Démonstration expérimentale de cryptographie quantique à états cohérents

Sommaire

Présentation de l'expérience

Suivant les propositions théoriques de notre équipe pour la cryptographie quantique avec des états cohérents [70, 73], l'utilisation des variables quantiques continues offre une alternative intéressante aux protocoles basés sur l'exploitation de photons uniques [40]. En effet, l'usage

d'impulsions cohérentes comportant un grand nombre de photons ouvre des perspectives particulièrement prometteuses en terme de débit de clé et de simplicité de réalisation. Afin de valider ces propositions et d'en évaluer les paramètres caractéristiques, nous avons réalisé une démonstration expérimentale du principe de distribution de clé quantique avec des variables continues.

Des états cohérents sont modulés suivant une distribution gaussienne avant d'être échangés puis mesurés avec une détection homodyne résolue en temps limitée au bruit de photon. Les données sont ensuite traitées pour aboutir à une extraction pratique de clé secrète suivant l'ensemble des étapes nécessaires : extraction de chaînes binaires, correction d'erreurs (réconciliation directe ou inverse) et suppression de la connaissance de l'espion (amplification de confidentialité). Notre système a ainsi généré une clé secrète à un débit de 1.7 Mbits/s en l'absence de pertes et 75 kbits/s pour une transmission présentant 3.1 dB de pertes. Cet ensemble constitue le premier dispositif *complet* et *sûr* de cryptographie quantique avec des variables continues [73].

Notre schéma possède plusieurs spécificités essentielles qui le distinguent des autres protocoles à variables continues (voir la référence [70] pour une présentation rapide de ce domaine). Premièrement, aucune particularité quantique comme l'intrication ou la compression des fluctuations quantiques n'est physiquement requise pour notre dispositif. Deuxièmement, la partie optique de ce système est entièrement continue : des variables quantiques continues sont modulées suivant une distribution gaussienne avant d'être mesurées avec une détection homodyne. Un protocole particulièrement efficace d'extraction de bits [56] permet l'exploitation de quasiment toute l'information de Shannon contenue dans ces mesures. Troisièmement, notre système de détection homodyne est résolu en temps et non pas en fréquence. Il est ainsi directement sensible à la distribution statistique des quadratures du champ signal et permet une exploitation simple des débits d'information. Enfin, grâce à l'inversion du sens de la correction des erreurs, ce système est théoriquement sûr quelle que soit la transmission du canal.

Conception du dispositif optique

Le schéma optique de l'expérience est relativement simple : Alice envoie à Bob à travers un canal quantique authentifié des états cohérents modulés continûment suivant une distribution gaussienne dans l'espace des phases. Par ailleurs, elle transmet un faisceau de référence (considéré comme classique et public) servant d'oscillateur local pour la détection homodyne ainsi que divers signaux classiques de synchronisation. Bob choisit alors aléatoirement de mesurer la quadrature X ou la quadrature P de chaque impulsion incidente. Il vient ensuite une seconde étape purement algorithmique où Alice et Bob échangent classiquement et publiquement certaines informations pour évaluer la qualité du transfert et extraire une clé parfaitement secrète.

Une réalisation expérimentale complète doit vérifier strictement le cahier des charges suivant :

- *Source* : états cohérents monomodes sans excès de bruit à cadence régulière.
- *Modulation* : arbitraire en amplitude et phase pour chaque impulsion suivant une distribution gaussienne en (X, P).
- *Canal* : authentifié, permettant la synchronisation entre les partenaires, la qualité du canal (G et χ_B) doit être testée sur un échantillon représentatif des impulsions échangées.
- *Détection* : résolue en temps pour chaque impulsion, limitée au bruit de photon, choix aléatoire de la quadrature mesurée, fort rapport signal à bruit, faible bruit électronique, excellente efficacité globale.
- *Réconciliation* : directe ou inverse par communication uni-directionnelle.

Notre dispositif expérimental ne valide cependant pas l'ensemble de ces points. Comme nous le verrons dans ce chapitre, la modulation en phase est déterministe, les nombres (pseudo) aléatoires ne sont pas de qualité cryptographique, le canal n'a pas été authentifié (Alice et Bob partagent le même ordinateur), la réconciliation uni-directionnelle a été approximée... Si notre système ne permet donc pas un échange de clé secrète au sens strict, il fournit cependant des données physiques qui suivent la même répartition statistique que pour un transfert réel. L'ensemble des paramètres utiles pour la caractérisation de nos protocoles pourra ainsi être évalué expérimentalement. Notre philosophie pour le développement de cette expérience sera donc de réaliser une démonstration de principe pertinente plutôt que de concevoir un réel système de cryptographie.

Ce chapitre détaille le dispositif expérimental décrit dans [73]. Les résultats concernant l'évaluation effective de l'espionnage et l'extraction de clé [1] sont ensuite présentés avant d'aborder enfin les perspectives pratiques offertes par ce dispositif en terme de réalisations futures.

5.1 Dispositif expérimental détaillé

Données techniques pour l'expérience de cryptographie cohérente	
Diode laser	Spectra Physics SDL 5412, λ 780nm, Cavité étendue en montage Littrow avec un réseau Jobin-Yvon 1200 traits/mm, seuil 36mA, largeur spectrale <40MHz, Puissance utile 40mW pour 100mA.
Modulateur Acousto-optique	A-A OptoElectronic Modèle AA.ST.110, caractéristiques avec une focalisation de 150mm : efficacité 30%, durée impulsion FWHM 120ns, cadence 800kHz.
Fibre optique	Thorlabs FS-PM-4611-HT, monomode à 780nm, maintien de polarisation (pol. mesurée en sortie 1:200), longueur 40cm, couplage 15% (pas de connecteurs).
Modulateur Electro-optique	United Technologies Photonics, λ 780nm, tension demi-onde $V_\pi = 2.5V$, bande passante 2GHz, efficacité couplage 15% (pas de connecteurs), extinction mesurée DC $\backsim$ 4% (14dB), à 800kHz $\backsim$ 1%, puissance max < 30dBm.
Cale piezo-électrique	Saint Gobain Quartz, tension demi-onde $V_\pi = 95V$, bande passante alimentation HT 700 Hz.
Puissance signal	$\backsim$ 250 photons/impulsion au maximum de la modulation soit 50pW moyens à 800kHz. Modulation typ. $V_A = 43$.
Puissance OL	$1.3\,10^8$ photons/impulsion soit 26.5μW moyens à 800kHz.
Détection homodyne	Modèle à amplificateur de tension, efficacité globale $\eta_{hom} = \eta_{opt}\,\eta_{phot}\,\eta_{mod}^2 = 79\%$ ou 83% avec $\eta_{opt} = 92\%$, $\eta_{phot} = 92\%$, $\eta_{mod} = 96.5\%$ ou 99% suivant l'expérience; bruit de photon 4.23mV, bruit électronique 2.14mV, SNR en variance modulation / bruit total 27.

[1] L'extraction de bits, la correction d'erreurs et l'amplification de confidentialité ont été réalisées par Gilles Van Assche et Nicolas Cerf de l'Université Libre de Bruxelles avec qui nous avons collaboré pour ce projet.

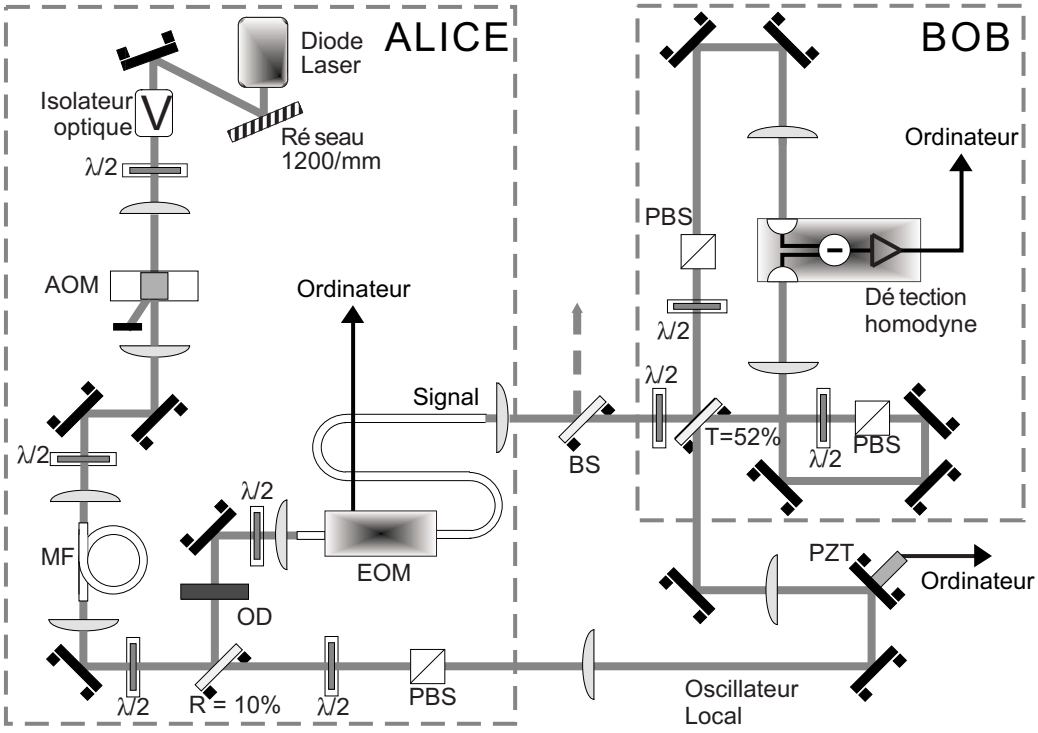

Figure 5.1: *Dispositif expérimental complet. AOM : modulateur acousto-optique, MF : fibre optique monomode à maintien de polarisation, EOM : modulateur électro-optique d'amplitude, OD : densité optique, BS : lame séparatrice simulant les pertes de transmission.*

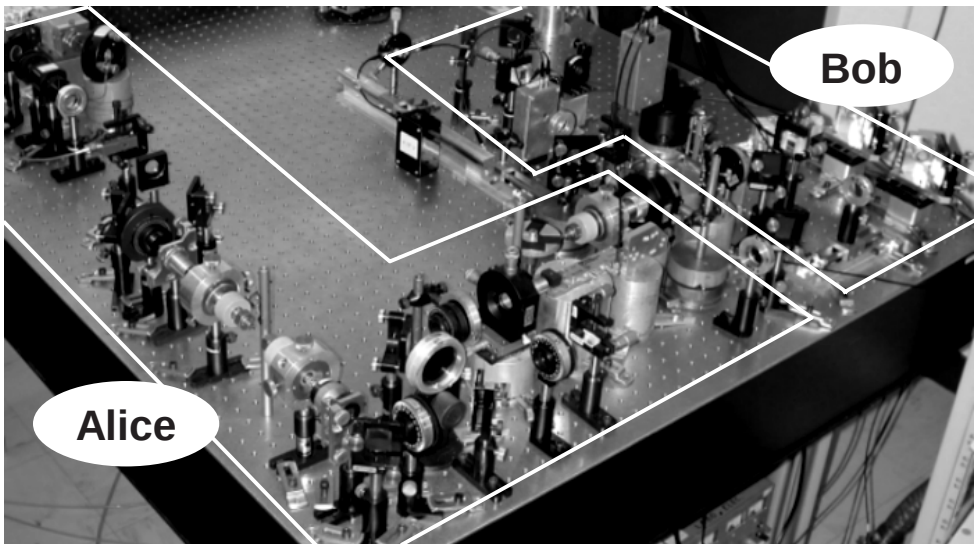

Figure 5.2: *Photographie du montage expérimental. Alice et Bob ne sont distants que de 7cm, mais des éloignements arbitraires peuvent être simulés en induisant des pertes grâce à la lame BS de transmission variable.*

5.1.1 Source d'impulsions cohérentes

Le dispositif expérimental présenté sur la figure 5.1 utilise comme source une diode laser continue émettant à 780nm. Pour générer des impulsions lumineuses de durée 120ns (largeur totale à mi-hauteur FWHM) à la cadence de 800kHz, le faisceau continu est modulé en puissance par un modulateur acousto-optique. Afin de réduire l'excès de bruit de la diode, un réseau optique réalise une cavité optique étendue en configuration de Littrow. Enfin, une fibre optique monomode à maintien de polarisation permet un filtrage spatial efficace du faisceau. Une forte atténuation optique du faisceau signal avant l'étage de modulation permet enfin de rendre négligeable l'excès de bruit introduit par la diode laser et ainsi de disposer d'une source cohérente d'impulsions au niveau du bruit de photon. Les caractéristiques techniques des différents éléments sont résumées dans le tableau page précédente.

5.1.2 Modulation en amplitude

Caractéristique du modulateur

La distribution gaussienne des états cohérents dans l'espace des phases est générée en modulant à la fois l'amplitude et la phase des impulsions lumineuses. Dans notre mise en œuvre expérimentale, l'amplitude de chaque impulsion est arbitrairement modulée à la cadence de 800kHz par un modulateur d'amplitude électro-optique[2] formant un interféromètre de Mach-Zehnder intégré en niobate de lithium $LiNbO_3$. La transmission en amplitude de cet appareil pour la quadrature X en phase avec l'oscillateur local est présentée sur la figure 5.3(c) en fonction de la tension de commande. L'utilisation d'une technologie d'optique intégrée permet notamment de travailler avec une faible tension demi-onde ($V_\pi = 2.5\,V$) et une large bande passante de modulation (jusqu'à 2 GHz).

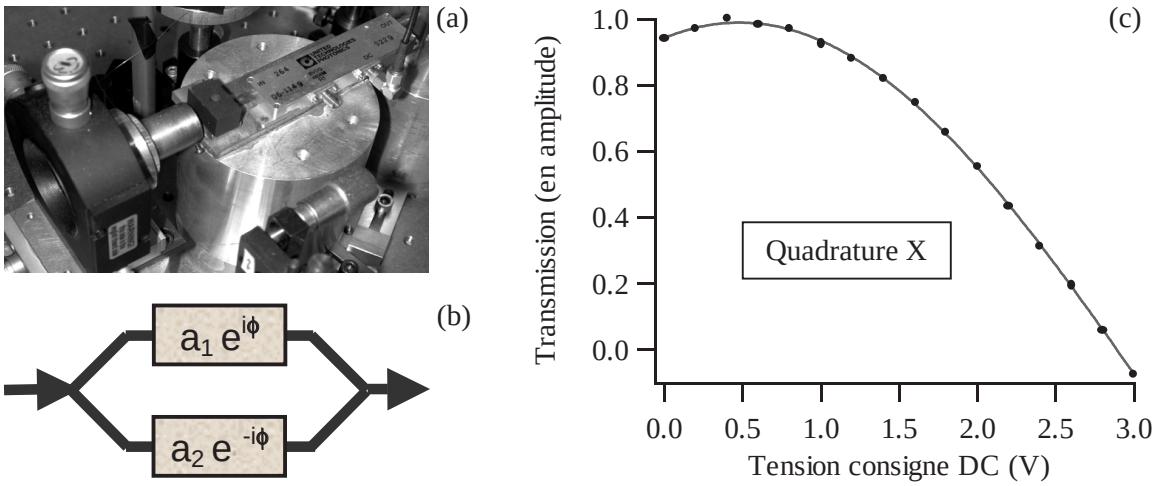

Figure 5.3: *(a) Photographie et (b) modèle simple du modulateur électro-optique d'amplitude (a_i désigne la transmission en amplitude de chaque voie). (c) Transmission expérimentale en amplitude du modulateur pour la quadrature X en phase avec l'oscillateur local, en fonction de la tension de consigne, la courbe est une interpolation suivant un modèle sinusoïdal.*

[2]Je remercie vivement la société Thalès TRT et M. Thierry Debuisschert pour le prêt de cet appareil.

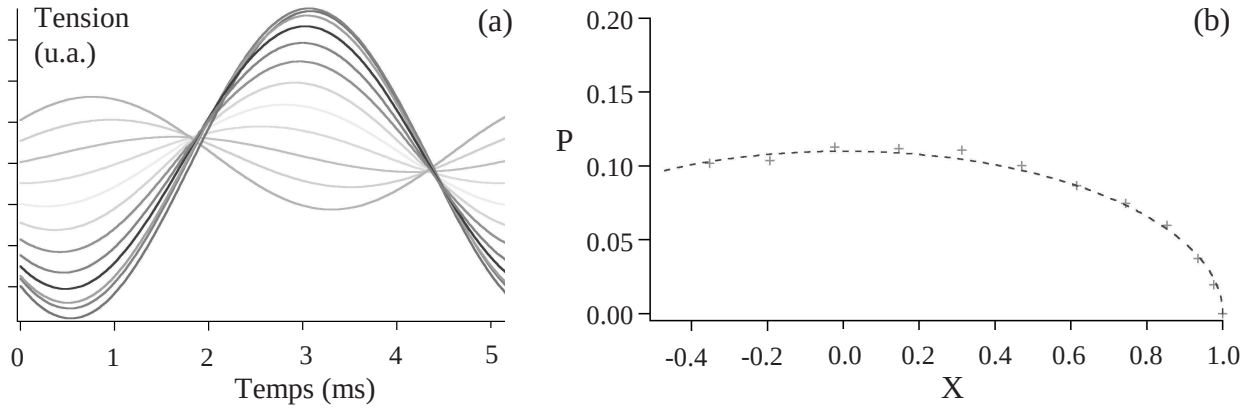

Figure 5.4: *Caractéristique du modulateur d'amplitude mesurée dans l'espace des phases. (a) Champs moyens transmis par le modulateur et mesurés par la détection homodyne pour différents échelons de tension en consigne du modulateur de 0 à 3V alors que la phase de l'oscillateur local est balayée linéairement. Il apparaît que l'extinction est non-négligeable, de même que le déphasage induit entre les niveaux de transmission. (b) Caractéristique déduite dans l'espace* (X, P)*, la courbe en tirets indique une simulation théorique (suivant le schéma 5.3) considérant que chaque bras de l'interféromètre formant le modulateur induit la même phase en valeur absolue.*

La caractéristique transmission-tension tracée sur la figure 5.3(c) est à considérer avec certaines précautions. Cette courbe est obtenue d'après une mesure à la détection homodyne : la quantité mesurée résulte donc de la projection du champ signal sur la direction de l'oscillateur local. En particulier, la figure 5.3(c) n'indique donc pas forcément que l'extinction en sortie du modulateur peut être parfaitement nulle. Afin d'obtenir une caractéristique complète du modulateur dans l'espace des phases, nous avons appliqué différents échelons de tension en consigne et mesuré simultanément le champ signal à la détection homodyne lorsque la phase de l'oscillateur local est balayée linéairement. Les résultats expérimentaux sont présentés sur la figure 5.4. Il apparaît alors que l'extinction est de 11% en amplitude, ce qui se traduit par une caractéristique non-linéaire dans l'espace des phases (figure 5.4(b)). Cet effet peut assez simplement s'expliquer par un déséquilibre entre les voies de l'interféromètre formant le modulateur comme le montre le modèle tracé en tirets sur la figure 5.4(b) ($a_2 \neq a_1$ où a_i désigne la transmission en amplitude de la voie i). D'après nos mesures d'extinction, en posant que la transmission maximale vaut $a_1 + a_2 = 1$ et la transmission minimale $a_1 - a_2 = 0.11$, on obtient $a_1 \approx 0.55$ et $a_2 \approx 0.45$.

Avec le modèle de la figure 5.3(b), le champ transmis par le modulateur d'amplitude est proportionnel à la transmission complexe de l'élément, qui s'exprime par :

$$a_1\, e^{\imath\,\phi} + a_2\, e^{-\imath\,\phi} = (a_1 + a_2)\cos\phi + \imath(a_1 - a_2)\sin\phi \tag{5.1}$$

Si Alice applique de plus un déphasage θ, la quadrature directement mesurée par Bob s'écrit alors (voir la figure 5.5) :

$$X_{B,mes} = X_{A,max}\left[(a_1 + a_2)\cos\phi\cos\theta - (a_1 - a_2)\sin\phi\sin\theta\right] \tag{5.2}$$

où $X_{A,max}$ désigne la valeur maximale de la modulation d'Alice. Cette équation contient le terme de modulation parfaite en $(a_1 + a_2)\cos\phi\cos\theta$, plus un terme traduisant la mauvaise extinction

du modulateur d'amplitude. Il devient alors possible de décomposer le champ transmis en un champ utile modulé suivant la quadrature X avec une extinction parfaite et un champ parasite déphasé de $\pi/2$. Pour une preuve de cryptographie parfaite, il faudrait supprimer ce champ en superposant au niveau d'Alice un champ supplémentaire dont les interférences annuleraient les effets du champ parasite. Une autre solution serait d'utiliser un meilleur modulateur (dans le cas d'un prototype complet à 1.55μm, des modulateurs d'extinction supérieure à 30 dB sont commercialement disponibles).

Dans notre expérience, qui est simplement vouée à être une démonstration du principe de cryptographie quantique avec des états cohérents, nous avons choisi de corriger les effets de cette mauvaise extinction lors d'un traitement a posteriori des données de Bob. Pour supprimer parfaitement les effets du champ parasite, il faudrait connaître à la fois l'amplitude et la phase choisie par Alice (ce qui revient à disposer des quantités θ et ϕ dans l'équation (5.2)). Cependant, si on choisit cette option de correction, le transfert d'information perd alors tout son sens : pour traiter ses données, Bob doit être informé parfaitement des valeurs de modulation d'Alice ! Nous avons décidé de mettre en œuvre une correction qui soit davantage dans l'esprit d'un échange de données. Dans notre dispositif, le champ parasite maximal $(a_1 - a_2)\sin\theta$ est soustrait des données mesurées, ce qui revient à translater la caractéristique du modulateur suivant l'axe P pour obtenir une extinction parfaite (figure 5.4). Cette opération est possible car comme nous le verrons à la section suivante, la phase θ n'est pas modulée aléatoirement, mais est déterministe dans notre expérience. Bob peut ainsi connaître simplement le champ parasite en $-(a_1-a_2)\sin\theta$ à soustraire de ses mesures. Les données effectives de Bob correspondent alors à :

$$X_{B,corr} = X_{A,max}\left[(a_1+a_2)\cos\phi\cos\theta - (a_1-a_2)\sin\theta(\sin\phi - 1)\right] \tag{5.3}$$

Cette équation contient le terme de modulation parfaite en $(a_1 + a_2)\cos\phi\cos\theta$, plus un terme de correction pour tenir compte de la non-linéarité de la réponse du modulateur d'amplitude. Cette non-linéarité résiduelle après corrections sera également prise en compte dans les calculs des données d'Alice.

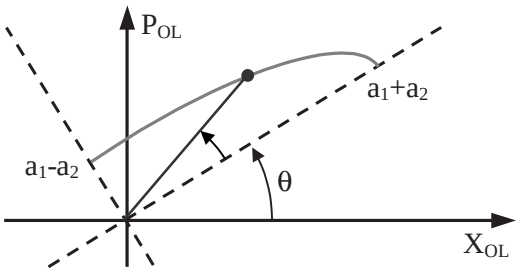

Figure 5.5: *Modèle utilisé pour le calcul de la quadrature mesurée par Bob. Le point indique la valeur de transmission choisie par Alice. La caractérisation du modulateur électro-optique fournit* $a_1 + a_2 = 1$ *et* $a_1 - a_2 = 0.11$.

Génération d'une modulation gaussienne

Pour la génération de la modulation gaussienne de variance $V_A\,N_0$, nous avons choisi de fixer la valeur de la variance par le nombre de photons maximal $\mathcal{N}_s$ du faisceau d'Alice (calibré d'après une mesure avec une photodiode). Ce choix permet d'utiliser l'ensemble de la plage

disponible du modulateur, dont la transmission varie entre 0 et 1. L'écart-type de la modulation en transmission vaut donc $\sigma_{\mathrm{T}} = 1/3$ (pour une distribution gaussienne, l'écart-type est pris égal au tiers de la valeur maximale admise, soit une transmission de 1 dans notre cas). Le lien entre V_A et le nombre de photons $\mathcal{N}_s$ est alors donné par $V_A = 2\,\mathcal{N}_s\,\sigma_{\mathrm{T}}^2 = 2/9\,\mathcal{N}_s$.

Quelle distribution de probabilité en amplitude r et phase θ choisir pour obtenir une modulation gaussienne en (X, P) ? Ce calcul a été effectué par Frédéric Grosshans dans [71] et sera brièvement repris ici. Nous posons l'amplitude r comme la transmission en champ du modulateur : $0 < r < 1$. Le point de départ consiste à identifier les densités de probabilité suivant [203] :

$$\mathcal{P}_{X,P}\,dX\,dP = \frac{1}{2\pi\sigma^2} e^{-\frac{X^2+P^2}{2\sigma^2}}\,dX\,dP = \mathcal{P}_{r,\theta}\,dr\,d\theta \tag{5.4}$$

où $\sigma = 1/3$ est l'écart-type de la distribution gaussienne pour la transmission en amplitude, choisie de telle sorte que 3σ soit égal à une transmission unité. Avec $dX\,dP = r\,dr\,d\theta$, une identification dans (5.7) fournit :

$$\mathcal{P}_r\,dr = \frac{r}{\sigma^2} e^{-\frac{r^2}{2\sigma^2}}\,dr = -d\left\{e^{-\frac{r^2}{2\sigma^2}}\right\} \tag{5.5}$$

$$\mathcal{P}_\theta\,d\theta = \frac{d\theta}{2\pi} \tag{5.6}$$

Ce qui donne explicitement la forme de la modulation en amplitude r à choisir et prouve comme on pouvait s'y attendre que la distribution en phase à appliquer est une loi uniforme sur $[0, 2\pi]$.

Pour passer d'une variable (pseudo-) aléatoire y, générée par l'ordinateur et uniformément répartie dans l'intervalle $[0, 1]$, à la variable r définie suivant la distribution (5.5), il faut à nouveau appliquer une relation du type :

$$|\mathcal{P}_y\,dy| = |\mathcal{P}_r\,dr| \tag{5.7}$$

Puisque la variable y est uniforme sur $[0, 1]$, $\mathcal{P}_y = 1$ d'où :

$$dy = d\left\{e^{-\frac{r^2}{2\sigma^2}}\right\} \qquad \Leftrightarrow \qquad y = e^{-\frac{r^2}{2\sigma^2}} \tag{5.8}$$

Avec le modèle du modulateur électro-optique, le lien entre la tension V à appliquer et la transmission en amplitude s'écrit :

$$r = \sin\left(\frac{\pi}{2}\,\frac{V_{min} - V}{V_\pi}\right) = \sigma\sqrt{-2\ln y} \tag{5.9}$$

où V_{min} est la tension d'annulation de la transmission et V_π la tension demi-onde du modulateur. Pour obtenir une modulation gaussienne entre 0 et 1 de la transmission, la tension à appliquer au modulateur s'écrit finalement à partir de la variable pseudo-aléatoire y fournie par l'ordinateur :

$$V = V_{min} - \frac{2}{\pi}\,V_\pi\,\arcsin(\sigma\sqrt{-2\ln y}) \tag{5.10}$$

Pour éviter une divergence dans cette formule lorsque y tend vers zéro, il faut tronquer la distribution de cette variable à $[y_{min}, 1]$. y_{min} est obtenu lorsque l'amplitude normalisée r transmise par le modulateur vaut 1, soit avec notre choix $\sigma = 1/3$: $y_{min} = \exp(-1/2\sigma^2) = e^{-4.5} \approx 0.011$.

Effets du codage discret

La tension de commande appliquée au modulateur élecro-optique est générée par la carte d'acquisition (*National Instruments* PCI 6111E) connectée à un ordinateur. Cette tension prend uniquement des valeurs discrètes, bien que nos propositions théoriques de protocoles supposent une distribution continue. Cependant, cette contrainte expérimentale peut ne pas être gênante si le nombre de niveaux de discrétisation codés par la carte est très grand devant le nombre de niveaux requis pour masquer le "quadrillage" de la distribution sous le bruit de photon. Dans ce cas, la distribution discrète est suffisamment dense par rapport au bruit quantique pour que l'espion ne puisse discerner les différents niveaux.

Un calcul très simple permet de quantifier l'influence des niveaux discrets de la tension fournie par la carte (une autre approche est développée dans [71]). Suivant la direction de la modulation d'amplitude, la quadrature envoyée par Alice s'écrit :

$$X_A = X_{A,max} \sin\left(\frac{\pi}{2}\frac{V_{min}-V}{V_\pi}\right) = 3\sqrt{V_A\,N_0}\,\sin\left(\frac{\pi}{2}\frac{V_{min}-V}{V_\pi}\right) \tag{5.11}$$

L'influence d'une faible variation de tension sur la transmission du modulateur est plus critique dans la portion où la transmission varie linéairement par rapport à la tension de commande, c'est-à-dire au voisinage du minimum d'amplitude transmise $V \approx V_{min}$. L'écart maximum en quadrature entre deux niveaux de tension séparés de δV vaut alors :

$$\delta X_r = X_A(V_{min}) - X_A(V_{min}-\delta V) \approx 3\,\sqrt{V_A\,N_0}\,\frac{\pi}{2}\,\frac{\delta V}{V_\pi} \tag{5.12}$$

Pour que les niveaux discrets générés par la carte soient noyés sous le bruit quantique, il faut $\delta X_r \ll \sqrt{N_0}$. Avec nos conditions expérimentales, $V_A \backsimeq 40$, $V_\pi = 2.5$ V, le critère $\delta X_r = 0.05\sqrt{N_0}$ impose une résolution en tension de $\delta V = 4$ mV, soit environ 12 bits dans la plage $\pm$10V de notre carte. Les sorties de notre carte étant codées sur 16 bits, nous pouvons donc très raisonnablement considérer que la modulation en amplitude est continue et que les effets de la discrétisation sont négligeables.

5.1.3 Modulation de phase

La société *Thalès* a pu nous prêter un modulateur intégré d'amplitude à 780 nm. Il s'agit d'un système datant d'une dizaine d'années et qui n'était plus disponible commercialement dans cette gamme de longueurs d'ondes au moment de notre expérience. Malheureusement, nous n'avons pas pu trouver de modulateur de phase fonctionnant à la longueur d'onde de 780 nm pour adresser arbitrairement la phase à la cadence nominale de 800 kHz. En effet, l'essentiel de la branche des modulateurs intégrés se concentre sur la fenêtre télécom 1.3-1.5 μm (depuis lors, de nouveaux modulateurs intégrés sont apparus sur le marché pour les longueurs d'onde 810 ou 1064 nm, commercialisés par la société *Linos*). En conséquence, la phase expérimentale des données d'Alice n'est pas modulée mais balayée continûment entre 0 et 2π par une cale piezo-électrique [3]. Les données sont ensuite permutées aléatoirement par un traitement informatique de sorte à obtenir exactement la même structure de données que pour une expérience réelle de cryptographie. Aucune clé secrète ne peut être rigoureusement transmise avec une telle variation déterministe de la phase, mais l'expérience permet de valider en conditions réelles les

[3] Sur le montage expérimental, cette cale piezo-électrique est commune à Alice et Bob qui l'utilisent alternativement pour moduler les données ou recaler la référence de phase entre les transferts.

caractéristiques du dispositif optique ainsi que le fonctionnement des algorithmes d'extraction de clé.

De même que pour la modulation d'amplitude, les effets du codage discret de la tension de commande doivent être évalués pour la modulation en phase, afin d'assurer que cette modulation peut raisonnablement être considérée comme continue. La modulation en phase étant uniforme sur $[0, 2\pi]$, deux points de phase adjacents sont séparés de la phase $\delta\theta = 2\pi/2^{n_\theta}$ où n_θ est le nombre de bits du codage en phase. L'écart maximal en quadrature entre deux points adjacents pour la modulation de phase s'écrit alors :

$$\delta X_\theta = X_{A,max}\,\delta\theta = 3\sqrt{V_A\,N_0}\,\frac{2\pi}{2^{n_\theta}} \tag{5.13}$$

A nouveau, la condition $\delta X_\theta \ll \sqrt{N_0}$ doit être vérifiée pour que les niveaux discrets de phase générés par la carte soient noyés sous le bruit quantique. Avec nos conditions expérimentales, $V_A \backsimeq 40$, le critère $\delta X_\theta = 0.05\sqrt{N_0}$ impose un codage de la phase sur $n_\theta = 11.2$ bits. Comme notre générateur de haute tension associé à la cale piezo-électrique n'utilise qu'une gamme de 4 V de la plage ± 10 V de la tension en sortie de carte, le codage au niveau de la sortie de la carte doit comporter 13.5 bits. Le codage en phase est donc plus critique que celui en amplitude, mais comme nous utilisons des sorties codées sur 16 bits, les effets de la discrétisation ne seront pas un problème expérimental.

5.1.4 Stabilisation de la phase

L'information secrète étant codée sur les quadratures du champ électromagnétique, notre système de détection interférométrique nécessite un faisceau de référence de phase (fourni par l'oscillateur local OL). Ainsi, l'ensemble du montage de la figure 5.1 peut être considéré comme un seul interféromètre de Mach-Zehnder dont chaque bras mesure plus d'un mètre de long. Pour garantir la qualité interférométrique de l'échange, aucune fluctuation incontrôlée de phase ne devrait perturber la phase relative entre l'impulsion signal d'Alice et l'impulsion OL correspondante. Expérimentalement, cette phase relative ne peut cependant pas être parfaitement maîtrisée, ce qui se traduit par des fluctuations ajoutées sur les mesures de Bob. Deux types de bruits de phase d'origines distinctes interviennent : des perturbations lentes (de l'ordre du Hz) d'origine mécanique ou thermique (modification de l'indice de l'air) et des perturbations rapides (de l'ordre de la centaine de Hz) d'origine acoustique. Les fluctuations lentes seront contrôlées et corrigées par un asservissement numérique et une rétroaction sur la cale piezo-électrique de l'oscillateur local. Les fluctuations rapides de phase seront atténuées par un choix approprié des puissances optiques des faisceaux. Ce problème de stabilité de la phase relative conduit alors à une limite supérieure de la puissance signal, afin de limiter l'influence de ces fluctuations sur le signal de sortie.

Fluctuations lentes de phase et asservissement

L'utilisation des entrées et sorties de la carte d'acquisition numérique, couplée à un ordinateur et à une cale piezo-électrique permet de concevoir simplement une boucle d'asservissement numérique des fluctuations lentes de la carte (le temps de réponse de l'alimentation haute tension de la cale et le temps d'échange de données entre la carte *NiDAQ* et le logiciel *Igor* limitent la vitesse de l'asservissement à des corrections de fluctuations de l'ordre de quelques Hz). Le principe retenu pour l'asservissement est le suivant : pour toute la durée de la mesure et la correction de la phase, Alice envoie la puissance maximale pour le faisceau signal. Bob cherche

alors à fixer la phase de l'oscillateur local pour annuler le signal d'interférence mesuré à la détection homodyne. Ceci s'effectue en 10 étapes identiques où une mesure de la tension moyenne sur 2000 impulsions en sortie de détection fournit le signal de correction à appliquer sur la cale piezo-électrique pour annuler les interférences. Le choix d'un nombre fixe de 10 itérations permet une précision dans la mesure de la phase de 0.7 mV (bruit de photon de 4.2 mV) ainsi qu'une convergence à la fin d'une durée fixe. Enfin, un déphasage supplémentaire de $\pi/2$ induit par la cale piezo-électrique permet de recaler la quadrature mesurée par Bob avec la direction X de la modulation d'Alice.

Fluctuations rapides de phase et choix de la modulation

Une première série d'expériences avait été effectuée avec une puissance moyenne signal de 1 nW (soit environ 5000 photons/impulsion à 800kHz) et une puissance OL de 10 μW. La variance de modulation est alors de l'ordre de $1000\,N_0$, ce qui devrait permettre un taux de transfert I_{AB} en l'absence de pertes et de bruit ajouté de l'ordre de 5 bits par impulsion. Cependant, pour cette puissance signal relativement "intense", des différences de phase relative aussi faibles que $\lambda/250$ viennent entacher le signal en sortie de la détection homodyne. Une étude du spectre de bruit révèle alors la présence de différentes fréquences particulières entre 200 et 300 Hz, ce qui indique que des vibrations acoustiques sont à l'origine des incertitudes de phase. Ces fluctuations se traduisent par une incertitude supplémentaire d'un écart-type de 5 mV sur une mesure moyenne de la phase, lorsque l'écart-type du bruit de photon correspondant est de 4.2 mV. Cette incertitude, qui devrait être très inférieure au bruit de photon, ne permet donc pas pour cette configuration un échange adéquat de données.

Afin de limiter l'influence des perturbations de phase, la puissance signal a été réduite à 250 photons par impulsion, tout en conservant une puissance OL de 10 μW, soit $1.3\,10^8$ photons par impulsion. Cette réduction de la puissance signal permet une diminution de la visibilité des franges d'interférences parasites sur chaque voie de la détection, ce qui atténue l'effet des perturbations rapides de phase, mais n'a pas d'influence sur l'efficacité de la détection homodyne. Pour ces puissances optiques, la précision de mesure moyenne de la phase est de 0.7 mV, à comparer au bruit de photon de 4.2 mV. Le prix à payer pour s'être quasiment débarrassé des fluctuations rapides de phase est une variance de modulation réduite, mais qui atteint tout de même la valeur de $43\,N_0$. Cette variance apparaît encore tout à fait acceptable pour la transmission d'information avec $I_{AB} = 2.7$ bits/impulsion en l'absence de pertes et une détection parfaite. [4]

Grâce à un choix adéquat des puissances optiques et à un asservissement actif des fluctuations lentes de la phase, le signal moyen en sortie de la détection homodyne est stable à mieux de 1% pour des durées supérieures à 0.1s, soit des ensembles de 80 000 impulsions, ce qui nous permet dès lors d'envisager des transferts de blocs de quelques dizaines de milliers de symboles.

5.1.5 Structure des données et synchronisation

Le traitement informatique utilisé pour l'amplification de confidentialité [73] est optimisé pour des blocs de données de 36 800 ou 55 200 bits. Expérimentalement, nous avons choisi

[4] Du fait des perturbations rapides de la phase, le meilleur choix pour la variance de modulation V_A n'est pas forcément la valeur la plus élevée possible évitant la saturation de la détection homodyne. Un autre argument dans ce sens est de remarquer que l'information mutuelle $I_{AB} = 1/2\log_2(1+V_A)$ en l'absence de pertes augmente relativement lentement par rapport à V_A au-delà de $V_A = 30$. Enfin, comme nous le verrons dans la section sur les taux de transfert expérimentaux, il peut être avantageux de travailler avec des variances de modulation réduites pour optimiser l'extraction de bits secrets compte tenu de l'efficacité limitée de nos algorithmes de réconciliation.

d'organiser les transferts de données par blocs de 60 000 points, ce qui permet de conserver quelques valeurs supplémentaires pour évaluer la qualité du canal de transmission. La durée utile d'un transfert de 60 000 impulsions à 800kHz est de 75 ms, ce qui permet de garantir une stabilité satisfaisante de la phase relative entre les faisceaux. Entre chaque bloc de données, des séquences d'impulsions sont envoyées pour recaler la phase relative suivant l'asservissement décrit précédemment, puis une autre séquence permet la synchronisation des partenaires. Dans notre expérience, un bloc de données de 60 000 points est envoyé toutes les 1.6 secondes, soit un rapport cyclique de l'ordre de 5%. Ce rapport cyclique n'a pas été conçu pour être le plus efficace possible et est clairement sous-optimisé pour cette expérience, mais il devrait pouvoir être amélioré simplement lors de prototypes futurs.

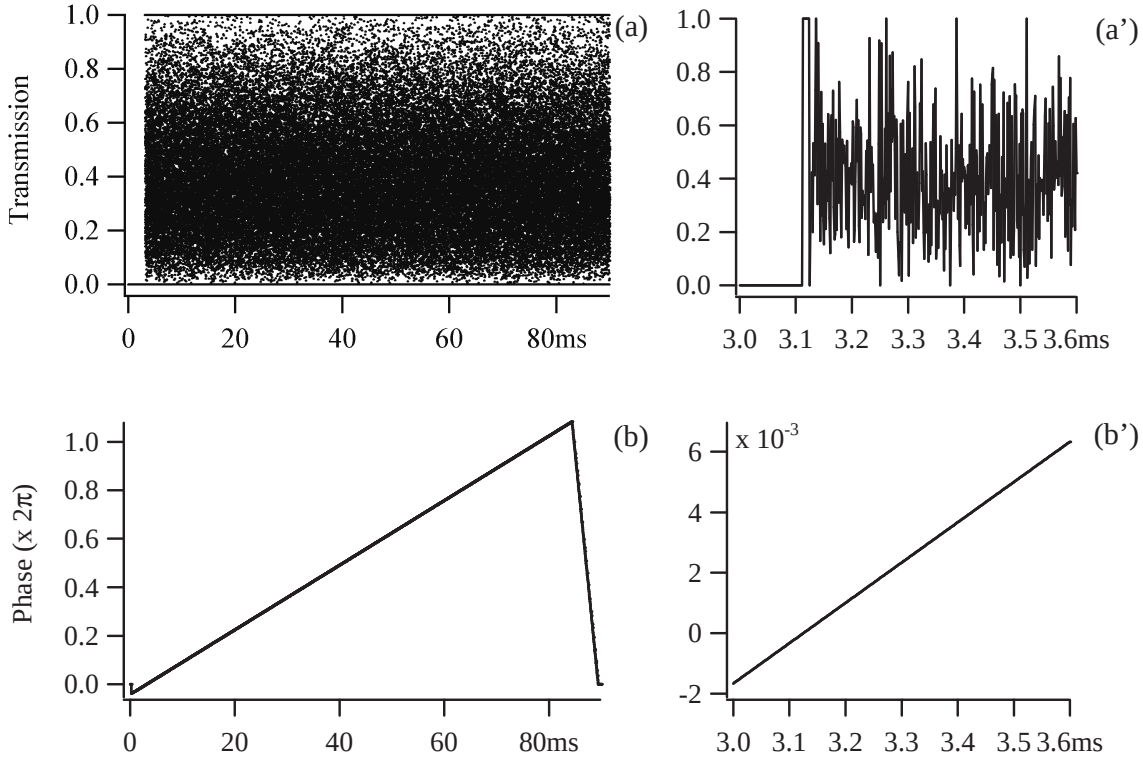

Figure 5.6: *Modulations expérimentales pour un bloc de 60 000 points. (a) transmission (calculée) en quadrature du modulateur, (b) phase (en unités de 2π) appliquée par la cale piezoélectrique. (a') et (b') sont des agrandissements des courbes (a) et (b) au début du transfert.*

La figure 5.6 présente les modulations expérimentales en transmission et en phase pour un bloc de données. Au cours d'un transfert, ces signaux sont envoyés dès que l'asservissement de correction des dérives de phase a bouclé un cycle d'itérations. Avant l'envoi des données proprement dites, un sous-bloc de 2500 impulsions permet de signaler le début du transfert. Ce bloc se compose de la manière suivante : pour les 2490 premiers points, la transmission du modulateur est mise au minimum, puis elle est fixée au maximum pour les 10 derniers points. Le récepteur peut alors facilement détecter le front montant dans l'amplitude, et savoir alors que le transfert débute 10 impulsions plus tard (pour notre démonstration de principe où Alice et Bob partagent le même ordinateur, nous n'avons besoin que de cette synchronisation simple du début du transfert).

En plus des données utiles pour le transfert de clé, Alice envoie une impulsion à la transmission minimale du modulateur toutes les 100 impulsions signal à partir de la première impulsion. Ceci permet à Bob de connaître précisément la valeur correspondante du champ parasite du modulateur électro-optique. Une interpolation sur ces données fournit ensuite les valeurs à soustraire aux données brutes du transfert pour corriger la mauvaise extinction du modulateur. Enfin, Alice envoie également une impulsion à la transmission maximale du modulateur toutes les 100 impulsions signal à partir de la dixième impulsion, ce qui permet a posteriori de connaître précisément la phase envoyée et de sélectionner exclusivement la plage $[0, 2\pi]$.

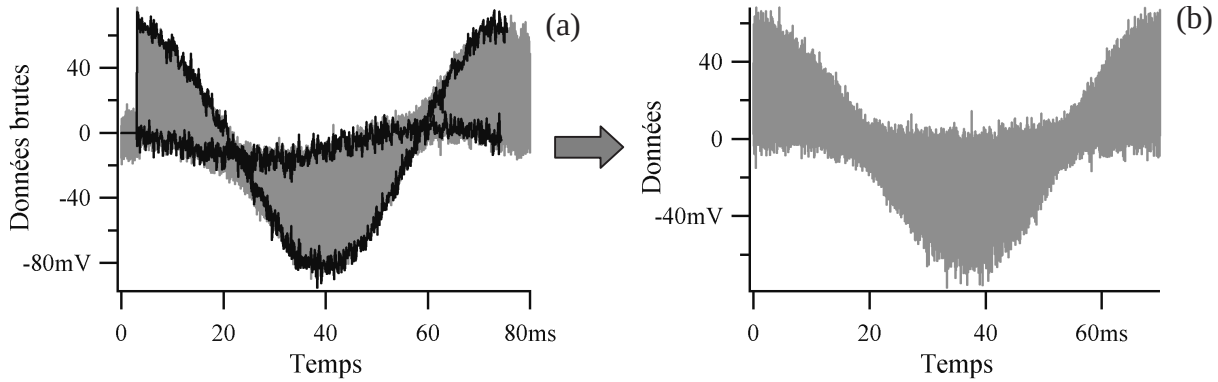

Figure 5.7: *(a) Exemple de données brutes (gris) mesurées en sortie de la détection homodyne avant traitement. (b) Données corrigées après synchronisation et suppression du champ parasite. Les courbes noires désignent les points au maximum et au minimum de transmission du modulateur, utilisés pour sélectionner la plage* $[0, 2\pi]$ *et pour soustraire le champ parasite introduit par le modulateur électro-optique.*

5.1.6 Détection homodyne impulsionnelle

Notre expérience utilise le premier prototype de détection homodyne résolue en temps, fonctionnant sur le principe d'un premier étage amplificateur de tension, décrit dans la section 3.4. Cette détection est limitée au bruit de photon jusqu'à des puissances oscillateur local de 500 millions de photons par impulsion, mais nous n'utiliserons qu'une puissance OL de 130 millions de photons par impulsion, pour des impulsions signal contenant jusqu'à 250 photons. Suivant les réglages expérimentaux, l'efficacité globale de la détection η_{hom} vaut typiquement 79%. Cette efficacité s'exprime suivant les résultats de la section 3.2.5 comme $\eta_{hom} = \eta_{opt}\,\eta_{phot}\,\eta_{mod}^2$ avec la transmission des optiques de la détection $\eta_{opt} = 92\%$, l'efficacité quantique des photodiodes (*Centronix* BPX65) $\eta_{phot} = 92\%$, et l'efficacité d'adaptation des modes (visibilité des franges d'interférence) $\eta_{mod} = 96.5\%$. Au niveau de la quadrature détectée en entrée de la détection homodyne, ces inefficacités se traduisent par un bruit ajouté de variance $\chi_{hom}\,N_0$ suivant le résultat (5.19) : $\chi_{hom} = (1 - \eta_{hom})/\eta_{hom}$. Pour notre dispositif expérimental, on obtient $\chi_{hom} = 0.27$.

En plus du bruit de photon et du bruit équivalent virtuellement introduit par les pertes, la détection homodyne présente également un bruit électronique non-négligeable. Pour notre puissance OL de $1.3\,10^8$ photons/impulsion, l'écart-type du bruit de photon détecté est de 4.23mV alors que l'écart-type du bruit électronique est de 2.14mV. Le bruit électronique apparaît alors comme un bruit additif sur les valeurs mesurées en sortie avec une variance de $(2.14/4.23)^2 = 0.26\,N_0$. Si de plus on considère les bruits en entrée de la détection homodyne, donc tenant

compte de l'efficacité limitée η_{hom} de la détection, la variance de bruit électronique à considérer d'après (5.19) est $\chi_{elec}\,N_0 = 0.26/\eta_{hom}\,N_0 = 0.33\,N_0$.

Le bruit total ajouté par la détection vaut $(\chi_{hom} + \chi_{elec})\,N_0$ auquel il faut encore additionner une unité N_0 pour le bruit de photon du faisceau d'Alice. Avec une variance de modulation de $V_A = 43$, le rapport signal à bruit (en variances selon Shannon) en l'absence bruit ajouté en ligne est $SNR = V_A/(1 + \chi_{hom} + \chi_{elec}) = 27$, ce qui permet en théorie d'atteindre le débit $I_{AB} = 1/2\,\log_2(1 + SNR) = 2.4$ bits par impulsion.

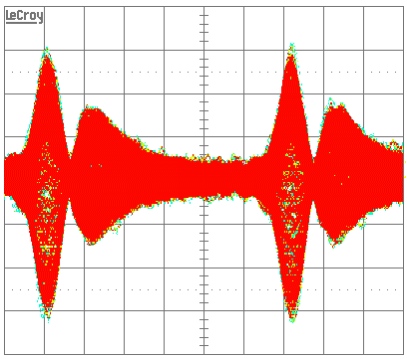

Figure 5.8: *Observation à l'oscilloscope du signal en sortie de la détection pour des impulsions signal d'amplitude maximale et modulées en phase. La persistence de l'oscilloscope est utilisée pour superposer de nombreuses réponses (temps de persistence 5 s). Puissance OL* $9.7\,10^7$ *photons/impulsion, puissance signal 80 photons/impulsion, échelles H : 0.2µs/div, V : 20mV/div.*

Après cette description détaillée du dispositif expérimental de cryptographie quantique avec des états cohérents, la section suivante aborde les échanges physiques de clés, ainsi que les résultats obtenus pour l'extraction finale de l'information binaire. En particulier, l'influence précise des bruits de la détection homodyne de Bob dans l'évaluation de l'espionnage sera présentée dans la section 5.2.3.

5.2 Discussion des résultats expérimentaux

5.2.1 Echange quantique de données

Le canal quantique complet, incluant la détection imparfaite de Bob, peut être modélisé par le schéma présenté sur la figure 5.9. Par la suite, nous n'écrivons les relations que pour la quadrature X, étant entendu que les relations sont identiques pour la quadrature P. Le canal de transmission proprement dit entre Alice et Bob est caractérisé par sa transmission (en intensité) G et sa variance de bruit équivalent en entrée χ_{ligne} comme nous l'avons vu au chapitre précédent. La quadrature en sortie de ce canal est notée X_{ligne} et s'exprime selon (4.2) :

$$X_{ligne} = \sqrt{G}\,(\,\overline{X}_A + \delta X_A + B_{ligne}\,) \tag{5.14}$$

L'état cohérent modulé en sortie de la source d'Alice est donné par $\overline{X}_A + \delta X_A$ où $\overline{X}_A$ est la valeur classique de modulation parfaitement connue d'Alice et δX_A désigne les fluctuations quantiques du faisceau. Le bruit équivalent en entrée rajouté par le canal est noté par B_{ligne}, de variance $\langle {B_{ligne}}^2 \rangle = \chi_{ligne}\,N_0$.

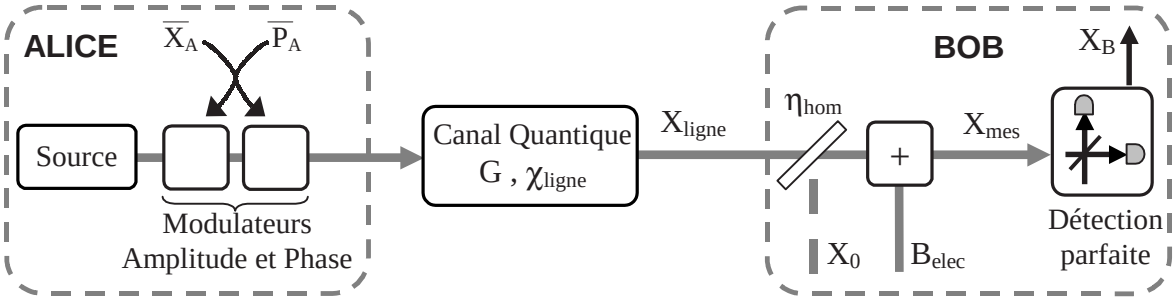

Figure 5.9: *Modèle de la transmission quantique et notations dans le cas d'une prise en compte "réaliste" du bruit de la détection homodyne de Bob (voir la discussion section 5.2.3).*

Pour tenir compte des imperfections de la détection homodyne, les différentes pertes sont modélisées par une lame de transmission égale à l'efficacité globale de la détection η_{hom}. De plus, un bruit supplémentaire B_{elec} non lié à une atténuation tient compte du bruit électronique de la détection. La variance de ce bruit, exprimée en unités de bruit de photon, est égale au rapport de la variance mesurée du bruit électronique sur la variance mesurée du bruit de photon. La quadrature mesurée par la détection homodyne peut alors s'exprimer selon :

$$X_{mes} = \sqrt{\eta_{hom}}\, X_{ligne} + \sqrt{1-\eta_{hom}}\, X_0 + B_{elec} \tag{5.15}$$

Enfin, Bob déduit son estimation de la quadrature reçue en sortie de la ligne en corrigeant ses mesures de l'atténuation $\sqrt{\eta_{hom}}$:

$$X_B = \frac{X_{mes}}{\sqrt{\eta_{hom}}} = \sqrt{G}\,(\,\overline{X}_A + \delta X_A + B_{ligne}\,) + \sqrt{\frac{1-\eta_{hom}}{\eta_{hom}}}\, X_0 + \frac{1}{\sqrt{\eta_{hom}}}\, B_{elec} \tag{5.16}$$

La variance des données X_B de Bob vaut alors, en unités de N_0 :

$$V_B = \frac{\langle {X_B}^2 \rangle}{N_0} = G\,(\,V_A + 1 + \chi_{ligne}\,) + \frac{1-\eta_{hom}}{\eta_{hom}} + \frac{\langle {B_{elec}}^2 \rangle}{\eta_{hom}} \tag{5.17}$$

Ce qui peut se réécrire sous la forme condensée :

$$V_B = G\,(\,V + \chi_{ligne}\,) + \chi_{hom} + \chi_{elec} = G\,(\,V + \chi_{tot}\,) \tag{5.18}$$

Avec $V = V_A + 1$ la variance totale de la modulation d'Alice et les bruits χ_{hom}, χ_{elec} ajoutés par la détection homodyne

$$\chi_{hom} = \frac{1-\eta_{hom}}{\eta_{hom}} \qquad\qquad \chi_{elec} = \frac{\langle {B_{elec}}^2 \rangle}{\eta_{hom}} \tag{5.19}$$

Finalement, le bruit équivalent total de la transmission χ_{tot} s'exprime par :

$$\chi_{tot} = \chi_{ligne} + \frac{\chi_{hom} + \chi_{elec}}{G} \tag{5.20}$$

Ces différentes définitions du bruit ajouté seront utiles suivant les hypothèses de la prise en compte par l'espion des bruits de la détection de Bob (voir la discussion section 5.2.3).

Les figures 5.10 et 5.11 présentent les données X_B et $\overline{X}_A$ ainsi définies, pour un bloc de données de 60 000 impulsions correspondant à une transmission de $G = 100\%$. Pour ce transfert, la variance des données d'Alice vaut $V_A = 40.7$, celle des données de Bob vaut $V_B = 42.3$. La différence entre V_B et V_A est liée au bruit de photon (une unité N_0) ainsi qu'aux différents autres bruits : bruit ajouté en ligne, pertes de la détection homodyne, bruit électronique. D'après (5.18) pour une transmission de 100%, on attendrait $V_B = V_A+1+\chi_{hom}+\chi_{elec} = 40.7+1+0.27+0.33 = 42.3$, ce qui correspond bien à la variance mesurée et indique que $\chi_{ligne} = 0$, comme on pouvait l'espérer pour une ligne sans pertes.

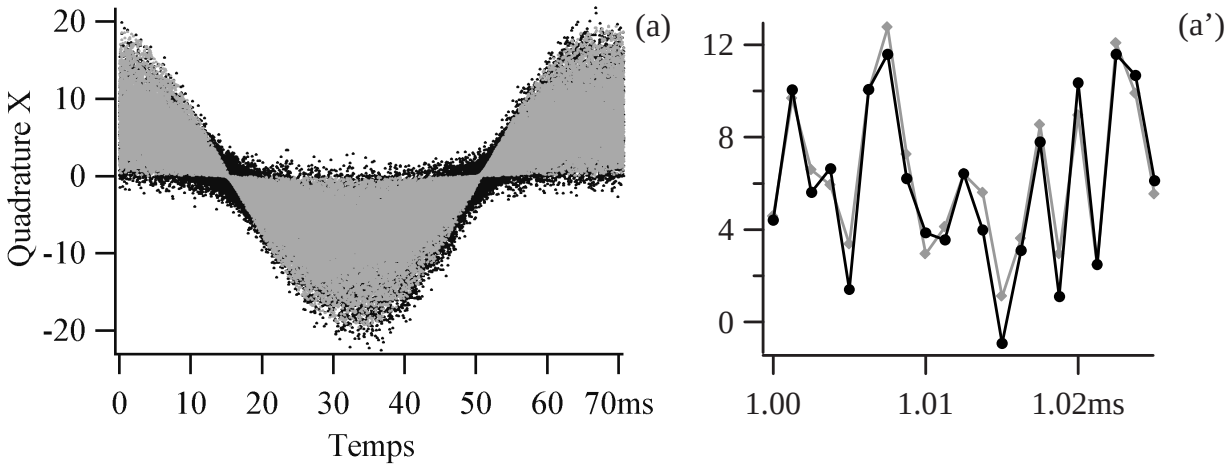

Figure 5.10: *(a) Quadrature mesurée X_B par Bob (noir) et quadrature envoyée $\overline{X}_A$ par Alice (gris) en fonction du temps pour un bloc de 60 000 points à la cadence de 800kHz. La transmission du canal est de 100% et la variance de modulation vaut $V_A = 40.7$. (a') est un agrandissement de (a) montrant un échantillon des données de Bob (noir) par rapport à celles d'Alice (gris).*

5.2.2 Estimation des paramètres de la ligne

Une fois l'échange quantique effectué, une première étape vers l'extraction d'une clé secrète binaire est d'estimer les paramètres G et χ_{ligne} du canal quantique. Lors d'un échange cryptographique réel, cette estimation s'effectue en révélant publiquement un sous-ensemble de données statitistiquement représentatif et choisi aléatoirement (donc inconnu d'Eve lors de l'espionnage). Alice et Bob peuvent alors comparer leurs résultats pour estimer les paramètres utiles. Bien sûr, les données ainsi révélées sont ensuite supprimées et n'interviennent plus pour l'extraction d'une clé secrète. Pour notre démonstration de principe, l'intégralité des 60 000 impulsions transmises est utilisée pour évaluer les paramètres G et χ_{ligne} (l'efficacité et le bruit de la détection homodyne sont par ailleurs calibrés avant et après chaque transfert).

L'évaluation des caractéristiques du canal utilise le coefficient de corrélation ρ^2 entre les données d'Alice et Bob.

$$\rho^2 = \frac{\langle \overline{X}_A X_B \rangle}{\sqrt{\langle \overline{X}_A{}^2 \rangle \langle X_B{}^2 \rangle}} = G\,\frac{V_A}{V_B} = \frac{V_A}{V_A + 1 + \chi_{tot}} \tag{5.21}$$

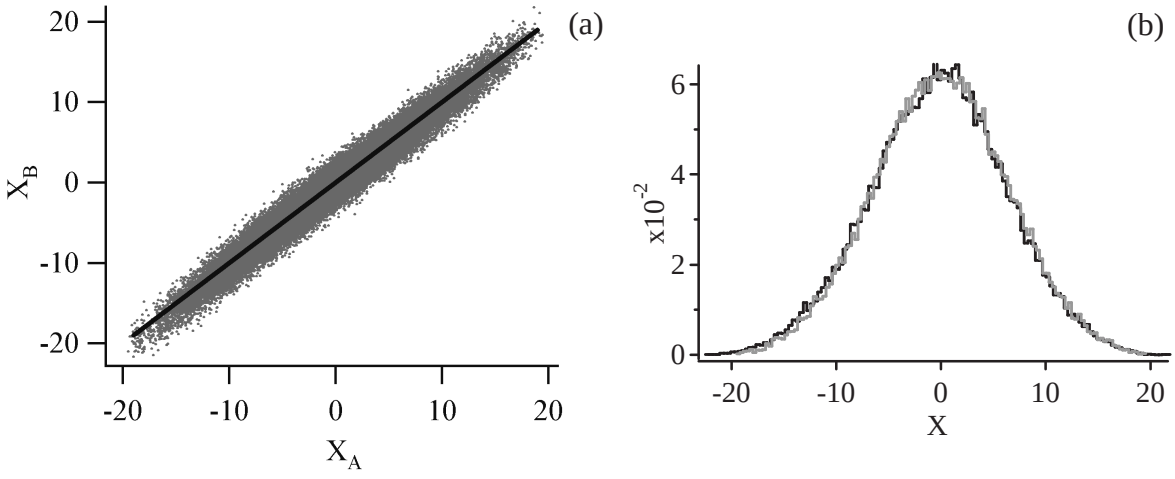

Figure 5.11: *(a) Quadrature mesurée X_B par Bob en fonction de la quadrature envoyée $\overline{X}_A$ par Alice pour un bloc de 60 000 points. La transmission du canal est de 100% et la variance de modulation vaut $V_A = 40.7$. La courbe en trait plein représente la droite de pente unité attendue. (b) Histogrammes des données d'Alice (gris) et de Bob (noir). La variance des données d'Alice vaut $V_A = 40.7$, celle des données de Bob vaut $V_B = 42.3$.*

Ce coefficient permet d'exprimer l'ensemble des caractéristiques selon :

$$G = \rho^2 \frac{V_B}{V_A} \tag{5.22}$$

$$\chi_{tot} = V_A \frac{1-\rho^2}{\rho^2} - 1 \tag{5.23}$$

$$I_{AB} = -\frac{1}{2}\log_2(1-\rho^2) \tag{5.24}$$

Les seuls paramètres nécessaires en plus du coefficient de corrélation sont les variances V_A et V_B des distributions d'Alice et Bob. Une propriété essentielle qui nous a fait préférer l'utilisation du coefficient ρ^2 est qu'il est indépendant du gain G et permet de s'affranchir ainsi de l'incertitude sur la calibration de la transmission.

Plus spécifiquement, pour évaluer le gain de la transmission lors de notre expérience, nous utilisons un faisceau intense à la place du faisceau signal d'Alice et mesurons directement au puissancemètre la transmission de la lame BS qui simule les pertes de la ligne entre Alice et Bob. La formule (5.22) est ensuite utilisée pour vérifier la calibration de la variance d'Alice, qui avait été effectuée avant le transfert par une mesure directe de la puissance maximale du signal émis (photodiode silicium calibrée avec une résistance de charge de 10 MΩ).

Afin d'estimer le bruit ajouté par la ligne, nous calibrons précisément les paramètres η_{hom} et χ_{elec} avant chaque transfert. Ceci nous permet de calculer le bruit total ajouté par la détection homodyne, et connaissant de plus le coefficient de corrélation ρ^2 entre Alice et Bob, les formules (5.23) et (5.20) permettent d'accéder au bruit ajouté par la ligne χ_{ligne}. En modifiant la transmission de la lame BS simulant les pertes de la transmission, nous avons mesuré ce coefficient de bruit ajouté par la ligne en fonction de la transmission de la lame G. Nos résultats expérimentaux sont présentés sur la figure 5.12, et suivent raisonnablement la prédiction théorique $\chi_{ligne} = (1-G)/G$, notre expérience ne faisant intervenir qu'un bruit additif provenant de pertes pures (l'excès de bruit en ligne ε_{ligne} est nul dans ce cas).

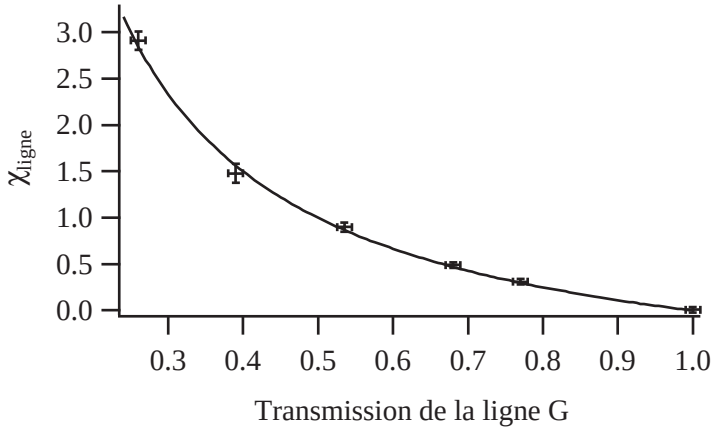

Figure 5.12: *Variance expérimentale χ_{ligne} du bruit équivalent en entrée en fonction de la transmission du canal G. La courbe en trait plein indique la prédiction théorique $(1-G)/G$.*

5.2.3 Caractérisation de l'espionnage

Les bruits ajoutés par la détection homodyne χ_{hom} et χ_{elec} sont clairement pris en compte dans le calcul (5.24) de l'information mutuelle I_{AB} entre Alice et Bob, que l'on peut par ailleurs exprimer selon :

$$I_{AB} = I_{BA} = \frac{1}{2}\log_2\left(1+\frac{V_A}{1+\chi_{tot}}\right) = \frac{1}{2}\log_2\left(1+\frac{V_A}{1+\chi_{ligne}+\frac{\chi_{hom}+\chi_{elec}}{G}}\right) \tag{5.25}$$

La question est plus délicate en ce qui concerne l'influence des bruits ajoutés par la détection de Bob sur l'évaluation de l'espionnage. Un premier point de vue – extrême – serait de considérer que tous les bruits dans le système de détection de Bob peuvent être contrôlés par Eve, qui peut intriquer librement ses faisceaux avec la détection de Bob. Ce point de vue constitue l'approche que nous qualifions de *paranoïaque*. Le paramètre pertinent pour évaluer l'action de l'espion dans les formules (4.10) et (4.26) est alors le bruit total χ_{tot} comprenant le bruit ajouté par la ligne ainsi que celui provenant de la détection homodyne. Le gain effectif à considérer est alors le produit $G\,\eta_{hom}$. L'information espionnée en réconciliation directe $I_{AE,par}$ ou inverse $I_{BE,par}$ dans la prise en compte "paranoïaque" du bruit de la détection s'écrit :

$$I_{AE,par} = \frac{1}{2}\log_2\left(1+\frac{V_A}{1+\frac{1}{\chi_{tot}}}\right) \tag{5.26}$$

$$I_{BE,par} = \frac{1}{2}\log_2\left(\frac{\eta_{hom}\,V_B}{\frac{1}{\eta_{hom}\,G\,(\chi_{tot}+1/V)}}\right) = \frac{1}{2}\log_2\left(G^2\,{\eta_{hom}}^2\,(V+\chi_{tot})\,(\frac{1}{V}+\chi_{tot})\right) \tag{5.27}$$

Dans une deuxième approche, appelée *réaliste*, nous pouvons considérer que puisque les bruits χ_{hom} et χ_{elec} proviennent de la détection homodyne de Bob, ces bruits ne peuvent pas contribuer à la connaissance d'Eve qui n'a pas accès à cette détection. La quantité pertinente pour quantifier l'espionnage est alors uniquement le bruit χ_{ligne} ajouté par la ligne de transmission, c'est à dire quand les états quantiques sont dans le domaine d'Eve. L'évaluation de l'information espionnée sur les données d'Alice (réconciliation directe) prend donc uniquement en compte χ_{ligne} pour

borner χ_E :

$$I_{AE,real} = \frac{1}{2}\log_2\left(1 + \frac{V_A}{1+\frac{1}{\chi_{ligne}}}\right) \tag{5.28}$$

Dans le cadre de la réconciliation directe, il découle de la définition de la variance conditionnelle que :

$$\begin{aligned} V_{B|E,real} &= V_{B|E,ligne} + \chi_{hom} + \chi_{elec} \\ &= \frac{1}{G(\chi_{ligne}+1/V)} + \chi_{hom} + \chi_{elec} \end{aligned} \tag{5.29}$$

car les bruits ajoutés par la détection homodyne sont des bruits indépendants. L'information espionnée sur les données de Bob (réconciliation inverse) s'exprime alors selon :

$$I_{BE,real} = \frac{1}{2}\log_2\left(\frac{V_B}{\frac{1}{G(\chi_{ligne}+1/V)} + \chi_{hom} + \chi_{elec}}\right) \tag{5.30}$$

Il faut préciser ici que cette prise en compte "réaliste" des bruits ne limite en rien les actions d'espionnage sur la ligne. Eve peut mettre en œuvre toutes les attaques compatibles avec l'évaluation de χ_{ligne} : duplicateur quantique optimal, mémoire quantique, source EPR parfaite...

Les informations mutuelles entre les partenaires sont représentées sur la figure 5.13 pour les paramètres expérimentaux réels et suivant les deux points de vue de prise en compte des bruits de la détection homodyne. On peut noter que même dans l'hypothèse "paranoïaque", notre système permet tout de même une extraction de clé secrète en réconciliation inverse pour les fortes transmissions. Par la suite, nous considérerons exclusivement l'approche "réaliste" où le bruit de la détection homodyne n'est pas contrôlé par Eve.

5.2.4 Extraction d'une clé secrète

Pour extraire une clé secrète binaire des données continues échangées, il faut utiliser un traitement informatique assez élaboré, réalisé par Gilles Van Assche, Kim-Chi Nguyen et Nicolas Cerf de l'Université Libre de Bruxelles avec qui nous avons collaboré pour la réalisation d'un dispositif complet de cryptographie quantique à impulsions cohérentes [73]. Ce traitement se décompose en deux étapes principales : la correction des erreurs (réconciliation directe ou inverse) et le filtrage de l'information espionnée (amplification de confidentialité).

Réconciliation par tranches

Le principe de l'extraction de données binaires et de la correction des erreurs repose sur l'utilisation d'un algorithme de "réconciliation par tranches" introduit par Gilles Van Assche, Jean Cardinal et Nicolas Cerf dans [56] et qui a été présenté dans la section 1.3.

Pour l'extraction de bits dans le cadre de notre expérience, cet algorithme décompose la distribution des données continues en $2^5 = 32$ intervalles et associe à chaque donnée continue un mot binaire de 5 bits correspondant au numéro de l'intervalle dans lequel se trouve la valeur continue. Le nombre d'intervalles ainsi que la largeur de chaque intervalle ont été optimisés numériquement compte tenu de nos rapports signal à bruit expérimentaux.

Du fait des pertes optiques, de l'espionnage et des bruits de la détection, différentes erreurs sont présentes dans ces chaînes binaires. Pour corriger ces erreurs suivant l'algorithme de réconciliation binaire *Cascade* [52, 57], notre traitement n'utilise pas la totalité des bits en une

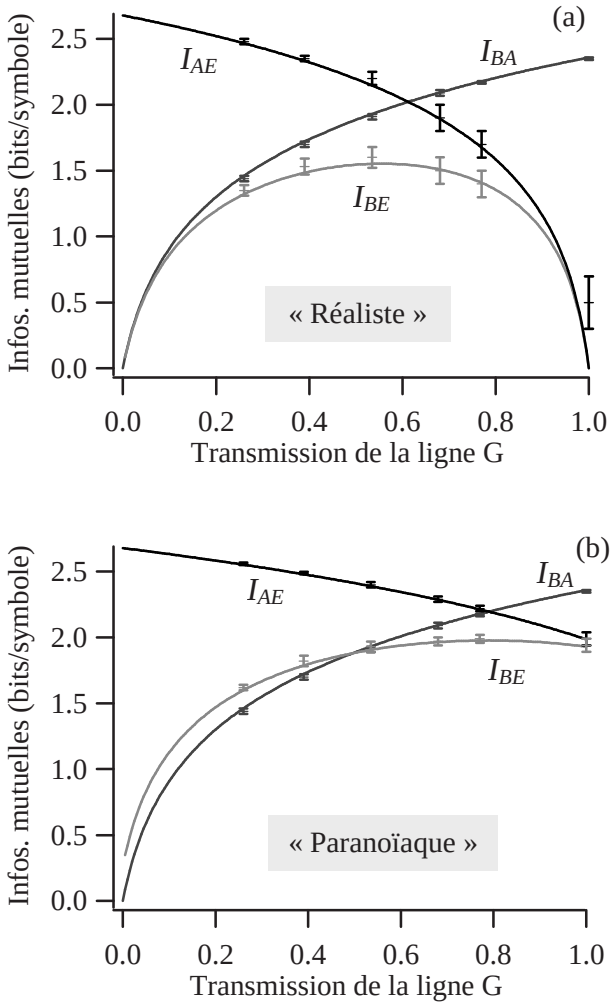

Figure 5.13: *Informations mutuelles I_{BA}, I_{BE} et I_{AE} en fonction de la transmission G du canal évaluées pour $V \approx 40$ et avec les bruits expérimentaux χ_{hom} et χ_{elec} réels pris en compte selon les hypothèses d'espionnage "réaliste" (a) ou "paranoïaque" (b). L'information mutuelle I_{BA} entre Alice et Bob est bien sûr inchangée suivant les hypothèses d'espionnage. La cryptographie par réconciliation directe fournit une clé secrète si $I_{AB} > I_{AE}$, la réconciliation inverse opère pour $I_{BA} > I_{BE}$.*

seule opération, mais discrimine entre les bits de poids différents. Plus précisément, on forme des ensembles de bits ("tranches") de niveaux successifs suivant le poids du bit au sein de chaque mot binaire. La première tranche contient tous les bits de poids faible des différentes impulsions, et ainsi de suite jusqu'à la cinquième tranche constituée des bits de poids forts. L'intérêt de cette procédure est de corriger successivement les différentes tranches, ce qui permet d'utiliser l'information déjà obtenue sur les tranches précédentes pour affiner l'estimation de la tranche suivante et extraire le maximum d'information au sens de Shannon.

Parmi les cinq ensembles de bits dont nous disposons, les deux premiers (de poids faibles, donc de fort taux d'erreur) sont simplement révélés, et ne servent qu'à améliorer la précision des estimations suivantes. Ces deux tranches sont ensuite supprimées et ne participent pas à

l'élaboration de la clé finale. Les trois tranches suivantes (de poids forts) sont ensuite corrigées séquentiellement en utilisant la procédure *Cascade*. Afin d'éviter qu'Eve utilise l'information échangée au cours de la procédure de réconciliation pour améliorer ses connaissances, Alice et Bob cryptent toutes leurs communications classiques avec un code de Vernam (*one-time-pad*) en utilisant une fraction des bits secrets préalablement échangés. Les blocs de parités échangés au cours de la procédure sont codés avec la même clé secrète par Alice et Bob [59], ce qui renseigne Eve sur la position des erreurs, mais ne l'informe pas de la valeur de ces erreurs. Eve peut toutefois obtenir une information supplémentaire en couplant sa connaissance des données avec la position des erreurs. Dans la procédure actuelle, cette quantité d'information est numériquement calculée et majorée en supposant une attaque par une cloneuse intriquante [73]. Cette information est ensuite supprimée lors de l'amplification de confidentialité.

Amplification de confidentialité

Afin de filtrer la connaissance de l'espion sur les éléments de clé, les bits réconciliés sont traités par une classe des fonctions de hachage [54], ce qui a pour effet de répartir les incertitudes d'Eve à l'ensemble des bits de clé finale dont elle n'aura aucune information. Dans notre cas, les bits corrigés sont considérés comme les coefficients d'un polynôme $r(x)$ dans le corps fini $GF(2^{110503})/p$ des polynômes à coefficients binaires modulo le polynôme premier $p(x) = x^{110503} + x^{519} + 1$. Le fait que cette opération soit connue et puisse être mise en œuvre efficacement a motivé notre choix [5]. Les bits secrets sont obtenus en multipliant le polynôme r par un polynôme arbitrairement choisi dans $GF(2^{110503})/p$ et publiquement annoncé. La clé finale est alors formée des coefficients binaires de la multiplication polynomiale, dont on ne conserve qu'un nombre déterminé par la borne sur l'information espionnée. Afin d'obtenir une taille de clé et une qualité de secret satisfaisantes, il est absolument crucial pour cette étape d'avoir une estimation aussi précise que possible de la quantité maximale d'information espionnée et des pertes d'information lors de la réconciliation. Enfin, le coût du codage de Vernam lors de la réconciliation est soustrait de la taille de la clé finale.

5.2.5 Taux de transferts expérimentaux

D'après le théorème de Csiszar et Körner [50, 51], la taille minimale $\mathcal{S}$ de la clé finale qu'il est possible d'extraire est donnée par $\mathcal{S} > \max(I_{AB} - I_{AE}, I_{BA} - I_{BE})$. Dans une mise en œuvre pratique, ce théorème n'est toutefois vrai que dans la mesure où les différentes parties parviennent à extraire suffisamment d'information de leur corrélations pour atteindre le taux d'information mutuelle au sens de Shannon. Si nous supposons que l'espion possède une capacité de calcul illimitée et peut atteindre les taux théoriques I_{AE} et I_{BE}, il n'en va pas de même pour la capacité de calcul de réconciliation entre Alice et Bob : des écarts inévitables de nos algorithmes réels à la limite de Shannon réduisent le taux d'information réconciliée I_{rec} entre Alice et Bob. Avec nos données expérimentales ($V \approx 40$, $\chi_{hom} + \chi_{elec} \approx 0.6$), l'efficacité des protocoles η_{rec} de réconciliation se situe autour de 85% pour le domaine des faibles atténuations du canal puis diminue entre 80% et 75% pour des atténuations plus fortes. Ceci permet d'extraire expérimentalement une information réconciliée I_{rec} égale à η_{rec} de la limite de Shannon I_{BA}. Le taux de transfert effectif de clé secrète est alors diminué pour valoir $\max(I_{rec} - I_{AE}, I_{rec} - I_{BE})$ et la portée effective de nos échanges est réduite. Pour une certaine transmission G_{min} telle que $I_{rec}(G_{min}) < I_{BE}(G_{min})$, Alice et Bob ne peuvent plus exploiter simplement leur avantage

[5] Le degré 110503 du polynôme permet de traiter 110503 bits à la fois, soit 3 tranches de 36800 impulsions ou 2 tranches de 55200 impulsions, ce qui a dirigé la structure des données optiques échangées.

V_A	G	Pertes (dB)	I_{BA} (bit)	I_{BE} ($\%I_{BA}$)	I_{rec} ($\%I_{BA}$)	Taux Réc. Inverse idéal (kbit/s)	Inverse effectif (kbit/s)	Taux Réc. Directe idéal (kbit/s)	Directe effectif (kbit/s)
40.7	1	0	2.39	0	88	1 920	1 690	1 910	1 660
37.6	0.79	1.0	2.17	58	85	730	470	540	270
31.3	0.68	1.7	1.93	67	79	510	185	190	–
26	0.49	3.1	1.66	72	78	370	75	0	–
42.7	0.26	5.9	1.48	93	71	85	–	0	–

Tableau 5.1: *Paramètres caractéristiques de l'échange de clé obtenus pour différentes valeurs de la transmission G du canal. Les différentes valeurs de la variance de la modulation d'Alice $V_A = V - 1$ sont dues à des ajustements expérimentaux différents. L'information I_{BA} est exprimée en bits par impulsion. I_{rec} est la quantité d'information obtenue par Alice et Bob avec nos algorithmes réels de réconciliation, exprimée en pourcentage de I_{AB}. Les taux idéaux seraient atteints par une réconciliation parfaite fournissant $I_{BA} - I_{BE}$ en réconciliation inverse et $I_{AB} - I_{AE}$ en direct, alors que les taux effectifs sont ceux obtenus avec notre procédure réelle (le bruit ajouté par la détection de Bob est considéré suivant l'approche "réaliste" où Eve ne contrôle pas ce bruit). Les débits d'information sont tous exprimés pour des blocs de 60 000 impulsions à 800kHz et ne prennent pas en compte le rapport cyclique (5%) de notre dispositif expérimental, ni la durée du traitement classique des données.*

quantique en réconciliation inverse, tandis que notre dispositif expérimental ne fournit plus de clé secrète.

Le tableau 5.1 présente les différents résultats de taux de transfert pour la réconciliation directe et inverse en fonction de la transmission G de la ligne. Les taux idéaux correspondent à la limite de Shannon, tandis que les taux effectifs prennent en compte notre efficacité limitée de réconciliation. Dans le cas des transmissions sans pertes avec une modulation $V \approx 40$, notre dispositif atteint le taux net de clé secrète de 1.7 Mbits/s, à comparer à une limite théorique attendue de 1.9 Mbits/s.

Avec une modulation $V \approx 40$ et une réconciliation inverse, la transmission minimale G_{min} pour extraire expérimentalement une clé secrète se situe autour de 55%. Cette transmission est alors principalement limitée par notre efficacité de réconciliation $\eta_{rec} = 80\%$. Afin d'améliorer la portée expérimentale, il est avantageux de diminuer la variance de modulation, ce qui atténue les informations mutuelles I_{BA} et I_{BE}, mais augmente le quotient I_{BA}/I_{BE} (voir la courbe 5.14). L'information à filtrer lors de l'amplification de confidentialité est donc plus faible, ce qui permet d'atteindre expérimentalement la portée de $G = 49\%$ (3.1 dB) pour $V = 27$ avec un débit de 75 kbits/s. Ceci démontre que la réconciliation inverse avec des états cohérents peut fonctionner au-dessus de la limite théorique de 3 dB des protocoles à réconciliation directe.

Une amélioration de l'efficacité de réconciliation η_{rec} se traduirait immédiatement par une augmentation de la portée de notre système. Par ailleurs, nous pourrions également limiter les possibilités d'attaques de l'espionnage : dans les deux approches "réaliste" et "paranoïaque", nous supposons toujours que l'espion dispose de dispositifs quantiques parfaits et que sa capacité de calcul est infinie. Si ces hypothèses étaient quelque peu relâchées, la portée de notre dispositif pourrait être étendue au-delà de la limite actuelle. Cependant, cette démarche n'a pas été poursuivie car nous considérons qu'il n'est pas dans le principe de la cryptographie quantique de poser des limites technologiques aux actions d'espionnage. [6]

[6] Même si on considère la prise en compte "paranoïaque" des bruits de la détection homodyne, le taux de secret

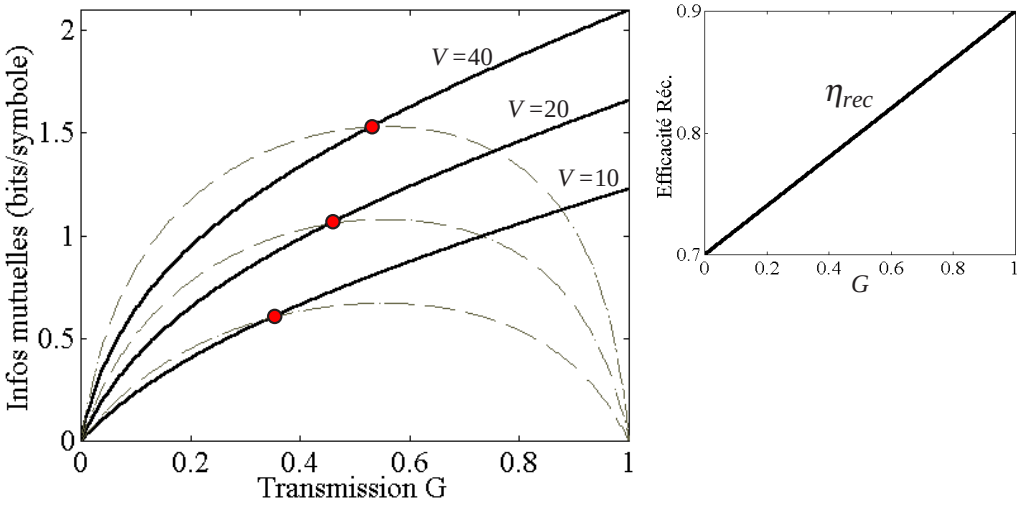

Figure 5.14: *Informations $I_{rec} = \eta_{rec} I_{BA}$ (trait plein) et I_{BE} (tirets) en fonction de la transmission G et de la variance de modulation V avec les bruits $\chi_{hom} = 0.27$ et $\chi_{elec} = 0.33$ pris en compte de façon "réaliste" et dans le cas d'un bruit du canal $\chi_{ligne} = (1-G)/G$. L'efficacité de réconciliation η_{rec} est supposée varier linéairement entre 70% pour les faibles transmissions et 90% pour les fortes transmissions (courbe de droite), ce qui est confirmé par le tableau 5.1. De plus, l'approximation simple considère que η_{rec} est indépendante de V pour $10 < V < 40$. Les points indiquent la portée maximale effective où $I_{rec} = I_{BE}$. Cette portée augmente lorsque V diminue car le ratio I_{BA}/I_{BE} devient alors plus avantageux, bien que la quantité d'information nette soit plus faible.*

5.2.6 Conclusions sur notre démonstration expérimentale

Une démonstration expérimentale *complète* du principe de distribution de clé quantique avec des états cohérents a été réalisée, incluant l'échange d'états quantiques et l'extraction algorithmique d'une clé secrète. Notre système a ainsi généré une clé secrète à un débit de 1.7 Mbits/s en l'absence de pertes et 75 kbits/s pour une transmission présentant 3.1 dB de pertes, soit dans un cas où l'espion dispose virtuellement de plus de 50% du faisceau signal. Cet ensemble constitue le premier dispositif complet et sûr de cryptographie quantique avec des variables continues [73].

De très hauts débits d'information sont ainsi atteignables tant que l'atténuation du canal de transmission n'est pas trop grande. Dans le domaine des fortes pertes, la portée de notre protocole est pour le moment limitée par l'efficacité de nos algorithmes de réconciliation, mais ses performances intrinsèques demeurent élevées par rapport aux protocoles à photons uniques [40]. A ce sujet, il faut garder à l'esprit que le domaine de la cryptographie quantique avec des variables discrètes bénéficie de progrès notables et d'un recul acquis au cours de dix années de développement depuis la première démonstration par Bennett et Brassard en 1992, alors qu'en comparaison notre première démonstration expérimentale avec des variables continues n'a été effectuée qu'en 2002.

Les limitations actuelles étant essentiellement de nature technologique (absence de modulateurs efficaces à 780nm, programmation de la réconciliation,...), de nombreuses améliorations restent possibles, tant sur le point du dispositif optique (cadence augmentée, réduction du bruit

effectif en réconciliation inverse pour une ligne sans pertes reste non-nul et vaut 195 kbits/s (le taux idéal serait de 420 kbits/s), ce qui atteste de la robustesse et du niveau de sécurité de notre système.

électronique, amélioration de l'efficacité homodyne...) que des logiciels de réconciliation (réconciliation multi-dimensionnelle [56], utilisation de turbo-codes [53, 60], nouveaux algorithmes de réconciliation binaire [58]...). La voie apparaît donc ouverte pour des protocoles simples et efficaces de cryptographie quantique à hauts débits, dont nous détaillons certaines perspectives à la section suivante.

5.3 Perspectives pratiques

5.3.1 Distances et débits atteignables

Afin d'être plus quantitatif sur les perspectives à court terme de ce dispositif, quelques éléments pratiques peuvent être avancés dans l'estimation des débits et des portées maximales atteignables de manière réaliste. Concernant le domaine des fortes transmissions ($G \approx 100\%$), il est raisonnable de concevoir une détection homodyne fonctionnant à une cadence de quelques MHz. A titre d'exemple, nous prenons 5 MHz, ce qui correspond à la vitesse maximale de la carte d'acquisition. Avec une modulation $V = 100$, notre détection homodyne à amplification de charge réalisant $\chi_{hom} = 0.25$ ($\eta_{hom} = 80\%$) et $\chi_{elec} = 0.01$, une efficacité de réconciliation $\eta_{rec} = 95\%$ aux fortes transmissions, on obtient pour $G = 1$ et dans le cas d'une absence de bruit ajouté ($\varepsilon = 0$) un taux secret net $\underleftarrow{\Delta I} = 3$ bits/impulsion, soit un débit secret net de 15 Mbits/s. Si on intègre de plus un faible bruit ajouté lors de l'échange $\varepsilon = 0.1$, le taux de secret aux fortes transmissions demeure à $\underleftarrow{\Delta I} = 1.3$ bits/impulsion, soit un débit de 6.5 Mbits/s.

Concernant la distance maximale atteignable de façon réaliste avec nos protocoles, notre dispositif a déjà obtenu le résultat d'échanger une clé secrète pour une transmission $G = 0.49$ soit des pertes de 3.1 dB, que l'on associe à une distance atteignable de l'ordre de 15 km lors d'une transmission par fibre optique (étendue au domaine 1.55 μm avec des pertes standard de 0.2 dB/km). En améliorant sensiblement le dispositif tel que décrit dans le paragraphe précédent (débit 5 MHz, bruit $\chi_{hom} = 0.25$, $\chi_{elec} = 0.01$) et en optimisant la variance de modulation à $V = 15$, ce système atteindrait la transmission de $G = 0.32$ (pertes 5 dB ou distance de 25 km) avec un taux de transfert de $\underleftarrow{\Delta I} = 0.05$ bits/impulsion, soit un débit appréciable de 250 kbits/s. L'efficacité de réconciliation requise pour ce niveau est $\eta_{rec} = 85\%$, ce qui semble encore tout à fait raisonnable.

5.3.2 Prototype complet

L'essentiel des limitations du dispositif optique actuel provient de l'absence de modulateurs d'amplitude et de phase adéquats à 780 nm. Afin d'éviter de plus une forte atténuation lors d'une propagation fibrée, il est judicieux de concevoir un système opérant aux longueurs d'ondes télécom (1540-1580 nm) où la technologie commercialement disponible est plus appropriée. Par ailleurs, du fait des problèmes de stabilisation de la phase, il n'est pas réaliste de transmettre séparément le faisceau oscillateur local et le faisceau signal. Une possibilité serait alors de transmettre dans la même fibre optique les impulsions signal et oscillateur local décalées temporellement d'une durée relativement faible (typiquement 5 ns pour un modulateur au GHz et des impulsions de durée 1 ns). La figure 5.15 donne un schéma de principe d'un dispositif optique de ce type. Les impulsions suivent alors sensiblement le même chemin optique et toute perturbation de phase de fréquence inférieure à la centaine de MHz n'affectera pas la phase relative. Pour faire interférer l'impulsion signal avec l'impulsion oscillateur local correspondante, il faut séparer à nouveau les impulsions afin de compenser le retard introduit. Cette opération doit impérativement conserver la phase relative, mais comme la démodulation est effectuée au sein

de l'unité réceptrice et ne fait intervenir que des bras d'interféromètre de quelques mètres (1.5 m pour un décalage de 5 ns), la conservation de la phase relative devrait être plus simple à réaliser expérimentalement. Ce dispositif demeure cependant une réalisation technologique d'envergure et se heurte à de nombreux autres problèmes comme le maintien de la polarisation ou les pertes d'insertion dans le démodulateur.

Dans le cadre du projet européen *SECOQC* (*SEcure COmmunication based on Quantum Cryptography*), un partenariat avec la société *Thalès* est actuellement en cours afin de réaliser un prototype complet de cryptographie quantique avec des états cohérents opérant à la longueur d'onde télécom 1.55 μm. Notre équipe a ainsi l'opportunité de collaborer spécifiquement avec Mrs. Thierry Debuisschert (*Thalès TRT*) et Jérôme Lodewyck (*Thalès TRT / LCFIO*).

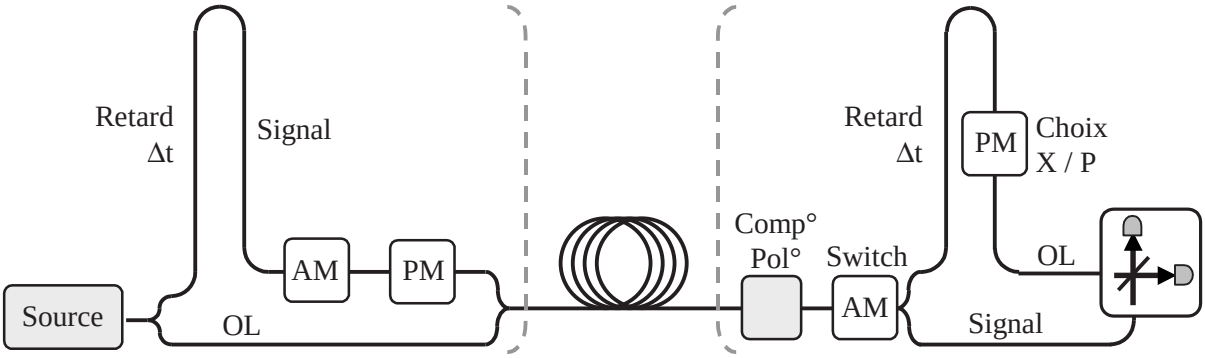

Figure 5.15: *Esquisse de prototype de cryptographie quantique avec des impulsions cohérentes. Pour ce dispositif, les impulsions signal et oscillateur local sont décalées temporellement de* $\Delta t \approx$ *quelques ns. AM : modulateur d'amplitude, PM : modulateur de phase.*

5.3.3 Que faire avec des bits parfaitement secrets ?

Cette question quelque peu iconoclaste a été soulevée par Gilles Brassard [204]. Si la très large majorité des protocoles de cryptographie quantique conçoit le transfert de clé secrète pour une utilisation ultérieure avec un code de Vernam (*one-time-pad*), cette application n'est peut-être pas forcément la plus adéquate. En effet, bien que depuis la démonstration de Shannon [41], le code de Vernam est connu pour être parfaitement sûr (lorsque la clé binaire aléatoire est aussi longue que le message et utilisée une seule fois), ce code est également connu pour souffrir d'un débit lent et d'une forte consommation de bits secrets.

Une autre possibilité [204] – non inconditionnellement sûre – serait d'utiliser les bits secrets pour effectuer un cryptage à clé privée de type AES [39] sur 128 bits et d'utiliser des techniques standard d'expansion de clé. Ce dispositif permet alors de hauts débits de cryptage. De plus, si le canal quantique fonctionne en parallèle, il est tout à fait possible de changer de nombreuses fois par seconde les 128 bits secrets de la base AES, ce qui fournirait déjà un niveau de sécurité inégalé pour ces débits.