Influence de l'intrication en cryptographie quantique avec des variables continues

Sommaire

Nous avons démontré qu'il était possible de concevoir des protocoles de cryptographie quantique avec des états quasi-classiques (chapitre 4). Ces protocoles peuvent être simplement mis en œuvre en modulant une source laser impulsionnelle et en effectuant des mesures homodynes résolues en temps (chapitre 5). Même si aucun état intriqué n'est expérimentalement utilisé, le phénomène d'intrication quantique joue cependant un rôle essentiel dans l'analyse de la sécurité d'un protocole inverse à états cohérents. L'argument majeur dans la démonstration de sécurité est que l'espionnage d'Eve doit vérifier la relation d'Heisenberg pour toute valeur de corrélations physiquement autorisées par le champ émis par Alice, indépendamment de la technique effectivement utilisée. Ainsi, la borne supérieure sur l'information espionnée repose sur l'intrication qu'Alice et Bob *auraient* pu utiliser étant données les propriétés de leurs dispositifs quantiques, et non pas sur l'intrication effectivement utilisée.

L'objectif de ce chapitre est de discuter l'influence précise de l'intrication pour la transmission d'une clé secrète. Après la présentation détaillée et comparée d'un protocole à états intriqués (sections 6.1 et 6.2), il est démontré dans la section 6.3 que les protocoles directs et inverses de cryptographie quantique à états cohérents (sans intrication) sont équivalents à des protocoles

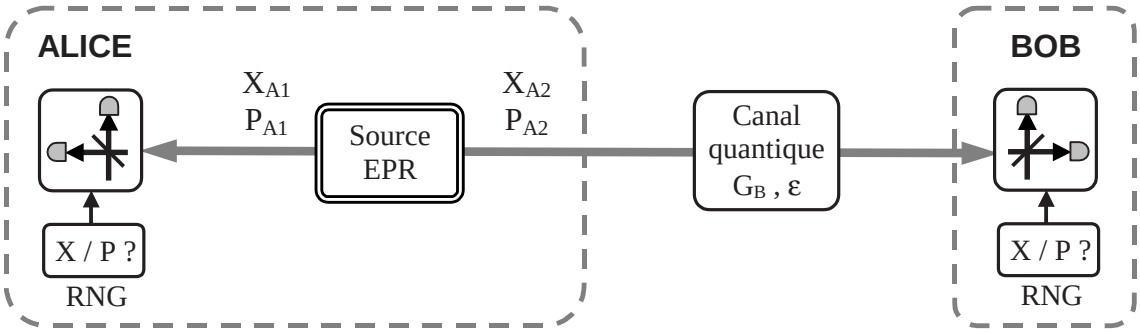

Figure 6.1: *Protocole simple à états intriqués. Un générateur de nombres aléatoires binaires (RNG : random number generator) permet d'effectuer le choix de la quadrature de mesure pour chaque impulsion incidente sur la détection homodyne.*

utilisant des états intriqués. Enfin, les critères de sécurité de nos protocoles sont comparés aux conditions de séparabilité de l'intrication pour des variables continues. La sécurité d'un protocole de cryptographie apparaît alors comme reliée à la capacité du canal à transmettre de l'intrication quantique, et non pas à l'intrication effectivement transmise [1].

6.1 Premier protocole à états EPR

Dans un protocole simple utilisant des états intriqués tel que présenté sur la figure 6.1, Alice dispose d'une source d'états EPR à deux modes dont les quadratures (X_{A1}, P_{A1}) et (X_{A2}, P_{A2}) sont de valeurs moyennes nulles. Pour chaque impulsion, Alice choisit aléatoirement de mesurer la quadrature X ou P du faisceau $A1$ tandis que le faisceau $A2$ est envoyé à Bob au travers d'un canal quantique de gain G et de bruit ajouté $\chi_B = (1-G)/G + \varepsilon$. De son côté, Bob effectue également une mesure homodyne après un choix aléatoire de la quadrature à mesurer. A la fin de l'échange d'états quantiques, Alice et Bob annoncent publiquement la direction de mesure qu'ils avaient choisie pour chaque impulsion, ce qui leur permet de supprimer les mesures où leurs directions diffèrent pour ne conserver que les mesures corrélées. Nécessairement, à ce niveau, Alice et Bob perdent environ la moitié des impulsions échangées. Ceci diminue d'un facteur 2 le débit de clé secrète mais simplifie l'analyse de la sécurité. La suite du protocole se poursuit alors comme pour le protocole à états cohérents : estimation publique des paramètres G et χ_B de la ligne, réconciliation par tranches et amplification de confidentialité.

Pour mettre ce protocole en équation, nous utilisons la représentation des états EPR par un paramètre V tel que décrit dans le tableau 2.1 de la section 2.3.5. On a alors :

$$\langle {X_{A1}}^2 \rangle = \langle {P_{A1}}^2 \rangle = \langle {X_{A2}}^2 \rangle = \langle {P_{A2}}^2 \rangle = V\, N_0 \tag{6.1}$$

$$\langle X_{A1}\, X_{A2} \rangle = \sqrt{V^2-1}\, N_0 \qquad \langle P_{A1}\, P_{A2} \rangle = -\sqrt{V^2-1}\, N_0 \tag{6.2}$$

$$V_{X_{A2}|X_{A1}} = V_{P_{A2}|P_{A1}} = \frac{N_0}{V} \tag{6.3}$$

[1] Ce travail a donné lieu à la publication [75] et a été mené postérieurement aux propositions théoriques de cryptographie avec des états cohérents [70, 74] ainsi qu'à leur réalisation expérimentale [73]. L'équivalence entre un protocole à états cohérent et un protocole utilisant de l'intrication a constitué un prérequis essentiel pour la preuve de sécurité inconditionnelle de la cryptographie inverse à états cohérents [76].

Une interprétation générale de cette source est de considérer qu'en mesurant une quadrature X_θ du mode $A1$, Alice projette le faisceau $A2$ sur un état comprimé en X_θ de variance $s\,N_0 = V_{A2|A1} = N_0/V$. L'utilisation de faisceaux intriqués garantit une compression $s = 1/V$ maximale étant donnée la modulation. On peut également relever que l'utilisation d'états intriqués assure par la même occasion la modulation du faisceau suivant une distribution gaussienne de variance V. Alice n'a alors pas besoin d'utiliser des modulateurs d'amplitude et de phase. De même, la valeur aléatoire de la modulation est directement effectuée au niveau quantique sans nécessiter une source externe classique de nombres aléatoires, qui constitue toujours un point délicat à réaliser en cryptographie.

Par exemple, une des quadratures du faisceau reçu par Bob s'écrit :

$$X_B = \sqrt{G}\,(\,X_{A2} + N_{X,B}\,) \tag{6.4}$$

où $N_{X,B}$ est un terme de bruit indépendant équivalent en entrée de variance $\chi_B\,N_0$. Ce protocole étant symétrique par rapport aux quadratures X et P, le meilleur espionnage sera lui aussi nécessairement symétrique, et on considère alors que le bruit ajouté est de même variance sur les quadratures X et P. La variance des mesures de quadratures de Bob s'écrit comme dans le cas des états cohérents :

$$\langle {X_B}^2 \rangle = V_B\,N_0 = G\,(V + \chi_B)\,N_0 \tag{6.5}$$

Dans le cas présent des états intriqués, la variance conditionnelle d'Alice sur les mesures de Bob vaut :

$$\begin{aligned} V_{B|A,EPR} = V_{X_B|X_{A1}} = V_{P_B|P_{A1}} &= \langle {X_B}^2 \rangle - \frac{\langle X_{A1}\,X_B \rangle^2}{\langle {X_{A1}}^2 \rangle} && \text{(6.6a)} \\ &= G\,(V + \chi_B)\,N_0 - G_B\,\frac{V^2 - 1}{V}\,N_0 && \text{(6.6b)} \\ &= G\,(\frac{1}{V} + \chi_B)\,N_0 && \text{(6.6c)} \end{aligned}$$

L'équation (6.6c) indique la valeur minimale de la variance conditionnelle d'Alice sur Bob étant donnée la matrice densité ρ_A de l'état transmis à Bob et la variance totale de modulation V [75]. Dans le cas de la réconciliation inverse, c'est cette valeur qui doit être utilisée pour borner l'espionnage d'Eve en saturant la relation d'Heisenberg (4.22), même si aucune intrication n'est physiquement exploitée dans le montage.

6.2 Sécurité du protocole à états EPR

6.2.1 Informations mutuelles

Pour analyser la sécurité d'un protocole à états intriqués, nous reprenons la démarche introduite au chapitre 4 et exprimons les différentes informations mutuelles entre Alice, Bob et Eve. Il faut tenir compte ici que du fait du choix aléatoire de mesure par Alice et Bob, seuls 50% des impulsions sont mesurées pour la même quadrature et seront utilisées dans l'élaboration d'une

clé secrète.

$$I_{AB,EPR} = I_{BA,EPR} = \frac{1}{2}\frac{1}{2}\log_2\left(\frac{\langle {X_B}^2\rangle}{V_{B|A,EPR}}\right) = \frac{1}{4}\log_2\left(\frac{V+\chi_B}{\frac{1}{V}+\chi_B}\right) \quad (6.7)$$

$$I_{AE,EPR} = \frac{1}{2}\frac{1}{2}\log_2\left(\frac{V+\frac{1}{\chi_B}}{\frac{1}{V}+\frac{1}{\chi_B}}\right) = \frac{1}{4}\log_2\left(\frac{\chi_B V+1}{\frac{\chi_B}{V}+1}\right) \quad (6.8)$$

$$I_{BE,EPR} = \frac{1}{2}\frac{1}{2}\log_2\left(\frac{\langle {X_B}^2\rangle}{V_{B|E,opt}}\right) = \frac{1}{4}\log_2\left(G^2\,(V+\chi_B)(\frac{1}{V}+\chi_B)\right) \quad (6.9)$$

On peut remarquer à ce niveau que la variance conditionnelle optimale d'Eve sur les données de Bob est la même avec des états EPR qu'avec des états cohérents. Ceci provient du fait que l'on considère toujours un espionnage maximal selon la physique autorisée par la relation d'Heisenberg (4.22), indépendamment de la nature physique exacte des états employés.

6.2.2 Réconciliation directe

Un protocole de réconciliation directe est sûr si $I_{AB} > I_{AE}$ [50] et le taux de transfert secret vaut au moins :

$$\underrightarrow{\Delta I}_{EPR} = I_{AB,EPR} - I_{AE,EPR} = \frac{1}{2}\log_2\left(\frac{V+\chi_B}{\chi_B\,V+1}\right) = \underrightarrow{\Delta I}_{coh} \quad (6.10)$$

On retrouve ici le taux de transfert $\underrightarrow{\Delta I}_{coh}$ obtenu pour les protocoles directs à états cohérents. La condition de sécurité est alors la même : $\chi_B < 1$, ce qui n'est possible que pour des transmissions supérieures à 50%.

D'une manière générale, on peut montrer que le taux de transfert en réconciliation directe ne dépend pas du facteur de compression utilisé [70, 71]. Il faut cependant noter que l'on considère seulement des protocoles simples à états EPR, où Alice et Bob ne s'accordent pas sur le choix de quadrature une impulsion sur deux en moyenne. Si Alice et Bob pouvaient s'accorder de manière déterministe et secrète sur la quadrature à mesurer, le taux de transfert serait alors doublé dans le cas d'un protocole EPR (théoriquement, il suffirait que Bob puisse disposer d'une mémoire quantique parfaite identique à celles utilisées par Eve pour attendre qu'Alice révèle sa direction de mesure). On pourrait imaginer qu'Alice et Bob se servent d'une clé secrète aléatoire préétablie entre eux pour déterminer leur choix de mesure. Dans ce cas, le taux de transfert secret vaudrait $2\underrightarrow{\Delta I}_{coh} - 1$ pour tenir compte du bit de codage de la direction de mesure consommé par chaque impulsion.

Une autre possibilité serait de faire varier la répartition entre les mesures de quadratures pour privilégier une certaine direction : Alice et Bob mesurent par exemple aléatoirement la quadrature X avec une probabilité ξ ($\approx 90\%$)et la quadrature P avec une probabilité $1-\xi$. Dans ce cas, Alice et Bob s'accordent sur le choix de quadrature mesurée à hauteur d'une portion $\xi^2 + (1-\xi)^2$ des impulsions échangées. Le taux de transfert avec des états EPR serait alors de $2\left[\xi^2 + (1-\xi)^2\right]\underrightarrow{\Delta I}_{coh}$. Le point délicat dans l'analyse de la sécurité est qu'alors il n'est pas immédiat de prouver que la meilleure attaque d'Eve est une attaque symétrique. Par ailleurs, Eve pourrait également modifier la statistique de la répartition entre les quadratures.

6.2.3 Réconciliation inverse

Le taux de transfert secret en réconciliation inverse est donné par :

$$\underleftarrow{\Delta I}_{EPR} = I_{BA,EPR} - I_{BE,EPR} = -\frac{1}{2}\log_2\left(G\,(\chi_B + \frac{1}{V})\right) \quad (6.11)$$

Ce terme est positif et le protocole est sûr à la condition $G(\chi_B + 1/V) < 1$, ce qui est possible pour toute valeur de la transmission de la ligne et s'écrit en fonction du bruit ajouté ε :

$$\textit{Sécurité protocole EPR inverse} \Leftrightarrow \varepsilon < \frac{V-1}{V} \approx 1 \tag{6.12}$$

Un protocole inverse à états EPR est donc plus robuste à un excès de bruit qu'un protocole à états cohérents qui ne peut tolérer que $\varepsilon < (V-1)/2V \approx 1/2$.

On peut comparer le taux de transfert avec des états EPR au cas des états cohérents :

$$\underleftarrow{\Delta} I_{coh} = -\frac{1}{2}\log_2\left(G^2\,(1+\chi_B)\,(\frac{1}{V}+\chi_B)\right) \tag{6.13a}$$

$$= \underleftarrow{\Delta} I_{EPR} - \frac{1}{2}\log_2\left(G\,(1+\chi_B)\right) \tag{6.13b}$$

$$= \underleftarrow{\Delta} I_{EPR} - \frac{1}{2}\log_2\left(1+G\,\varepsilon\right) \tag{6.13c}$$

D'une manière générale on a alors :

$$\underleftarrow{\Delta} I_{coh} \leq \underleftarrow{\Delta} I_{EPR} \tag{6.14}$$

avec égalité si l'excès de bruit ε est nul. Dans un cas où tout le bruit ajouté provient exclusivement des pertes, l'utilisation de l'intrication n'améliore donc pas le taux de transfert secret pour ce type de protocole.

Même si les protocoles simples à états intriqués présentent des taux de transfert sensiblement identiques à un protocole à états cohérents, ils offrent néanmoins certains avantages spécifiques, liés à l'utilisation physique de l'intrication. Les quantités d'information espionnées I_{AE} et I_{BE} sont plus faibles dans le cas EPR que dans le cas des états cohérents. La procédure d'amplification de confidentialité est donc plus simple et plus robuste à mettre en œuvre. De plus, le dispositif expérimental à états intriqués est aussi dispensé d'une source aléatoire externe de modulation continue. Ceci constitue une particularité importante pour un système de cryptographie, où la qualité des sources classiques de nombres aléatoires est toujours un point délicat. Enfin, un avantage quantique spécifique des protocoles EPR est qu'il est possible d'envisager l'utilisation de protocoles de distillation de l'intrication pour augmenter la portée de distribution pratique.

Nous introduisons maintenant un second protocole à états EPR, dont l'étude apporte un éclairage nouveau sur l'influence de l'intrication dans la sécurité quantique.

6.3 Intrication virtuelle et états cohérents

Une autre possibilité pour Alice d'utiliser des états intriqués est de mesurer simultanément les quadratures X_{A1} et P_{A1} de son faisceau (voir la figure 6.2). Une telle mesure simultanée peut se faire par exemple en divisant le faisceau sur une lame séparatrice de réflectivité 50% puis en effectuant une mesure homodyne de chaque bras. Ces mesures sont alors notées $\overline{X}_A$ et $\overline{P}_A$ et suivent une distribution gaussienne de variance $\langle \overline{X}_A{}^2 \rangle = \langle \overline{P}_A{}^2 \rangle = \frac{V+1}{2} N_0$.

Par rapport à l'autre faisceau (X_{A2}, P_{A2}) en sortie de la source, les mesures d'Alice fournissent les informations :

$$\langle \overline{X}_A\, X_{A2} \rangle = -\langle \overline{P}_A\, P_{A2} \rangle = \sqrt{\frac{V^2-1}{2}}\, N_0 \tag{6.15}$$

$$V_{X_{A2}|\overline{X}_A} = V_{P_{A2}|\overline{P}_A} = V\, N_0 - \frac{(V^2-1)/2}{(V+1)/2}\, N_0 = N_0 \tag{6.16}$$

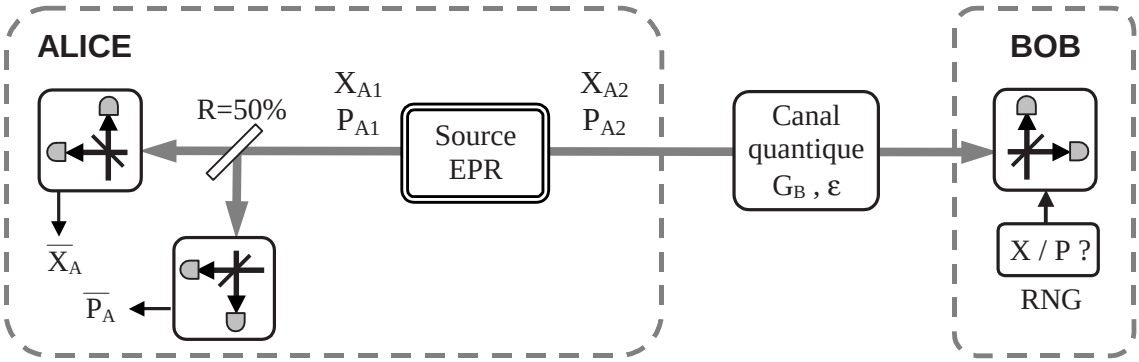

Figure 6.2: *Protocole symétrique à états intriqués : Alice divise son faisceau EPR en deux parties qu'elle mesure avec une détection homodyne, ce qui fournit les résultats* $(\overline{X}_A, \overline{P}_A)$ *pour chaque impulsion.*

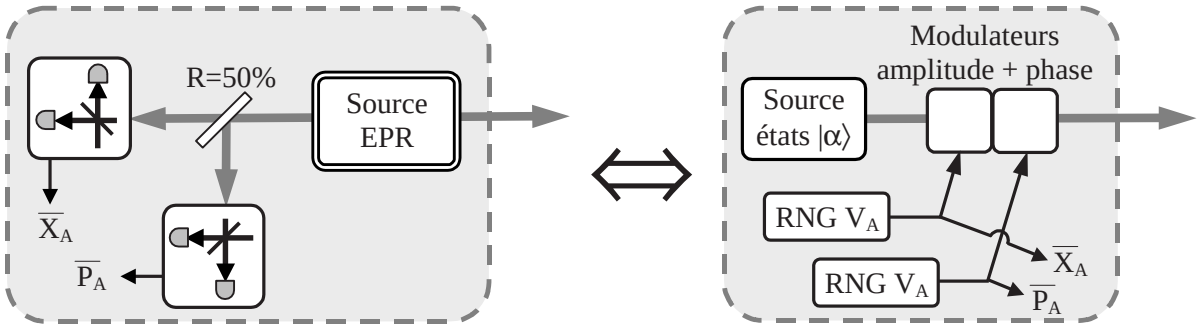

Figure 6.3: *Sources équivalentes pour la cryptographie quantique(avec ou sans intrication réelle). RNG* V_A *désigne un générateur parfait de nombre aléatoire suivant une distribution gaussienne de variance* V_A*.*

En d'autres termes, la mesure simultanée d'Alice projette l'état $A2$ en un état cohérent. Les valeurs moyennes des quadratures sont proportionnelles aux résultats d'Alice $(\overline{X}_A, \overline{P}_A)$ et avec une incertitude fixée au bruit de photon N_0, comme si Alice avait préparé un état cohérent modulé suivant une distribution gaussienne (voir la figure 6.3).

Par rapport aux mesures de Bob (X_B, P_B), Alice dispose des corrélations :

$$\langle \overline{X}_A \, X_B \rangle = -\langle \overline{P}_A \, P_B \rangle = \sqrt{\frac{G}{2}} \sqrt{V^2 - 1} \, N_0 \tag{6.17}$$

$$\begin{aligned} V_{B|A,EPR} = V_{X_B|\overline{X}_A} = V_{P_B|\overline{P}_A} &= G\,(V + \chi_B)\,N_0 - G\,\frac{V^2-1}{V+1}\,N_0 \\ &= G\,(1 + \chi_B)\,N_0 \\ &= V_{B|A,coh} \end{aligned} \tag{6.18}$$

Dans le cas présent, Alice ne possède ainsi pas davantage d'information sur la mesure de Bob que dans le cas d'un état cohérent modulé.

Supposons que l'ensemble de la source d'Alice soit placé dans une boîte noire. Les seuls éléments émergeant de cette boîte sont le faisceau (X_{A2}, P_{A2}) et les valeurs $\overline{X}_A$ et $\overline{P}_A$. Cette boîte noire n'est alors pas distinguable d'une autre boîte noire, représentée sur la figure 6.3, où les nombres $\overline{X}_A$ et $\overline{P}_A$ sont choisis par un générateur aléatoire gaussien de variance adéquate et le faisceau émergent (X_{A2}, P_{A2}) est issu d'une source d'états cohérents modulés.

Nous appelons cette possibilité l'*intrication virtuelle* [75] : même si Alice n'utilise pas effectivement d'intrication pour générer ses états cohérents modulés, il existe un dispositif absolument équivalent (la boîte noire présentée sur la figure 6.3) qui utilise l'intrication quantique. Cette affirmation s'appuie sur le fait que la sortie de tout appareil physique, y compris le système d'espionnage d'Eve, ne peut dépendre que de la matrice densité de ses entrées (ici le faisceau émis par Alice) et non pas de la manière dont ces entrées ont été préparées. La sécurité d'un protocole de cryptographie apparaît alors comme reliée à la capacité du canal à transmettre de l'intrication quantique, et non pas à l'intrication effectivement transmise, comme nous allons le souligner plus précisément à la section suivante.

6.4 Critères de sécurité et de séparabilité

6.4.1 Séparabilité d'une intrication en quadratures

Si le canal quantique entre Alice et Bob est de trop mauvaise qualité, l'*intrication virtuelle* entre (X_{A1}, P_{A1}) et (X_B, P_B) sera détruite. Le seuil à partir duquel cet effet intervient peut être calculé en utilisant le critère de séparabilité de Duan et Simon pour les variables continues d'un état gaussien à deux modes [134, 135]. D'après l'équation (17) de la référence [134], le critère pour que l'état entre Alice et Bob présente toujours de l'intrication virtuelle s'écrit :

$$(\langle {X_{A1}}^2 \rangle - N_0)\,(\langle {X_B}^2 \rangle - N_0) < \langle X_{A1}\, X_B \rangle^2 \tag{6.19}$$

avec

$$\langle {X_{A1}}^2 \rangle = V\, N_0 \tag{6.20a}$$

$$\langle {X_B}^2 \rangle = G\,(V + \frac{1-G}{G} + \varepsilon)\, N_0 \tag{6.20b}$$

$$\langle X_{A1}\, X_B \rangle = \sqrt{G}\,\sqrt{V^2-1}\, N_0 \tag{6.20c}$$

Dans notre cas, le critère (6.19) devient :

$$G(V-1)(V-1+\varepsilon) < G(V-1)(V+1) \tag{6.21}$$

Ce qui se formalise en le résultat :

$$Non - séparabilité\ \ Duan - Simon \Leftrightarrow \varepsilon < 2 \tag{6.22}$$

L'intrication virtuelle est donc présente dès que la modulation et la transmission de la ligne sont non-nulles ($V > 1$ et $G > 0$), à la seule condition que l'excès de bruit ajouté par le canal ne dépasse pas le seuil de deux fois le niveau de bruit de photon N_0.

6.4.2 Comparaison aux critères de sécurité

Le tableau 6.1 résume les différents critères de sécurité pour nos protocoles de cryptographie en fonction de l'excès de bruit ε de la ligne. Pour les protocoles directs, à états cohérents ou

intriqués, le critère de sécurité impose $\varepsilon < 1$ de telle sorte que la condition d'intrication virtuelle (6.22) est toujours vérifiée. Pour les protocoles inverses, la condition de sécurité requiert $\varepsilon < 1/2$ pour les états cohérents et $\varepsilon < 1$ pour les états EPR, et ainsi la condition de non-séparabilité $\varepsilon < 2$ est également toujours vérifiée. Ces résultats sont présentés sur la figure 6.4, où la condition d'intrication est comparée à nos seuils de sécurité. Il apparaît alors clairement que les zones de sécurité des différents protocoles directs et inverses sont nettement à l'intérieur de la zone d'intrication, où le canal quantique peut distribuer de l'intrication utile.

Protocole	**Direct**	**Inverse**
Etats cohérents	$\varepsilon < 2 - \frac{1}{G}$	$\varepsilon < \frac{V-1}{2V} \approx \frac{1}{2}$
Etats intriqués	$\varepsilon < 2 - \frac{1}{G}$	$\varepsilon < \frac{V-1}{V} \approx 1$

Tableau 6.1: *Conditions de sécurité des protocoles de cryptographie quantique à variables continues [70, 73] pour un canal de gain G et de bruit équivalent en entrée $\chi_B = (1-G)/G + \varepsilon$, où ε désigne l'excès de bruit non-lié aux pertes.*

Le seuil de non-séparabilité $\varepsilon = 2$ correspond physiquement au cas d'un espionnage de type *intercept-resend* [63] où Eve divise le faisceau $A2$ provenant d'Alice en deux parties pour effectuer une mesure simultanée des quadratures X et P et ré-émettre un faisceau cohérent centré sur le résultat de ses mesures. Eve doit alors supporter le coût d'un bruit en entrée d'une fois le bruit de photon N_0 ("taxe quantique" selon [146]) pour la mesure simultanée de X et P, puis une deuxième "taxe quantique" N_0 au niveau de la ré-émission de l'état cohérent. Le bruit ajouté du côté de Bob (en plus du bruit de photon) sera alors de $2\,N_0$, soit $\varepsilon = 2$ [63]. En d'autres termes, au niveau où l'état conjoint d'Alice et Bob devient séparable ($\varepsilon = 2$), il existe une attaque explicite d'espionnage, ce qui interdit l'existence de tout protocole sûr de cryptographie.

La région entre la condition de non-séparabilité et la limite de sécurité des protocoles EPR connus, $1 < \varepsilon < 2$ correspond à une région où le canal quantique peut toujours transmettre de l'intrication, mais où les protocoles connus ne sont plus sûrs. L'existence même de protocoles sûrs opérant dans cette région reste pour le moment une question ouverte. La différence entre nos conditions de sécurité et la condition d'intrication semble indiquer que nos protocoles n'utilisent pas efficacement toutes les ressources d'intrication disponible. En principe, des procédures basées sur la purification quantique de l'intrication [1], ou sur la distillation classique de l'avantage (*advantage distillation* [55]) permettent d'exploiter l'intrication jusqu'à ses limites ultimes, mais ces procédures soit sont très difficiles à mettre en œuvre expérimentalement (purification quantique), soit proposent des débits de clé secrète extrêmement bas (distillation classique). Une seconde question ouverte est de déterminer l'origine de la différence entre les seuils de sécurité et d'intrication. Est-ce que cet effet provient des observables de mesure limitées, de la procédure d'extraction de bits ou bien d'un autre phénomène ?

Enfin, nous pouvons également nous intéresser à un autre critère caractérisant l'intrication, énoncé par Reid et Drummond [133]. Ce critère, plus restrictif que celui de Duan-Simon (6.19), caractérise la violation du "paradoxe" Einstein-Podolsky-Rosen (voir le chapitre 10) :

$$V_{X_B|X_{A1}}\, V_{P_B|P_{A1}} < {N_0}^2 \tag{6.23}$$

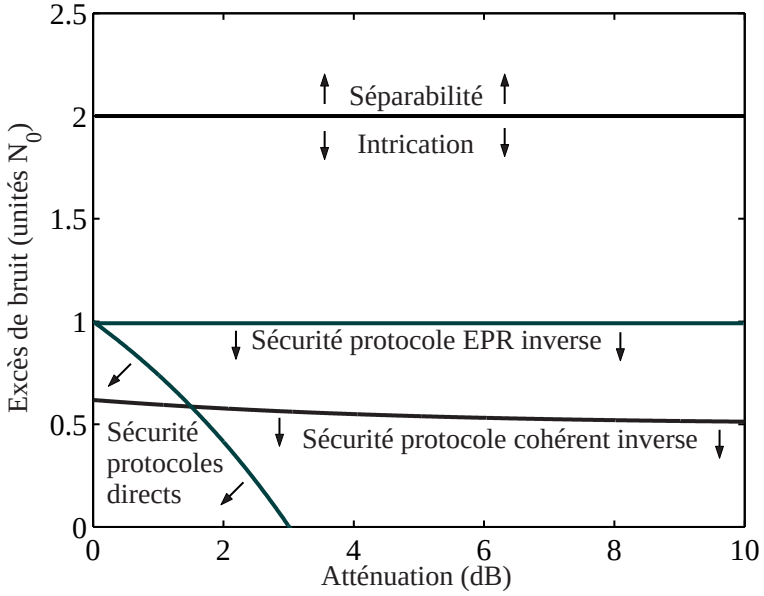

Figure 6.4: *Excès de bruit ε en fonction de l'atténuation de la ligne $-10\log_{10} G$, dans le cas des fortes modulations ($V \gg 1$).*

Pour le cas du protocole à intrication réelle vu à la section 6.1, on a $V_{X_B|X_{A1}} = V_{P_B|P_{A1}} = G(\chi_B + 1/V)N_0$ et le critère de Reid-Drummond devient :

$$G\,(\frac{1-G}{G} + \varepsilon + \frac{1}{V}) < 1 \tag{6.24}$$

soit

$$\varepsilon < \frac{V-1}{V} \tag{6.25}$$

ce qui correspond exactement à la limite de sécurité de nos protocoles inverses à états intriqués.

Pour le cas des protocoles à intrication virtuelle, $V_{X_B|X_{A1}} = V_{P_B|P_{A1}} = G(\chi_B + 1)N_0$. Le critère de Reid-Drummond (6.23) s'écrit alors $1 + G\varepsilon < 1$, ce qui trivialement ne peut pas être vérifié pour G et $\varepsilon \geq 0$. Ce résultat était tout à fait prévisible : dans le cas de l'intrication virtuelle, Alice et Bob ne possèdent pas davantage d'information que dans le cas où Alice utilise des états cohérents déplacés, qui ne présentent aucune intrication physique et ne peuvent prétendre violer le paradoxe EPR (6.23). Cependant, même si le protocole à intrication virtuelle ne vérifie pas la condition d'intrication de Reid-Drummond, ce protocole peut tout de même être sûr si $\varepsilon < 1/2$. Les conditions de sécurité suivent donc une intrication virtuelle qui pourrait être présente, mais n'est pas réellement utilisée...

6.5 Conclusion

Nous avons démontré dans ce chapitre le résultat qu'un protocole à états cohérents pouvait être considéré comme complètement équivalent à un protocole utilisant des états intriqués. Par ailleurs, les conditions de sécurité de nos protocoles à états cohérents sont nettement dans le domaine de la non-séparabilité de l'intrication au sens de Duan et Simon. Ces résultats ont

offert une nouvelle compréhension du lien entre la sécurité quantique et l'usage de l'intrication, et ont contribué aux preuves ultérieures de sécurité inconditionnelle de nos protocoles [76, 77].

L'équivalence dans le domaine des variables continues entre un protocole à états cohérents et un protocole à états intriqués n'est pas sans rappeler l'analogie présentée dans [45] pour les variables discrètes entre le protocole sans intrication BB84 [43] et le protocole EPR proposé par Ekert [44]. L'étude du lien entre la sécurité et l'intrication a été poussée plus loin par Acin et ses collaborateurs [49], qui démontrent une équivalence complète dans le cas des variables quantiques discrètes entre l'intrication de deux qubits et la sécurité d'un protocole de distribution de clé : une clé secrète peut être échangée de manière sûre au travers d'un canal quantique si et seulement si ce canal permet la distribution de l'intrication.

Si dans le domaine des variables continues nos preuves de sécurité ne possèdent pas encore ce recul, il serait cependant faux de conclure de cette étude que l'utilisation réelle de faisceaux EPR ne présente aucun intérêt pour la cryptographie quantique. Comme nous l'avons vu lors de la réalisation expérimentale des protocoles à états cohérents (chapitre 5), l'usage des variables continues avec des états cohérents ne permet pas d'envisager des portées de transmission plus grandes que celles des protocoles à photons uniques. Du fait de l'absorption exponentielle dans une fibre optique, les protocoles actuels atteignent une limite en distance de transmission entre 10 et 100km. Au-delà de cette distance, les bits secrets sont noyés dans diverses erreurs, qui vont des coups d'obscurité des détecteurs à un traitement imparfait des données. Pour dépasser ces distances et améliorer la situation actuelle, un défi expérimental majeur serait de mettre en œuvre des procédures de distillation de l'intrication pour réaliser un répéteur quantique [160]. De façon ultime, les bits secrets seraient simplement téléportés dans la station réceptrice avec laquelle un partage d'intrication quantique aurait été préalablement effectué [158]. Pour toutes ces propositions de distribution de clé à longue distance, l'utilisation réelle de l'intrication et des états EPR apparaît comme un prérequis essentiel : sans intrication, aucune distillation quantique n'est évidemment envisageable. Cet état de fait nous a donc conduit à développer un dispositif expérimental de génération d'états spécifiquement quantiques, en vue de futures applications pour des protocoles de communication quantique à longue distance. La description de ce dispositif et de ses applications fera l'objet de la prochaine partie de cette thèse.