde [m]

ν = fréquence optique [Hz]

ω_0 = pulsation (dans le vide) [rad/s]

ω_m = pulsation de modulation [rad/s]

$\phi_{1,2}$ = phase accumulée dans les branches (1 et 2) de l'interféromètre [rad]

ϕ_{tr}^x = phase accumulée en un tour pour la polarisation x [rad]

ϕ_{tr}^y = phase accumulée en un tour pour la polarisation y [rad]

$\phi_{tr}^{xy} = \phi_{tr}^y - \phi_{tr}^x$ = phase relative entre les états de polarisation x et y [rad]

ϕ_0 = phase initiale [rad]

ϕ_m = phase initiale de modulation [rad]

ρ = rayon de courbure de la fibre [m]

τ = délai de l'interféromètre [s]

ξ = position du segment dL dans l'enroulement [m]

Indices

indice 1 = relatif à la branche 1 de l'interféromètre

indice 2 = relatif à la branche 2 de l'interféromètre

Fonctions

$f(t)$ = fonction de modulation

$J_n(z)$ = fonction de Bessel de première espèce, d'ordre n

Acronymes

DPSK = Differential Phase Shift Keying

QKD = Quantum Key Distribution

QBER = Quantum Bit Error Rate

PNS = Photon number splitting

IEEE = Institute of Electric and Electronic Engineers

RTD = Resistance Temperature Detector

PLL = Phase Lock Loop

GPIB = General Purpose Interface Bus

Introduction

La cryptographie quantique est une technique de protection du secret dans les télécommunications. Elle porte le nom *quantique* au fait que ce type de cryptographie est basé sur les lois de la mécanique quantique. Il s'agit donc d'une technique unique en cryptographie car elle est fondée sur les lois fondamentales de la physique.

Depuis ses débuts, l'étude de la cryptographie quantique se trouve à la croisée de la science informatique et de la physique. Or, son utilisation plus répandue dans le télécommunications requiert le développement de technologies spécifiquement créées pour la réalisation des ces protocoles.

Comme nous le verrons, presque tout les protocoles font appel à une opération d'interférométrie afin d'extraire l'information que peut porter la phase d'un photon. Malheureusement, les interféromètres tout-fibre souffrent normalement de deux problèmes d'instabilité qui les rendent souvent inopérants : ils sont très sensibles à la température et à la polarisation. Pour contourner le problème de la polarisation, des chercheurs ont élaboré des schémas de cryptographie basés sur des miroirs de Faraday [1]. De plus, pour éviter le problème d'instabilité en température, plusieurs chercheurs ont utilisé des interféromètres issus de la microfabrication. Malheureusement, ceci apporte un nouveau problème, celui des pertes d'insertion très élevées ce qui équivaut, en cryptographie quantique, à une diminution de la distance de transmission sécuritaire.

Dans ce mémoire, on présente un interféromètre tout-fibre à très long délai adapté pour l'utilisation dans un protocole de cryptographie quantique par encodage de phase. En plus d'offrir des pertes d'insertion presque négligeables, celui-ci vise à être

insensible à la fois polarisation et à la température.

Afin de justifier les spécifications pour l'interféromètre, le premier chapitre décrit les rudiments de la cryptographie quantique et en particulier la cryptographie quantique par encodage de phase. Le second chapitre présente les méthodes à la base du design et de la fabrication de l'interféromètre. Le troisième chapitre illustre la technique utilisée pour caractériser l'interféromètre. Finalement, on présente au chapitre 4 les résultats de sensibilité en température et en polarisation obtenus pour deux interféromètres.

Chapitre 1

La cryptographie quantique

Ce chapitre décrit quelques notions théoriques à la base de la cryptographie quantique. Il y est également exposé la manière dont ces notions s'expriment sous forme de protocoles, et comment ceux-ci ont été réalisés expérimentalement. Finalement, le protocole de cryptographie quantique par DPSK (*differential phase shift keying*) sera traité plus en détail afin d'élaborer sur les enjeux liés à la technologie interférométrique qui est le sujet de ce mémoire.

1.1 Les limitations de la cryptographie classique

La cryptographie classique est très répandue dans les télécommunications modernes. Ainsi, l'internaute use de cryptographie lorsqu'il transige avec la banque, lorsqu'il transmet un numéro de carte de crédit, par exemple. La cryptographie protège l'usager contre l'interception indésirable de cette information.

Sur internet, le protocole de sécurité généralement utilisé est le protocole RSA[1]. Sa popularité est reliée au fait qu'il se réalise très facilement en pratique : les clefs de déchiffrement (information permettant d'obtenir le message à partir du cryptogramme) peuvent être échangées à distance, sans compromettre la sécurité.

[1]Ce protocole est décrit en détail à l'annexe C.

La sécurité de ce protocole est basée sur la difficulté du problème qu'aurait à résoudre un espion afin de déchiffrer un cryptogramme. En effet, celui-ci doit factoriser un très grand nombre en deux facteurs *premiers*, eux mêmes très grands. Or, il n'existe aucune méthode, soit numérique, soit analytique pour résoudre ce problème efficacement. De manière générale, la solution à ce problème est l'affaire de plusieurs années de calcul sur un ordinateur moderne. Donc, ce protocole garantit une sécurité acceptable pour de nombreuses applications.

Cependant, la recherche continue pour trouver des algorithmes de factorisation de plus en plus efficaces. Qui plus est, une découverte en mathématique analytique pourrait du jour au lendemain rendre ce protocole inutilisable.

Or, depuis 1932, il existe un protocole offrant une *sécurité parfaite* au sens de la théorie de l'information[2]. En effet, Shannon [2] a proposé un protocole nommé *masque jetable* accompagné d'un formalisme par lequel il a démontré que ce protocole est d'une sécurité absolue[3].

Malheureusement, ce protocole est relativement peu utilisé. Sa faiblesse tient au fait que chaque clef ne peut être utilisée plus d'une fois (d'où le nom *masque jetable*), et qu'il n'existe aucun moyen *classique* permettant d'échanger des clefs à distance (sauf en faisant appel à un tiers fiable). Inversement, s'il était possible d'échanger des clefs à distance, les participants à la communication[4] pourraient échanger leur message dans un secret absolu.

Or, la *cryptographie quantique* est justement un protocole permettant l'échange de clefs cryptographiques à distance, en utilisant les lois de la physique quantique.

Il est utile à ce stade-ci de remarquer que l'expression *cryptographie quantique* est quelque peut trompeuse puisque cette technique s'insère dans un protocole de cryptographie entièrement classique (le *masque jetable*). La partie proprement *quan-*

---

[2]Voir l'annexe A pour une description détaillée sur l'application de la théorie de l'information à la science cryptographique.

[3]Voir l'annexe B pour une description détaillée du protocole du masque jetable.

[4]Les participants à une communication encryptée sont communément appelés Alice et Bob. Il existe également le personnage de l'espion, nommée Ève.

tique dans la cryptographie quantique est le protocole de distribution de la clé cryptographique entre les participants légitimes à la communication. Pour cette raison, il existe une expression anglaise alternative pour décrire la cryptographie quantique : *Quantum Key Distribution* ou QKD. Dans ce texte, on utilisera l'acronyme QKD pour faire référence au sens implicite du terme *cryptographie quantique.*

1.2 La distribution quantique de clefs

Cette section décrit comment sont utilisées les lois de la mécanique quantique dans la construction des algorithmes de distribution quantique de clefs. Plus particulièrement, on y présente l'algorithme BB84 et l'algorithme de QKD par DPSK. On y démontre notamment la manière dont on peut utiliser les lois de l'optique quantique pour réaliser concrètement ces protocoles.

1.2.1 Algorithme BB84

Le protocole BB84 fut publié en 1984 par Gilles Brassard et Charles H. Bennett[3]. Il s'agit de l'article fondateur du domaine de recherche qu'est la cryptographie quantique.

Soient deux ensembles d'états quantiques[5], $B_+ = \{|0_+\rangle, |1_+\rangle\}$ et $B_\times = \{|0_\times\rangle, |1_\times\rangle\}$. Les états $|0_+\rangle$ et $|1_+\rangle$ sont orthonormés, tout comme $|0_\times\rangle$ et $|1_\times\rangle$ de telle sorte que les ensembles B_+ et $B_\times$ forment chacun une base. De plus, les bases $B_\times$ et B_+ sont dites *maximalement conjuguées* de sorte que l'application d'un opérateur de mesure de l'une des bases sur un état dans l'autre base produit un résultat totalement aléatoire.

[5]Il n'est pas nécessaire de spécifier ce que représente physiquement ces états quantiques, le protocole est général et n'en dépend pas.

Autrement dit,

$$|\langle 0_+|0_\times\rangle|^2 = \frac{1}{2}$$
$$|\langle 0_+|1_\times\rangle|^2 = \frac{1}{2}$$
$$|\langle 1_+|0_\times\rangle|^2 = \frac{1}{2}$$
$$|\langle 1_+|1_\times\rangle|^2 = \frac{1}{2}$$

Le protocole procède donc comme suit.

1. Alice prépare un état 0 ou 1 codé dans l'une des deux bases choisie aléatoirement (par exemple, elle choisit aléatoirement entre $|0_+\rangle$ et $|0_\times\rangle$) et transmet le qubit produit à Bob via un canal public.
2. Bob mesure le qubit reçu dans l'une des deux bases, également choisie aléatoirement. S'il a choisi la même base qu'Alice, alors la mesure qu'il effectue devrait certainement être l'état (0 ou 1) qu'a transmis Alice. S'il n'a pas choisi la même base, alors il mesure soit un 0 soit un 1 avec une probabilité égale.
3. Bob indique à Alice, par une transmission classique et par voie publique, la base dans laquelle il a fait sa mesure, sans divulguer le résultat de cette mesure. Alice répond publiquement à Bob si oui ou non elle a codé son état dans la même base que Bob a utilisée pour sa mesure. Si oui, Bob conserve le bit mesuré, et Alice fait de même. Sinon, le bit n'a absolument aucune valeur informationnelle et n'est pas conservé par les participants.
4. Les étapes 1 à 3 sont répétés jusqu'à l'obtention d'une séquence de bits $\mathcal{K}$ conservées *plus longue* que le texte clair $P \in \mathcal{P}$ qu'Alice veut transmettre à Bob[6].

[6]Ceci est pour permettre l'implémentation des algorithmes de correction d'erreur et d'amplification du secret qui réduisent considérablement la longueur de la séquence de bits que possèdent Alice et Bob.

5. Alice et Bob dévoilent publiquement une fraction de leur séquence de bits afin d'en calculer le *taux d'erreur quantique* (QBER[7]).
6. Alice et Bob appliquent un *algorithme de correction d'erreurs* afin de compenser pour toute erreur de transmission sur le canal quantique.
7. Alice et Bob appliquent un *algorithme d'amplification du secret*[4] afin de réduire l'information que pourrait posséder Eve à zéro.

Par la suite, Alice utilise la séquence de bits que se partagent désormais Alice et Bob comme clef K dans un l'algorithme du *masque jetable* pour transmettre à Bob son message P.

Si Ève ne possède aucune information sur K, alors le système cryptographique est d'une sécurité parfaite au sens de la théorie de l'information. Inversement, si Ève possède une information, même partielle, sur K, la sécurité du protocole est fortement affaiblie. Ainsi, la sécurité et l'utilité du protocole BB84 dépend de sa capacité à ne laisser fuir aucune information sur K à Ève.

Ève, bien sûr, tente par tous les moyens de découvrir quoi que ce soit sur les *qubits*[8] que s'échangent Alice et Bob. La sécurité dans le protocole BB84 réside dans le fait qu'un espion ne peut manipuler des états quantiques sans les perturber. Ainsi, de façon générale, tout effort par Ève pour intercepter les qubit qu'envoi Alice sera apparent dans le taux d'erreur quantique (le QBER). Avec cette information, Alice et Bob peuvent détecter la présence d'Ève. En pratique, Alice et Bob se donneront un seuil, le QBER_{max}, au dela duquel le QBER est tel qu'il est possible qu'Ève ait espionné le canal quantique. Dans ce cas, Alice et Bob jugeront que leur canal quantique n'est pas sûr et par conséquent que la clef échangée ne l'est pas non plus. Il ne s'en serviront donc pas pour encoder le texte clair.

[7]De l'anglais *quantum bit error rate.*
[8]On nomme *qubit* tout objet dont l'état quantique est représentatif d'une information.

1.2.2 Taux de génération de clef sécurisée

Le taux de génération de clef sécurisée, R, est défini comme étant le taux avec lequel on peut obtenir des bits de clef sécurisés. Il est variable en fonction du protocole de QKD, de correction d'erreurs et d'amplification du secret, ainsi que des caractéristiques physiques du système. C'est également le moyen par lequel on peut étudier et comparer les protocoles et les systèmes. Il est bien sûr préférable d'obtenir le taux R le plus élevé possible.

Pour le protocole BB84, lorsqu'on utilise des "impulsions faible" (voir la section 1.3.2), l'existence de l'attaque nommée *photon number splitting attack*(PNS) fait en sorte que l'efficacité de transmission η_T se doit d'être telle que [5]

$$\eta_T > 2\sqrt{d_B}/\eta_B \tag{1.1}$$

où d_B est le taux de production de comptes au détecteur en absence de signal (en anglais : *dark count rate*) et η_B est l'efficacité quantique du détecteur. De plus, cette équation suppose que l'on a optimalement choisi $\bar{n} = 2\sqrt{d_B}$. On montre [6] que cela est équivalent à un taux de génération de clef sécurisée R donnée par

$$R_{\text{BB84}} = f_r \frac{1}{4} \eta_B^2 \eta_T^2 \tag{1.2}$$

Ainsi, le taux de génération sécuritaire de la clef chute avec les pertes du canal au carré, donc avec la distance au carré. Éventuellement, ce taux s'approchera de zéro asymptotiquement en fonction de la distance ℓ. En effet, en fonction des pertes de la fibre Γ_ℓ (en dB/km) et de d'autres pertes constantes Γ_c (en dB), le taux d'efficacité de transmission est de

$$\eta_T = 10^{-(\Gamma_\ell \ell + \Gamma_c)/10} \tag{1.3}$$

ce qui montre que la distance de transmission ℓ est très rapidement réduite par les pertes de la fibre et les autres pertes constantes de montage.

1.3 La QKD par DPSK

Cette section présente une méthode de QKD techniquement plus simple à réaliser que le BB84, sans compromettre la sécurité. Dans un premier temps, il est nécessaire d'illustrer une méthode de télécommunication classique connue sous l'acronyme DPSK. Ensuite, un protocole de QKD utilisant le DPSK est exposé. Sui une analyse de sa sécurité.

1.3.1 La télécommunication par DPSK

L'acronyme "DPSK" réfère à un protocole de télécommunication classique nommé *Differential Phase Shift Keying*. Celui-ci code l'information à communiquer dans le déphasage entre deux impulsions lumineuses consécutives. Par exemple, si le déphasage entre deux impulsions est de 0 ou π, le bit correspondant est 0 ou 1 respectivement.

Souvent, les réseaux de télécommunication différencient le 0 ou le 1 par leur intensité : le 0 possède une intensité plus faible (ou nulle) que le 1. Les bits sont ainsi reçus par des détecteurs optiques et le signal optique est transformé en signal électrique (numérique). Toute intensité détectée au delà d'un certain seuil correspond à un 1 en deçà d'un autre seuil à un zéro. Pour insérer la télécommunication optique par DPSK dans ce schéma, il est donc nécessaire de traduire la phase entre les impulsions consécutives en intensité faible (0) ou forte (1). Or, cette opération est bien connue en optique : toute opération qui traduit la phase en intensité est une opération d'interférométrie. Dans le cadre du protocole DPSK, un interféromètre de type Mach-Zehnder est utilisé.

1.3.2 Les impulsions faibles

Par analogie avec la méthode DPSK classique, on peut également appliquer le même protocole de communication dans une limite quantique. Or, cette limite correspond au cas où les impulsions sont dites *faibles*. Cela réfère à la limite où l'intensité des

impulsions est telle que la description quantique du rayonnement devient nécessaire.

On réalise simplement les impulsions faibles en atténuant très fortement les impulsions d'un laser, auquel cas la description correcte de cette radiation se fait au moyen du formalisme des *états cohérents*[9]. On peut montrer qu'un état cohérent correspond à une superposition d'états nombres distribués sur l'espace des nombres de photons n selon une loi de probabilité poissonienne. Ainsi, un état cohérent possède un nombre non déterminé de photons. En revanche, on peut pleinement décrire un état cohérent en spécifiant le nombre moyen de photons, noté $\bar{n}$, qui est directement relié à l'amplitude du champ électrique de l'onde électromagnétique classique. Ainsi dans le formalisme de l'état cohérent, l'atténuation du laser correspond à l'abaissement de $\bar{n}$. Généralement, une impulsion faible possède un nombre moyen de photons de l'ordre de $\bar{n} \approx 0,01$. En moyenne donc, pour un tel train d'impulsions, seul une impulsion sur cent possède un photon, les autres sont "vides" avec une amplitude qui correspond à *l'état du vide*[10].

Les impulsions faibles conservent toutes les propriétés de la radiation laser classique, incluant le fait que l'on peut leur attribuer une phase qui se manipule de manière semblable à celle d'une impulsion non faible. On peut donc les manipuler selon les prescriptions du protocole DPSK, incluant l'interférence.

1.3.3 Le protocole de QKD par DPSK

Puisque le protocole de QKD par DPSK est conçu pour produire des manipulations techniquement réalisables, il importe de décrire le protocole en fonction de ces manipulations et des éléments technologiques qui les réalisent. Un montage typique de QKD par DPSK est présenté à la figure 1.1.

Alice possède un laser (source de lumière cohérente), un modulateur de phase et

[9]Pour une description plus complète de l'état cohérent, incluant une justification pour son utilisation pour décrire la radiation laser, voir l'annexe A section 2.

[10]Pour une description formelle de l'état nombre incluant l'état du vide voir l'annexe A section 1.

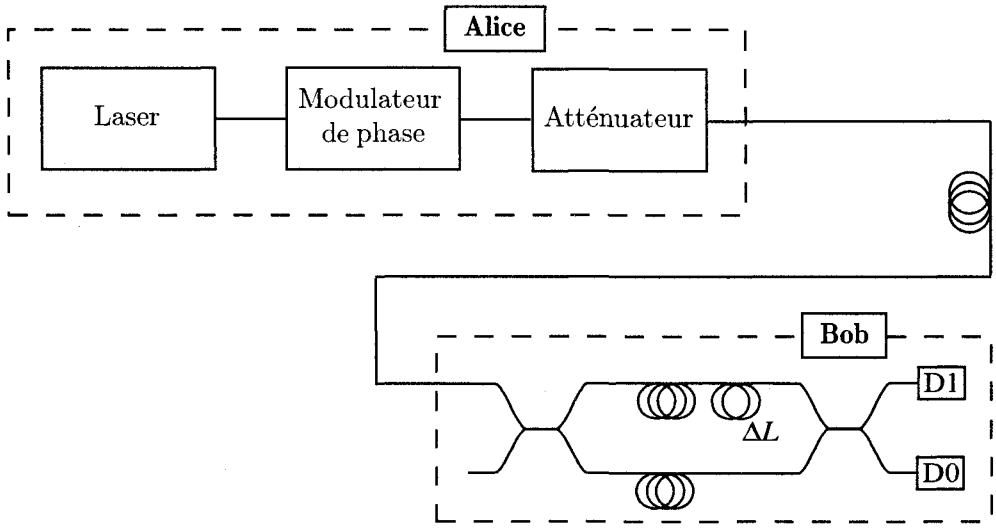


FIG. 1.1 – Montage typique de QKD par DPSK.

un atténuateur. Bob possède un interféromètre de Mach-Zehnder et deux détecteurs optiques placés à chaque branche de sortie de l'interféromètre. Entre Alice et Bob, une fibre optique est utilisée comme voie de transmission. Le laser produit un train d'impulsions régulier dont Bob connaît la période[11].

L'algorithme procède comme suit :

1. Alice choisi *aléatoirement* une phase $\varphi \in \{0, \pi\}$, utilise sont modulateur de phase pour l'appliquer sur une impulsion.
2. Alice répète cette même opération pour l'impulsion suivante, de sorte que le déphasage entre ces deux impulsions est 0 ou π, aléatoirement. Elle mémorise cette valeur dans un lieu sûr.
3. Ces deux impulsions sont fortement et également atténuées par l'atténuateur d'Alice, de sorte que ces impulsions deviennent des impulsions faibles avec $\bar{n} < 1$
4. Les impulsions faibles se propagent dans la fibre vers l'interféromètre de Bob. Cet interféromètre est tel que le délai ΔL entre les deux branches correspond

[11] Alice et Bob peuvent par exemple se partager, classiquement, un signal d'horloge.

exactement au délai entre les deux impulsions de sorte que l'interférence se fait toujours entre deux bits consécutifs. Si la phase entre les impulsions est de 0, l'interférence sera constructive au détecteur D0 alors qu'elle sera constructive à D1 si la phase est de π.

5. Puisque $\bar{n} < 1$, pour la plupart du temps, ni D0 ou ni D1 n'enregistre de signal "click"). Lorsqu'il y a un click, Bob enregistrera de quel détecteur il provient ainsi que l'instant t_i de ce click.
6. Bob annonce publiquement qu'il a enregistré un click et publie l'instant t_i de détection (mais conserve secret le détecteur qui a enregistré le click).
7. Alice sait quelle phase elle avait choisi et appliqué sur les impulsions qui correspondent au moment t_i et peut donc savoir le résultat (0 ou 1) de la mesure de Bob. Elle conserve alors ce bit. Bob fait de même.
8. Les étapes 1 à 7 sont répétées jusqu'à ce que la séquence de bits K conservée par Alice et Bob soit *plus longue* que le texte clair $P \in \mathcal{P}$ qu'Alice veut transmettre à Bob.
9. Alice et Bob dévoilent publiquement une fraction de leur séquence de bits afin d'en calculer le *taux d'erreur quantique* (QBER).
10. Alice et Bob appliquent un *algorithme de correction d'erreur* afin de compenser pour toute erreur de transmission sur le canal quantique.
11. Alice et Bob appliquent un *algorithme d'amplification du secret* afin de réduire l'information que pourrait posséder Ève à un niveau arbitrairement petit.

La sécurité de ce protocole ne se démontre pas de façon aussi intuitive que pour le BB84. Néanmoins, mentionnons que la sécurité repose sur le fait que le nombre moyen de photons par impulsion est beaucoup plus petit que 1, de sorte que la plupart des impulsion sont vides. Ainsi, par exemple, si Ève tente une attaque de type *intercept-resend*[12], elle introduirait généralement une erreur dans l'indexation t_i des qubits

[12]Attaque où Ève intercepte les qubits provenant d'Alice, les mesure et les revoit à Bob afin de

d'Alice et Bob.

Par contre, puisqu'on utilise ici des impulsions faibles, il est peu probable (mais certainement pas impossible) qu'une impulsion contienne plus d'un photon. Dans ce cas, en utilisant une mesure non-destructive (QND[13]) Eve peut apprendre, sans perturber l'information que porte l'impulsion, que cette dernière contient plus d'un photon. Elle peut alors utiliser un photon pour apprendre une information partielle sur la séquence de bits qui sera la clef. Cette attaque s'appelle le *photon number splitting attack* (PNS) et est particulièrement efficace lorsqu'appliquée sur un échange BB84 où l'on utilise des impulsions faibles. Or, dans le cas du protocole DPSK, le fait que l'information soit en fait codée sur deux impulsions consécutives rend cette attaque beaucoup moins efficace. Donc, outre la simplicité de sa mise en application, le protocole DPSK accroît le niveau de sécurité ce qui se transformera en un taux de génération de clef plus élevée par rapport à BB84.

Pour une démonstration satisfaisante de la sécurité de la QKD par DPSK, voir Takesue et al. [7] ainsi que Inoue et al. [8].

1.3.4 Taux de génération de clef sécurisé

Pour le protocole DPSK, la taux de génération de clef sécurisée est [7] :

$$R_{\text{DPSK}} = f_r \bar{n}(1 - 2\bar{n})\eta_B \eta_T \tag{1.4}$$

On voit donc que le protocole DPSK produit un gain substantiel par rapport au protocole BB84 : la taux de génération de clef sécurisée diminue linéairement avec les pertes, repoussant la distance de transmission sécurisée d'autant.

---

tenter de se rendre invisible.

[13]De l'anglais *Quantum non-demolition attack*

1.4 L'interféromètre pour application en QKD par DPSK

Outre les défis majeurs que représentent les détecteurs (voir [9] et [10]), les pertes de transmission (dans la fibre ou autre pertes), un autre élément joue un rôle majeur dans la QKD par DPSK, soit l'interféromètre. Servant de décodeur dans ce protocole, le design, la fabrication et la caractérisation d'un interféromètre construit explicitement pour cette application fait l'objet de cet ouvrage.

L'interféromètre à construire ne doit pas être seulement un instrument de recherche en QKD ; celui-ci doit être conçu pour une utilisation *pratique* hors laboratoire. Il doit donc être conçu pour fonctionner dans un réseau de télécommunications à fibres optiques. Il doit donc être utilisable dans un environnement variable et dans des installations diverses. Nous explicitons ici dans quel contexte l'interféromètre doit opérer et nous traduisons cela en termes de spécifications.

1.4.1 Compatibilité avec les réseaux de télécommunications

Puisque la QKD se construit généralement à l'aide de manipulations sur des qubits optiques, l'ingénieur est alors placé devant un choix de deux mediums de communication pour la réaliser : (1) les fibres optiques ; (2) la communication "sans-fil". Or, pour le protocole DPSK pour lequel on cherche à maximiser la distance de communication, le premier choix s'impose. En effet, les fibres optiques présentent de très faibles pertes et celles-ci sont constantes. Dans le sans-fil, la divergence des impulsions faibles à la sortie du laser produit une source de pertes inévitable [1]. De plus, toute perturbation atmosphérique (comme la foudre par exemple) risque de faire augmenter de manière imprévisible le taux d'erreur, rendant l'implémentation beaucoup plus difficile. Finalement, l'alignement d'interféromètres peut poser problème. Ainsi, par élimination, le réseau de télécommunications par fibres optiques se présente comme choix naturel pour la QKD par DPSK.

Les réseaux de télécommunications par fibres optiques sont articulés autour d'un très vaste déploiement international et même intercontinental de fibres unimodales, dont la fibre SMF-28^{TM}de Corning. Celles-ci ont étés retenues à cause de leur faibles pertes et leur relative simplicité de fabrication. Elles possèdent un spectre de pertes avec un minimum à $\lambda = 1550$ nm. À cette longueur d'onde, les pertes sont de 0.2 dB/km. Pour cette raison, ce sont ces niveaux de pertes qui sont généralement utilisés pour construire les preuves de sécurité en fonction de la distance de transmission. On doit donc construire un interféromètre pour qu'il soit utilisé autour de 1550 nm.

De plus, la SMF-28 est une fibre unimodale à 1550 nm. Ceci constitue un avantage pour la QKD. Lorsqu'on effectue l'interférence des qubits dans l'interféromètre, Bob ne peut espérer avoir un contraste maximum (et donc un QBER minimisé) que si chaque état cohérent qu'il fait interférer possède la même distribution spatiale. Or, on peut considérer la fibre unimodale comme un *filtre spatial* extrêmement sélectif puisque seul le mode fondamental de la fibre peut s'y propager sur des distances plus grandes que quelques mètres. Ainsi, Bob peut espérer un contraste optimal sans manipulation supplémentaire sur la distribution spatiale des impulsions faibles que lui transmet Alice. Par contre, pour minimiser les pertes d'insertion, son interféromètre doit être tel que les modes qui s'y propagent soient exactement identiques à ceux de la fibre, sans quoi le couplage entre le mode de la fibre et celui de l'interféromètre sera imparfait ce qui se traduit par des pertes pouvant être importantes[14].

Cependant, pour l'obtention simplifiée d'un contraste maximum à l'interféromètre de Bob, il aurait été souhaitable que la fibre SMF-28 conserve l'état de polarisation des impulsions qui s'y propagent. Cela n'est pas le cas : la fibre SMF-28, en fonction surtout des contraintes qui lui sont imposées (comme sa courbure par exemple), autorise le couplage entre modes de différentes polarisations. Cela fait en sorte que dans les réseaux de télécommunications par fibres optiques, les autres éléments du réseaux comme les répéteurs, les détecteurs et les protocoles eux-mêmes, sont conçus

[14]Ce phénomène est souvent appelé (en anglais) le *mode matching*.

pour ne pas être sensibles à la polarisation. Dans le cas de la QKD donc, cela devra aussi être le cas, ce qui constitue un défi puisque l'interférence est toujours sensible à la polarisation : seules des impulsions faibles de même polarisation peuvent interagir en interférant.

Dans le protocole DPSK, les impulsions à faire interférer sont deux impulsions successives séparées de quelques nanosecondes. Puisque les changements dans le couplage des modes de différentes polarisations ne peuvent qu'être très lents par rapport au délai entre les implusions, on peut considérer que *chaque impulsion d'une paire* sera à toutes fins pratiques de même polarisation et ce en tout temps. Cependant, cela ne signifie pas que les *paires* seront toutes de la même polarisation. Si la communication s'étend sur quelques secondes, il en envisageable que le couplage des polarisations ait évolué de manière appréciable. Dans ce cas, les *paires* impulsions du départ ne seront pas de la même polarisation que celles de la fin. Pour composer avec ce fait, l'interféromètre doit produire une interférence identique et la plus contrastée possible pour toutes les polarisations, mais on suppose que deux impulsions successives ont toujours de la même polarisation.

De plus, il est essentiel de tenir compte du fait que les qubits optiques ne sont pas directement compatibles avec les réseaux de télécommunication installés puisque ceux-ci contiennent des éléments optoélectoniques (répéteurs, multipleuxeurs, etc.). Ces éléments ont pour but de transformer les signaux lumineux en signaux électriques afin de les manipuler avec de l'électronique pour ensuite reconvertir le signal en signal optique pour poursuivre la transmission à faible perte dans la fibre. Or, la mesure d'amplitude d'un état cohérent par un détecteur ne permet pas du tout d'en conserver la phase puisque ces deux variables sont reliées quantiquement par une relation d'incertitude[15]. Puisqu'on mesure l'amplitude, on détruit l'information de phase et puisque la phase contient *l'information* du *qubit optique*, les éléments optoélectroniques ne sont pas compatibles avec la QKD optique.

[15]Pour une discussion plus complète sur ce sujet, voir l'annexe D

Ainsi, la QKD nécessite un réseau *dédié* qui ne contient en fait que de fibres optiques et qui, à cause du théorème de non-clonage ne contient aucun élément amplificateur[16]. Cependant, il n'est pas déraisonnable de considérer qu'un tel réseau existe à moyen terme pour certaines applications où la QKD pourrait être d'une utilité première, comme la communication entre installations militaires par exemple. En revanche, il n'est pas exclu de pouvoir effectuer du multiplexage des communications dans la même fibre (une Alice et plusieurs Bob) ou même de faire partager la bande passante de la fibre entre des communications classiques (implusions fortes) quantiques (impulsions faibles) [11, 12].

Également, comme Alice et Bob doivent absolument posséder une base de temps commune afin de procéder à la réconciliation de leurs clefs dans le protocole DPSK, ils devront se donner une horloge commune et précise. Ce système sera normalement constitué d'un signal d'horloge et d'une électronique associée. Cette horloge peut prendre diverse formes (comme un train d'impulsions fortes dans la fibre par exemple), mais on suppose ici que ce signal d'horloge est indépendant du signal du canal quantique d'Alice et de Bob (bien que ce train d'impulsions puisse se multiplexer dans la même fibre). Ainsi, en plus des exigences citées ci-dessus, Alice et Bob devront se doter d'un système d'horloge précis afin de se donner une base de temps commune.

Finalement, on cherche un interféromètre d'une taille raisonnable, soit approximativement celle d'un ordinateur de table. De plus, il doit être utilisable dans un environnement intérieur ayant des conditions environnementales typiques, soit une température d'environ 23°C.

En résumé, l'interféromètre pour la QKD par DPSK doit :

- être conçu pour un fonctionnement à $\lambda = 1550$ nm ;
- être adapté pour le profil spacial du mode de la fibre SMF-28 ;
- produire une interférence uniforme pour tout état de polarisation ;

[16]En particulier, bien qu'ils ne soient pas des éléments optoélectroniques, les amplificateurs EDFA ne peuvent être utilisés dans un réseau de QKD

- être contenu dans un ensemble dont le volume est comparable à celui d'un ordinateur de table typique ;
- être conçu pour fonctionner dans un environnement intérieur d'une température de 23°C.

À ces spécifications applicables à l'interféromètre, on doit ajouter que la QKD par DPSK nécessite un réseau dédié ne contenant que des éléments en fibres optiques SMF-28 (et aucun élément optoélectronique) et qu'Alice et Bob doivent se doter d'un système d'horloge pour permettre la réconciliation de leurs clefs.

1.4.2 La compatibilité avec le protocole de QKD par DPSK

Les fait d'utiliser le l'interféromètre pour la QKD par DPSK a des conséquences supplémentaires sur les caractéristiques de celui-ci. En particulier, il doit être conçu pour fonctionner à un taux de répétition imposé par le taux de répétition des impulsions qu'envoie Alice. Également, il devra permettre une minimisation du taux d'erreur (le QBER) qui lui est associé.

1.4.2.1 Le taux de répétition

Le taux de répétition est définit par :

$$f_r = \frac{1}{\Delta t_{imp}} \tag{1.5}$$

où Δt_{imp} représente le délai entre deux impulsions. La DPSK impose à l'interféromètre de faire en sorte que chaque impulsion interfère avec la précédente afin que la phase relative entre ces impulsions traduise l'information qu'Alice veut communiquer à Bob. Ainsi, le délai τ de l'interféromètre doit être exactement égal au délai entre les impulsions

$$\tau = \Delta t_{imp} \tag{1.6}$$

Le délai de l'interféromètre est égal à

$$\tau = \frac{n\Delta L}{c} \tag{1.7}$$

où c est la vitesse de la lumière, n est l'indice de réfraction des bras de l'interféromètre et ΔL est la différence de longueur des bras. Il vient donc que l'interféromètre doit satisfaire

$$\Delta L = \frac{c}{nf_r} \tag{1.8}$$

Un taux de répétition le plus grand possible mène à un taux de génération de clef le plus rapide possible, ce qui est bien sûr souhaitable. Donc, ce taux n'est limité que par la technologie. Il y a a priori trois sources de limitation possibles : (1) les détecteurs ; (2) le taux de répétition du laser ; (3) le taux de répétition du modulateur de phase à Alice et (4) la vitesse maximale à laquelle peut fonctionner un système de synchronisation entre les bases de temps d'Alice et Bob (l'horloge).

Au lieu de moduler la phase des impulsions d'un laser, il peut être pratique pour Alice de simplement moduler la phase d'un signal laser continu. Comme le signal laser continu et atténué constitue, comme le train d'impulsions atténué, un état cohérent cela n'a pas d'impact sur le principe de fonctionnement du protocole DPSK. Par contre, cela élimine le besoin de synchroniser tout le système avec le taux de répétition du laser et ainsi augmente la flexibilité du système.

De plus, puisqu'ils sont conçus pour les réseaux de télécommunications où les fréquences de fonctionnent sont maintenant réalisables à 40 Gbit/s, Alice dispose assez facilement d'un modulateur de phase qui fonctionne sans problème jusqu'à cette fréquence. Comme la fréquence de l'impulsion elle même ($\nu = c/\lambda$) est de l'ordre du THz, une modulation dans les Gbit/s est tout à fait possible.

Par contre, le système d'horloge fait intervenir une électronique dont le coût augmente avec le taux de répétition. Donc, pour limiter les coûts de ce système dans nos expériences, le *taux de répétition du protocole DPSK est limité à 100 Mbit/s.* Par

contre, il est possible en principe d'effectuer de la QKD par DPSK jusqu'au Gbit/s avec un système d'horloge approprié.

1.4.2.2 Le QBER

La minimisation du taux d'erreur quantique, le QBER, est la principale exigence pour un interféromètre de Mach-Zehnder pour la QKD. De manière générale, comme on l'a vu au chapitre 1, il existe un QBER limite au delà duquel Alice et Bob ne pourront s'échanger une clef de manière sécuritaire. Puisque les pertes de transmission dans la fibre sont inhérentes et ne peuvent être minimisées autrement qu'en limitant la distance de transmission, le fait de minimiser le QBER associé exclusivement à l'interféromètre résulte en une distance de transmission possible plus grande.

D'emblée, on fixe la limite du QBER relié à l'interféromètre à 0,01 soit 1%.

En supposant que les impulsions successives constituant les paires sont de même amplitude, ce qui est réaliste puisque les pertes dans la fibres ne varient pas de manière appréciable sur l'échelle de temps de quelques ns ou μs, le QBER de l'interféromètre est donné par :

$$\text{QBER} = \frac{1 - V}{2} \tag{1.9}$$

où V est la visibilité de l'interféromètre.

On requiert un QBER $\leq 1\%$.

Chapitre 2

Design et fabrication

Nous abordons dans ce chapitre la méthode de conception et de fabrication d'un interféromètre optimisé pour utilisation comme *décodeur* quantique dans un schéma de QKD par DPSK. Après avoir décrit formellement le Mach-Zehnder tout-fibre et établi les tolérances sur son comportement, nous présentons les deux éléments principaux du design (1) la *compensation thermique passive* et (2) la *compensation de biréfringence*. Finalement, nous décrivons et justifions les étapes de la fabrication de l'interféromètre.

2.1 Le Mach-Zehnder tout fibre

D'abord, il est utile d'établir que pour un fonctionnement dans un protocole de DPSK à 100 Mbit/sec, l'application de l'équation 1.8 donne $\Delta L = 2{,}042$ m.

Cela étant dit, afin de réaliser un interféromètre ayant les requis donnés au chapitre précédent, plusieurs types d'interféromètre sont à considérer. Citons les exemples suivants :

- Mach-Zehnder sur table optique
- Mach-Zehnder sur guide d'ondes "microfabriqué"
- Mach-Zehnder tout-fibre

De tous ces choix, le Mach-Zehnder sur table optique est clairement le plus simple à construire. Tous les éléments, incluant les miroirs et les diviseurs d'onde sont commercialement disponibles, et le tout se construit assez facilement sur une table optique. Cependant, ce sont des fibres optiques qui transportent les états vers l'interféromètre. À leur sortie, comme la lumière est divergente, il est nécessaire d'inclure des éléments optiques focalisants comme des lentilles afin d'insérer la lumière dans l'interféromètre. Or, inhérent à toutes ces transformation sont des pertes. De plus, à $\Delta L = 2{,}042$ m de différence de longueur de ce type d'interféromètre risque d'être difficile à utiliser hors laboratoire.

Pour ce qui est du Mach-Zehnder microfabriqué, en plus de produire des pertes d'insertion certainement trop élevées (de l'ordre de 3 dB - l'équivalent de 15 km de fibre), ce type d'interféromètre n'est pas réalisable pour un schéma DPSK à 100 Mbit/sec. En effet, il n'est pas raisonnable de tenter de microfabriquer un interféromètre ayant $\Delta L = 2{,}042$ m. Par contre, ce type d'interféromètre offre des propriétés de stabilité suffisamment intéressantes pour qu'il soit souvent choisi pour des expériences de QKD par DPSK qui se font à des taux de répétitions plus élevés que 100 Mbit/s [8, 7].

Quant à l'interféromètre Mach-Zehnder tout-fibre, il présente un potentiel très intéressant. Inhérent à sa construction tout-fibre, cet interféromètre offre une perte d'insertion absolument minimale. De plus, puisqu'on peut envisager d'enrouler les fibres optiques qui composeraient les branches, le délai correspondant à 100 Mbit/sec n'est pas nécessairement un obstacle à sa réalisation et à son utilité dans une multitude d'environnements. Par contre, ce type d'interféromètres présente a priori un problème pour ce qui est des spécifications de stabilité et d'insensibilité à la polarisation. Or, on montre par la suite que ces problèmes peuvent se résoudre par conception et sans avoir recours à un système de contrôle actif.

Si ce type d'interféromètre peut se réaliser afin qu'il soit stable, bien contrasté et insensible à la polarisation, alors l'interféromètre Mach-Zehnder tout-fibre représente

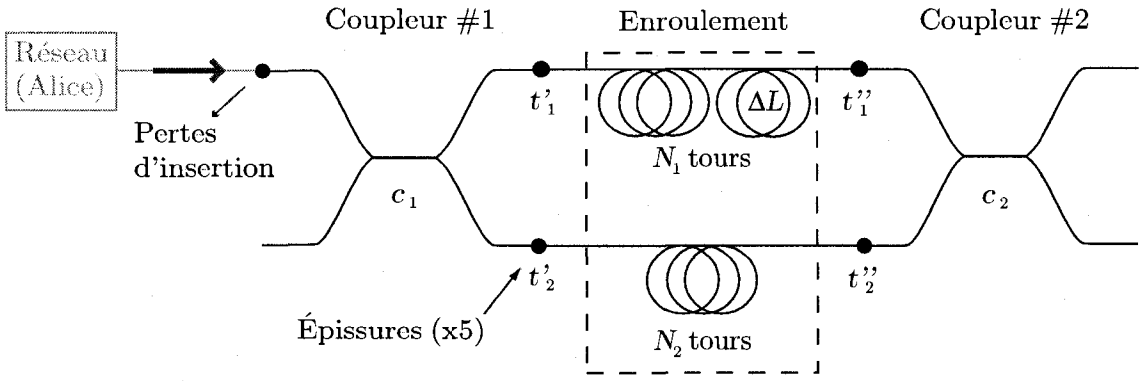


FIG. 2.1 – Le Mach-Zehnder tout fibre avec enroulement des branches.

la solution idéale pour la QKD par DPSK puisque le taux d'erreur quantique relié à cet élément est minimisé.

2.1.1 Description

L'interféromètre tout-fibre est composé de deux coupleurs fusionnés entre lesquels les branches sont constituées de fibres optiques. On présente à la figure 2.1 un schéma de ce type d'interféromètre.

Les coupleurs fusionnés, éléments couramment utilisés dans les réseaux de télécommunication pour effectuer du multiplexage en longueur d'onde représentent une technologie bien maîtrisée. Ils sont constitués de deux fibres dont les gaines optiques ont étés fusionnées ensemble de telle sorte que les cœurs des fibres soient rapprochés suffisamment pour induire un couplage. En ajustant la longueur et le profil de la section fusionnée, on peut obtenir des coupleurs tels que si on leur injecte de la lumière uniquement dans une branche, cette lumière sera divisée à 50/50 entre les deux branches de sortie. Ce type de coupleur est caractérisé par une matrice de transfert comme suit

$$C = \begin{bmatrix} c_1 & jc_2 \\ -jc_2 & c_1 \end{bmatrix} \tag{2.1}$$

avec $c_1 = c_2 = 1/\sqrt{2}$. On utilise ce type de coupleur pour les deux coupleurs représentés à la figure 2.1. Les pertes pour ce type de composant peuvent être très faibles : moins de 0,1 dB. Celles-ci contribuent uniquement aux pertes d'insertion de l'interféromètre.

Entre les coupleurs, on insère les fibres constituant les branches de l'interféromètre. Dans le cas qui nous concerne, ces fibres seront enroulées de sorte que l'interféromètre a une petite taille malgré la grande longueur de ses branches. Les épissures, entre les coupleurs et les branches, mènent à des pertes équivalant à $t_1 = t_1' t_1''$ et $t_2 = t_2' t_2''$ dans les branches 1 et 2 de l'interféromètre, tel que montré sur la figure 2.1. L'effet de la propagation dans les branches est donné par la matrice de transfert suivante

$$\begin{bmatrix} t_1 e^{j\beta L_1} & 0 \\ 0 & t_2 e^{j\beta L_2} \end{bmatrix} \tag{2.2}$$

On peut décrire le comportement de l'interféromètre en considérant que si les impulsions provenant d'Alice sont insérés dans la branche 1, la radiation entrant dans l'interféromètre est notée par

$$\begin{bmatrix} E_0 \\ 0 \end{bmatrix} \tag{2.3}$$

Ainsi, l'effet de l'interféromètre sur l'impulsion d'Alice est donnée par

$$\mathbf{E}_f = \begin{bmatrix} c_1' & jc_2' \\ -jc_2' & c_1' \end{bmatrix} \begin{bmatrix} t_1 e^{j\beta L_1} & 0 \\ 0 & t_2 e^{j\beta L_2} \end{bmatrix} \begin{bmatrix} c_1 & jc_2 \\ -jc_2 & c_1 \end{bmatrix} \begin{bmatrix} E_0 \\ 0 \end{bmatrix} \tag{2.4}$$

En effectuant la multiplication, il vient

$$\mathbf{E}_f = \begin{bmatrix} \left(c_1' c_1 t_1 e^{j\beta L_1} - c_2' c_2 t_2 e^{j\beta L_2}\right) E_0 \\ \left(c_2' c_1 t_1 e^{j\beta L_1} - c_1' c_2 t_2 e^{j\beta L_2}\right) E_0 \end{bmatrix} \tag{2.5}$$

En notant $a_1 = c_1' c_1 t_1$ et $a_2 = c_2' c_2 t_2$, et si Bob lit la sortie de l'interféromètre sur la

branche de sortie 1, l'intensité sera

$$I_1 = E_0^2 \left(a_1 e^{j\beta L_1} - a_2 e^{j\beta L_1}\right)\left(a_1 e^{-j\beta L_1} - a_2 e^{-j\beta L_1}\right) \quad (2.6)$$

$$= E_0^2 \left\{a_1^2 + a_2^2 - 2a_1 a_2 \cos\left[\beta(L_1 - L_2)\right]\right\} \quad (2.7)$$

Pour des fibres optiques, le paramètre de propagation β est donné par le produit du vecteur d'onde k_0 et de l'indice de réfraction n, de sorte que la différence de phase entre les branches s'écrit

$$\Delta\phi = k_0 n \Delta L \quad (2.8)$$

Puisque les longueurs d'onde utilisées en télécommunication sont autour de $\lambda = 1{,}55\ \mu$m et que le vecteur d'ondes k_0 est de l'ordre de $4 \times 10^6\ \mathrm{m}^{-1}$, on voit immédiatement que $\Delta\phi$ est très sensible aux variations de ΔL et de n. Dans la fibre, les effets de température sur n sont en général non négligeables, rendant la transmission de l'interféromètre Mach-Zehnder tout-fibre normalement très instable vis-à-vis les changement de température.

Pour tenir compte des effets d'instabilité dans $\Delta\phi$ dans la visibilité de l'interféromètre, on peut comptabiliser les instabilités comme une tolérance sur $\Delta\phi$. Dans ce cas, on dira que les maxima et minima sur la courbe d'interférence seront pour des multiples de

$$I_{max} \rightarrow \Delta\phi_{tol} \bmod 2\pi \quad (2.9)$$

$$I_{min} \rightarrow \pi + \Delta\phi_{tol} \bmod 2\pi \quad (2.10)$$

Donc

$$I_{max} = E_0^2 \left[a_1^2 + a_2^2 + 2a_1 a_2 \cos(\Delta\phi_{tol})\right] \quad (2.11)$$

$$I_{min} = E_0^2 \left[a_1^2 + a_2^2 + 2a_1 a_2 \cos(\pi + \Delta\phi_{tol})\right] \quad (2.12)$$

de sorte que la visibilité est donnée par

$$V \equiv \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{2.13}$$

$$= \frac{2a_1a_2\left[\cos(\Delta\phi_{tol}) - \cos(\pi + \Delta\phi_{tol})\right]}{2(a_1^2 + a_2^2 + 2a_1a_2\left[\cos(\Delta\phi_{tol}) + \cos(\pi + \Delta\phi_{tol})\right]} \tag{2.14}$$

Ce résultat permet de déterminer des tolérances réalistes pour les paramètres de l'interféromètre.

2.1.2 Budget de tolérances

Nous avons fixé la tolérance sur le QBER à 1%. En observant l'équation 2.14, on voit que la visibilité est fonction

- du taux de couplage dans les coupleurs #1 et #2 ;
- des pertes dans les branches ;
- de l'instabilité.

On tolère une erreur sur les taux de couplage d'au plus 1%. On tolère également des pertes dans les branches, principalement aux épissures (entre les coupleurs et les fibres qui composent les branches) d'au plus 0,1 dB (et d'au moins 0,01 dB).

Pour fixer la tolérance sur les taux de couplage, on cherche le cas où l'effet des coupleurs et des pertes mène au contraste le plus faible. Cela correspond au cas où a_1 et a_2 (l'effet amalgamé des coupleurs et des pertes) sont les plus différents possibles.

Pour les pertes, on considère le cas où celles-ci sont de 0,1 dB dans chaque épissure de la branche 1 et de 0,01 dB dans chaque épissure de la branche 2. Dans ce cas, on a $t_1 = \sqrt{0{,}950} = 0{,}977$ et $t_2 = \sqrt{0{,}995} = 0{,}998$.

Pour les coupleurs, le pire cas est celui ou $c_1'c_1 = \sqrt{0{,}495}^2 = 0{,}495$ et $c_2'c_2 = 0{,}505$. Ainsi, on obtient

$$a_1 \approx 0{,}483$$

$$a_2 \approx 0{,}503$$

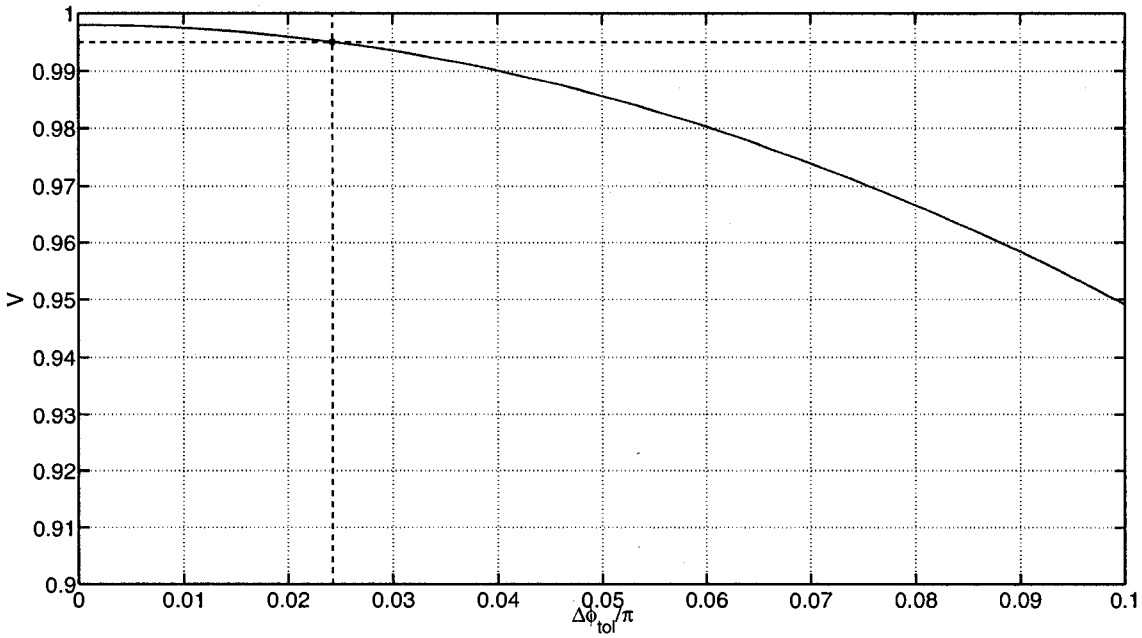


FIG. 2.2 – Visibilité de l'interféromètre en fonction des instabilités de phase.

Dans ce cas, la visibilité est donnée par

$$V = \frac{0{,}487\left[\cos(\Delta\phi_{tol}) - \cos(\pi + \Delta\phi_{tol})\right]}{0{,}976 + 0{,}487\left[\cos(\Delta\phi_{tol}) + \cos(\pi + \Delta\phi_{tol})\right]} \tag{2.15}$$

Il reste à fixer la tolérance sur la phase. Pour ce faire, la figure 2.2 donne un graphique de la visibilité de l'interféromètre (suivant l'équation 2.15) en fonction de la tolérance sur la différence de phase. On remarque sur cette figure que la *visibilité nominale* désirée (soit $V = 0{,}995$) est atteinte pour $\Delta\phi \approx 0{,}025\pi$. On définit donc la tolérance sur la phase à $\Delta\phi_{tol} \approx 0{,}025\pi$.

Afin de bien décrire les effets thermiques et la biréfringence des fibres optiques et leur influence sur $\Delta\phi$, il est nécessaire de décrire les effets thermiques et élastiques dans les fibres optiques qui sont à l'origine des variations de n, et de la biréfringence d'une fibre, respectivement. Ceci est couvert à l'annexe E.

2.2 La compensation thermique passive

La *compensation thermique passive* se veut une méthode par laquelle les effets thermiques d'une branche de l'interféromètre sont utilisés afin de compenser les effets thermiques de l'autre branche.

La phase accumulée dans une branche de l'interféromètre s'écrit

$$\phi_1 = k n_1 L_1 \tag{2.16}$$

Face à un changement de température infinitésimal, la variation de ϕ_1 est donnée par la somme de l'effet thermo-optique et l'effet de l'expansion thermique :

$$\frac{\phi_1}{dT} = k\frac{d}{dT}\left[n_1(T)L_1(T)\right] \tag{2.17}$$

$$= k\left[n_1\frac{dL_1}{dT} + L_1\frac{dn_1}{dT}\right] \tag{2.18}$$

Ainsi, pour un changement de température de T_0 à T

$$\phi_1(T) - \phi_1(T_0) = k\int_{T_0}^{T}\left[n_1\frac{dL_1}{dT} + L_1\frac{dn_1}{dT}\right]dT \tag{2.19}$$

$$\approx k\left[n_1\left.\frac{dL_1}{dT}\right|_{T_0}(T-T_0) + L_1\left.\frac{dn_1}{dT}\right|_{T_0}(T-T_0)\right] \tag{2.20}$$

Soit, en introduisant le *coefficient d'expansion thermique*

$$\alpha_L = \frac{1}{L}\frac{dL}{dT} \tag{2.21}$$

et le *coefficient thermo-optique*

$$\alpha_n = \frac{dn}{dT} \tag{2.22}$$

on obtient

$$\phi_1(T) - \phi_1(T_0) = k\left[n_1 L_1 \alpha_{L_1} + L_1\alpha_{n_1}\right](T - T_0) \tag{2.23}$$

Similairement pour la branche 2, en supposant la même variation de température

$$\phi_2(T) - \phi_2(T_0) = k\left[n_2 L_2 \alpha_{L_2} + L_2 \alpha_{n_2}\right](T - T_0) \tag{2.24}$$

Pour simplifier la notation, on suppose dorénavant que toutes les quantités variables avec la température sont référées à T_0. Ainsi, la variation de la différence de phase entre les branches de l'interféromètre s'écrit

$$\begin{aligned}
\Delta\phi(T) - \Delta\phi(T_0) &= [\phi_1(T) - \phi_2(T)] - [\phi_1(T_0) - \phi_2(T_0)] && (2.25)\\
&= [\phi_1(T) - \phi_1(T_0)] - [\phi_2(T) - \phi_2(T_0)] && (2.26)\\
&= k\left[(n_1 L_1 \alpha_{L_1} - n_2 L_2 \alpha_{L_2}) + (L_1 \alpha_{n_1} - L_2 \alpha_{n_2})\right](T - T_0) && (2.27)\\
&= k\left[L_1\left(n_1 \alpha_{L_1} + \alpha_{n_1}\right) - L_2\left(n_2 \alpha_{L_2} + \alpha_{n_2}\right)\right](T - T_0) && (2.28)\\
& && (2.29)
\end{aligned}$$

L'objectif de la *compensation thermique passive* est de faire en sorte que la variation de température n'a pas d'effets significatifs sur la différence de marche optique de l'interféromètre, c.-à.-d. $\Delta\phi(T) = \Delta\phi(T_0)$. Pour réaliser ceci, il vient immédiatement que le terme entre crochets dans l'expression 2.29 doit être nul. Ainsi, on cherche L_1 et L_2 tels que

$$L_1 \alpha_{n_1} - L_2 \alpha_{n_2} = L_2 n_2 \alpha_{L_2} - L_1 n_1 \alpha_{L_1} \tag{2.30}$$

D'où on tire

$$\frac{L_1}{L_2} = \frac{\alpha_{n_2} + n_2 \alpha_{L_2}}{\alpha_{n_1} + n_1 \alpha_{L_1}} \tag{2.31}$$

Ainsi, puisque pour un interféromètre $L_1 \neq L_2$, si $\alpha_{n_1} \neq \alpha_{n_2}$, alors il existe un rapport des longueurs pour lequel $\Delta\phi$ n'est plus sensible à la température. Il s'agit de compensation *passive* puisque l'interféromètre est stable par rapport à l'effet thermo-optique, si l'équation 2.31 est respectée[1], et ce, de manière *inhérente.*

[1]Il est à noter que puisque dans les faits, les coefficients thermo-optiques des fibres sont légèrement

En pratique, puisqu'il est impossible de fabriquer des branches avec une précision infinie sur les longueurs L_1 et L_2, il est utile d'établir une tolérance sur ces longueurs.

On définit s_T, la sensibilité de $\Delta\phi$ à la température

$$s_T = \frac{1}{k_0}\frac{d\Delta\phi(T)}{dT} \tag{2.32}$$

$$= [L_2(n_2\alpha_2 + \alpha_{n_2}) - L_1(n_1\alpha_1 + \alpha_{n_1})] \tag{2.33}$$

On cherche une sensibilité $s_T(L_1, L_2)$ maximale qui respectera la tolérance sur la différence de phase $\Delta\phi_{tol}$ sur une plage de $T_0 \pm \Delta T_{tol}$. Cette sensibilité maximale est donc donnée par

$$s_T|_{max} = \frac{1}{k_0}\frac{\Delta\phi_{tol}}{\Delta T_{tol}} \tag{2.34}$$

Pour traduire cette sensibilité maximale en tolérance sur L_1 et L_2, il est utile d'effectuer un développement de s_T en série de Taylor. Pour ce faire, on pose

$$s_T(x_1, x_2) = \frac{1}{k_0}[x_2(n_2\alpha_2 + \alpha_{n_2}) - x_1(n_1\alpha_1 + \alpha_{n_1})] \tag{2.35}$$

On effectue alors le développement de Taylor autour de L_1 et L_2, quantités qui satisfont à l'équation 2.31, c.-à.-d.

$$s_T(x_1, x_2) = s_T(L_1, L_2) + \left.\frac{\partial s_T(x_1, x_2)}{\partial x_1}\right|_{L_1,L_2}(x_1 - L_1) \tag{2.36}$$

$$+ \left.\frac{\partial s_T(x_1, x_2)}{\partial x_2}\right|_{L_1,L_2}(x_2 - L_2) \tag{2.37}$$

$$\tag{2.38}$$

où nous avons supposé que les termes d'ordre supérieur de la série sont nuls. Les différences $(x_1 - L_1)$ et $(x_2 - L_2)$ apparaissent donc comme les tolérances sur L_1 et L_2. On notera ces tolérances $(x_1 - L_1) \equiv L_{tol_1}$ et $(x_2 - L_2) \equiv L_{tol_2}$ et on les choisit

variables avec la température, c.-à.-d. $\alpha_n = \alpha_n(T)$, l'égalité 2.31 n'est vraie que pour une température de référence T_0

égales, soit $L_{tol_1} = L_{tol_2} = L_{tol}$. Finalement, par définition, on a que $s_T(L_1, L_2) = 0$ (selon l'équation 2.31). Pour se mettre dans le pire cas (où la tolérance est la plus petite, on prend le cas où l'erreur sur L_1 est positive et l'erreur sur L_2 est négative. On a donc

$$L_{tol} = k_0 \left| \frac{s_T|_{max}}{\frac{\partial s_T}{\partial x_1}\Big|_{L_1,L_2} - \frac{\partial s_T}{\partial x_1}\Big|_{L_1,L_2}} \right| \tag{2.39}$$

Soit, en évaluant les dérivées

$$L_{tol} = k_0 \left| \frac{s_T|_{max}}{(n_1\alpha_1 + \alpha_{n_1}) + (n_2\alpha_2 + \alpha_{n_2})} \right| \tag{2.40}$$

Ainsi, on a que $|\Delta\phi(T) - \Delta\phi(T_0)| \leq \Delta\phi_{tol}$ si L_1 et L_2 satisfont à l'équation 2.31 à l'intérieur de L_{tol}, pour $|T - T_0| \leq \Delta T_{tol}$.

2.2.1 Résultats et tolérances

Pour réaliser l'interféromètre passivement compensé, nous utilisons de la fibre SMF-28 de Corning pour la branche 1. Pour la branche 2, nous utilisons une fibre spéciale de marque Coractive. Cette fibre possède un dopage supplémentaire de phosphore (P) dans son cœur, ce qui a pour effet de réduire le coefficient thermo-optique par rapport à la fibre SMF-28, avec laquelle elle partage cependant une géométrie. Nous désignons cette fibre P+. Les propriétés optiques de ces fibres utilisées pour les calculs relatifs à l'interféromètre sont donnés dans le tableau 2.1. Il est à noter que nous avons choisi de négliger l'effet de l'expansion thermique sur l'interféromètre, ceci étant justifié par le fait que celui-ci a un effet deux ordres de grandeurs moindre que l'effet thermo-optique sur le comportement de l'interféromètre. De plus, notons que la valeur utilisée pour α_{n_1} est tirée de la référence [13] et la valeur α_{n_2} est connue comme étant 10% inférieure à cette dernière.

L'application de la formule pour le taux de répétition de l'interféromètre (éq. 1.8) combinée avec la formule pour la compensation thermique passive (éq. 2.31) mène à

une solution pour la longueur des branches de l'interféromètre. De plus, l'application de l'équation 2.40 donne la tolérance sur les longueurs de branche. Finalement, les pertes dans les épissures, les taux de couplage et leurs tolérances respectives ont étés établis à la section 2.1.2. Le résultat de tout ces calculs est présenté au tableau 2.2.

Dans le cadre de ce travail, les calculs sont effectués avec la routine `ParamInterf.m` (MATLAB). Ce programme est discuté à l'annexe F.

TAB. 2.1 – Constantes utilisées pour le design de l'interféromètre.

Constante	**Symbole**	**Valeur**	**Unités**
Indice effectif (SMF-28)	n_1	1,468 2	n/a
Indice effectif (P+)	n_2	1,468 2	n/a
Coefficient thermo-optique (SMF-28)	α_{n_1}	$0{,}92 \times 10^{-5}$	K^{-1}
Coefficient thermo-optique (P+)	α_{n_2}	$0{,}83 \times 10^{-5}$	K^{-1}
Tolérance en température	ΔT_{tol}	0,5	K
Tolérance sur $\Delta\phi$	$\Delta\phi_{tol}$	$0{,}025\pi$	rad

TAB. 2.2 – Valeur des paramètres de design de l'interféromètre.

Paramètre	**Symbole**	**Valeur**	**Tolérance**	**Unités**
Pertes dans les épissures	$1 - t^2$	0,01	+0,09	dB
Taux de couplage	$c'c$	50	0,5	%
Longueur de la branche 1	L_1	18,377	0,001	m
Longueur de la branche 2	L_2	20,419	0,001	m

Notons que l'application de l'équation 2.34 indique que la sensibilité en température maximale tolérable est de $s_T = 3{,}875 \times 10^{-8}$ [mK^{-1}]. Cela s'est traduit par les tolérances données dans le tableau 2.2.

Finalement, il est très important de remarquer qu'une des suppositions utilisée dans les calculs ci-haut est que la température est uniforme et égale pour les deux branches. Si tel n'est pas le cas, l'utilisation de la *compensation thermique passive* peut résulter en une augmentation de la sensibilité à la température.

2.3 Compensation de biréfringence

Comme la longueur des branches est de l'ordre des dizaines de mètres et que l'interféromètre doit éventuellement être contenu dans une enceinte de taille suffisamment petite pour en contrôler la température à 1 degré près, l'enroulement des branches est nécessaire. Or, comme la courbure de la fibre mène à une biréfringence, l'interféromètre est a priori sensible à la polarisation.

2.3.1 Problématique

Pour de la fibre de type SMF-28 enroulée, il n'existe aucune manière rigoureuse capable de réduire la biréfringence à zéro[2].

Par contre, il n'est pas nécessaire pour que l'interféromètre soit insensible (c.-à.-d. à visibilité égale et maximale) pour toutes les polarisations à l'entrée. Il suffit que les états de polarisation, après passage dans chaque branche, soient les mêmes.

On peut concevoir que l'enroulement de l'interféromètre soit identique pour les deux branches. Dans ce cas, *une condition nécessaire et suffisante pour que l'interféromètre soit insensible à la polarisation est que la différence de longueur entre les branches correspondent à un multiple entier de la longueur de battements de polarisation.* La résolution du problème de l'insensibilité à la polarisation revient alors à chercher une géométrie d'enroulement tel que cela se réalise.

De plus, l'enroulement doit d'être tel que les branches ne soient pas tributaires de la dilatation thermique de la structure autour duquel se fait l'enroulement. Autrement dit, l'enroulement ne doit pas être en contradiction avec les hypothèses de stabilisation par compensation thermique passive. En général, cela équivaut à dire que les fibres ne doivent avoir qu'un contact minimal avec la structure d'enroulement.

Pour cette raison, une structure basée sur des poteaux (voir la figure 2.3) fut choisie

[2]Pour une description des effets de la courbure sur la biréfringence d'une fibre optique, voir l'annexe E.

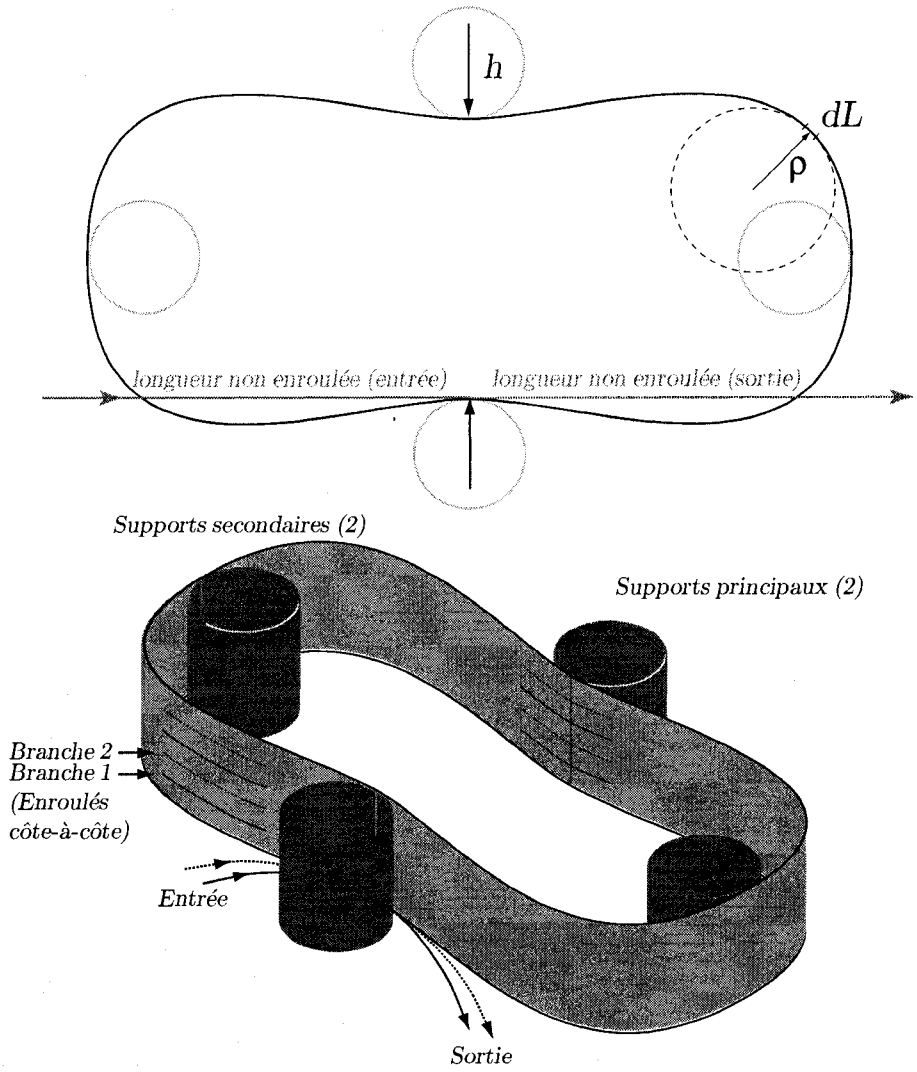


FIG. 2.3 – Géométrie d'enroulement des branches de l'interféromètre.

comme configuration pour l'enroulement. Cette structure possède quatre poteaux qui supportent la fibre ; deux poteaux supportent l'enroulement de l'extérieur et les deux autres de l'intérieur. On cherche un enroulement sans tension afin de réduire au minimum l'effet de la dilatation thermique des poteaux sur l'interféromètre.

2.3.1.1 Le choix du diamètre équivalent de l'enroulement

Dans ce texte, la longueur enroulée sur un tour sera mesurée par un diamètre équivalent d'enroulement, notée D_{eq} de sorte que la longueur sur un tour est de πD_{eq}.

La *compensation thermique passive* exige que les fibres des deux branches soient toujours à la même température. Ceci amène donc à enrouler les fibres des deux branches côte à côte sur toute leur longueur. Pour cette raison, les fibres de chaque branche sont enroulées autour des mêmes supports tel qu'illustré à la figure 2.3.

Par conséquent, il faut que l'enroulement soit en mesure d'accommoder les longueurs L_1 et L_2 avec un nombre entier de tours, ce qui pose le problème du choix d'un diamètre d'enroulement. Pour permettre un plus grand nombre de solutions à ce problème, on se donne une longueur non enroulée, notée L_{ne}.

En notant les longueurs à enrouler $(L_1)_e$ et $(L_2)_e$, on a

$$\begin{aligned} (L_1)_e &= L_1 - L_{ne} \\ (L_2)_e &= L_2 - L_{ne} \end{aligned}$$

On note N_1 et N_2 le nombre de tours dans chaque branche. Le problème revient à trouver un diamètre d'enroulement circulaire, noté D_{eq}, tel que la différence de longueur des branches s'enroule entièrement sur $N_2 - N_1 = \Delta N$ tours

$$D_{eq} = \frac{(L_1)_e - (L_2)_e}{\pi \Delta N} \tag{2.41}$$

Cette équation possède plusieurs solutions pour différentes valeurs de ΔN données.

Le choix sera en fait en fonction du nombre de tours à effectuer pour chaque branche

$$N_1 = \frac{(L_1)_e}{\pi D_{eq}}$$
$$N_2 = \frac{(L_2)_e}{\pi D_{eq}}$$

On choisit une solution donnant un bon compromis entre le nombre de tours à effectuer (à minimiser) et la taille finale de l'enroulement, fonction de D_{eq} (également à minimiser).

2.3.2 Algorithme d'optimisation

La configuration de la figure 2.3 est aussi choisie puisqu'elle permet une optimisation de la forme d'enroulement en fonction d'un seul paramètre : la dimension h. En effet, sans tension et avec D_{eq} fixée, la dimension h définit totalement la forme de l'enroulement. Les poteaux qui supportent la fibre de l'intérieur sont alors placés pour être en contact avec la forme naturelle de la fibre à cet endoit. Le problème de l'optimisation de la forme repose alors sur la recherche d'un paramètre h optimal.

Compte tenu des effets de polarisation (et en supposant des coupleurs 50/50 parfaits), l'intensité à la sortie de l'interféromètre est de la forme

$$I(\Delta\phi) = E_x^2\left[1+\cos(\Delta\phi+\Delta N\phi_{tr}^x)\right] + E_y^2\left[1+\cos(\Delta\phi+\Delta N\phi_{tr}^y)\right] \qquad (2.42)$$

où x est la direction de polarisation dans l'axe d'enroulement, y est la direction de polarisation perpendiculaire, ΔN est la différence du nombre de tours enroulés des deux branches (le nombre de tours qui correspond à ΔL), et ϕ_{tr}^x et ϕ_{tr}^y sont les phases accumulées en un tour pour les polarisations x et y respectivement.

On suppose que la fibre est enroulée sans torsion ni pression latérale. De plus, ni la fibre SMF-28 ni la fibre P+ ne possèdent de biréfringence intrinsèque. Dans ce cas,

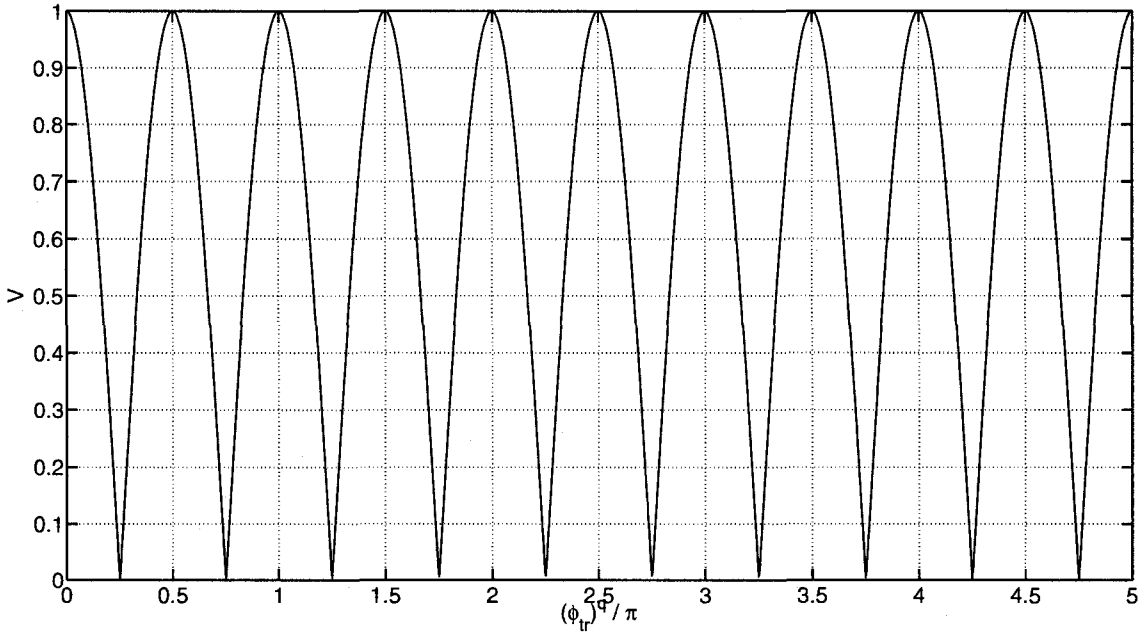


FIG. 2.4 – Visibilité de l'interféromètre enroulé en fonction de ϕ_{tr}^{xy} pour $\Delta N = 4$.

il n'y a que la biréfringence de courbure[3]. La phase accumulée sur l'axe x peut être prise comme référence. On a

$$I(\Delta\phi) = E_x^2\left[1 + \cos(\Delta\phi)\right] + E_y^2\left[1 + \cos(\Delta\phi + \Delta N\phi_{tr}^{xy})\right] \tag{2.43}$$

où $\phi_{tr}^{xy} = \phi_{tr}^{y} - \phi_{tr}^{x}$. On voit donc que l'intensité est la somme de deux interférences indépendantes, l'une pour la polarisation sur l'axe x, l'autre sur l'axe y. Immédiatement, on peut voir que pour $\Delta N\phi_{tr}^{xy} = m2\pi$ ou m est entier, ces interférences sont *en phase*, produisant une visibilité parfaite, $V = 1$. Ceci est confirmé en observant la figure 2.4 où l'on donne visibilité V en fonction ϕ_{tr}^{xy} pour $\Delta N = 4$.

L'optimisation de la visibilité requiert donc de trouver la phase relative de biréfringence $\phi_{tr}^{xy}(h)$ en fonction du paramètre h.

Pour cela, on procède comme suit.

[3]Voir l'annexe E.

1. Calcul de la forme, sans tension, de la fibre pour une valeur de h (voir la section 2.3.2.1) ;
2. Calcul du rayon de courbure $\rho(h)$ pour chaque segment dL de la fibre ;
3. Calcul de la biréfringence de courbure[4] pour chaque segment (avec ξ, la position du segment dL dans l'enroulement)

$$\beta_b(h,\xi) = C_s \frac{r^2}{2\rho(h,\xi)^2} \tag{2.44}$$

où C_s est le coefficient élasto-optique et r le rayon de la fibre ;

4. Calcul de la phase relative de biréfringence résultante pour chaque $dL(\xi)$

$$d\phi^{xy}(h,\xi) = k_0 \beta_b(h,\xi) dL(\xi) \tag{2.45}$$

5. Intégration des $d\phi^{xy}(h,\xi))$ sur un tour de l'enroulement

$$\phi_{tr}^{xy}(h) = \int_{tour} d\phi^{xy} d\xi \tag{2.46}$$

6. *Optimisation* : Recherche des h tels que $\Delta N \phi_{tr}^{xy}(h) = m2\pi$ (où m est un entier).

Le calcul de l'effet elasto-optique requiert le coefficient élasto-optique (voir l'annexe E). Les constantes utilisées pour ce calcul sont données dans le tableau 2.3 [14].

TAB. 2.3 – Constantes utilisées pour le calcul du coefficient élasto-optique C_s des fibres SMF-28 et P+.

Paramètre	**Valeur**	**Unités**
n_0	1,46	(sans unités)
p_{11}	0,113	(sans unités)
p_{12}	0,252	(sans unités)
ν_p	0,16	(sans unités)

[4]Voir l'annexe E.

2.3.2.1 Le calcul de la courbure libre de la fibre

L'optimisation de la visibilité de l'interféromètre en fonction de h requiert le calcul de la forme de l'enroulement. Comme nous cherchons la forme libre et sans tension de la fibre, on procède selon une méthode de tir tel qu'illustré à la figure 2.5. Suivant cette méthode, on fixe la tension T (toujours nulle), la force normale N et le moment de force M au point de départ de la fibre courbée, ici fixée au point de contact avec l'un des supports principaux (ref. figure 2.3). Ensuite, on cherche une forme de longueur $\pi D_{eq}/4$ dont la pointe atteint la cible, tel qu'illustré sur la figure 2.5.

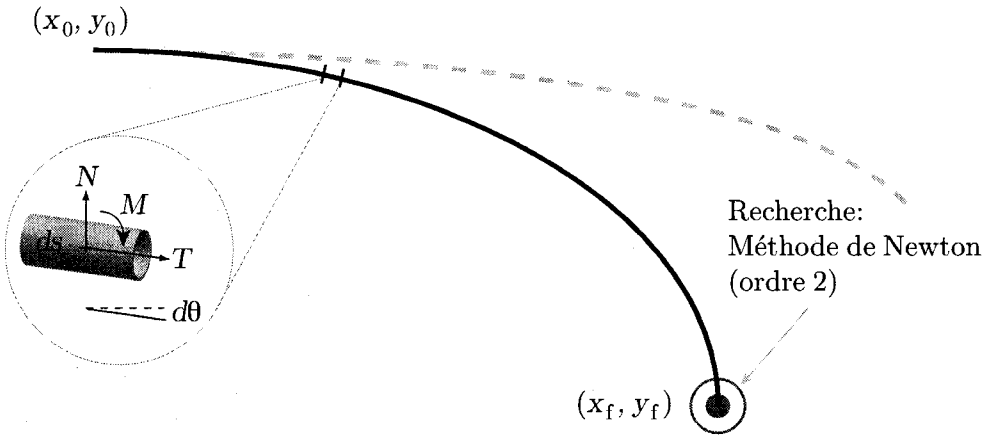


FIG. 2.5 – Recherche de la courbure libre de la fibre dans d'enroulement : Méthode de tir.

Pour ce faire, on suit la forme de la fibre courbée, segment par segment, en calculant la déviation angulaire due au moment de force

$$d\theta = \frac{M}{EI} ds \tag{2.47}$$

où E et I sont respectivement le module d'Young et le moment d'inertie de la fibre. Le moment M sur le segment suivant est alors calculé via les relations différentielles

suivantes .

$$\begin{aligned} \frac{dM}{ds} &= -N \\ \frac{dT}{d\theta} &= N \\ \frac{dN}{d\theta} &= -T \end{aligned}$$

Le résultat de ce calcul est alors soumis à une méthode de recherche de Newton (ordre 2) pour atteindre la cible (x_f, y_f).

2.3.3 Résultats et tolérances

2.3.3.1 Géométrie d'enroulement

L'algorithme d'optimisation décrit ci-haut est mis en œuvre dans la routine MATLAB écrite à cet effet : ParamInterf.m (voir l'annexe F). Celle-ci produit, en fonction d'une fréquence d'interféromètre, une dimension d'enroulement h donnant une forme optimisée pour la visibilité.

Ainsi, pour l'interféromètre opérant à 100 Mbit/sec du tableau 2.2, on obtient la forme optimale présentée à la figure 2.6. Les détails de cette solution sont présentés au tableau 2.4.

Les figures 2.7 et 2.8 illustrent le processus d'optimisation menant à l'enroulement optimal obtenu. En effet, la figure 2.7 donne la relation $\phi_{tr}^{xy}(h)$ obtenue alors que la figure 2.8 illustre l'effet de la biréfringence sur la visibilité de l'interféromètre en fonction de h. L'optimisation donne $h = 11{,}60$ cm. En faisant appel à la tolérance fixée sur V_{pol} (voir le chapitre 1), on obtient une tolérance de $\Delta h = 0{,}2$ cm. On note que ceci est facile à réaliser expérimentalement.

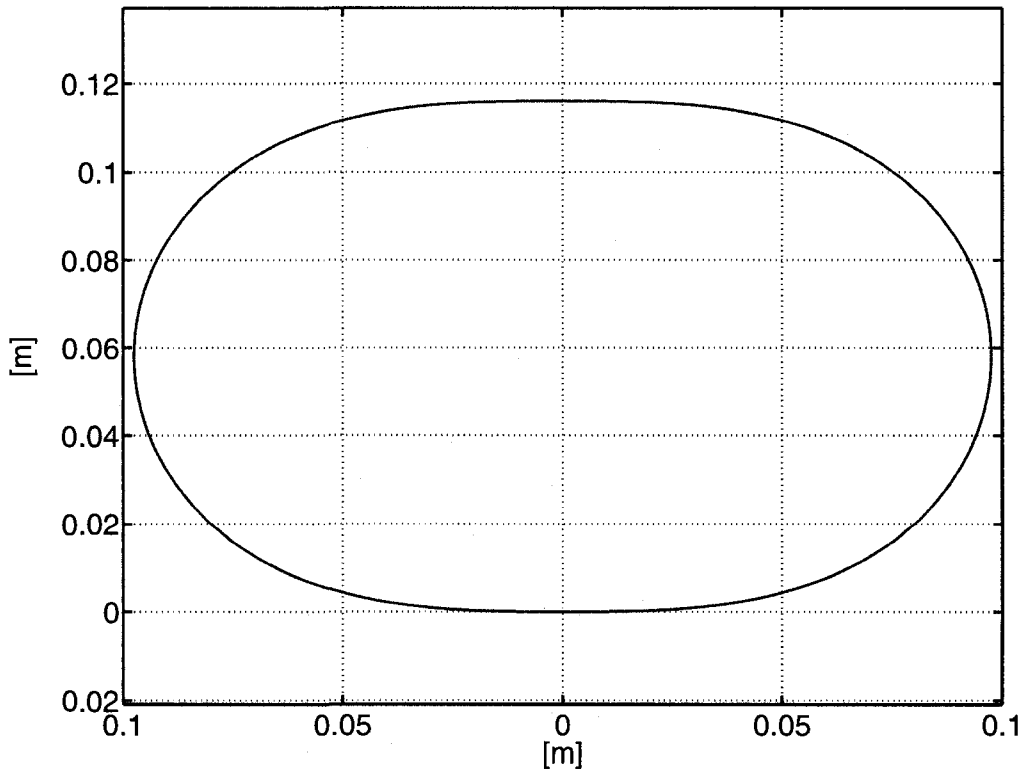


FIG. 2.6 – Géométrie d'enroulement optimale.

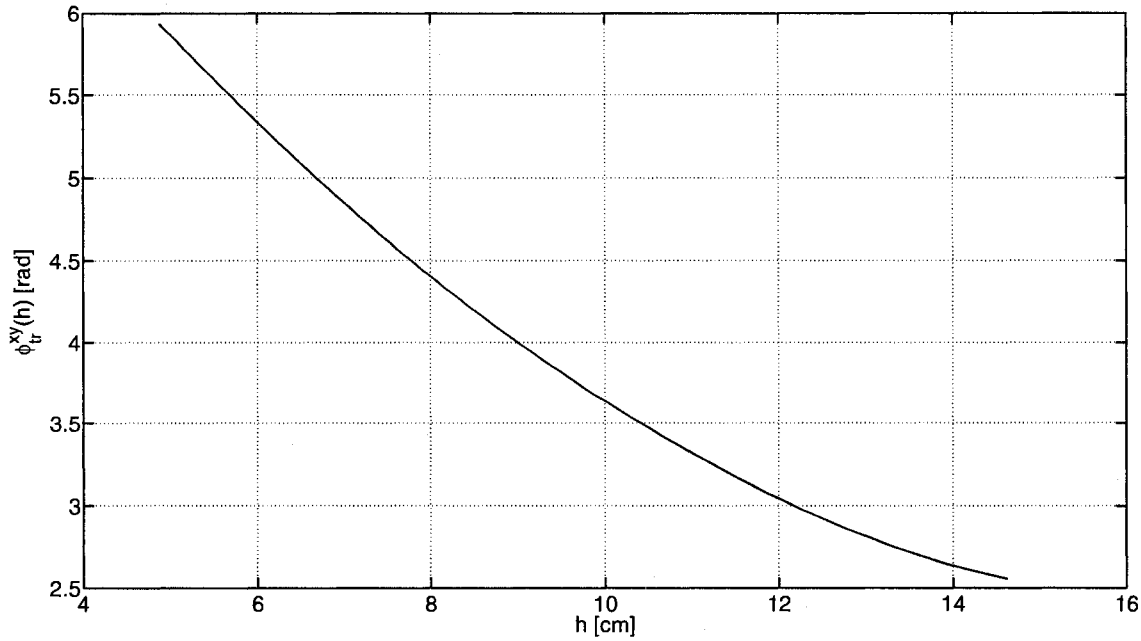


FIG. 2.7 – ϕ_{tr}^{xy} en fonction de h.

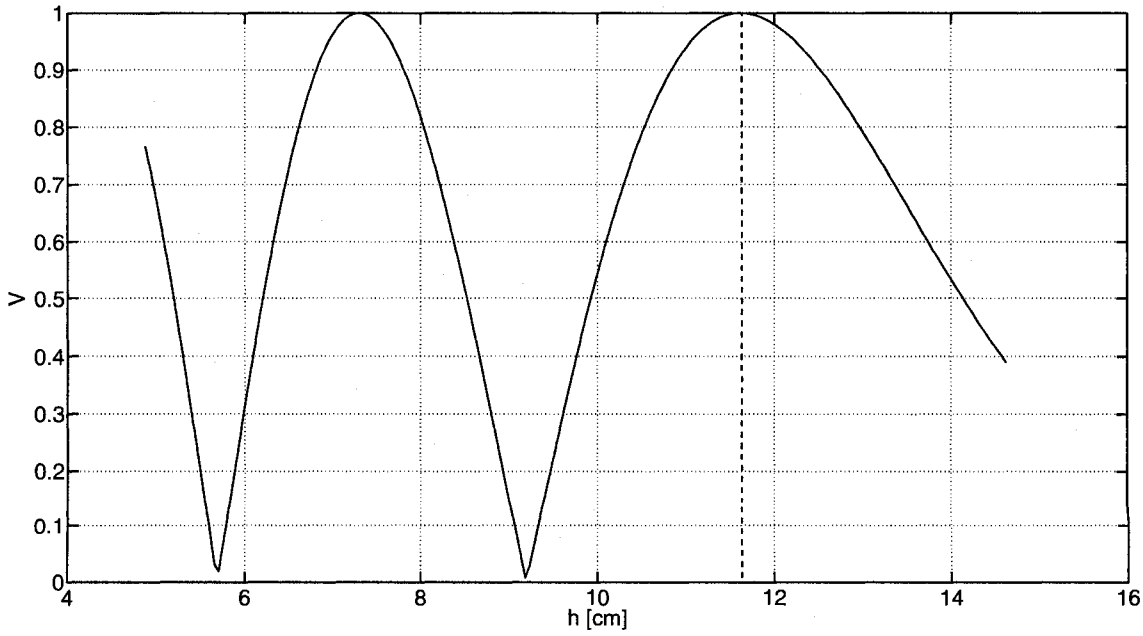


FIG. 2.8 – Optimisation de la visibilité de l'interféromètre en fonction de h.

TAB. 2.4 – Géométrie d'enroulement optimal pour l'interféromètre de 100 Mbit/s.

Paramètre	**Symbole**	**Valeur**	**Unités**
Diamètre équivalant	D_{eq}	16,249	cm
Hauteur de l'enroulement	h	11,64	cm
Largeur de l'enroulement	ℓ	19,48	cm
Nb. tours branche 1	N_1	35	n/a
Nb. tours branche 2	N_2	39	n/a
Nb. battements de biref.	n/a	2	n/a
Longueur non-enroulée totale	L_{ne}	31,05	cm

2.3.3.2 Les premiers et derniers tours

La configuration l'enroulement final, incluant les coupleurs, est illustrée sur la figure 2.9(A). On choisit de placer le premier et le dernier tour de l'enroulement sur une cercle de diamètre égal à la largeur ℓ de l'enroulement. Quatre considérations ont mené à cette configuration.

1. Les coupleurs possèdent une longueur de fibre suivant l'endroit du coupleur en tant que tel. En pratique, on doit donc considérer que l'interféromètre inclue une certaine longueur de fibre dans les branches 1 et 2 associée aux coupleurs. Afin de ne pas modifier l'effet de la compensation thermique et la fréquence de fonctionnement de l'interféromètre, ces longueurs doivent être égales dans les deux branches. Par contre, ces longueurs peuvent être différentes pour le coupleur à l'entrée et à la sortie de l'interféromètre. Ainsi, on doit avoir

$$(L_{c,E})_1 = (L_{c,E})_2 \tag{2.48}$$

$$(L_{c,S})_1 = (L_{c,S})_2 \tag{2.49}$$

mais

$$(L_{c,E})_1 \neq (L_{c,S})_1 \tag{2.50}$$

$$(L_{c,E})_2 \neq (L_{c,S})_2 \tag{2.51}$$

est acceptable. Puisque ces longueurs sont égales pour les deux branches, c.-à-d. que

$$(L_{c,E})_1 + (L_{c,S})_1 = (L_{c,E})_2 + (L_{c,S})_2, \tag{2.52}$$

les longueurs de fibre associées aux coupleurs n'ont d'effet ni sur la fréquence de fonctionnement de l'interféromètre (ΔL demeure inchangé) ni sur la *compensation thermique passive* (les longueurs égales dans les branches se compensent toujours, si elles sont de la même fibre).

2. L'enroulement prévoit qu'une partie de la longueur des branches soit non enroulée, soit une longueur (commune au deux branches de L_{ne}. Cette longueur peut également se séparer comme on le veut sur une longueur à l'entrée $L_{ne,E}$ et à la sortie $L_{ne,S}$

$$L_{ne} = L_{ne,E} + L_{ne,S} \tag{2.53}$$

3. Une épissure (fusion) joint les fibres des branches (de longueurs L_1 et L_2) et les fibres des coupleurs. En pratique, ces épissures peuvent être fragiles. On évite donc de placer ces épissures directement contre un support d'enroulement, endroit ou pourrait subvenir une brisure en cas d'application accidentelle de tension sur la fibre.

4. Comme il est possible que la *compensation thermique passive* ne soit pas parfaite dès la première fabrication, on cherche une configuration permettant d'ajuster L_1 et L_2 sans devoir défaire l'ensemble de l'enroulement. Ainsi, il est utile de biaiser notre choix de partage entre $L_{ne,E}$ et $L_{ne,S}$ en faveur d'un $L_{ne,S}$ plus long. Ceci permet d'avoir une bonne longueur, facile à ajuster, sur le tour de

sortie de l'interféromètre.

De plus, les coupleurs sont placés sur des supports aux positions montrées sur la figure 2.9(a), soit

$$L_{ne,E} + L_{c,E} = \frac{3}{8}\pi\ell \tag{2.54}$$

$$L_{ne,S} + L_{c,S} = \frac{7}{8}\pi\ell \tag{2.55}$$

$$\tag{2.56}$$

Les choix effectués pour ces paramètres sont présentés au tableau 2.5.

TAB. 2.5 – Paramètres du premier et dernier tour de l'enroulement pour l'interféromètre de 100Mbit/sec.

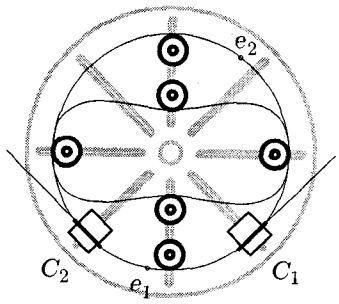
Paramètre	**Symbole**	**Valeur**	**Unités**
Longueur non enroulée à l'entrée	$L_{ne,E}$	12	cm
Longueur non enroulée à la sortie	$L_{ne,S}$	19,05	cm
Longueur des branches du coupleur d'entrée	$L_{c,E}$	10,98	cm
Longueur des branches du coupleur de sortie	$L_{c,S}$	34,57	cm

2.4 Méthode de fabrication

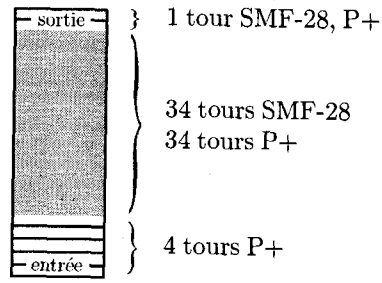
La fabrication de l'interféromètre apporte plusieurs défis. Principalement, sa fabrication nécessite la coupe des fibres qui constituent les branches avec une très grande précision (de l'ordre de 1 mm sur 20 m), tout en cherchant à produire un enroulement suivant les spécifications de la section précédente.

2.4.1 Enroulement

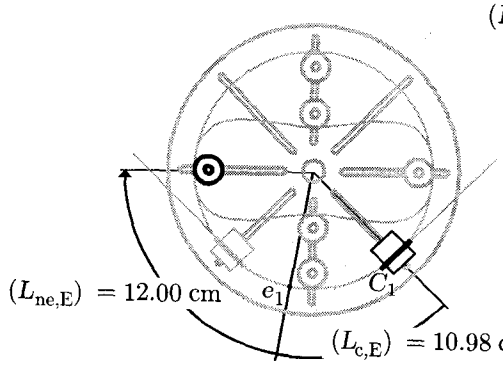
La fabrication de l'interféromètre est basée sur un enroulement de précision. De ce point de vue, la forme de la figure 2.6 pose une difficulté particulière, puisqu'il est



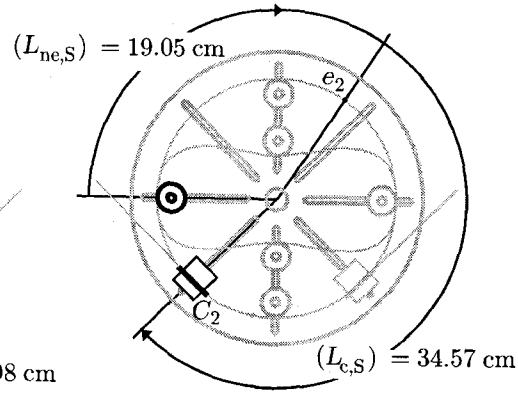
(A) L'interféromètre enroulé.



(B) Positionnement des tours sur les supports d'enroulement.



(C) Entrée de l'enroulement.



(D) Sortie de l'enroulement.

FIG. 2.9 – Détails de l'enroulement pour l'interféromètre de 100 Mbit/sec.

difficile en pratique de produire exactement cette forme au moment de l'enroulement. De plus, cette forme est conçue pour ne pas produire de tension dans la fibre, alors que l'enroulement implique une certaine application de tension. Pour résoudre ce problème, on propose d'effectuer l'enroulement et la mesure des longueurs de fibre sur un patron de supports disposés en carré (voir la figure 2.10, étape 1). Si la distance entre les supports (poteaux) d'enroulement est de x_r et que leur diamètre est de d, la longueur enroulée sur un tour est de

$$L_e(1) = 4(x_r + d) + 4\left(\frac{\pi d}{4}\right) \tag{2.57}$$

Par définition, $L_e = \pi D_{eq}$. Ainsi

$$\pi D_{eq} = 4(x_r + d) + 4\left(\frac{\pi d}{4}\right) \tag{2.58}$$

d'où

$$x_r = \frac{\pi D_{eq} - (4 + \pi)d}{4} \tag{2.59}$$

Un mandrin d'enroulement avec des supports cylindriques (poteaux filetés) a été fabriqué afin de permettre l'enroulement initial ainsi que des étapes subséquentes, tel qu'illustré sur la figure 2.10. Pour ce mandrin, le diamètre moyen de poteaux d'enroulement mesuré au moyen d'un vernier micrométrique est de $d = 3{,}180$ cm. Ainsi, on obtient, pour l'interféromètre de 100 Mbit/sec, $x_r = 7{,}084$ cm.

2.4.2 Séquence de fabrication

Suivant l'enroulement, plusieurs étapes sont nécessaires afin d'obtenir le produit final. La figure 2.10 présente les étapes de cette fabrication.

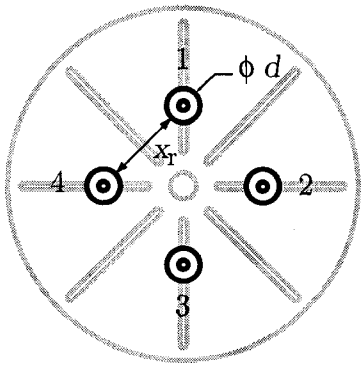
- Étape 1 : *Ajustement des supports d'enroulement.* Fixer sur le mandrin d'enroulement quattre supports (1 à 4), et à l'aide d'un vernier micrométrique, ajuster la distance entre eux à $x_r = 7{,}084$ cm.

- Étape 2 : *Enroulement et clivage.* Pour chacune de fibres constituant les deux branches, enrouler le nombre de tours prévus en s'assurant de les positionner sur les supports tel qu'illustré sur la figure 2.9b. Notez que l'enroulement doit être réalisé sans appliquer de torsion sur la fibre. Pour cela, effectuer l'enroulement avec une distance d'au moins 1 m entre le rouleau de fibre et le mandrin d'enroulement. Une fois enroulées, cliver les fibres. Pour le tour d'entrée, effectuer le clivage à $L_{ne,E} = 12$ cm par rapport au support d'entrée/sortie (cf. figure 2.9). Pour le tour de sortie, effectuer la clivage à $L_{ne,S} = 19{,}05$ cm par rapport au même support.
- Étape 3 : *Pose des coupleurs.* Premièrement, cliver les fibres des coupleurs à $L_{c,E} = 10{,}98$ cm et $L_{c,S} = 34{,}57$ cm pour le coupleur d'entrée C_1 et de sortie C_2, respectivement. Deuxièmement, effectuer l'épissure à l'aide d'une fusionneuse. S'assurer que les pertes dans les épissures estimées sont conformes aux tolérances établies au tableau 2.2. Troisièmement, à l'endroit des épissures, regainer en polymère les fibres à l'aide d'une re-gaineuse afin de les protéger adéquatement. Finalement, insérer les coupleurs dans les supports prévus à leur mise en place sur le mandrin d'enroulement.
- Étape 4 : *Installation des supports principaux.* Installer les supports $2'$ et $4'$ du côté extérieur de l'enroulement carré, contre sur les supports 2 et 4 qui sont dans l'axe ne contenant pas l'entrée et la sortie de l'enroulement.
- Étape 5 : *Ajustement du paramètre h.* Rapprocher, avec les supports 2 et 4, les supports principaux $2'$ et $4'$ vers le centre du mandrin afin obtenir la valeur h prescrite (voir le tableau 2.2). La forme de l'enroulement (figure 2.6) se mettra tout naturellement en place avec cette opération. Ensuite, éloigner les deux autres supports 1 et 3 vers l'extérieur du mandrin jusqu'à l'obtention d'un léger contact entre ceux-ci et les fibres enroulés de façon à soutenir minimalement l'enroulement[5]. Finalement, retirer les supports intérieurs 2 et 4.

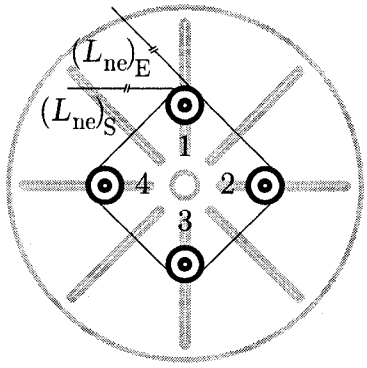
[5]De manière générale, il est important de supporter minimalement l'enroulement. Ceci évite de

– Étape 6 : *Mise en place des supports secondaires et des coupleurs.* Installer les supports 5 et 6. La distance entre eux doit être égale à celle des supports 1 et 3. Mettre en place le coupleur d'entrée C_1 sur le guide du mandrin tel qu'illustré à la figure 2.10. La fibre doit suivre une forme circulaire jusqu'au support d'entrée/sortie de sorte qu'il n'y ait pas de tension sur la fibre. Procéder de la même manière pour le coupleur C_2.

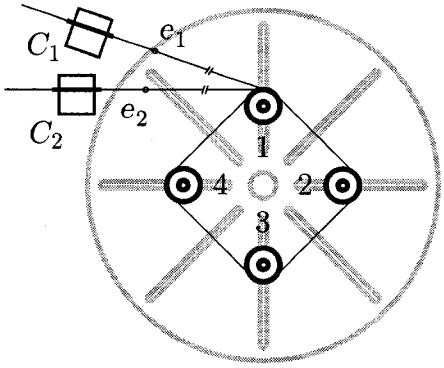
rendre l'enroulement et les longueurs des branches tributaires de l'expansion thermique du mandrin et des supports.



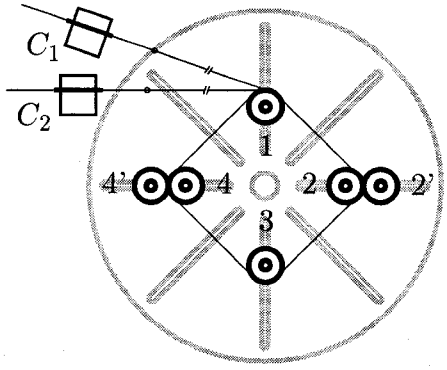
ÉTAPE 1: Ajustement des supports d'enroulement.



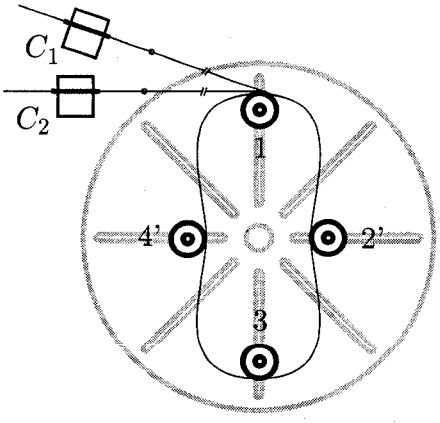
ÉTAPE 2: Enroulement et clivages.



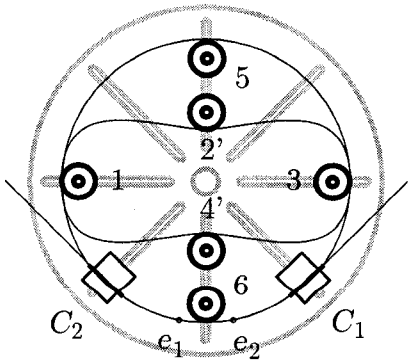
ÉTAPE 3: Pose des coupleurs.



ÉTAPE 4: Installation des supports principaux.



ÉTAPE 5: Ajustement du paramètre h.



ÉTAPE 6: Mise en place des supports secondaires et des coupleurs.

FIG. 2.10 – Étapes de fabrication de l'interféromètre.

Chapitre 3

Méthode de caractérisation

L'interféromètre de 100 Mbit/sec conçu et fabriqué selon les prescriptions du chapitre 2 doit, bien sûr, être testé afin de caractériser son comportement en température et en polarisation. Les méthodes retenues, et le montage expérimental réalisé font l'objet de ce chapitre.

3.1 Objectifs et problématique

La méthode de caractérisation de l'interféromètre a pour objectif principal de déterminer la variation dans le délai de l'interféromètre en fonction de la température. Un second objectif est de rendre la méthode capable de mesurer la sensibilité en polarisation de l'interféromètre.

Deux méthodes viennent immédiatement à l'esprit :

- Méthode 1 : Mesurer directement (à une longueur d'onde donnée) l'intensité sur les deux branches de sortie de l'interféromètre en fonction de la température ;
- Méthode 2 : Mesurer la translation du spectre en longueur d'onde en fonction de la température.

Ces deux méthodes sont séduisantes puisqu'elles ne requièrent qu'un minimum d'équipement. La méthode 1 ne requiert que deux détecteurs et un laser alors que la méthode

2 ne requiert qu'une source large bande et un analyseur de spectre optique.

La méthode 1 permettrait de réaliser une caractérisation au moyen de la réponse de l'interféromètre aux changements de différence de chemin optique entre les deux branches en fonction des changements de température

$$I_1(t) = \frac{I_0}{2}\{1 + V\cos[\Delta\phi(T)]\} \tag{3.1}$$

$$I_2(t) = \frac{I_0}{2}\{1 - V\cos[\Delta\phi(T)]\} \tag{3.2}$$

Or, les équations 3.1 et 3.2 montrent que cette méthode ne permet pas de déterminer le sens de la variation de la phase. En effet, la variation étant cosinusoïdale, l'accès à $\Delta\phi(T)$ comporte une incertitude sur le signe de la variation. Ainsi, cette méthode ne permet pas de distinguer un interféromètre sur-compensé d'un interféromètre sous-compensé. Pour cette raison, cette méthode doit être écartée.

La méthode 2, en principe, permet de remédier à ce problème. La position des minima sur la courbe spectrale de l'interféromètre varie avec la différence de chemin optique

$$\lambda_{min} \propto \Delta \mathrm{L}_{opt}(T) \tag{3.3}$$

Cependant, la période spectrale varie également avec l'inverse de la différence de phase

$$\Lambda = \frac{\lambda^2}{n_g \Delta L(T)} \tag{3.4}$$

où $n_g = n - \lambda\frac{dn}{d\lambda}$ est l'indice de groupe du monde fondamental. Ainsi, pour λ proche de 1,55 μm et pour ΔL_{opt} de l'ordre de 1,46 $\times 2$ m, on a Λ de l'ordre de 0,8 picomètres. Or, les analyseurs de spectre optique possèdent généralement une résolution maximale de l'ordre de quelques dizaines de pm. Donc, la technologie des analyseurs de spectre empêche l'observation de la structure spectrale de l'interféromètre, ce qui oblige l'élimination de la méthode.

Nous sommes donc contraints de chercher une autre méthode de caractérisation

adéquate.

3.2 La caractérisation par modulation de phase

L'idée ici est d'utiliser un signal modulé en phase avant l'entrée dans l'interféromètre pour le caractériser. Cette idée vient du fait qu'une petite modulation de phase peut sonder localement la pente de la fonction de transfert $I(\Delta\phi)$ de l'interféromètre. Nous verrons que cette méthode permet de déterminer à la fois l'importance et le sens de la variation du délai de l'interféromètre. La modulation de phase est un processus par lequel un délai proportionnel à la valeur instantanée d'un signal de modulation est appliqué sur une porteuse, ici optique

$$\cos(\phi) \longrightarrow \cos(\phi + f(t)) \tag{3.5}$$

3.2.1 La réponse de l'interféromètre à un signal modulé en phase

Nous dérivons ici la réponse de l'interféromètre à une porteuse modulée en phase par un signal sinusïdal. Nous suivons ici une démarche en partie inspirée de la référence [15] et est cohérente avec la référence [16].

L'onde électromagnétique d'un laser peut être décrite au moyen de son champ électrique

$$\mathbf{E}(t) = \mathbf{E_0} \cos\left[\omega_0 t + \phi_0 + f(t)\right] \tag{3.6}$$

Si le signal de modulation $f(t)$ est de type sinusoïdal, le champ électrique peut s'écrire

$$\mathbf{E}(t) = \mathbf{E_0} \cos\left[\omega_0 t + \phi_0 + \frac{\Delta\bar{\phi}}{2} \cos\left(\omega_m t + \phi_m\right)\right] \tag{3.7}$$

$$= \mathbf{E_0} \cos\left[\phi_1(t)\right] \tag{3.8}$$

où $\Delta\bar{\phi}$, ω_m et ϕ_m sont respectivement l'amplitude crête à crête, la pulsation et la

phase initiale du signal de modulation. Pour simplifier, nous poursuivons en prenant $\phi_m = 0$, ce qui équivaut à dire que la modulation et la porteuse sont parfaitement en phase. Après passage dans l'interféromètre, l'onde ayant passé dans la branche longue, par rapport à l'onde ayant passé par la branche courte, a subi le délai de l'interféromètre, τ

$$\begin{aligned} \mathbf{E}(t) &= \mathbf{E_0} \cos\left[\omega_0(t-\tau) + \phi_0 + \frac{\Delta\bar{\phi}}{2}\cos\left(\omega_m(t-\tau)\right)\right] && (3.9) \\ &= \mathbf{E_0}\cos\left(\phi_2(t)\right) && (3.10) \end{aligned}$$

Donc, la différence de phase des porteuses dans chaque branche de l'interféromètre est

$$\begin{aligned} \Delta\phi(t) &= \phi_1(t) - \phi_2(t) && (3.11) \\ &= \frac{\Delta\bar{\phi}}{2}\left\{\cos\left[\omega_m t\right] - \cos\left[\omega_m(t-\tau)\right]\right\} + \omega_0\tau && (3.12) \end{aligned}$$

En utilisant l'identité suivante,

$$\cos x - \cos y = -2\sin\left(\frac{x+y}{2}\right)\sin\left(\frac{x-y}{2}\right) \qquad (3.13)$$

$\Delta\phi(t)$ se réécrit

$$\Delta\phi(t) = \Delta\bar{\phi}\sin\left(\frac{\omega_m\tau}{2}\right)\sin\left[\omega_m\left(t-\frac{\tau}{2}\right)\right] + \omega_0\tau \qquad (3.14)$$

En pratique, comme le délai τ est de l'ordre de 10 ns et que la fréquence de modulation est de l'ordre de quelques kHz, on a $\omega_m\tau \ll 1$. Ainsi, on obtient

$$\Delta\phi(t) = \frac{\Delta\bar{\phi}\omega_m\tau}{2}\sin\left(\omega_m t\right) + \omega_0\tau \qquad (3.15)$$

L'intensité à la sortie de l'interféromètre, pour une branche, est donnée par

$$\begin{aligned} I(\tau,t) &= \frac{I_0}{2}\left[1+V\cos\Delta\bar{\phi}(t)\right] \\ &= \frac{I_0}{2}\left\{1+V\cos\left[\frac{\Delta\bar{\phi}\omega_m\tau}{2}\sin\left(\omega_m t\right)+\omega_0\tau\right]\right\} \end{aligned} \tag{3.16}$$

Cette expression représente la réponse d'un interféromètre à un signal modulé en phase. Cependant, il est utile de poursuivre le calcul plus loin dans le but d'obtenir la décomposition de ce signal en série de Fourier.

D'abord, $I(\tau,t)$ peut être reformulé de la manière suivante

$$\begin{aligned} I(\tau,t) = \frac{I_0}{2}\Bigg\{1 \;+\; V\Bigg[&\underbrace{\cos\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\sin(\omega_m t)\right)}_{A(\tau,t)}\cos\omega_0\tau \\ &- \underbrace{\sin\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\sin\omega_m t\right)}_{B(\tau,t)}\sin(\omega_0\tau)\Bigg]\Bigg\} \\ = I_0\{1 \;+\; V\left[A(\tau,t)\cos(\omega_0\tau) - B(\tau,t)\sin(\omega_0\tau)\right]\} \end{aligned} \tag{3.17}$$

Écrivons $A(\tau,t)$ en série de Fourier, d'abord en trouvant a_0

$$a_0 = \frac{\omega_m}{\pi}\int_{-\pi/\omega_m}^{\pi/\omega_m}\cos\left[\frac{\Delta\bar{\phi}\omega_m\tau}{2}\sin(\omega_m t)\right]\mathrm{d}t \tag{3.18}$$

$$\overset{pair}{=} \frac{2\omega_m}{\pi}\int_{0}^{\pi/\omega_m}\cos\left[\frac{\Delta\bar{\phi}\omega_m\tau}{2}\sin(\omega_m t)\right]\mathrm{d}t \tag{3.19}$$

$$\tag{3.20}$$

Posons $z = \Delta\bar{\phi}\omega_m\tau/2$ et $\theta = \omega_m t$. On obtient

$$a_0 = \frac{2}{\pi}\int_0^{\pi}\cos\left[z\sin\theta\right]\mathrm{d}\theta \tag{3.21}$$

En utilisant la définition de la fonction de Bessel de première espèce

$$J_n(z) \equiv \frac{1}{\pi}\int_0^{\pi} \cos\left(z\sin\theta - n\theta\right) \mathrm{d}\theta \tag{3.22}$$

on voit que

$$a_0 = 2J_0\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right) \tag{3.23}$$

Similairement, trouvons les a_n

$$\begin{aligned} a_n &= \frac{\omega_m}{\pi}\int_{-\pi/\omega_m}^{\pi/\omega_m} \cos\left[\frac{\Delta\bar{\phi}\omega_m\tau}{2}\sin\omega_m t\right]\cos\omega_m t \mathrm{d}t & (3.24)\\ &\overset{pair}{=} \frac{1}{\pi}\int_0^{\theta}\cos\left[z\sin\theta + n\theta\right]\mathrm{d}\theta + \frac{1}{\pi}\int_0^{\theta}\cos\left[z\sin\theta - n\theta\right]\mathrm{d}\theta & (3.25)\\ &= J_{-n}(z) + J_n(z) & (3.26)\end{aligned}$$

Or, $J_{-n}(z) = -J_n(z)$ pour un ordre n impair et $J_{-n}(z) = J_n(z)$ pour un ordre n pair. Ainsi, on obtient

$$a_n = \begin{cases} 0 & : \quad n \quad \text{impair} \\ 2J_n(z) & : \quad n \quad \text{pair} \end{cases} \tag{3.27}$$

Pour les b_n, on procède de façon parallèle

$$\begin{aligned} b_n &= \frac{\omega_m}{\pi}\int_{-\pi/\omega_m}^{\pi/\omega_m}\cos\left[\frac{\Delta\bar{\phi}\omega_m\tau}{2}\sin(\omega_m t)\right]\sin(\omega_m t)\mathrm{d}t & (3.28)\\ &\overset{impair}{=} 0 & (3.29)\end{aligned}$$

Donc, $A(\tau, t)$, sous forme de série de Fourier, peut s'écrire

$$A(\tau,t) = 2J_0\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right) + \sum_{n\ pair} 2J_n\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\cos(n\omega_m t) \tag{3.30}$$

Par un calcul en tout point similaire, on peut obtenir

$$B(\tau,t) = \sum_{n\ impair} 2J_n\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\sin(n\omega_m t) \tag{3.31}$$

Donc, l'expression de l'intensité du champ à la sortie de l'interféromètre est

$$I(\tau,t) = I_0\left\{1+2V\left[\left(J_0\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)+\sum_{n\ pair} J_n\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\cos n\omega_m t\right)\cos\omega_0\tau - \left(\sum_{n\ impair} J_n\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\sin n\omega_m t\right)\sin\omega_0\tau\right]\right\} \tag{3.32}$$

Sous cette forme, on voit clairement que dans le domaine spectral, l'intensité est donnée par une série d'harmoniques de la fréquence de modulation ω_m. L'amplitude de ces harmoniques est donnée par une fonction de Bessel d'ordre égal à l'ordre de l'harmonique et dont l'argument est variable avec l'amplitude du signal de modulation, et du délai. Le déphasage entre deux harmoniques successifs est précisément de $\pi/2$.

On peut aussi remarquer que chaque terme de la série de Fourier contient l'information qui est recherchée, soit la modulation du délai de l'interféromètre. Ainsi, il est plus simple d'isoler l'amplitude d'une des fréquences de la série pour observer cet effet. Par exemple, on peut isoler l'amplitude de la première et de la deuxième harmonique ($n = \{1,2\}$)

$$|I_{n=1}(\tau,t)| = I_{n=1}(\tau) = 2I_0VJ_1\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\sin\omega_0\tau \tag{3.33}$$

$$|I_{n=2}(\tau,t)| = I_{n=2}(\tau) = 2I_0VJ_2\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\cos\omega_0\tau \tag{3.34}$$

Dans le cas ou $\omega_m \sim 50\times10^3$ Hz, $\Delta\bar{\phi}\sim\pi$ et $\tau\sim 1$ ns, l'argument de la fonction de Bessel est de l'ordre de 10^{-5}. De plus, les variations attendues de τ sont de l'ordre de 10 fs pour 1°C ce qui produit une variation de l'argument de la fonction de Bessel

de l'ordre de 10^{-9}. Pour quantifier l'effet de la variation du délai de l'interféromètre sur la valeur des fonctions de Bessel, il est utile d'utiliser le développement de Taylor. Pour $\epsilon \ll 1$, on a

$$J_1(z+\epsilon) \simeq \frac{z+\epsilon}{2} \tag{3.35}$$

$$J_2(z+\epsilon) \simeq \frac{(z+\epsilon)^2}{8} \tag{3.36}$$

Ainsi, en fonction de ϵ, les variations relatives des fonctions de Bessel sont données par

$$\frac{J_1(z+\epsilon)}{J_1(z)} \simeq \frac{\epsilon}{z} \tag{3.37}$$

$$\frac{J_2(z+\epsilon)}{J_2(z)} \simeq \frac{\epsilon}{4z} \tag{3.38}$$

ce qui donne, pour $z = 10^{-5}$ et $\epsilon = 10^{-9}$

$$\frac{J_1(10^{-5}+10^{-9})}{J_1(10^{-5})} \simeq 10^{-4} \tag{3.39}$$

$$\frac{J_2(10^{-5}+10^{-9})}{J_2(10^{-5})} \simeq 10^{-5} \tag{3.40}$$

Ainsi, les fonctions de Bessel sont approximativement invariables. Pour clarifier ce point dans la notation, on pose $J_1\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right) = \gamma_1$ et $J_2\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right) = \gamma_2$

$$I_{n=1}(\tau) \simeq I_0 V \gamma_1 \sin(\omega_0\tau) \tag{3.41}$$

$$I_{n=2}(\tau) \simeq I_0 V \gamma_2 \cos(\omega_0\tau) \tag{3.42}$$

Cependant, puisque ω_0 est de l'ordre de $10^{14}\mathrm{s}^{-1}$, les termes sinusoïdaux sont fortement variables avec les variations du délai de l'interféromètre.

On voit donc que $I_{n=1}(\tau)$ et $I_{n=2}(\tau)$ peuvent être utilisés comme *signaux de caractérisation* de l'interféromètre. Ces deux quantités étant en quadrature, l'évolution

de l'une par rapport à l'autre permet de distinguer le signe de la variation du délai.

3.2.1.1 Obtention de la sensibilité en température

Le délai de l'interféromètre est relié à sa différence de phase

$$\tau = \Delta\phi/\omega_0 \tag{3.43}$$

Ainsi, en introduisant la sensibilité en température s_T tel que définie par l'équation 2.32, on a

$$\tau(T) = \tau_0 + k\frac{s_T}{\omega_0}\Delta T \tag{3.44}$$

donc,

$$\begin{aligned} \frac{d\Delta\phi}{dT} &= \omega_0 \frac{d}{dT}\left[\tau_0 + k\frac{s_T}{\omega_0}\Delta T\right] && (3.45)\\ &= k s_T && (3.46) \end{aligned}$$

Le signal de caractérisation donne accès à la sensibilité en température s_T via la fréquence observée de la caractéristique $I_{n=1}(\tau)$ et $I_{n=2}(\tau)$ vs. T. En effet, en définissant ω_T, la "fréquence en température" des signaux de caractérisation, on a que

$$\begin{aligned} \frac{d\Delta\phi}{dT} &= \frac{d}{dT}\left[\omega_T T + \text{const.}\right] && (3.47)\\ &= \omega_T && (3.48) \end{aligned}$$

Donc, on a

$$s_T = \frac{\omega_T}{k} \tag{3.49}$$

3.2.2 Caractérisation en polarisation

Par son design, l'interféromètre doit avoir un comportement en polarisation variable suivant le paramètre d'enroulement h. On propose donc une méthode de car-

actérisation en polarisation en fonction de h qui utilise également la méthode de la modulation de phase.

Plus l'interféromètre est sensible à la polarisation, plus l'effet de la polarisation est grand sur la sa visibilité V. Ainsi, la méthode consiste à injecter dans l'interféromètre des états de polarisation aléatoires et de constater, pour une température fixe, la variabilité dans la puissance de sortie sur une des branches de l'interféromètre. On effectue cela pour plusieurs valeurs du paramètre h. La puissance peut être prise comme proportionnelle à $I_{n=1}$ ou $I_{n=2}$, ces deux quantités étant proportionnelles à V.

On s'attend à ce que la variabilité (mesurée par l'écart type σ) suive une forme inverse à la courbe présentée à la figure 2.8.

En référence à l'équation 2.43, faire varier aléatoirement l'état de polarisation à l'entrée de l'interféromètre revient à faire varier aléatoirement les grandeurs relatives des variables E_x^2 et E_y^2. Notons que la phase relative initiale entre E_x et E_y n'a aucun impact sur la visibilité de l'interféromètre. Ensuite, on mesure l'écart type σ sur $I_{n=1}$ ou $I_{n=2}$ obtenu en fonction du paramètre d'enroulement h. Le résultat simulé attendu est présenté à la figure 3.1. On note que les minima sur cette courbe correspondent au maxima de la courbe de visibilité en fonction de h, soit la courbe illustrée à la figure 2.8. De plus, cette courbe a été normalisée avec l'écart type maximal attendu, de sorte que $\sigma_{pol}|_{max} = 1$.

3.3 Réalisation expérimentale

Un montage a été assemblé pour réaliser la méthode présentée à la section précédente. Ce montage permet de produire le signal modulé en phase que nous appellerons *signal sonde*, de produire de manière contrôlée des variations dans la température de l'interféromètre ainsi que d'acquérir les signaux d'intérêt. Le montage est entièrement pris en charge par un PC équipé d'un logiciel *Labview* qui gère la séquence expérimentale et qui acquiert et mémorise les données du test.

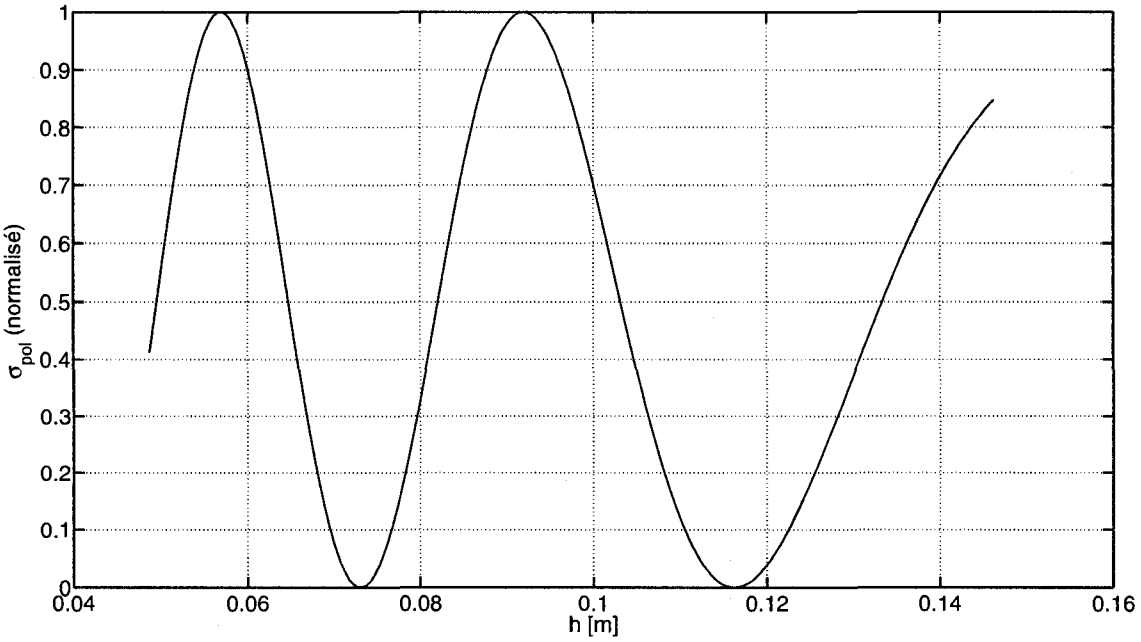


FIG. 3.1 – Écart type σ_{pol} normalisé attendu dans la réponse de l'interféromètre face à des états de polarisation aléatoires.

Les paragraphes suivants décrivent le montage et ses différents éléments pour en venir à spécifier les performances du montage.

3.3.1 Description du montage

Le montage est divisé en quatre sous-systèmes, soit un système optique, électrique, thermique et informatique. L'ensemble est schématisé sur la figure 3.2. Le système optique comporte la source laser, un contrôleur de polarisation, l'interféromètre lui-même, un détecteur, et des fibres optiques de connexion. Le système électrique regroupe un module de détection synchrone et un thermomètre numérique de type RTD de haute précision. Le système thermique est composé d'un refroidisseur à eau, d'un bain thermique et d'un échangeur de chaleur. Finalement, un système informatique, composé d'un PC et d'un logiciel *Labview* est relié électriquement à l'amplificateur, le refroidisseur à eau et le thermomètre RTD.

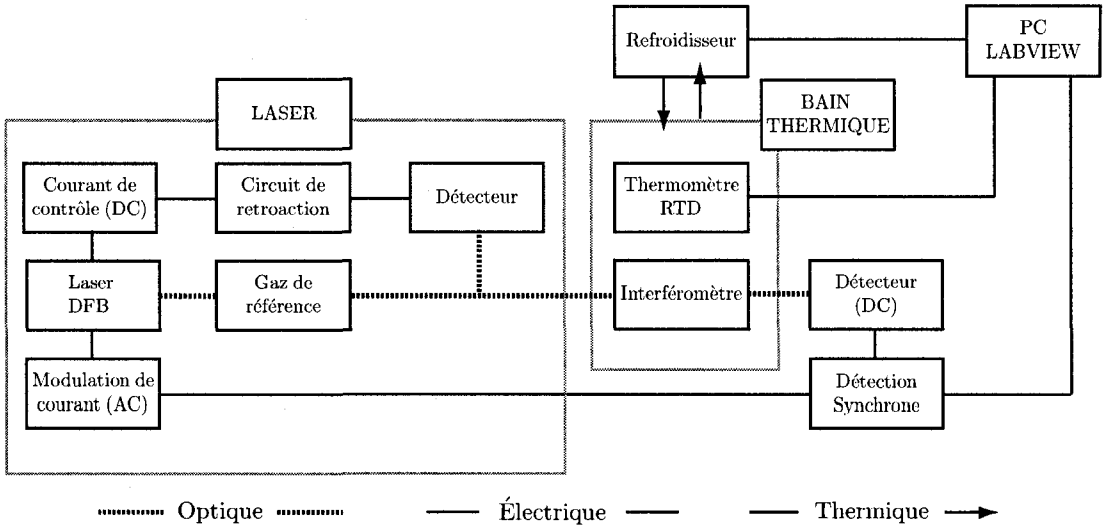


FIG. 3.2 – Montage expérimental.

Le montage est conçu de manière à permettre la caractérisation d'interféromètres jusqu'à 2 m de différence de chemin optique. Cette donnée constitue la principale contrainte sur les sous-systèmes du montage.

3.3.2 La source laser

La source laser sert de source de puissance optique pour le montage. Pour servir dans le montage, ce laser doit être

1. très étroit en longueur d'onde (par rapport à la structure du spectre de l'interféromètre)
2. très stable en longueur d'onde.

La première contrainte est reliée au fait que le laser doit permettre de bien discriminer en longueur d'onde. La deuxième contrainte traduit le fait que le laser doit être une source de variabilité négligeable devant les variations dans les caractéristiques de l'interféromètre à tester.

En supposant le délai τ fixé, on peut quantifier le premier critère, en limitant la largeur en longueur d'onde, à 5 % de l'écart entre deux franges de l'interféromètre, soit 0,8 pm pour un interféromètre 100 Mbit/sec à $\lambda = 1550$ nm

$$\begin{aligned} \Delta\lambda_{laser} &\leq 0{,}8 \text{ pm} \times 0,05 \\ &\leq 0{,}04 \text{ pm} \end{aligned}$$

Le second critère se quantifie en considérant un délai τ constant, et en limitant le changement de phase entre les extrémités dans la bande où varie la longueur d'onde, à 5 % de 2π. Ainsi, en fréquence

$$\Delta\omega_0\tau \leq 2\pi \times \frac{1}{2} \times 0{,}05 \sim 0{,}15 \text{ rad} \tag{3.50}$$

Avec $\tau \sim 10$ ns, on trouve

$$\Delta\omega_0 \leq 10^9 \text{ s}^{-1} \tag{3.51}$$

Pour $\lambda = 1550$ nm, ceci donne

$$\Delta\lambda_0 \leq 0{,}02 \text{ pm} \tag{3.52}$$

Dans le but de satisfaire ces spécifications, particulièrement la spécification de stabilité en fréquence, nous avons utilisé un laser spécial qui est asservi sur une raie d'émission d'un gaz. La raie d'émission du gaz étant extrêmement stable, une boucle de rétroaction utilise cette raie comme référence pour contrôler la longueur d'onde d'émission d'un laser DFB.

Ce laser possède également d'autres avantages. La rétroaction en longueur d'onde fonctionne en modulant légèrement la fréquence du laser autour d'une valeur fixe (modulation de quelques kHz sur une fréquence optique de l'ordre de 200 THz) et en mesurant le retard de phase de la modulation après que le rayon laser ait été filtré par le gaz de référence. Comme pour un filtre basse-bande électrique, le retard de

phase de la modulation est nulle si la longueur d'onde du laser est centrée sur la raie d'émission du gaz.

Ainsi, en plus de stabiliser la longueur d'onde d'émission du laser, cela signifie que *le laser est modulé en fréquence.* Cette modulation, sinusoïdale, est formellement équivalente à une modulation de phase, de la forme voulue. On a

$$\nu(t) = \nu_0 - \Delta\nu \sin(\omega_m t + \phi_m) \tag{3.53}$$

Puisque $2\pi\nu = d\Phi/dt$, on intègre pour obtenir la phase

$$\Phi(t) = 2\pi \left[\nu_0 t + \frac{\Delta\nu}{\omega_m} \cos(\omega_m t + \phi_m)\right] + \phi_0 \tag{3.54}$$

ce qui est équivalent à la modulation de phase supposée dans l'équation 3.9 avec $\frac{\Delta\bar{\phi}}{2} = \frac{2\pi\Delta\nu}{\omega_m}$. Ainsi, il n'est pas nécessaire d'inclure un modulateur de phase proprement dit dans le montage : *le laser construit de manière inhérente et rigoureuse le signal sonde.*

3.3.3 Le module de détection synchrone

Le module de détection synchrone est un dispositif de filtrage électronique qui agit comme un filtre passe-bande analogique ajustable de haute qualité, centré sur la fréquence d'un signal de référence.

Ce dispositif a donc deux entrées : (1) le signal à filtrer et (2) le signal de référence, tel qu'illustré à la figure 3.3. Le signal de référence est utilisé pour fixer la fréquence et la phase d'un oscillateur interne de haute qualité. La fréquence est déterminée par comparaison du signal avec un seuil de 1 V. Celle-ci peut être fixée égale à celle du signal de référence ($1f$) ou à son double ($2f$) . Le signal de l'oscillateur interne et le signal de référence sont comparés via un *phase-lock loop* (PLL) qui produit une synchronisation entre les deux signaux (ou un déphasage fixe). Cette façon de fonctionner permet au signal de référence d'avoir n'importe quelle forme, pourvue

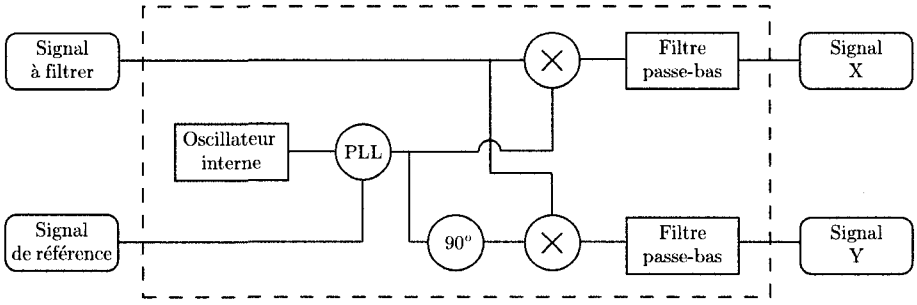


FIG. 3.3 – Fonctionnement général du module de détection synchrone

qu'elle soit périodique, de période et de phase constante. Pour le reste du circuit du module de détection synchrone, c'est le signal de l'oscillateur interne qui est utilisée pour faire le traitement du signal.

Le filtrage est réalisé en multipliant le signal à filtrer par le signal de l'oscillateur interne et en passant le résultat dans un filtre passe-bas. Ceci est fait avec le signal de référence et avec ce même signal, déphasé de 90°. Ainsi, on obtient deux signaux de sortie, identifiés par X et Y, qui peuvent être considérés comme étant la projection sur $\cos(\omega_r t)$ et $\sin(\omega_r t)$ respectivement (où ω_r est la pulsation du signal de référence).

On obtient donc non seulement l'équivalent d'un filtrage passe-bande, mais aussi une indication sur l'évolution de la phase entre le signal à filtrer et le signal de référence. On peut aussi séparer l'effet de la phase et de l'amplitude du signal filtré en prenant la somme rectifiée de X et Y : $R = \sqrt{X^2 + Y^2}$ et en prenant la tangente inverse du quotient de X et Y : $\phi = \tan^{-1} Y/X$

Dans le cas du signal recueilli à la sortie de l'interféromètre excité par le *signal sonde* $I(\tau, t)$ tel que donné par l'équation 3.32, on peut trouver la forme attendue pour les signaux X et Y. On écrira les signaux de l'oscillateur interne comme suit

$$V_X^{int} = \cos(\omega_{int} t + \phi_{int}) \tag{3.55}$$

$$V_Y^{int} = \sin(\omega_{int} t + \phi_{int}) \tag{3.56}$$

En se référant à la figure 3.2, on voit que le générateur de fonctions est connecté au modulateur de phase et au module de détection synchrone. On réalise ce branchement pour utiliser le *signal de modulation* comme signal de référence pour le module de détection synchrone. Donc, si la fréquence de modulation est de ω_m, on aura

$$\omega_{int} = \omega_m \tag{3.57}$$

sous l'action du PLL.

Via le détecteur branché sur le port d'entrée du module de détection synchrone (*signal à filtrer*), pour le canal de sortie X, l'appareil réalise une multiplication par V_X^{int} pour donner $V_X^{\times}$

$$V_X^{\times} = I_0 \left\{ 1 + V \left[\left(2J_0 \left(\frac{\Delta\bar{\phi}\omega_m\tau}{2} \right) + \sum_{n\ pair} J_n \left(\frac{\Delta\bar{\phi}\omega_m\tau}{2} \right) \cos n\omega_m t \right) \cos\omega_0\tau \right. \right.$$
$$\left. \left. + \left(\sum_{n\ impair} J_n \left(\frac{\Delta\bar{\phi}\omega_m\tau}{2} \right) \sin n\omega_m t \right) \sin\omega_0\tau \right] \right\} \times \cos(\omega_m t + \phi_{int})$$

En distribuant la multiplication par $\cos(\omega_m t + \phi_{int})$, il vient

$$\begin{aligned} V_X^{\times} &= I_0 \cos(\omega_m t + \phi_{int}) \\ &+ 2I_0 V \cos(\omega_m t + \phi_{int}) J_0 \left(\frac{\Delta\bar{\phi}\omega_m\tau}{2} \right) \\ &+ I_0 V \cos\omega_0\tau \sum_{n\ pair} J_n \left(\frac{\Delta\bar{\phi}\omega_m\tau}{2} \right) \cos n\omega_m t \cos(\omega_m t + \phi_{int}) \\ &+ I_0 V \sin\omega_0\tau \sum_{n\ impair} J_n \left(\frac{\Delta\bar{\phi}\omega_m\tau}{2} \right) \sin n\omega_m t \cos(\omega_m t + \phi_{int}) \end{aligned}$$

On utilise alors les identités trigonométriques suivantes

$$\begin{aligned} \cos s \cos t &= \frac{\cos(s+t) + \cos(s-t)}{2} \\ \sin s \cos t &= \frac{\sin(s+t) + \sin(s-t)}{2} \end{aligned}$$

et on trouve

$$\begin{aligned} V_X^{\times} &= I_0 \cos(\omega_m t + \phi_{int}) \\ &+ 2I_0 V \cos(\omega_m t + \phi_{int}) J_0\left(\frac{\Delta\bar{\phi}\omega_m \tau}{2}\right) \\ &+ \frac{I_0 V}{2} \cos\omega_0\tau \sum_{n\ pair} J_n\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\{\cos((n+1)\omega_m t + \phi_{int}) + \cos((n-1)\omega_m t - \phi_{int})\} \\ &+ \frac{I_0 V}{2} \sin\omega_0\tau \sum_{n\ impair} J_n\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\{\sin((n+1)\omega_m t + \phi_{int}) + \sin((n-1)\omega_m t - \phi_{int})\} \end{aligned}$$

Le module de détection synchrone appliquera alors un filtre passe-bas sur $V_X^{\times}$ qui filtre tout sauf le niveau DC. Dans l'équation ci-haut, on peut remarquer que seul le terme avec $n = 1$ fera une contribution de fréquence nulle. Tout les autres termes ont une fréquence multiple de ω_m. Donc, le signal de sortie X est donné par

$$X_{\omega_m} = -\frac{I_0 V}{2} \sin(\omega_0\tau)\, J_1\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right) \sin(\phi_{int}) \tag{3.58}$$

De façon similaire on a

$$Y_{\omega_m} = \frac{I_0 V}{2} \sin(\omega_0\tau)\, J_1\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right) \cos(\phi_{int}) \tag{3.59}$$

Si l'on calcule $R = \sqrt{X^2 + Y^2}$, on trouve

$$R_{\omega_m} = \frac{I_0 V}{2} \left|\sin(\omega_0\tau)\, J_1\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\right| \tag{3.60}$$

Ainsi, les signaux X_{ω_m} et Y_{ω_m} sont en tout point semblable à la forme générique de l'équation 3.41, et donc chacun peut être utilisé comme ce *signal de caractérisation.*

L'oscillateur interne du module de détection synchrone peut aussi être réglé pour

osciller à deux fois la fréquence du *signal de modulation.* Dans ce cas, on a

$$V_X^{int} = \cos(2\omega_m t + \phi_{int}) \tag{3.61}$$

$$V_Y^{int} = \sin(2\omega_m t + \phi_{int}) \tag{3.62}$$

Ainsi, pour $V_X^{\times}$, on a

$$\begin{aligned} V_X^{\times} &= I_0 \cos(\omega_m t + \phi_{int}) \\ &+ 2I_0 V \cos(\omega_m t + \phi_{int}) J_0\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right) \\ &+ \frac{I_0 V}{2}\cos\omega_0\tau \sum_{n\ pair} J_n\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\{\cos((n+2)\omega_m t + \phi_{int}) + \cos((n-2)\omega_m t - \phi_{int})\} \\ &+ \frac{I_0 V}{2}\sin\omega_0\tau \sum_{n\ impair} J_n\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\{\sin((n+2)\omega_m t + \phi_{int}) + \sin((n-2)\omega_m t - \phi_{int})\} \end{aligned}$$

En cherchant les termes de fréquence nulle (avec $n = 2$), on voit que le signal X est

$$X_{2\omega_m} = \frac{I_0 V}{2}\cos(\omega_0\tau)\, J_2\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\cos(\phi_{int}) \tag{3.63}$$

Similairement pour Y

$$Y_{2\omega_m} = -\frac{I_0 V}{2}\cos(\omega_0\tau)\, J_2\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\sin(\phi_{int}) \tag{3.64}$$

D'où

$$R_{2\omega_m} = \frac{I_0 V}{2}\left|\cos(\omega_0\tau)\, J_2\left(\frac{\Delta\bar{\phi}\omega_m\tau}{2}\right)\right| \tag{3.65}$$

Donc, les signaux $X_{2\omega_m}$ et $Y_{2\omega_m}$ sont chacun analogues à la forme du *signal de caractérisation* 3.42.

On voit donc que l'utilisation du module de détection synchrone permet concrètement d'obtenir les *signaux de caractérisation* en quadrature recherchés.

Dans notre montage, nous avons utilisé le module de détection synchrone SR530

de *Stanford Research Systems.* Celui-ci donne accès aux signaux de caractérisation via un port IEEE 488 (GPIB).

3.3.4 Le système de contrôle de la température et d'acquisition des signaux

Le but du système de contrôle et de la température est d'imposer un balayage en température à l'interféromètre.

Pour cela, un refroidisseur à eau [1] fait circuler de l'eau distillée de température controlée dans un serpentin de tuyau de cuivre à l'intérieur d'un bain thermique. La température de l'eau est fixée et contrôlée par le refroidisseur à eau. Le bain thermique est composé d'un grand bassin d'eau dans lequel flotte un contenant pour l'interféromètre, le tout isolé thermiquement de son environnement via une épaisse enveloppe de polystyrène expansé. Dans le bain, on trouve également un thermomètre numérique de haute précision de type RTD[2]. Un ordinateur avec un logiciel Labview permet de fixer la température du refroidisseur à eau, acquiert du thermomètre la température dans le bain et agit pour contrôler celle-ci.

Pour faire le balayage, le programme est réglé pour maintenir un différentiel de $-3°C$ entre le refroidisseur à eau et le bain (le balayage se fait toujours en température décroissante). Cela produit un taux très lent de variation de la température : environ 0,35°C/heure, afin de permettre le temps pour l'acquisition des signaux de caractérisation.

Le système d'acquisition est basé sur l'interrogation du module de détection synchrone par le logiciel Labview via son IEEE 488. Toutes les 5 secondes environ, le logiciel obtient une mesure des signaux X_{ω_m} et Y_{ω_m}.

---

[1] Il s'agit d'un appareil chauffant ou refroidissant permettant de produire et pomper un fluide à une température fixée.

[2] *Resistance Temperature Detector* : instrument de mesure de température basé sur la variation de la résistance d'un élément sensible.

3.3.5 Contrôle de polarisation

Pour effectuer la caractérisation en polarisation, le montage est identique à celui de la caractérisation en température, mais on insère une boucle de Lefèvre [17] entre le laser et l'entrée de l'interféromètre. La boucle de Lefèvre permet d'arbitrairement transformer l'état de polarisation du signal sonde : en configurant aléatoirement la boucle de Lefèvre, on insère des états de polarisation aléatoires dans l'interféromètre.

Chapitre 4

Résultats

En appliquant la méthode de conception et de fabrication du chapitre 2, deux interféromètres de Mach-Zehnder tout-fibre ont été fabriqués. L'objet de ce chapitre est la présentation des résultats obtenus pour les caractérisations en température et en polarisation de ceux-ci.

4.1 Caractéristiques des interféromètres fabriqués

On présente au tableau 4.1 les caractéristiques décrivant les interféromètres qui ont été fabriqués.

On remarque que l'interféromètre B ne possède pas les longueurs de branches qui lui permet de réaliser la *compensation thermique passive*. En effet, pour cet interféromètre, on a $L_1/L_2 = 0{,}909$ alors que l'interféromètre A possède le rapport de longueurs requis pour la compensation thermique passive, soit $L_1/L_2 = 0{,}900$. Par conséquent, on ne s'attend pas à ce que l'interféromètre B soit thermiquement stabilisé. Par contre, les deux interféromètre ont $\Delta N = 4$ et des caractéristiques d'enroulement identiques.

Ainsi, nous avons utilisé l'interféromètre A pour étudier la *compensation thermique passive* et l'interféromètre B pour étudier la *compensation de biréfringence*.

TAB. 4.1 – Caractéristiques des interféromètres testés.

Caractéristique	Interf. A	Interf. B	Incertitude	Unités
f_r	100	100	n/a	MHz
L_1	18,38	20,62	0,02	m
L_2	20,42	22,66	0,02	m
N_1	35	39	n/a	n/a
N_2	39	43	n/a	n/a
$L_{ne,E}$	12	12	0,1	cm
$L_{ne,S}$	19,0	59,0	0,1	cm
$L_{c,E}$	11,0	11,0	0,1	cm
$L_{c,S}$	34,6	9,9	0,1	cm
D_{eq}	16,25	16,25	n/a	cm
h	(variable)	11,6	0,1	cm
$1-t^2$	0,01	0,01	0,01	dB
$c'c$	50	50	0,5	%

4.2 Présentation des résultats

4.2.1 Caractérisations en température

4.2.1.1 Résultats bruts

Chaque interféromètre, A et B, fut caractérisé en température deux fois afin de vérifier la répétabilité des résultats.

Pour l'interféromètre A, les deux caractérisations ont été faites sur une plage de températures entre 20°C à 24°C. Pour la première caractérisation les *signaux de caractérisation* $(X_{\omega_m}, X_{2\omega_m})$ et $(Y_{\omega_m}, Y_{2\omega_m})$ obtenus sont présentés sur les figures 4.5 et 4.6 respectivement. Les résultats de la seconde caractérisation sont donnés sur les figures 4.7 et 4.8.

Dans le cas de l'interféromètre B, les résultats obtenus sur une plage de 22°C à 24°C sont illustrés sur les figures 4.1 à 4.4.

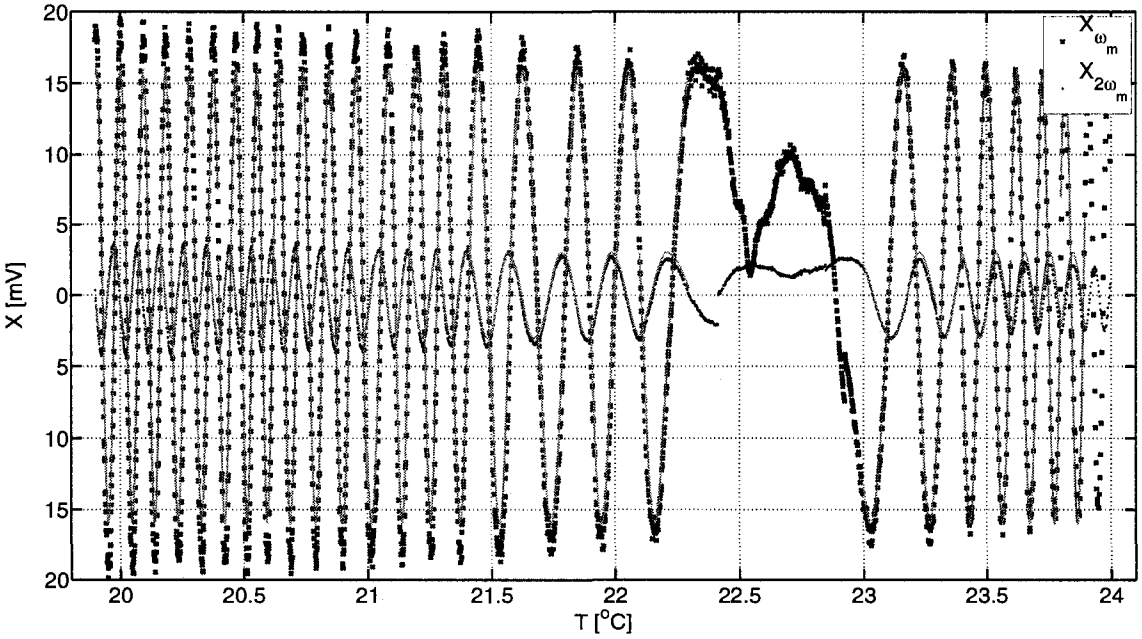


FIG. 4.1 – Interf. A : signaux de caractérisation X_{ω_m} et $X_{2\omega_m}$ (expérience #1).

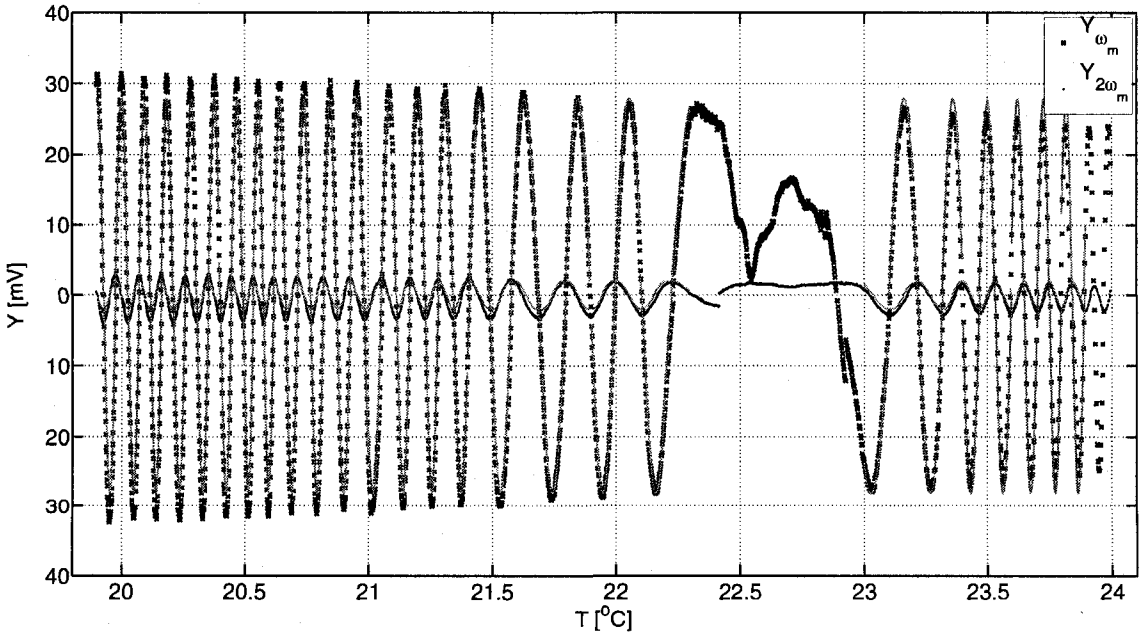


FIG. 4.2 – Interf. A : signaux de caractérisation Y_{ω_m} et $Y_{2\omega_m}$ (expérience #1).

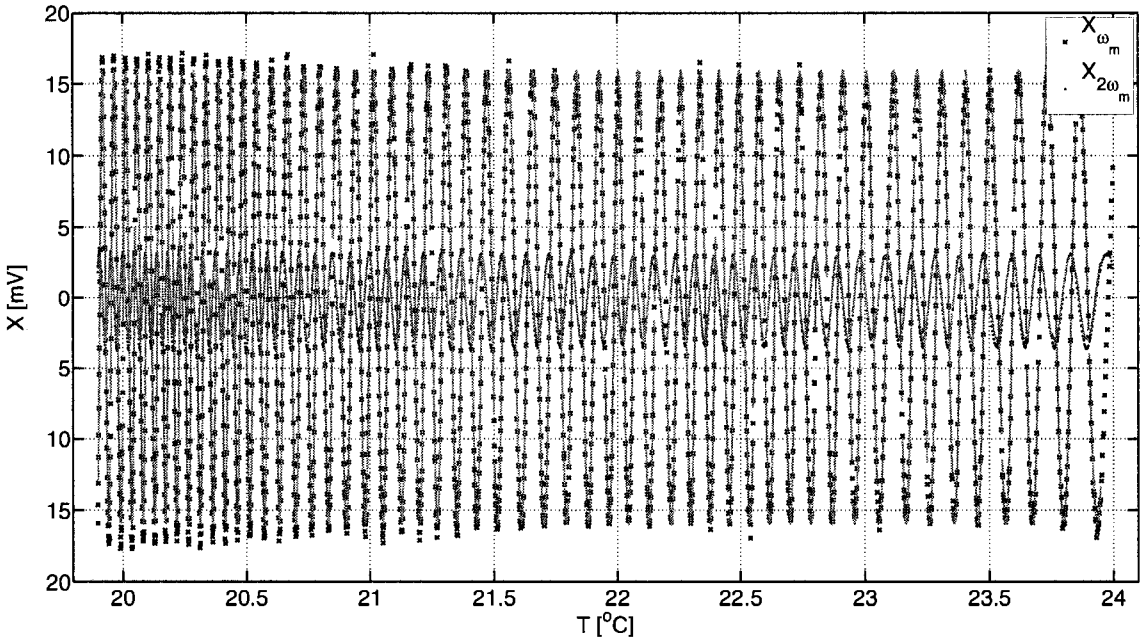


FIG. 4.3 – Interf. A : signaux de caractérisation X_{ω_m} et $X_{2\omega_m}$ (expérience #2).

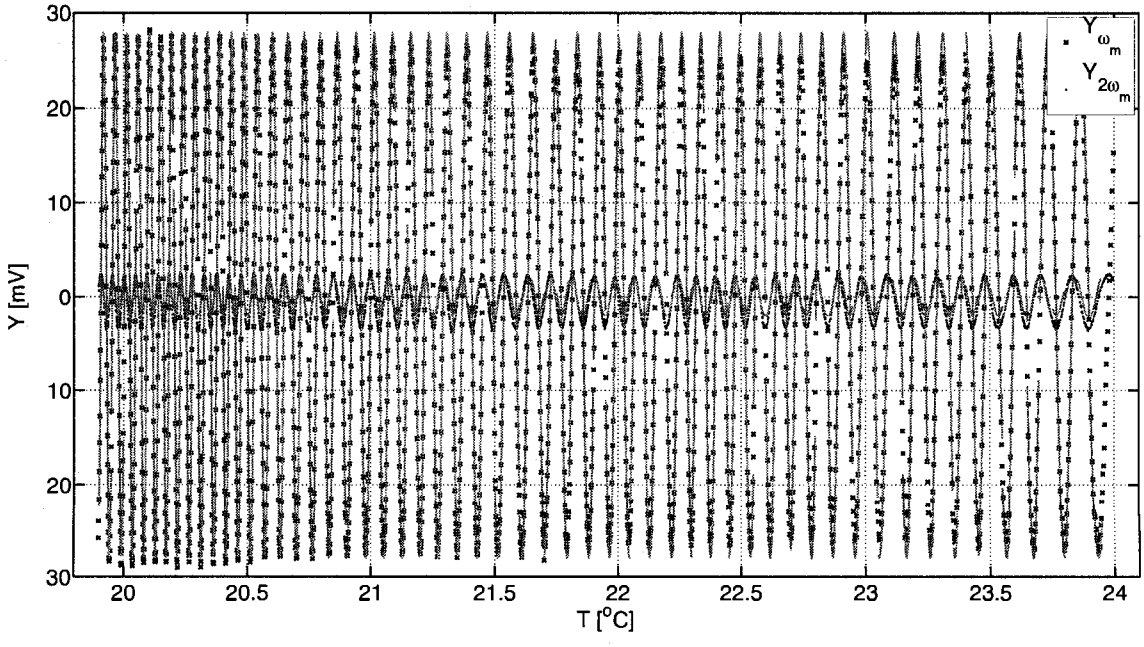


FIG. 4.4 – Interf. A : signaux de caractérisation Y_{ω_m} et $Y_{2\omega_m}$ (expérience #2).

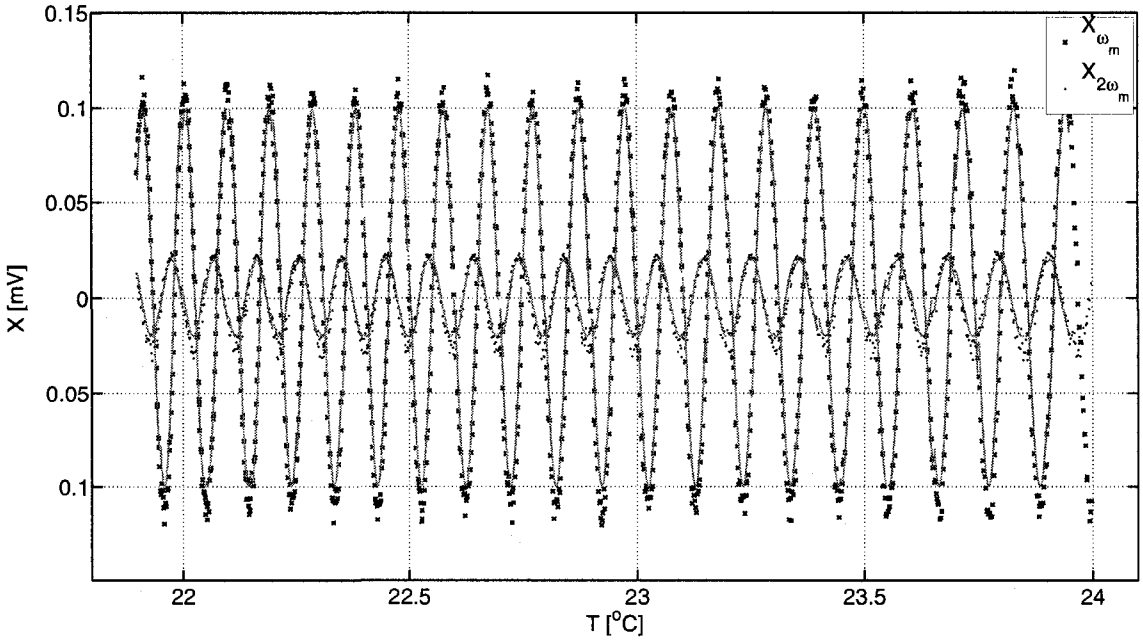


FIG. 4.5 – Interf. B : signaux de caractérisation X_{ω_m} et $X_{2\omega_m}$ (expérience #1).

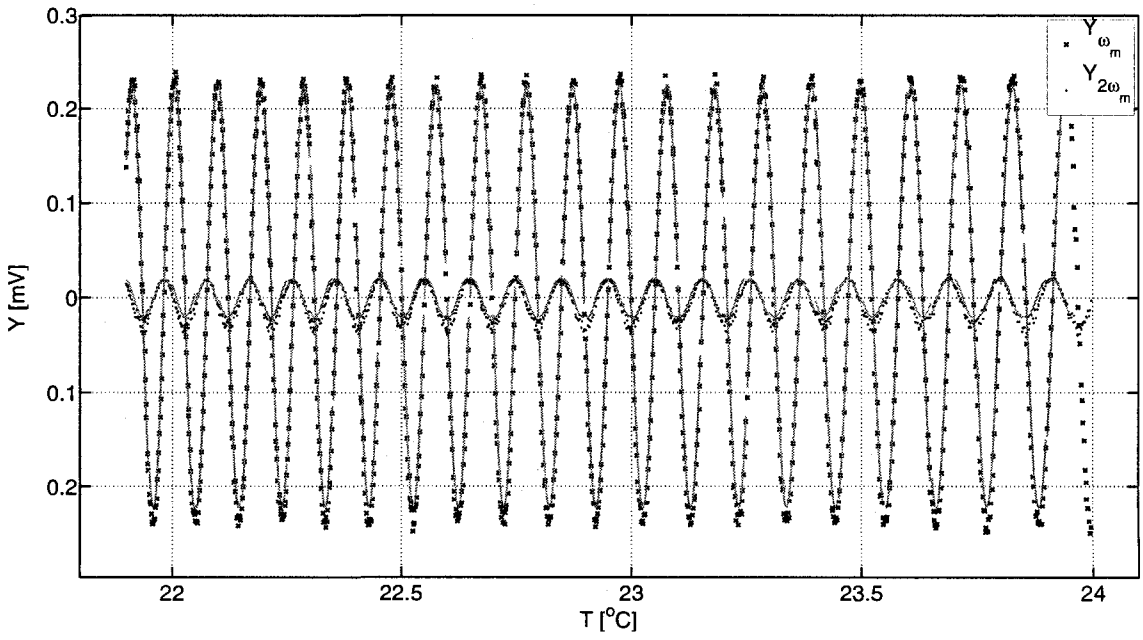


FIG. 4.6 – Interf. B : signaux de caractérisation Y_{ω_m} et $Y_{2\omega_m}$ (expérience #1).

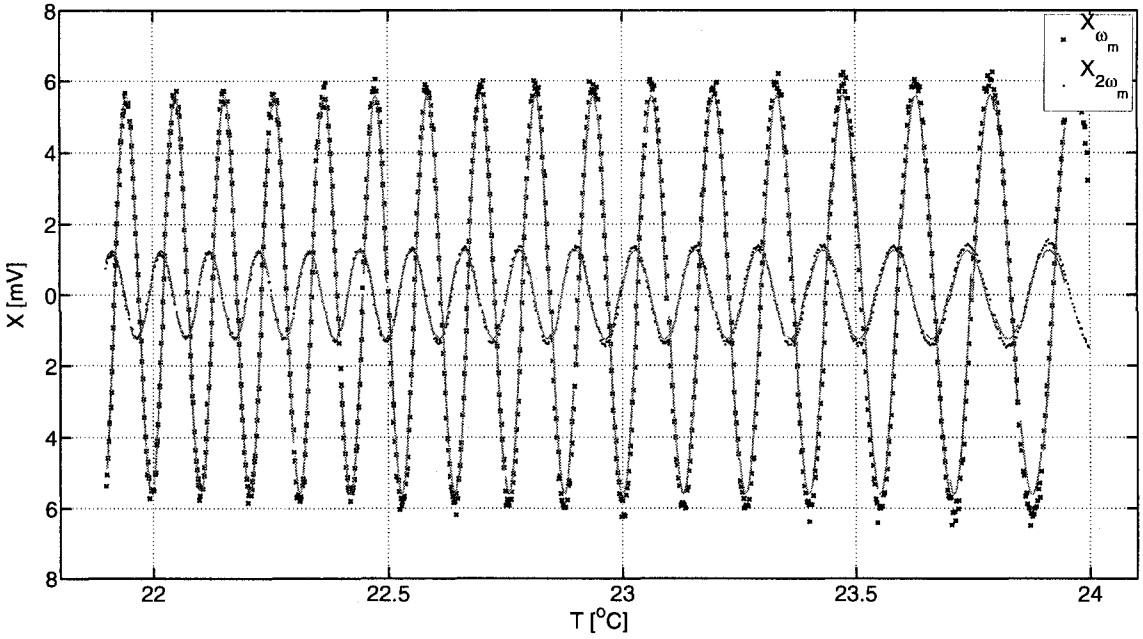


FIG. 4.7 – Interf. B : signaux de caractérisation X_{ω_m} et $X_{2\omega_m}$ (expérience #2).

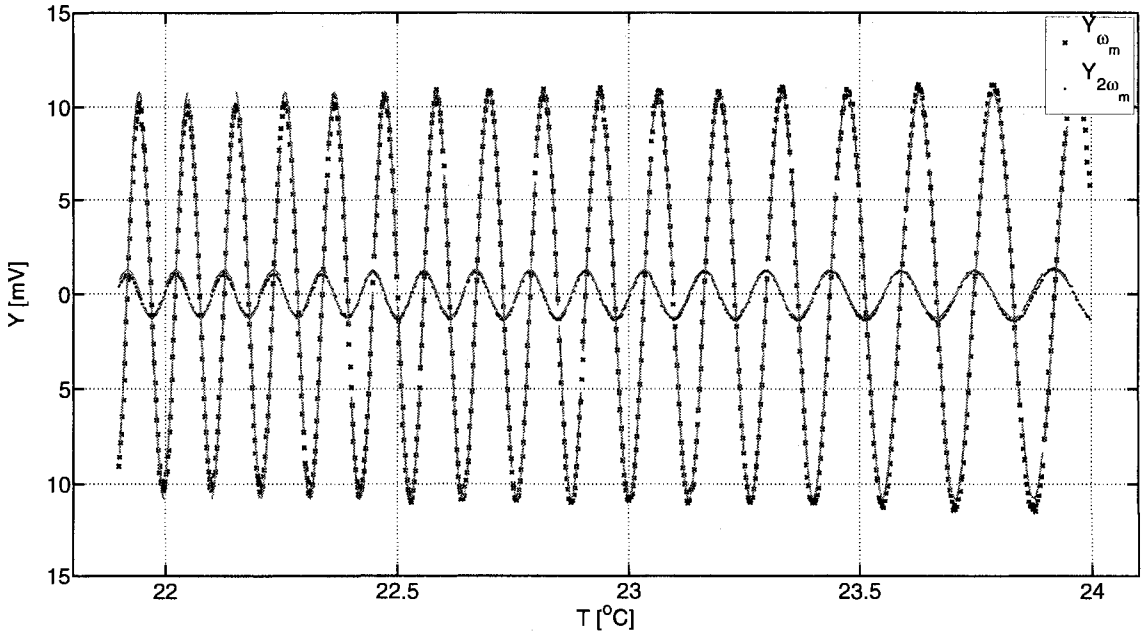


FIG. 4.8 – Interf. B : signaux de caractérisation Y_{ω_m} et $Y_{2\omega_m}$ (expérience #2)

4.2.1.2 Sensibilité en température

Sur les graphiques de résultats bruts, chaque point représente une acquisition des signaux à la température mesurée correspondante. Superposé sur ce graphique, on aperçoit plusieurs segments de courbes (en gris) lissés. Ceux-ci sont de la forme

$$X^i_{\omega_m} = a_{const} \sin(\omega^i_T T + \varphi^i) \tag{4.1}$$

$$X^i_{2\omega_m} = b_{const} \cos(\omega^i_T T + \varphi^i) \tag{4.2}$$

où l'indice i désigne le segment. Chaque signal, X_{ω_m} et $X_{2\omega_m}$ a été lissé indépendamment sur les points expérimentaux par la méthode des moindres carrés sur (ω^i_T, φ^i). Les amplitudes a et b ont étés maintenues constantes afin de réduire l'espace de lissage. De plus, il importe de noter que chaque segment est lissé sur une plage de température plus petite que la période des signaux de caractérisation, de sorte que chaque (ω^i_T, φ^i) donne une mesure *locale* de la fréquence en température en fonction de cette dernière.

De ces signaux de caractérisation, nous pouvons en extraire la valeur de la sensibilité en température s_T en utilisant la méthode présentée à la section 3.2.1.1. Ainsi, on peut utiliser les valeurs des ω^i_T pour obtenir une sensibilité locale

$$s^i_T = \frac{\omega^i_T}{k_0} \tag{4.3}$$

Comme la sensibilité est commune pour tous les signaux de caractérisation et que les lissages sur chaque signal sont indépendants, nous avons quatre mesures indépendantes de la sensibilité en température.

Pour l'interféromètre A, les figures 4.9 et 4.10 donnent la sensibilité en température obtenue lors des caractérisations #1 et #2 respectivement. Les points sur ces courbes représentent la moyenne des quatre mesures de la sensibilité alors que les barres donnent une intervalle de confiance de 95% basée sur la variance des 4 mesures.

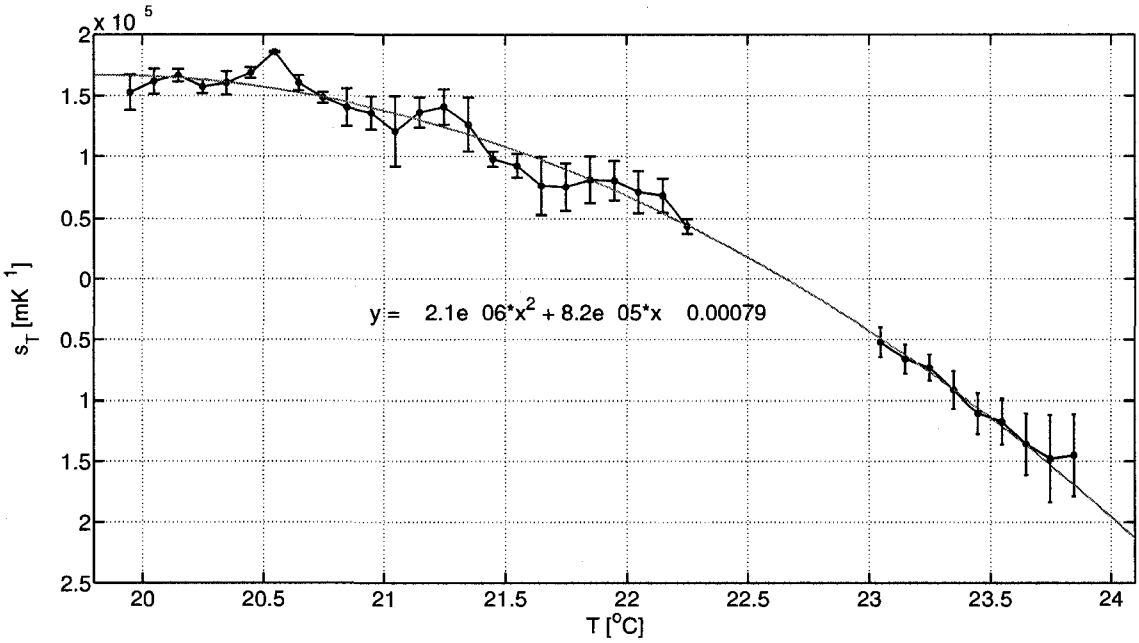


FIG. 4.9 – Interf. A : sensibilité en température (expérience #1).

Les figures 4.11 et 4.12 donnent la même information pour l'interféromètre B.

4.2.2 Caractérisation en polarisation

Seul l'interféromètre B est caractérisé en polarisation.

Pour cela, nous avons appliqué la méthode présentée à la section 3.2.2. Les résultats sont présentés à la figure 4.13.

Ainsi, pour une valeur h donnée, nous avons placé l'interféromètre dans le bain thermique afin de stabiliser sa température comme le suppose cette méthode. Cependant, le bain ne permet pas de stabiliser la température jusqu'au niveau requis, soit environ une stabilité à ±0,006°C. Nous avons donc eu recours à une méthode de "filtrage" par lequel seuls des points obtenus pour une température moyenne ±0,006°C ont étés retenus pour l'analyse. Ceci permet de réduire l'effet de la variabilité en température assez pour structurer les résultats, sans totalement l'éliminer cette source d'erreurs.

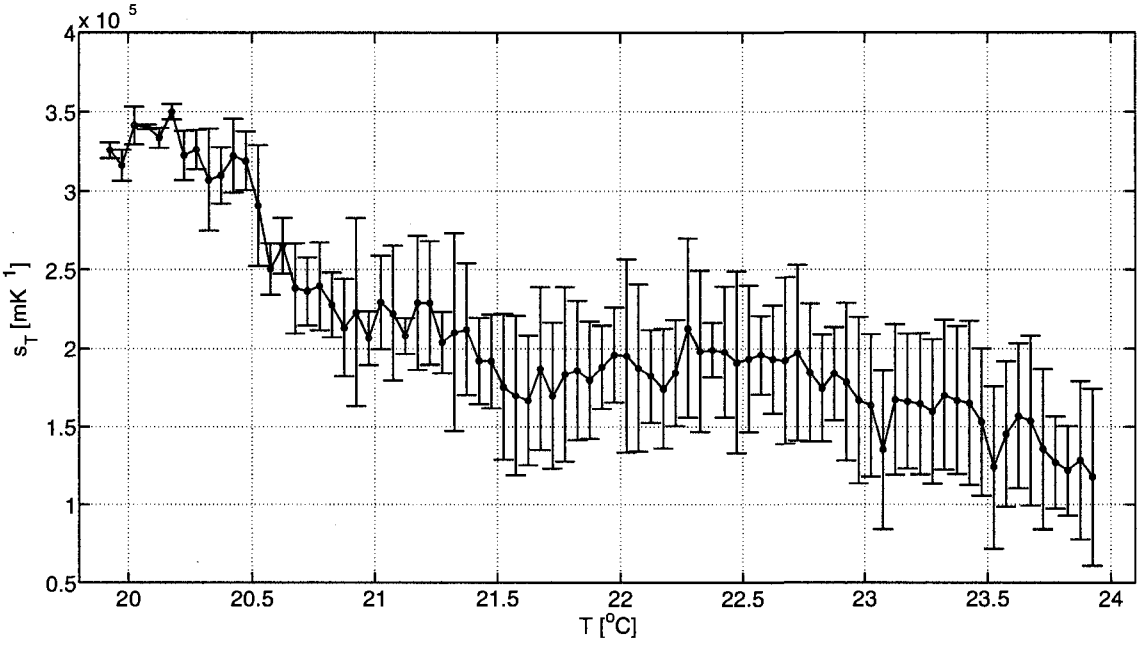


FIG. 4.10 – Interf. A : sensibilité en température (expérience #2).

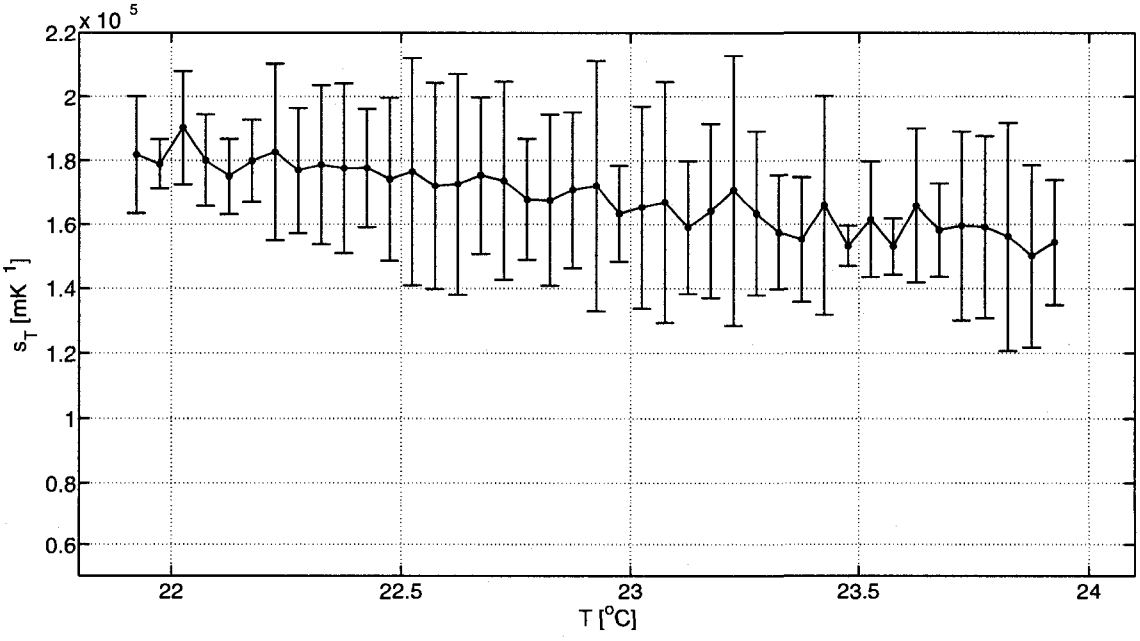


FIG. 4.11 – Interf. B : sensibilité en température (expérience #1).

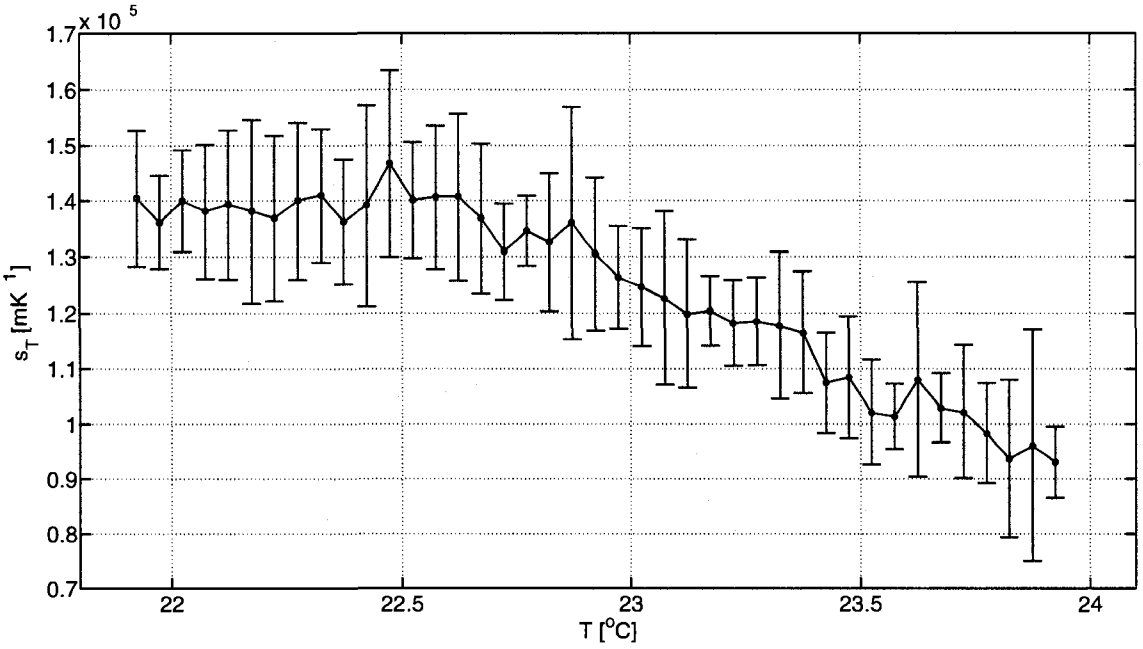


FIG. 4.12 – Interf. B : sensibilité en température (expérience #2).

On voit également sur la figure 4.13 la variance attendue en fonction de h, ainsi qu'une variance ajustée. Cet ajustement correspond à une diminution uniforme de 45% en termes de ϕ_{tr}^{xy} en fonction de h (c.-à-d. que $\phi_{tr,ajuste}^{xy}(h) = 0{,}55\phi_{tr}^{xy}(h)$).

4.3 Discussion

4.3.1 Sensibilité en température

D'abord, il est utile de noter que, si des fibres SMF-28 avaient étés utilisés pour les deux branches, des interféromètres la sensibilité thermique aurait été de

$$\begin{aligned} s_T|_{SMF-28} &= \alpha_{n_1}\left[L_2 - L_1\right] \\ &= 0{,}92 \times 10^{-5}\left[20{,}419 - 18{,}377\right] \\ &= 1{,}87 \times 10^{-5}\text{m/K} \end{aligned}$$

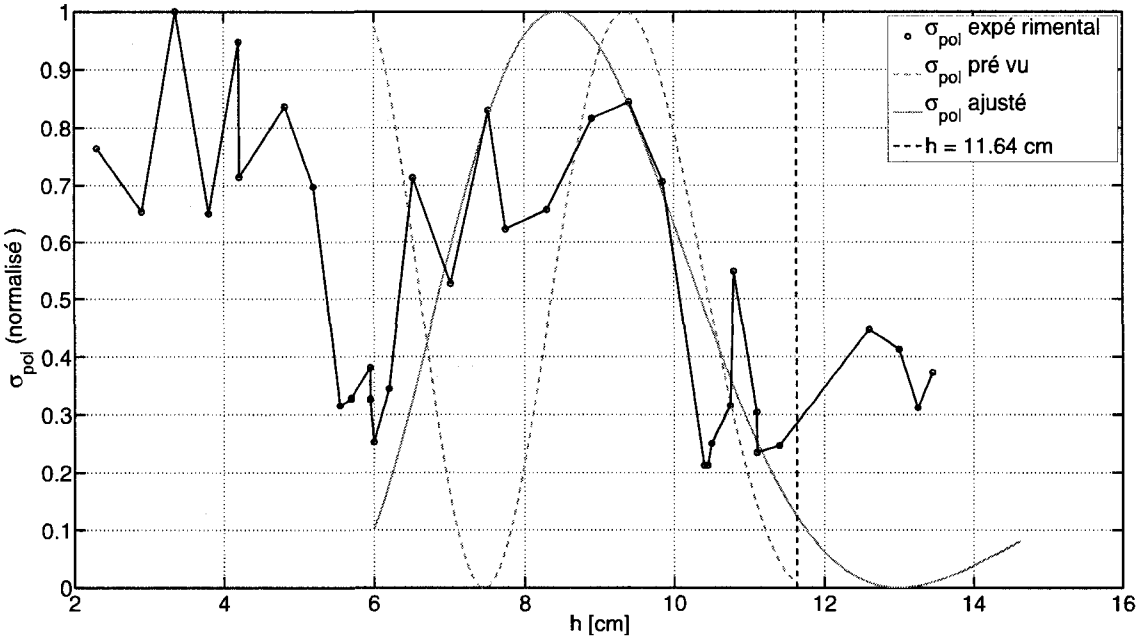


FIG. 4.13 – σ_{pol} en fonction de h.

Ainsi, tel qu'attendu, on voit sur les figures 4.5 à 4.8 que l'interféromètre B n'est pas stable en température, mais sa sensibilité est améliorée par un facteur d'approximativement 2 par rapport à un interféromètre non compensé.

Par ailleurs, l'observation des figures 4.1, 4.2 et 4.9 nous permet de constater une stabilisation thermique de l'interféromètre A autour de 22,6°C, ce qui est tout-à-fait conforme aux prédictions. Ceci semble donc démontrer de l'on a atteint un des plus importants objectifs des design, soit la *compensation thermique passive.*

Malheureusement, l'observation des 4.3, 4.4 et 4.10 vient troubler cette conclusion. Ces figures montrent non seulement que le comportement thermique n'a pas été répété d'une caractérisation (identique) à l'autre, mais que la stabilité thermique est en fait inférieure à celle attendue pour un interféromètre sans compensation thermique. En effet, on remarque sur la figure 4.10 que pour $T < 21$°C, on a $s_T > 1{,}87 \times 10^{-5}$ m/K.

Ces résultats sont contradictoires et démontrent certainement qu'un paramètre affectant le comportement thermique des fibres échappe au modèle supposé pour la

compensation thermique passive.

Deux effets pourraient être à l'origine de ce comportement, soit (1) une température non-uniforme dans le bain de caractérisation ou (2) l'effet des gaines polymériques des fibres sur les caractéristiques thermiques de celles-ci.

4.3.1.1 L'effet d'une température non-uniforme dans le bain de caractérisation

Comme nous n'avions qu'une mesure de la température dans le bain, nous ne pouvons rétroactivement évaluer la présence ou l'importance d'une température non-uniforme dans le bain de caractérisation. Cependant, on peut tenter d'étudier la crédibilité de cette hypothèse en considérant l'effet d'une différence de température d'une branche (ou portion de branche) par rapport à l'autre.

Dans la discussion sur l'effet de la compensation thermique passive (section 2.2), on suppose en tout temps une température égale sur les deux branches. Ceci a été reflété dans la conception et la fabrication des interféromètres : a enroulé le plus possible les fibres des deux branches côte à côte, tel qu'illustré sur la figure 2.9(b). Or, la branche de P+ est plus longue que la branche de SMF-28. Donc, les quatre tours supplémentaires de cette fibre, dans l'enroulement, ne peuvent être mis en correspondance directe avec un segment de fibre SMF-28 pour ce qui est de la *compensation thermique passive.*

Supposons, pour fins de discussion, qu'une portion L' de la branche de fibre P+ soit à une température différente de celle du reste de l'enroulement. On notera alors la température de ce segment T' et la température du reste T. Dans ce cas, en référence à l'équation 2.29 (moins l'effet négligeable de la dilatation thermique), la différence de phase de l'interféromètre s'écrit

$$\begin{aligned} \Delta\phi(T_0, T, T') &= k\left[(L_2 - L')\alpha_{n_2} - (L_1)\alpha_{n_1}\right](T - T_0) \\ &+ kL'\alpha_{n_2}(T' - T_0) \end{aligned}$$

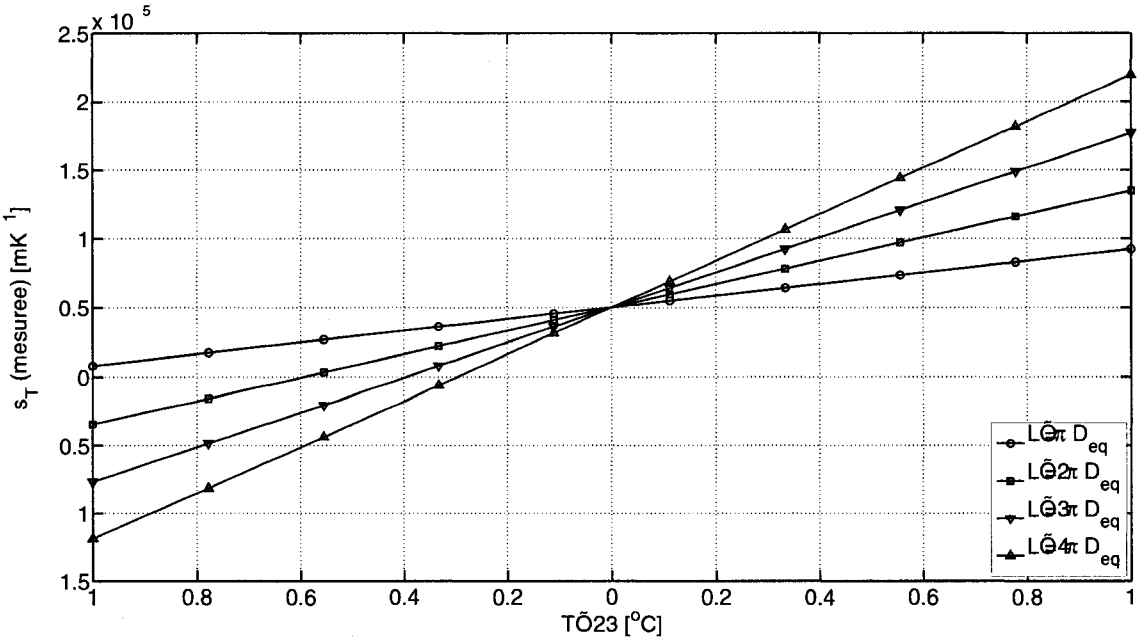


FIG. 4.14 – Non-uniformité de la température du bain : variation de la sensibilité mesurée.

Ceci mène à la définition de deux termes de sensibilité en température

$$s'_T = [(L_2 - L')\alpha_{n_2} - L_1\alpha_{n_1}] \tag{4.4}$$

$$s''_T = L'\alpha_{n_2} \tag{4.5}$$

Dans ce cas, si on mesure une sensibilité s'_T à la température T, la sensibilité changera en fonction de $T' - T$

$$s_T|_{mesuree} = s'_T + s''_T(T' - T) \tag{4.6}$$

Sur la figure 4.14, on trace l'équation 4.6 avec T fixé à 23°C en fonction de T' pour différentes valeurs de L' et avec la sensibilité nominale s'_T fixée à $0{,}5 \times 10^{-5}$ m/K.

On voit sur cette figure que la non-uniformité de la température dans le bain peut résulter en une variation appréciable de la sensibilité mesurée. Il est même possible que la sensibilité approche 0 pour des gros gradients de température. Par contre, des

variations dans le bain au delà de $(T' - T) = \pm 0{,}1°C$ semblent invraisemblables. En effet, comme le taux variation de température dans celui-ci est de 0,35°C/heure, il semble irréaliste d'imaginer des gradients de températures au delà de 0,1°C. Des gradients de 1°C sont certainement exclus.

Or, on voit que même pour $L' = 4\pi D_{eq}$ (soit une longueur égale à toute la longueur excédente de fibre P+) la sensibilité ne varie qu'entre $0{,}3 \times 10^{-5}$ m/K et $0{,}7 \times 10^{-5}$ m/K pour $(T' - T) = \pm 0{,}1°C$.

Ainsi, l'effet de la non-uniformité de la température dans le bain ne peut expliquer les variations importantes dans les valeurs de s_T mesurés. En particulier, cet effet ne peut expliquer le passage par zéro dans la sensibilité de l'interféromètre A observée à la figure 4.9.

4.3.1.2 Effet de la gaine polymérique

Il semble raisonnable d'émettre l'hypothèse que, dans le bain thermique, la présence d'humidité qui serait absorbée par la gaine polymérique des fibres, pourrait affecter les résultats. Il semble en effet probable que le bain thermique puisse imbiber cette gaine d'humidité, contrairement à la silice de la fibre. Suivant cette logique, les gaines rajoutés sur les épissures pourrait aussi s'humidifier.

Ceci pourrait expliquer les variations entre caractérisations, bien que nous n'ayons aucune façon de le démontrer. Les mesures #1 de l'interféromètre A ont été effectuées immédiatement suivant sa fabrication. Les mesures #2 ont été effectuées le lendemain. Ces caractérisations se font toujours de la température élevée (ici 24°C) vers la température basse (ici 20°C). Pour faire les deux caractérisations, la température fut cyclée complètement une fois entre 24°C et 20°C. Si effectivement la gaine polymérique absorbe de l'humidité, on s'attendrait à un comportement de forte hystéresis.

On peut donc imaginer que la gaine était complètement sèche lors de l'introduction de l'interféromètre dans le bain. Elle a alors absorbé de l'humidité pendant plusieurs heures atteignant la saturation vers la fin de la caractérisation #1, tel que suggéré

par le comportement asymptotique de la courbe de la figure 4.9. Entre les deux caractérisations, on observe un effet d'hystérisis sur la gaine polymérique.

Si cela est vrai, alors (1) la gaine affecte très significativement le comportement en température des fibres et (2) la gaine est assez fortement affecté par l'humidité. C'est l'intuition de l'auteur que ce phénomène est responsable de la variabilité observée entre les caractérisations.

4.3.2 Sensibilité en polarisation

En fonction du paramètre d'enroulement h, la figure 4.13 montre un comportement qualitativement conforme aux attentes : la biréfringence produit des battements pour des valeurs de h discrètes. Dans notre cas, on observe un minimum de variabilité σ_{pol} (correspondant directement à un maximum de visibilité V) vers $h \approx 11{,}25$ cm et $h \approx 6$ cm, alors que la simulation a mené à la valeur optimisée $h = 11{,}64$ cm.

Il est à noter que la méthode utilisée, en particulier pour réduire l'effet de la température, ne permet pas de réduire la variabilité à zéro comme ce serait le cas théoriquement. En effet, la méthode de "filtrage en température" utilisée a ses limites : le thermomètre RTD utilisé possède une résolution officielle de 0,01°C, ce qui est au delà de la tolérance voulue de 0,006°C. Cependant, le thermomètre fournit une troisième décimale lorsqu'utilisé en mode RS-232. Il est probable que cette troisième décimale ne soit pas métrologiquement significative, mais on l'utilise ici néanmoins pour effectuer le filtrage. Comme cette troisième décimale est très incertaine, la variabilité due à la température ne peut être éliminée et, par conséquent, on ne peut réduire la variabilité σ_{pol} à zéro.

Par ailleurs, l'observation de la figure 4.13 montre que le comportement quantitatif de σ_{pol} versus h n'est pas conforme aux attentes (voir la ligne tiretée "σ_{pol} prévu"). Plus précisément, les résultats obtenus montrent que la simulation a mené à une exagération de la biréfringence de la fibre en fonction de h. Pour estimer l'ampleur de cette exagération, nous avons empiriquement ajusté la courbe de ϕ_{tr}^{xy} en fonction de h

afin d'obtenir un comportement conforme aux mesures. Le résultat de cet ajustement est la courbe "σ_{pol} ajusté" sur la figure 4.13. Cette courbe représente un ajustement constant de -40% de la dépendance de ϕ_{tr}^{xy} avec h, soit un ajustement considérable.

Deux causes sont probablement en jeu.

Premièrement, dans le calcul de la biréfringence, il y a une ambiguïté sur le fait d'inclure ou non la gaine polymérique dans la valeur de r, soit le rayon transversal de la fibre. À ce sujet, les références ne sont pas claires. Dans la référence [14] on spécifie qu'on a retiré la gaine polymérique de la fibre afin d'en caractériser les effets de biréfringence, sans spécifier si ces résultats sont utilisables ou pas si la gaine est en place. Dans la référence [18] on n'est pas spécifique du tout. Dans le calcul de théorique de ϕ_{tr}^{xy} effectué (voir la figure 2.4), nous avons inclus la gaine polymérique dans la valeur de r, donc $r = 250$ μm (vs. $r = 125$ μm si on l'avait exclut). Cependant, comme la gaine polymérique possède des caractéristiques mécaniques très différentes de celles de la silice, il serait raisonnable de ne pas compter la rayon de cette gaine à 100%. On pourrait, par exemple, se donner un rayon effectif de $r_{eq} \approx 190$ μm. Comme la biréfringence de courbure varie en r^2, le fait de prendre $r_{eq} \approx 190$ μm correspond à un ajustement d'environs -40% sur ϕ_{tr}^{xy} vs h. Ainsi, de manière générale, l'incertitude sur la valeur r à utiliser dans les calculs est une source importante d'incertitude affectant la relation théorique de ϕ_{tr}^{xy} vs h.

Deuxièmement, bien que l'interféromètre soit fabriqué en évitant d'introduire de la torsion dans la fibre enroulée, il n'est pas totalement impossible que celle-ci soit présente. L'effet de la torsion est, en théorie, petit, mais son effet peut s'ajouter ou se soustraire à la biréfringence totale en fonction de la direction de la torsion.

Par contre, il semble improbable que la torsion soit responsable du comportement mesuré. Pour s'en convaincre, on note que la biréfringence de torsion est approximativement de [18]

$$\beta_\tau \approx 0{,}146\tau \ [\mathrm{m}^{-1}] \tag{4.7}$$

où τ est le nombre de tours/m (en torsion) de la fibre. Il est important de noter que

cette biréfringence est circulaire. Donc, une torsion pouvant ajuster la biréfringence de 40% serait de l'ordre de 2 tours/m, soit approximativement 1 tour de torsion par tour d'enroulement. Puisque l'enroulement s'est fait directement du rouleau de fibre au mandrin d'enroulement, avec une distance entre les deux d'environs 1 m, la présence d'un tour de torsion par tour d'enroulement semble improbable.

Conclusion

Dans ce mémoire, nous avons présentés un design d'interféromètre à très long délai adapté pour une utilisation comme décodeur de qubits dans un schéma de QKD par DPSK. Celui-ci fut développé à partir des contraintes et tolérances spécifiques à cette utilisation. Nous avons également présenté une méthode très précise de caractérisation, la *caractérisation par modulation de phase* permettant la caractérisation thermique de tels interféromètres.

Le design de l'interféromètre est fondé sur deux concepts *originaux*, essentiellement sans précédent dans la littérature scientifique, soit la *compensation thermique passive* et la *compensation de biréfringence.* De plus, la *caractérisation par modulation de phase*, également *originale*, représente une méthode très pratique et extrêmement précise développée à partir de quelques méthodes semblables publiées.

L'application de la *caractérisation par modulation de phase*, nous a permis de tester les concepts de *compensation thermique passive* et de *compensation de biréfringence.* Par ce fait même, nous avons également validé la méthode de caractérisation.

Les résultats obtenus ont démontré le fonctionnement de la compensation thermique passive : nous avons obtenu un interféromètre de 100 MHz stable autour de 22.6°C. Par contre, la stabilité de cet interféromètre semble elle même "volatile", probablement à cause des variations des caractéristiques de la gaine, tel que suggéré par des caractérisations répétées.

Pour ce qui est de la compensation de biréfringence, les caractérisations ont également montré le fonctionnement de ce concept. Cependant, les tests on démontré

que le modèle utilisé pour le design doit être *calibré* afin de le faire correspondre quantitativement avec les résultats obtenus.

Plusieurs travaux pourraient être effectués pour poursuivre ce travail.

Premièrement, la compensation thermique passive repose sur la connaissance très précise du rapport des coefficients thermo-optiques des fibres SMF-28 et P+. Malheureusement, les auteurs sur ce sujet ne s'intéressent généralement qu'à l'influence de l'effet thermo-optique sur la dispersion dans les télécommunications optiques et donc seule la fibre SMF-28 est caractérisée. Il serait donc très intéressant d'utiliser le montage de caractérisation par modulation de phase afin d'effectuer des mesures comparatives précises de l'effet thermo-optique dans les fibres P+ et SMF-28.

Deuxièmement, les résultats obtenus ont mis en lumière l'effet possible de la gaine polymérique sur le comportement thermique de l'interféromètre. Conséquemment, il serait souhaitable de réaliser des interféromètres ayant différents types de gaines par exemple en aluminium, en or, en cuivre voire même sans aucune gaine protectrice. Pour l'interféromètre sans gaine, afin de maintenir une certaine robustesse, il serait fort utile de développer une protection secondaire, un packaging pour l'ensemble de l'interféromètre par exemple.

Troisièmement, la tolérance calculée pour les longueurs de fibres de branches, soit 1 mm, représente sur des longueurs de l'ordre de 20 m, une tolérance de 0,005%. La méthode de fabrication proposée dans ce texte ne permet pas de contrôler avec une telle précision la longueur des fibres. On estime plutôt avoir une précision de l'ordre de 1 cm, soit 0.05%, ce qui est déjà très précis. Dans ce contexte, le fait d'obtenir un interféromètre stable relève d'une certaine chance. Il serait par conséquent très utile de développer une méthode de fabrication permettant de contrôler la longueur des fibres jusqu'à 1 mm.

Quatrièmement, afin d'être utile pour la QKD par DPSK à l'extérieur d'un laboratoire, l'interféromètre devra être inséré dans une enceinte protectrice permettant également le contrôle de la température.

En conclusion, il est l'espoir de l'auteur de ce mémoire qu'il jette les bases formelles permettant le développement futur de cette technologie.

Bibliographie

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74 :145–195, 2002.

[2] D. Stinson. *Cryptographie : Théorie et pratique.* Vuibert, Paris, 2003.

[3] C.H. Bennett and G. Brassard. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984. IEEE.

[4] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41 :1915–1923, 1995.

[5] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85(6) :1330–1333, 2000.

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

[7] H. Takesue, E. Diamanti, T. Honjo, . Langrock, M. M. Fejer, K. Inoue, and Y. Yamamoto. Differential phase shift quantum key distribution experiment over 105 km fibre. *New Journal of Physics*, 7(232), 2005.

[8] K. Inoue, E. Waks, and Y. Yamamoto. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A*, 68(022317), 2003.

[9] I. Prochazka. Semiconducting single photon detectors : the state of the art. *Phys. Stat. Sol.*, 2(5) :1524–1532, 2005.

[10] S. Nam, A.J. Miller, and D. Rosenberg. Low-temperature optical photon detectors for quantum information applications. *Nuclear Instruments and Methods in Physics Research A*, (520) :523–526, 2004.

[11] P.D. Townsend. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelengths-division multiplexing. *Elec. Lett.*, 33(3) :188–190, 1997.

[12] P. Toliver, R. J. Runser, T. E. Chapuran, J. L. Jackel, T. C. Banwell, M. S. Goodman, R. J. Hughes, C. G. Peterson, D. Derkacs, J. E. Nordholt, L. Mercer, S. McNown, A. Goldman, and J. Blake. Experimental investigation of quantum key distribution through transparent optical switch elements. *IEEE Photonics Technology Letters*, 15(11) :1669–1671, 2003.

[13] S. Chang, C.-C. Hsu, T.-H. Huang, W.-C. Chuang, Y.-S. Tsai, J.-Y. Shieh, and C.-Y. Leung. Heterodyne interferometric measurement of the thermo-optic coefficient of single mode fiber. *Chinese Journal of Phys.*, 38(3-1) :437–442, 2000.

[14] A. Bertholds and R. Dändliker. Deformation of single-mode optical fibers under static longitudinal stress. *J. of Lightwave Tech.*, LT-5(7) :895–900, 1987.

[15] J. Zheng. Analysis of optical frequency-modulated continuous-wave interference. *Appl. Optics*, 43(21) :4189–4198, 2004.

[16] L. De Maria and M. Martinelli. External frequency modulation of a laser source for non-incremental interferometric measurements. *Meas. Sci. Technol.*, 4 :1228–1231, 1993.

[17] H. C. Lefevre. Single-mode fiber fractional wave devices and polarisation controllers. *Electronics Letters*, 16(20) :778–780, 1980.

[18] S. C. Rashleigh. Origins and control of polarisation effets in single mode fibers. *J. of Lightwave Tech.*, LT-1(2) :312–331, 1983.

[19] S. Cavallar, B. Dodson, A. Lenstra, W. Lionen, P. Montgomery, B. Murphy, H. te Rielle, K. Aardal, J. Gilchrist, G. Guillerm, P. Leyland, J. Marchand,

F. Morain, A Muffet, C. Putnam, and P. Zimmermann. Factorisation of a 512-bit RSA modulus. *Lecture Notes in Computer Science*, 1807, 2000.

[20] R. Maciejko. *Optique Quantique.* (Notes de cours), Montréal, 2006.

Annexe A

Éléments de science cryptographique

Pour clarifier leur utilisation dans ce texte, il est utile de définir certains termes. Nous nous inspirons ici de la référence [2].

Alice et Bob Deux participants légitimes à une communication.

Eve Participant illégitime (espion) de la communication entre Alice et Bob.

Texte clair Un texte organisé et normalement compréhensible (comme un texte français par exemple), contenant les informations à transmettre entre Alice et Bob.

Clef Information détenue uniquement par Alice et Bob (et pas Eve), qu'ils utilisent respectivement pour chiffrer et déchiffrer un cryptogramme.

Texte chiffré Texte résultant de l'application de la clef et du protocole cryptographique sur le texte clair ; normalement incompréhensible pour Eve qui n'a pas (a priori) la clef.

Canal Voie de transmission entre Alice et Bob.

Système cryptographique Un quintuplet formé de $\{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$ satisfaisant les conditions suivantes

1. $\mathcal{P}$ désigne l'espace des textes clairs ;
2. $\mathcal{C}$ désigne l'espace des textes chiffrés ;
3. $\mathcal{K}$ désigne l'espace des clefs ;
4. Pour tout $K \in \mathcal{K}$, il existe une règle de chiffrement $e_K \in \mathcal{E}$ et une règle de déchiffrement $d_K \in \mathcal{D}$ correspondante. Les fonctions $e_K : \mathcal{P} \rightarrow \mathcal{C}$ et $d_K : \mathcal{C} \rightarrow \mathcal{P}$ sont telles que $e_K(d_K(x)) = x$ pour un texte clair $x \in \mathcal{P}$.

Ainsi, l'objectif de la cryptographie est de produire, à partir d'un texte clair, un texte chiffré tel qu'Alice et Bob puissent se le communiquer via un canal non-sécurisé sans qu'Eve ne puisse comprendre le texte chiffré qu'elle voudrait intercepter.

Le secret parfait

En 1949, un chercheur de *Bell Labs* Claude Shannon publia l'article fondateur de ce qui est maintenant connu sous le nom de la théorie de l'information. Cette théorie permet de décrire formellement ce qui définit le secret, notion fondamentale en cryptographie.

Soit une distribution de probabilité sur l'espace des textes clairs $\mathcal{P}$. Soit une distribution de probabilité sur l'espace des textes chiffrés $\mathcal{C}$. Soit un texte clair $x \in X$ et un texte chiffré $y \in Y$, où X et Y sont des variables aléatoires soumises aux distributions $\mathcal{P}$ et $\mathcal{C}$, respectivement. On note $\mathbf{Pr}[X = x] \equiv \mathbf{Pr}[x]$ la probabilité que le texte clair soit *a priori* égal à x.

Un système cryptographique assure la *confidentialité parfaite* au sens de la théorie de l'information si

$$\mathbf{Pr}[x|y] = \mathbf{Pr}[x] \tag{A.1}$$

Autrement dit, si la probabilité d'occurrence d'un texte clair demeure inchangée étant

donnée le texte chiffré, l'obtention du texte chiffré ne diminue en rien l'incertitude qu'on avait a priori sur le texte clair. Dans ce cas, le texte chiffré ne révèle *aucune* information sur le texte clair, et le système est d'une confidentialité parfaite.

On peut utiliser cette définition très générale pour décrire davantage ce que constitue un système à confidentialité parfaite. L'équation A.1 implique que $\mathbf{Pr}[y|x] = \mathbf{Pr}[y]$. Or, si l'élément y existe dans $\mathcal{C}$, c'est que $\mathbf{Pr}[y] > 0$ (si $\mathbf{Pr}[y] = 0$, l'élément y serait éjecté de $\mathcal{C}$). Donc, si $\mathbf{Pr}[y|x] > 0$, il existe au moins une clé K pour chaque texte clair x tel que $e_K(x) = y$. Ainsi, un système à confidentialité parfaite doit satisfaire

$$|\mathcal{K}| \geq |\mathcal{C}| \tag{A.2}$$

Puisque toute règle de déchiffrement doit faire correspondre de manière unique un texte chiffré y avec un texte clair x (règle injective), on a toujours

$$|\mathcal{C}| \geq |\mathcal{P}| \tag{A.3}$$

Dans le cas limite où $|\mathcal{P}| = |\mathcal{K}| = |\mathcal{C}|$, on peut pousser le raisonnement plus loin. L'espace $|\mathcal{C}|$ est donné par l'application de la règle de chiffrement $e_K(x)$ sur l'espace $|\mathcal{P}|$. Ainsi

$$|\mathcal{C}| = |\{e_K(x) : K \in \mathcal{K}\}| \tag{A.4}$$

$$= |\mathcal{K}| \tag{A.5}$$

Donc, dans ce cas, il n'existe pas deux clefs K_1 et K_2 distinctes telles que $e_{K_1}(x) = e_{K_2}(x) = y.$, c.à.d. qu'il n'existe qu'une clef K pour chaque texte chiffré y. En termes de probabilité, ceci équivaut à $\mathbf{Pr}[y|x] = \mathbf{Pr}[\mathbf{K} = K]$. En utilisant le théorème de Bayes, on a

$$\mathbf{Pr}[x|y] = \frac{\mathbf{Pr}[y|x]\mathbf{Pr}[x]}{\mathbf{Pr}[y]} \tag{A.6}$$

D'où, en vertu de la règle du secret parfait A.1, on tire

$$\frac{\mathbf{Pr}[K]\mathbf{Pr}[x]}{\mathbf{Pr}[y]} = \mathbf{Pr}[x] \tag{A.7}$$

Donc

$$\mathbf{Pr}[K] = \mathbf{Pr}[y] \tag{A.8}$$

Comme K peut être n'importe quel élément de $\mathcal{K}$ et que y peut être n'importe quel élément de $\mathcal{C}$, cette égalité est indépendante du texte chiffré choisi. Donc, chaque clef possède la même probabilité uniformément égale à $\mathbf{Pr}[y]$. Comme il y a $|\mathcal{K}|$ clefs, cette probabilité est de

$$\mathbf{Pr}[K] = \frac{1}{|\mathcal{K}|} \tag{A.9}$$

Inversement, on a que chaque texte chiffré est équiprobable avec $\mathbf{Pr}[y] = 1/|\mathcal{K}|$.

Cette démonstration est intéressante puisqu'elle ne fait pas intervenir la distribution de probabilité sur les textes clairs. Donc, en satisfaisant les conditions ci-hauts, le système cryptographique est *parfait* (au sens de la théorie de l'information), peu importe la distribution des textes clairs dans $\mathcal{P}$.

Annexe B

Le protocole du masque jetable

Soit l'espace des textes clairs $\mathcal{P}$ et l'espace des clefs $\mathcal{K}$. Soit un texte clair x en format binaire de longueur de n bits. Soit une clef K, également en format binaire et de longueur n, élément aléatoirement choisi dans l'espace $|\mathcal{K}|$. Dans ce cas, $|\mathcal{P}| = |\mathcal{K}| = 2^n$ et donc chaque clef K est équiprobable dans $\mathcal{K}$ avec la probabilité $1/2^n$.

Dans le protocole du masque jetable, la règle de chiffrement est simplement la somme, bit par bit du texte clair x et de la clef K (modulo 2)

$$\begin{aligned} y &= e_K(x) \\ &= x \oplus K \end{aligned}$$

où l'opération $\oplus$ désigne une somme bit par bit modulo 2. Le texte chiffré résultant est donc aussi une séquence de bits de longueur n, c.-à-d. $|\mathcal{C}| = 2^n$. La règle de déchiffrement est identique

$$\begin{aligned} d_K(y) &= y \oplus K \\ &= x \oplus (K \oplus K) \\ &= x \end{aligned}$$

où nous avons utilisé le fait que sommer deux fois un même bit sur un autre, correspond à inverser ce bit deux fois, le laissant en fait avec sa valeur initiale.

Sans être formel, on aurait pu se convaincre que le système assure une sécurité parfaite en utilisant un argument intuitif. Si l'on somme une séquence de bits totalement aléatoire sur un texte clair de la même longueur, le résultat de cette somme, le texte chiffré, est également totalement aléatoire. Un espion ne peut alors absolument rien apprendre sur le texte clair en observant le texte chiffré puisque celui-ci "masque" le texte clair.

Cependant, avec la théorie de l'information, cette intuition se confirme rigoureusement. Ce protocole satisfait alors à la définition du secret parfait puisque $|\mathcal{P}| = |\mathcal{K}| = |\mathcal{C}|$ et que $\mathbf{Pr}[K] = 1/|\mathcal{K}|$. Par conséquent, tous les textes chiffrés sont également équiprobables comme nous l'avons vu à l'annexe A.

Ce protocole est donc extrêmement attrayant. Pourtant, il comporte une faiblesse qui le rend presque inutile en pratique. En effet, chaque clef K ne peut être utilisée qu'une fois (d'où le nom"Masque jetable"). Dans ce protocole, cela s'exprime par le fait que chaque clef est aléatoirement choisie dans un ensemble comportant autant d'éléments possibles que l'espace des textes clairs. Donc, si l'on parcourt tout l'espace des textes clairs, chaque élément de l'espace des clef ne sera utilisée qu'une fois. Intuitivement, on peut voir que violer ce principe résulterait en un problème de sécurité. Si une même clef K est utilisée deux fois avec deux textes clairs x_1 et x_2, l'espion peut sommer les textes chiffrés résultants pour obtenir la somme de deux messages

$$\begin{aligned} y_1 \oplus y_2 &= (x_1 \oplus K) \oplus (x_2 \oplus K) \\ &= x_1 \oplus x_2 \oplus (K \oplus K) \\ &= x_1 \oplus x_2 \end{aligned}$$

Dans ce cas, on considère que l'espion peut assez facilement se débrouiller pour trouver

les textes clairs distincts[1].

Alors, si à chaque fois qu'Alice et Bob souhaitent se télécommuniquer un texte clair de façon sécurisée ils doivent s'échanger une nouvelle clef par un moyen absolument certain, ils ne sont pas très avancés ! Le problème est déplacé sur le fait de devoir s'échanger la clef de façon totalement sécurisée, ce qui les ramène à la case départ. Puisqu'il n'existe aucun moyen classique connu pour réaliser l'échange de la clef, ce protocole n'est utilisé que pour des applications très particulières, bien qu'il soit le seul protocole pouvant permettre la sécurité parfaite.

[1]Par exemple, il peut deviner que le début du premier texte clair est "cher général". Pour cet exemple, il obtient donc par soustraction les bits correspondants dans l'autre texte, comme "cher command". Il devine alors que cela correspond à "cher commandant", duquel il peut obtenir les lettres correspondantes dans l'autre message, et ainsi de suite jusqu'à ce que les deux messages soient complètement explicités.

Annexe C

Le protocole RSA

Contrairement au masque jetable, le protocole RSA est très couramment utilisé dans les télécommunications modernes, notamment pour les communications sécurisés sur Internet.

Nommé d'après ses inventeurs, Rivest, Shamir et Adleman (1977), le chiffrement RSA est fondamentalement différent du chiffrement par le masque jetable car il s'agit d'un protocole *asymétrique*, c.-à.-d. que les rôles d'Alice et de Bob ne sont pas interchangeables. Avec le masque jetable, les participants qui connaissent la clef sont chacun en mesure d'effectuer un chiffrement e_K et un déchiffrement d_K. Avec le protocole RSA, seul Bob connaît les deux règles e_K et d_K. Il communique la règle de chiffrement e_K publiquement de sorte qu'Alice ne connaît que celle-ci. Pour faire une analogie, c'est comme si Bob possède un coffre-fort dont lui seul a la clef et qu'il l'ouvre pour demander à Alice d'y mettre son message[1]. Alice ferme alors le coffre fort et le remet à Bob[2]. Du point de vue d'Alice (qui cherche à communiquer son message uniquement à Bob) et de Bob (qui veut s'assurer que personne à part lui

[1]En utilisant la même analogie, le masque jetable est tel qu'il existe un coffre-fort dont seuls Alice et Bob possèdent la clef. Ils sont chacun capables d'y introduire un message ou d'y retirer un message : leurs rôles sont donc *symétriques*.

[2]Notons que puisque celui-ci est "ouvert", quiconque peut alors introduire un message dans le coffre fort. Pour que le protocole fonctionne, il faut que Bob possède un moyen pour authentifier le fait que le message provient bien d'Alice

ne peut lire le message), le système est sécurisé. Par contre, cette sécurité n'est pas abosolue au sens de la théorie de l'information. En fait, si Ève possède une puissance de calcul infinie (ou suffisamment grande), il peut facilement réussir à compromettre ce système de chiffrement.

On présente ici l'essentiel du fonctionnement du protocole RSA et on tente de qualifier son niveau de sécurité.

Soit $n \equiv pq$ où p et q sont premiers. Soit $\phi(n) \equiv (p-1)(q-1)$. On note $\mathbb{Z}_n$ l'espace de tout les entiers modulo n et $\mathbb{Z}_n^*$ l'ensemble des entiers modulo n qui sont mutuellement premiers avec n. Soit $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. On définit :

$$\mathcal{K} = \{(n, p, q, a, b) : ab \bmod \phi(n) \equiv 1\}$$

Pour un ensemble $\mathcal{K}$ donné par (n, p, q, a, b), on définit les règles de chiffrement et de déchiffrement comme suit :

$$\begin{aligned} e_K(x) &\equiv x^b \bmod n \\ d_K(y) &\equiv y^a \bmod n \end{aligned}$$

où $x, y \in \mathbb{Z}_n$. Les valeurs n et b forment une *clef publique* et les valeurs p, q et a une *clef privée*. En utilisant certains éléments de la théorie des groupes, on peut montrer qu'en respectant les règles ci-dessus, les opérations de chiffrement et de déchiffrement sont bien réciproques de sorte que $d_K[e_K(x)] = x$. De plus, on affirme (sans démonstration) qu'il existe des algorithmes *efficaces* pour effectuer toute les opérations indiquées ci-dessus, c.-à.-d. que toute ces opérations sont faciles à effectuer.

Le protocole est comme suit. Bob choisit deux nombres premiers p et q, et calcule n et $\phi(n)$. Il choisit alors b et calcule a. À ce moment, Bob possède toutes les informations sur $\mathcal{K} = (n, p, q, a, b)$. Il publie ouvertement la *clef publique* (n, b). Alice utilise alors b et n pour calculer $y = e_K(x) \equiv x^b \bmod n$ et ainsi réaliser le chiffrement. Elle transmet y sur le canal. Comme seul Bob (et non Eve) connaît a, lui seul peut

effectuer le déchiffrement $x = d_K(y) \equiv y^a \bmod n$.

Un attaque évidente contre le système de chiffrement RSA est de tenter de factoriser n en deux entiers premiers (soit p et q). Si Ève réussit cela, elle aussi peut calculer $\phi(n)$ et déduire la valeur de a via la *clef publique* de la même façon que Bob l'a fait. Dans ce cas, la sécurité du système est évidemment compromise. Heureusement, la complexité calculatoire du problème de factorisation en entiers premiers croît exponentiellement avec n, de sorte qu'en pratique, cela est prohibitivement difficile pour Eve. Ainsi, la sécurité de RSA repose sur le fait que la fonction $f(p,q) \equiv pq$ est une *fonction à sens unique* puisqu'appliquer f est facile alors qu'appliquer f^{-1} ne l'est pas du tout pour des grands nombres.

Aujourd'hui, les algorithmes classiques les plus efficaces pour factoriser n sont des algorithmes utilisant les règles des groupes elliptiques. Le plus puissant de tous est connu sous le nom de *crible algébrique*. Cet algorithme possède une complexité donnée par :

$$\mathcal{O}\left(e^{(1,92+O(1))(\ln n)^{1/3}(\ln \ln n)^{2/3}}\right)$$

En fonction de la taille de n, cette complexité est tracée sur la figure C.1. On quantifie généralement la taille de n en fonction du plus grand nombre pouvant être représenté en code binaire de m bits. Ainsi, on parle souvent d'encryption RSA 128 bits ou 512 bits. On voit sur le graphique que la complexité de calcul croît sous-exponentiellement pour n suffisamment grand.

En 2000, Cavallar et al. [19] ont réussi une factorisation d'une clé de 512 bits en 8400 MIPS-années[3] en utilisant 300 ordinateurs répartis dans six pays. Aujourd'hui (en 2006), un processeur moderne tel que le *Core 2 Extreme* d'Intel possède un pouvoir de calcul de 61 119 MIPS lorsque cadencé à 3.33 GHz. Ainsi, il prendrait environ 51 jours pour un ordinateur personnel commercialement disponible à prix raisonnable, équipé de ce processeur, pour factoriser un nombre dans un espace binaire à 512 bits.

[3]L'unité MIPS-années représente le nombre d'instructions exécutés pendent une année à une cadence d'un million d'instructions à la seconde.

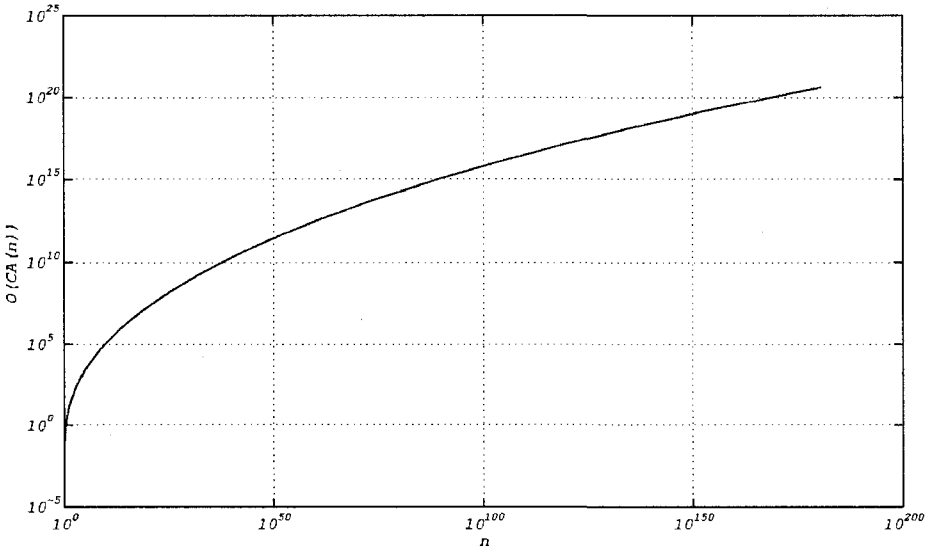


FIG. C.1 – Complexité de l'algorithme du *Crible Algébrique* en fonction de la taille de n.

Cela montre que la sécurité d'un chiffrement RSA n'est pas nécessairement très forte et n'est que temporaire. Si, aujourd'hui Alice et Bob s'échangent un texte clair x via un texte chiffré par RSA 512 bits y, Eve peut intercepter et conserver en mémoire y le temps que sont ordinateur personnel factorise n. Elle peut alors apprendre le texte clair x, avec quelques dizaines de jours de retard sur Bob. Si le texte clair contenait des informations encore utiles après ce délai (par exemple, le mot de passe vers un compte bancaire encore actif), Alice et Bob seront malmenés !

En fait, avec le progrès constant dans la puissance de calcul des ordinateurs, il devient nécessaire de constamment augmenter la taille de n. Cependant, il existe un algorithme de factorisation contre lequel même l'augmentation de n ne peut assurer la sécurité. Il s'agit de l'algorithme de Shor qui ne peut s'appliquer que si Ève possède un ordinateur quantique. Cet algorithme possède une complexité qui n'est pas du tout exponentielle avec n mais qui est sous-linéaire : $\mathcal{O}((\log n)^3)$! Autrement dit, cet algorithme compromet totalement la sécurité de tout protocole RSA. Puisque l'ordinateur quantique sera presque certainement une réalité au cours de la première

moitié du 21e siècle, on peut affirmer que le protocole RSA ne sera plus utilisable dans un avenir relativement proche.

De plus, on ne peut exclure qu'un algorithme ou même une méthode analytique puisse être découverte qui permettrait de facilement factoriser n. Si tel est le cas, la sécurité de la majorité des transactions par Internet serait compromise du jour au lendemain.

Ainsi, la sécurité d'un protocole RSA peut-être décrite comme *temporairement acceptable*. Pour cette raison, il est impératif de (1) trouver d'autres méthodes de chiffrement plus robustes ou (2) trouver un façon de rendre l'utilisation du masque jetable praticable. Or, c'est justement ce que la QKD permet, en rendant possible l'échange de clefs privées à distance.

Annexe D

Éléments d'optique quantique

La physique quantique décrit plusieurs effets qui peuvent être utiles pour construire un système cryptographique très puissant, entre autres. L'informatique quantique, dont la cryptographie quantique est un exemple, est basée sur la nature discrète des états quantiques de la matière et du rayonnement (ce qui offre une base de codage pour l'information), et de la manipulation de ces états. On nomme *qubit* tout objet dont l'état quantique est représentatif d'une information. Bien que tout état quantique permette théoriquement la réalisation d'un *qubit*, c'est le rayonnement électromagnétique qui est généralement utilisé comme médium de transmission pour l'information quantique. Il s'agit de *qubit*s optiques.

Nous traitons ici de quelques notions d'optique quantique intéressantes en cryptographie quantique, suivant une démarche inspirée de [20].

Les états nombre

Pour décrire les *états nombre*, il convient de décrire l'oscillateur harmonique en mécanique quantique, tel qu'il est utile pour décrire l'Hamiltonien d'un champs électromagnétique.

Considérons un champ électrique dans une cavité de volume V avec des parois par-

faitement conductrices, sans sources, charges, ni courants. Dans ce cas, les équations de Maxwell admettent les solutions modales suivantes pour les champs électriques et magnétiques,

$$E(z,t) = \left(\omega^2 m/2V\varepsilon_0\right)^{1/2} q(t) \sin kz \tag{D.1}$$

$$H(z,t) = \left(\frac{\varepsilon_0}{k}\right) \left(\omega^2 m/2V\varepsilon_0\right)^{1/2} \frac{dq(t)}{dt} \cos kz \tag{D.2}$$

où k est le nombre d'onde qui désigne le mode. L'énergie de ce mode est donnée par la fonction Hamiltonienne $\mathcal{H}$

$$\mathcal{H} = \frac{1}{2} \int dV \left[\varepsilon_0 E^2 + \mu_0 H^2\right] \tag{D.3}$$

Pour le mode en question, en posant $p = mdq/dt$, l'Hamiltonien donne

$$\mathcal{H} = \frac{1}{2} m\omega^2 q^2 + \frac{p^2}{2m} \tag{D.4}$$

que l'on reconnait comme la forme de l'Hamiltonien de l'oscillateur harmonique. Puisque tout champ électromagnétique peut être décrit comme une superposition des modes d'une cavité, on peut se contenter de déterminer le comportement quantique d'un oscillateur harmonique afin de pouvoir écrire les modes quantiques d'un champ qui pourront également servir de base pour tout champ quantique. En mécanique quantique, en utilisant le formalisme de Heisenberg, on effectue la quantification de l'oscillateur en se dotant des opérateurs suivants

$$q \rightarrow \hat{q} \tag{D.5}$$

$$p \rightarrow \hat{p} \tag{D.6}$$

tels que $[\hat{q}, \hat{p}] = j\hbar$. De plus, il convient de définir les opérateurs suivants

$$\hat{a} = (2m\hbar\omega)^{-1/2}(m\omega\hat{q} + j\hat{p}) \tag{D.7}$$

$$\hat{a}^\dagger = (2m\hbar\omega)^{-1/2}(m\omega\hat{q} - j\hat{p}) \tag{D.8}$$

tel que $\left[\hat{a}, \hat{a}^\dagger\right] = 1$. On montre alors que l'opérateur Hamiltonien s'écrit

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right) \tag{D.9}$$

On démontre facilement que

$$\left[\hat{H}, \hat{a}\right] = -\hbar\omega\hat{a} \tag{D.10}$$

$$\left[\hat{H}, \hat{a}^\dagger\right] = \hbar\omega\hat{a}^\dagger \tag{D.11}$$

Soit un état $|n\rangle$, état propre de l'opérateur Hamiltonien avec la valeur propre (l'énergie) E_n

$$\hat{H}|n\rangle = E_n|n\rangle \tag{D.12}$$

On a

$$\begin{aligned}\hat{H}\hat{a}|n\rangle &= \left(\left[\hat{H}, \hat{a}\right] + \hat{a}\hat{H}\right)|n\rangle \\ &= \left(-\hbar\omega\hat{a} + \hat{a}E_n\right)|n\rangle \\ &= \left(E_n - \hbar\omega\right)\hat{a}|n\rangle\end{aligned}$$

Similairement

$$\hat{H}\hat{a}^\dagger|n\rangle = \left(E_n + \hbar\omega\right)\hat{a}^\dagger|n\rangle \tag{D.13}$$

On voit donc que l'application des l'opérateurs $\hat{a}$ et $\hat{a}^\dagger$ sur un état propre de l'opérateur Hamiltonien a pour effet de produire un nouvel état dont l'énergie est abaissée ou rehaussée de $\hbar\omega$, respectivement. Pour cette raison, l'opérateur $\hat{a}$ est appelé *opérateur*

annihilation et $\hat{a}^\dagger$ est appelé *opérateur création.* Également, on remarque que les niveaux d'énergie de l'oscillateur harmonique sont séparés de $\hbar\omega$. Pour clarifier ce point dans la notation, on pose

$$\hat{a}|n\rangle \equiv C_n|n-1\rangle \tag{D.14}$$

$$\hat{a}^\dagger|n\rangle \equiv C_{n+1}|n+1\rangle \tag{D.15}$$

où C_n est une constante de normalisation que l'on montre égale à $C_n = \sqrt{n}$. Soit $|0\rangle$, l'énergie du niveau fondamental avec l'énergie E_0. On a

$$\hat{H}\hat{a}|0\rangle = (E_0 - \hbar\omega)\,\hat{a}|0\rangle$$

Comme il ne peut exister un niveau d'énergie inférieur au niveau fondamental, on trouve que $E_0 = \frac{1}{2}\hbar\omega$ et

$$E_n = \left(n + \frac{1}{2}\right)\hbar\omega \tag{D.16}$$

Soit $\hat{n}$ l'opérateur donné par le produit de l'opérateur création et annihilation

$$\hat{n} \equiv \hat{a}^\dagger\hat{a} \tag{D.17}$$

En vertu de l'équation D.16 et des propriétés de $\hat{a}^\dagger$ et $\hat{a}$, on a que :

$$\hat{n}|n\rangle = n|n\rangle \tag{D.18}$$

Puisque cet opérateur a pour état propre $|n\rangle$ avec la valeur propre n, on nomme $\hat{n}$ *opérateur nombre.* Celui-ci retourne le nombre de quanta dans un état propre de l'oscillateur harmonique. De plus, ceci justifie de nommer l'état $|n\rangle$ *état nombre.*

Nous avons établi ci-dessus que l'oscillateur harmonique et ses états propres peuvent décrire (en les superposant) tout champ électromagnétique. En se référant à

l'équation D.1, on trouve que l'opérateur pour ce champ électrique peut s'écrire

$$\begin{aligned}\hat{E}(z,t) &= \left(\omega^2 m/2V\varepsilon_0\right)^{1/2} \hat{q}(t) \sin kz \\ &= \left(\omega^2 m/2V\varepsilon_0\right)^{1/2} \left[\hat{a} + \hat{a}^\dagger\right] \sin kz\end{aligned}$$

Nous avons donc un formalisme par lequel on peut décrire tout champ électromagnétique quantifié. En particulier, nous avons montré que l'état $|n\rangle$ est l'élément d'une base qui peut décrire tout champ. Cette base, notée $\{|n_k\rangle\}$ est nommée *base de Fock*. On peut obtenir les éléments de la base par application successive de l'opérateur création sur l'état fondamental

$$|n_k\rangle = \frac{\left(\hat{a}_k^\dagger\right)^{n_k}}{\sqrt{n_k!}}|0\rangle \tag{D.19}$$

Si l'on définit le *photon* comme un quantum d'énergie électromagnétique (sans démontrer formellement qu'il s'agit d'une particule), alors les éléments de la base de Fock sont des états ayant un nombre déterministe de photons.

Les états nombre possèdent quelques propriétés intéressantes :

1. L'opérateur $\hat{n}$ ne commute pas avec l'opérateur champ électrique c.-à-d. que le champ électrique et le nombre de photons ne peuvent être connus simultanément ;

2. L'amplitude du champ, A, est fixée par le nombre de photons

$$A = \frac{\hbar\omega_k}{\varepsilon_0 V}\left(n + \frac{1}{2}\right) \tag{D.20}$$

3. Si l'on prend un très grand nombre de mesures d'un même champ E, la variance dans ces mesures, σ_E^2, sera égale à l'amplitude du champ au carré

$$\sigma_E^2 = A^2 \tag{D.21}$$

4. Si l'on prend un très grand nombre de mesures d'un même champ E, la moyenne

est nulle

$$\begin{aligned} \langle n|\hat{E}|n\rangle &\propto \langle n|\hat{a}(t)|n\rangle + \langle n|\hat{a}^{\dagger}(t)|n\rangle \\ &= 0 \end{aligned}$$

Ces propriétés peuvent paraître former un paradoxe. Or, on résout ce paradoxe en considérant que la phase de l'oscillateur qu'est l'état nombre est aléatoire. Chaque oscillateur a une amplitude donnée par l'équation D.20, possède exactement n photons et d'une mesure du champ à l'autre la phase est totalement aléatoire. Ainsi, chaque mesure nous donne un point sur une courbe sinusoïdale d'amplitude A. En prenant plusieurs mesures, la phase varie aléatoirement et on finie par parcourir la pleine portée de l'amplitude de la sinusoïde : l'amplitude du champ s'exprime via la variance de ces mesures et la moyenne des mesures est nulle. Dans ce contexte, la propriété #1 découle logiquement puisque la mesure du champ ne donne pas à coup sûr l'amplitude du champ (et donc n) avec une seule mesure.

En fait, de manière générale en mécanique quantique, on a la relation d'incertitude suivante (qui découle de la relation d'incertitude d'Heisenberg)

$$\Delta E \Delta t \geq \hbar/2 \tag{D.22}$$

$$(\hbar\omega\Delta n)\left(\frac{\Delta\phi}{\omega}\right) \geq \hbar/2 \tag{D.23}$$

$$\Rightarrow \Delta n \Delta\phi \geq 1/2 \tag{D.24}$$

Cette relation implique que pour l'état nombre où $\Delta n = 0$, la phase est totalement indéterminée : $\Delta\phi \to \infty$.

Cela implique que *l'état nombre ne peut porter de l'information quantique dans sa phase.* En effet, pour traduire la phase en information, on doit en pratique opérer une interférence pour traduire la phase en amplitude. Or, la phase étant totalement aléatoire, l'opération donnera un résultat totalement aléatoire, indépendamment de

la manière dont on a préparé l'état nombre. Dans les schémas de cryptographie quantique comme BB84, l'état nombre est donc *inutile* comme *qubit*.

L'état cohérent

Le formalisme de l'état nombre permet cependant de décrire un état quantique qui peut permettre l'existence des opérations informatiques des protocoles du type BB84. Il s'agit de *l'état cohérent*, aussi appelé état *semi-classique* car ces états peuvent servir de base pour décrire les phénomènes de l'optique classique.

L'état cohérent, noté $|\alpha\rangle$, est un état propre de l'opérateur annihilation[1]

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \tag{D.25}$$

où α est un nombre complexe (puisque $\hat{a}$ est non-hermitien). Puisque

$$\langle n|\hat{a} = \sqrt{n+1}\langle n+1| \tag{D.26}$$

on a la relation de récurrence suivante,

$$\sqrt{n+1}\langle n+1|\alpha\rangle = \alpha\langle n|\alpha\rangle \tag{D.27}$$

d'où on peut tirer

$$\langle n|\alpha\rangle = \frac{\alpha^n}{\sqrt{n!}}\langle 0|\alpha\rangle \tag{D.28}$$

[1]Ainsi, si l'on mesure de la lumière en état cohérent par un processus *d'absorption* de photons, ce processus laisse la lumière dans le même état cohérent. Les états céhérents sont donc facilement observables via un détecteur optique tel une photodiode.

En insérant la relation de fermeture des états nombres (non-démontrée), il vient que

$$|\alpha\rangle = \sum_{n=0}^{\infty} |n\rangle\langle n|\alpha\rangle \tag{D.29}$$

$$= \langle 0|\alpha\rangle \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{D.30}$$

où $\langle 0|\alpha\rangle$ joue le rôle d'une constante de normalisation. La normalisation est satisfaite lorsqu'on choisit

$$\langle 0|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \tag{D.31}$$

Décomposée sur la base des états nombres, l'état cohérent s'écrit donc

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{D.32}$$

Il est facile de montrer que le nombre moyen de photons dans un état cohérent est

$$\langle n\rangle = \langle\alpha|\hat{n}|\alpha\rangle \tag{D.33}$$

$$= |\alpha|^2 \tag{D.34}$$

De plus, on montre que la variance dans le nombre de photons est

$$(\Delta n) = \langle n^2\rangle - \langle n\rangle^2 \tag{D.35}$$

$$= |\alpha|^2 \tag{D.36}$$

On en déduit que l'état cohérent possède un nombre non-déterministe de photons, mais possède plutôt une distribution de probabilité sur le nombre de photons. Cette distribution est donnée par

$$\mathcal{P}(n) = |\langle n|\alpha\rangle|^2 \tag{D.37}$$

$$= \frac{|\alpha|^{2n}}{n!} e^{-|\alpha|^2} \tag{D.38}$$

On voit donc que l'état cohérent est un état qui possède une distribution de Poisson sur le nombre de photons, avec la valeur moyenne et la variance égales à $|\alpha|^2$.

Puisque l'état cohérent n'est pas un état propre de l'opérateur Hamilitonien, celui-ci évolue dans le temps. Cependant, on montre que vis-à-vis l'opérateur annihilation, l'état cohérent reste cohérent, mais sa valeur propre évolue dans le temps à la façon d'une onde se propageant dans le temps

$$\hat{a}|\alpha(t)\rangle = e^{-j\omega t}|\alpha||\alpha(t)\rangle \tag{D.39}$$

Ceci justifie l'appelation "état cohérent" car l'état se propage dans le temps sans se modifier, tout comme un oscillateur classique. Pour cette raison, cet état décrit fidèlement l'oscillateur optique qu'est le laser stabilisé au dessus de son seuil de fonctionnement. Ainsi, *l'état cohérent décrit, d'un point de vue quantique, la radiation d'un laser.*

Également, puisque $\Delta n \neq 0$, l'état cohérent possède une phase non aléatoire : $\Delta n \in \mathbb{R}$ (tel qu'il se doit si l'état cohérent doit décrire le rayonnement laser). Pour cette raison, il est raisonnable d'utiliser des états cohérents dans des schémas d'information quantique où l'on souhaite coder l'information dans la phase : l'opération d'interférence donne un résultat prévisible, bien que probabiliste.

Finalement, notons qu'il est possible de montrer que l'état cohérent correspond à une onde électrique classique avec l'amplitude proportionnelle à $|\alpha|$

$$E = \sqrt{\frac{2\hbar\omega}{\varepsilon_0 V}}|\alpha| \tag{D.40}$$

Ainsi, il est facile, en pratique, de fixer le paramètre $|\alpha|$ (qui décrit totalement l'état cohérent) : on n'a qu'à contrôler l'intensité d'une onde laser. Pour cela, les choix technologiques abondent.

Annexe E

Effets thermiques et élastiques dans les fibres optiques

L'effet thermo-optique

L'indice de réfraction d'un matériau est généralement variable avec la température, c.-à-d. $n = n(T)$, ce que l'on peut désigner comme l'effet thermo-optique. En tenant compte de cet effet, l'indice de réfraction réél d'un matériau peut s'écrire

$$n(T - T_0) = n(T_0) + \frac{dn}{dT}[T - T_0] \tag{E.1}$$

Cette relation équivaut à effectuer un développement de Taylor d'ordre 1 de la fonction décrivant l'indice de réfraction en fonction de la température autour de la température de référence T_0. Pour de petites valeurs de $\Delta T = T - T_0$, le développement de Taylor tronqué au premier ordre est généralement admis comme une excellente approximation de la fonction $n(T)$.

Ainsi, chaque matériau est caractérisé par un *coefficient thermo-optique*, soit dn/dT.

L'effet élasto-optique

En plus de varier avec la température, l'indice de réfraction est également fonction des contraintes dans un matériau. Ceci est l'effet élasto-optique.

Nous suivons ici la théorie résumée dans [18] par Rashleigh.

On peut décrire l'effet élasto-optique au moyen du *coefficient élasto-optique*, qui, dans le cas d'une fibre optique est donnée par :

$$\frac{C_s}{k_0} = \frac{1}{2} n_0^3 \left(p_{11} - p_{12}\right)\left(1 + \nu_p\right) \tag{E.2}$$

où ν_p est le coefficient de Poisson, p_{11} et p_{12} sont les éléments non-nuls du tenseur élasto-optique, n_0 est l'indice de réfraction moyen de la fibre. Toutes ces propriétés sont sensibles uniquement aux matériaux qui composent la fibre.

Les propriétés de biréfringence d'une fibre sont directement reliées à cet effet. En effet, tout ce qui impose une contrainte sur la fibre modifie son indice de réfraction. En particulier, si les contraintes sont non-symétriques dans le plan perpendiculaire à l'axe de la fibre, l'indice de réfraction de la fibre ne sera pas uniforme dans ce plan. Dans ce cas, l'indice de réfraction sera fonction de la direction de la polarisation de la lumière qui se propage dans la fibre et la fibre sera donc biréfringente.

En fonction du moyen utilisé pour l'installer, ou en fonction simplement de la forme que l'on donne à la fibre, celle-ci a une biréfringence très différente. Cependant, on peut tenter de classifier les mécanismes de biréfringence (incluant les mécanismes reliés aux contraintes) comme on le voit à la figure E.1. On voit, sur cette figure, que diverses manières de fabriquer des fibres optiques avec des cœurs pré-contraints par exemple, mènent à des fibres intrinsèquement biréfringentes. De plus, pour une fibre n'ayant aucune pré-contrainte, le fait de la courber ou de l'installer de diverses manières mène à une biréfringence. Finalement, la présence d'un fort champ magnétique ou électrique peut également mener à la biréfringence.

Pour les différents mécanismes présentés de la figure E.1, on peut donner la

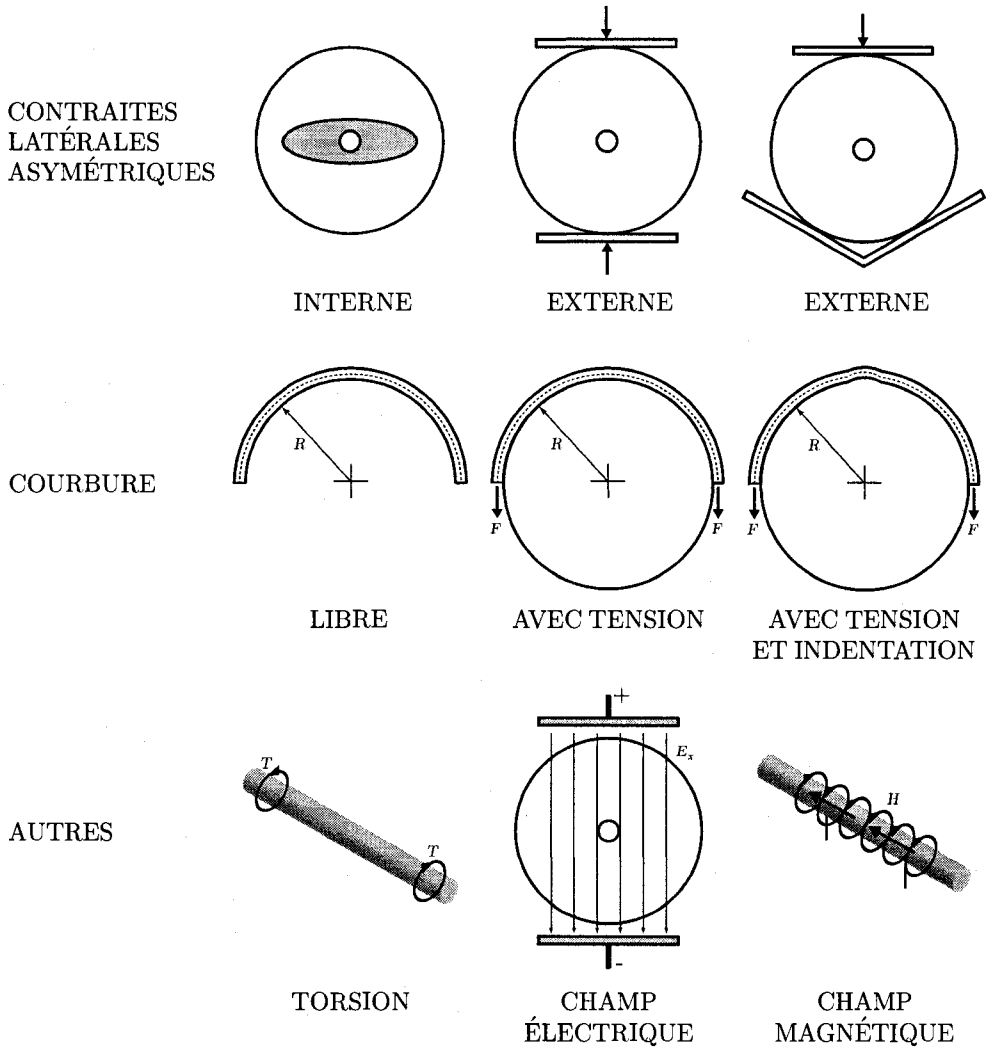


FIG. E.1 – Classification de Rashleigh des mécanismes de biréfringence dans une fibre optique.

biréfringence associée en fonction du coefficient élasto-optique. Spécifions la biréfringence pour les cas suivants :

- Biréfringence de courbure (libre) :

$$\beta_b = C_s \frac{r^2}{2R^2} \tag{E.3}$$

où R est le rayon de courbure de la fibre et r est le rayon de la section transversale de la fibre.

- Biréfringence de courbure (avec tension) :

$$\beta_{bt} = C_s \frac{2 - 3\nu_p}{1 - nu_p} \left(\frac{r}{R}\right) \left(\frac{F}{\pi r^2 E}\right) \tag{E.4}$$

où $F/\pi r^2 E$ est la contrainte moyenne axiale appliquée sur la fibre.

- Biréfringence reliée à l'application d'une pression sur la fibre dans un *coin en V* :

$$\beta_V = 2C_s \left(1 - \cos 2\delta \sin \delta\right) \frac{f}{\pi r E} \tag{E.5}$$

où 2δ est l'angle d'ouverture du *coin en V* et f est la force appliquée latéralement.

- Biréfringence de torsion :

$$\beta_\tau = -\frac{1}{2} n_0^2 \left(p_{11} - p_{12}\right) \tau \tag{E.6}$$

où β_τ est la biréfringence circulaire induite par la torsion reliée à τ tours/m.

Annexe F

Le programme ParamInterf.m

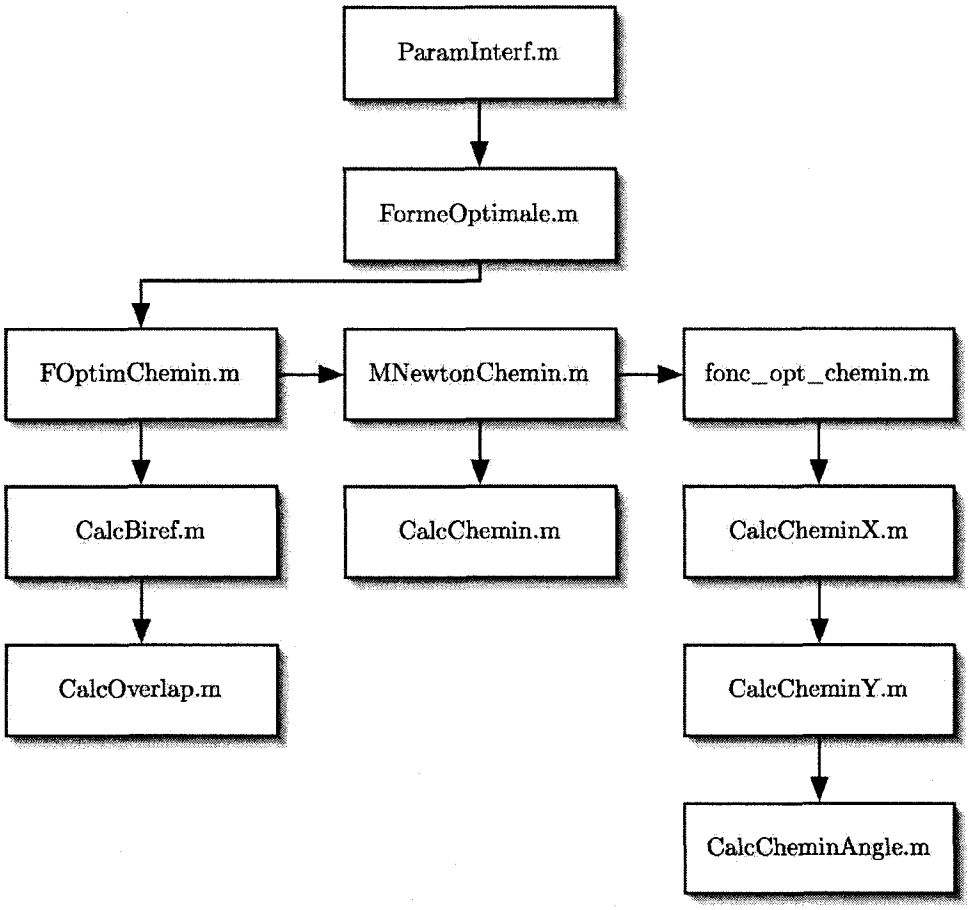


FIG. F.1 – Arborescence du programme ParamInterf.m

ParamInterf.m

```
% ParamInterf.m

freq = 100e6;

R = 0.9;        % rapport des dn/dT
delta_L = 299792458/(freq*1.4682)

%L_SMF = delta_L/(1-R)
%L_COR = delta_L*(2-R)/(1-R)
L_SMF = delta_L*(R)/(1-R);
L_COR = delta_L/(1-R);
```

```
% L1 = delta_L/(1-R)+0.2
% L2 = delta_L*(2-R)/(1-R)+0.2
L1 = L_SMF-0.2;
L2 = L_COR-0.2;

n1 = [1:100];
n2 = [1:100];

% L1 = 10;
% L2 = 11.11;

for i = 1:length(n1)
    for j = 1:length(n2)
        if n1(i)~=n2(j)
            X(i,j) = (L2-L1)./(pi*(n2(j)-n1(i)));
            ell(i,j) = L1 - n1(i)*pi*X(i,j);
        else
            X(i,j) = 0;
            ell(i,j) = 0;
        end
        if X(i,j) < 0
            X(i,j) = 0;
            ell(i,j) = 0;
        end
    end
end

[ind_poss1, ind_poss2] = find(ell<=0.4 & ell>0.01);

for i = 1:length(ind_poss1)
    ell_poss(i,1) = ell(ind_poss1(i), ind_poss2(i));
    X_poss(i,1) = X(ind_poss1(i), ind_poss2(i));
    n1_poss = ind_poss1;
    n2_poss = ind_poss2;
end

tab_res = [n1_poss, n2_poss, X_poss, ell_poss]

disp(['nb. possibilites = ' num2str(length(n1_poss))])

disp(' ')
sol = input('Quelle solution analyser ?')
disp(' ')
```

```
x_op = [];
y_op = [];
alpha = [];
F = [];
delta_phi_biref = [];
delta_phi_biref_i = [];

X_comp = [0.3533, 0.1767, 0.1178, 0.0883];
Sigma0 = [3.755e-6, -8.6e-6, -10e-10; 5.7e-6, -6.5e-5,
-2.1e-7; 5.9e-6, -0.0002, -9.6e-7; 4.7e-6, -0.00046, -2.6e-6];


for i=sol
    disp(['Optimisation de la solution ' num2str(i)])
    CI_op = find(abs(X_comp - X_poss(i))==min(abs(X_comp - X_poss(i))));
    Sigma0_op = Sigma0(CI_op,:);
    [x_opi,y_opi,alphai,Fi,diff_phase_tot_i,diff_phase_i,exit_flag] =
     FormeOptimale(n1_poss(i), n2_poss(i), Sigma0_op, X_poss(i));
    x_op = [x_op;x_opi];
    y_op = [y_op;y_opi];
    alpha = [alpha;alphai];
    F = [F;Fi];
    delta_phi_biref = [delta_phi_biref; diff_phase_tot_i];
    delta_phi_biref_i = [delta_phi_biref_i; diff_phase_i];
end

% GRAPHES

disp(['La forme optimale pour la solution ' int2str(sol) ' a un dephasage de birefringence de '
num2str(delta_phi_biref/(2*pi)) ' longueurs de battements.'])
% figure
% hold on
% bar(X_poss(sol), delta_phi_biref/(2*pi))
% xlabel('Rayon equivalent [m]')
% ylabel('Nb. longueurs de battement [rad]')
% grid on

% trouver meilleure solution

i_meil = find(delta_phi_biref == min(delta_phi_biref));
x_f = x_op(i_meil,:);
y_f = y_op(i_meil,:);
```

```
F_f = F(i_meil,:);


% Calcul de son contraste possible


%wt = linspace(0,2*pi,200);

%for i=1:length(F(i_meil,:))
%    phi_1trs = delta_phi_biref_i(i_meil,i)/(n2_poss(i_meil) - n1_poss(i_meil));
%    x_e1 = cos(wt);
%    y_e1 = cos(wt - n1_poss(i_meil)*phi_1trs);
%    x_e2 = cos(wt);
%    y_e2 = cos(wt - n2_poss(i_meil)*phi_1trs);
%    C(i) = 10*log10(sum((x_e1-x_e2).^2 + (y_e1-y_e2).^2)/sum((x_e1+x_e2).^2 + (y_e1%+y_e2).^2));
%end

% Calcul de la tolérance sur les dimentions de l'enroulement
i_tol = [];
i_min = find(F_f==min(F_f));
for i=1:i_min-1
    if C(i_min-i)<-20
        i_tol = [i_tol;i_min-i];
    else
        break
    end
end
i_tol = sort(i_tol);
i_tol = [i_tol; i_min];
for i=1:(length(F_f)-i_min)
    if C(i_min+i)<-20
        i_tol = [i_tol;i_min+i];
    else
        break
    end
end
dim_y_tol = alpha(i_meil,i_tol).*X_poss(sol);
tolerance = (max(dim_y_tol') - min(dim_y_tol'))/2;

% Graphe de la meilleure solution

figure
hold on
```

```
plot(x_f, y_f)
plot(-x_f,y_f)
grid on
title('Forme optimale [m]')
axis equal

figure
hold on
plot(alpha(i_meil,:).*X_poss(sol), C, '-b')
% plot(alpha(i_meil,:).*X_poss(sol), F_f, '-k')
plot([max(y_f) max(y_f)], [0 -50], '--b')
grid on
xlabel('Dimention verticale [m]')
ylabel('Contraste')
title('Tolerance')

% Informations pour enrouler carré (avec tension)

Circ = pi*X_poss(sol);          % circomférence de l'enroulement (équivalent)
Circ_poteau = pi*31.9/1000;     % circomférence des poteaux de l'enroulement (réel, mesuré)
a = (Circ - Circ_poteau)/4;     % taille d'un coté (droit) du "carré"
b = sqrt(2)*a;                  % diagonale du carré, jusqu'au bord des poteaux.


% Sauvegarder les paramètres importants de la solution

% Soit: x_f, y_f, tab_res(sol,:), alpha(i_meil,:).*X_poss(sol), min(C(i))

disp('CARACTERISTIQUES DE LA SOLUTION ')
disp('-------------------------------------------------------------------------')
disp(['Frequence de fonctionnement:' num2str(freq/1e6) ' MHz'])
disp(['Longueur des branches: L1 = ' num2str(L1) ' m, L2 = ' num2str(L2) ' m'])
disp(['Diametre equivalent de l''enroulement: X =' num2str(100*X_poss(sol)) ' cm'])
disp(['Diagonale du carré d''enroulement sous tension =' num2str(100*b) ' cm (par rapport au
centre des poteaux)'])
disp(['Diagonale du carré d''enroulement sous tension =' num2str(100*(b-31.9/1000)) ' cm (bord de
poteau à bord de poteau)'])
disp(['Hauteur de l''enroulement = ' num2str(100*alpha(i_meil,find(C==min(C))).*X_poss(sol)) '
cm +/- ' num2str(100*tolerance) ' cm'])
disp(['Largueur de l''enroulement = ' num2str(200*max(x_f)) ' cm'])
disp(['Longueur non enroulee: l = ' num2str(100*ell_poss(sol)) ' cm'])
disp(['Nb. tours: n1 = ' num2str(n1_poss(sol)) ', n2 = ' num2str(n2_poss(sol)) ])
disp(['Contraste potentiel: ' num2str(abs(min(C))) ' dB'])
```

```
disp(['Nb. de battements de birefringence sur un tour: ' num2str(delta_phi_biref/(2*pi))])
disp('--------------------------------------------------------------------------')

n1 = n1_poss(sol);
n2 = n2_poss(sol);
diam_eq = X_poss(sol);
H_enroul = alpha(i_meil,find(C==min(C))).*X_poss(sol);
Tol_H_enroul = tolerance;
L_enroul = 2*max(x_f);
l_non_enroul = ell_poss(sol);
C_pot = abs(min(C));
Nb_batt = delta_phi_biref/(2*pi);

filename = ['Sol_D_' num2str(100*diam_eq,2) '.mat'];

save('filename', 'freq', 'L1', 'L2', 'n1', 'n2', 'diam_eq', 'H_enroul', 'Tol_H_enroul', 'L_enroul',
'l_non_enroul', 'C_pot', 'Nb_batt', 'x_f', 'y_f')
```

FormeOptimale.m

```
function [x_op,y_op,alpha, F, diff_phase_tot, diff_phase_i, exit_flag] = FormeOptimale(N_trs_1,
N_trs_2, Sigma0, X_r)

% % Pour X 1
% N_trs_1 = 9;
% N_trs_2 = 10;
% M0 = 3.755e-6;
% N0 = -8.6e-6;
% T0 = -10e-10;
% Sigma0 = [M0, N0, T0];
% X_r = 0.3533;

% % Pour X 2
% N_trs_1 = 18;
% N_trs_2 = 20;
% M0 = 5.7e-6;
% N0 = -6.5e-5;
% T0 = -2.1e-7;
% Sigma0 = [M0, N0, T0];
% X_r = 0.1767;

% % Pour X 3 et 4
```

```
% N_trs_1 = 27;
% N_trs_2 = 30;
% M0 = 5.9e-6;
% N0 = -0.0002;
% T0 = -9.6e-7;
% Sigma0 = [M0, N0, T0];
% X_r = 0.1178;

% % Pour X 5 et 6
% N_trs_1 = 36;
% N_trs_2 = 40;
% M0 = 4.7e-6;
% N0 = -0.00046;
% T0 = -2.6e-6;
% Sigma0 = [M0, N0, T0];
% X_r = 0.0883;

% % Pour X 7 et 8
% N_trs_1 = 44;
% N_trs_2 = 50;
% M0 = 2e-6;
% N0 = -0.00086;
% T0 = -5.58e-6;
% Sigma0 = [M0, N0, T0];
% X_r = 0.0883;



wt = linspace(0,2*pi,100);

alpha = linspace(0.3,0.9, 200);
% alpha = linspace(0.4,0.9, 200); % original

for i=1:length(alpha)
    [x,y,exit_flag] = F0ptimChemin(X_r, alpha(i), Sigma0);
    [delta_phase, beta_eq] = CalcBiref(x,y);
    delta_phase_1tr = 2*delta_phase;
    beta_eq_tot = 2*beta_eq;
    delta_phase_tot1(i) = N_trs_1*delta_phase_1tr;
    delta_phase_tot2(i) = N_trs_2*delta_phase_1tr;
    diff_phase_i(i) = delta_phase_tot2(i) - delta_phase_tot1(i);
    x_e1 = cos(wt);
    y_e1 = cos(wt-delta_phase_tot1(i));
```

```
    x_e2 = cos(wt);
    y_e2 = cos(wt-delta_phase_tot2(i));

    F(i) = CalcOverLap(x_e1,y_e1,x_e2,y_e2);

    if i==round(0.25*length(alpha));
        disp('25 %')
    end
    if i==round(0.50*length(alpha));
        disp('50 %')
    end
    if i==round(0.75*length(alpha));
        disp('75 %')
    end
    if i==round(length(alpha));
        disp('100 %')
    end

end

i_optim = find(F==min(F));
x_e1_op = cos(wt);
y_e1_op = cos(wt-delta_phase_tot1(i_optim));
x_e2_op = cos(wt);
y_e2_op = cos(wt-delta_phase_tot2(i_optim));

diff_phase_tot = delta_phase_tot2(i_optim) - delta_phase_tot1(i_optim);

[x_op,y_op,exit_flag] = FOptimChemin(X_r, alpha(i_optim), Sigma0);
%
% % Graphe
%
%
% % Forme optimale
%
% figure
% hold on
% plot(x_op, y_op)
% plot(-x_op, y_op)
% grid on
% axis equal
%
%
```

```
% figure
% hold on
% plot(x_e1_op, y_e1_op, '--b')
% plot(x_e2_op, y_e2_op, '-b')
% axis equal
% grid on
```

FOptimeChemin.m

```
function [x,y,exit_flag] = FOptimChemin(X_r, alpha, Sigma0)

L = pi*X_r/2;           % longueur de fibre en m
pts = 1000;     % nb de points sur la longueur de la fibre

% Défintion du point final

x_f = 0;
y_f = (alpha)*X_r;


% Définition de l'angle final (dans le plan cartérien avec la définition
% habituelle: sens anti-horaire par rapport à y = 0)

angle_f = 180;

if angle_f>90
    angle_f = angle_f-180;      % pente finale (dans le premier quadrant)
end

% recherche de la solution

[SigmaF, exit_flag] = MNewt_chemin(Sigma0, 1e-9, 1e-8, 30, L,pts, [x_f y_f angle_f]);

% Résultat

[Chemin_f, MNT] = CalcChemin(SigmaF, L,pts);
x = Chemin_f(1,:);
y = Chemin_f(2,:);
```

MNewt_Chemin.m

```
function [Sol, exit_flag] = MNewt_chemin(X0, eps_x,eps_f, N_trial, L,pts, CondF)

X = X0';     % pt. de départ de l'algorythme de recherche

for i_trial = 1:N_trial

    % Définition de la matrice Jacobienne

    F_M_1 = func_optim_chemin([X(1)-X(1)/(2*pts), X(2), X(3)], L, pts, CondF);
    F_M_2 = func_optim_chemin([X(1)+X(1)/(2*pts), X(2), X(3)], L, pts, CondF);

    F_N_1 = func_optim_chemin([X(1), X(2)-X(2)/(2*pts), X(3)], L, pts, CondF);
    F_N_2 = func_optim_chemin([X(1), X(2)+X(2)/(2*pts), X(3)], L, pts, CondF);

    F_T_1 = func_optim_chemin([X(1), X(2), X(3)-X(3)/(2*pts)], L, pts, CondF);
    F_T_2 = func_optim_chemin([X(1), X(2), X(3)+X(3)/(2*pts)], L, pts, CondF);

    % (dérivées par différence fini d'ordre 2 centrée)

    J(:,1) = (F_M_2(:) - F_M_1(:))./(X(1)/(pts));
    J(:,2) = (F_N_2(:) - F_N_1(:))./(X(2)/(pts));
    J(:,3) = (F_T_2(:) - F_T_1(:))./(X(3)/(pts));

    % Définition du vecteur résidu

    R = func_optim_chemin(X, L, pts, CondF);

    % Définition de la direction de recherche

    delta_X = -inv(J)*R;

    % Test de convergence

    X_n = X + delta_X;
    R_n = func_optim_chemin(X_n, L, pts, CondF);

    if (norm(delta_X)/norm(X_n) < eps_x && norm(R_n) < eps_f)
        Sol = X_n;
        exit_flag = 1;
        break;
```

```
    else
        X = X_n;
    end

end

if i_trial == N_trial
    Sol = X_n;
    exit_flag = 0;
    norm(delta_X)/norm(X_n)
    norm(R_n)
end
```

func_optim_chemin.m

```
function F = func_optim_chemin(CondInit,L,pts, CondF)

F = [(CalcCheminX(CondInit, L, pts)-CondF(1))
       (CalcCheminY(CondInit, L, pts)- CondF(2))
       (CalcCheminANGLE(CondInit, L, pts)- CondF(3))];

dum2 = 1;
```

CalcCheminX.m

```
function x_final = CalcCheminX(CondInit, L, pts)

E_young = 70e9;     % Module d'Young de la fibre
I_y = 1.2e-17;      % Moment d'inertie de la fibre

ds = L/(pts);        % Élément de longueur sur la fibre
M(1) = CondInit(1);     % Moment
N(1) = CondInit(2);     % Force latérale (à l'élément ds)
T(1) = CondInit(3);     % Tension (parallel à ds)

th(1) = 0;      % initialisation de theta
x(1) = 0;       % initialisation de x
y(1) = 0;       % initialisation de y
```

```
for i = 1:(pts)
    dth = M(i)*ds/(E_young*I_y);        % Déviation de theta dû au moment (courbure)
    th(i+1) = th(i) + dth;              % update theta
    M(i+1) = M(i) - N(i)*ds;            % Relation différentielle entre M et N
    N(i+1) = N(i) - T(i)*dth;           % Relation différentielle entre N et T
    T(i+1) = T(i) + N(i)*dth;           % Relation différentielle entre T et N
    x(i+1) = x(i) + ds*cos(th(i));      % conversion en coordonnées cartériennes
    y(i+1) = y(i) + ds*sin(th(i));      % conversion en coordonnées cartériennes
end

x_final = x(length(x));

dum=1;
```

CalcCheminY.m

```
function y_final = CalcCheminY(CondInit, L, pts)

E_young = 70e9;     % Module d'Young de la fibre
I_y = 1.2e-17;      % Moment d'inertie de la fibre

ds = L/(pts);        % Élément de longueur sur la fibre
M(1) = CondInit(1);     % Moment
N(1) = CondInit(2);     % Force latérale (à l'élément ds)
T(1) = CondInit(3);     % Tension (parallel à ds)

th(1) = 0;      % initialisation de theta
x(1) = 0;       % initialisation de x
y(1) = 0;       % initialisation de y

for i = 1:(pts)
    dth = M(i)*ds/(E_young*I_y);        % Déviation de theta dû au moment (courbure)
    th(i+1) = th(i) + dth;              % update theta
    M(i+1) = M(i) - N(i)*ds;            % Relation différentielle entre M et N
    N(i+1) = N(i) - T(i)*dth;           % Relation différentielle entre N et T
    T(i+1) = T(i) + N(i)*dth;              % Relation différentielle entre T et N
    x(i+1) = x(i) + ds*cos(th(i));      % conversion en coordonnées cartériennes
    y(i+1) = y(i) + ds*sin(th(i));      % conversion en coordonnées cartériennes
end
```

```
y_final = y(length(y));
```

CalcCheminANGLE.m

```
function angle_final = CalcCheminANGLE(CondInit, L, pts)

E_young = 70e9;     % Module d'Young de la fibre
I_y = 1.2e-17;      % Moment d'inertie de la fibre

ds = L/(pts);        % Élément de longueur sur la fibre
M(1) = CondInit(1);     % Moment
N(1) = CondInit(2);     % Force latérale (à l'élément ds)
T(1) = CondInit(3);     % Tension (parallel à ds)

th(1) = 0;      % initialisation de theta
x(1) = 0;       % initialisation de x
y(1) = 0;       % initialisation de y

for i = 1:(pts)
    dth = M(i)*ds/(E_young*I_y);        % Déviation de theta dû au moment (courbure)
    th(i+1) = th(i) + dth;              % update theta
    M(i+1) = M(i) - N(i)*ds;            % Relation différentielle entre M et N
    N(i+1) = N(i) - T(i)*dth;           % Relation différentielle entre N et T
    T(i+1) = T(i) + N(i)*dth;           % Relation différentielle entre T et N
    x(i+1) = x(i) + ds*cos(th(i));      % conversion en coordonnées cartériennes
    y(i+1) = y(i) + ds*sin(th(i));      % conversion en coordonnées cartériennes
end

angle_final = (180/pi)*atan((y(pts)-y(pts-1))./(x(pts)-x(pts-1)));

dum = 1;
```

CalcChemin.m

```
function [Chemin_init, MNT] = CalcChemin(CondInit, L,pts)

E_young = 70e9;     % Module d'Young de la fibre
```

```
I_y = 1.2e-17;      % Moment d'inertie de la fibre

ds = L/(pts);        % Élément de longueur sur la fibre
M(1) = CondInit(1);     % Moment
N(1) = CondInit(2);     % Force latérale (à l'élément ds)
T(1) = CondInit(3);     % Tension (parallel à ds)

th(1) = 0;      % initialisation de theta
x(1) = 0;       % initialisation de x
y(1) = 0;       % initialisation de y

for i = 1:(pts)
    dth = M(i)*ds/(E_young*I_y);        % Déviation de theta dû au moment (courbure)
    th(i+1) = th(i) + dth;              % update theta
    M(i+1) = M(i) - N(i)*ds;            % Relation différentielle entre M et N
    N(i+1) = N(i) - T(i)*dth;           % Relation différentielle entre N et T
    T(i+1) = T(i) + N(i)*dth;              % Relation différentielle entre T et N
    x(i+1) = x(i) + ds*cos(th(i));      % conversion en coordonnées cartériennes
    y(i+1) = y(i) + ds*sin(th(i));      % conversion en coordonnées cartériennes
end

angle = atan(diff(y)./diff(x));

Chemin_init = [x
               y];

MNT = [M; N; T];

% Résultat du calcul: Chemin x,y, theta de la fibre sous les conditions M0, T0, N0
% au point x = y = 0.
```

CalcBiref.m

```
function [Chemin_init, MNT] = CalcChemin(CondInit, L,pts)

function [delta_phase, beta_eq] = CalcBiref(x,y)

pente = diff(y)./diff(x);

delta_s = sqrt(diff(x).^2 + diff(y).^2);
```

```
for i = 1:length(pente)-1
    A = [(x(i+2)-x(i)) ; pente(i)*(x(i+2)-x(i))];
    B = [(x(i+2)-x(i+1)) ; pente(i+1)*(x(i+2)-x(i+1))];
    test(i) = (A'*B)/(norm(A)*norm(B));
    delta_phi(i) = acos((A'*B)/(norm(A)*norm(B)));
end

rho = delta_s(find(delta_phi~=0))./delta_phi(find(delta_phi~=0));

lambda = 1.55e-6;     % original
%lambda = 1527.41e-9;
n0 = 1.46;
p11 = 0.113;
p12 = 0.252;
nu = 0.16;
r = 250e-6;           % original et correct
%r = 180e-6;

C_s = 0.5*(2*pi/(lambda))*(n0)^3*abs(p11 - p12)*(1+nu);

beta = 0.5*C_s*(r.^2)./(rho.^2);

delta_phase = sum(beta.*delta_s(1:length(beta)));

beta_eq = delta_phase/(sum(delta_s));
```

CalcOverLap.m

```
function F = CalcOverLap(x1,y1,x2,y2)

F = sum((x2-x1).^2 + (y2-y1).^2);
```