Cryptographie quantique

Ce dernier chapitre est consacré aux expériences de cryptographie quantique que nous avons effectuées avec notre source de photons uniques polarisés. Après une description succincte du protocole de cryptographie quantique utilisé, je détaillerai le principe de fonctionnement de notre prototype et présenterai les résultats que nous avons obtenus. Les performances de notre montage de cryptographie seront ensuite comparées à celles d'autres réalisations actuelles de cryptographie quantique, basées sur des sources cohérentes atténuées.

6.1 Principe du protocole de cryptographie

Pour distribuer une clé de codage quantique (Quantum Key Distribution: QKD), nous allons coder l'information sur l'état de polarisation d'un photon unique. Soit un photon dont l'état de polarisation $|\psi\rangle$ dans la base de polarisation $|H\rangle$ et $|V\rangle$ (Horizontale et Verticale) est $|\psi\rangle = \alpha\,|H\rangle + \beta\,|V\rangle$ avec la normalisation $|\alpha|^2 + |\beta|^2 = 1$. Une mesure effectuée à l'aide d'un cube séparateur de polarisation revient à projeter l'état de polarisation sur l'un des vecteurs de base. La probabilité que le photon soit transmis est alors $T = |\alpha|^2$, tandis que celle qu'il soit réfléchi est $R = |\beta|^2$. Si on prépare le photon avec $\alpha = 1$ ou $\beta = 1$, alors on connaît par avance avec certitude le résultat de la mesure.

Si au contraire on choisit $\alpha = 1/\sqrt{2}$ et $\beta = \pm i/\sqrt{2}$ (polarisation circulaire), alors les probabilités pour que le photon soit transmis ou réfléchi sont égales et données par $T = R = 1/2$. Par contre, le résultat sera parfaitement déterminé si, pour faire la mesure, on effectue un changement de base et l'on se place dans la base circulaire, soit $|D\rangle = 1/\sqrt{2}\,|H\rangle + i/\sqrt{2}\,|V\rangle$ et $|G\rangle = 1/\sqrt{2}\,|H\rangle - i/\sqrt{2}\,|V\rangle$. On peut donc coder un bit d'information sur l'état de polarisation d'un photon unique, mais cette information ne pourra être lue que si l'on connaît la base de polarisation dans laquelle elle a été codée.

La propriété de la mécanique quantique qui va garantir la sécurité de la transmission de la clé est le théorème de non-clonage : il n'est pas possible de copier parfaitement un état quantique inconnu [6]. Une démonstration par l'absurde montre cette impossibilité.

Supposons qu'il existe un opérateur unitaire de clonage U capable de dupliquer l'état d'un qubit[1] sur un autre, et qui s'écrirait (en recopiant l'état du premier qubit sur le second) :

$$\begin{cases} |0\rangle\,|0\rangle \xrightarrow{U} |0\rangle\,|0\rangle \\ |1\rangle\,|0\rangle \xrightarrow{U} |1\rangle\,|1\rangle \end{cases} \tag{6.1}$$

[1] Un qu-bit est l'équivalent quantique d'un bit d'ordinateur classique. Il se distingue du fait qu'il peut être dans une superposition des états $|0\rangle$ et $|1\rangle$

On veut copier à l'aide de l'opérateur U l'état $|\varphi\rangle = (a\,|0\rangle + b\,|1\rangle)$ sur l'état $|0\rangle$, il faut donc réaliser la transformation :

$$|\varphi\rangle\,|0\rangle \xrightarrow{U} |\varphi\rangle\,|\varphi\rangle = a^2\,|0\rangle\,|0\rangle + b^2\,|1\rangle\,|1\rangle + ab\,(|0\rangle\,|1\rangle + |1\rangle\,|0\rangle) \tag{6.2}$$

Or les opérateurs de la mécanique quantique sont linéaires et d'après 6.1

$$(a\,|0\rangle + b\,|1\rangle)\,|0\rangle \xrightarrow{U} a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|1\rangle \tag{6.3}$$

Les équations 6.2 et 6.3 sont contradictoires, sauf dans le cas particulier où $ab = 0$. Il n'est donc pas possible de cloner un état arbitraire. Appliqué à la cryptographie quantique, ceci implique qu'un espion n'est pas capable de recopier un qubit, choisi arbitrairement dans un ensemble d'états non orthogonaux.

6.1.1 Le protocole BB84

Le protocole BB84, introduit en 1984 par Bennett et Brassard, est la réalisation concrète de la méthode de cryptage suggérée au paragraphe précédent. C'est actuellement le protocole QKD à variables discrètes le plus utilisé. Initialement, il a été prouvé que le protocole est inconditionnellement sûr à condition d'utiliser des particules uniques et des détecteurs parfaits [90, 91]. Par la suite, il a été prouvé sûr pour des états plus proches des réalisations expérimentales, à condition de prendre quelques précautions [12, 13] (voir discussion à la fin de ce chapitre).

Dans le protocole BB84 on choisit deux bases de codage de l'information. La première est la base des polarisations linéaires horizontales et verticales $|H\rangle$ et $|V\rangle$, la seconde correspond aux polarisations circulaires droite et gauche (respectivement $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i\,|V\rangle)$ et $|G\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i\,|V\rangle)$).

Si l'on n'utilise qu'un seul photon à la fois, il est impossible de connaître exactement l'état du photon, si l'on ne connaît pas la base dans laquelle il a été préparé. En utilisant ces deux bases, on peut écrire le protocole de communication (BB84) entre Alice et Bob :

- Alice choisit au hasard une base puis une polarisation dans cette base.
- Elle prépare ainsi un photon unique dans un des quatre états ($|H\rangle\ |V\rangle\ |D\rangle\ |G\rangle$) qu'elle envoie à Bob.
- Bob choisit au hasard une base dans laquelle il va faire la mesure de l'état de polarisation.
- A la fin de la communication dite quantique, Alice et Bob révèlent publiquement la base qu'ils ont choisie pour coder ou analyser la polarisation. Dans le cas où le choix n'est pas le même, le bit reçu est écarté. Sinon il est utilisé comme bit de la clé secrète. Cette information n'est échangée que pour les bits où Bob a reçu un photon.

Le tableau 6.1 résume le protocole BB84.

Remarques : On remarque qu'à la fin de la communication, Alice et Bob ne partagent que quelques bits d'information. Ceci n'est pas un problème en soi, puisque la communication ne transporte aucun message. Elle est seulement constituée d'une suite de nombres aléatoires, qui forment la clé secrète. Alice et Bob peuvent ensuite utiliser cette clé pour coder un message qu'ils échangerons par voie classique[2]. Le codage de choix sera bien sûr le code de Vernam si la clé est aussi longue que le message.

[2] Par voie classique on désigne tous les moyens de communications usuels

	Bit 1	Bit 2	Bit 3	Bit 4	Bit 5	Bit 6	Bit 7	Bit 8	Bit 9	Bit 10
Alice Base	HV	HV	DG	DG	DG	HV	DG	DG	HV	HV
Alice Bit	0	1	1	0	0	0	1	1	1	0
Bob Base	HV	DG	DG	HV	DG	HV	DG	HV	HV	DG
Bob Bit	0	1	1	1	0	0	1	0	1	0
Clé Secrete	0	-	1	-	0	0	1	-	1	-

Tableau 6.1: *Tableau récapitulatif du protocole BB84*

Ce protocole est en principe inconditionnellement sûr. Néanmoins, des imperfections dans la réalisation peuvent créer des failles de sécurité. Elles seront étudiées plus tard dans ce chapitre.

6.2 Réalisations actuelles

Depuis la première expérience de cryptographie quantique réalisée en 1992 par Bennett et Brassard sur une distance de 30 cm [8], plusieurs expériences se sont succédées sur différentes distances et avec différents milieux de propagation. Ces expériences ont été réalisées avec deux approximations de sources de photons uniques : une source cohérente atténuée, et une source de photons intriqués. Un très bon aperçu de l'état de l'art est donné dans la référence [10].

6.2.1 Source cohérente atténuée

Une façon simple de simuler une source à photons uniques est d'atténuer la lumière d'un laser impulsionnel. La statistique du nombre de photons par impulsion est régie par la distribution poissonnienne. Ainsi pour un nombre moyen de $\mu = 0.1$ photon par impulsion, on obtient 90.5% d'impulsions vides, 9% d'impulsions contenant 1 photon, et 0.5% d'impulsions contenant deux photons.

A l'air libre, une clé secrète a été échangée sur 1.9 km [92] ainsi que sur 0.5 km [93]. Les problèmes essentiels sont les fluctuations de l'atmosphère, ainsi que la lumière parasite. La réalisation la plus récente a atteint une portée de 23.4 km en montagne [94].

Dans des fibres optiques, l'échange de clé est compliqué à cause de la biréfringence naturelle des fibres optiques, qui introduit des erreurs dans la polarisation. La biréfringence dépend aussi des contraintes que subit la fibre. Une méthode possible pour éliminer ce défaut, mise en œuvre à l'Université de Genève, est de faire effectuer à la lumière un aller-retour dans la fibre optique, après réflexion sur un miroir de Faraday [95, 96]. Ces systèmes sont actuellement disponibles commercialement chez idQuantique [11].

Les prototypes décrits plus haut utilisent la polarisation pour coder l'information. Il est également possible d'utiliser comme base de codage la phase qu'acquiert le photon unique en traversant un interféromètre chez Alice, et chez Bob. Cette base de codage à l'avantage d'être insensible à la biréfringence de la fibre. On peut citer plusieurs réalisations sur 48 km [97, 98]. Par contre cette méthode nécessite une bonne stabilisation des interféromètres.

Une autre approche originale [99] utilise la modulation de la phase des photons uniques. L'avantage de cette méthode est de ne pas avoir besoin de stabiliser les interféromètres. De plus, tout les éléments optiques sont fibrés, tiennent dans un espace réduit, et sont faciles à mettre en place. Par contre, il est nécessaire de transmettre aussi un signal RF (hyperfréquence) de synchronisation pour pouvoir reconstituer la phase optique.

6.2.2 Avec des photons intriqués

Un autre implémentation de la cryptographie quantique est possible suivant le protocole proposé initialement par Artur Ekert [100]. Pour cela on utilise une paire de photons intriqués, et Alice et Bob reçoivent chacun un photon de la paire. De nouveau Alice et Bob choisissent indépendamment la base de mesure pour chaque photon, et révèlent leur choix à la fin de la transmission. Pour détecter une intervention d'Eve, Alice et Bob effectuent ensuite une expérience de violation des inégalités de Bell. Dans le cas où le message a été intercepté, l'intrication disparaît et les inégalités de Bell ne sont pas violées. Ce protocole a été mis en œuvre pour des paires intriquées en polarisation [101, 102], ainsi qu'en temps-énergie [103, 104].

6.2.3 Avec des photons uniques

Dans la première partie de la thèse nous avons mis en place une source efficace de photons uniques, stable et facile à mettre en œuvre. Dans cette partie, nous allons utiliser cette source, pour la distribution de clé quantique. Nous allons voir que le prototype ainsi réalisé peut transmettre environ 8000 bits secrets par seconde sur une distance de 50 m, ce qui est la première réalisation de cryptographie quantique avec des photons uniques "à la demande" [105]. Le démonstrateur se compose de deux parties : l'émetteur (Alice), et le récepteur (Bob), que nous allons décrire successivement.

6.3 Alice

La partie émetteur du démonstrateur comporte la source de photons uniques, un modulateur électro-optique pour coder l'information, ainsi que toute l'électronique de contrôle pour synchroniser l'expérience.

6.3.1 Le modulateur électro-optique

La modulation de la polarisation suivant un des quatre états de BB84 est obtenue grâce à un modulateur électro-optique. Son principe de fonctionnement est équivalent à une lame de phase, dont on peut choisir le déphasage en fonction de la tension appliquée, l'application d'un champ électrique statique ayant pour effet de modifier les indices du cristal anisotrope. Le déphasage (Γ) introduit par le cristal entre les deux modes propres de propagation va modifier la polarisation de l'onde en sortie du cristal. On a:

$$\Gamma = \frac{2\pi\Delta n L}{\lambda} = \frac{2\pi m \lambda_0}{\lambda} \tag{6.4}$$

où $\Delta n = n_e - n_o$ est la différence d'indice entre l'axe ordinaire et extraordinaire, L la longueur du cristal, et m l'ordre du modulateur pour la longueur d'onde λ_0. Le déphasage n'est pas le même pour toutes les longueurs d'onde, et il varie d'autant plus que l'ordre est élevé. Pour moduler une source à spectre large comme les centres NV, il faudrait travailler avec un ordre faible, de préférence égal à un, et donc une petite valeur de L. Mais dans un modulateur électro-optique, une longueur de cristal L relativement importante est nécessaire pour pouvoir introduire un déphasage de π sans avoir à appliquer une tension trop importante. Il est donc nécessaire de compenser cet effet.

6.3.1.1 Compensation

A tension nulle, on souhaite que le modulateur n'introduise pas de déphasage. Pour cela on utilise deux cristaux orientés de façon à ce que les axes ordinaire et extraordinaire de l'un soient respectivement confondus avec les axes extraordinaire et ordinaire de l'autre. Ainsi le déphasage accumulé à la traversée du premier cristal est annulé par le deuxième. Cependant, de petites imperfections sur la taille des cristaux ne permettent en général pas de s'affranchir de la totalité de la biréfringence. Nous devons donc éliminer cette biréfringence résiduelle avec une lame de compensation. Pour mesurer l'ordre résiduel du modulateur, on le place entre polariseur et analyseur croisés. La transmission après l'analyseur s'écrit :

$$T = sin^2\left(\Gamma/2\right) \tag{6.5}$$

En éclairant le système avec une lumière blanche, on obtient en sortie un spectre cannelé. Comme on l'observe sur la figure 6.1, l'ordre résiduel du modulateur est encore relativement élevé.

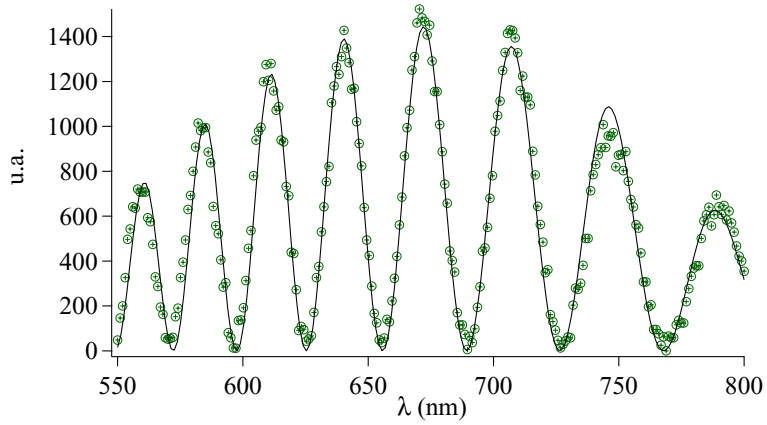


Figure 6.1: *Spectre de la lumière blanche après passage par le modulateur électro-optique placé entre polariseur et analyseur croisés (cercles). La courbe représente un ajustement avec une lame de quartz.*

La compensation du modulateur n'est pas évidente. En effet, la lame de compensation doit avoir une dépendance en longueur d'onde de l'indice ordinaire et extraordinaire proche de celle du cristal du modulateur. Notre modulateur est composé de quatre cristaux d'ADP (Ammonium Dihydrogen Phosphate) en ordre de compensation. Par contre la lame de compensation sera en quartz, en raison de contraintes de fabrication. Les valeurs de n_o et n_e pour le quartz et l'ADP sont données dans le tableau 6.2 pour le domaine spectral qui nous intéresse.

Un ajustement linéaire de Δn^q et Δn^{ADP} sur une plage de 660nm à 800nm donne $\Delta n^q = 0.009769 - 1.1177 \cdot 10^{-6} \times \lambda(nm)$ et $\Delta n^{ADP} = -.053125 + 12.944 \cdot 10^{-6} \times \lambda(nm)$. Il y a donc un ordre de grandeur entre la pente du quartz et celle de l'ADP. La simulation montre qu'il est quand même possible de compenser approximativement les deux cristaux sur une plage de 100 nm. Comme le spectre d'émission d'un centre NV a une largeur à mi-hauteur de 50 nm, cette compensation pourra être suffisante.

Pour calculer l'épaisseur de la lame de compensation à utiliser, il faut ajuster la courbe expérimentale donnée sur la figure 6.1 avec la formule 6.5, en prenant en compte la dépendance de Δn en fonction de la longueur d'onde pour la lame de quartz. On obtient ainsi l'épaisseur de la lame à

λ (nm)	n_o^q	n_e^q	Δn^q	λ (nm)	n_o^{ADP}	n_e^{ADP}	Δn^{ADP}
508.6	1.54822	1.55746	0.00924	532	1.52775	1.4815	-0.04625
589.3	1.54424	1.55335	0.00911	589.3	1.52418	1.47869	-0.045450
670.8	1.54145	1.55047	0.00902	632.8	1.5222	1.4773	-0.0448999
768.2	1.53903	1.54794	0.00891	656.3	1.52097	1.47633	-0.0446399
832.5	1.53773	1.54661	0.00888	694.3	1.5195	1.4754	-0.0441
				706.5	1.5189	1.47489	-0.04401

Tableau 6.2: *Indices n_o et n_e pour le quartz et l'ADP en fonction de la longueur d'onde*

utiliser pour compenser le modulateur, qui est de 1.378 mm, soit un ordre de $m = 17.68$ pour une longueur d'onde de 700 nm.

Par ailleurs nous avons jusqu'à présent supposé que l'incidence sur la lame de compensation était normale à la surface. Mais si l'on incline la lame autour de l'axe optique, ou bien perpendiculairement à celui-ci, l'ordre vu par l'onde lumineuse est modifié. Nous disposons ainsi d'un réglage fin de la compensation. L'équation 6.6 donne l'évolution de l'ordre en fonction du vecteur d'incidence $\vec{u} = (x, y, z)$.

$$m = \frac{e}{\lambda} \times \left[n_e \sqrt{1 - \frac{x^2}{n_o^2} - \frac{y^2}{n_e^2}} - n_o \sqrt{1 - \frac{x^2 y^2}{n_o^2}} \right] \tag{6.6}$$

où e est l'épaisseur de la lame, n_o l'indice ordinaire et n_e l'indice extraordinaire. Sur la figure 6.2 on a reporté l'ordre de la lame en fonction de l'inclinaison de la lame de quartz perpendiculairement à l'axe optique, ou autour de l'axe. On remarque qu'avec une inclinaison de 15^o on obtient un changement de l'ordre de 0.5. Cette inclinaison permet donc effectivement un réglage fin de la compensation.

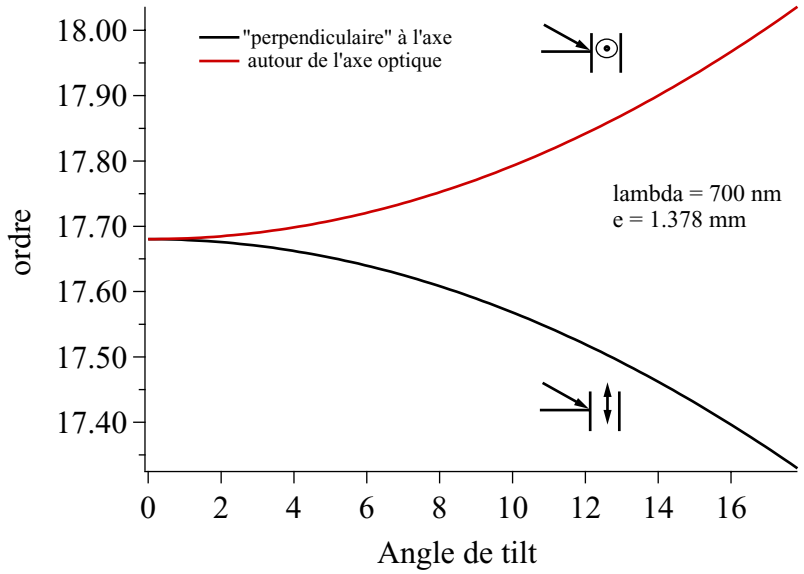


Figure 6.2: *Ordre de la lame de compensation en fonction de l'angle d'inclinaison*

6.3.1.2 Modulation

Nous allons maintenant étudier la dépendance du déphasage en fonction de la tension appliquée. Celle-ci s'écrit, pour un modulateur compensé:

$$\Gamma = \pi \frac{V}{V_\pi} \tag{6.7}$$

avec $V_\pi = \frac{\lambda d}{n_o^3 r L}$ où L est la longueur du cristal, d son épaisseur et r un facteur du tenseur électro-optique. V_π correspond à la tension qu'il faut appliquer sur le modulateur pour avoir l'équivalent d'une lame demi-onde: si la polarisation incidente est à 45^o de l'axe optique du modulateur, ce dernier tournera la polarisation de 90^o. La valeur de V_π est fixée par les dimensions et la composition du cristal. Dans le cas de notre modulateur (*Linos-LM0202*) la tension V_π donnée par le constructeur est $V_\pi = 160$ V à 488 nm, ce qui implique que $V_\pi = 230$ V à 700 nm.

La fréquence maximale de modulation est fixée par la charge capacitive du modulateur, soit une coupure à -3 dB à 100 MHz.

Pour le codage du protocole BB84, il nous faut 4 tensions différentes qui produiront 2 polarisations linéaires, et 2 circulaires. On choisit donc les tensions V_0, $V_{\pi/2}$, V_π et $V_{3\pi/2}$ soit 0V, $115V$, 230V, et 345V, ce qui équivaut aux polarisations H D V G (Horizontale, Circulaire Droite, Verticale, Circulaire Gauche) respectivement.

6.3.1.3 Précision nécessaire sur la compensation

Pour réussir nos expériences de cryptographie quantique, la compensation par la lame de quartz doit être très précise. Dans le tableau ci-dessous nous avons reporté le taux d'erreur pour chacune des polarisations du protocole BB84 en fonction de l'ordre résiduel après compensation par la lame de quartz. Ces taux sont obtenus en modélisant le spectre d'émission d'un centre NV (voir figure 2.2) par une gaussienne centrée à 700, nm avec une largeur à mi-hauteur de 50 nm.

m	H	V	D	G	Moyenne
0	0	0.24%	0.24%	0.93%	0.35%
1	0.07%	2.1%	2.1%	3.6%	2.1%
2	3.6%	5.6%	5.6%	7.7%	5.6%

D'après le tableau on voit qu'il faut avoir une précision de 1 ordre sur la compensation pour minimiser le taux d'erreur global.

6.3.1.4 Mise en œuvre

Lors du protocole BB84, pour chaque photon, Alice choisira aléatoirement l'une des quatre tensions de polarisation. La commutation entre deux tensions successives doit s'effectuer à la cadence imposée par la source de photons uniques. Plus précisément, le taux de répétition de la source est de 5.3 MHz $= 1/187.5$ ns (voir section 5) et la durée de vie du centre NV de $\Gamma_{NV}^{-1} \approx 23$ ns (voir section 3.6.1 et 5.2.2.1). La durée de vie donne une incertitude sur le temps d'arrivée du photon au niveau du modulateur. En effet 90% des photons seront émis dans une fenêtre de $2.2 \times \Gamma_{NV}^{-1}$ après l'impulsion excitatrice. La tension aux bornes du modulateur doit donc être impérativement maintenue pour une durée minimum de 50 ns. Il ne reste donc que $187.5 - 50 = 137.5$ ns pour basculer d'une tension à la suivante. En pratique, la tension ne se stabilisera pas tout de suite à la valeur attendue, il faut donc

prévoir un certain temps pour que le système atteigne son équilibre. Ainsi, il faut que la tension de contrôle puisse basculer de 0 V à 350 V en moins de 100 ns.

Nous avons réalisé, avec A. Villing du service d'électronique de l'Institut d'Optique, un commutateur de haute tension à haute fréquence (CHTHF). Les détails du fonctionnement ainsi que les schémas électriques sont décrits dans l'annexe A.1. Ce commutateur a un temps de montée $10\%-90\%$ de 50 ns entre 0 et 500 V.

6.3.2 L'électronique de contrôle

L'électronique de synchronisation est une partie importante de l'expérience. Elle doit contrôler le laser impulsionnel, commander l'acousto-optique pour diviser la fréquence, puis produire un nombre aléatoire et appliquer la tension sur le modulateur électro-optique en commandant le CHTHF. Le moyen le plus simple de réaliser ces fonctions est d'utiliser une puce programmable FPGA (Xilinx). On peut ainsi écrire un programme [3] qui se chargera des différentes opérations.

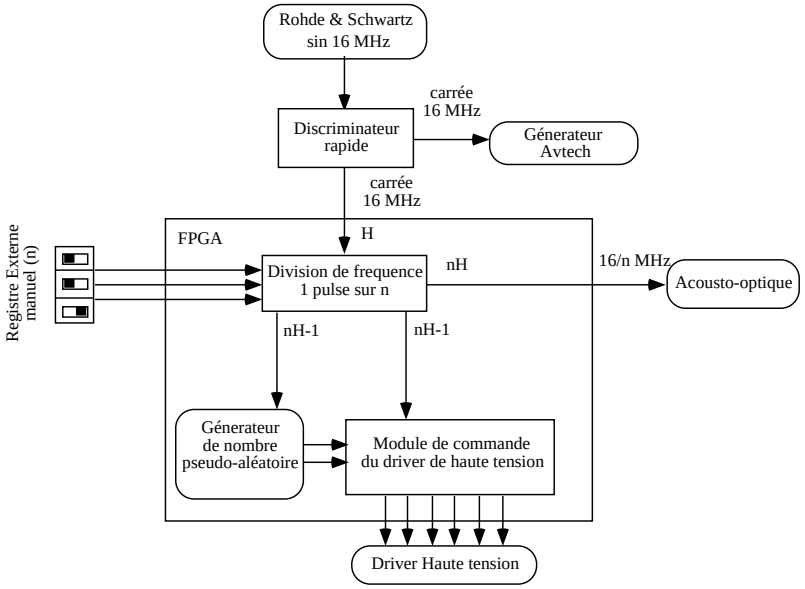


Figure 6.3: *Schéma des synchronisations*

Le schéma des synchronisations est décrit sur la figure 6.3. L'entrée est l'horloge externe stable de 16 MHz décrite en section 6.3.2.1. Un registre externe permet de choisir le facteur de division. Tous les n coups de l'horloge, le module délivre un signal d'une largeur d'approximativement 20 ns qui commande l'acousto-optique. Ce signal est retardé à l'aide d'un module électronique réglable par pas de 5 ns, ainsi que de cables BNC de longueurs appropriées, pour être synchronisé avec l'arrivée de l'impulsion lumineuse au niveau de l'acousto-optique.

6.3.2.1 Horloge stable

L'horloge de base au niveau de l'émetteur doit être très stable. En effet, Alice et Bob ne pourront comparer correctement leurs bits que s'ils sont d'accord sur l'instant d'arrivée de chaque photon. Dans notre montage, Bob ne connaît que l'instant de départ de l'échange de clé, les tops d'horloge ne

[3] La programmation en langage VHDL a été réalisée par Frédéric Moron du service électronique de l'Institut d'Optique

sont pas transmis d'Alice à Bob, qui doit se fier à l'indication de sa propre horloge. Ainsi l'horloge pilote (d'Alice), doit être stable pendant toute la durée de l'échange de la clé. Dans notre cas, la durée de la communication est de 10 ms avec un taux de répétition de 5.3 MHz, et il faut une précision d'horloge à mieux que 10^{-5}. L'horloge d'Alice est composée d'un synthétiseur Rohde & Schwartz délivrant une sinusoïde de fréquence 16 MHz, qui est mise en forme par un discriminateur rapide. On transforme ainsi le signal sinusoïdal en un signal rectangulaire de même fréquence, dont la largeur est d'environ 10 ns (voir figure 6.3). L'horloge ainsi créée a la même précision que le synthétiseur, soit une stabilité meilleure que 10^{-6}.

6.3.2.2 Générateur de nombres aléatoires

Alice à besoin de choisir deux nombres aléatoires pour chaque photon, un pour la base, l'autre pour la valeur du bit. En pratique, le codage utilisé dans cette expérience est le suivant :

Code (MSB-LSB)	Polarisation
00	Horizontal
01	Circulaire Droite
10	Vertical
11	Circulaire Gauche

Nous avons besoin d'un générateur de nombre aléatoire pour le bit de poids fort (Most Significant Bit: MSB), et un autre pour le bit de poids faible (Less Significant Bit: LSB).

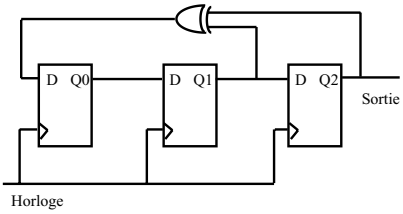
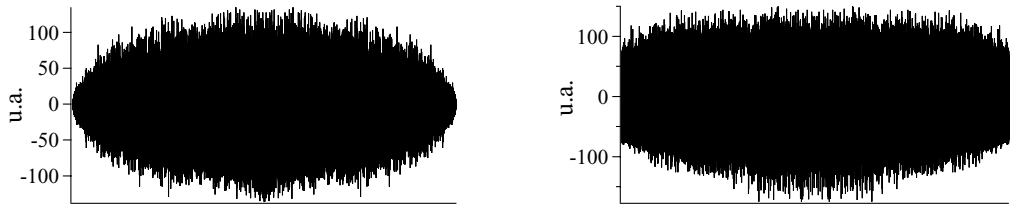


Figure 6.4: *Registre à décalage à* 3 *bits dans la configuration de Fibonacci. Les registres* 1 *et* 2 *sont reliés à l'entrée du registre* 0 *par une porte XOR*

En pratique nous utilisons un générateur de nombre pseudo-aléatoire, pour chaque bit, basé sur un registre à décalage linéaire dans la configuration de Fibonnaci [106, 107], facile à coder sur la puce FPGA déjà utilisée pour les synchronisations. Un registre à décalage est tout simplement l'enchaînement de plusieurs bascules. La bascule N prend la valeur de la bascule N-1 à chaque coup d'horloge. Ce processus est totalement déterministe. Par contre, dans le cas d'un cablage type Fibonnaci (voir figure 6.4), on ne peut deviner la $\mathrm{K}^{\mathrm{ième}}$ valeur du dernier registre même si on connaît les (K-1) valeurs précédentes. La séquence des nombres semble aléatoire. Nous utiliserons deux de ces registres comme générateurs de nombres aléatoires.

Le premier générateur de nombres aléatoires fournit la valeur du MSB. Il est composé de 16 registres, et l'on relie à l'entrée les registres numéro $Q16, Q15, Q13, Q4$, via un OU Exclusif. Le deuxième générateur code la valeur du LSB et il est constitué de 17 registres. On relie à l'entrée les registres numéro $Q17$ et $Q14$ par un OU exclusif.

Ainsi avec le registre à 16 bits (ou bascules) le générateur est remis à zéro après $2^{16} - 1 = 65535$ valeurs, tandis que pour le registre à 17 bits le générateur n'est remis à zéro qu'après $2^{17} - 1 = 131071$ valeurs. En pratique on initialisera le deuxième registre en même temps que le premier. Nous utilisons deux registres de longueur différente pour éviter toute corrélation entre les deux registres.



Autocorrelation MSB Autocorrelation LSB

Figure 6.5: *Fonction d'autocorrélation des valeurs des générateurs de nombres aléatoires MSB et LSB*

La fonction d'autocorrélation circulaire des nombres produits par les générateurs de nombres pseudo-aleatoires ne présentent aucune corrélation significative (voir figure 6.5). La suite des nombres aléatoires peut être simulée sur un ordinateur par un programme simple qui décrit la connexion des bascules. On connait ainsi les bits codés et envoyés au récepteur.

Signalons la possibilité d'utiliser un générateur quantique de nombres aléatoires, décrit en détail dans les références [108, 109, 110]. Il est constitué d'une source lumineuse atténuée, d'une séparatrice $50/50$ et deux photodiodes à avalanche. Chaque photon incident sur la séparatrice à une probabilité égale à 0.5 d'être transmis ou réfléchi, ce qui fournit le bit aléatoire désiré. Moyennant quelques astuces pour compenser les imperfections de la lame séparatrice, la chaîne de bits ainsi obtenue est complétement aléatoire.

6.3.3 Montage expérimental

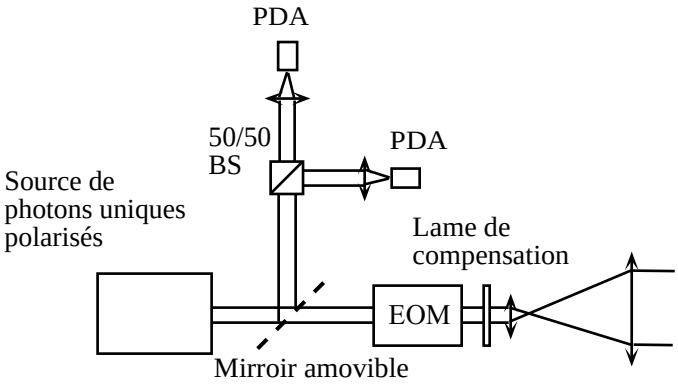


Figure 6.6: *Montage expérimental d'Alice*

Le montage expérimental (fig.6.6) est très similaire à celui décrit dans les chapitres précédents. La source de photons uniques englobe le laser impulsionnel et le microscope confocal (fig.2.5) qui ont été décrits en détail dans la section 5.3. Les nanocristaux de diamants sont posés sur un miroir diélectrique. Un cube polariseur permet de polariser la lumière du centre NV. Une lame achromatique $\lambda/2$ devant le cube permet de tourner la polarisation pour maximiser la transmission. La lumière issue du microscope confocal peut être étudiée par un dispositif de corrélation type Hanbury-Brown et Twiss. On contrôle ainsi la qualité de la source de photons uniques.

Les photons polarisés sont codés par le modulateur électro-optique et envoyés à Bob à l'aide d'un télescope. Le diamètre du faisceau est de 2 cm pour éviter la diffraction. Le centre NV que nous avons utilisé a un taux de polarisation de 46%. Cette valeur varie certainement avec l'orientation du dipôle, mais cet effet n'a pas été étudié systématiquement : nous avons seulement recherché un nanocristal présentant le moins de bruit de fond possible, c'est-à-dire le $g^{(2)}(0)$ le plus faible possible.

6.3.3.1 Qualité des photons uniques

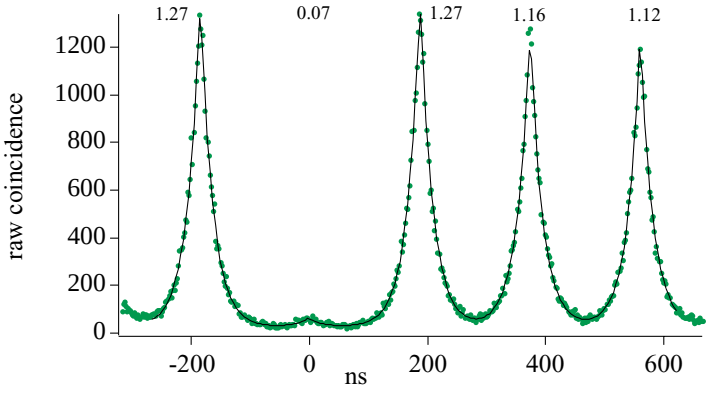


Figure 6.7: *Fonction d'autocorrélation de la source utilisée par Alice*

La fonction d'autocorrélation est présentée sur la figure 6.7. La valeur de $C_N(0)$ mesurée est de 0.07, soit 14 fois plus faible qu'une lumière avec une statistique poissonnienne. La puissance d'excitation est de 0.2 mW, soit tout juste au moment où commence la saturation. On maximise ainsi le facteur de mérite Ξ (voir section 1.5,5.2.2.3). La probabilité d'exciter le centre NV est proche de 0.92. Le taux de répétition est de 5.3 MHz et la largeur de l'impulsion d'excitation est de $\delta T = 0.8$ ns. Le temps d'intégration de la fonction d'autocorrélation est de 166 s. Nous avons mesuré environ 35000 photons par seconde sur chaque PDA. En tenant compte de l'efficacité des PDA de $\eta_{PDA} = 0.6$ nous obtenons 116000 photons uniques polarisés par seconde utilisables pour la cryptographie quantique, soit un rendement de notre source de $\eta_{prod} = 2.2\%$. La transmission du modulateur est de $T_{EOM} = 0.65$. Ainsi le nombre de photons uniques codés envoyés par Alice vers Bob est de 75800s^{-1}, soit en moyenne $\mu = 0.014$ photons par impulsion.

En résumé les caractéristiques de la station d'Alice sont :

- Fréquence d'excitation du centre NV : 5.3 MHz
- Taux de photons uniques codés : 75800 s^{-1} soit un nombre moyen de photons par impulsion : $\mu = 0.014$.
- Le taux d'impulsions contenant deux photons est de 37 s^{-1} seulement, contre 520 s^{-1} pour une source cohérente attenuée ayant le même paramètre μ.
- La base et la polarisation de chaque photon sont codées à l'aide d'un modulateur électro-optique. Les nombres pseudo-aléatoires sont générés par deux registres à décalage.
- Une électronique de contrôle, synchronisée sur une horloge stable à mieux que 10^{-6}, gère l'ensemble de l'expérience.

6.4 Bob

Nous allons maintenant décrire la partie récepteur du montage. Nous avons choisi une méthode passive de choix de la base de mesure. Pour paraphraser une citation célèbre, "nous laissons Dieu jouer aux dés" [4]. Les photons seront soit réfléchis, soit transmis par une lame séparatrice $50/50$, indépendamment de leur polarisation.

6.4.1 Montage expérimental

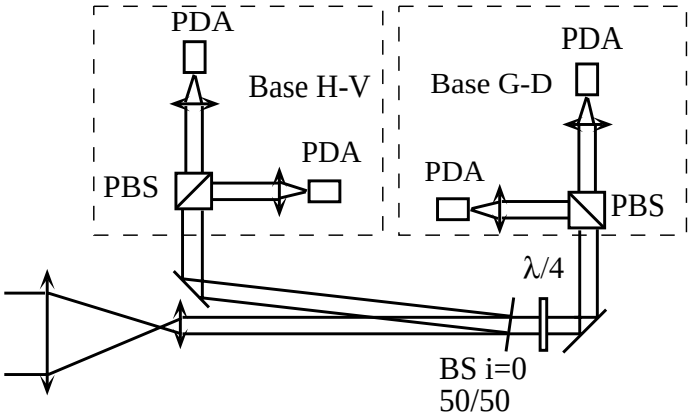


Figure 6.8: *Montage expérimental de Bob*

La figure 6.8 présente le montage expérimental utilisé pour la détection. Les photons sont collimatés en un faisceau plus petit avec exactement le même télescope que celui d'Alice. Le choix de la base est fait de façon aléatoire par une séparatrice $50/50$ large bande (Layertec) à incidence quasi nulle. L'angle est de seulement 2^o. Dans cette configuration, la polarisation de la lumière réfléchie, ou transmise n'est pas affectée. Les photons qui sont réfléchis seront analysés dans la base $(|H\rangle, |V\rangle)$ par un cube polariseur large bande (Gsänger). De même les photons transmis seront analysés dans la base $(|D\rangle, |G\rangle)$ après avoir traversé une lame achromatique (Newport) $\lambda/4$ convenablement réglée. Les photons sont détectés par quatre photodiodes à avalanches (EG & G) identiques à celles qui ont été utilisées dans le chapitre 3. Nous utilisons des miroirs en argent pour avoir une réflexion maximale, indépendamment de la polarisation.

6.4.1.1 Détection

Les quatre photodiodes à avalanches (PDA) sont reliées aux quatre voies d'un oscilloscope numérique (LeCroy). Chaque voie à une profondeur mémoire d'un million de points et un taux d'échantillonnage maximal de 1 GHz. Sachant que le signal TTL d'une PDA a une durée d'environ 25 à 30 ns, nous pouvons diminuer le taux d'échantillonnage à 100 MHz, c'est-à-dire 1 point toutes les 10 ns. Ainsi en une seule fois, nous pouvons acquérir 10 ms de clé. Sachant que la cadence de production des photons uniques est de 5.3 MHz, Alice doit coder 53000 bits distincts. Ceci justifie le fait que les générateurs de nombres pseudo-aléatoires soient limités à 16 bits. Les traces de l'oscilloscope sont par la suite téléchargées sur le PC de Bob via le réseau Ethernet. Un traitement informatique simple permet d'extraire le temps d'arrivée de chaque photon, ainsi que sa base et sa valeur.

[4] D'après A. Einstein, repris par John Rarity pour décrire ce montage

L'horloge interne de l'oscilloscope est suffisamment précise pendant le temps d'acquisition, et il n'y a pas besoin d'une horloge externe stable comme dans le cas d'Alice.

6.4.2 Caractéristiques du montage récepteur

6.4.2.1 Caractéristiques optiques

Dans un premier temps, nous allons caractériser le montage en remplacant le télescope par un laser He-Ne ($\lambda = 633$ nm).

- La transmission de la lame séparatrice est de 50.6%.
- La transmission de la lame achromatique $\lambda/4$ est de 90%
- La transmission totale du système depuis le télescope est d'environ 42% pour chaque voie, en incluant la lame $50/50$
- Le taux d'erreur par bit et par base est d'environ 1%.

Bien que la longueur d'onde d'un laser He-Ne soit décalée d'environ 60 nm du maximum d'émission du centre NV, ces résultats sont une bonne indication des performances du récepteur.

Au taux d'erreur optique, il faut ajouter le taux d'erreur introduit par les coups d'obscurité des PDA ainsi que par la lumière ambiante. Les taux mesurés (dans les conditions expérimentales décrites dans la prochaine section) sont $(d_H, d_V, d_G, d_D) = (150, 180, 380, 160)$ photons par seconde. Nous avons pris soin d'éliminer méticuleusement toute lumière parasite qui pourrait augmenter le taux d'obscurité. De plus, seuls les photons arrivant dans une fenêtre temporelle de 50 ns suivant le signal de synchronisation sont pris en compte. Ainsi on détecte $\eta_g = 90\%$ des photons uniques émis par le centre NV (durée de vie ≈ 23 ns) mais on ne comptabilise que $\beta_g = 27\%$ des coups d'obscurité totaux.

6.5 Distribution de clé quantique avec une source de photons uniques

6.5.1 Disposition et mesures préliminaires

Nous avons installé Alice et Bob à une distance de 15 m pour des mesures préliminaires, puis à 50 m dans un couloir de l'Institut d'Optique. Pour minimiser le taux d'erreur dû au bruit ambiant, les expériences se déroulent dans l'obscurité. L'image 6.9 montre Alice (premier plan) et Bob à une distance de 15 m dans le couloir à l'Institut d'Optique.

6.5.1.1 Alignement

La lumière émise par le centre NV étant trop ténue pour procéder à l'alignement du faisceau, on remplace alors l'échantillon de diamant par un miroir. La lumière d'excitation y est réfléchie, puis emprunte le même chemin que la lumière de fluorescence à travers le microscope confocal, le modulateur électro-optique, et le montage de Bob. On peut ainsi faire simplement les alignements.

Figure 6.9: *Alice et Bob dans le couloir*

6.5.1.2 Caractérisation

Dans cette disposition, nous pouvons estimer une borne inférieure du taux d'erreur. Pour cela Alice code une par une les quatre tensions sur le modulateur électro-optique, et l'on mesure le taux d'erreur au niveau de Bob. Nous obtenons ainsi en utilisant la source de photons uniques:

Base d'analyse	Taux d'erreur
Base H-V	$p_{\mathrm{pol}}^{\mathrm{HV}} = 1.2\%$
Base D-G	$p_{\mathrm{pol}}^{\mathrm{DG}} = 3.2\%$
Moyenne	$p_{\mathrm{pol}} = 2.2\%$

La légère différence provient de l'imperfection de la lame achromatique dans la base circulaire. Cette estimation du taux d'erreur de polarisation tient aussi compte des erreurs de codage du modulateur électro-optique, ainsi que de la compensation imparfaite. Cependant, le taux d'erreur est très proche du taux d'erreur minimal mesuré avec le laser He-Ne.

A cela il faut ajouter le taux d'erreur dû aux coups d'obscurité et à la lumière parasite. Le nombre de photons détectés par Bob est d'environ $N_D^{(b)} = 39300s^{-1}$ sur les quatre photodiodes. Le taux d'erreur p_{dark} vaut donc $p_{\mathrm{dark}} = \beta_g \sum_{i=H,V,L,R} d_i/(\eta_g N_D^{(b)}) = 0.7\%$. Nous pouvons estimer une borne inférieure du taux d'erreur quantique total (QBER : Quantum Bit Error Rate)

$$Q_b^{err} = (p_{\mathrm{dark}} + p_{\mathrm{pol}}^{\mathrm{HV}} + p_{\mathrm{pol}}^{\mathrm{LR}})/2 = 2.6\% \tag{6.8}$$

Remarque : Dans la mesure du taux d'erreur quantique, nous ne devons prendre en compte les taux d'obscurité qu'une fois sur deux, puisqu'ils ne sont comptabilisé que s'ils "arrivent" dans la même base que celle choisie par Alice.

6.5.2 Expérience de cryptographie quantique

L'expérience de cryptographie quantique se déroule en cinq phases :

Communication quantique : Un signal de synchronisation généré par Alice est envoyé à l'aide d'un cable coaxial[5] à Bob qui déclenche une acquisition de 10 ms simultanément sur les quatre voies de détection. Il enregistre les instants d'arrivée de tous les photons détectés.

Post sélection : Bob récupère les données sur son ordinateur et effectue une post-sélection avec des fenêtres de 50 ns. Il sélectionne ainsi 90% des photons uniques tout en rejetant 73% du bruit. A la fin il devrait récupérer 88% des impulsions. En parallèle, il note la fenêtre temporelle dans laquelle il a reçu chaque photon.

Annonce des bases : Bob annonce à Alice le moment de détection de chaque photon ainsi que la base choisie. Alice confirme ou non son choix de base. La clé obtenue est appelée "clé filtrée" (sifted key en anglais).

Mesure du taux d'erreur : Alice et Bob comparent une fraction de leur clé pour estimer le taux d'erreur. En pratique, nous vérifions le taux d'erreur sur la totalité de la clé, afin d'éliminer les fluctuations statistiques (le nombre de bits reçus lors d'une séquence étant relativement faible). Par contre, lorsqu'on utilisera le programme QuCrypt pour effectuer la correction d'erreur, on demandera au programme de ne révéler qu'une partie de la clé.

Correction d'erreur et amplification de confidentialité : Finalement Alice et Bob corrigent les erreurs dans la clé filtrée, puis appliquent l'amplification de confidentialité pour extraire la clé secrète.

Nous avons effectué trois expériences sur une distance de 50 m et 6 sur 10 m. Le tableau 6.3 résume les résultats que nous avons obtenus pour 50 m.

Run	Photons détectés	Photons dans fenêtres	%	Bits filtrés	%	Bits erronnés	%
1	410	328	80	171	52	9	5.2
2	368	279	76	153	55	6	3.9
3	402	293	72	149	51	7	4.6
Moyenne ($10ms$)	393	300	76	157.6	52	7.3	4.6

Tableau 6.3: *Résultats de la distribution de clé quantique sur* 50 *m*

Le nombre total de photons détectés par Bob est de 39300 par seconde. Il en reste 30000 après la post-sélection (réduction des coups d'obscurité), et finalement le taux brut échangé entre Alice et Bob est de l'ordre de 15 kbits / sec avant correction des erreurs.

Le taux d'erreur total sur les trois run est de $Q_b^{err} = 4.6\% \pm 1\%$. Pour minimiser les fluctuations statistiques, nous avons mesuré le taux d'erreur en concaténant les trois clés. Les mesures sur une distance de 10 m avaient donné un taux d'erreur de 4.68%, très proche du taux d'erreur mesuré sur 50 m. L'écart entre la valeur de $Q_b^{err} = 4.6\%$ réellement obtenue et celle estimée dans la section 6.5.1 $(Q_b^{err})^{esti} = 2.6\%$ provient essentiellement du fait que l'estimation ne prend pas en compte la dynamique du modulateur électro-optique et du commutateur CHTHF.

[5] Nous avons choisi un cable coaxial pour des raisons de simplicité. Il serait assez simple de modifier le montage et d'envoyer une impulsion optique

Remarque : Plusieurs problèmes techniques ont limité le nombre d'expériences réalisées, le principal étant l'absence d'automatisation des transferts entre l'oscilloscope à 4 voies qui enregistrait tous les photons détectés par Bob, et l'ordinateur qui stockait et traitait les données. Il serait facile de remplacer l'oscilloscope par une carte d'entrée sortie digitale pour éliminer tous ces problèmes, et avoir une transmission en temps réel d'une clé quantique. Ce dispositif sera prochainement mis en place, mais n'avait pas été implémenté dans le prototype présenté ici.

6.5.3 Correction d'erreurs et amplification de confidentialité.

La correction d'erreurs et l'amplification de confidentialité ont été réalisées à l'aide du programme **QuCrypt** créé par Louis Salvail [111]. Il fait partie du domaine public et le code source est accessible. Il est composé de quatre modules indépendants qui gèrent la communication par le canal quantique ainsi que le canal classique. La communication entre les modules se fait par le protocole standard TCP / IP. Les modules peuvent tourner indifféremment sur un seul ordinateur, ou sur des ordinateurs séparés.

6.5.3.1 Interface avec notre expérience

Dans la version préliminaire de l'expérience de cryptographie que nous avons réalisée, le traitement des données pour notre expérience de cryptographie se fait essentiellement "off line". La limitation matérielle et les contraintes d'utilisation de l'oscilloscope ne nous permettent pas d'avoir un échange de clé en temps réel.

Ainsi nous disposons, après les trois run, d'un fichier pour Alice et Bob contenant les 473 bits après réconciliation des bases (voir section 6.5.2). Pour implémenter QuCrypt, nous avons écrit un programme qui se substitue au canal quantique. Il permet de charger dans QuCrypt la clé filtrée de Alice et Bob, en les transmettant au module correspondant.

6.5.3.2 Correction d'erreurs

La clé filtrée d'Alice et Bob contient typiquement entre 3 et 5% d'erreurs. Cette valeur est beaucoup trop importante pour être acceptable pour une application cryptographique. Il faut donc corriger les erreurs introduites en révélant le moins possible d'information à Eve. Pour cela, Alice et Bob s'échangent la parité de blocs découpés dans la clé originale.

Le théorème de Shannon [112] donne le nombre de bit de parité $N^{Shannon}$ que doivent s'échanger Alice et Bob pour corriger toutes les erreurs introduites pour une clé de taille n.

$$\frac{N^{Shannon}}{n} = -elog_2e - (1-e)log_2(1-e) \tag{6.9}$$

où e est le taux d'erreur. En réalité le nombre de bits de parité dépend de l'algorithme utilisé. Pour les algorithmes existants actuellement et pour des taux d'erreurs inférieurs à 5% , il faut le multiplier par $f[e] \approx 1.16$ [13].

Une fois la clé chargée dans QuCrypt pour chacun des modules (Alice et Bob), le protocole de correction d'erreurs est lancé en appliquant l'algorithme CASCADE. Il consiste en un échange interactif de bits de parité par bloc. La taille du bloc initial est choisie par la formule $k_0 = 1/e + 1/(4e)$, ou e est le taux d'erreur estimé publiquement. Il est obtenu en révélant une partie de la clé, qui a été empiriquement fixé à 10%. La taille du bloc $i+1$ est définie par $k_{i+1} = 2k_i$. Le protocole s'arrête d'incrémenter la taille des blocs lorsque ceux-ci ont une taille supérieure à $1/4$ de la clé totale. Ceci

correspond au passage $i-2$. On effectue ensuite encore deux passages pour vérifier que toutes les erreurs ont bien été corrigées.

6.5.3.3 Amplification de confidentialité

La phase de correction d'erreur a dévoilé de l'information à l'espion. Pendant cette phase Alice et Bob ont échangé k bits pour estimer le taux d'erreur, l bits de parité pour la correction d'erreur, et finalement t bits de confirmation, ce qui correspond à $n_c = k + l + t$ bits révélés pour corriger les erreurs. Par ailleurs, Eve a pu prendre connaissance de n_a bits en attaquant le canal quantique pendant la transmission des photons. Il faut ainsi procéder à l'amplification de confidentialité pour distiller une clé plus petite, mais dont Eve n'a aucune connaissance. Cela est obtenu en choisissant au hasard une fonction de hachage de $\{0,1\}^n \rightarrow \{0,1\}^{n-n_c-n_a-s}$. Alice et Bob obtiennent ainsi une clé contenant n_c+n_a+s moins de bits. Le nombre s correspond à un paramètre de sécurité qui réduit encore la connaissance qu'Eve aura de la clé finale, aux dépends bien sûr de la taille de cette clé; ce paramètre est ajustable au gré de l'utilisateur, et dans la suite nous prendrons simplement $s = 0$.

6.5.3.4 Exemple de mise en oeuvre

Pour fonctionner correctement, l'algorithme de correction d'erreurs doit évaluer le taux d'erreur en sacrifiant une fraction de la clé. Cette évaluation est très efficace lorsque le nombre total de bits échangés est très grand, car le taux d'erreur peut être évalué avec une grande précision sur un échantillon contenant un grand nombre de bits, mais de taille très petite en valeur relative. Par contre, lorsque le nombre total de bits échangés est faible, la fraction à sacrifier devient grande en valeur relative, ce qui est à priori défavorable. De plus, l'algorithme Cascade "consomme" un nombre de bits bien supérieur à la valeur asymptotique donnée par l'éq. 6.9.

A titre d'exemple, nous indiquons ici le déroulement d'une réconciliation des 473 bits contenant 22 erreurs du tableau 6.3, en évaluant le taux d'erreur sur 10% des bits choisis aléatoirement par l'algorithme :

- Taux d'erreur estimé : 2.1% (cette estimation est faussée par la petite taille de l'échantillon)
- Le taille du bloc initial : $k_0 = 33$
- Le nombre de passages : 6

Passage	Erreurs corrigées	Taille bloc	Bits de parité révélés
0	5	33	38
1	12	66	74
2	4	132	27
3	0	132	4
4	0	132	4
5	0	132	4

Tableau 6.4: *Résultats de l'algorithme cascade*

L'algorithme a ainsi corrigé un total de 21 erreurs en révélant 151 bits de parité. La réconciliation a produit une clé identique pour Alice et Bob avec une probabilité de 0.999023. Toutes les erreurs ont été corrigées (il y avait 22 erreurs, mais un bit erronné a fait partie des 10% utilisés pour l'estimation).

Cet exemple appelle plusieurs commentaires. Tout d'abord, l'algorithme consomme plus de bits que ce qui est prévu théoriquement. En effet la formule 6.9 indique que le nombre de bits de parité à révéler doit être de $n_{rev,th} = 133$ avec $f[e] = 1.16$, alors qu'expérimentalement on a $n_{rev,exp} = 151$. De plus, si on relance l'exécution du programme, le taux d'erreur sera évalué sur un autre échantillon, et $n_{rev,exp}$ sera en général différent (voir figure 6.10 ci-dessous). Ces observations confirment donc que le nombre total de bits utilisés est trop faible pour assurer un bon fonctionnement de Cascade. On peut néanmoins évaluer notre dispositif en corrigeant les effets dus à la petite taille de la clé; nous reviendrons sur ce point à la fin de ce chapitre.

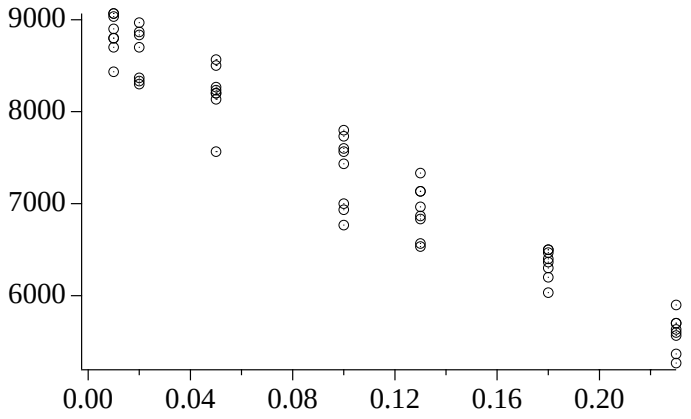


Figure 6.10: *Taux de bits secrets par seconde en fonction du paramètre PA.*

Pour réaliser pratiquement l'amplification de la confidentialité, on introduit dans le programme QuCrypt un paramètre PA donné par par $PA \times (n - k) = n_a$, où n_a est le nombre de bits connus d'Eve suite à son attaque du canal quantique. Sur la figure 6.10 on a reporté le taux de bits secrets en fonction de PA. Pour chaque valeur de PA, nous avons reporté le taux de bits secrets obtenus par 8 exécutions indépendantes du programme : on voit donc apparaître directement les "fluctuations d'efficacité" de Cascade citées dans le paragraphe précédent, et dues à la trop petite taille de l'échantillon.

Nous montrerons ci-dessous que la valeur PA=0.23 correspond à la connaissance acquise par Eve si elle possède "tous les pouvoirs" autorisés par la mécanique quantique. Dans ce cas, Alice et Bob partagent 176 bits secrets à partir des 473 bits initialement échangés. Avant de conclure sur l'analyse de ces résultats expérimentaux, nous allons examiner plus en détail l'évaluation de PA, qui est directement fonction du type d'attaque qu'Eve peut effectuer sur le canal quantique.

6.6 Etude théorique de la sécurité

Dans cette section, nous voulons obtenir une formule qui donne le nombre de bits secrets par seconde qu'Alice et Bob peuvent s'échanger, ainsi que la distance maximale à laquelle une communication secrète est possible. Ces deux paramètres vont largement dépendre de la nature de la source utilisée dans le canal quantique. Les calculs de cette section utilisent les formules établies dans [13, 113], et n'ont pas pour but de re-démontrer les résultats.

Avant d'entreprendre l'étude de la sécurité, nous allons donner un bref aperçu des attaques que peut effectuer l'espion, ainsi que des outils dont il dispose.

Nous allons considérer ici qu'Eve peut utiliser toute la technologie théoriquement accessible. Il peut paraître que les conditions que nous allons énumérer sont excessives, et qu'elle sont loin d'être expérimentalement réalisées. Néanmoins, cette approche basée sur l'idée de la "sécurité inconditionnelle" est utile pour montrer les avantages de notre prototype de cryptographie à photon uniques par rapport aux source cohérentes atténuées (Weak Coherent Pulse WCP). Par contre, on limite les attaques d'Eve aux lignes de transmission (aussi bien classiques que quantiques). Les attaques à l'intérieur des appareils d'Alice et Bob ne sont pas prises en compte. Ainsi les outils que possède Eve sont :

- **Mesure QND parfaite :** Eve est capable de mesurer le nombre de photons qu'il y a dans une impulsion, sans en perturber l'état de polarisation. Ceci est un défi technologique, car même si les mesures QND [114] sont très efficaces, elles n'ont jamais été réalisées pour un seul photon en optique. Néanmoins des progrès ont été réalisés dans le domaine des micro-ondes [115].

- **Mémoires quantiques :** Eve peut stocker aussi longtemps qu'elle le souhaite un photon sans le perturber. Pour cela elle recopie l'état du photon sur un autre système quantique, par exemple un atome dans une cavité. Dans les meilleures réalisations actuelles de telles mémoires ont une durée de vie très faible (ms) et un taux d'erreur très élevé.

- **Fibres optique sans pertes, ou téléportation parfaite :** Eve est capable de transporter un photon d'un endroit à un autre sans pertes. Il semble que même théoriquement, une fibre optique sans pertes est irréalisable, mais Eve peut effectuer une téléportation parfaite du photon intercepté. Actuellement la fidélité de la téléportation est d'environ $F \approx 0.83$ [116]. Beaucoup de progrès doivent encore être réalisés.

- **Etat de Fock arbitraire :** On suppose aussi qu'Eve possède une source de photons avec laquelle elle peut recréer n'importe quel état de Fock. Diverses études avec des atomes piégés dans des microcavités montrent qu'il est envisageable de générer un état de Fock arbitraire [117, 118].

- **Canal classique :** En plus des attaques sur le canal quantique, Eve a accès au canal classique mais ne peut personnifier ni Alice ni Bob. On considère qu'Alice et Bob se sont échangés préalablement une clé secrète qui leur sert d'authentification. Si le canal classique est crypté par les méthodes algorithmiques actuelles, on suppose qu'Eve connait des algorithmes très puissants ou possède un ordinteur quantique, ce qui lui permettent de casser le code.

6.6.1 Tactiques d'attaque

Nous allons maintenant décrire quelques attaques qu'Eve peut effectuer sur la ligne de communication quantique. Nous allons commencer par l'attaque d'Eve sur les photons uniques, puis décrire deux attaques sur les impulsions contenant plusieurs photons, l'une d'elles étant technologiquement possible actuellement.

6.6.1.1 Attaque des simples

Pour attaquer les impulsions contenant un seul photon, Eve doit faire une mesure, puis renvoyer vers Bob un photon codé avec le résultat de sa mesure[6] [111, 9]. Pour cela Eve choisit aléatoirement

[6] Cette attaque est couramment appelé Intercept-Resend dans la littérature

une base (H-V ou D-G), et il est facile à voir que dans 75% des cas elle aura deviné de façon exacte la valeur du bit qu'Alice a envoyé, mais que dans 25% des cas, la valeur du bit partagée par Alice et Bob sera fausse.

Une attaque plus fine[7] consiste à utiliser la base de Breidbart [119] orientée à 22.5^o par rapport aux bases d'Alice et Bob. Dans ce cas, Eve devinera correctement avec une probabilité de $cos^2(\pi/8) \approx 0.85$. Elle n'introduira que 15% d'erreur.

Cette attaque est très facilement réalisable par Eve. Il lui suffit d'avoir une source de photons uniques ainsi que le même montage que Bob (ou bien une version améliorée). Mais, lors de cette attaque, elle révèle sa présence à cause des erreurs qu'elle introduit dans la transmission. On peut ainsi évaluer une limite supérieure sur le taux d'erreur admissible pour la cryptographie quantique. En effet, si le taux d'erreur est supérieur à 15% alors Alice et Bob savent qu'un espion a écouté une grande partie de la communication, et qu'aucune clé secrète ne peut être déduite. Si le taux d'erreur est inférieur à 15% ils peuvent distiller une clé secrète par correction d'erreur et amplification de confidentialité. Le protocole BB84 laisse peu de marge de manoeuvre à Eve. En fait, elle préférera attaquer les impulsions contenant plusieurs photons.

6.6.1.2 Attaque des doubles

Supposons qu'Alice possède une source qui émet N_1 impulsions contenant un seul photon et N_2 impulsions contenant plus de deux photons. Bob détectera alors N_{b1} simples et N_{b2} doubles, mais il ne peut pas distinguer les impulsions simples des impulsions doubles. On se place dans le cas ou les pertes sont très élevées et donc $N_{b2} \ll N_{b1} + N_{b2}$. Alors si $N_{b1} = N_2$ l'attaque est la suivante :

- Eve se place juste à la sortie des locaux d'Alice.
- Pour chaque impulsion, elle effectue une mesure QND du nombre de photons. S'il n'y a qu'un seul photon dans l'impulsion, alors elle la bloque. Sinon elle sépare les photons de l'impulsion pour n'en garder qu'un seul, qu'elle place dans une mémoire quantique.
- Par le biais d'une fibre sans perte, ou bien d'un téléporteur quantique, elle transfère le deuxième photon chez Bob. Bob recevra alors le même nombre d'impulsions et ne se rendra compte de rien. Pour déjouer ce type d'attaque, Bob peut analyser la statistique des impulsions, et s'assurer que la probabilité d'avoir 2 ou 3 photons par impulsion est conforme à celle attendue. Eve doit alors s'adapter et "créer" des impulsions avec un nombre de photons donné, afin de garder la statistique de Bob inchangée [120, 121, 122].
- Une fois qu'Alice et Bob auront révélé leur base, Eve va mesurer dans la bonne base le photon qu'elle a gardé dans la mémoire.

Ainsi, Eve est en possession de toute l'information qu'Alice et Bob ont échangée, sans introduire d'erreurs, et donc sans révéler sa présence. Ceci nous donne une deuxième limite sur le taux de pertes tolérable dans un système de cryptographie quantique pour un nombre moyen d'impulsions contenant deux photons. Ainsi pour une source cohérente atténuée, la limite est donnée par $p(2) = p(1)^2/2 = \eta p(1)$, où η décrit les pertes de la liaison Alice-Bob. Pour un nombre moyen de photon par impulsion $p(1) = 0.1$ ceci équivaut à des pertes maximales de 13 dB.

Bien sûr, Eve peut utiliser aussi cette attaque pour des pertes plus faibles. Dans ce cas elle ne récupère qu'une partie de l'information.

[7] Cette attaque existe dans le cas ou la polarisation est codée sur la base $|H\rangle$ $|V\rangle$ $|45\rangle$ $|135\rangle$. Une version similaire existe pour notre codage

6.6.1.3 Attaque des triples

L'attaque sur les impulsions à deux photons demande des capacités technologiques importantes qui sont encore loin d'être réalisées expérimentalement. Par contre si les pertes sont importantes, Eve peut choisir de s'attaquer aux impulsions contenant trois photons. Une telle attaque est possible avec la technologie actuelle.

Le dispositif expérimental de l'espion est exactement le même que celui de notre récepteur décrit dans la figure 6.8, constitué de 4 PDA correspondant aux 4 états de polarisation. On suppose qu'Eve se place de nouveau juste à la sortie d'Alice et qu'elle est en possession d'une source de photons uniques.

- Pour chaque impulsion elle regarde le nombre de photodiodes qui ont enregistré un évènement. Si elle détecte un évènement sur 3 des 4 photodiodes à avalanche, alors, elle peut déterminer de façon non-ambigüe, la polarisation des photons.
- Au niveau de Bob elle place une source de photons uniques, et envoie à Bob un seul photon avec la polarisation qu'elle a mesurée.
- Si moins de 3 photodiodes enregistrent un évènement alors elle ne fait rien.

Cette attaque est simple à mettre en œuvre, et ne nécessite pas de nouvelles technologies. Pour une source cohérente atténuée, la probabilité d'avoir 3 photons dans l'impulsion est donnée par $p(3) = p(1)^3/6$. Dans le cas décrit ici, compte tenu du dispositif expérimental, Eve aura $p(1)^3/16$ évènements où elle est capable de déterminer de façon non ambigüe la polarisation du photon. Lorsque le nombre d'évènements triple au niveau d'Alice est égal au nombre d'évènements simple chez Bob $p(1)^3/16 = \eta p(1)$, alors Eve peut tromper l'adversaire. Il en découle une condition sur la probabilité $p(1)$ pour une source cohérente atténuée, en fonction des pertes de la ligne.

- Pour des pertes de 20dB, $p(1) < 0.4$
- Pour des pertes de 30dB, $p(1) < 0.13$

Ainsi pour des canaux de communication avec de grande pertes, les source cohérentes atténuées sont peu adaptées.

6.6.2 Pertes maximales et taux de bits sûrs

En fonction de l'attaque qu'Eve va pouvoir faire sur le canal quantique, nous pouvons déduire le taux maximal de pertes tolérées pour avoir une communication sécurisée. Pour cela nous allons dériver le taux de bits sûrs par impulsion après correction d'erreurs et amplification de confidentialité. Comme nous l'avons vu plus haut, la correction d'erreur conduit au sacrifice d'un certain nombre de bits en fonction du taux d'erreur donnée par la formule de Shannon (eq. 6.9). Le taux de bits qu'il faut sacrifier pendant l'amplification de confidentialité va dépendre du type d'attaque que fera Eve.

6.6.2.1 Attaque sur les simples seulement.

Eve peut se contenter de n'attaquer que les impulsions contenant un photon. Dans ce cas, le taux de bits à sacrifier, pour l'amplification de confidentialité, est donné par la formule $ln_2(1 + 4e - 4e^2)$ [13] en fonction du QBER e. Ainsi le taux de bits sûrs, après correction d'erreur et amplification de confidentialité, s'écrit

$$G^{simples} = \frac{1}{2} p_{exp} \left(1 - ln_2(1 + 4e - 4e^2) + elog_2 e + (1-e)log_2(1-e)\right) \tag{6.10}$$

où p_{exp} le nombre de photons que détecte Bob. Prenons le cas idéal ou $p_{exp} = 1$. On peut ainsi mesurer le taux d'erreur maximal toléré dans le cadre de la cryptographie quantique. La valeur de $G^{simples}$ donnée par l'équation 6.10 est nulle pour un taux d'erreur égal à $e \approx 0.11$. Il est impossible à Alice et Bob de s'échanger une clé secrète s'ils mesurent un taux d'erreur supérieur à 11%. Le nombre de bit sacrifiés est égal à la taille de la clé échangée.

6.6.2.2 Formule de gain pour un système réel

Un espion tout-puissant va aussi attaquer les impulsions contenant plusieurs photons. Dans ce cas, on suppose qu'Eve peut extraire toute l'information des impulsions à plusieurs photons, et ceci sans révéler sa présence (voir discussion au-dessus).

On peut dériver la formule qui donne le nombre de bits sûrs par impulsion dans des conditions réelles (G^{multi}). Elle est donnée par [13] :

$$\begin{gathered} G^{multi} = \frac{1}{2} p_{exp} \times \\ \left\{ \frac{p_{exp} - S_m}{p_{exp}} \times \left(1 - log_2 \left[1 + 4e \frac{p_{exp}}{p_{exp} - S_m} - 4 \left(e \frac{p_{exp}}{p_{exp} - S_m} \right)^2 \right] \right) \right. \\ \left. + f[e][elog_2 e + (1-e)log_2(1-e)] \right\} \end{gathered} \tag{6.11}$$

où S_m et le taux d'impulsions contenant au moins deux photons. La probabilité p_{exp} que Bob détecte un signal a deux composantes. La première provient de la détection des photons p_{exp}^{signal} envoyés par Alice, et la deuxième des coups d'obscurité des détecteurs par fenêtre de détection p_{exp}^{dark}. Ainsi on obtient :

$$p_{exp} = p_{exp}^{signal} + p_{exp}^{dark} - p_{exp}^{signal} p_{exp}^{dark} \tag{6.12}$$

De même le taux d'erreur e a deux contributions. L'imperfection du montage de détection, ainsi que les erreurs de codage de la polarisation, vont avoir un effet sur le taux d'extinction dans chacune des bases. Ce taux d'erreur est constant et proportionnel à p_{exp}^{signal}, et le facteur de proportionnalité est nommé c. Dans notre cas nous obtenons (c) en soustrayant le taux d'erreur dû au taux d'obscurité au QBER mesuré expérimentalement, soit $c = 0.046 - 0.007 = 0.039$. Le taux d'obscurité a aussi une contribution non négligeable. En effet si un coup d'obscurité arrive pendant une fenêtre de détection, il sera interprété aléatoirement comme un des deux résultats possibles (bit 0 ou bit 1) pour Bob, ce qui introduit 50 % d'erreur. Ainsi le taux d'erreur dans la clé filtrée est modélisé par :

$$e \approx \frac{c p_{exp}^{signal} + \frac{1}{2} p_{exp}^{dark}}{p_{exp}} \tag{6.13}$$

On peut tout de suite remarquer que lorsque $p_{exp}^{signal} \approx p_{exp}^{dark}$ alors le taux d'erreur $e \approx \frac{2c+1}{4} > 0.11 \; \forall c$. Aucune communication secrète ne peut être établie. Ainsi un des facteurs limitant pour la cryptographie à grande distance va être le taux d'obscurité par fenêtre temporelle des détecteurs.

Pour les PDA en silicium le taux d'obscurité est approximativement 150 cps, tandis que pour les détecteurs InGaS, utilisés pour les longueurs d'onde telecom de 1.3μm et 1.5μm, le taux d'obscurité est compris entre 10^3 et 10^4 cps. Dans notre cas nous utilisons des fenêtres de 50 ns, tandis que les prototypes basées sur des sources cohérentes atténuées utilisent des fenêtres de 2 ns [95]. Ils seront donc moins sensibles aux coups d'obscurité.

Il faut maintenant estimer p_{exp}^{signal} ainsi que S_m qui est la contribution des impulsions contenant deux photons. Pour cela nous allons considérer que la source de photons d'Alice à une distribution poissonnienne du nombre de photons, avec une valeur moyenne μ d'où :

$$S_m^{WCP} = 1 - (1+\mu)exp(-\mu) \tag{6.14}$$

$$p_{exp}^{signal} = 1 - exp(-\eta_B \eta_T \mu) \tag{6.15}$$

Il est important de noter que le facteur S_m est le taux d'impulsions contenant plusieurs photons à la sortie de l'émetteur d'Alice. Dans le cas de notre source à photons uniques $S_m^{SPP} = C(0)S_m^{WCP}$, où $C(0)$ est l'aire du pic à temps nul de la fonction d'autocorrélation (voir fig. 6.7). Dans l'expression de p_{exp}^{signal}, le terme η_B représente l'efficacité de détection de Bob. La transmission (η_T) entre Alice et Bob est exprimée en fonction de α (coefficient de pertes en dB / km) et l (distance en km) :

$$\eta_T = 10^{-\frac{\alpha l}{10}} \tag{6.16}$$

6.6.2.3 Comparaison

Afin de comparer un système de cryptographie quantique à photons uniques avec un système basé sur une source cohérente atténuée, on considère le même montage expérimental dans les deux cas, en ajustant les paramètres propres à chaque source. Les paramètres sont résumés dans le tableau 6.5.

	Source photons uniques	Source cohérente atténuée
α	0.25dB / km	0.25dB / km
Coups d'obscurité	150 s^{-1}	150 s^{-1}
c	0.039	0.039
η_B	-2.2dB	-2.2dB
$C(0)$	0.07	1
Fenêtre	50 ns	2 ns

Tableau 6.5: *Paramètres utilisés pour la simulation.*

Remarquons que les résultats dépendent de la distance de propagation l seulement par la valeur des pertes totales en ligne αl exprimées en dB, qui sont indiquées sur l'axe horizontal de la figure 6.11. Les courbes de la fig. 6.11 pourraient aussi bien êtres exprimées en unités arbitraires, sans pour autant changer les conclusions de la comparaison. Les courbes de la fig. 6.11 représentent le taux de bits sûrs par impulsion pour une source de photons uniques et une source cohérente atténuée, calculé à partir des valeurs du tableau 6.5.

Plus les pertes deviennent importantes, plus le nombre de bits "sacrifiés" pour la correction d'erreur et l'amplification de confidentialité devient important. On remarque un net avantage pour notre source de photons uniques avec $\mu = 0.014$, par rapport à une source cohérente de même nombre moyen de photons. L'avantage se creuse encore plus pour un nombre moyen de photons de $\mu = 0.1$

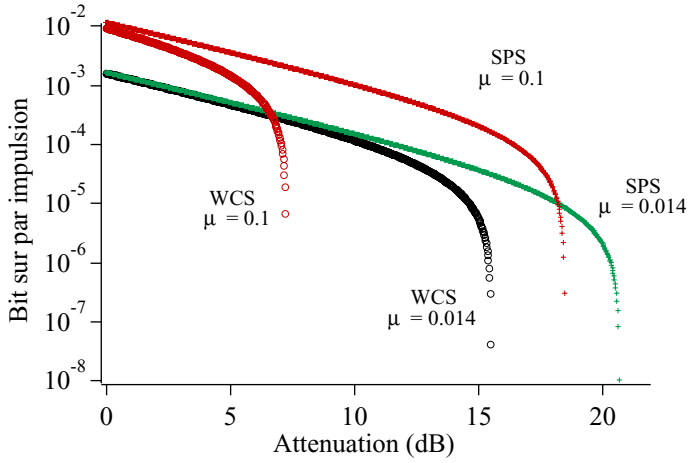


Figure 6.11: *Taux de bit secrets par impulsion pour une source à photons uniques et une source cohérente atténuée. Les courbes représentent deux valeurs différentes du nombre moyen de photons par impulsion.*

6.6.2.4 Pertes maximales autorisées.

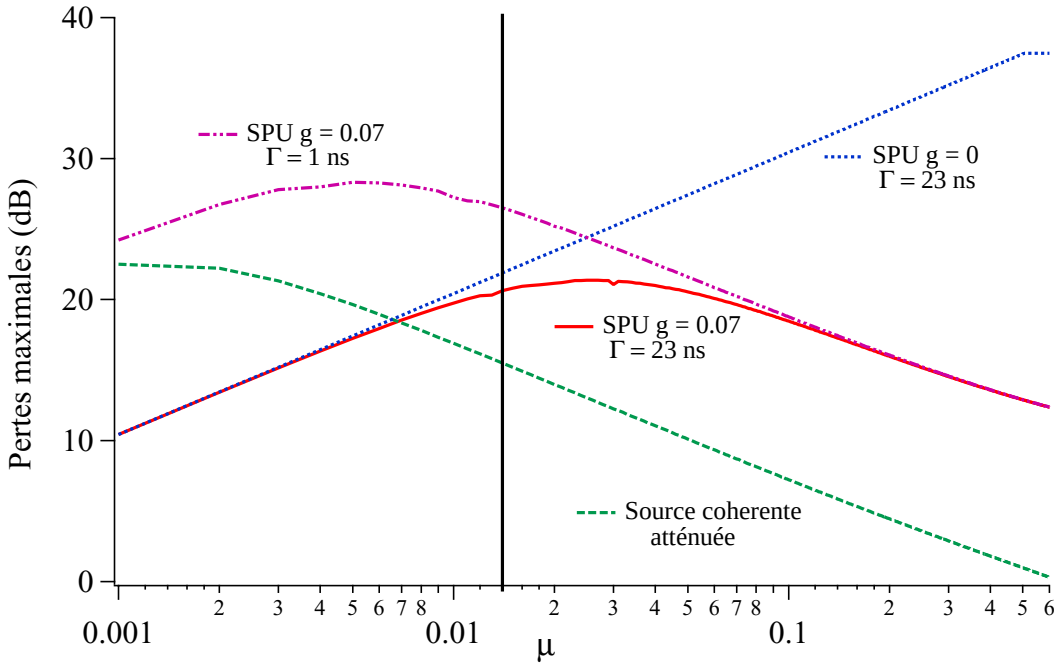


Figure 6.12: *Pertes maximum admissibles pour une communication sûre, en fonction du nombre moyen de photons par impulsion.*

Sur la figure 6.12 nous avons reporté les pertes maximales admissibles pour que la communication reste sûre, en fonction du nombre moyen de photons dans chaque impulsion, en considérant un système basé soit sur une source cohérente atténuée, soit sur une source de photons uniques. Pour tracer la courbe de la figure 6.12, nous avons fixé le seuil de pertes maximale admissibles à $G^{multi} = 10^{-6}$ (voir fig. 6.11). Compte tenu du taux de répétition des sources actuellement utilisées,

ceci correspondrait à un taux de 5 à 10 bits sûrs par seconde.

Sur la figure 6.12, nous avons aussi tracé une courbe pour une source de photons uniques parfaite avec la même fenêtre d'acquisition que notre système (courbe bleue en pointillés), et une courbe pour une source équivalente à la nôtre mais avec une durée de vie de 1 ns (courbe mauve (-..-)) et donc une fenêtre d'acquisition de 2 ns. On remarque clairement que la courbe représentant notre expérience est tangente aux deux autres. A faible μ nous sommes limités par la taille de la fenêtre, tandis qu'à fort μ ce sont les impulsions résiduelles contenant deux photons qui limitent la portée. Ainsi en améliorant la qualité de la source de photons uniques, nous pourrions accepter des pertes plus importantes.

Le système de cryptographie que nous avons mis en place présente un nombre moyen de photons $\mu = 0.014$ (ligne noire). Les pertes maximales admissibles pour garantir une communication secrète sont de $\varsigma^{SPU} = 20.6$ dB pour notre source de photons uniques contre $\varsigma^{WCS} = 15.5$ dB pour un prototype utilisant une source cohérente atténuée. En améliorant l'efficacité de la source de photons uniques, cet avantage devient de plus en plus important. Par exemple, pour la valeur $\mu = 0.05$ qui semble expérimentalement accessible, le taux maximal de pertes est peu modifiée pour la source de photons uniques ($\varsigma^{SPU} = 20.5$ dB), tandis que pour une source cohérente atténuée il n'est plus que de $\varsigma^{WCS} = 10.1$ dB.

6.6.2.5 Avantage en taux de bits sûrs

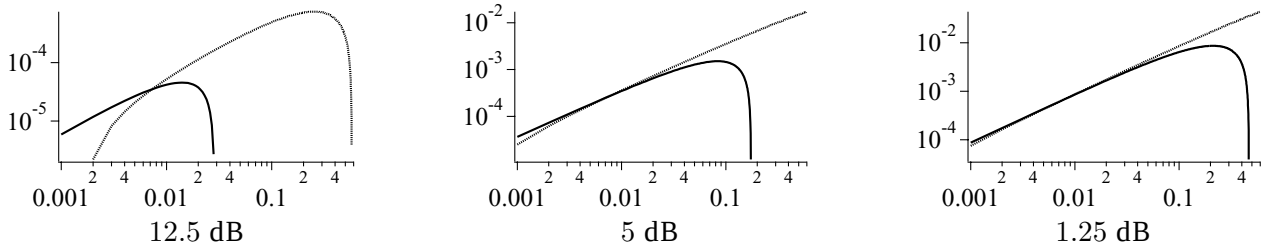


Figure 6.13: *Taux de bits secrets par impulsion pour* $12.5, 5, 1.25$ *dB de pertes en fonction du nombre moyen de photons par impulsion. Les paramètres sont ceux du tableau 6.5. Les pointillés représentent la source de photons uniques, et le trait plein la source cohérente atténuée.*

Nous avons représenté sur la figure 6.13 le taux de bits sûrs par impulsion en fonction du nombre moyen de photons par impulsion pour différentes pertes. Dans la limite de faibles pertes, (1.25 dB) il y a un faible écart entre une source de photons uniques et une source cohérente atténuée. Par contre pour des fortes pertes (> 12.5 dB) et dans la limite où $\mu < 0.03$ (domaine ou les deux sources peuvent être en compétition) les sources à photons uniques présentent un avantage quantitatif sur le taux de bits sûrs.

6.7 Analyse des performances du système réalisé

6.7.1 Confrontation théorie-expérience

Comme nous l'avons vu, la comparaison entre nos résultats expérimentaux actuels et les calculs ci-dessus est compliquée par la petite taille de la clé échangée. Nous allons d'abord donner les résultats attendus théoriquement, puis nous reviendrons sur la comparison théorie-expérience.

Nous pouvons utiliser la formule 6.11 pour évaluer notre expérience, qui est décrite par les paramètres suivants :

$$p_{exp} = 7.4 \times 10^{-3} \times 0.9, S_m = 7 \times 10^{-6}, e = 4.6 \times 10^{-2}$$

où on a tenu compte du fait que seulement 90% des photons sont détectés dans la fenêtre. Rappelons également que la valeur de S_m correspond au nombre d'impulsions doubles quittant la station d'Alice, suivant la discussion effectuée à la section 6.6.1.2.

On obtient ainsi $G^{multi} = 1.68 \times 10^{-3}$. En multipliant par le taux d'excitation de 5.3 MHz, le taux de bits secrets attendus est de 8100 bits sûrs par seconde.

Pour comparer cette valeur au résultat obtenu avec QuCrypt, nous devons estimer la connaissance d'Eve $n_a = PA(n-k)$, en supposant qu'Eve à tous les pouvoirs autorisés par la mécanique quantique. Le facteur PA est alors donné par [13, 113] :

$$PA = \frac{p_{exp} - S_m}{p_{exp}} \times log_2 \left[1 + 4e\frac{p_{exp}}{p_{exp} - S_m} - 4\left(e\frac{p_{exp}}{p_{exp} - S_m} \right)^2 \right] \tag{6.17}$$

soit $PA = 0.23$ pour les paramètres précédents. Dans le taux d'erreur on inclut aussi bien les erreurs de polarisation que les erreurs dues au taux d'obscurité, car on considère qu'Eve est capable de modifier le taux d'obscurité des détecteurs de Bob. En utilisant le programme QuCrypt nous avons ainsi obtenu 5500 ± 200 bits secrets par seconde (voir figure 6.10). On observe donc un écart significatif entre la valeur théorique et la valeur obtenue expérimentalement. Cette différence est attribuée à la taille finie de la clé échangée, qui oblige à sacrifier une trop grande fraction des bits pour estimer le taux d'erreur (dans notre cas 10% de la clé). De plus, le nombre de bits de parité qui doivent être échangés est plus important que celui prévu théoriquement par l'équation 6.9.

Le tableau ci-dessous décrit les différentes tailles de clé que nous devons obtenir en fonction de la "qualité" de l'algorithme. Ce sont les valeurs prises pour un seul run, à titre de comparaison. On définit le taux de reconciliation $R = (n-l)/n$, qui est donné par QuCrypt indique à chaque exécution du traitement.

	Theoriquement	QuCrypt sans estimation	QuCrypt avec estimation
Bits filtrés	473	473	473
Bits d'estimation	0	0	$474 * 0.1 = 47$
R	0.71	0.62	0.62
Bits de parités	127	178	160
Bits de confirmation	0	0	10
PA =0.23	$474 \times PA = 109$	$474 \times PA = 109$	$427 \times PA = 98$
Total (bit / s)	7930	6200	5300

Le tableau montre clairement que QuCrypt consomme globalement beaucoup trop de bits dans la phase de correction d'erreur. En simulant des tailles de clé plus importantes, il apparaît clairement qu'il suffit de moins de 1% des bits pour estimer le taux d'erreur, et que Cascade s'approche de son efficacité théorique donnée par la formule 6.9. Nous pouvons donc conclure que notre système fournit un taux d'environ 8000 bits secrets par seconde, qui n'a pas été atteint par le programme QuCrypt à cause de la trop petite taille de l'échantillon traité.

00001 10010 01110 01101 11011	11111 10110 00010 10100 00111
11101 00101 11000 00000 00111	10001 01111 11100 01010 11101
11100 11110 10011 00010 00100	00110 10110 00101 01011 00110
00101 10110 01011 11101 01111	0

Tableau 6.6: *Clé secrète partagé entre Alice et Bob*

6.7.2 Clé extraite

Pour conclure, la clé échangée est reprise dans le tableau 6.7.2. Pour coder un message, on regroupe la clé en bloc de 8 bits. Le tableau ASCII[8] fait la correspondance entre une lettre et un chiffre de compris entre 0 et 255 (2^8 valeurs). Alice a ainsi envoyé le message suivant "Cryptographie quantique" en utilisant la clé de chiffrement ci-dessus " o-3"hw*f*pe@c+1*"pY8IN&|% ". Le message ainsi codé correspond à la chaîne " ,@+3\X:BD/K#5J0Ex9}g4I!".

6.8 Perspectives

L'efficacité totale de notre source de photons uniques place notre prototype de cryptographie quantique dans un domaine où l'on observe un petit avantage quantitatif par rapport à un dispositif utilisant une sources cohérente atténuée. Plusieurs améliorations simples pourraient permettre d'augmenter le nombre moyen de photons polarisés par impulsion, ce qui se traduirait immédiatement par une amélioration des performances de notre source.

Premièrement, le taux de transmission du modulateur électro-optique est faible. Il n'est que de $T_{EOM} = 0.65$, et des modulateurs plus récents présentent une transmission plus élevée ($> 90\%$). Deuxièmement, le centre utilisé ici présente un taux de polarisation de 46%, et une bonne partie de la lumière ne traverse donc pas le cube polariseur. Cette valeur peut probablement être améliorée En tenant compte de ces deux effets, on peut penser augmenter le nombre moyen de photons, pour passer de $\mu = 0.014$ à $\mu = 0.027$ soit 143000 photons uniques codés par seconde.

Par ailleurs, nous pouvons placer les nanocristaux de diamant dans une microcavité pour exalter l'émission dans la direction de l'objectif. La microcavité peut aussi réduire la largeur du spectre d'émission, sans diminuer le nombre de photons émis. Ceci permettrait d'utiliser des fenêtres spectrales plus petites, et donc de mieux éliminer la lumière ambiante, tout en diminuant le taux d'erreur du modulateur. Il est raisonnable de penser que nous pouvons améliorer la source et atteindre un nombre moyen de photons de $\mu = 0.08$. Dans ce cas notre système de cryptographie quantique sera très compétitif par rapport aux sources cohérentes atténuées. De plus, on pourrait alors envisager une expérience de cryptographie quantique avec une source de photons uniques en extérieur pendant la nuit. Ceci confirmerait les possibilités de notre système pour des communications longue distance à l'air libre, comme la distribution de clés secrètes par satellite.

[8] Tableau complet sur www.asciitable.com